Relatório de Riscos e Tendências da IBM X-Force 2011

Março de 2012

Colaboradores

O Relatório de Riscos e Tendências da IBM X-Force é resultado de um trabalho colaborativo envolvendo toda a IBM. Gostaríamos de agradecer as pessoas a seguir por sua atenção e contribuição na publicação deste relatório.

Colaborador	Cargo
Bryan Casey	Market Manager, IBM Security Systems
Carsten Hagemann	X-Force Software Engineer, Content Security
Colin Bell	Security Solution Architect, Lab Services & Support, IBM Security Systems
Clay Blankenship	Senior Incident Response Analyst
Cynthia Schneider	Information Developer
David McMillen	Security Intelligence Analyst, IBM Security Services
David Merrill	STSM, IBM Chief Information Security Office, CISA
Dr. Jens Thamm	Database Management Content Security
Dr. Ashok Kallarakkal	Sr. Manager, Product Management and Beta Ops
Gina Stefanelli	X-Force Marketing Manager
Jason Kravitz	Techline Specialist for IBM Security Systems and E-Config
John C. Pierce	Threat Intelligence Analyst, AI, MSS
John Kuhn	Security Intelligence Analyst, IBM Security Services
Kimberly Madia	Data Security Strategy, InfoSphere Guardium & Optim
Leslie Horacek	X-Force Threat Response Manager
Marc Noske	Database Administration, Content Security

Colaborador	Cargo
Mark E. Wallis	Senior Information Developer, IBM Security Systems
Marne Gordan	Regulatory Analyst, IBM Security Systems
Michael Applebaum	Director of Product Marketing, Q1 Labs
Michael Montecillo	Managed Security Services Threat Research and Intelligence Principal
Michelle Alvarez	Manager, MSS Global Operations
Paul Sabanal	X-Force Advanced Research
Phil Neray	Q1 Labs Marketing Leader, IBM Security Systems
Ralf Iffert	Manager X-Force Content Security
Randy Burton	Senior Incident Response Analyst
Robert Lelewski	Senior Incident Response Analyst
Ron Black	Senior Incident Response Analyst
Ryan Berg	Cloud Security Strategy Lead
Scott Moore	X-Force Software Developer and X-Force Database Team Lead
Shane Garrett	Team Lead, X-Force Advanced Research
Tom Cross	Manager, X-Force Strategy and Threat Intelligence
Veronica Shelley	Segment Marketing Manager IBM Security Systems

Sobre a X-Force

As equipes de pesquisa e desenvolvimento da IBM X-Force® estudam e monitoram as tendências mais recentes de ameaças, incluindo vulnerabilidades, explorações e ataques ativos, vírus e outros malwares, spams, phishing e conteúdo malicioso da web. Além de orientar os clientes e o público em geral sobre as ameaças emergentes e críticas, a X-Force também fornece conteúdo de segurança para ajudar a proteger os clientes IBM dessas ameaças.

DEDICATÓRIA

O Relatório de Riscos e Tendências da IBM X-Force 2011 é dedicado à memória de nossa amiga e colega de trabalho ***Marne Gordon****, que faleceu durante sua produção. Regulatory Analyst da equipe de estratégia de segurança da Divisão de Segurança da IBM, o conhecimento e o foco de Marne sobre a segurança das nuvens e da mídia social são apresentados neste relatório. Ela era palestrante frequente em eventos do segmento de mercado e publicou diversos artigos sobre os tópicos de segurança e conformidade. Marne e as contribuições que fez à segurança, à conformidade e à IBM serão lembradas com muita saudade.*

Colaboração da IBM Security

A IBM Security representa diversas marcas que oferecem um amplo espectro da competência da segurança.

- Enquanto as equipes de pesquisa e desenvolvimento da X-Force estão ocupadas analisando as tendências e métodos mais recentes utilizados pelos invasores, os outros grupos da IBM utilizam estes dados ricos para desenvolver técnicas de proteção aos clientes.
- A equipe de pesquisa e desenvolvimento da IBM X-Force descobre, analisa, monitora e registra uma grande variedade de ameaças e vulnerabilidades à segurança dos computadores.
- Os Serviços Gerenciados de Segurança (MSS) da IBM são responsáveis pelo monitoramento de explorações relacionado aos terminais, servidores (incluindo servidores da web) e pela infraestrutura geral de rede. Os MSS controlam as explorações realizadas pela web e outros vetores, como emails e mensagens instantâneas.
- Os Serviços Profissionais de Segurança (PSS) fornecem serviços de avaliação, design e implementação de segurança em toda a empresa para ajudar a desenvolver soluções efetivas de segurança das informações.
- A equipe de segurança de conteúdo da IBM X-Force pontua e categoriza a web de modo independente por meio de crawling, descobertas independentes e por meio dos feeds fornecidos pelos MSS.
- A IBM reuniu dados reais de vulnerabilidade dos testes de segurança realizados nos últimos anos pelo IBM AppScan® OnDemand Premium Service. Este serviço combina os resultados de avaliações de segurança de aplicativos obtidos do IBM AppScan aos testes e verificações manuais de segurança.
- A IBM Security Services oferece suporte à nuvem de duas maneiras: Serviços de Segurança para Nuvem, que ajudam os clientes a começarem sua jornada à nuvem fornecendo experiência em segurança e Segurança a partir de um modelo baseado em nuvem que ajuda a reduzir os custos e a complexidade, melhorar a postura de segurança e atender os requisitos de conformidade.
- As soluções de gerenciamento de identidade e acesso da IBM permitem que as organizações centralizem e automatizem de modo eficiente o gerenciamento de perfis de identidade e privilégios de acesso dos usuários autorizados. Estas soluções podem reforçar ainda mais a segurança com sólidas ferramentas de autenticação, sign on único e auditoria/relatórios, a fim de monitorar a atividade de acesso dos usuários.
- As soluções de segurança de dados e informações da IBM fornecem recursos para ajudar a proteger o gerenciamento de dados e de acesso e abordar a segurança do ciclo de vida de informações em toda a empresa.
- A IBM InfoSphere® Guardium® fornece uma solução corporativa escalável para segurança e conformidade de bancos de dados que pode ser rapidamente implementada e gerenciada com recursos mínimos.
- A Plataforma de Inteligência de Segurança QRadar da Q1 Labs, uma Empresa IBM, oferece uma solução integrada para SIEM, gerenciamento de logs, gerenciamento de configuração e detecção de anomalias. Ela fornece um painel unificado e insights em tempo real sobre os riscos de segurança e de conformidade relacionados às pessoas, aos dados, aos aplicativos e à infraestrutura.

Índice
Seção I

Colaboradores	**2**
Sobre a X-Force	2
Colaboração da IBM Security	3
Seção I – Ameaças	**6**
Visão geral executiva	**6**
Destaques de 2011	**8**
Ameaças	8
Infraestrutura operacional segura	9
Prática de segurança de desenvolvimento de software	10
Tendências emergentes em segurança	10
2011 – Ano da violação de segurança	**12**
De meados do ano ao novo ano – a violação continua	12
Alteradores de cenário do segundo semestre de 2011	13
Lições aprendidas	14
O caminho para o futuro	15
Serviços Gerenciados de Segurança da IBM – Uma paisagem global de ameaças	**16**
MSS – Principais assinaturas de alto volume de 2011	**16**
A ameaça contínua da injeção de SQL	**27**
Injeção de SQL	27
A natureza da ameaça	28
Ajudando a proteger seu código	29
Ajudando a proteger seu servidor	30
Ajudando a proteger sua rede	31
Conclusão	32
Desafios à segurança do SSL	**33**
THC-SSL-DOS	33
A troca do TLS	33
Mitigação	34
A BEAST	35
Mitigação	36
Comprometimentos da DigiNotar e Comodo	36
Revogação de certificados	37
Modelo de confiança do SSL	37
Problemas com o modelo de confiança do SSL	38
Revisando a confiança do SSL	38
O que o futuro reserva?	39
O surgimento de malwares de Mac	**39**
Introdução	39
MacDefender	39
Flashback	40
DevilRobber	41
Conclusão	41
Tendências de conteúdo da web	**43**
Metodologia de análise	43
Implementação de IPv6 para websites	43
Aumento de proxies anônimos	44
Websites maliciosos	46
Spams e phishing	**49**
O volume de spams continua a cair	49
Principais tendências de spam em 2011	50
Principais domínios comuns dos spams de URL, incluindo tendências de longo prazo	53
Spam – país de tendências originadoras	55
Scams e phishing de email	56
Evolução dos spams	61
Prospectos futuros sobre os spams	65

Índice
Seção II, III e IV

Seção II – Práticas Operacionais de Segurança	**66**
Apresentando a Inteligência de Segurança: Uma abordagem integrada à segurança em tempo real	**66**
Definindo a Inteligência de Segurança	66
A analogia com a Inteligência de Negócios	67
Os princípios da Inteligência de Segurança	68
Como a Inteligência de Segurança difere do SIEM?	69
Quais são os principais benefícios?	70
Melhores práticas de Inteligência de Segurança	72
Conclusão	73
Divulgações de vulnerabilidades em 2011	**74**
Aplicativos da web	74
Reduções das explorações	78
Invasores que mudam para novas áreas de foco	82
Vulnerabilidades dos softwares corporativos	84
Engenharia social de mídia social: Como os invasores fazem isso?	**89**
Visão geral	89
Coleção de inteligência	90
Coleção de inteligência de software livre	90
Como funciona – não é um bicho de sete cabeças	91
Etapas que as organizações podem realizar para mitigar os riscos de mídia social	93
Tendências futuras	96
Dez principais erros comuns de CSIRP	**97**
Resposta aos incidentes – preparando sua infraestrutura para respostas em escala	**100**
Preparação: A base sólida de todas as respostas aos incidentes	101
Não registrar causa mais danos	101
A automação é sempre sua melhor amiga	103
Finalmente e mais importante: A autenticação	104
Trabalhe de modo mais inteligente e faça bons amigos	104
Segurança e privacidade de dados, entendendo as diferenças para ajudar a realizar a conformidade-	**105**
Dando sentido à confusão: Por que há um crescente foco sobre a proteção de dados?	106
Alterações nos ambientes de TI e iniciativas de negócios em evolução	106
Invasores mais inteligentes e sofisticados	106
Mandatos de conformidade	106
Aproveitando uma abordagem holística de segurança e privacidade de dados	108
Uma abordagem de três camadas para assegurar a proteção de dados holística	109
Seção III – Práticas de Segurança de Desenvolvimento de Software	**111**
Conclusões das avaliações de aplicativos da web reais	**111**
Metodologia	111
Pontos métricos	112
Tendências de vulnerabilidades dos aplicativos em 2011	113
Tendências anuais (2007 – 2011)	114
Segmentos de negócios	116
Ciclo de testes de segurança dos aplicativos	118
Seção IV – Tendências Emergentes em Segurança	**120**
Segurança móvel e a empresa – um ano em revisão	**120**
Perspectiva de malwares móveis	121
BYOD e o isolamento seguro	123
A importância da convergência do gerenciamento de dispositivos em empresas com base em funções	124
Uma análise retrospectiva do estado de segurança da nuvem	**126**
Adotando segurança para a nuvem	127
Considerações sobre o design	127
Considerações sobre a implementação	127
Considerações sobre o consumo	128
Melhorando a segurança da nuvem por meio de ANSs	**128**
Introdução	128
Problemas a serem considerados	128
Conclusão	131
Gerenciamento de identidade e acesso na nuvem	**131**
Desafios de segurança nos ambientes de nuvem	131

Seção I
Ameaças

Nesta seção, serão explorados tópicos relacionados às ameaças e serão descritos muitos ataques corporativos enfrentados pelos especialistas em segurança. Discutiremos a atividade maliciosa observada no espectro da IBM e o modo como ajudamos a proteger as redes dessas ameaças. Além disso, serão apresentadas informações atualizadas sobre as tendências de ataques mais recentes identificadas pela IBM.

Visão geral executiva

2011 foi um ano notável para a segurança de TI. Até o meio do ano, entre relatórios frequentes de vazamentos de dados, ataques DOS e atividade de hackers na mídia social, a IBM X-Force declarou que 2011 foi o "ano da violação de segurança". Até o final do ano, a frequência e o escopo destes incidentes persistiram e continuam a gerar reconhecimento sobre os princípios básicos da operação de um negócio e da proteção de seus ativos em um mundo cada vez mais conectado. O número absoluto de incidentes de alto perfil e altamente públicos de 2011 foi um catalisador para que os executivos e líderes de negócios reavaliassem a eficácia das estruturas, políticas e tecnologias existentes nas empresas.

Com qualquer grande desafio, surgem grandes oportunidades de aprendizagem e melhoria. Embora as empresas tenham sido rápidas em divulgar a ocorrência de uma violação e o seu possível impacto sobre seus clientes, pouco se diz em relação a como a violação ocorreu e o que poderia ter sido feito para impedi-la. Uma dificuldade encontrada no segmento de mercado de segurança está relacionada ao modo de divulgar uma violação com responsabilidade, a fim de que os detalhes técnicos possam ajudar a assegurar que os outros negócios não sejam afetados de modo similar. Neste relatório, refletiremos sobre o que pode ser identificado nesses infelizes incidentes e como podemos realizar uma etapa afirmativa de comunicação das informações da violação para contribuir com uma cultura de divulgação benéfica para o futuro.

Por meio da divulgação de violações ocorridas, ainda se vê a injeção de SQL como um ponto de entrada preferencial dos invasores. Os ataques de injeção automatizada de SQL, como LizaMoon, estão escaneando a Internet com êxito e explorando os hosts vulneráveis. Estes ataques de injeção de SQL têm sido comuns há muito tempo. Recentemente, também começamos a ver um aumento dos ataques que visam às vulnerabilidades de injeção de comandos Shell. Até o final de 2011, a X-Force observou de duas a três vezes mais atividades de ataque de injeção de comandos Shell em relação ao ano anterior. Também foram observados grandes aumentos de atividades de quebra de senhas SSH quase ao final de 2011.

Houve novos ataques sem precedentes, como o comprometimento de diversas autoridades de certificação. Este tipo de ataque violação uma confiança básica dos usuários – a confiança de que visitar uma página criptografada SSL significa uma comunicação segura. Os métodos antigos de ataque, como os ataques tradicionais de phishing e spam, estão sendo substituídos por métodos novos de implementação de malware. Os ataques de mídia social estão aumentando e ela tem se tornado um alvo principal dos invasores, que estão transgredindo com êxito o círculo de confiança de seus alvos infiltrando seus amigos e seguidores.

Apesar dessas dificuldades, ao longo deste relatório, também foram observadas algumas tendências e melhorias positivas. O número total de vulnerabilidades relatadas de aplicativos de web é menor em relação a 2005 e a X-Force vê uma redução significativa no número de explorações reais que foram divulgados ao público. Quando o código de exploração é divulgado na Internet, ele pode fornecer um meio fácil para que os invasores visem às vulnerabilidades. Nos últimos anos, o código de exploração foi divulgado para cerca de 15% das vulnerabilidades divulgadas ao público. Este ano, este número caiu para 11%. A frequência das divulgações de códigos de exploração que visam aos navegadores de web, bem como aos leitores e editores de documentos, caiu para níveis não observados há mais de quatro anos. As vulnerabilidades divulgadas ao público também tinham mais probabilidade de receber correções. A porcentagem de vulnerabilidades não corrigidas caiu para 36%, em comparação aos 43% do ano passado.

Nos testes de vulnerabilidades de aplicativos de web, a equipe IBM AppScan observou melhorias significativas nas áreas de Falsificação de Solicitação Entre Sites (CSRF) e Scripting Entre Sites (XSS).

À medida que nós e nossos negócios nos aprofundamos em uma presença social online mais conectada e aberta, o mesmo ocorre com os indivíduos oportunistas, que descobrem novas maneiras de explorar o sistema com versatilidade e facilidade. Utilizando uma abordagem de menor denominador comum, eles não apenas visam à tecnologia, mas diretamente ao indivíduo, aproveitando as vantagens da natureza humana básica e utilizando a confiança de má fé. A mídia social e os dispositivos móveis continuam a ofuscar as linhas entre os limites da empresa e do mundo externo.

Juntamente com estas linhas, neste relatório, continuaremos a explorar a maneira como as empresas estão acompanhando as complexidades dos dispositivos móveis e da nuvem. A adoção em massa dos dispositivos móveis traz para primeiro plano a discussão sobre os programas “traga seu próprio dispositivo” (BYOD), sobre o modo de mitigação dos riscos associados a estas políticas e sobre as maiores ameaças que afetam esta plataforma.

A adoção de nuvem enfrenta discussões similares. A questão não é se a nuvem é mais ou menos segura, mas sobre quais controles e processos de negócios específicos são necessários para abordar os riscos e ajudar a assegurar a segurança em um ambiente em nuvem. É importante que qualquer organização, ao planejar-se para realizar uma adoção mais ampla de infraestruturas baseadas em nuvem, tenha um entendimento sobre a função da organização em relação à função do provedor de serviços de nuvem, em termos de segurança e mitigação de riscos.

Ao longo de 2011, as equipes de segurança foram constantemente desafiadas a ter um melhor desempenho. Muitas foram desafiadas a melhorar os processos e tecnologias, a instruir os funcionários e clientes sobre as práticas seguras e a aumentar a postura de segurança aumentando a visibilidade da postura de segurança do negócio. A IBM acredita que a maneira de ajudar os clientes a ficar à frente das ameaças de segurança é conectar nossos recursos de analítica e inteligência a uma organização, a fim de obter melhor prevenção e detecção. A IBM fez uma grande mudança ao adquirir a Q1 Labs em outubro de 2011 e criar a nova divisão de Sistemas de Segurança. As notícias contínuas sobre o avanço de nossa plataforma de inteligência de segurança mostra a seriedade como abordamos o mercado. Com o reconhecimento, vêm as ações e as mudanças. Ele é a nossa esperança para realmente fazer mudanças.

Destaques de 2011

Ameaças:

Malware e a web maliciosa

- O ano de 2011 começou com uma explosão de violações de dados, que continuaram ao longo do ano. A IBM X-Force declarou que 2011 foi "o ano da violação de segurança". (página 12)
- A injeção de SQL continuou a ser um ponto fraco principal explorado nas empresas-alvo. A injeção de SQL existe há algum tempo, mas continua a ser um meio bem-sucedido de entrada. (página 17)
- Outro marco ocorreu em 2011 após invasores terem comprometido diversas autoridades de certificação; a mais divulgada foi a empresa holandesa DigiNotar. Os invasores conseguiram gerar certificados não autorizados que, mais tarde, interceptariam utilizando um tipo de ataque man-in-the-middle como um modo de ouvir uma conexão criptografada. Este tipo de ataque viola uma confiança básica dos usuários – a confiança de que visitar uma página criptografada SSL significa que a comunicação é segura. (página 33)
- Uma ferramenta comprovada para realizar um ataque de negação de serviços (DOS) contra servidores que se comunicam por SSL/TLS foi liberada em 2011. Esta ferramenta mostrou o potencial que um laptop rotineiro em uma conexão média tem de desativar um servidor de web corporativo. (página 33)
- As principais assinaturas de alto volume do grupo de Serviços Gerenciados de Segurança da IBM (MSS) demonstram que os métodos preferenciais dos invasores são a injeção de SQL, aumentos de ataques de força bruta de SSH e atividades de injeção de comandos Shell e que o desvio de proxy continua a se classificar no topo do tráfego de sensores do MSS. (página 16)
- Até agora, mais que no ano anterior, 2011 viu muitas atividades no mundo de malwares de Mac. Isso se aplica não apenas ao volume em comparação aos anos anteriores, mas também à funcionalidade. Em 2011, começamos a ver malwares de Mac com funcionalidades somente vistas nos malwares de Windows®. (página 39)

Tendências de conteúdo de web, spam e phishing

- No primeiro semestre de 2011, os proxies anônimos aumentaram estavelmente, com um número mais que quadruplicado em comparação a três anos atrás. No entanto, no segundo semestre do ano, pela primeira vez desde o início de 2009, não houve nenhum outro aumento deste volume. Os proxies anônimos são um tipo crítico de website para ser rastreado, já que permitem que as pessoas ocultem intenções possivelmente maliciosas. (página 44)
- Em 2011, os volumes de spam continuaram a cair ao final do ano, quando os spams que fornecem malwares com anexos em zip se tornaram um método preferencial. (página 49)
- O principal país de distribuição de spams do ano, a Índia, continuou a dominar o topo da lista, enviando praticamente 14% de todos os spams já registrados. Os EUA, que estavam no topo da lista no ano anterior, realizou uma redução para menos de 2% dos spams enviados em geral. A Índia é seguida por Vietnã, Indonésia, Rússia, Brasil e, pela primeira vez, Austrália - que ficou em sexto lugar e é responsável por 5,6% de todos os spams distribuídos até o final de 2011. (página 55)
- Quase no fim de 2011, começamos a ver a emergência de emails ao estilo de phishing, que se relacionam a websites que não necessariamente realizam um ataque de phishing. Estes emails usam a boa reputação de uma marca bem conhecida para fazer com que os usuários cliquem em um link de malware ou, em alguns casos, um link a um site inofensivo, como um site de varejo. Uma possível explicação para este último tipo de emails pode ser a fraude do clique, na qual os geradores de spam geram tráfego a estes sites em troca de taxas de propaganda. Independentemente da explicação, esta perturbação contribuiu para um grande aumento de emails ao estilo de phishing vistos nos últimos meses do ano. (página 56)

Infraestrutura operacional segura:

Vulnerabilidades e explorações

- O ano de 2011 relatou um pouco mais de sete mil novas vulnerabilidades de segurança. Ao passo que isso é uma redução significativa desde 2010, quando houve vulnerabilidades sem precedentes, houve um ciclo de dois anos de divulgações de vulnerabilidade desde 2006 e os níveis de cada ponto alto e de cada ponto baixo continuam subindo. (página 74)
- Nos últimos cinco anos, cerca de metade das vulnerabilidades de segurança divulgadas eram relacionadas a vulnerabilidades de aplicativos de web. No entanto, neste ano, o número caiu para 41%, uma porcentagem que não é vista desde 2005. (página 75)
- Uma categoria de aplicativo de web que está sujeita a divulgação pública de vulnerabilidades e muitas atividades de ataques são os sistemas de gerenciamento de conteúdo com base em web (CMS). Foram analisados quatro sistemas populares de gerenciamento de conteúdo com base em web e os dados mostram que os pontos fracos mais importantes destes sistemas são provenientes do ecossistema de plug-ins de terceiros ao qual eles oferecem suporte. (página 77)
- Em 2011, a X-Force observou uma redução significativa no número de explorações reais que foram liberados ao público. Este foi o menor número visto desde 2006. O número é menor em termos de porcentagem e em termos reais. Nos últimos anos, a porcentagem de vulnerabilidades com explorações públicas girou em torno de 15%, mas estes ano, chegou aos 11%. (página 78)
- As vulnerabilidades altas e críticas dos navegadores continuam a aumentar e também foi observado um aumento nos ataques acionados por downloads que passaram a visar aos plug-ins de navegadores de terceiros, em vez de visar ao próprio navegador. Os leitores de documentos são um desses componentes de terceiros preferidos pelos invasores, já que os arquivos de documentos maliciosos podem ser usados nos cenários de acionamento por download, bem como nos anexos de emails. (página 78)
- Continuamos a ver aumentos no número de vulnerabilidades divulgadas em players multimídia e, em 2011, vimos quase o mesmo número de explorações públicas relacionadas às vulnerabilidades de multimídia que foi visto em 2010. Isso continua a ser uma área de foco para os invasores. (página 81)
- Os maiores fornecedores de software corporativo representaram uma porcentagem constantemente crescente do número total de vulnerabilidades divulgadas, de 19% em 2008 a 31% em 2011. Não se acredita que isso é apenas uma medida de consolidação do segmento de mercado de software. As práticas seguras de desenvolvimento se tornaram uma parte cada vez mais importante do ciclo de vida de desenvolvimento de software e os fornecedores responsáveis realizaram etapas nos últimos anos para melhorar sua capacidade de identificar e eliminar as vulnerabilidades de seu código. (página 84)
- Nos últimos sete anos, a rede social passou de um passatempo alternativo à principal atividade online do mundo, deixando para trás até mesmo o uso de mecanismos de busca. Naturalmente, esta atividade concentrada representa um ambiente fértil para o crime. As fraudes e scams por email que eram bem-sucedidos há anos encontraram vida nova nos fóruns de mídia social, bem como um grupo recém-formado de possíveis alvos. (página 89)

Práticas de segurança de desenvolvimento de software

Vulnerabilidades de aplicativos de web

- Muitos problemas das dez principais categorias de OWASP de 2010 foram exibidos frequentemente nos softwares enviados ao IBM AppScan OnDemand Application Vulnerability Testing Service. Autenticação quebrada e problemas relacionados ao controle de sessões foram encontrados praticamente em oito de cada 10 testes. Muitos aplicativos testados falharam ao restringir a violação de sessões e foram expostos aos ataques de sessões ao estilo de fixação. Além disso, problemas relacionados ao encerramento e reutilização de sessões também foram atribuídos a esta alta estatística. (página 113)
- Em 2011, a Falsificação de Solicitações Entre Sites (CSRF) foi encontrada em 28% dos testes realizados, mas este número foi reduzido em relação a 2010, quando a porcentagem era de 59%. Uma parte desta redução parece estar no maior reconhecimento deste tipo de vulnerabilidade e também nas melhorias dos métodos usados para incluir tokens de CRSF. (página 116)
- O fato de que o Scripting Entre Sites (XSS) ainda é encontrado em mais de 40% dos aplicativos testados destaca que, provavelmente, ainda há muitos aplicativos que não aderem completamente às práticas de codificação segura. Não há dúvidas de que as coisas estão melhorando, mas isso não é motivo para ter calma. A probabilidade de 40% para vulnerabilidades de XSS ainda é alta, principalmente para algo que é tão facilmente entendido, demonstrado e corrigido. As vulnerabilidades de aplicativos de web permanecem sendo a chave para muitas violações de dados, que continuaram a aumentar no primeiro semestre de 2011. Isso é tão real que a X-Force declarou que 2011 foi o "ano da violação de segurança". (página 114)
- Outro importante ponto de dados que captamos é "o número médio de determinada descoberta por teste de segurança". O que estamos vendo é uma redução das instâncias de XSS quando esta vulnerabilidade é encontrada. Em 2009, o número médio estava acima de 40, enquanto em 2011 estava um pouco acima de três. Agora, é muito menos provável encontrar um aplicativo com absolutamente nenhum controle de entrada implementado. (página 114)
- Em 2011, os aplicativos Financeiros foram novamente o segmento com melhor desempenho. Os aplicativos governamentais tiveram o pior desempenho em todas as três categorias. Não está claro por que isso acontece, mas os danos à reputação podem ser um fator. As violações dos aplicativos governamentais são menos prováveis de acionar um investimento em mitigação de segurança, ao contrário do que aconteceria com os aplicativos financeiros. (página 116)

Tendências emergentes em segurança:

Móvel

- Os dispositivos móveis são outra área que está ganhando em importância. Há muitas vulnerabilidades de sistemas operacionais móveis sendo divulgadas e há várias explorações destas vulnerabilidades sendo liberadas ao público. O desejo de desbloquear ou disponibilizar os dispositivos móveis é um fator motivador que leva as pessoas a postarem o código de exploração móvel online. Obviamente, assim que este código é disponibilizado, ele pode ser usado para propósitos maliciosos em relação aos telefones que não são desbloqueados. (página 82)
- As grandes botnets de dispositivos móveis infectados começaram a aparecer em cena e isso é apenas o começo. (página 83)
- Os dispositivos móveis (porque geralmente têm hardware GPS, com serviços de voz, mensagens e dados) detectaram a presença de aplicativos espiões que monitoram diversos aspectos do comportamento de seus usuários – incluindo registro de locais, mensagens, emails e chamadas de voz para que seu invasor possa revisá-los. Isso é particularmente desconcertante quando é comparado aos tipos de ataques que vemos em computadores pessoais. Já que os dispositivos móveis realmente se tornaram "o seu escritório em seu bolso", eles podem fornecer uma oportunidade para um ataque espião. (página 122)

- Um dos desenvolvimentos mais recentes deste ano foi o aumento do interesse em fornecer a capacidade de separar os aplicativos e dados corporativos dos aplicativos e dados pessoais dos funcionários. Obviamente, um principal acionador deste desenvolvimento foi a natureza disseminada do interesse em programas BYOD. **(página 125)**

Segurança da nuvem

- A questão não é se a nuvem é mais ou menos segura, mas quais os controles e processos de negócios específicos devem ser concentrados para abordar os riscos e ajudar a assegurar a segurança em um ambiente em nuvem. É importante que qualquer organização que busque uma adoção mais ampla de infraestruturas com base em nuvem tenha um entendimento da função da organização em relação à função do provedor de serviços de nuvem, em termos de segurança e mitigação de riscos. **(página 126)**
- O sucesso da computação em nuvem segura pode ser mais que uma questão de um simples gerenciamento de contratos, mas este gerenciamento pode ser fundamental ao sucesso da implementação da nuvem. A criação de um Acordo de Nível de Serviço (ANS) que leve em consideração o gerenciamento de ciclo de vida e a estratégia
- alternativa pode ser benéfica. **(página 128)**
  Os ANSs devem ser acordos reais, específicos em termos e escopo, alteráveis somente com aviso adequado e conhecedores dos requisitos específicos de negócios e segurança de informações da organização. **(página 131)**

2011 – Ano da violação de segurança

De meados do ano ao novo ano – a violação continua

Em meados do ano, a IBM X-Force declarou que 2011 foi o "Ano da Violação de Segurança", marcado por uma série de violações de segurança de redes externas significativas e amplamente relatadas e outros incidentes, notáveis não apenas por sua frequência, mas pela competência operacional presumida de muitas das vítimas.

O segundo semestre de 2011 continuou a demonstrar relatórios comuns de violações de segurança semanais de redes de grande escala, deixando uma onda de vazamentos de dados de clientes, serviços de web inacessíveis e bilhões de dólares de danos. A segurança da TI agora é uma discussão de conselho que afeta os resultados dos negócios, a imagem das marcas, a cadeia de fornecimento, a exposição legal e o risco de auditoria. No Relatório de Riscos e Tendências de Meados do Ano da IBM X-Force 2011, foram analisadas as motivações subjacentes, os métodos dos ataques e as práticas básicas de segurança que foram evitadas para destacar 2011 como o ano da violação de segurança.

Estes incidentes não discriminaram qualquer segmento de mercado ou setor. O Cumprimento da Lei, os governos, as comunidades de redes sociais, o varejo, o entretenimento, os bancos, as organizações sem fins lucrativos, as empresas Fortune 500 e até mesmo as empresas de segurança foram atacados. Nenhuma geografia específica foi o foco; no entanto, obviamente, estes ataques ocorreram em escala global. À medida que o ano foi chegando ao fim, a tendência não mostrou sinais de redução. Dezembro marcou algumas das violações de maior impacto por custo que afetaram diversos sites massivos sociais e de entretenimento da China, com bilhões de dólares de possíveis perdas.

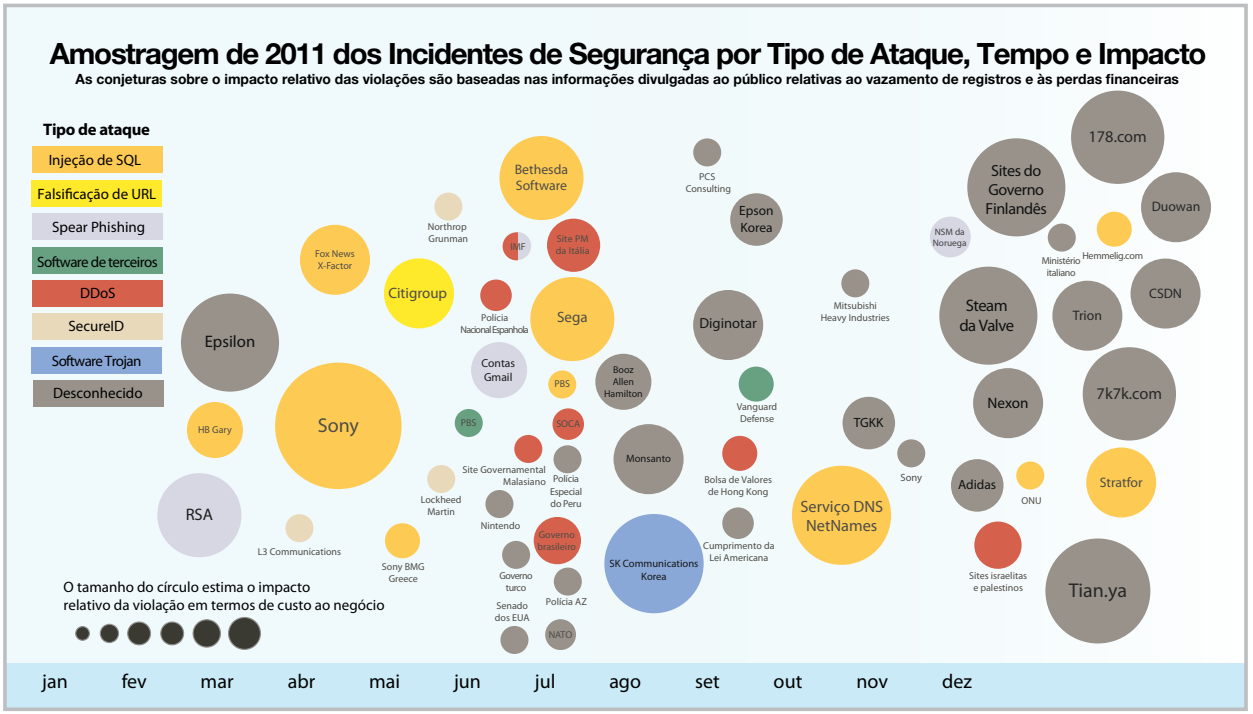


Figura 1: Amostragem de 2011 dos Incidentes de Segurança por Tipo de Ataque, Tempo e Impacto

Alteradores de cenários do segundo semestre de 2011

Conforme ilustrado na Figura 1, **a injeção de SQL** continuou sendo um principal ponto fraco explorado nas empresas-alvo. A injeção de SQL tem ocorrido há algum tempo, mas continua sendo um meio bem-sucedido de entrada. Posteriormente, são discutidas as complexidades da injeção de SQL e por que é tão difícil identificá-la e proteger as redes contra ela.

Incluindo uma dimensão adicional de sofisticação às violações de 2011, vimos vários exemplos de tecnologias principais comprometidas levando a uma exploração em grande escala de outros alvos. No início do ano, um ataque à RSA resultou no roubo de códigos e dados sensíveis associados ao produto de autenticação da empresa, o SecureID. Depois, divulgou-se[1] que a tecnologia comprometida foi usada para obter entrada em, no mínimo, três outras corporações. Isso representa um aumento da complexidade, já que os invasores não estão apenas explorando um alvo final específico, mas também obtendo presença nas tecnologias subjacentes usadas por uma base maior de possíveis vitimas.

Outra tendência emergente que continuou em 2012 foi os invasores que visam aos servidores DNS como um meio de redirecionar os usuários inocentes às variantes maliciosas de sites bem conhecidos. Todas as vezes que um usuário entra em um domínio da web em um navegador como http://www.empresa.com, o nome deve ser traduzido ao endereço de IP do servidor que hospeda o site.

Uma injeção de SQL em um servidor DNS de nomes NetNames permitiu que os invasores atualizassem os registros DNS de diversos sites de alto perfil, como os sites The Register, The Daily Telegraph e UPS[2].

Ao comprometer o próprio servidor DNS de nomes, os invasores reencaminham as solicitações a um servidor de sua escolha, muitas vezes criando uma variante com aparência similar à de um site bem conhecido que contém malwares ou formulários para download configurados para informações sensíveis a phishing. Este tipo de ataque viola um princípio básico de confiança: o princípio de que digitar um nome de website nos levará ao servidor correto.

Outro marco ocorreu depois que os invasores comprometeram diversas autoridades de certificação[3]; a mais pública foi a empresa holandesa DigiNotar. As autoridades de certificação distribuem certificados de segurança, que fornecem a função segura do protocolo HTTPS usado para criptografar o tráfego dos usuários aos serviços online. Os invasores conseguiram gerar certificados não autorizados que, posteriormente, podiam interceptar usando um ataque de tipo man-in-the-middle como um meio de ouvir uma conexão criptografa. Novamente, isso viola uma confiança básica dos usuários – a de que visitar uma página criptografada **SSL** significa que a comunicação é segura. Posteriormente, neste relatório, serão discutidos em mais detalhes os riscos associados ao modelo atual de confiança SSL. Em cada caso, vemos invasores que usam uma estratégia de diversas camadas que compreende uma principal tecnologia e, depois, usam-na para criar uma grande rede de possíveis alvos.

1 http://www.nytimes.com/2011/06/04/technology/04security.html
http://www.infosecisland.com/blogview/14142-RSA-SecurID-Breach-Spreads-to-L3-and-Northrop.html
2. http://www.theregister.co.uk/2011/09/05/dns_hijack_service_updated/
3. http://www.theregister.co.uk/2011/10/27/ssl_certificate_authorities_hacked/

Lições aprendidas

Como pode ser visto no gráfico de violações de segurança de 2011, houve muitos casos no último semestre do ano nos quais uma violação foi relatada ao público, mas não há informações sobre como ela ocorreu. Há várias motivações diferentes que acionam a divulgação pública de violações de segurança, mas geralmente o desejo de informar o público sobre a vulnerabilidade técnica explorada pelo invasor não é uma delas. Muitas vezes, a divulgação é motivada pelo desejo de informar os clientes cujas informações pessoais ou dados corporativos podem ter sido expostos ou de informar que uma tecnologia produzida pela vítima foi comprometida. Recentemente, os analistas financeiros começaram a se interessar pelo uso de informações sobre riscos de segurança aos computadores ao avaliar as decisões de investimento. No entanto, é relativamente raro ver empresas que divulgam as violações de segurança especificamente porque querem chamar a atenção para um problema de segurança de computadores que as outras firmas podem enfrentar. Acreditamos que este é um fato infeliz, já que os profissionais de segurança poderiam se beneficiar das duras lições aprendidas por outros.

Muitas revistas de navegação e voo imprimem colunas mensais que descrevem situações reais que foram muito perigosas ou que resultaram em acidentes. Por meio da leitura desses relatórios mensais, os pilotos e comandantes têm o benefício de analisar regularmente as ações de outros de forma retrospectiva. Por meio deste processo, eles podem aprender como lidar com situações difíceis e desenvolver uma confiança que pode ser valiosa em uma crise. De modo similar, as pessoas responsáveis pela proteção de redes de computadores contra ataques devem buscar regularmente informações sobre falhas de segurança, a fim de que possam desenvolve bons instintos sobre quais ciladas devem ser evitadas. Conhecer as falhas técnicas e de processos exatas que causaram uma violação pode iluminar as lacunas de sua própria postura.

Muitas vezes, a segurança de computadores é percebida como um custo da condução de negócios e os negócios procuram evitar investir recursos na correção de falhas de segurança que podem nunca ser exploradas. Há o desejo de encontrar o "lugar ao sol" onde o dinheiro é gasto de modo suficiente nos investimentos certos em segurança para proteger a empresa, mas sem um dólar a mais. Isso significa que, geralmente, apenas identificar uma lacuna técnica ou de procedimentos não é suficiente para convencer um negócio a investir na eliminação daquela lacuna – deve haver um risco real demonstrável de que esta lacuna será explorada caso não seja corrigida. Quando as vítimas de violações de segurança expõem lacunas técnicas e de procedimentos particulares que causaram as violações pelas quais passaram, estas informações ajudam a fornecer ao negócio a justificativa para que as outras obtenham o investimento necessário para eliminar lacunas similares. Quando surgem situações que resultam em violações tecnicamente similares em diversas empresas, a divulgação da vulnerabilidade técnica específica envolvida pode acionar discussões relacionadas à abordagem deste tipo de vulnerabilidade em todo o mercado de trabalho.

As vítimas de crimes de computadores devem considerar o valor de conversar com o público em relação aos detalhes técnicos dos "erros ocorridos" quando divulgarem publicamente uma violação de segurança. Haverá casos nos quais os riscos envolvidos na divulgação deste tipo de informações podem compensar em benefícios. Obviamente, fornecer muitos detalhes técnicos pode criar um roteiro para futuros ataques. No entanto, é importante compreender quais podem ser os benefícios da divulgação. Ajudar as outras pessoas a aprenderem com seus erros é uma etapa afirmativa que pode ser realizada para limitar o sucesso futuro do tipo de criminosos que comprometeram a sua rede.

O caminho para o futuro

No Relatório de Riscos e Tendências de Meados do Ano da X-Force 2011, foram identificadas dez etapas que a X-Force sugere para mitigar alguns dos ataques que ocorreram neste ano. Nenhuma das etapas sugeridas é uma revelação revolucionária para os profissionais de segurança de TI. O desafio não é saber o que fazer, mas como executar de modo consistente em uma organização complexa e descentralizada. Para que um programa de segurança seja bem-sucedido, é preciso ter os recursos, o apoio político e o respeito institucional necessários para assegurar a conformidade com as melhores práticas de toda a organização. Atingir este nível de eficácia é o real desafio da liderança em segurança de TI.

Se a IBM X-Force estivesse executando o departamento de TI

1. Realize auditorias regulares da segurança terceirizada interna e externa
2. Controle seus terminais
3. Separe os sistemas e informações sensíveis
4. Proteja sua rede
5. Realize auditorias de seus aplicativos de web
6. Treine os usuários finais sobre phishing e spear phishing
7. Busque senhas fracas
8. Integre a segurança em cada plano de projeto
9. Examine as políticas dos parceiros de negócios
10. Tenha um plano sólido de resposta a incidentes

Para mais informações detalhadas sobre quaisquer pontos anteriores, faça o download e leia o **Relatório de Riscos e Tendências de Meados do Ano da IBM X-Force**.

Serviços Gerenciados de Segurança da IBM – Uma paisagem global das ameaças

Os Serviços Gerenciados de Segurança da IBM (MSS) monitoram dezenas de bilhões de eventos por dia em mais de 130 países, 24 horas por dia, 365 dias por ano. A presença global dos MSS da IBM fornece uma visão em primeira mão das ameaças atuais. Os analistas da IBM utilizam esta riqueza de dados para fornecer um entendimento único da paisagem de ameaças cibernéticas. A identificação de tendências de ameaças é vital para estabelecer a estratégia futura de segurança e o entendimento da importância das ameaças.

MSS – principais assinaturas de alto volume de 2011

Principais assinaturas de alto volume

A Tabela 1 mostra a colocação das principais assinaturas de alto volume dos Serviços Gerenciados de Segurança e sua linha de tendências para 2011 em comparação ao final de 2010. Quatro das dez principais assinaturas de 2010 mantiveram um lugar na lista de final de ano de 2011. Os eventos SQL_Injection e SQL_SSRP_Slammer_Worm conseguiram permanecer em uma alta posição em nossa lista há dois anos, embora as atividades de Criadores de Slams tenham apresentado uma tendência ligeiramente decrescente. A tendência decrescente do SQL_Injection foi revertida em 2011. O SSH_Brute_Force continua em uma posição entre os dez principais, mas caiu para o nono lugar. O HTTP_Unix_Passwords também persiste entre os dez principais do relatório de 2011, embora tenha caído do sexto ao décimo lugar, apesar de seu contínuo crescimento ascendente.

Nome do evento	Classificação em 2011	Tendência	Classificação em 2010	Tendência
SQL_Injection	1	Ascendente	2	Decrescente
HTTP_Suspicious_Unknown_Content	2	Decrescente		
SQL_SSRP_Slammer_Worm	3	Ligeiramente Decrescente	1	Decrescente
SNMP_Crack	4	Decrescente		
HTTP_GET_DotDot_Data	5	Ascendente		
Cross_Site_Scripting	6	Ligeiramente Ascendente		
SSH_Brute_Force	7	Ligeiramente Ascendente	4	Ligeiramente Decrescente
HTTP_Unix_Passwords	8	Ascendente	6	Ligeiramente Ascendente
Shell_Command_Injection	9	Ascendente		
Proxy_Bounce_Deep	10	Ascendente		

Tabela 1: Principais assinaturas de alto volume de MSS e linha de tendências – Final de Ano de 2011 versus Final de Ano de 2010

Injeção de SQL

Nossa assinatura heurística de SQL, que se classificou em segundo lugar em 2010, subiu ao primeiro lugar e manteve uma tendência ascendente. 2011 foi um ano estandarte para a exploração de pontos fracos de SQL e tornaram-se públicos diversos episódios de alto perfil e interessantes de ataques bem-sucedidos de injeção de SQL. Os grupos de atividades hackers Anonymous e Lulzsec foram os principais responsáveis pelas táticas de injeção de SQÇ e continuam a mostrar suas capacidades com novos vetores de ataques de injeção. Além disso, há ataques automatizados de injeção de SQL, como o LizaMoon, que escaneiam a Internet em busca de hosts vulneráveis e são os originadores da maior parte das atividades que ocorrem. Os MSS da IBM adicionaram diversas outras coberturas aos vetores dos ataques aos seus conjuntos de regras de Gerenciamento de Eventos e Informações de Segurança (SIEM) e continuam a monitorar e analisar novos vetores todos os dias. A seção a seguir, intitulada “A Ameaça Contínua da injeção de SQL”, discute detalhadamente a natureza desta ameaça e explica as ações que as organizações podem realizar para ajudar a proteger os códigos, de seus aplicativos de web, os servidores e as redes contra a injeção de SQL.

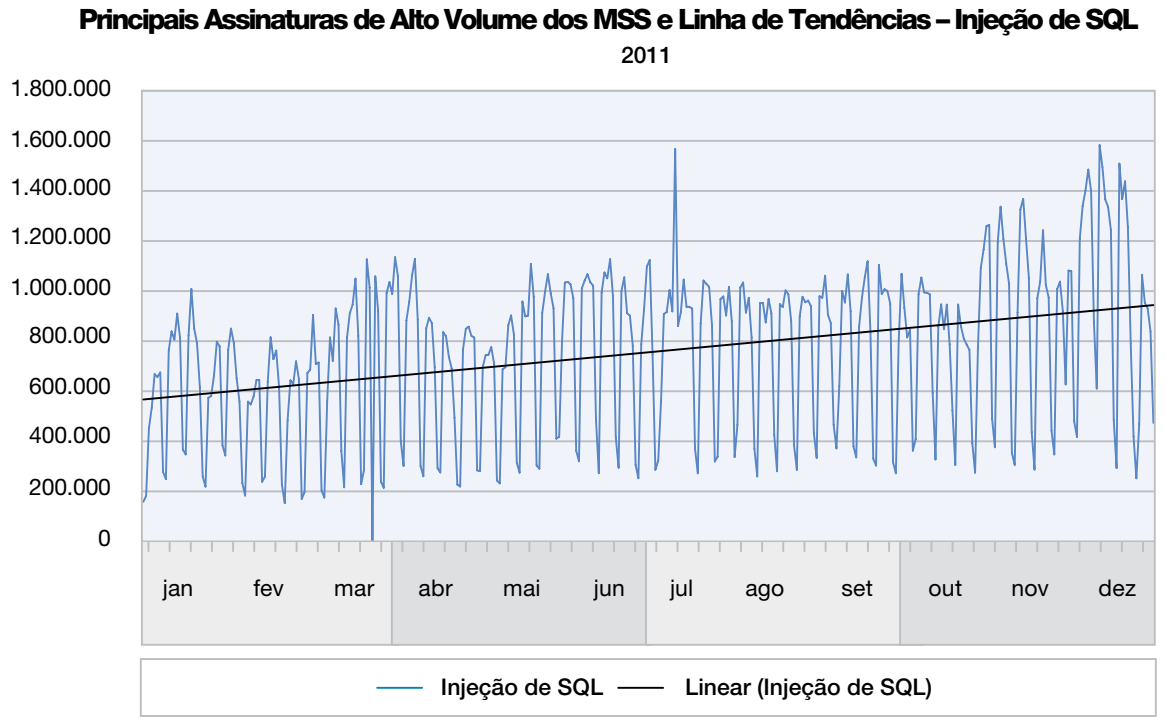


Figura 2: Principais assinaturas de alto volume dos MSS e linha de tendências – Injeção de SQL

Zeus em nosso meio?

A atividade de HTTP que aciona nossa assinatura em segundo lugar, o HTP_Suspicious_Unknown_Content, pode ser normal. No entanto, ela pode indicar que uma BotNet, como Zeus, está ativa em nossa rede. Zeus é um Trojan financeiro amplamente conhecido que foi identificado primeiramente em julho de 2007 e se tornou difundido até meados de 2009. Os principais vetores de infecção são acionados por download e phishing. Há muitos grupos e indivíduos diferentes que têm botnets Zeus configuradas. O objetivo destas botnets, geralmente, é roubar informações pessoais. Na maioria das vezes, estas informações são dados financeiros online que podem ser usados para acessar as contas bancárias para transferência de dinheiro.

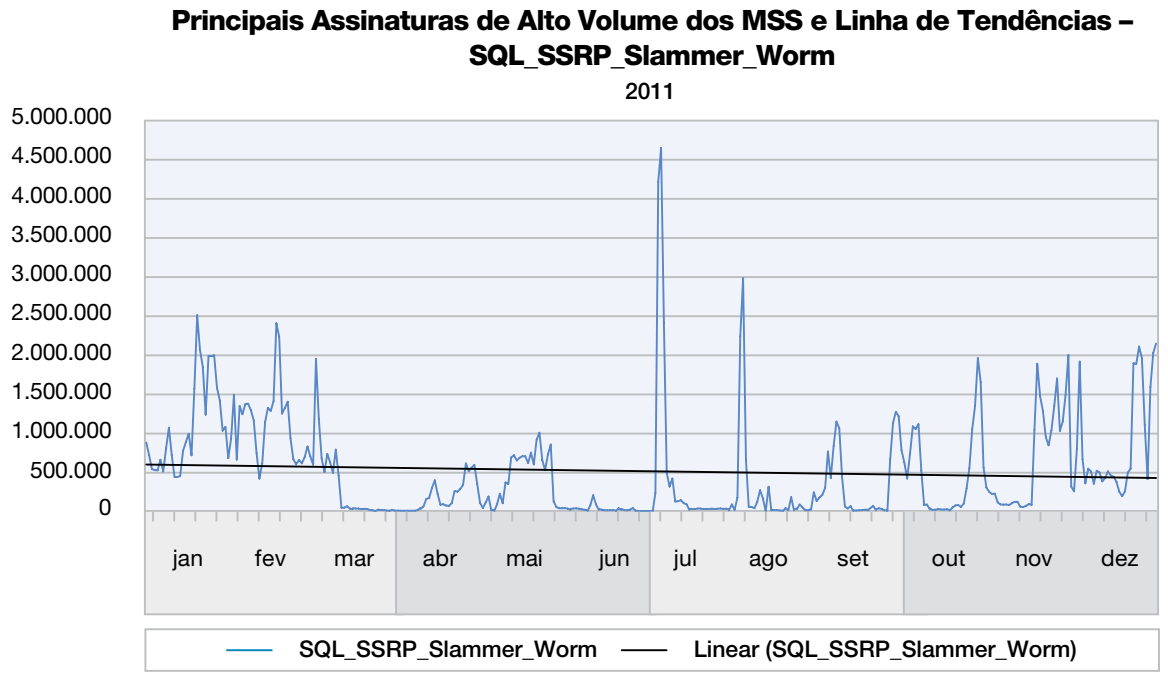
O FBI vem perseguindo agressivamente diversos grupos que criam botnets usando Zeus. No entanto, apesar da desativação bem-sucedida de muitos dos servidores originais de controles e comandos Zeus em 2010, os MSS rastrearam um grande número de infecções por Zeus. Já que a proteção contra Zeus é algo muito difícil de fazer e que os produtos antivírus estão em suas melhores lacunas de paradas temporárias para a propagação de Zeus, a instrução dos usuários se tornou o foco principal de combate. Treinar os funcionários para não clicar em links hostis ou suspeitos de emails ou na web e, ao mesmo tempo, acompanhar as atualizações de antivírus tem se tornado a principal estratégia de defesa.

Redução contínua de SQL Slammers

Em 25 de janeiro de 2003, um worm agressivo que explorava um sobrefluxo de buffer no Resolution Service da Microsoft® iniciou uma infecção em massa dos servidores conectados à Internet. Embora o worm não tenha usado uma vulnerabilidade de SQL para se propagar, a grande maioria das infecções ocorreu em servidores que executavam o Microsoft SQL Server Desktop Engine (MSDE). Os Criadores de Slams continuaram sendo uma ameaça disseminada no decorrer dos anos e os pacotes de infecções por Criadores de Slams ainda são responsáveis por uma porção considerável de tráfego UDP na Internet. De fato, a principal assinatura de 2010 foi para o SQL_SSRP_Slammer_Worm. No entanto, esta assinatura caiu para segundo lugar em nossa verificação de meados do ano e caiu para terceiro lugar na avaliação dos dados de final de ano. A seção "O dia em que o SQL Slammer desapareceu" do Relatório de Riscos e Tendências de Meados do Ano da X-Force 2011 discute a queda drástica das atividades de SQL Slammer em março de 2011, que contribuiu para a menor colocação desta assinatura em nossa lista.

Houve algumas vezes em 2011 em que a atividade preparou um retorno moderado, somente para cair novamente, conforme mostra a Figura 3.

Foi observado um volume superior ao normal para Slammers em dezembro, mas isso não parece ser uma retomada dos padrões anteriores a março. Estamos monitorando a situação e observaremos quaisquer novas tendências que continuarem crescendo.



Principais assinaturas de alto volume dos MSS e linha de tendências – SQL_SSRP_Slammer_Worm

Vulnerabilidades de SNMP

Nossa assinatura de SNMP_Crack indica uma tentativa de ataques de força bruta às Sequências de Comunidade SNMP. SNMP é um serviço que facilita o monitoramento do status de dispositivos móveis por parte dos administradores de rede e, às vezes, o controle de sua configuração. Os sistemas operacionais, hubs, comutadores e roteadores utilizam SNMP. Este serviço utiliza Sequências de Comunidade, como senhas, para proteger o acesso às informações e controles sensíveis. Muitas vezes, os serviços de SNMP são configurados com sequências de comunidade-padrão; este tipo de serviço é a primeira coisa que os invasores buscam. Caso contrário, os invasores tentarão adivinhar as Sequências de Comunidade por meio de força bruta. Recomenda-se que as organizações avaliem a necessidade de ter o SNMP ativo em seus dispositivos e que o desativem caso não seja necessário.

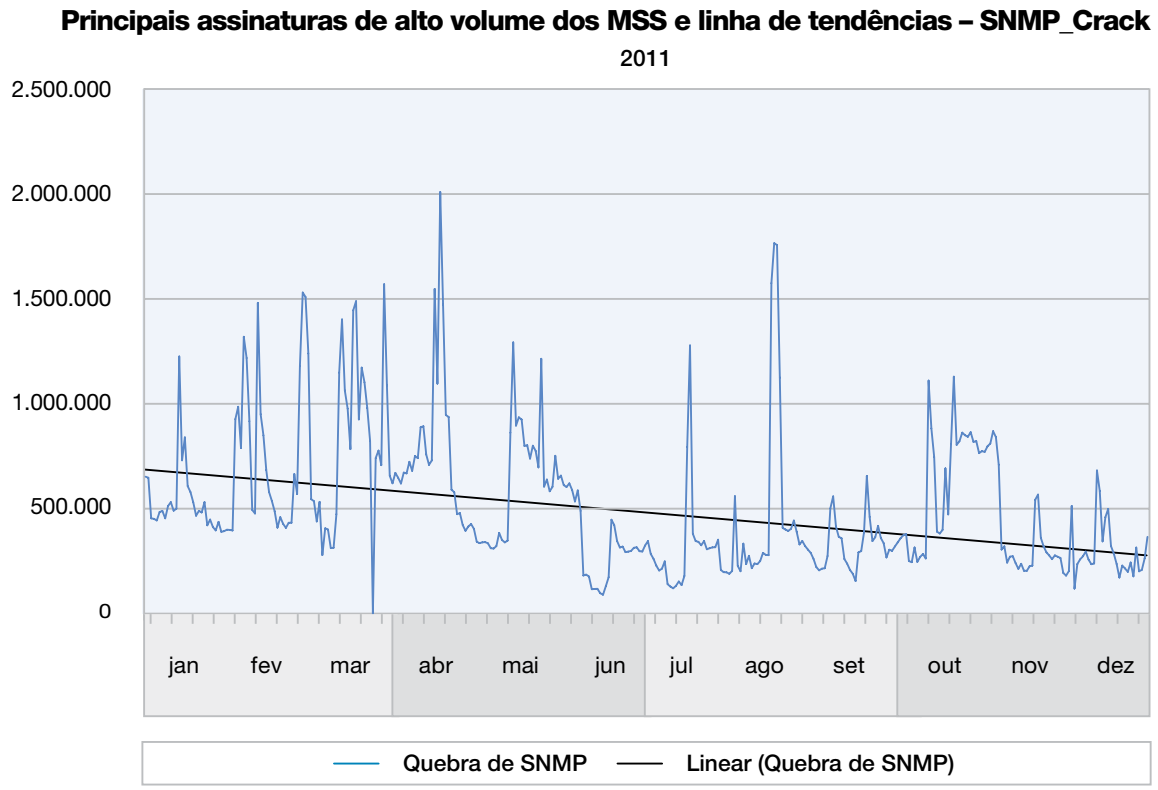


Figura 4: Principais assinaturas de alto volume dos MSS e linha de tendências – SNMP_Crack

Atravessando diretórios

A assinatura de HTTP_GET_DotDot_Data detecta a tentativa de um invasor de contornar a segurança normal imposta pelo servidor da web para acessar os arquivos normalmente restritos. Um invasor pode atravessar diretórios em servidores da web vulneráveis usando sequências “dot dot” (/../) nas URLs, o que permite que o invasor leia qualquer arquivo no servidor HTTP de destino que seja compatível com o Word ou legível pelo ID do processo de HTTP. Por exemplo, uma URL com forma (http://www.dominio.com/..\) permite que qualquer um navegue e faça download de arquivos fora do diretório raiz de conteúdo do servidor da web. As URLs, como o nome de script (http://www.dominio.com/scripts..\..\), podem permitir que um invasor execute o script de destino. Um invasor pode usar uma listagem deste diretório como informações adicionais para planejar um ataque estruturado ou pode fazer download dos arquivos em qualquer outro lugar do sistema de arquivos.

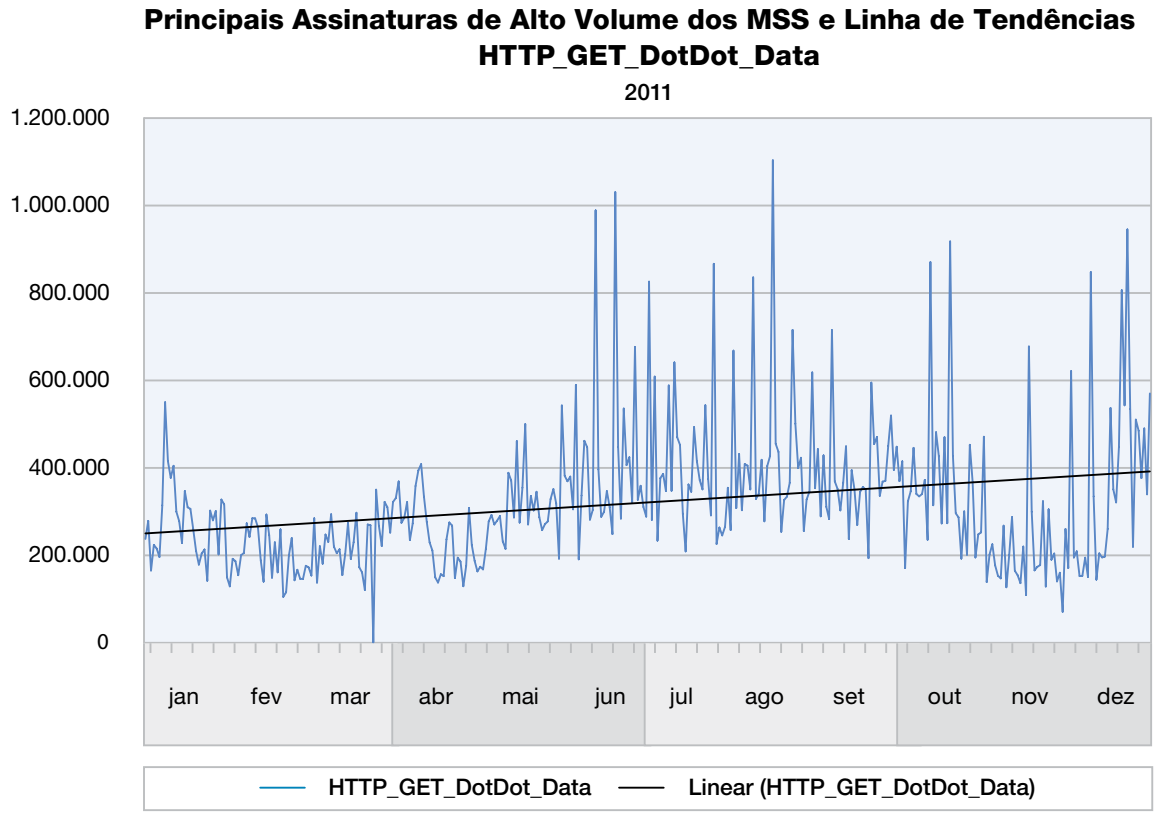


Figura 5: Principais assinaturas de alto volume dos MSS e Linha de Tendências HTTP_Get_DotDot_Data

Cross_Site_Scripting

Geralmente encontrado em aplicativos de web, um ataque de scripting entre sites permite que os invasores injetem scripts da parte dos clientes nas páginas de web vistas por outros usuários. Este ataque também pode ser usado pelos invasores para contornar os controles de acesso. Este ataque tem uma popularidade extremamente alta e representa um risco significativo à segurança. O scripting entre sites é popular desde a década de 90, sendo o tipo mais comum de vulnerabilidade de Aplicativos de web. Nossa assinatura de Cross_Site_Scripting cai para a oitava posição de nossa lista das dez principais assinaturas rastreadas por volume. Reduzir a ameaça exige diversas táticas, incluindo a validação de entradas HTML, segurança de cookies e desativação de scripts da parte dos clientes. Atualmente, estão disponíveis tecnologias emergentes mais recentes, como a Política de Segurança de Conteúdo do Mozilla, as ferramentas Javascript Sandbox e os modelos Auto-escaping que, embora ainda estejam evoluindo, ajudam a reduzir a ameaça.

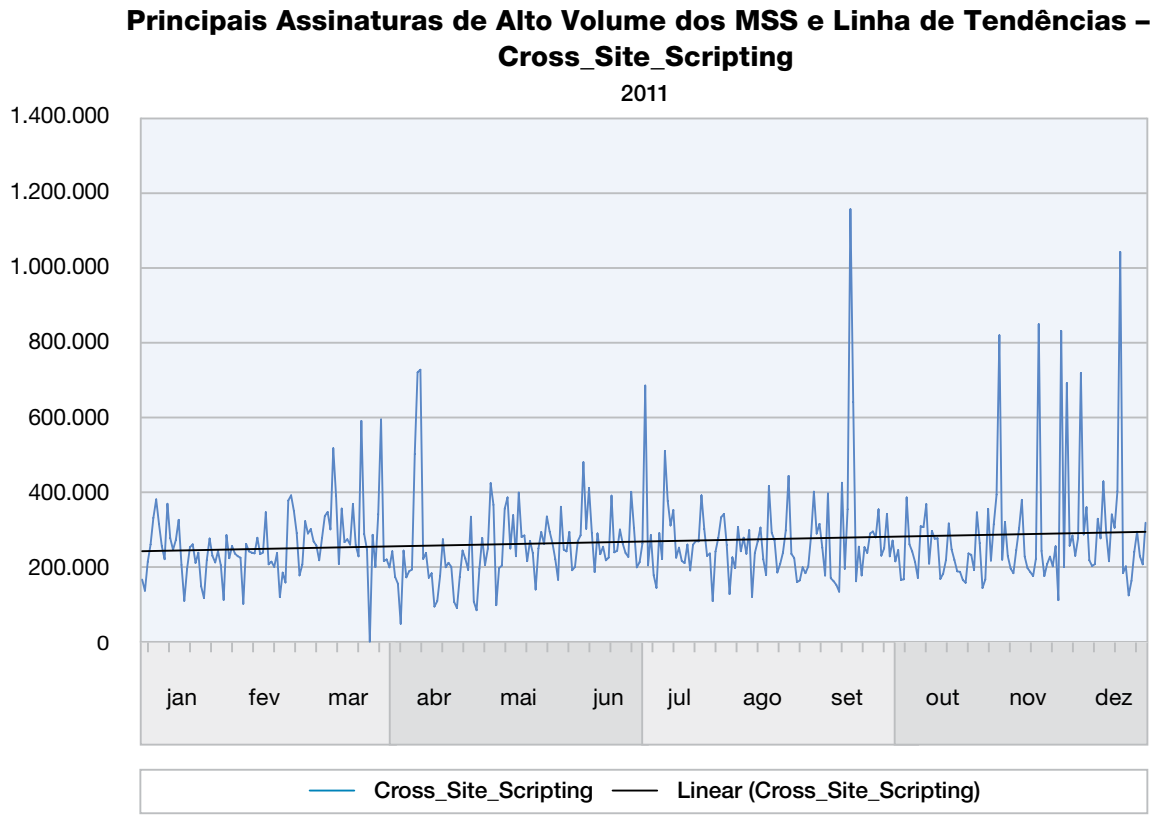


Figura 6: Principais assinaturas de alto volume dos MSS e linha de tendências – Cross_Site_Scripting

Ataques de força bruta

O SSH_Brute_Force ocupa o sétimo lugar, caindo três lugares em relação à sua classificação de quarto lugar em 2010. Um ataque de força bruta envolve um invasor que tenta obter acesso não autorizado a um sistema, tentando um grande número de possibilidades de senhas. A assinatura detecta um número excessivo de Identificações de Servidor SSH a partir de um servidor SSH em um intervalo de tempo especificado. Por meio deste tipo de ataque, um indivíduo malicioso pode conseguir visualizar, copiar ou excluir arquivos importantes do servidor acessado ou executar códigos maliciosos. Em 2011, foram observadas atividades constantes que escaneavam a Internet em busca de servidores SSH inseguros com senhas fracas. As organizações devem realizar a mitigação de ataques de força bruta, desativando o acesso direto às contas raiz e utilizando fortes nomes de usuário e senhas.

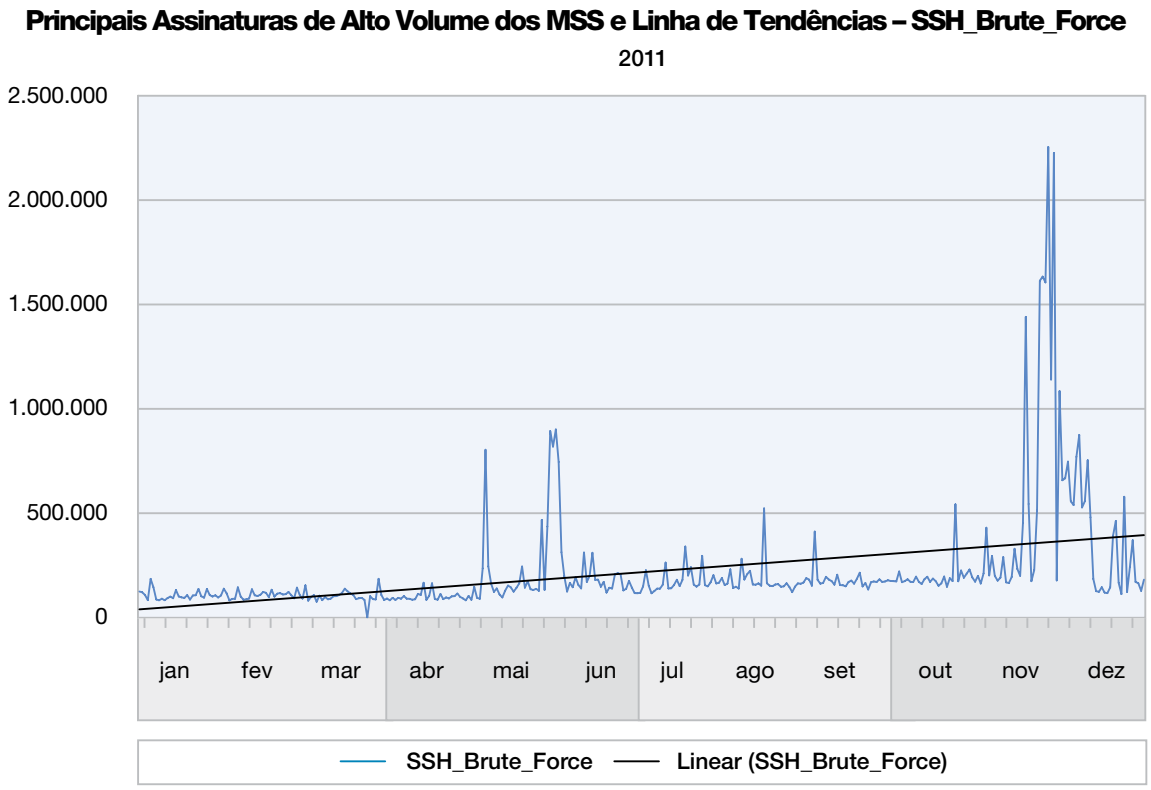


Figura 7: Principais assinaturas de alto volume dos MSS e linha de tendências – SSH_Brute_Force

Ataques contra UNIX

Embora a assinatura de HTTP_Unix_Passwords permaneça na lista de principais assinaturas de alto volume e continue a apresentar uma tendência ascendente, ela cai do sexto lugar em 2010 ao décimo lugar em 2011. Esta assinatura detecta tentativas de acessar o arquivo /etc/passwd dos sistemas UNIX por meio de um servidor da web (HTTP). Embora esta atividade possa ser autorizada, às vezes pode ser suspeita. Este é um ataque muito antigo, mas ainda é bem-sucedido.

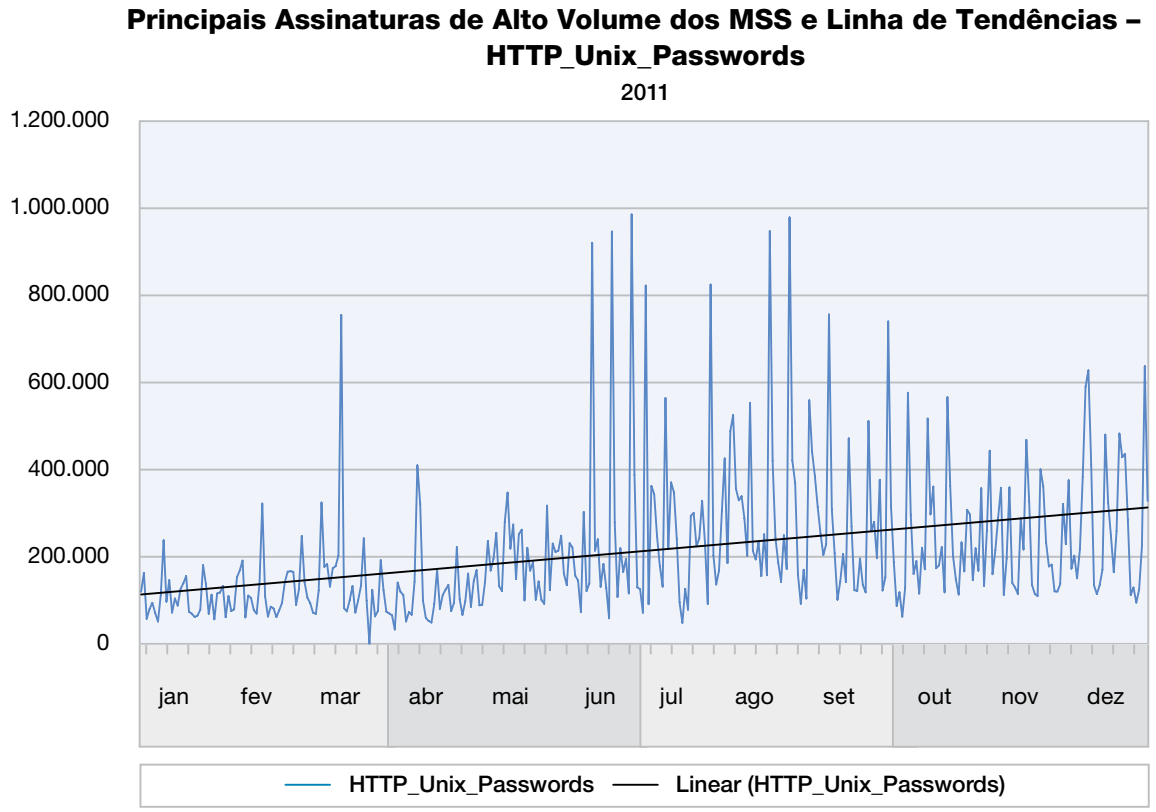


Figura 8: Principais assinaturas de alto volume dos MSS e linha de tendências – HTTP_Unix_Passwords

Injeção remota de comandos

Os MSS têm rastreado ataques de injeção Remota de comandos globalmente. Estas vulnerabilidades existem quando as entradas dos usuários não são devidamente depuradas e, então, são usadas com funções que executam comandos Shell do sistema, como funções PHP, como exec() e system(). Isso permite que os invasores executem comandos no servidor da web. Este é um ataque bastante básico, mas muitas vezes bem-sucedido, pelo mesmo motivo que a injeção de SQL: não ocorreu a segurança adequada no nível de aplicativos.

Muitas das cargas úteis testemunhadas consistem em fazer com que o servidor da web faça o download de um script remoto via wget, armazene-o em um diretório de tmp e, finalmente, execute-o. O script é desenvolvido para manter o acesso remoto ao sistema, reunir Intel e estabelecer os comandos e controles de volta ao servidor do invasor. Então, o servidor é usado para escanear e atacar outros servidores encontrados localmente e remotamente por meio do Google. Este é um meio muito rápido e efeito para que os invasores obtenham controle sobre centenas de websites vulneráveis. Em 2012, somente podemos esperar ver um aumento estável da atividade, já que algumas botnets estão crescendo e outros invasores começam a usar as vulnerabilidades para seu uso próprio.

A proteção pode ser tão simples quanto depurar quaisquer entradas de seu website, a fim de excluir muitos comandos shell populares, como passwd, wget, dir, entre outros.

Além disso, certamente, a remoção do comando wget do servidor pode prejudicar as ações de um invasor sem investigações adicionais.

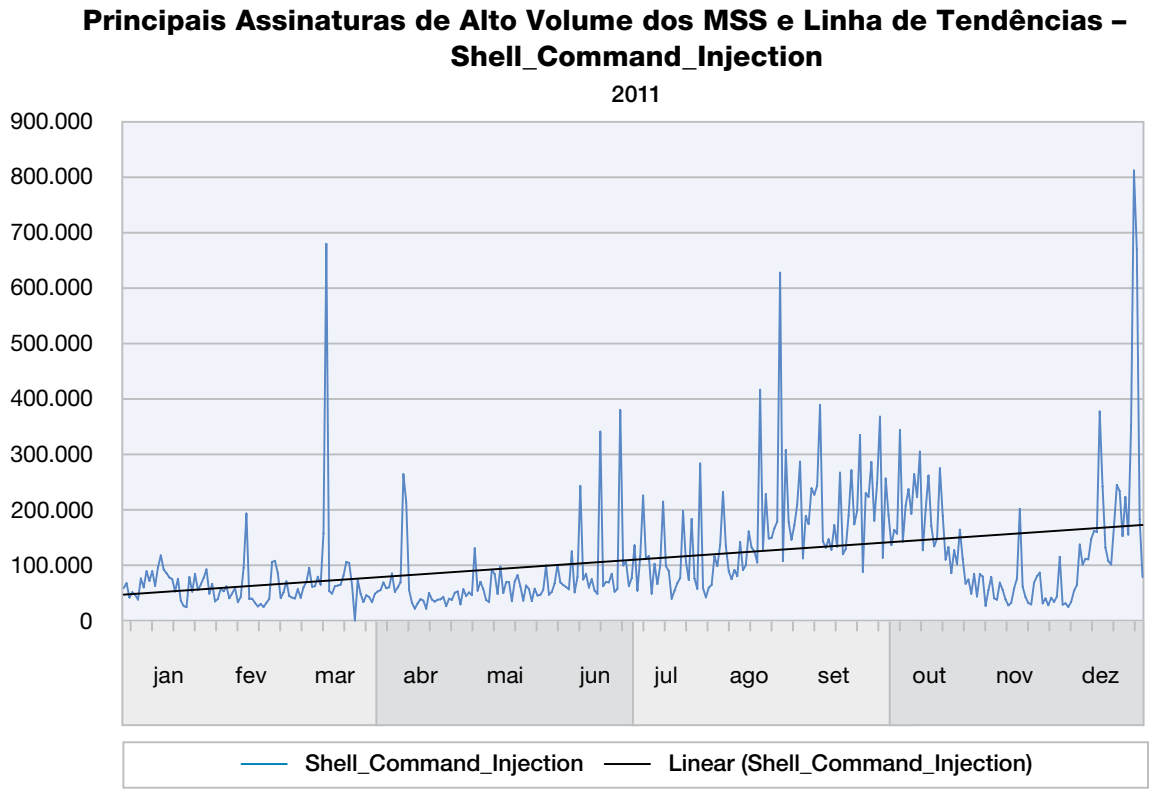


Figura 9: Principais assinaturas de alto volume dos MSS e linha de tendências – Shell_Command_Injection

Proxies anônimos aninhados

A assinatura Proxy_Bounce_Deep da X-Force detecta situações nas quais os clientes estão tentando acessar websites por meio de uma corrente de proxies HTTP. Grandes lotes desta atividade surgiram nas redes de diferentes clientes. Isso pode parecer uma navegação na web extremamente paranoica, mas é legítima; no entanto, às vezes, os invasores fazem isso para obscurecer o endereço de origem a partir do qual estão lançando ataques contra os servidores da web. Nos últimos anos, foram vistos aumentos significativos no número de proxies anônimos na Internet, que podem usados para este propósito. É possível saber mais detalhes sobre este tópico de **proxies anônimos na seção de conteúdo da web** deste relatório.

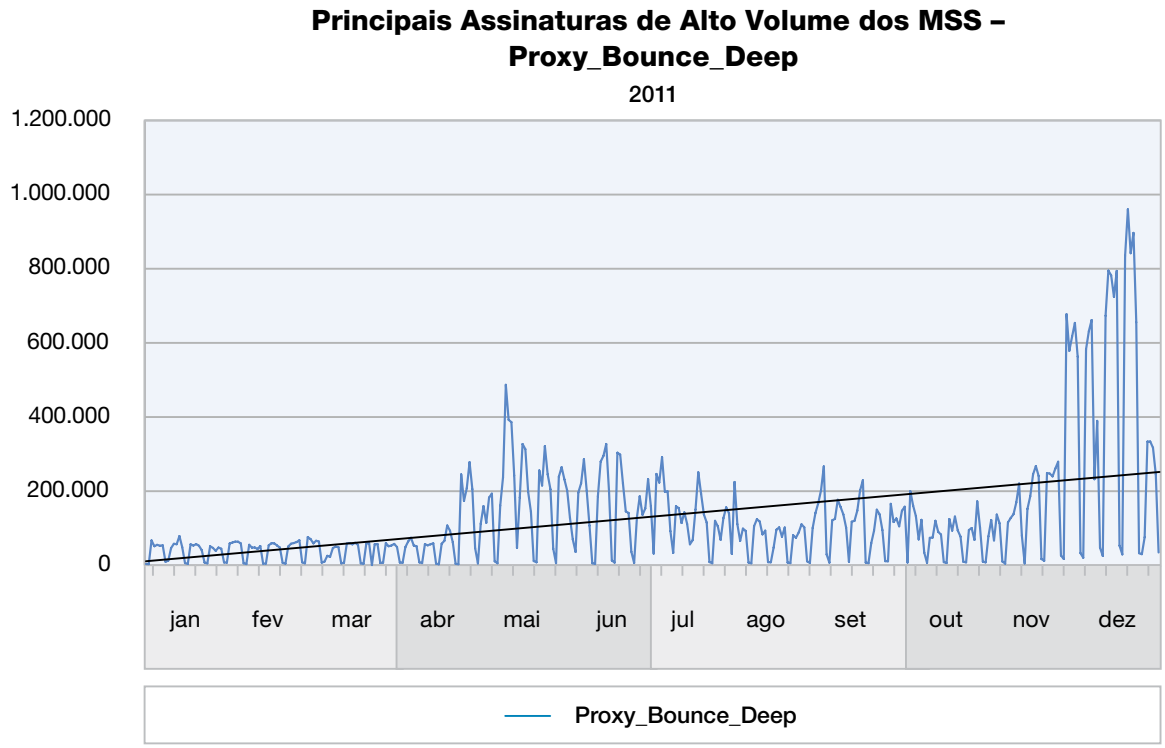


Figura 10: Principais assinaturas de alto volume dos MSS – Proxy_Bounce_Deep

A ameaça contínua da injeção de SQL

Injeção de SQL

A Linguagem de Consulta Estruturada (SQL), concebida originalmente na década de 70, é uma linguagem poderosa usada para gerenciar os dados nos bancos de dados relacionais. Embora tenha sido inventado para uso em farm de dados, o banco de dados relacional ganhou novas funções em comparação à interatividade da web. Os formulários de busca, o gerenciamento de contas, o rastreamento de pedidos e as ferramentas de colaboração são possíveis por meio da união destas duas tecnologias. Esta combinação resultou em inovação, mas também criou o risco de vazamento de dados e forneceu um meio efetivo de ataque.

Durante anos, os invasores usaram sequências especialmente formatadas nos formulários da web e contra as interfaces de programação de aplicativos da web. Estas sequências são desenvolvidas para manipular o banco de dados subjacente injetando declarações de SQL no código do aplicativo da web. Este processo, conhecido como injeção de SQL, pode ser usado para contornar a autenticação, acessar os conteúdos não publicados do banco de dados ou a te mesmo comprometer o sistema operacional que hospeda o banco de dados.

Inicialmente, a injeção de SQL era um ataque direcionado, já que o esquema dos bancos de dados e o código dos aplicativos da web eram diferentes para cada site. Assim que um invasor encontrava um aplicativo da web vulnerável, ele usava consultas fabricadas para mapear o banco de dados. Equipado com nomes de tabelas e campos, o invasor podia acessar as informações e explorar as emissões de permissões. Os ataques eram lentos, direcionados e o processo era praticamente manual. Este tipo de ataque direcionado ainda existe. Quando o CEO da HBGary Federal, Aaron Barr, declarou que havia conseguido identificar membros de alta classificação do Anonymous, o grupo usou um ataque de injeção de SQL contra o website da empresa. Este ataque causou um comprometimento raiz da rede da empresa, a divulgação de dados sensíveis e a renúncia de Aaron Barr. Quando a Sony anunciou que eles tinham protegido sua rede após a maior violação de dados de clientes na história, o LulzSec respondeu postando mais de cento e cinquenta mil detalhes de clientes que obtiveram com a injeção de SQL.

Começando em 2008, surgiu um novo tipo de ataque de injeção de SQL que não exigia mais o conhecimento das estruturas subjacentes dos bancos de dados ou dos códigos de aplicativos da web. Em vez de tentar acessar os dados armazenados no banco de dados, o invasor injetaria um script e obteria o banco de dados para executá-lo. Já que o único reconhecimento necessário para este tipo de ataque era encontrar um servidor vulnerável, ele era muito fácil de automatizar. Nasceram os primeiros ataques em massa de injeção de SQL. Em vez de buscar os conteúdos do banco de dados, geralmente, estes ataques buscam obter acesso raiz ou usar o servidor da web para atacar os usuários que acessam o site. Isso pode ser realizado

por inserção de uma vulnerabilidade de Scripting Entre Sites (XSS) ou outros conteúdos maliciosos no aplicativo da web ou em seu cache. A marca destes ataques são as tentativas de injeção de SQL que incluem declarações DECLARE para inserir o script e declarações EXEC para executá-lo. Os Serviços Gerenciados da IBM observaram um grande aumento no número destes tipos de ataques em 2011, conforme mostra a Figura 11, principalmente no último semestre, quando jjghui e outras variantes atacaram os sites ASP.NET. O jjghui é um ataque em massa de injeção de SQL que se refere ao website ao qual ele redireciona o seu tráfego.

Em 2011, surgiu uma nova técnica de injeção em massa que combina uma carga útil de scripts com certos conhecimentos da estrutura subjacente dos bancos de dados. Isso foi visto pela primeira vez em março, com os ataques LizaMoon. Estes ataques usam os comandos UPDATE e REPLACE contra uma tabela válida, em vez de comandos cegos DECLARE e EXEC. Isso exige um pouco mais de trabalho, mas é mais difícil de detectar com uma combinação de padrões simples – principalmente quando a URL é obscurecida.

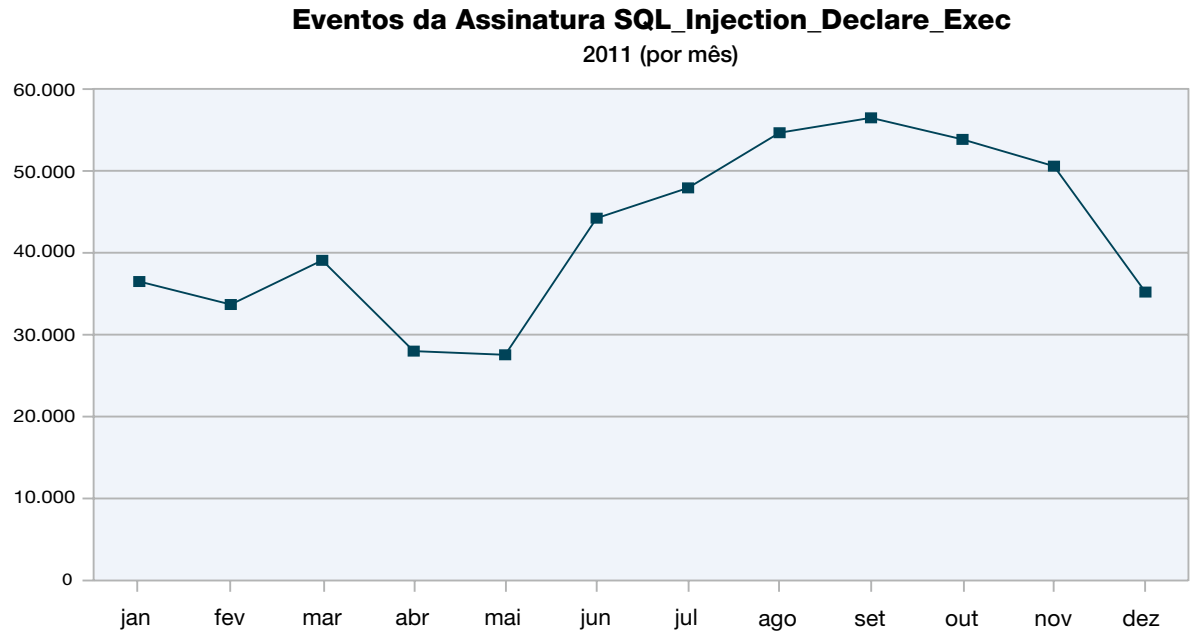


Figura 11: Eventos da assinatura SQL_Injection_Declare_Exec 2011 (por mês)

A natureza da ameaça

Os ataques de injeção de SQL existem há muito tempo, mas ainda são o tipo mais comum de ataques na Internet. Muitas vezes, eles são malsucedidos, mas geralmente podem ser impedidos por meio da depuração de todas as entradas de usuários e da proteção do banco de dados. De uma perspectiva de segurança, há dois tipos de sistemas que são vulneráveis a este ataque. Há os bancos dados conectados à web conhecidos e desconhecidos. A sua rede pode conter páginas de web com contas de login, serviços de funcionários, uma fachada de loja ou qualquer número de sites de contato com o público. Estes são os sites conhecidos e que, provavelmente, contêm informações sensíveis, como contas de usuário, números de cartões de crédito ou informações de contato dos clientes. Caso os bancos de dados que contêm este tipo de informação interajam com um de seus servidores da web, provavelmente, você realizou as etapas para proteger os dados. Mas elas são suficientes?

Você pode ter uma política de codificação segura implementada e pode ter realizado uma revisão completa de segurança quando a primeira versão de seu website foi implementada. Mas, no decorrer do tempo, existem muitas oportunidades para o surgimento de vulnerabilidades. À medida que novos recursos são implementados, é realizada uma revisão dos seus códigos? À medida que novos scripts ou aplicativos de software são inclusos, eles são pesquisados e testados em relação às suas vulnerabilidades? À medida que novas tabelas e campos são inclusos ao banco de dados, as permissões são configuradas devidamente?

À medida que novos desenvolvedores são contratados, eles recebem treinamento sobre a programação segura da web? A perda de dados confidenciais pode ter sérias repercussões. Estes custos não são apenas custos financeiros diretos, como também criam problemas de confiança com seus clientes.

Além dos servidores conhecidos, pode haver alguns servidores em sua rede que não se conhecem. Com o advento dos bancos de dados de software livre e das ferramentas da web, integrar os servidores de bancos de dados e da web se tornou bastante simples. Com um servidor da web Apache, um banco de dados MySQL ou Postgres e com um código da web suportado pela comunidade – qualquer pessoa com uma ideia para um novo aplicativo da web pode desenvolver um, caso esteja disposta a investir o tempo de pesquisa. As bases de conhecimento, as ferramentas de colaboração, o rastreamento de chamados e as ferramentas de teste são exemplos comuns destes aplicativos internos. Embora este caminho possa causar grandes inovações, os desenvolvedores desses aplicativos podem não ter recebido treinamento de desenvolvimento seguro da web. Há muitos recursos disponíveis para aprender sobre as melhores práticas, mas os desenvolvedores da web de meio período geralmente estão mais preocupados com o funcionamento que com a segurança. Sem um treinamento adequado, eles podem não estar cientes de que a injeção de SQL é uma possibilidade. Os desenvolvedores novatos também têm mais probabilidade de fazer download de módulos pré-formatados ou copiar códigos exemplo – duas coisas que podem aumentar bastante as chances de que eles sejam vítimas de um ataque de injeção em massa.

Embora esses tipos de sistemas tenham menos probabilidade de ter informações como números de contas de cartão de crédito, eles ainda podem conter dados sensíveis. Mesmo se os dados armazenados no banco de dados não forem sensíveis, os nomes de usuário e as senhas do banco de dados podem ser. Caso as permissões do banco de dados sejam muito liberais, o invasor pode obter acesso raiz à máquina que executa o banco de dados. Com uma presença em sua rede, o invasor pode continuar a atacar os alvos de maior valor. Eles também podem instalar bots e usar sua rede para atacar terceiros.

Ajudando a proteger seu código

Como qualquer outra vulnerabilidade, a chave para ajudar a parar a injeção de SQL é uma defesa gradual. O código do aplicativo da web é sua primeira linha de defesa. Este é o ponto de entrada de um ataque de injeção de SQL. Para ajudar a proteger o banco de dados a partir deste código:

- Remova todos os caracteres reservados de SQL que sejam excedentes e desnecessários de quaisquer dados fornecidos pelos usuários. Recomenda-se usar as bibliotecas revisadas por colegas fornecidas pela sua linguagem de programação escolhida, em vez de tentar fazê-lo por conta própria. Há muitas maneiras de codificar caracteres perigosos e você pode não estar ciente de todas elas.
- Valide os tipos de dados e codificações enviados pelos usuários – caso espere um número inteiro de dados, verifique se este foi o tipo de dados obtido.
- Nunca permita que os dados fornecidos pelos usuários interajam diretamente com o banco de dados. Mesmo se tiver depurado os dados fornecidos pelos usuários, evite desenvolver declarações de SQL com esses dados. Em vez disso, use declarações preparadas, declarações parametrizadas ou procedimentos armazenados para separar seu código SQL dos dados fornecidos pelos usuários.
- Nunca envie informações de depuração de volta ao usuário – em vez disso, registre-as localmente.
- Verifique periodicamente se sua linguagem de programação, estrutura de servidores ou qualquer software de terceiros usado tenha quaisquer vulnerabilidades conhecidas.

Caso sejam depurados todos os dados fornecidos pelos usuários, isso nega ao invasor uma maneira de obter o banco de dados. No entanto, não é possível contar somente com essa tática, já que basta apenas um campo desmarcado para possibilitar a um invasor a oportunidade de invasão. É preciso assegurar que todas as pessoas que alteram os códigos de seu aplicativo da web tenham sido treinadas sobre como programar com segurança. Considere transformar a obtenção de acesso ao código em um requisito e aumentar periodicamente o reconhecimento sobre a importância de um código seguro.

Até mesmo os melhores desenvolvedores podem cometer erros caso estejam com pressa ou acreditem que estejam fazendo uma pequena mudança. A melhor maneira de identificar isso é por meio de uma revisão do código por colegas. A visão de outra pessoa ajuda a reduzir a chance de erros simples. Com a implementação de uma nova tecnologia, a grande inclusão de recursos ou quaisquer mudanças significativas a um sistema com dados altamente sensíveis, considere uma revisão externa do código ou um teste de penetração antes de disponibilizar o aplicativo ao público.

Ajudando a proteger seu servidor

Sua segunda linha de defesa é a conexão com o banco de dados. É preciso:

- Nunca permitir que seu aplicativo da web use uma conta raiz ou de superusuário.
- Usar as permissões mais restritivas possíveis para a conta usada para acessar o servidor do banco de dados. Somente conceder permissões aos campos que devem ser acessados pelo banco de dados e somente permitir acesso de edição aos campos obrigatórios.
- Remover as contas-padrão, códigos exemplo e aplicativos de teste que podem ter sido instalados com o seu servidor de banco de dados. Caso você não os tenha editado e não os utilize, não há motivos para mantê-los.
- Usar senhas fortes e nunca armazená-las em texto simples.
- Auditar rotineiramente os logs de seus bancos de dados e aplicativos da web em busca de erros estranhos ou repetidos.
- Considerar usar softwares de monitoramento de logs ou de bancos de dados para impedir comprometimentos ou notificar a sua ocorrência.

Ter um servidor de banco de dados devidamente configurado pode ser a diferença entre perder alguns dados e um comprometimento raiz do sistema. É preciso assegurar que a segurança do banco de dados seja uma prioridade ao interagir com um servidor da web, até mesmo quando os dados não são considerados sensíveis. É preciso auditar periodicamente qualquer banco de dados em busca de permissões adequadas e contas desnecessárias. É muito fácil para essas permissões e contas sejam corrompidas à medida que novos campos e tabelas são inclusos.

Caso um invasor consiga executar um ataque de injeção de SQL e obtenha as permissões suficientes, a segurança de seu sistema operacional será sua última linha de defesa. Algumas etapas que podem ser realizadas para ajudar a proteger seu sistema são:

- Proteger as contas e as permissões do sistema de arquivos de seus servidores de bancos de dados e da web.
- Usar uma detecção ou proteção de invasão com base em hosts que esteja alerta às tentativas de invasão.
- Usar antivírus e detecção de malwares para procurar infecções de bots.
- Monitorar aplicativos da web, servidores da web e logs de bancos de dados em busca de comportamentos suspeitos.

Ajudando a proteger sua rede

Seguir as etapas da seção anterior ajudará a manter seguros os servidores que está protegendo contra a injeção de SQL. No entanto, supervisionar estes servidores pode não ser suficiente para proteger sua rede contra injeção de SQL. Caso existam servidores desprotegidos ou desconhecidos em sua rede, eles podem fornecer uma base fértil para ataques. O uso adequado de firewalls e proteção ou detecção de invasões baseadas em rede pode ajudar a preencher esta lacuna. Bloquear as solicitações recebidas da web aos endereços que não sejam servidores autorizados pode ajudar a proteger os aplicativos internos contra ataques externos. É preciso considerar a utilização de firewalls dos aplicativos da rede ou defesas com base em proxy para o tráfego da web que é autorizado a entrar em sua rede. Além disso, todos os principais fornecedores de detecção de invasões baseadas em rede fornecem determinado nível de detecção de injeção de SQL. Os métodos de detecção podem variar de acordo com o fornecedor e variar de simples combinações de expressões regulares sobre as sequências conhecidas de ataques a algoritmos complexos de pontuação. Considere o seguinte ao proteger sua rede contra a injeção de SQL:

- Leia a descrição de quaisquer assinaturas de injeção de SQL oferecidas por seu fornecedor. Algumas assinaturas são muito específicas e somente disparam em circunstâncias limitadas, enquanto outras são mais amplas e propensas a falsos positivos. É importante saber quais critérios são usados para cada alerta.
- Muitas coisas se parecem com SQL para um Sistema de Detecção de Invasões, mas nem sempre o são. Os resultados das buscas, a Linguagem de Consulta do Yahoo (YQL), a Linguagem de Consulta do Facebook e os feeds de Twitter são falsos positivos comuns. Os eventos de saída de injeção de SQL podem ser uma preocupação caso haja muito conteúdo proveniente do mesmo endereço, mas é provável que existam falsos positivos em muitas assinaturas de injeção de SQL devido aos eventos acionados por usuários. Mais interessantes são as tentativas recebidas de injeção de SQL, já que são elas que podem comprometer sua rede.
- Escaneie periodicamente sua rede em busca de servidores da web desconhecidos. Caso encontre um, rastreie o seu proprietário e assegure que foram realizadas as etapas para mitigar um ataque de injeção de SQL. Considere também os testes terceirizados de penetração ou a compra de softwares que procurem especificamente os sites vulneráveis à injeção de SQL.
- Forneça uma política ou diretrizes de segurança que identifiquem os possíveis problemas de segurança e que ofereçam soluções.

Apenas a proteção da rede não é uma proteção suficientemente adequada; no entanto, caso seja possível identificar e abordar uma violação de segurança com antecedência, é possível mitigar os danos que podem ser causados pelo invasor. Isso é especialmente importante para os sistemas que não contêm dados sensíveis, já que são os sistemas com menor probabilidade de serem protegidos. Mesmo se o sistema em si não for crítico, um comprometimento quanto à raiz de sua rede é uma coisa perigosa.

Conclusão

Se forem adotadas as precauções adequadas, o risco de um ataque de injeção de SQL ser bem-sucedido é muito baixo. No entanto, é importante permanecer sempre alerta, à medida que as novas necessidades de negócios tendem a trazer novos recursos e tecnologias. Sempre que um aplicativo da web conectado a um banco de dados é implementado ou passa por uma revisão de código, existem riscos. Todas as alterações de códigos devem ser revisadas e a instrução de seus desenvolvedores de web deve ser um processo contínuo. Assim que os invasores conseguirem explorar com êxito uma entrada de usuário não verificada, eles continuarão a tentar ataques de injeção de SQL. Com a tendência de ataques de injeção em massa acionados por bots, é quase possível garantir que alguém tentará atacar seus sites. Você estará pronto?

Para mais informações sobre a proteção de seus servidores contra a injeção de SQL, visite os links a seguir:

Protegendo Java:
http://today.java.net/pub/a/today/2005/09/08/handling-java-web-app-input.html

Protegendo ASP.NET:
http://msdn.microsoft.com/en-us/library/ff648339.aspx

Protegendo PHP:
http://php.net/manual/en/security.database.sql-injection.php

Dicas de Segurança de Bancos de Dados:
http://en.wikipedia.org/wiki/Database_security

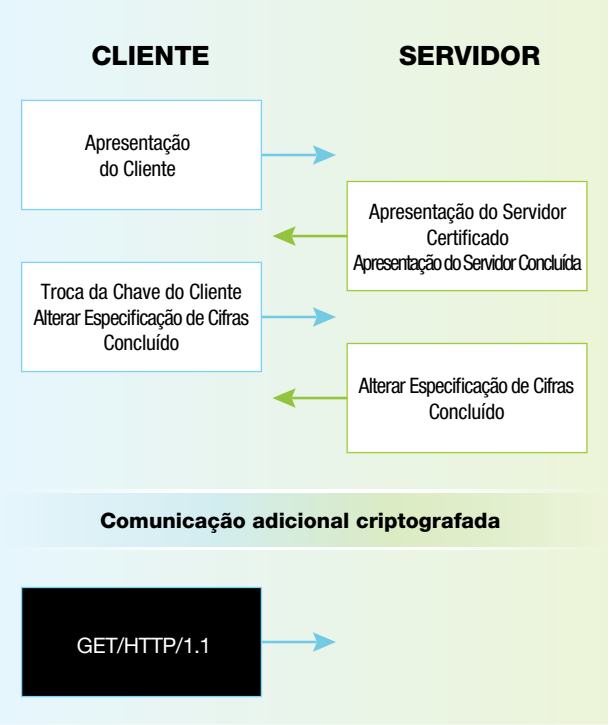
Desafios à segurança do SSL

A liberação do plug-in Firesheep em 2010 demonstrou a segurança inerente de HTTP e como o seu uso era bastante difundido nos websites populares que hospedavam informações pessoais sensíveis. Em resposta, sites como Facebook e Twitter também adotaram HTTPS para trazer mais segurança e privacidade aos seus usuários. Em virtude deste progresso, foi desanimador ver o ano de 2011 apresentar diversos problemas de alto perfil com os protocolos SSL e TLS que servem de base para HTTPS. Este artigo apresenta uma análise mais próxima de três dos incidentes proeminentes do ano que afetaram SSL/TLS e o seu impacto sobre a paisagem de ameaças.

THC-SSL-DOS

Em fevereiro (e novamente com mais publicidade no fim de outubro), um grupo de segurança, o The Hacker's Choice, forneceu uma ferramenta comprovada para realizar um ataque de negação de serviços (DOS) contra os servidores que se comunicavam por SSL/TLS. A ferramenta mostrou o potencial que um laptop rotineiro de uma conexão média tinha de desativar todo o servidor da web de uma empresa. Ela funcionava explorando as assimetrias conhecidas dos recursos computacionais necessários para configurar a criptografia durante a troca do TLS.

A troca do TLS



Durante uma troca típica de TLS, há vários eventos. O cliente inicia a troca com uma mensagem de "Apresentação do Cliente", listando uma série de conjuntos de cifras que podem ser executadas. Então, o servidor responde com uma mensagem de "Apresentação do Servidor", indicando o conjunto de cifras selecionado para criptografar a comunicação. No mesmo pacote, o servidor inclui uma mensagem de "Certificado" que contém o certificado do site, que estabelece sua identidade e fornece uma chave pública para a criptografia.

Caso as informações fornecidas correspondam às do cliente, ele responde com uma mensagem "Troca da Chave do Cliente" (seguida das mensagens "Alterar Especificação de Cifras" e "Concluído"). A "Troca da chave do cliente" contém um segredo pré-mestre criptografado com a chave pública do certificado do servidor. Mediante o recebimento da mensagem "Troca da Chave do Cliente", o servidor descriptografa o segredo pré-mestre com sua chave privada (e responde com suas próprias mensagens "Alterar Especificação de Cifras" e "Concluído"). Neste momento, o cliente e o servidor podem gerar suas chaves mestre e configurar sua criptografia, que será usada no resto da sessão.

Na troca (e, posteriormente, na criptografia simétrica do tráfego), o maior sucesso dos custos computacionais é encontrado na criptografia e descriptografia do segredo pré-mestre na mensagem "Troca da Chave do Cliente". Embora o cliente e o servidor usem o algoritmo RSA, o servidor tem um custo computacional maior (e, dependendo de coisas como a extensão da chave RSA, um custo ainda maior). As especificidades deste comportamento são interessantes, mas estão além do escopo deste artigo.

A ferramenta pode ser particularmente efetiva para desativar um servidor devido ao seu uso de renegociação de conjuntos de cifras iniciados pelos clientes. No protocolo TLS, há uma capacidade integrada para que cada extremidade do canal criptografado renegocie o conjunto de cifras utilizado. Essencialmente, a renegociação causa outra troca e, com ela, o mesmo custo computacional. A renegociação iniciada pelos clientes permite que um único cliente faça com que um servidor execute trocas de TLS que são realizadas com a mesma rapidez com que é possível solicitá-las. Usar a renegociação permite que um ataque use um número menor de máquinas e, portanto, fique sob o radar dos limites típicos de conexão de ataques de negação de serviços (DOS) distribuídos.

Mitigação

O impacto da exploração pode ser mitigado por várias coisas, mas nenhuma delas é uma solução genial. A maneira mais simples é desativar a renegociação iniciada pelos clientes. 99% dos sites não precisam oferecer suporte a este recurso; portanto, ele deve ser desativado quando for desnecessário. Devido a uma vulnerabilidade anterior a ataques man-in-the-middle (MITM) de TLS (CVE-2009-3555), muitos servidores da web desativam este recurso de modo padrão.

Nem todos os conjuntos de cifras incorrem nos mesmos custos computacionais relacionados aos servidores que o RSA. Infelizmente, nem todos os navegadores oferecem suporte a estes conjuntos de cifras e, mesmo assim, seriam escolhas ruins para clientes de baixo desempenho, como os dispositivos móveis. Não oferecer suporte a RSA não é uma opção viável, especialmente considerando-se que ele é obrigatório para TLS 1.1 e 1.2.

Se a renegociação iniciada pelos clientes for desativada, o custo computacional de 10.000 trocas em uma única conexão pode ser atingido com a troca inicial em 10.000 conexões. Assim, este ataque se torna um ataque DOS tradicional. O dano causado por ataques distribuídos pode ser mitigado com os standbys antigos de IDS e/ou com a inclusão de mais hardware.

Vale a pena observar que a assimetria computacional de determinados conjuntos de cifras não será fixada no TLS/SSL. A assimetria computacional pode ser levada ao lado do cliente por meio de um "quebra-cabeça" que exige que o cliente tenha mais esforços, mas esta não é uma solução geralmente aceita. Como Eric Rescorla enfatizou em uma postagem de blog sobre este problema: "(...) os invasores de DOS geralmente usam botnets (isto é, os computadores comprometidos de outras pessoas) para fazer seus ataques e, portanto, possuem uma quantidade bem grande de CPUs disponíveis. Isso dificulta bastante a criação de um quebra-cabeça que, por sua vez, cria um desafio suficiente aos invasores, a fim de reduzir a ameaça de ataques sem causar grandes impactos sobre as pessoas com poucos recursos computacionais, como as pessoas em dispositivos móveis" [4].

A BEAST

Em 23 de setembro, os pesquisadores de segurança Juliano Rizzo e Thai Duong demonstraram um ataque aos participantes da conferência de segurança Ekoparty que descriptografava os cookies de sessões da conexão HTTPS de um cliente ao paypal.com. A ferramenta era chamada BEAST (Browser Exploit Against SSL/TLS). O ataque explora os pontos fracos há muito conhecidos do uso do SSL 3.0 e do TLS 1.0 de um Vetor de inicialização implícito (IV) ao usar o modo de encadeamento de blocos de cifras (CBC). Embora esta vulnerabilidade seja conhecida há muito tempo, ela era considerada hipotética até que estes dois pesquisadores demonstraram a sua viabilidade.

A discussão anterior de conjuntos de cifras na troca do TLS concentrava-se no algoritmo de troca de chaves. O conjunto de cifras também define o algoritmo de criptografia em massa que é usado para criptografar os dados por meio da conexão estabelecida de TLS. O TLS oferece suporte a duas famílias de algoritmos de criptografia em massa, as cifras sequenciais e as cifras de bloco. Este último tipo opera em modo CBC.

As cifras de bloco trabalham quebrando o texto simples em blocos discretos com um tamanho fixo e, depois, criptografando-os. Em modo CBC, o texto simples de um bloco é testado por XORed com o texto cifrado do bloco anterior e, depois, criptografado. No entanto, o primeiro bloco a ser criptografado não tem um texto cifrado precedente e deve substituir o IV. A vulnerabilidade está na maneira como as versões afetadas do SSL/TSL usam um IV implícito do texto cifrado do último bloco ao criptografar um novo registro.

O invasor tem que atender alguns requisitos para realizar o ataque. Primeiro, ele precisa conseguir monitorar os dados HTTPS criptografados do cliente. Depois, ele precisa conseguir controlar as partes do texto simples enviadas do cliente por meio do canal HTTPS, como um caminho de URL, e também encontrar uma maneira de controlar o texto simples do último bloco criptografado. O primeiro requisito, embora mais difícil de conseguir em relação a um acionamento por download, não é impossível. O protocolo TLS/SSL existe porque as pessoas não confiam nos intermediários da Internet; sem ele, seria possível simplesmente entrar em uma rede wireless insegura.

4 http://www.educatedguesswork.org/2011/10/ssltls_and_computational_dos.html

Os pesquisadores indicaram algumas tecnologias comuns, como Java e Silverlight, que satisfazem a capacidade do segundo requisito para criar tráfego (e incluir um cookie). Na demonstração, a exploração do segundo requisito era facilitada pelo aproveitamento de uma vulnerabilidade (agora abordada) das verificações de política de mesma origem (SOP) dos plug-ins de Java, que permitiam que um applet de uma origem, por exemplo, http://www.invasor.com.br, enviasse solicitações a outro, http://www.paypal.com.

Com isso, o invasor pode descriptografar de modo efetivo as partes de texto simples, um byte por vez. Em termos gerais, o invasor faz com que o cliente faça uma solicitação da qual, para determinado bloco, o invasor já sabe tudo, menos um único byte do texto simples. Então, o bloco criptografado da transferência é interceptado e registrado. Assim, o invasor adivinha o byte desconhecido e o coloca no fim de um registro para que ele possa ser usado como o IV do próximo registro. Em média, bastam 126 tentativas para que o invasor veja um bloco criptografado que corresponde ao que está procurando. Agora, o invasor sabe qual é o byte e ajusta a próxima solicitação para decifrar o próximo byte. Isso continua até que o invasor decifre o cookie da sessão (ou o que mais estiver buscando).

Mitigação

O problema de usar um Vetor de inicialização implícito é conhecido há anos e foi corrigido no TLS 1.1. Infelizmente, poucos navegadores realmente oferecem suporte ao TLS 1.1; portanto, alterar os servidores para usar apenas o TLS 1.1 pode não ser uma opção. As cifras sequenciais, como RC4, não têm este problema e, então, priorizar um servidor para usar este tipo de cifras para a comunicação era a única alternativa razoável para isso. Uma solução para esse problema precisa ser encontrada por parte do cliente. Infelizmente, existem algumas implementações do SSL/TLS que não funcionam com a correção de backport do TLS 1.1. Os fornecedores estão abordando este problema, embora os problemas com a interoperabilidade compliquem a questão. A Microsoft, por exemplo, liberou uma correção para abordar esta vulnerabilidade na atualização mensal de janeiro de 2012.

Comprometimentos da DigiNotar e da Comodo

O problema de usar um Vetor de inicialização implícito é conhecido há anos e foi corrigido no TLS 1.1. Infelizmente, poucos navegadores realmente oferecem suporte ao TLS 1.1; portanto, alterar os servidores para usar apenas o TLS 1.1 pode não ser uma opção. As cifras sequenciais, como RC4, não têm este problema e, então, priorizar um servidor para usar este tipo de cifras para a comunicação era a única alternativa razoável para isso. Uma solução para esse problema precisa ser encontrada por parte do cliente. Infelizmente, existem algumas implementações do SSL/TLS que não funcionam com a correção de backport do TLS 1.1. Os fornecedores estão abordando este problema, embora os problemas com a interoperabilidade compliquem a questão. A Microsoft, por exemplo, liberou uma correção para abordar esta vulnerabilidade na atualização mensal de janeiro de 2012.

Em meados de julho, houve outro comprometimento, desta vez da CA DigiNotar. Se o que aconteceu com a Comodo foi um desastre, esse foi uma catástrofe da segurança. Foram emitidos mais de 500 certificados fraudulentos para domínios como "*.google.com", bem como para o incrivelmente amplo "*.*.com". O relatório oficial Fox-IT sobre a violação indicou que mais de 300.000 IPs únicos tinham acessado um certificado fraudulento do Google. A resposta para isso, assim como na violação anterior, exigiu que os fornecedores de navegadores se esforçassem para liberar atualizações para seus produtos, a fim de revogar estes certificados do modo mais rápido possível.

As atualizações de produtos podem parecer uma medida drástica para revogar certificados; no entanto, devido aos mecanismos atuais, elas são compreensíveis.

Revogação de certificados

A necessidade de revogação de certificados em virtude de fraudes ou de atualização de informações foi compreendida e foram criadas soluções para isso. Dois métodos são geralmente utilizados para verificar o status da revogação: as listas de revogação de certificados (CRLs) e o protocolo de status de certificados online (OCSP). Infelizmente, nenhuma dessas soluções é realmente efetiva.

Usando o primeiro método, as informações das CRLs podem ser inclusas em um certificado. Quando o cliente estiver autenticando um certificado, ele pode fazer o download deste na CRL indicada, fazer o download de uma lista dos números de série dos certificados revogados e verificá-los para determinar se quaisquer certificados encontrados foram revogados. O OCSP, por outro lado, é um protocolo desenvolvido para que um cliente possa emitir uma solicitação para um certificado individual, em vez de fazer o download de toda uma lista, a fim de verificar o status da revogação.

Nenhuma abordagem funciona bem porque as implementações têm o padrão de falhar, permanecendo abertas. Caso o cliente não receba uma notificação da revogação, ele supõe que o servidor estava inativo e que o certificado era válido. O problema óbvio é que, caso um MITM possa interceptar o tráfego e apresentar um certificado inválido, provavelmente, ele também pode bloquear qualquer resposta de revogação.

Mais importante do que não haver um bom método para revogar os certificados fraudulentos, é o fato de que esses comprometimentos indicam problemas muito maiores no próprio modelo de confiança do SSL.

Modelo de confiança do SSL

Os dois principais objetivos do SSL e TLS são estabelecer a autenticidade e a confidencialidade das comunicações. Para fornecer autenticidade e impedir que um MITM personifique um servidor, o SSL foi desenvolvido com a noção de certificados e autoridades de certificação (CAs). Caso um site deseje fornecer HTTPS, isso exige um certificado, que ele pode solicitar de uma autoridade de certificação. As CAs são entidades confiáveis, representadas por empresas como Verisign, Thawte, Comodo ou DigiNotar, cujo trabalho é verificar se o site corresponde ao identificado e, então, emitir um certificado para representar este fato.

Assim, os navegadores da web podem vir pré-instalados com certificados destas autoridades confiáveis para que, quando for apresentado um certificado arbitrário, os navegadores possam verificar a validade deste certificado em relação aos seus certificados confiáveis. No entanto, voltando ao caso do MITM, um invasor pode criar um certificado falso para um site e, depois, apresentá-lo a um cliente que tenta se conectar a um site legítimo. Já que o certificado do invasor não foi assinado por uma autoridade de certificação confiável, o navegador do cliente apresenta um aviso e, assim, o cliente sabe que não acessou o site autêntico.

Problemas com o modelo de confiança do SSL

Este modelo tem alguns problemas. No sistema, todas as CAs são tratadas como iguais. Um certificado emitido por uma CA é tão válido quando um emitido por outra. Um exemplo seria um certificado emitido para "*.google.com" a partir de uma CA aleatória, que será tão válido para um navegador quanto um certificado emitido pela autoridade de registro real do Google.

De acordo com o projeto observatório do SSL da Electronic Frontier Foundation (EFF), há mais de 600 entidades que podem emitir certificados. Com este grande número de empresas, não é surpreendente descobrir que há níveis diversos de qualidade da segurança dos sites, bem como níveis diversos de verificação de um certificado solicitado. As CAs não precisam ser hackeadas para que um certificado seja emitido à parte errada. Isso já ocorreu no passado e, sem dúvidas, continuará no futuro.

Outra consequência do sistema é que, assim que uma CA se torna confiável, ela permanece assim. As CAs podem emitir certificados para milhões de sites. Caso um cliente decida não confiar mais em uma CA e remova seu certificado de seu armazenamento, todos os sites assinados por aquela CA não ficam mais disponíveis no HTTPS.

Revisando a confiança do SSL

Foram propostas soluções para abordar estes problemas. Existem propostas de uso de DNS para manipular a confiança, como DNS-based Authentication of Named Entities (DANE) e a Certificate Authority Authorization (CAA). Estas propostas permitem que as informações sobre as CAs autorizadas sejam integradas no registro DNS de um domínio. Uma CA pode usar essas informações para verificar quem deveria emitir certificados para determinado domínio, como um meio de ajudar a impedir a emissão inadvertida às partes incorretas. Os clientes podem usar essas informações para verificar se um certificado foi emitido por uma CA adequada.

A DANE também possibilita uma alternativa à confiança das CAs. Um site pode integrar informações de certificados ao registro de seu domínio. Quando um cliente acessa um site, é possível comparar o certificado do domínio ao certificado fornecido. Se os certificados forem correspondentes, é possível presumir que o site foi autenticado. As desvantagens dessas abordagens é que a CAA e a DANE exigem Domain Name System Security Extensions (DNSSEC) para que sejam seguras e a DNSSEC ainda não é amplamente utilizada.

O caso de uma alternativa ao mecanismo atual de confiança e o uso de DNS foram propostos por Moxie Marlinspike[5] em um artigo de blog e, posteriormente, apresentados na BlackHat USA. Ele enfatizou que o uso de DNS não torna um certificado mais confiável. Caso um cliente esteja preocupado com o fato de os certificados emitidos por uma CA governamental estarem sendo abusados para interceptar o tráfego, como a situação melhora ao depender dos dados dos certificados provenientes dos servidores DNS deste mesmo país?

Marlinspike falou sobre a necessidade de "agilidade da confiança" em SSL. Os dois principais princípios são: um cliente pode revogar a confiança de uma agência a qualquer momento e pode escolher onde depositar sua confiança. Consequentemente, Marlinspike desenvolveu um plug-in para Firefox chamado "Convergence", que implementa estes requisitos permitindo que um usuário escolha diversos "certificadores" que validam o certificado de um site, resultando em um sistema flexível no qual os certificadores são livres para impor seus próprios requisitos de segurança sobre a validação e os usuários são livres para escolher em quais certificadores confiarão.

5 http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity
http://www.youtube.com/watch?v=Z7Wl2FW2TcA

No modelo atual de CAs, assim que uma CA se torna confiável, ela é essencialmente confiável para sempre. As CAs podem emitir milhões de certificados usados em websites na Internet. Um exemplo seria o caso de, em algum momento, um cliente decidir não confiar na Verisign e remover o certificado da CA de seu armazenamento; como resultado, nenhum site com um certificado emitido por ela até mesmo um certificado emitido no passado, quando ela ainda era confiável – será acessível pelo HTTPS. Compare isso à agilidade da confiança por meio do uso do Convergence, no qual é possível parar de confiar de determinado certificador, mas os outros certificadores confiáveis ainda podem atestar a segurança do certificado do site. O sistema de certificadores parece uma ótima ideia, principalmente para os usuários; no entanto, não se sabe como as organizações seriam motivadas a iniciar seus negócios e a se sustentar sem um claro incentivo financeiro.

Outra solução que também fornece agilidade à confiança é estender o TLS/SSL para oferecer suporte a diversos certificados. Caso um site possa fornecer diversos certificados assinados por diferentes CAs, como um pela DigiNotar e um pela Verisign e, então, o cliente decida não confiar na DigiNotar, a Verisign ainda seria considerada confiável e, portanto, estabeleceria uma conexão segura. Um grande obstáculo para esta solução é o fato de ela exigir uma alteração ao protocolo TLS e a baixa adoção das novas versões do protocolo por parte dos fornecedores.

O que o futuro reserva?

O SSL foi desenvolvido inicialmente no início da década de 90 para proteger as comunicações de uma variedade de sites. Atualmente, ele está na versão TLS 1.2 e protege mais de dois milhões de websites. O TLS 1.1 ainda deve apresentar uma adoção difundida, mas, à medida que os problemas anteriormente considerados teóricos forem comprovados como reais, provavelmente haverá uma aceitação mais rápida das versões futuras. Espera-se que haja uma implementação mais difundida dos conjuntos de cifras mais recentes, como ECDHE_RSA, nos clientes e servidores, o que pode fornecer uma confidencialidade progressiva, a fim de que o vazamento da chave privada de um certificado não possa ser usado de modo retroativo para descriptografar o tráfego anteriormente registrado. É quase inevitável que o modo atual de confiança do SSL tenha que ser alterado, mas provavelmente este tipo de alteração a um aspecto estabelecido e defeituoso do protocolo ainda demore muito a chegar.

O surgimento de malwares de Mac

Introdução

Mais que no ano anterior, 2001 apresentou a maioria das atividades do ambiente de malwares de Mac[6]. Isso se aplica não apenas ao volume, mas também à funcionalidade. Em 2011, começamos a ver malwares de Mac com funcionalidades somente vistas anteriormente em malwares de Windows. Isso pode indicar que os criminosos cibernéticos agora estão se conscientizando da possível rentabilidade de visar ao SO X.

Analisaremos alguns dos malwares de Mac mais notáveis descobertos em 2011.

MacDefender

O MacDefender foi descoberto primeiramente em maio de 2011, com variantes subsequentes (chamadas MacSecurity, MacProtector, MacGuard e MacShield) descobertas nos meses seguintes. O que tornou o MacDefender interessante, é que este é o tipo de malware com um mecanismo difusor que aumentou no ambiente de Windows nos últimos anos. O MacDefender

6 http://blog.intego.com/dl/Intego-year-in-Mac-security-2011.pdf

pertence à categoria de malwares chamada “Rogue Antivírus”, que se disfarça de programas antivírus legítimos. Depois de instalado, ele finge escanear seu sistema, sinalizando arquivos aleatórios como maliciosos para fazer parecer que seu sistema está gravemente infectado.

A interface com o usuário tem aparência profissional e bem feita para fazer com que os usuários acreditem que este é um aplicativo legítimo. A interface com o usuário contém um botão Register que leva o usuário a um website no qual ele supostamente compra uma licença do MacDefender usando um cartão de crédito. O MacDefender exibe uma mensagem que diz que, para remover o malware detectado, é preciso pagar pela versão licenciada; portanto, um usuário pode se sentir forçado a se registrar. Depois, o cartão de crédito do usuário é cobrado em relação ao valor e, além disso, o número do cartão pode ser usado também para outros propósitos.

Figura 12: Captura de tela do malware MacDefender, 2011

O MacDefender e suas variantes são difundidos, visando aos usuários por meio de ataques de envenenamento de SEO, nos quais os autores de malware manipulam os resultados dos mecanismos de busca para fazer com os links que hospedam os malwares sejam exibidos próximos ao tipo dos resultados da busca. Quando um usuário clica em um destes links, O Javascript faz o download do instalador do MacDefender em seu sistema. Caso a configuração do navegador seja ajustada para abrir automaticamente os arquivos seguros após o download, o instalador é aberto automaticamente.

Os “rogue antivírus” são scams altamente lucrativos; portanto, a X-Force acredita que serão vistos mais destes tipos de malware no futuro. Os usuários devem ter cuidado ao clicar em um link, verificar se o nome do domínio deste link está relacionado ao que está buscando. Além disso, não instale softwares, a menos que tenha certeza de que ele é proveniente uma fonte confiável.

Flashback

O Flashback é um Trojan descoberto em setembro de 2011. As variantes deste malware apareceram nos meses seguintes, cada uma delas com várias melhorias em relação ao original. O Flashback se disfarça como um instalador do Flash Player cujo download pode ser feito ao visitar websites maliciosos que exibem um ícone de download ou instalação do Flash Player.

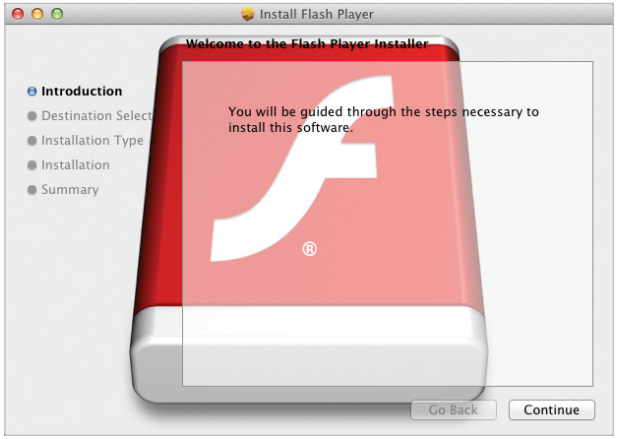


Figura 13: Captura de tela do Trojan Flashback, 2011

Quando instalado, o Flashback fornece um arquivo dinâmico de biblioteca compartilhada e usa a variável do ambiente DYLD_INSERT_LIBRARIES para injetar o código no aplicativo aberto pelo usuário. As variantes posteriores visam aos aplicativos específicos, como Safari e Firefox, para injetar o código. O código injetado é responsável por entrar em contato com um servidor remoto para fazer download de atualizações ou enviar dados a partir da máquina infectada. Esta técnica de injeção de código é similar à de alguns malwares notáveis de Windows, como o Zeus, que injeta o código nos navegadores da web. O Zeus intercepta as páginas da web passadas do servidor ao navegador e as modifica durante a execução antes de mostrá-la ao usuário. Geralmente, a página da web modificada mostra uma página de login falsa, permitindo que o malware roube informações sensíveis. Felizmente, até agora não foi observada nenhuma funcionalidade de injeção da web em nenhuma das variantes do Flashback.

O Flashback também tenta impedir atualizações futuras ao XProtect, sobrescrevendo alguns arquivos relevantes. O XProtect é o sistema integrado de proteção básica contra malwares da Apple, que usa combinação de sequências para detectar malwares. A Apple atualizar o XProtect sempre que é descoberto um malware de Mac de alto perfil.

O Flashback também tenta frustrar as análises dos pesquisadores, detectando se existe uma execução sendo feita em uma máquina virtual VMWare. Usar este mecanismo de evasão de detecção é comum em malwares de Windows, mas este é o primeiro malware de Mac que utiliza esta técnica. Isso demonstra que a tecnologia de malwares de Mac está acompanhando a tecnologia similar relacionada ao Windows.

DevilRobber

O DevilRobber é o malware de SO X mais recente de 2011. Ele foi descoberto em outubro de 2011 e teve variantes liberadas nos meses de novembro e dezembro. O DevilRobber foi descoberto nos aplicativos de Mac que eram compartilhados ilegalmente no BitTorrent, como o GraphicConverter, Flux, CorelPainter e Pixelmator.

O DevilRobber é o malware de Mac mais sofisticado encontrado até o momento e contém diversos componentes. Ele é principalmente uma porta dos fundos que permite que a máquina infectada receba comandos de um invasor remoto, mas uma funcionalidade interessante sua é a mineração BitCoin, na qual ele instala o aplicativo de mineração BitCoin chamado DiabloMiner para usar a potência computacional da CPU e da GPU (dos usuários com placas gráficas de alto desempenho) da máquina infectada, a fim de realizar a mineração de Bitcoins. Ele também tenta roubar a carteira de Bitcoin, caso ela seja encontrada. O DevilRobber também rouba a Keychain do usuário, com outras informações da máquina infectada e faz o upload delas em um servidor FTP remoto.

Ele também tem a capacidade de detectar se a máquina infectada funciona sob um dispositivo de gateway e, então, ativa o encaminhamento de portas por UPnP. Isso permite que o invasor acesse remotamente a máquina infectada usando a porta aberta pelo DevilRobber, mesmo se a máquina infectada funcionar sob um dispositivo de gateway.

Conclusão

Como pode ser observado, nenhum malware mencionado usa quaisquer explorações de vulnerabilidades de software para se espalhar. Especula-se que isso se deve à falta de explorações do SO X, que são disponíveis ao público para reuso. A maioria dos malwares de Windows que usa explorações muitas vezes reutiliza as explorações disponíveis ao púbico, como os encontrados em estruturas de exploração, como a Metasploit, com

pequenas modificações. No entanto, há poucas explorações disponíveis publicamente para SO X. Isso pode se dar devido à falta de interesse no desenvolvimento de explorações para uma plataforma com participação no mercado relativamente baixa ou à falta de informações técnicas disponíveis para isso. A barreira de entrada está maior agora com as recentes melhorias de segurança na última versão do SO X. O SO X Lion implementa processos completos ASLR de 64 bits de modo padrão e uma estrutura de ambiente de simulação. A partir de junho de 2012, a Apple também exigirá que todos os aplicativos enviados à Mac App Store tenham o ambiente de simulação ativado e, portanto, realizem a mitigação das tentativas de exploração por meio de aplicativos de terceiros.

Isso não quer dizer que os usuários Mac devem ficar tranquilos. Conforme mostra o exemplo anterior, os autores de malware encontrarão meios alternativos para seu fornecimento. Além disso, estas melhorias se concentrar na prevenção e mitigação de explorações e não abordam realmente os tipos de malware mencionados anteriormente; portanto, espera-se encontrar mais malwares de Mac em 2012.

Por outro lado, a Apple certamente está realizando as etapas para aumentar ainda mais o custo do desenvolvimento de malwares para SO X. Na próxima versão anunciada recentemente do SO X, a Mountain Lion, foi incluído um novo recurso chamado Gatekeeper. O Gatekeeper permite que o usuário escolha quais aplicativos podem ser instalados e executados em seu sistema com base em sua proveniência. Os usuários podem optar por permitir somente aplicativos da App Store ou da App Store e dos desenvolvedores identificados (aplicativos com um ID de Desenvolvedor Apple associado). Eles também podem desativar este recurso caso decidam assim. De modo padrão, somente os aplicativos da App Store ou de desenvolvedores identificados podem ser instalados ou executados. Acreditamos que há um longo caminho para impedir ataques de malware de grande escala e em longo prazo.

À medida que os invasores notam o SO X, os fornecedores fazem o mesmo. Assim, a X-Force prevê que a próxima onda de malware de Mac utilizará maneiras de evadir a detecção e as análises. De modo surpreendente, a maioria dos malwares de Mac encontrados até o momento não se incomodou com nenhum mecanismo de evasão. Prevemos que as técnicas comuns ao ambiente de Windows, como empacotamento, antidepuração e detecção de máquinas virtuais serão mais utilizadas. Também se espera ver mais técnicas avançadas que funcionam efetivamente nos malwares de Windows sendo adaptadas aos malwares de Mac, como a tecnologia de disfarce e injeção na web ao estilo do Zeus e os rootkits. Eventualmente, os novos malwares também terão que lidar com o Gatekeeper mencionado acima; portanto, podemos encontrar malwares que tentarão evitá-lo de alguma forma.

O número ainda é muito baixo em comparação ao de malwares de Windows, mas é claro que os invasores estão começando a notar que os Macs estão se tornando alvos viáveis. Os usuários de Mac devem estar cientes de que os malwares encontrados anteriormente apenas no Windows também são possíveis no SO X.

Tendências de conteúdo da web

A equipe IBM Content Security revisa e analisa constantemente os novos dados de conteúdo da web e 150 milhões de novas páginas da web e imagens por mês. Desde 1999, foram analisadas 16 bilhões de páginas da web e imagens.

O banco de filtro da web da IBM tem 68 categorias de filtros e 70 milhões de entradas, com 150.000 entradas novas ou atualizadas por dia.

Esta seção fornece uma revisão de:

- Metodologia de análise
- Implementação de IPv6 para websites
- Aumento da quantidade de proxies anônimos
- Websites maliciosos

Metodologia de análise

A X-Force capta informações sobre a distribuição de conteúdo na Internet, contando os hosts categorizados no banco de dados de filtro da web da IBM Security Systems. A contagem de hosts é um método aceito para determinar a distribuição de conteúdo e fornece uma avaliação realista. Ao usar outras metodologias – como a contagem de páginas e subpáginas da web – os resultados podem ser diferentes.

Implementação de IPv6 para websites

À medida que o IPv4 vai ficando sem espaço, espera-se que cada vez mais sites de Internet mudem para o IPv6. No entanto, ao analisar os últimos cinco meses, esta expectativa não foi atendida. Para medir a implementação de IPv6 para websites, foram realizadas solicitações DNS (verificação de um registro AAAA em DNS) para milhões de hosts todos os meses.

A porcentagem de domínios que tem, no mínimo, um host que oferece suporte a IPv6 permaneceu relativamente uniforme e variou entre 2,2 e 2,6%.

Será interessante ver se há um aumento significativo do suporte a IPv6 no próximo World IPv6 Day[7], em 6 de junho de 2012, quando muitas empresas e organizações planejam implementar o IPv6 de modo permanente.

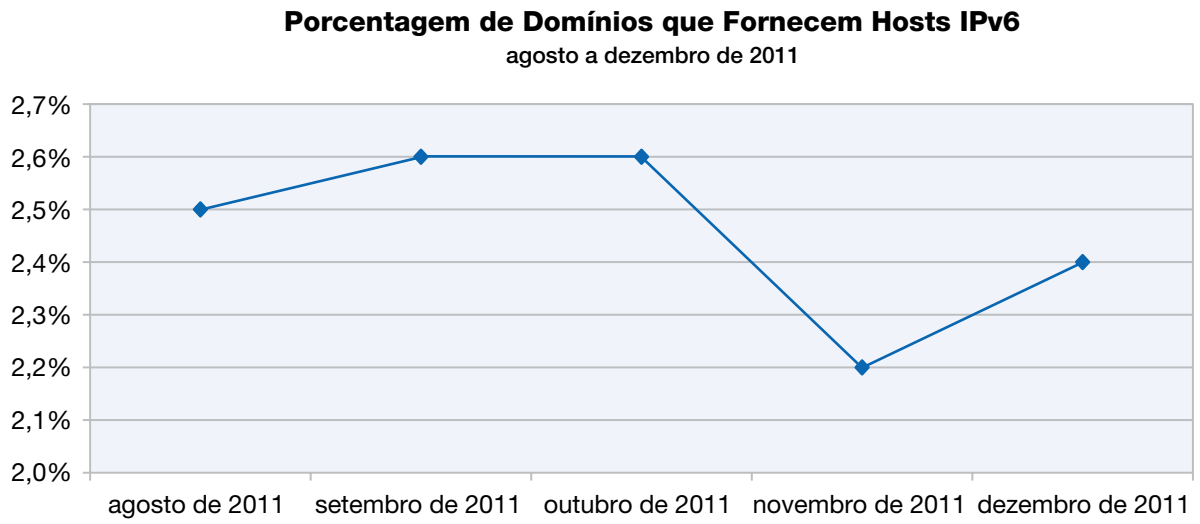


Figura 14: Porcentagem de Domínios que Fornecem Hosts IPv6 - agosto de 2011 a dezembro de 2011

7 http://en.wikipedia.org/wiki/World_ipv6_day

Aumento de proxies anônimos

À medida que a Internet se torna uma parte mais integrada de nossas vidas em casa, no trabalho e na escola, as organizações responsáveis por manter ambientes aceitáveis nestas configurações públicas encontram cada vez mais a necessidade de controlar os locais onde as pessoas podem navegar.

Um exemplo deste tipo de controle é um sistema de filtragem de conteúdo, que impede o acesso a websites inadequados ou inaceitáveis. Alguns indivíduos tentam usar proxies anônimos (também conhecidos como proxies da web) para evitar as tecnologias de filtragem da web.

Os proxies da web permitem que os usuários insiram uma URL em um formulário da web, em vez de visitar diretamente o website de destino. Usar o proxy oculta a URL de destino de um filtro da web. Caso este filtro não seja configurado para monitorar ou bloquear proxies anônimos, esta atividade (que geralmente poderia ter sido interrompida) contorna o filtro e permite que o usuário acesse o website não autorizado.

O crescimento de websites de proxies anônimos recém-registrados reflete esta tendência.

No primeiro semestre de 2011, houve quatro vezes mais proxies anônimos registrados em comparação a três anos atrás. No segundo semestre de 2011, houve ainda mais que três vezes o número de proxies anônimos que há três anos. No entanto, esta é a primeira vez desde o começo de 2009 em que não houve outro aumento deste volume. Talvez as atividades da Internet estejam mais focadas em redes sociais. Em muitos casos, estes sites não são bloqueados no trabalho ou nas escolas e, portanto, as pessoas não precisam mais evitar o sistema de filtragem de conteúdo.

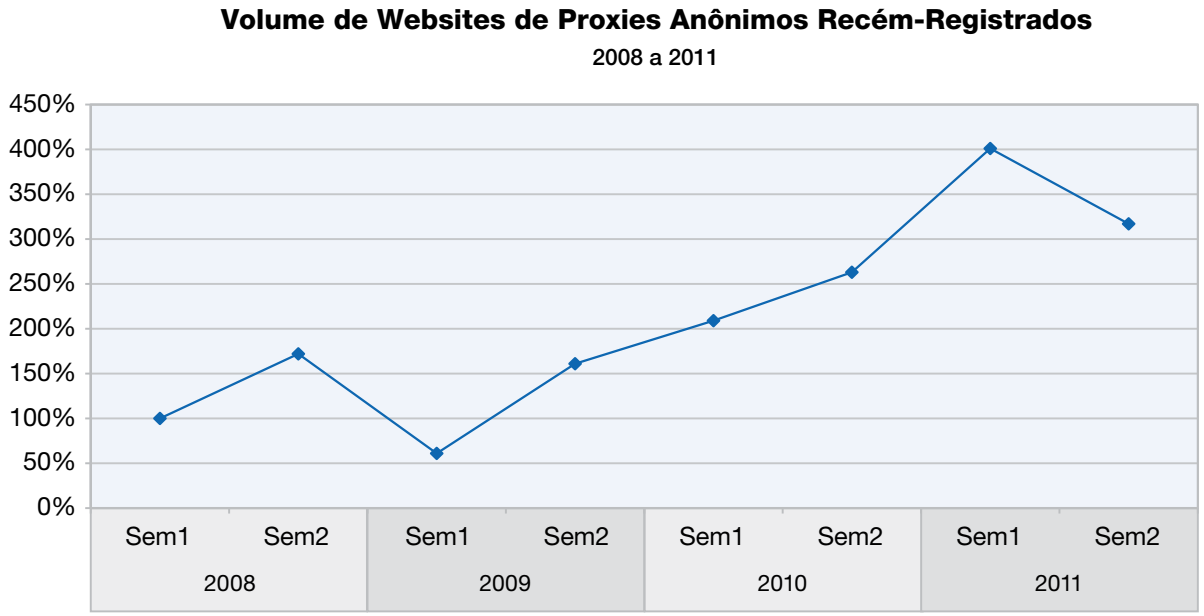


Figura 15: Volume de Websites de Proxies Anônimos Recém-Registrados - 2008 a 2011

No entanto, o uso de plataformas de rede social apresenta novos desafios, principalmente para as empresas que precisam controlar quais informações são compartilhadas com outros usuários e impedir o compartilhamento de informações confidenciais. Portanto, muitas empresas estão começando a usar sistemas de controle de aplicativos da web, muitas vezes como parte dos firewalls da próxima geração.

Os proxies anônimos permanecem um tipo fundamental de website a ser controlado por causa da facilidade com a qual os proxies permitem que as pessoas ocultem intenções possivelmente maliciosas.

Ao analisar os domínios de nível principal dos proxies anônimos recém-registrados, a tendência do primeiro semestre de 2011 – conforme relatado em detalhes no Relatório de Riscos e Tendências de Meados do Ano da IBM X-Force 2011 – continuou. Os domínios .tk e .com continuam a prevalecer, representando mais de 70% de todos os novos proxies anônimos.

Websites maliciosos

Esta seção discute os países responsáveis por hospedar links maliciosos com os tipos de websites que, muitas vezes, estão relacionados a estes websites maliciosos. A seção **Divulgações de vulnerabilidades de 2011** contém mais informações sobre os websites maliciosos no contexto de explorações.

Localização geográfica dos links maliciosos da web

Os Estados Unidos continuam a liderar como os principais hosts de links maliciosos. Mais de um terço de todos os links de malware estão hospedados nos EUA. O segundo da competição é a Romênia, que hospeda 8,5%. A China esteve na segunda posição nos últimos três anos; agora, está empatada com a França no terceiro lugar, responsável por 5,7%, como mostra a figura 16.

Os países da segunda camada também mudaram, mas estas mudanças são menores que 1% entre os números de 2010 e 2011.

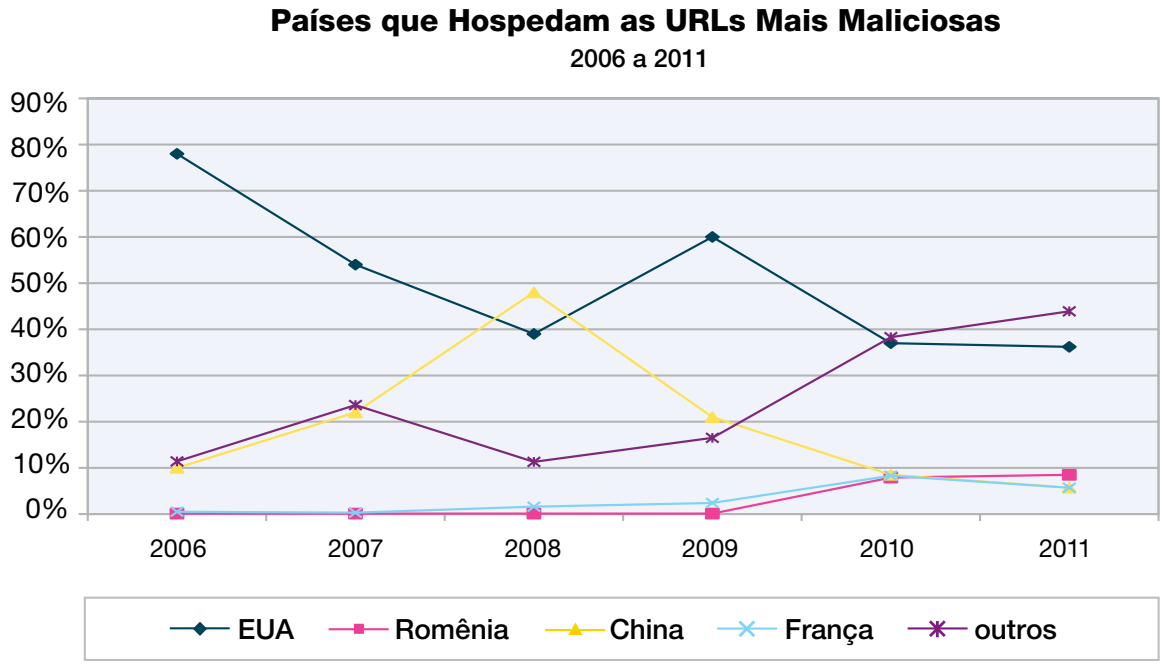


Figura 16: Países que Hospedam as URLs Mais Maliciosas - 2006 a 2011

Bons websites com links ruins

Como relatado nos Relatórios de Riscos e Tendências da IBM X-Force anteriores, os invasores estão se concentrando cada vez mais em usar a boa reputação dos websites confiáveis para reduzir a proteção dos usuários finais e ocultar suas tentativas com tecnologias de proteção. O uso de conteúdo malicioso da web não é diferente. A análise a seguir fornece um sinal dos tipos de websites que, muitas vezes, contêm links aos conteúdos maliciosos conhecidos.

Algumas das principais categorias podem não ser surpreendentes. Por exemplo, muitos podem esperar que a pornografia e os jogos estivessem no topo da lista. Juntos, eles agora compõem quase 40% de todos os links maliciosos. No entanto, os candidatos de segunda camada se enquadram em uma categoria mais confiável.

Os mecanismos de busca, blogs, quadros de avisos e websites pessoais se enquadram nesta categoria de segunda camada. A maioria destes websites permite que os usuários façam upload de conteúdo ou desenvolvam seu próprio website. Em outras palavras, é improvável que estes tipos de website estejam hospedando links maliciosos intencionalmente.

O gráfico a seguir mostra o histórico da distribuição de links de malware.

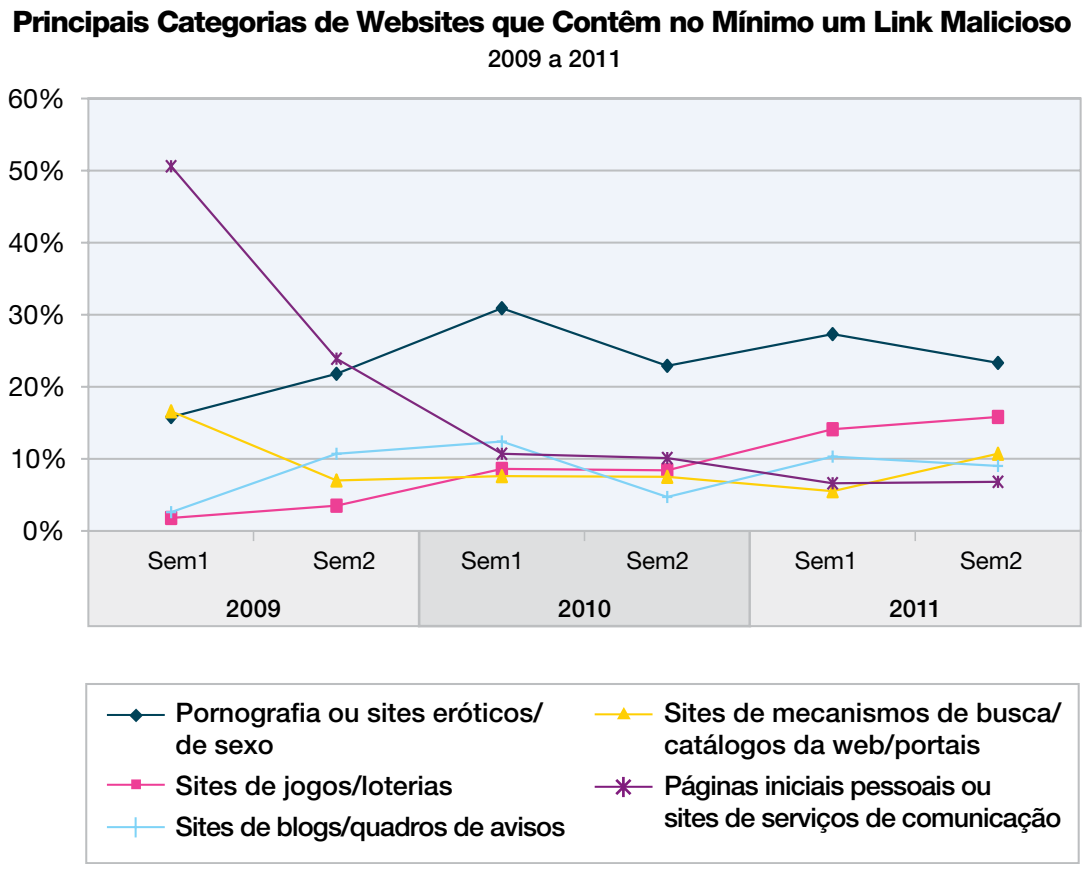


Figura 17: Principais Categorias de Websites que Contêm no Mínimo um Link Malicioso - 2009 a 2011

Ao analisar os últimos três anos, aparecem tendências interessantes.

- Atualmente, os websites profissionais "ruins", como de pornografia ou jogos, dominam claramente a situação e distribuem malwares de modo sistemático.
- A pornografia está no topo, estável em cerca de 23%.
- Os jogos são a única categoria com um aumento significativo periodicamente. Em relação ao histórico de 0,6% da população adulta que tem problemas com jogos[8], os sites de jogos são um alvo popular para os distribuidores de malware.
- Os blogs/quadros de avisos caíram para 9% nos últimos seis meses.
- As páginas iniciais pessoais – os websites Web 1.0 clássicos – perderam um terreno significativo. Um motivo pode ser que as páginas iniciais pessoais estejam mais fora de estilo em relação aos aplicativos Web 2.0, como perfis de redes sociais ou de negócios.
- Os sites de mecanismos de busca, catálogos na web e portais se recuperaram e atingiram mais de 10% pela primeira vez em dois anos e meio.

8 http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence

Spams e phishing

O banco de dados de filtros de URL e spams da IBM fornece uma visão abrangente dos ataques de spams e phishing. Com milhões de endereços de email sendo monitorados ativamente, a equipe de conteúdo identificou diversos avanços nas tecnologias de spams e phishing usadas pelos invasores.

Atualmente, o banco de dados de filtros de spam contém mais de 40 milhões de assinaturas relevantes de spam. Cada parte dos spams é dividida em várias partes lógicas (sentenças, parágrafos etc.). Uma assinatura única de 128 bits é computada para cada parte e para milhões de spams de URL. Todos os dias, há aproximadamente um milhão de assinaturas novas, atualizadas ou excluídas do banco de dados de filtros de spam.

Esta seção aborda os tópicos a seguir:

- O volume de spams continua a cair
- Principais tendências de spam em 2011
- Principais domínios comuns dos spams de URL
- Spam – o país9 das tendências originadoras
- Scams e phishing de email
- Flashback e prospectos futuros sobre os spams

O volume de spams continua a cair

No último Relatório de Riscos e Tendências, foram fornecidos detalhes aprofundados sobre o modo como os spams continuam a cair nos últimos três meses e até mesmo nos últimos anos. Acredita-se que isso se deve às diversas desativações de botnets, como foi discutido nos relatórios anteriores. No gráfico a seguir, é possível ver como esses números gerais continuam a cair.

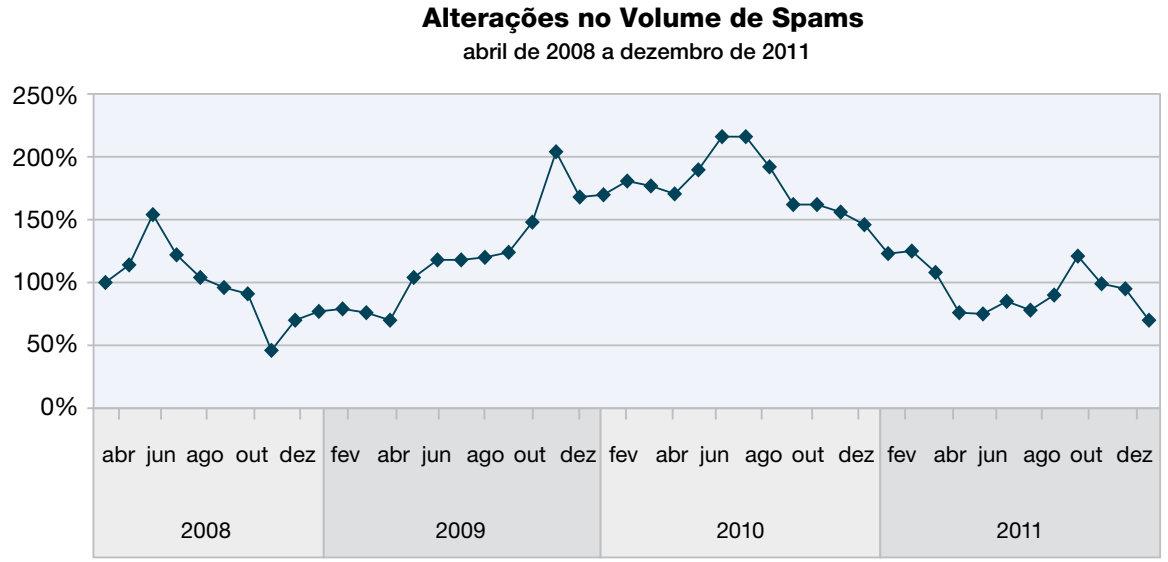


Figura 18: Alterações no Volume de Spams – abril de 2008 a dezembro de 2011

9 Neste relatório, as estatísticas de spams, phishing e URLs usam o IP-to-Country Database fornecido pela WebHosting.Info (http://www.webhosting.info), disponível em http://ip-to-country.webhosting.info. A distribuição geográfica foi determinada por solicitação dos endereços de IP dos hosts (em caso de distribuição de conteúdo) ou do servidor de correio de envio (em caso de spam e phishing) ao IP-to-Country Database.

Principais tendências de spams em 2011

O gráfico a seguir resume as principais tendências em spams que foram observadas em 2011.

É possível identificar diversas mudanças em relação aos aspectos dos spams enviados em 2011. Foram definidas diversas fases para destacar estas mudanças:

- **Fase 0 – Situação inicial:**
  Início em dezembro de 2010
- **Fase 1 – Primeira desativação da Rustock:**
  25 de dezembro de 2010 a 9 de janeiro de 2011
- **Fase 2 – Entre as desativações da Rustock:**
  10 de janeiro de 2011 a 15 de março de 2011
- **Fase 3 – Após a segunda desativação da Rustock:**
  16 de março de 2011 a 18 de maio de 2011
- **Fase 4 – Primeira recuperação do volume de spams:**
  19 de maio de 2011 a 22 de agosto de 2011
- **Fase 5 – Segunda recuperação do volume de spams:**
  23 de agosto de 2011 a 29 de novembro de 2011
- **Fase 6 – Redução do volume de spams ao final do ano:**
  Desde 30 de novembro de 2011

As fases de zero a quatro são discutidas em detalhes no Relatório de Riscos e Tendências de Meados do Ano da IBM X-Force. As novas fases cinco e seis foram dominadas por spam de Malware de ZIP ou RAR (novamente) e spams com base em imagens, como discutido nas duas próximas seções.

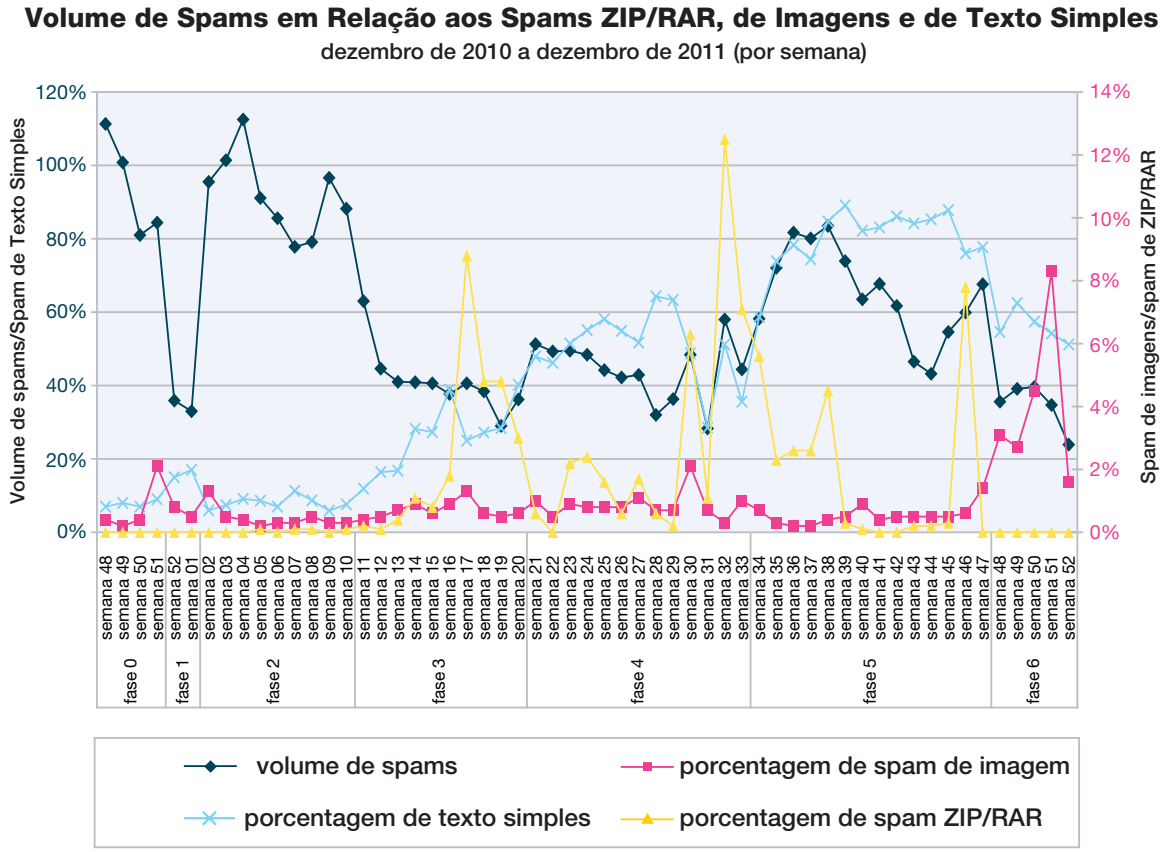


Figura 19: Volume de Spams em Relação aos Spams ZIP/RAR, de Imagens e de Texto Simples – de 2010 a dezembro de 2011 (por semana)

Ao analisar todo o intervalo de tempo, o aumento quase contínuo de spams de texto simples é particularmente significativo. Nos anos anteriores, foram encontrados de 5 a 30% de spams escritos em texto simples. Esta é a primeira vez que estes altos valores foram observados – algumas vezes superiores a 80% na fase cinco – por um período mais longo. Durante a fase seis, o valor caiu para cerca de 55%.

Os spams de texto simples dificultam a detecção de spams com base em conteúdo, já que não é um recurso fixo, como um tipo especial de anexo ou sequências de códigos html suspeitas que podem ser usadas para criar padrões. No entanto, a tendência nos emails legítimos é revertida. Há apenas alguns tipos restantes de mensagens de status ou newsletters que não usam html. Cedo ou tarde, os spams de texto simples como uma característica de emails vão se tornar cada vez mais suspeitos. Um dia, eles podem ser usados até mesmo como um critério para bloqueio.

Spams de Malware de ZIP de 2011

Os anexos ZIP de spams da fase três foram discutidos em detalhes no Relatório de Riscos e Tendências de Meados do Ano da IBM 2011.

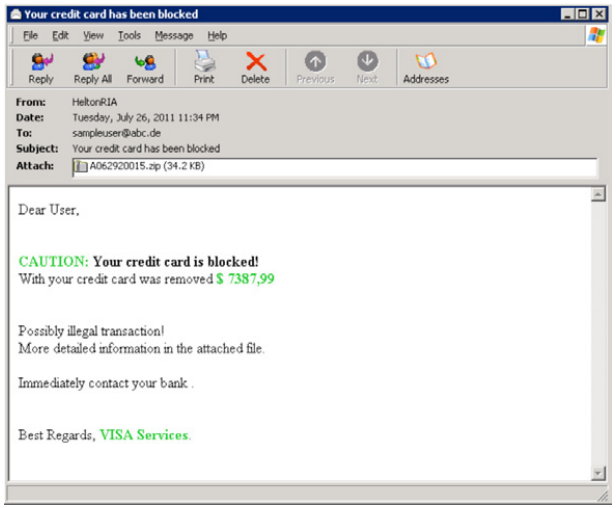


Figura 20: Mensagem falsa sobre cobrança de cartão de crédito – julho de 2011

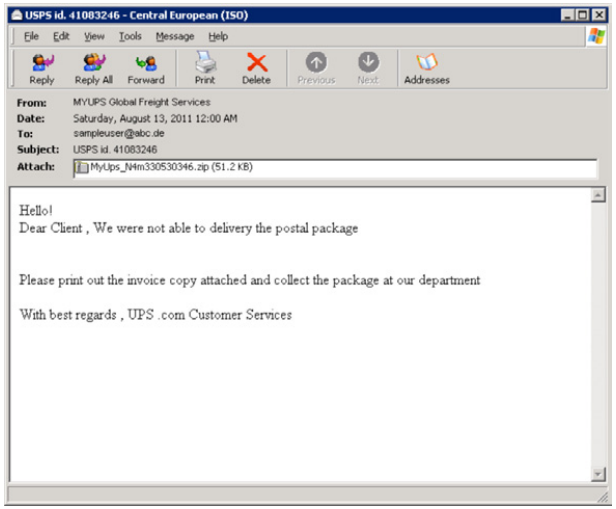


Figura 21: Falsa notificação de entrega – agosto de 2011

No segundo semestre de 2011, foram observados três aumentos de emails com anexos ZIP de 18 a 43%, cada um deles medido diariamente. Os trojans são o tipo favorito de anexo de malware. Mais de 50% dos anexos ZIP do aumento do final de julho continham o Trojan:Win32/Fivfrom.gen!B. Para incentivar os usuários a abrirem esses anexos e clicar no binário de malware, os criadores de spam usavam diversas variantes similares às usadas na fase três. Uma das principais era uma mensagem de que o cartão de crédito do usuário será cobrado em relação a um valor superior a cem dólares (americanos) e que o usuário poderia encontrar os detalhes no arquivo anexo.

É possível ver uma situação similar nos outros aumentos: o tipo dominante de malware de meados de agosto foi o TrojanDownloader:Win32/Cbeplay.M. Duas semanas após este aumento, a porcentagem de anexos ZIP era de cerca de 10% ao dia. A característica típica deste tipo eram os avisos de entrega não realizada de um serviço bem conhecido de pacotes, a fim de tentar convencer o usuário a abrir o anexo e clicar no binário.

O terceiro aumento foi por volta de 20 de setembro. O tipo dominante de malware foi o TrojanDownloader:Win32/Chepvil.N.

Spam de imagem em 2011

O renascimento dos spams de imagens foi um pouco surpreendente. Durante os dois últimos anos, não foram vistos grandes quantidades deste tipo de spam. Na maioria das vezes, a porcentagem deste tipo de spam era inferior a 1%. No entanto, desde o final de novembro, foram observados grandes aumentos destas estatísticas.

Os spams de imagens anteriores usavam imagens para transportar a mensagem de spam real, por exemplo, mostrando algumas pílulas ou exibindo a URL e solicitando que o usuário a digitasse em seu navegador. Ainda existem alguns desses spams de imagens antigos, mas a maioria dos spams de imagens mais recentes tem sido logotipos de organizações ou empresas legítimas. O texto do email declara algo similar a:

- Sua transação falhou. Clique no link para ver os detalhes.
- Recebemos uma reclamação sobre seu negócio. Clique aqui.

O objetivo real de usar esses logotipos é fazer com que os usuários cliquem no link fornecido – um link de malware que infecta a máquina do usuário. Este tipo de email se parece com phishing. Veja a seção "Scam e phishing de email" para mais detalhes sobre este tipo de spam.

Será interessante ver as outras abordagens que os criadores de spam podem usar em 2012 para fazer com que os usuários cliquem em links maliciosos.

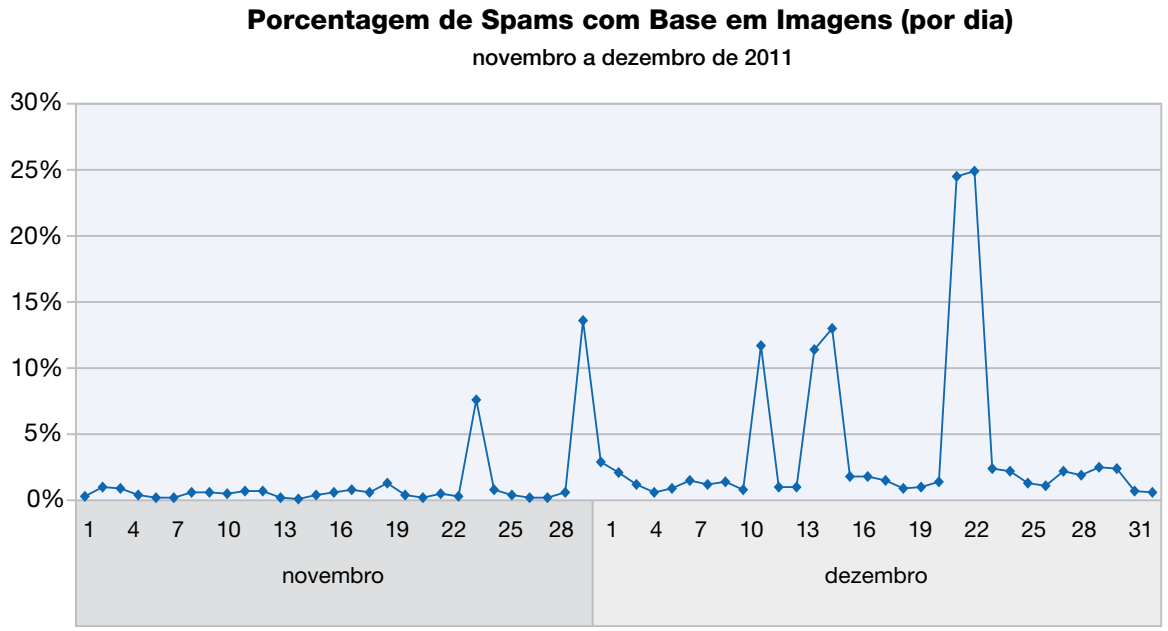


Figura 22: Porcentagem de Spams com Base em Imagens – novembro a dezembro de 2011 (por dia)

Principais domínios comuns dos spams de URL, incluindo as tendências de longo prazo

O principal domínio usado pelos criadores de spam em 2011 foi similar ao de 2010. A única exceção foi o .ua, o principal domínio da Ucrânia. Este domínio foi usado para fazer com que novos conteúdos fossem colocados na Internet. Os spams e phishing sempre pretendem fazer com que o usuário clique no link fornecido. Vale a pena analisar as tendências de longo prazo dos principais domínios usados pelos criminosos. Os últimos quatro anos apresentaram grandes mudanças.

- O principal domínio mais usado de 2008 a 2011 foi o .com., que sempre permanece na primeira ou segunda posição.
- Os outros principais domínios gerais, .net, .info e .org permaneceram populares para os criadores de spam ao longo dos anos. No entanto, eles caíram de modo significativo em 2011.
- Desde o início de 2010, o .cn (China) caiu de modo significativo e nunca voltou a ficar entre os 15 primeiros colocados.
- O .cn foi substituído pelo .ru (Rússia), que entrou nas 15 principais posições em 2008 e, desde 2010, se alterna com o .com na primeira posição.
- O novato de 2011 é o .ua (Ucrânia), que permanece em terceiro lugar desde a primavera de 2011.

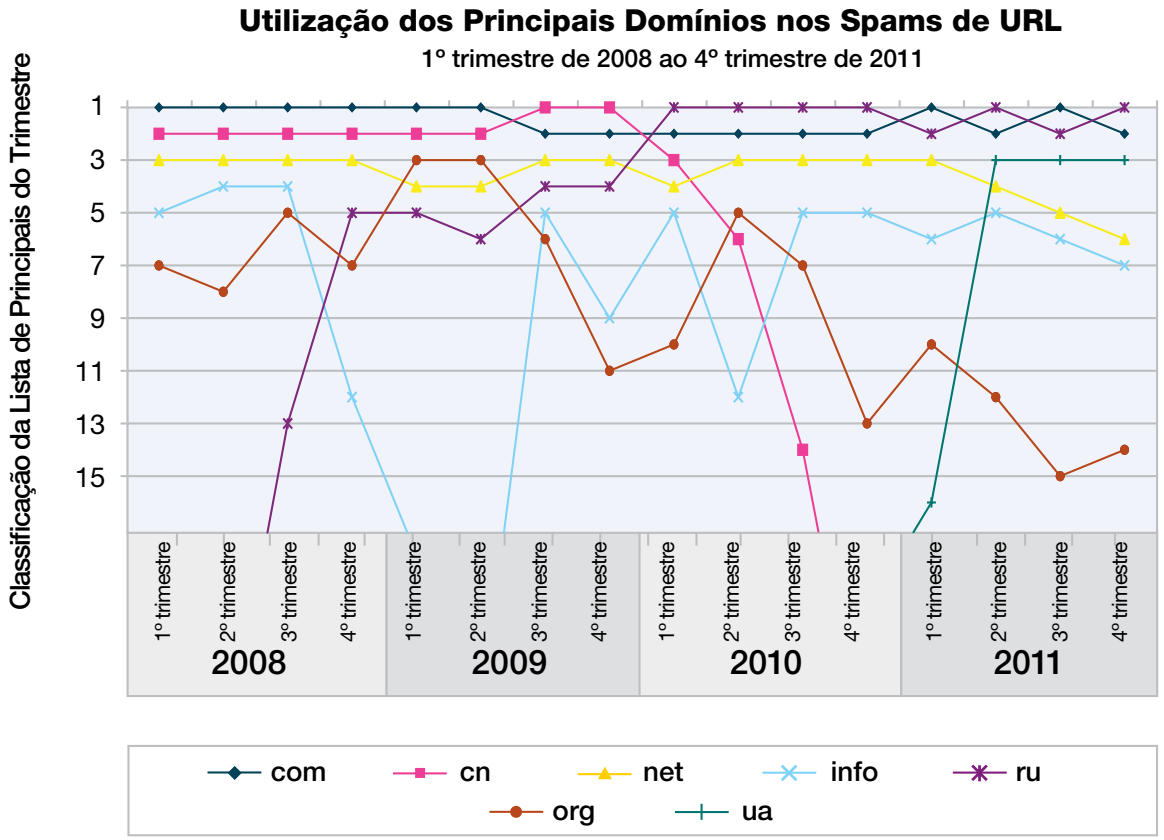


Figura 23: Utilização dos Principais Domínios nos Spams de URL – 1º trimestre de 2008 ao 4º trimestre de 2011

Algumas perguntas interessantes surgem com base nessas estatísticas de longo prazo:

- **Por que o .com é tão popular para os criadores de spam?** O domínio .com é, de longe, o principal domínio mais usado da Internet. Um domínio .com é barato e fácil de registrar. Além disso, uma URL .com de um email é totalmente livre de suspeitas.
- **O que aconteceu com o principal domínio .cn (China)?** Em 2008 e 2009, os domínios chineses eram os preferidos dos criadores de spam. No entanto, desde que a China reforçou as regras de registro de um domínio .cn[10] em meados de dezembro de 2009, isso parece ter detido os criadores de spam.
- **Por que a Rússia (.ru) não faz o mesmo que a China?** Ela tentou. Em 1o de abril de 2010, o NIC russo reforçou suas regras de registro de novos domínios[11]. Dezoito meses depois, ele reforçou as regras novamente[12]. No entanto, os criadores de spam continuam a escolher os domínios .ru para fazer suas ofertas. Atualmente, o .ru ainda é o principal domínio com o código de país mais usado para spams.
- **Já que apenas alguns principais domínios são amplamente usados para spams, este não seria um ponto de ação para combater os spams?** Sim e não. Se houvesse uma ação combinada pelos certificadores para aplicar as mesmas regras que a China, isso poderia ajudar. No entanto, esta não é uma expectativa realista. O registro é uma questão jurídica que cada país manipula de modo diferente. É provável que sempre haja um certificador fraco que forneça portas abertas aos criadores de spam. Além disso, o registro de domínios é apenas uma maneira de hospedar os conteúdos de spam. Outra maneira é usar outros hosts de conteúdo sem necessidade de registrar domínios.

10 http://www.cnnic.net.cn/html/Dir/2009/12/12/5750.htm
11 http://news.softpedia.com/news/Enhanced-Security-Measures-for-RU-Domain-Registrations-138234.shtml
12 http://www.abuse.ch/?p=3581

Spam – país de tendências originadoras

Ao analisar os países que enviaram a maioria dos spams nos últimos três anos, algumas tendências de longo prazo interessantes se tornam visíveis.

- Três anos atrás, o Brasil e os EUA dominavam o mercado de trabalho.
- A Índia mostrou um crescimento quase contínuo e, agora, domina a situação com uma grande margem, enviando mais de 14% de todos os spams.
- Os EUA ocupavam a primeira posição há um ano e, agora, enviam apenas 2% de todos os spams.
- O Vietnã, que estava crescendo em 2009, caiu de modo significativo no primeiro trimestre de 2011, mas se recuperou consideravelmente no segundo semestre, enviando mais de 10% de todos os spams.
- O Brasil reduziu sua porcentagem pela metade nos últimos 18 meses.
- A Indonésia é a novata. Ela mostrou um crescimento contínuo por três anos e, agora, gera 10% de todos os spams.
- A Austrália é outra novata, responsável por 5,6% de todos os spams até o final de 2011.

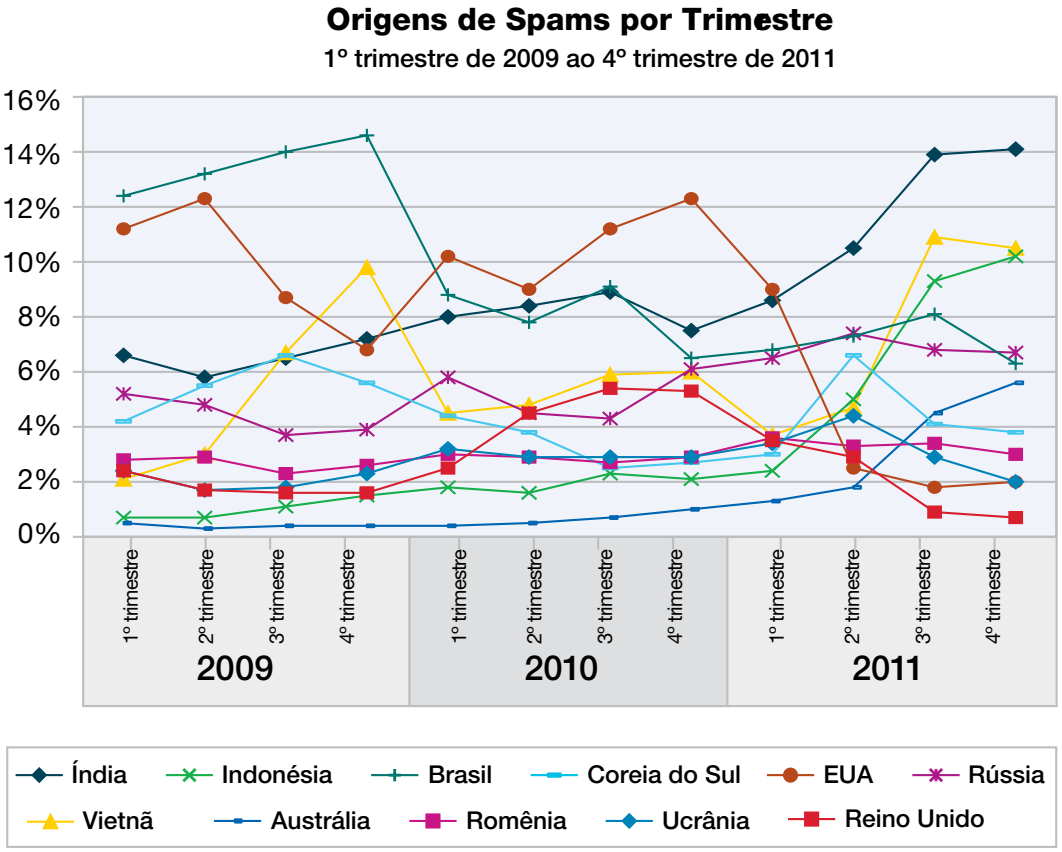


Figura 24: Origens de Spams por Trimestre – 1º trimestre de 2009 ao 4º trimestre de 2011

Scams e phishing de email

Metodologia das estatísticas fornecidas de scams e phishing

Como relatado nos Relatórios de Riscos e Tendências anteriores, foram observadas reduções no phishing de email tradicional em 2010 e no primeiro semestre de 2011.

No entanto, este segmento de mercado ainda não está morto. O phishing de email tradicional foi substituído por algumas novas abordagens que os criminosos estão usando, mas as diferenças não são óbvias. Ainda são vistos muitos spams que se parecem com o phishing normal, como:

- Emails que parecem ser enviados de bancos, que pedem que os usuários cliquem no link fornecido para atualizar a conta, confirmar seus dados etc.
- Emails que parecem ser enviados de redes sociais em relação à solicitação de um novo amigo, que pode ser confirmada clicando no link fornecido.

No contexto de phishing de email tradicional, foi observada uma grande mudança após algum tempo. Muitas das páginas de phishing contidas nos emails não são mais colocadas em um domínio recém-registrado. A vantagem destes domínios é que os criadores de phishing conseguem escolher um nome de domínio similar à vítima, por exemplo, hxxp://www.<nomedobancocompequenoerrodeortografia>.com.

Os criadores de phishing se aproveitaram dessas vantagens, algumas vezes em combinação com os novos nomes de domínios internacionalizados[13]. Uma ação contrária foi desativar estes domínios rapidamente. Os novos serviços de desativação de domínios foram criados em relação a estes sites de phishing.

Sempre mais inteligentes e ousados, os criadores de phishing encontraram outras maneiras de evitar este problema de desativação. Atualmente, muitas páginas de phishing são colocadas como subpáginas de websites legítimos, como hxxp://www.sitelegítimo>.com/<qualquerpalavra>.html. A vantagem para os criadores de phishing é que os domínios dessas subpáginas não podem ser desativados, já que pertencem a websites legítimos e, às vezes, até são websites relacionados a negócios. Para implementar esta subpágina, o website legítimo é atacado. Assim que invadem, os criadores de phishing podem simplesmente colocar a página adicional – que consiste somente em alguns kilobytes – no servidor da web. Depois, eles enviam seus emails de phishing que contêm um link para esta nova subpágina. Eles coletam as credenciais inseridas pelos usuários na subpágina que, como sempre, se parecem com o site de login de comércio bancário esperado.

Os criadores de phishing podem até mesmo dificultar a detecção dessas páginas pelos funcionários de segurança, usando a abordagem de apresentar a página somente à determinada porcentagem de usuários que clicam no link.

No entanto, o que pode ser mais surpreendente é que nem todos os emails que se parecem com phishing fornecem um link a um site malicioso. Em vez disso, muitas vezes há:

a) Uma loja online de produtos médicos, acessórios de moda ou softwares idênticos aos links fornecidos pelo spam normal.
b) Malwares que podem infectar computadores ao clicar neste link.

Então, por que os criadores de phishing mudam sua abordagem para algo que parece ilógico, principalmente no caso (a)? Alguns motivos podem ser:

- É uma abordagem comprovada para fazer com que os usuários cliquem em link quando um email parece vir de uma organização legítima, como bancos ou redes sociais. Portanto, é simplesmente uma fraude do clique[14]. É possível que estes websites estejam pagando a estes criadores de phishing para anunciar seus sites e não estejam cientes de como a propaganda está funcionando.
- É muito trabalho configurar sites falsos de comércio bancário que podem ser bloqueados por produtos de segurança em alguns minutos. É muito mais barato e mais conveniente instalar um Trojan no computador do usuário, já que ele pode captar as credenciais financeiras de modo independente do banco principal do usuário.

13 http://en.wikipedia.org/wiki/IDN_homograph_attack

14 A fraude do clique é um tipo de crime de Internet no contexto de propagandas online pay per click (veja http://en.wikipedia.org/wiki/Pay_per_click). A fraude é feita por imitação ou atração de cliques das propagandas. Cada clique gera um encargo. Em oposição a um usuário que tenha um interesse real no destino do link de anúncio, estes cliques não têm nenhum interesse e, portanto, o encargo é pago sem recompensa. Para mais detalhes, acesse http://en.wikipedia.org/wiki/Click_fraud.

- Vender produtos médicos, softwares e acessórios de moda falsificados ainda é um negócio lucrativo e alguns usuários podem não pensar por que uma loja online aparece ao clicar em um link fornecido em um email de um banco ou rede social. Portanto, é apenas um método entre vários para fazer com que os usuários entrem em seus sites de compras online.

Há outra consequência matemática e estatística dessas tendências recentes de phishing que foi observada, principalmente em 2011. Muitos spams que se parecem com emails de phishing são spams normais médicos ou de malware. No entanto, em muitas estatísticas, eles são contados como emails de phishing. Isso não é necessariamente um erro, já que, no caso de links fornecidos de malware, o malware que rouba dados pode realizar o phishing de credenciais e, portanto, ainda pode ser considerado correto chamá-lo de spam phishing.

As fronteiras entre spams normais, phishing e malwares se tornam cada vez mais obscuras. Outras facetas podem causar maiores impactos sobre as estatísticas de phishing, tais como:

- Esta seção somente considera o phishing proveniente de emails normais. Isso não inclui as mensagens de phishing vindas de redes sociais.
- As estatísticas fornecidas contam o número absoluto de emails de phishing recebidos. Em comparação com 2008, estes números caíram até meados de 2011. Por outro lado, há muitos relatórios sobre um aumento de phishing. Isso não é um conflito, já que representa o número de ataques. Pode haver mais ataques, mas cada um deles consiste em menos emails. No caso de spear phishing (veja a barra lateral), pode haver apenas um único email.
- As estatísticas fornecidas não contam spams com anexos ou links de malware, nos quais o texto não se relaciona à marca visada, mesmo se o malware estiver visando às suas credenciais financeiras.

Portanto, há muitos aspectos que podem resultar em diferentes estatísticas de phishing. As estatísticas fornecidas não contam spams com anexos ou links de malware, nos quais o texto não se relaciona à marca visada, mesmo se o malware estiver visando às suas credenciais financeiras.

As estatísticas a seguir incluem estes spams “similares a phishing” por causa dos aspectos mencionados anteriormente. É interessante medir e analisar quais os tipos das marcas que são abusadas pelos criminosos para fazer com que os usuários cliquem em seus links maliciosos. Um termo genérico para estes emails fraudulentos é “scam”.

Spear phishing

Spear phishing é um phishing personalizado. Primeiramente, os criadores de phishing reúnem muitos tipos de dados pessoais aplicando a engenharia social. Depois, estes dados são usados para compor uma mensagem pessoal à vítima. O conteúdo personalizado assegura a vítima de que a mensagem é legítima; assim, ela cai direto na armadilha. Para mais informações, acesse http://en.wikipedia.org/wiki/Spear_phishing#phishing_techniques.

Tendências mais recentes em scams e phishing de email

Quando consideramos a metodologia anteriormente mencionada, vemos uma redução significativa do phishing de email tradicional, principalmente em 2010. No entanto, no segundo semestre de 2011, a tendência de usar os nomes de marcas confiáveis para fazer com que os usuários cliquem no link fornecido resultou em aumento significativo destes emails ao estilo de phishing ou scams, respectivamente.

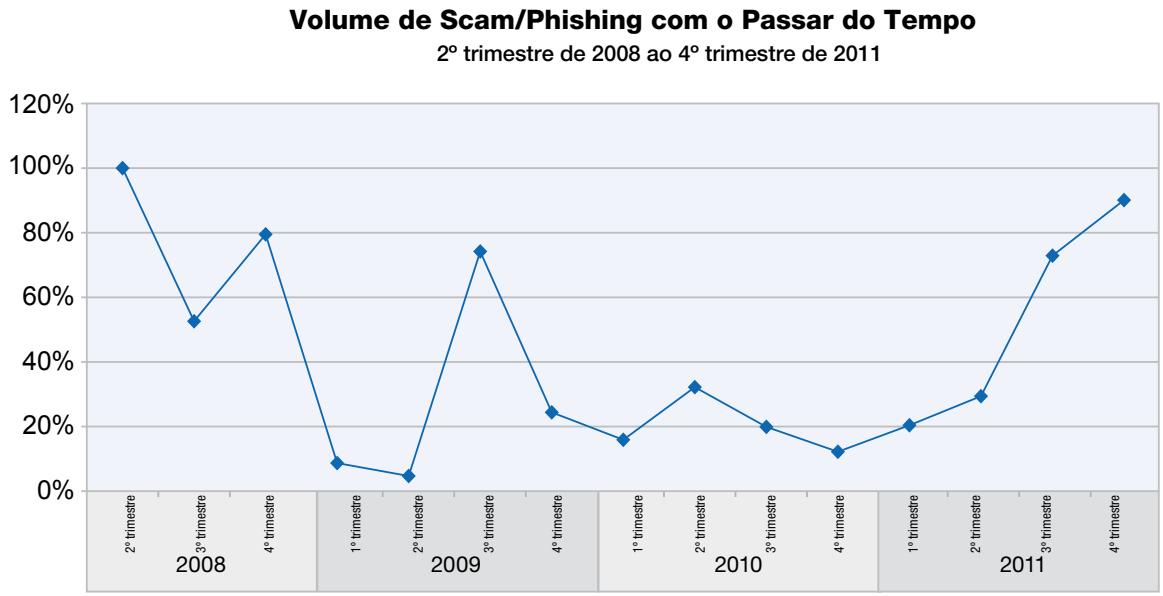


Figura 25: Volume de Scam/Phishing com o Passar do Tempo – 2º trimestre de 2008 ao 4º trimestre de 2011

O mapa a seguir mostra a partir de quais países os emails similares a phishing são enviados[15].

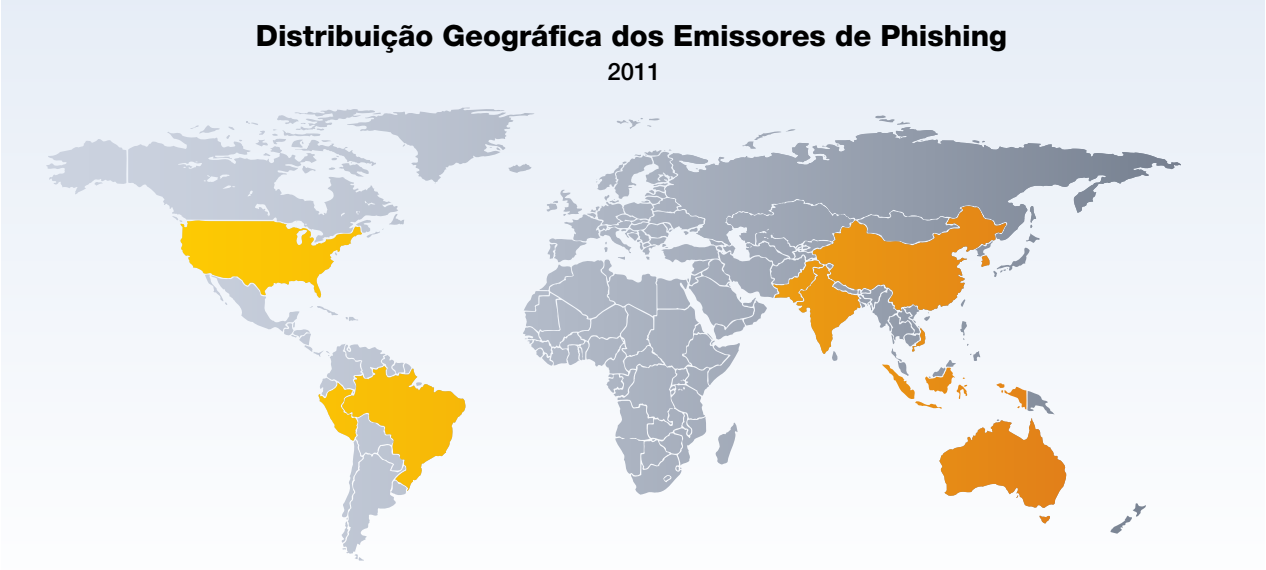


Figura 26: Distribuição Geográfica dos Emissores de Phishing – 2011

país	% de phishing
Indonésia	15,1%
Índia	10,7%
China	6,9%
Brasil	5,9%
Vietnã	5,8%

país	% de phishing
Austrália	5,0%
Coreia do Sul	4,5%
EUA	4,4%
Peru	3,8%
Paquistão	2,6%

Tabela 2: Dez Principais Países de Origem de Scam/Phishing – 2011

15 O país de origem indica o local do servidor que enviou o email de scam/phishing. A X-Force acredita que a maioria destes emails é enviada por redes bot. Já que as bots podem ser controladas de qualquer lugar, a nacionalidade dos invasores reais por trás dos emails de scam/phishing pode não ser a mesma do país a partir do qual os emails foram originados.

As mudanças de phishing/scam de email descritas no início desta seção também são refletidas nos segmentos de mercado visados[16].

- Até 2009, o phishing de email tradicional visava às instituições financeiras que dominam a situação, representando mais de 50% de todos os emails de phishing. Ele perdeu terreno em 2010 e até o outono de 2011, mas se recuperou para cerca de 15% até o final de 2011.
- As lojas online eram os alvos de maior preferência em meados de 2010, mas não desempenharam qualquer função em 2011.
- Os serviços de pacotes foram bastante utilizados para enganar os usuários no segundo semestre de 2010, quando atingiram cerca de 20% de todos os emails de scam/phishing. No segundo semestre de 2011, mais de 50% desses spams usaram a boa reputação dos serviços de pacote. Este tipo quase desapareceu até o final de 2011.
- Desde o início de 2010 – quando começamos a monitorar esta classe de emails – as redes sociais dominaram as estatísticas, ficando sempre na segunda posição. No início de 2011, mais de 80% das marcas legítimas com boa reputação e que usavam emails apostaram nas redes sociais, estabilizando-se em 43% no segundo semestre de 2011.

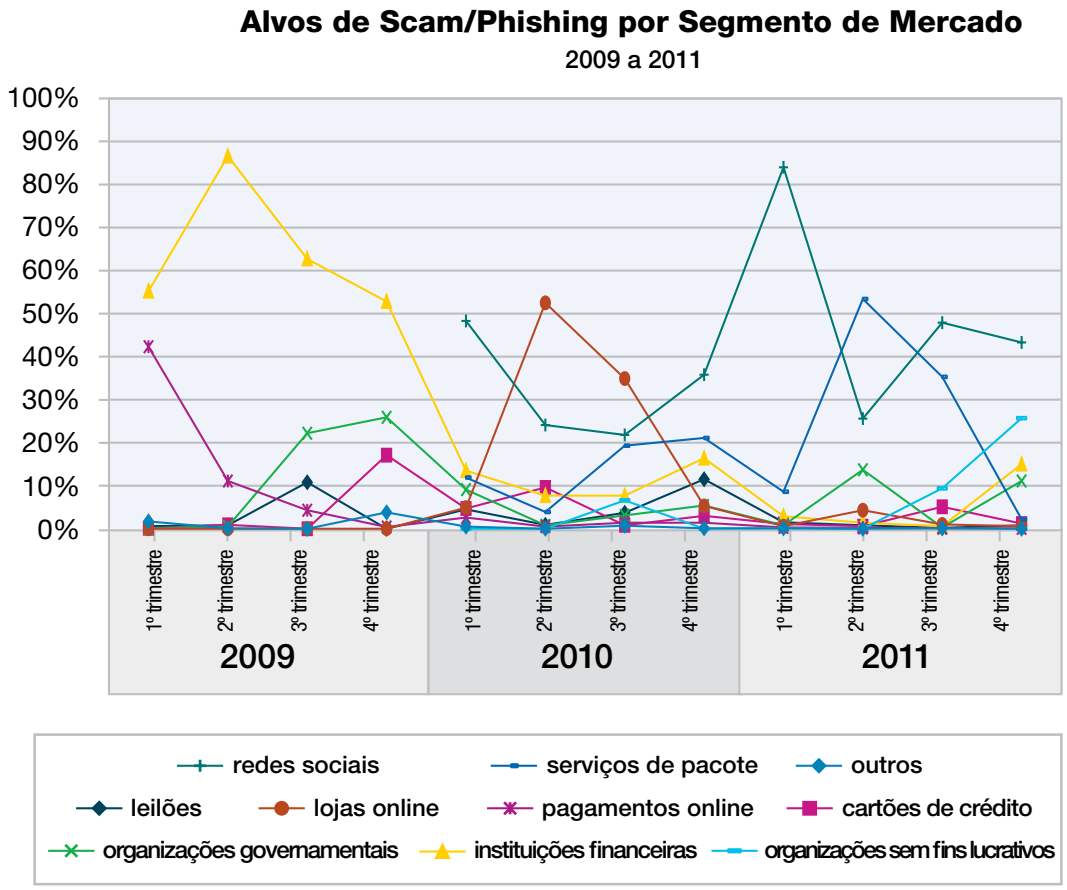


Figura 27: Alvos de Scam/Phishing por Segmento de Mercado – 2009 a 2011[17]

16 Nos Relatórios de Riscos e Tendências anteriores, os números são significativamente diferentes porque não incorporavam as redes sociais, serviços de pacote e organizações sem fins lucrativos. Além disso, os emails que "apenas" utilizavam incorretamente o nome da marca sem realizar phishing real e tradicional não foram contados.

17 Os números relacionados às redes sociais, serviços de pacote e organizações sem fins lucrativos não foram registrados antes do início de 2010.

Evolução dos spams

Ao longo dos anos, foram observadas muitas tendências e tipos de spams que foram discutidos em Relatórios de Riscos e Tendências da IBM X-Force anteriores. Pensamos que seria interessante analisar de modo retroativo as maneiras como os spams mudaram no decorrer do tempo.

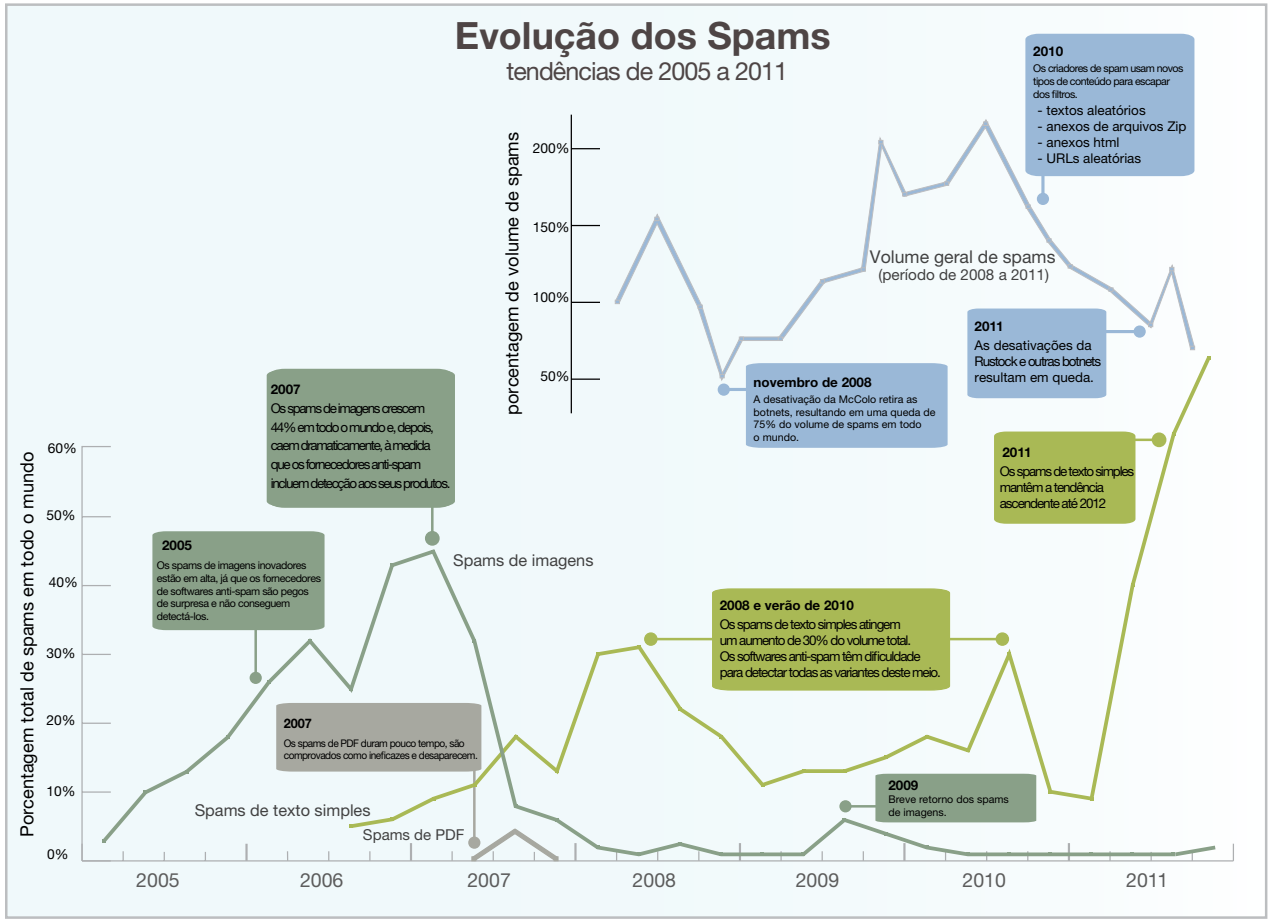


Figura 28: Evolução dos Spams – Tendências de 2005 a 2011

2005 a 2006 – Spams de imagens

Em 2005, os criadores de spam começaram o uso massivo de spams com base em imagens. Até o final de 2005, quase 20% de todos os spams eram baseados em imagens e tinha atingido uma alta máxima de mais de 44% até o início de 2007. Depois disso, essa tendência caiu de modo significativo. Mas por quê?

No começo, os criadores de spam tiveram bons resultados porque, na época, a maioria dos fornecedores antispam não esperava este tipo de spams e pode ter até mesmo considerado as imagens anexas como uma indicação de emails legítimos. No entanto, após dois anos de spams com base em imagens, os últimos fornecedores antispam ajustarem seus métodos de detecção para incluir este tipo. Já que estes spams predefinem muitas características dos emails de spam, era mais fácil verificar em busca de padrões suspeitos; portanto, até o início de 2007, quase todos os spams desse tipo estavam sendo bloqueados com confiança.

2007 – Spams PDF

Após a redução drástica dos spams com base em imagens na primavera e no início do verão de 2007, os spams que usavam anexos PDF começaram a ocupar o seu lugar. Em agosto de 2007, foram observadas grandes quantidades de spams PDF, que representavam quase 20% de todos os spams (em alguns dias). É possível ler mais detalhes sobre este encadeamento de spams PDF no blog Frequency-X.

Os spams PDF tiveram vida curta. Talvez os criadores de spam tentassem repetir o "sucesso" inicial que tiveram com os spams com base em imagens e esperavam que os fornecedores antispam não estivessem preparados para este tipo de anexos. Esse não foi o caso e os criadores de spams desistiram rapidamente da abordagem.

Os spams de MP3 tiveram uma vida útil ainda mais curta que os de PDF. Esta técnica surgiu em outubro e durou apenas alguns dias. No verão, o volume já era bem menor que o das atividades de spams PDF. O interessante é que o código-fonte dos spams MP3 era bastante similar ao dos spams PDF. Detalhes sobre os spams MP3 podem ser encontrados no blog Frequency-X.

2008 – Primeira grande redução dos spams causada pela desativação da McColo

No primeiro semestre de 2008, a porcentagem de spams de texto simples (sem código HTML) aumentou de modo significativo. Os spams escritos em texto simples atingiram um volume de 30% pela primeira vez. Após um aumento similar no verão de 2010, este tipo de spam atingiu sua alta máxima – gerando mais de 70% de todos os spams – ao final de 2011. Os spams de texto simples são mais difíceis ainda de detectar, como um fragmento de código HTML anormal ou um tipo especial de anexo em torno do qual podem ser criados padrões. No entanto, a tendência em emails legítimos ainda funciona de modo contrário. Hoje, há menos tipos de mensagens ou newsletters que não usam HTML. Os spams de texto simples como uma característica de email se tornaram mais suspeitos e, algum dia, podem ser usados como um critério para bloqueio.

No entanto, o maior golpe à evolução dos spams em 2008 foi a desativação da McColo em 11 de novembro. Naquele dia, o volume mundial de spams foi reduzido

em impressionantes 75%! Mais interessante, talvez, seja a mudança perceptível observada nas origens do spam (geralmente, o país da bot do spam). Embora a McColo fosse operada a partir dos Estados Unidos, o volume extremo e repentino de mudanças de distribuição de países observado após a desativação aponta para a McColo como o operador básico das bots de todo o mundo. Durante anos, os Estados Unidos tinham mantido um principal ponto na lista de origem de spams. Seis dias antes da desativação, eles estavam na primeira posição.

Seis dias após a desativação, a produção de spams dos EUA foi reduzida para meros 14% de sua capacidade original. Portanto, não foi uma terrível surpresa quando os EUA finalmente perderam sua principal posição na lista.

2009—First climax of spam volume

Em março, os criadores de spam começaram novamente a lançar várias ameaças, usando spams com base em imagens. Tecnicamente, não houve técnicas novas em sua abordagem; portanto, a maioria dos filtros antispam não teve problemas em reconhecê-los e bloqueá-los. No entanto, houve diferenças no conteúdo das imagens anexas a esta nova rodada de spams. Em 2007, a maioria dos spams com base em imagens concentrava-se na venda de ações. Com a crise financeira que ocorria, houve uma transformação mais lucrativa do foco em direção às drogas. Mais informações sobre o renascimento dos spams de imagens podem ser encontradas no **blog Frequency-X.**

Sendo assim, por que os criadores de spam voltaram a uma técnica antiga, principalmente quando o seu sucesso depende do usuário, já que é ele mesmo que realmente digita a URL (que ele somente vê na imagem e não pode clicar nela) no navegador? Uma resposta pode ser que, ao longo de 2009, os criadores de spam aumentaram significativamente o volume geral de spams. Neste sentido, os spams de imagens podem ser uma parte da estratégia de disparar com todas as armas.

Até novembro de 2009, um ano após a desativação da McColo, foi realizado um primeiro aumento do volume mundial de spams.

5 Principais Países de Envio de Spams Antes da desativação da McColo	
EUA	14,2%
Rússia	11,0%
Turquia	7,4%
Espanha	5,9%
Brasil	4,8%

5 Principais Países de Envio de Spams Após a desativação da McColo	
China	12,7%
Rússia	11,4%
EUA	8,0%
Coreia do Sul	6,2%
Brasil	5,8%

5 Principais Países de Envio de Spams No fim de 2008	
Brasil	11,7%
EUA	8,1%
China	6,6%
Turquia	5,7%
Rússia	5,7%

Tabela 3: Principais Países de Envio de Spams Antes e Depois da Desativação da McColo

2010 – Primeira redução de longo prazo dos spams, mas grandes e vastas variações de conteúdo dos spams, incluindo anexos HTML

Em oposição a todos os anos anteriores, este foi o primeiro ano no qual não se observou um aumento significativo dos níveis de spam. Em vez disso, houve mais variações de conteúdo do que as ocorridas em todos os anos anteriores. Os exemplos vistos em 2010 foram:

- Spams com textos aleatórios combinados com URLs aleatórias, que aumentaram significativamente o tamanho médio de bytes dos spams.
- No início de agosto de 2010, os criadores de spam começaram a enviar encadeamentos de spam com anexos ZIP. A X-Force analisou estas mensagens e cada arquivo ZIP continha um único arquivo EXE malicioso. Mais detalhes sobre esses encadeamentos de spam com anexos ZIP podem ser encontrados no blog Frequency-X.
- A diversidade do conteúdo dos spams observada em apenas um ano pode sugerir que os criadores de spam colocaram mais ênfase sobre a "qualidade" que na quantidade. O volume não era mais a solução para conseguir passar pelos filtros de spam.

2011 – Outra redução dos spams, causada principalmente pela desativação da Rustock

Em 16 de março, houve certo entusiasmo quando o volume de spams foi reduzido pela metade com a desativação da botnet Rustock. Os detalhes dessa desativação foram discutidos nos Relatórios de Riscos e Tendências de Meados de Ano da IBM X-Force anteriores. Em oposição à desativação da McColo em novembro de 2008, não houve uma rápida recuperação dos níveis de spam. No entanto, os criadores de spam não se cansavam de mudar suas abordagens para fazer com que os spams passassem pelos filtros, enviando novas ameaças de:

- Spams de malware de ZIP no verão e no outono
- Spams de imagens em dezembro

Tudo isso foi discutido em detalhes nas seções anteriores.

Tendências de spams de longo prazo – país de origem

- A Índia é o único país com um crescimento contínuo
- O Brasil foi o maior aproveitador da desativação da McColo em 2009, mas está caindo desde então
- A Rússia foi afetada de modo significativo pela desativação da McColo, mas está aumentando desde 2009
- A Indonésia é a novata de 2011, a maior aproveitadora da desativação da Rustock em março de 2011
- Os EUA caíram para menos de 4% pela primeira vez, principalmente por causa da desativação da Rustock
- A Coreia do Sul está estabilizada em 4%
- A França, Espanha e Turquia perderam sua função dominadora dos anos anteriores

Tendências de spams de longo prazo – o que não mudou

Apesar de toda a movimentação descrita anteriormente, alguns conceitos básicos não mudaram:

- Continuamos a ver os spams aproveitando-se dos tópicos clássicos, como réplicas de relógios, produtos médicos e softwares. Esta parece ser uma abordagem comprovada para receber dinheiro ilegítimo.
- Os spams, e particularmente o phishing, existem para fazer com que os usuários cliquem no link fornecido. Mas os criadores de spam desacoplam o conteúdo do texto fornecido no spam em relação ao que ocorre quando os usuários clicam no link. Isso resulta em:
  - Spams perfeitos similares a phishing que tentam vender produtos como os mencionados acima.
  - Spams que se aproveitam dos tópicos novos ou principais prometendo mais detalhes ao clicar no link – depois, infectam a máquina do usuário.
  - Massas de spams que não contêm nenhum texto, apenas um link.

- Aumento da velocidade. Os criadores de spam ajustam rapidamente suas abordagens para tentar ficar à frente de todas as melhores iniciativas para bloqueá-los. O principal uso dos spams com base em imagens durou mais de dois anos (2005 a 2007), ao passo que as diferentes fases de spams vistas em 2011 duraram de 10 a 14 semanas. Assim, as mudanças dos países que enviam spams acontecem muito mais lentamente. Em comparação, as botnets também estão crescendo lentamente. Será interessante ver se os criadores de spam conseguirão acelerar sua aquisição de botnets no futuro.

- Desde 2008, o tamanho médio em bytes continua voltando para três kilobytes. Podemos considerar este um tamanho-padrão dos spams.
- Os criadores de spam sempre tentam novas abordagens. Veja a próxima seção para obter alguns pontos de vista sobre o que poderá acontecer.

Prospectos futuros sobre os spams

No primeiro semestre de 2011, foram observadas reduções significativas do volume de spams sem a rápida recuperação que as caracterizaram no passado. A conjuntura de negócios para os spams tradicionais de email mudou.

- As organizações ou empresas foram bem-sucedidas em desativar as botnets ou a infraestrutura necessária ao envio de spams, como foi visto na desativação da McColo ou da Rustock (estas desativações foram discutidas em detalhes em meados do ano).
- Os filtros de spam estão melhorando de modo contínuo.
- Surgem outras abordagens que paralisam o negócio dos criadores de spam, como o "Click Trajectories: End-to-End Analysis of the Spam Value Chain"[18]. O estudo mostrou que 95% dos pagamentos de produtos anunciados em spam são manipulados apenas por três bancos. Os bancos da vítima de spam podem bloquear os pagamentos a estes três bancos.

Isso pode fazer com que os criminosos se concentrem em outras áreas, como o envio de spams em redes sociais ou a execução de ataques de negação de serviços (DOS) distribuídos. Existem até mesmo os criadores de spam experientes que consideram que o negócio de spam não é mais atrativo[19]. Por outro lado, também pode haver aspectos que podem enganar os invasores novos e antigos a enviar mais spams.

- O número de usuários da Internet ainda está aumentando. Assim, sempre há novas vítimas de ataques de spam e phishing, mesmo se apenas um de mil emails de spam chegar a uma caixa de entrada.
- O número de máquinas disponíveis também ainda está aumentando. Além disso, há um novo tipo de máquina para infectar: o smartphone. Estes computadores de mão têm outra vantagem, de acordo com a perspectiva do criador de spam: eles estão sempre online, ao contrário dos computadores de desktop, que são desligados quando não estão em uso. Hoje, ainda há limites de largura de banda no contexto dos smartphones, já que a maioria dos usuários não tem uma taxa fixa de Internet móvel. Provavelmente, isso mudará no futuro. Veja a seção "Perspectiva de malware móvel" para detalhes.
- Em relação ao tipo de conteúdo dos spams, ainda há algumas abordagens não usadas pelos criadores de spam, como usar os documentos Open Office como anexos de spam.
- Pode haver muitos nomes de marca bem conhecidos que os criadores de spam podem usar como emissores falsos de seus spams para fazer os usuários clicar nos links fornecidos.
- O IPv6 também pode fornecer novas abordagens para que os criadores incomodem os usuários e irritem os fornecedores antispam, principalmente quando os criadores de spam se concentram exclusivamente no bloqueio de IP.

18 http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf
19 http://www.itworld.com/security/178991/internet-evolves-there-place-spam

Seção II
Práticas Operacionais de Segurança

Nesta seção do Relatório de Tendências, serão explorados os tópicos relacionados aos pontos fracos dos processos, softwares e infraestruturas visadas pelas ameaças atuais. Serão discutidas as melhores práticas de conformidade, as ideias de redução do custo operacional, a automação, o menor custo de propriedade e a consolidação de tarefas, produtos e funções. Também serão apresentados os dados rastreados da IBM durante o processo de gerenciamento ou mitigação destes problemas.

Apresentando a Inteligência de Segurança: Uma abordagem integrada à segurança em tempo real

Nos últimos anos, os aumentos dos ataques, a expansão dos modelos computacionais (e, portanto, as superfícies dos ataques) e a explosão de dados criaram desafios significativos aos profissionais de segurança. As organizações estão se defendendo mais que nunca contra ameaças cada vez mais variadas.

Até mesmo determinar que uma violação ocorreu pode ser desafiador, deixando muitas empresas não cientes sobre sérios comprometimentos durante meses. Muitas vezes, elas têm os dados brutos, mas não a visibilidade e a analítica para detectar a violação. O **Relatório de Investigações de Violações de Dados da Verizon** 2011 concluiu que, em 69% das violações, houve evidências suficientes da violação nos arquivos de log da organização, mas elas raramente foram encontradas devido à sobrecarga de dados.

A detecção de ameaças atual, portanto, depende de dois elementos: a *identificação* de atividades suspeitas entre bilhões de pontos de dados e o *refino* de um grande conjunto de incidentes suspeitos até chegar aos incidentes relevantes. Para estas tarefas, as organizações precisam de abordagens que possam: 1) analisar todos os dados relevantes; 2) identificar sinais de modo inteligente; e 3) fornecer essa inteligência de modo prático.

Isso causou o desenvolvimento de uma nova classe de soluções chamada de Inteligência de Segurança, que fornece visibilidade unificada e analítica em tempo real a todo o espectro de operações de segurança.

Em reconhecimento da nova realidade, a IBM fez um movimento ousado para gerar o futuro da inteligência de segurança e da analítica. Por meio de um compromisso para unificar as diversas disciplinas da segurança de informações por meio de uma única divisão de Sistemas de Segurança e por meio da aquisição da Q1 Labs, líder em SIEM (Gerenciamento de Eventos e Informações de Segurança) e inteligência de segurança, a IBM está lidando diretamente com esse problema.

Definindo a Inteligência de Segurança

Começaremos considerando uma definição da Inteligência de Segurança:

Inteligência de Segurança (SI) *é a coleção, normalização e análise em tempo real dos dados gerados pelos usuários, aplicativos e infraestruturas que causam impacto sobre a segurança de TI e a postura de riscos de uma empresa. O objetivo da Inteligência de Segurança é fornecer insights acionáveis e abrangentes que reduzem os riscos e iniciativas operacionais para organizações de qualquer porte.*

Os dados coletados e armazenados pelas soluções de Inteligência de Segurança são logs, eventos, fluxos de rede, identidades de usuários, configurações de ativos e dados de ameaças externas. A Inteligência de Segurança fornece analítica para responder questões fundamentais que abordam as linhas de tempo antes/durante/depois do gerenciamento de riscos e ameaças.

Linha de Tempo da Inteligência de Segurança

A Inteligência de Segurança fornece uma visão unificada da postura de riscos e de segurança de uma organização, abrangendo os principais domínios de riscos: Pessoas, Dados, Aplicativos e Infraestrutura.

As pessoas familiarizadas com SIEM e produtos de gerenciamento de logs podem ver a Inteligência de Segurança como a próxima etapa lógica na jornada destas tecnologias. Incluindo recursos pré-exploração, uma captura de dados mais ampla e mais inteligência, a Inteligência de Segurança estende o SIEM e o gerenciamento de logs. Ela pode ativar melhor uma melhor prevenção, detecção e priorização de ameaças (externas e internas) e automatiza o monitoramento e os relatórios de conformidade.

A Inteligência de Segurança também fornece uma visibilidade ampla dos incidentes de segurança. Por exemplo, ao analisar os fluxos de rede por meio de uma inspeção de pacotes detalhada e monitorar a atividades dos usuários em busca de anomalias, ela pode ajudar a identificar quando as ações de um funcionário parecem suspeitas, sugerindo possível roubo de dados por detentores de informações privilegiadas ou comprometimento de contas por partes externas. Além disso, ao gerenciar os alertas IPS com resultados do escaneamento de vulnerabilidades e com o conhecimento da topologia da rede, a Inteligência de Segurança pode ajudar a identificar quais tentativas de invasão estão atacando os ativos vulneráveis e quais podem ser ignoradas.

A analogia com a Inteligência de Negócios

É instrutivo analisar os paralelos entre a Inteligência de Negócios (BI) e a Inteligência de Segurança. A BI sintetiza grandes volumes de informações de negócios para colher insights de negócios acionáveis:

Quais produtos vendem bem e em quais segmentos de clientes?

Quais geografias responderam com mais força a uma promoção recente?

Por que minha rentabilidade aumenta com uma linha de produto, mas falha com outra?

De modo similar, a Inteligência de Segurança (SI) sintetiza grandes volumes de informações de segurança para obter insights de segurança acionáveis que tenham relevância para a TI e a linha de negócios:

A quais tipos de ataques somos temos mais probabilidade de estarmos vulneráveis? (Como devemos ajustar nossas práticas e controles de segurança?)

Quais parceiros de negócios e fornecedores podem estar criando os maiores riscos de segurança para nossa empresa? (Devemos ajustar o seu acesso ou exigir controles mais fortes para eles?)

Existem quaisquer novos riscos de segurança ou conformidade a partir da computação móvel? (Em caso afirmativo, em quais riscos devemos nos focar?)

Uma diferença entre a SI e a BI é que a Inteligência de Segurança fornece insights e monitoramento em tempo real, enquanto a Inteligência de Negócios geralmente reflete informações point-in-time. As duas podem ser ferramentas de gerenciamento inestimáveis, mas no ambiente da segurança e conformidade, as informações atualizadas são fundamentais.

A Inteligência de Negócios se tornou uma ferramenta-padrão para o planejamento de negócios e a visibilidade executiva. De modo similar, a Inteligência de Segurança está se tornando uma ferramenta-padrão para o planejamento de segurança e a visibilidade executiva. Além disso, ela pode servir como a base factual para as conversas sobre segurança entre a TI e a linha de negócios, a fim de ajudar a avaliar as considerações de riscos/recompensas sobre as práticas e ofertas de negócios.

Os princípios da Inteligência de Segurança

Os três princípios da Inteligência de Segurança – **Inteligência, Integração e Automação** – ajudam a facilitar que os usuários tornem-se produtivos de modo mais rápido.

A seguir, há alguns exemplos de como isso funciona na prática:

1. **Inteligência**: A capacidade de dar sentido a grandes quantidades de dados relevantes à segurança e à conformidade. Isso significa armazenar, correlacionar, relatar e consultar uma grande variedade de informações em escala Big Data (as informações de segurança "são" Big Data), a fim de fornecer insights acionáveis.

2. **Integração**: A base da inteligência, ativando uma análise consistente e normalizada de dados muito diferentes. Ao reunir e combinar os dados relevantes à segurança – em tipo e volume – é possível expandir uma visão limitada e bidimensional de um evento de segurança em uma visão rica e tridimensional suportada pelo contexto.

- Exemplo: Os recursos de integração fornecidos em primeira mão pelas soluções de Inteligência de Segurança causam um enorme impacto sobre a produtividade de um analista de segurança. A normalização dos dados de centenas de fontes ajuda a impedir que os clientes (e consultores) tornem-se especialistas no esquema de dados de cada fornecedor. Por exemplo, um mandato de conformidade pode exigir a documentação dos eventos de autenticação (logins com falha, logins bem-sucedidos, logins bem-sucedidos seguidos de uma escalação de privilégios etc.). Com a SI, as organizações não podem mais rastrear isso de modo manual entre dúzias de ativos, já que cada um deles tem seu próprio esquema de dados.

3. **Automação:** O elemento que leva a Inteligência de Segurança à era moderna, ajudando a remover a complexidade desnecessária e a reduzir o custo total de propriedade (TCO). Isso inclui tarefas automatizadas pelo uso de dados mais amplos (como fluxos de rede) e propriedades intelectuais empacotadas para fácil aplicação.

Aplicando a Analítica Avançada ao Conjunto Mais Amplo de Dados

Como a Inteligência de Segurança difere do SIEM?

A Inteligência de Segurança ultrapassa as tecnologias de SIEM de primeira geração de várias maneiras significativas:

Monitoramento da atividade de rede e analítica de fluxo. No passado, os logs de dispositivos, aplicativos, servidores e serviços de infraestrutura apresentavam uma ideia básica do que estava ocorrendo. Hoje, os logs são apenas um ponto inicial. A coleção do fluxo de rede, a inspeção detalhada de pacotes e a captura de pacotes (conteúdo) são necessárias ao contexto e visibilidade tridimensionais. A Inteligência de Segurança usa a analítica de fluxo para ajudar a fornecer insights em tempo real sobre o comportamento dos usuários, a utilização da mídia social, as atividades móveis, as atividades em nuvem, entre outros.

A conversa usa tráfego da web de porta 80 ou uma comunicação oculta de IRC de botnet?

Os invasores estão usando uma conta de funcionário comprometida para extrair dados sensíveis?

Os funcionários estão acessando propriedades intelectuais sensíveis de modo inadequado?

A visibilidade quanto a pacotes, que vem da integração do monitoramento de atividade da rede (captura de conteúdo) e do SIEM, pode fornecer esses insights.

Analítica de prevenção e reconhecimento pré-exploração. A Inteligência de Segurança integra a configuração pré-exploração e os recursos de gerenciamento de vulnerabilidades. Isso permite que uma organização identifique, priorize e aborde sistematicamente os riscos criados por dispositivos mal configurados (como firewalls) e vulnerabilidades não corrigidas.

Detecção de anomalias. Muitas soluções tradicionais de segurança se concentram na proteção da organização contra as ameaças conhecidas, como as vulnerabilidades divulgadas ao público e os malwares comuns. No ambiente de segurança atual, há um maior desejo de detectar ataques direcionados sofisticados que podem usar metodologias de ataque completamente novas. Além disso, as ameaças de detentores de informações privilegiadas, muitas vezes, somente podem ser detectadas por meio da análise dos comportamentos autorizados. Uma abordagem centralizada em anomalias pode lançar luz sobre esses tipos de atividades.

Mais fácil de implementar e alocar pessoal. Quando os primeiros produtos de SIEM foram liberados, os primeiros adotantes estavam dispostos a gastar tempo e dinheiro consideráveis para colocá-los em operação. Os conectores e as regras precisavam ser escritos, os usuários precisavam ser treinados, e assim por diante. Assim que entraram em produção, os seus requisitos de alocação de pessoal também podiam ser significativos, devido à alta taxa de alertas "falsos positivos" que exigiam investigação. Agora, as soluções de Inteligência de Segurança usam um conjunto mais amplo de informações (eventos, fluxos, perfil de ativos, topologia de rede, vulnerabilidades etc.) e mais automação para ajudar a atingir uma redução significativa dos dados e dos requisitos de alocação de pessoal.

Quais são os principais benefícios?

A Inteligência de Segurança auxilia as atividades de conformidade por meio do registro e monitoramento proativo de diversas informações da empresa – quais usuários estão acessando sistemas de alto valor (de modo adequado ou não); se os dados sensíveis estão sendo transmitidos criptografados em redes abertas; se os firewalls estão configurados devidamente etc. A SI também pode melhorar a eficiência operacional – em alguns casos, economizando milhares de horas de esforço manual – por meio de relatórios automatizados e de uma fácil busca de logs e fluxos.

Detecção e correção mais rápida das ameaças. No mundo pós-perímetro, concentrar-se unicamente em prevenção ou detecção/correção é uma proposição perdedora. As organizações precisam realizar as duas coisas. Os limites podem ser obscuros devido à computação móvel, à mídia social e à computação em nuvem, causando o que a Forrester Research chama de um ambiente com "confiança zero". A Inteligência de Segurança aborda isso ajudando os negócios a detectar e corrigir as violações de modo mais rápido, além de ajudar a impedi-las em primeiro lugar (veja a seção "Redução dos Riscos Pré-Exploração" a seguir). Ao correlacionar os volumes massivos de dados em tempo real, a SI pode ajudar a encontrar a agulha no palheiro – analisando eventos da rede e dos dispositivos de segurança, servidores, aplicativos, servidores de diretório; fluxos de atividade de rede (com captura de pacotes); informações de ativos dados de configuração e informações de vulnerabilidades. A Inteligência de Segurança também pode acelerar a correção ajudando a identificar quais ativos e usuários possivelmente foram afetados por um comprometimento e aproveitando a captura de conteúdo para a pesquisa forense.

Por exemplo, quando o worm Conficker começou a se espalhar no final de 2008, isso causou um aumento dramático do tráfego da porta 445 de TCP na Internet. Os sistemas de inteligência de segurança destacaram este aumento de tráfego como suspeito, até mesmo antes de o Conficker ter recebido um nome pelos pesquisadores de segurança. Este tipo de detecção antecipada pode ajudar a proteger as redes de computadores contra ameaças avançadas e repentinas, para as quais pode não haver uma assinatura ou correção.

Redução de fraudes, roubos e vazamento de dados por detentores de informações privilegiadas.
Os ataques externos colecionam a maioria das manchetes, mas as ameaças de detentores de informações privilegiadas podem ser ainda mais danosas – comprometendo propriedades intelectuais inestimáveis e até mesmo prejudicando a segurança nacional. A Inteligência de Segurança permite que as organizações identifiquem e mitiguem esses tipos de ameaças, ajudando-as a detectar:

- Acesso ou utilização não autorizada de aplicativos
- Perda de dados, como dados transmitidos a destinos não autorizados ou não familiares
- Problemas de acesso de usuários, como exceções de acesso privilegiado
- Problemas de desempenho dos aplicativos, como perda de serviços ou excesso de utilização

Redução de riscos pré-exploração
A Inteligência de Segurança é desenvolvida com base em ferramentas de prevenção fundamentais, como firewalls e dispositivos IPS com novas correlações que ajudam a organização a impedir ataques por meio de:

- Monitoramento automático de configurações de dispositivos (como firewalls) e alerta sobre lacunas de segurança e violações de políticas
- Priorização de vulnerabilidades encontradas pelos scanners de VA (avaliação de vulnerabilidades), com base na topologia de rede e no valor dos ativos
- Modelagem preditiva contra ameaças e simulação de alterações à rede

A Inteligência de Segurança pode aplicar mais inteligência a um conjunto mais amplo de entradas em relação ao que era possível anteriormente. Os fluxos de atividades de rede baseados em captura de conteúdo,

por exemplo, podem fornecer uma visão mais confiável das regras dos dispositivos de segurança do que os próprios dados de configuração. Como observou um post de blog recente, "[Os dados de configuração, sozinhos, podem] não notar situações nas quais uma configuração é considerada adequada, mas, por algum motivo, ela ainda permite a propagação de um tráfego de rede possivelmente arriscado". De modo similar, o conhecimento das topologias de rede pode "minimizar os falsos positivos comuns entre os scanners de vulnerabilidades e... [priorizar as vulnerabilidades] que podem ser facilmente expostas por causa da maneira como a rede é configurada".

Operações simplificadas e redução dos esforços
As soluções de SI estão aplicando a automação inteligente para simplificar as operações de segurança e reduzir os ônus sobre a segurança e os profissionais de rede. Isso pode resultar em reduções de custo significativas. Estes benefícios derivam das maiores eficiências e da eliminação de tarefas manuais entediantes.

Melhores práticas de Inteligência de Segurança

Ao desenvolver a competência em Inteligência de Segurança, existem abordagens organizacionais e recursos técnicos que aumentam as chances de sucesso. A seguir, há diversas abordagens e recursos que podem ser priorizados:

Definição da política de escalação de incidentes. A solução de inteligência de segurança pode ser vista como um serviço de nuvem interna, atendendo os grupos como gerenciamento de firewall, gerenciamento de sistemas e gerenciamento de rede. Assim como ocorre em um serviço de nuvem pública, o provedor da solução de SI (geralmente o grupo de gerenciamento de riscos ou de segurança) deve definir um contrato com os consumidores da solução que defina como os incidentes de segurança são manipulados e escalados. Relatar imediatamente os problemas ao gerenciamento executivo pode não ser algo ideal e também pode danificar o relacionamento com os consumidores e fazê-los reter dados no futuro.

Definição dos principais casos de uso e relatórios de implementação inicial. A organização deve decidir sobre quais tópicos concentrarão suas iniciativas de monitoramento e relatórios. As categorias comuns são as ameaças externas gerais (como botnets e tráfego das darknets), os riscos específicos ao segmento de mercado, as ameaças de detentores de informações privilegiadas, as violações de políticas e as atividades de usuários privilegiados.

Detecção inteligente de anomalias. Para detectar o comportamento incomum, a solução deve gerar linhas de base de atividades em todas as dimensões da Internet (usuários, aplicativos e redes) com base no comportamento observado e, depois, identificar as anomalias que não se enquadram na norma. A comparação dinâmica que identifica automaticamente as mudanças da linha de base pode reduzir o trabalho manual subsequente.

Analítica de fluxo com base na inspeção detalhada de pacotes. Como descrito anteriormente, a analítica de fluxo com a captura de pacotes pode fornecer uma visibilidade detalhada sobre os riscos de segurança e conformidade. Ela pode aprimorar a prevenção por meio de identificação de configurações de rede incorretas, detecção por insights quanto a pacotes e à investigação forense, mostrando quais dados foram acessados por quais usuários em uma faixa de casos de uso.

Analítica de prevenção. As organizações que buscam uma postura de segurança mais proativa também devem priorizar os recursos como o monitoramento de configuração de dispositivos, o monitoramento das políticas de conformidade e a priorização de vulnerabilidades.

Conclusão

Em resumo, a Inteligência de Segurança é um acionador poderoso da segurança corporativa e pode auxiliar com o fornecimento de conformidade das informações acionáveis por meio de insights em tempo real e uma perícia detalhada. Ela pode fornecer benefícios significativos à TI e à linha de negócios por meio de melhor inteligência, integração e automação – áreas que, historicamente, têm sido o calcanhar de Aquiles das soluções de segurança. As soluções de Inteligência de Segurança oferecem implementação e gerenciamento razoáveis para organizações de pequeno e grande porte e podem fornecer uma solução prática para as necessidades do mundo real.

Referências:

1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
2. http://blog.q1labs.com/2011/07/28/defining-security-intelligence/
3. http://blog.q1labs.com/2010/08/26/do-we-need-a-security-analog-for-business-intelligence-absolutely-we-do/
4. http://q1labs.com/resource-center/white-papers/details.aspx?id=113
5. http://blog.q1labs.com/2011/10/20/three-ways-to-embrace-the-zero-trust-environment/
6. http://q1labs.com/resource-center/case-studies/details.aspx?id=114
7. http://blog.q1labs.com/2011/06/16/latest-gartner-report-shines-bright-light-on-qradar-risk-manager/
8. http://q1labs.com/resource-center/white-papers/details.aspx?id=113
9. http://blog.q1labs.com/2010/09/17/siem-is-a-security-intelligence-cloud/
10. http://q1labs.com/resource-center/brochures/details.aspx?id=129

Divulgações de vulnerabilidades de 2011

Desde 1997, a X-Force rastreia as divulgações públicas de vulnerabilidades de segurança dos produtos de software. Nossos analistas seguem as malas diretas e websites públicos nos quais as vulnerabilidades, as informações de correções e as explorações são divulgadas, bem como registram o que foi relatado publicamente.

Em 2011, relatamos um pouco mais de 7.000 novas vulnerabilidades de segurança. Embora isso seja uma redução significativa em relação a 2010, quando foram observadas mais vulnerabilidades que antes, houve um ciclo de dois anos de divulgações de vulnerabilidades desde 2006, e os níveis de cada ponto alto e baixo continuam aumentando.

A primeira vez em que se observou uma redução no número total de vulnerabilidades foi em 2007 e isso gerou muita especulação em relação ao porquê de a paisagem de vulnerabilidades estar mudando. No entanto, de modo retrospectivo, é claro que isso foi apenas uma aberração dos dados e que os totais estavam, na verdade, aumentando. Se o ciclo dos últimos seis anos foi verdadeiro, este ano de 2010 será outro ano de recordes de divulgações de vulnerabilidades.

Aplicativos da web

A categoria de vulnerabilidades de segurança que passou pela maior redução em 2011 foi a de vulnerabilidades de aplicativos da web. Nos últimos anos, cerca de metade das vulnerabilidades de segurança divulgadas correspondia a vulnerabilidades de aplicativos. No entanto, este ano, este número caiu para 41%, uma porcentagem não vista desde 2005. Isso é ilustrado na figura 30, que mostra as vulnerabilidades de aplicativos da web desde 2010. Analisando os tipos de vulnerabilidades divulgadas, a injeção de SQL se destaca como uma importante categoria que tem sido reduzida de modo significativo.

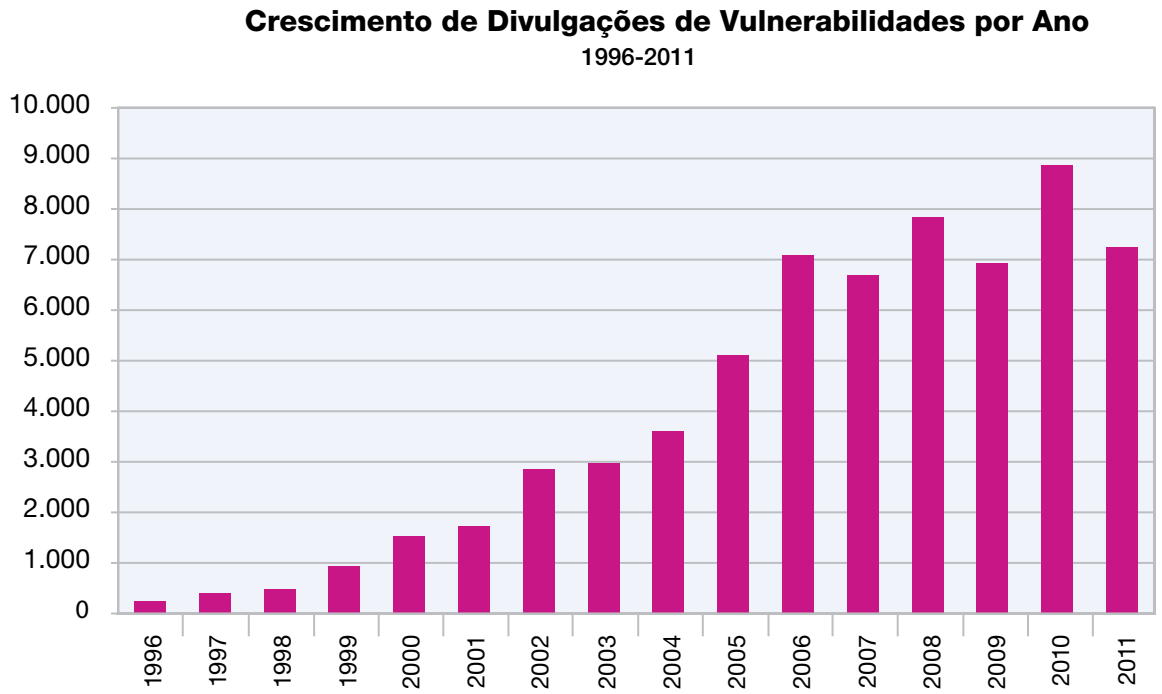


Figura 29: Crescimento de Divulgações de Vulnerabilidades por Ano – 1996 a 2011

As vulnerabilidades de injeção de SQL são particularmente importantes porque são o tipo de ataque mais comum identificado pela IBM nos milhares de redes que ela monitora e ajuda a proteger em todo o mundo. Os ataques automatizados de injeção de SQL lançados por desenvolvedores de botnets motivados financeiramente pesquisam a web procurando sites vulneráveis. Estes sites podem ser infectados com redirecionadores de Javascript, que acionam os seus visitantes aas explorações maliciosos. A injeção de SQL é favorecida pelos invasores não sofisticados que buscam a web por alvos fáceis de desfigurar. Os ataques de injeção de SQL também se apresentaram de modo proeminente em diversas violações de alto perfil deste ano, realizados por invasores mais sofisticados.

Caso esteja executando um aplicativo da web com contato com a Internet que tenha uma vulnerabilidade de injeção de SQL – ele provavelmente será direcionado a qualquer momento. Portanto, é importante corrigir essas vulnerabilidades. A redução do número identificado atualmente pode significar que os desenvolvedores de aplicativos da web estejam se tornando mais inteligentes e escrevendo aplicativos menos vulneráveis. Em caso afirmativo, este é um sinal positivo. No entanto, ainda resta muito trabalho a ser feito.

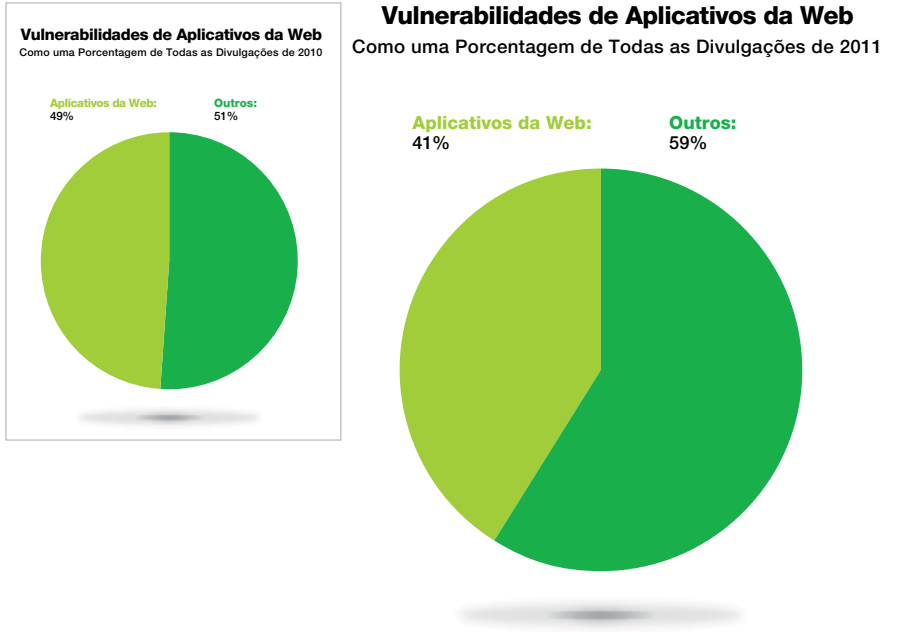


Figura 30: Vulnerabilidades de Aplicativos da Web Como uma Porcentagem de Todas as Divulgações de 2011

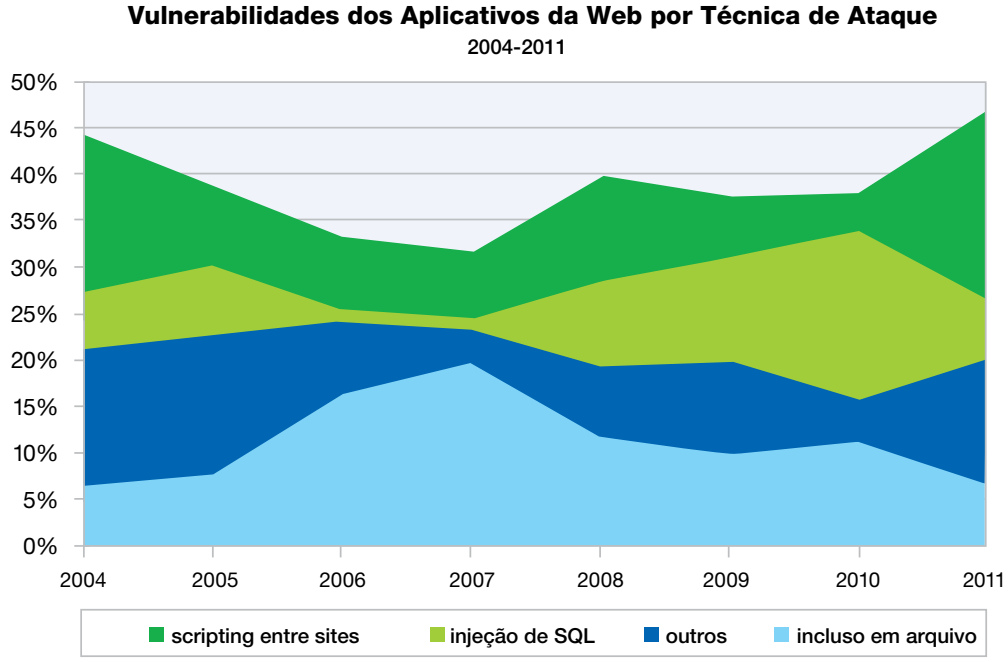


Figura 31: Vulnerabilidades dos Aplicativos da Web por Técnica de Ataque – 2004 a 2011

Em 2011, ainda foram observadas três mil vulnerabilidades de aplicativos da web divulgadas e o número total observado pela X-Force pode ser apenas a ponta do iceberg do que realmente existe na Internet aberta. O motivo é que a X-Force rastreia apenas as vulnerabilidades divulgadas ao público. Os aplicativos da web que são mantidos por uma empresa ou por um projeto de software livre para uso de terceiros estão sujeitos a essas divulgações de vulnerabilidades ao público. No entanto, a maioria dos aplicativos da web são softwares customizados desenvolvidos internamente ou por empresas privadas para uso exclusivo em um website específico. Estes aplicativos da web customizados não estão sujeitos às divulgações de vulnerabilidades ao público – eles não têm usuários terceiros e, portanto, não há necessidade de informar ao público sobre as suas vulnerabilidades.

Os dados dos usuários do IBM AppScan OnDemand fornecem insights sobre o estado dos aplicativos da web customizados e também apresentaram determinado nível de melhorias. No entanto, esta amostra provavelmente é autosseletiva – os desenvolvedores que são inteligentes o suficiente para trabalhar com a IBM para melhorarem a segurança de seu código, provavelmente, são melhores que a média em evitar problemas de segurança. Portanto, é provável que a realidade da segurança dos aplicativos da web na Internet seja um pouco pior que o indicado em nossos dados. A quantidade de atividades de ataque observada certamente sustenta esta conclusão.

Uma categoria de aplicativos da web que está sujeita à divulgação de vulnerabilidades ao público e a muitas atividades de ataque é a de sistemas de gerenciamento de conteúdo (CMS) com base na web. Analisamos quatro destes sistemas e nossos dados mostram que os pontos fracos mais importantes deles são provenientes do ecossistema de plug-ins de terceiros ao qual os sistemas oferecem suporte.

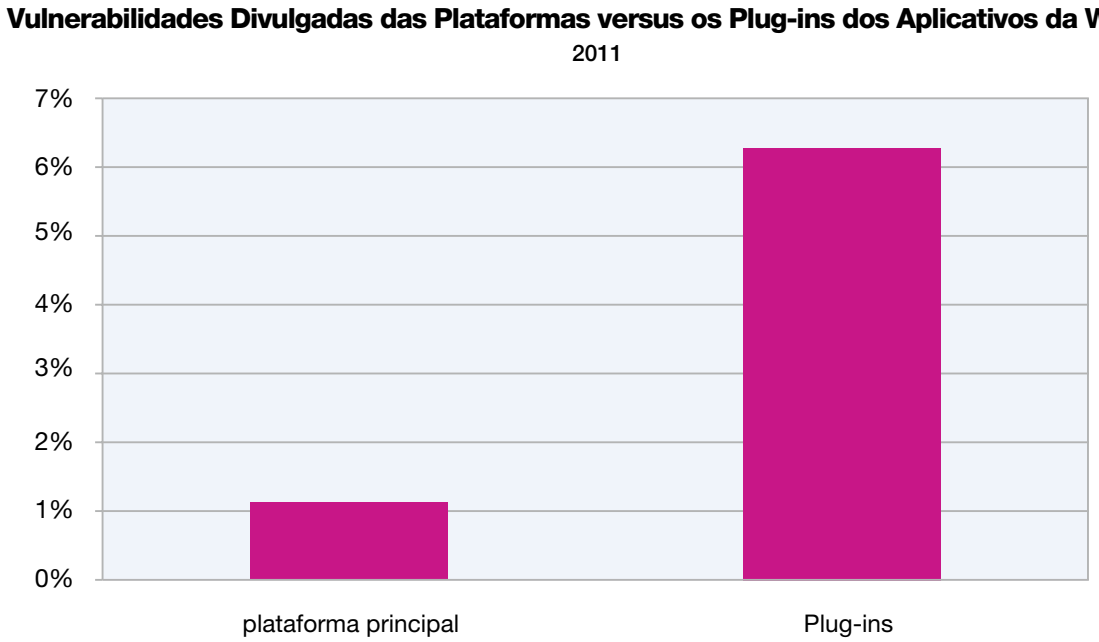


Figura 32: Vulnerabilidades Divulgadas das Plataformas versus os Plug-ins dos Aplicativos da Web – 2011

Há muito menos vulnerabilidades divulgadas nas principais plataformas de CMS que em seus plug-ins e as vulnerabilidades da plataforma principal têm mais probabilidade de ter correções disponíveis. Parte do motivo porque isso acontece, é que há uma grande variação do nível de suporte e atenção aos problemas de segurança oferecidos pelos diversos desenvolvedores de plug-in.

As vulnerabilidades do CMS da web são os alvos preferidos dos invasores porque elas são divulgadas ao público e causam impacto sobre um grande número de websites da Internet. Este ano, as vulnerabilidades repentinas destes sistemas foram decompostas em várias violações. Os usuários dos softwares de CMS da web devem tomar cuidado para avaliar as práticas de segurança dos mantenedores de qualquer plug-in que usarem. Eles devem monitorar de perto as divulgações de vulnerabilidades de segurança dos principais softwares e plug-ins e mantê-las corrigidas como uma principal prioridade. Eles também devem considerar a proteção adicional de seus websites com firewalls de camadas de aplicativos ou prevenção contra invasões.

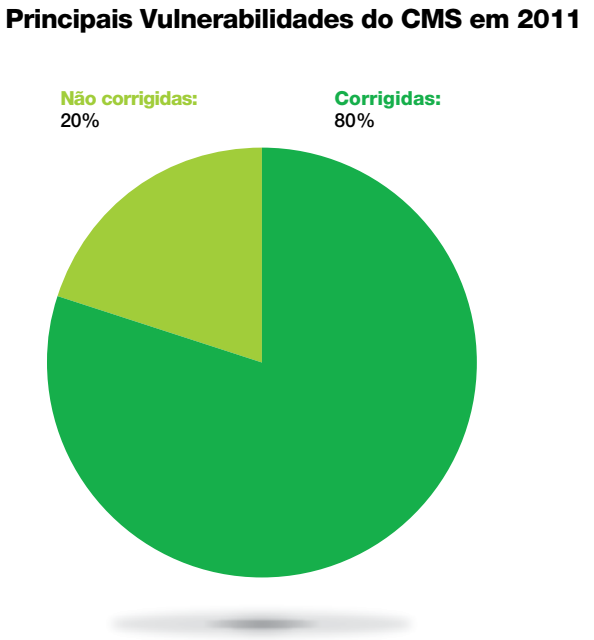


Figura 33: Vulnerabilidades Divulgadas dos principais sistemas de gerenciamento de conteúdo – não corrigidas versus corrigidas – 2011

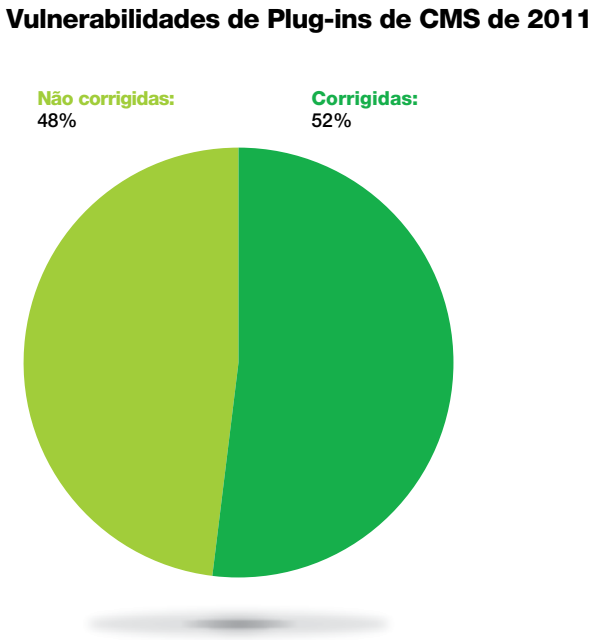


Figura 34: Vulnerabilidades divulgadas dos plug-ins dos sistemas de gerenciamento de conteúdo – não corrigidas versus corrigidas = 2011

Reduções das explorações

Além das melhorias da segurança dos aplicativos da web, existe outro motivo para otimismo. Em 2011, a X-Force identificou uma redução significativa no número de explorações que foi liberado ao público, o menor número observado desde 2006. Este número é inferior em termos percentuais e reais. Nos últimos anos, a porcentagem de vulnerabilidades com explorações públicas chegou a cerca de 15%, mas em 2011 foi de 11%.

Estas reduções refletem as áreas específicas que foram alvo de muitas atividades de ataque nos últimos anos. Durante anos, os navegadores da web foram o alvo principal de ataques acionados por download. Embora o número de vulnerabilidades altas e críticas dos navegadores esteja mais alto a cada ano, o número liberado de explorações destas vulnerabilidades é inferior a todos os anos desde 2006. Os ataques acionados por download passaram a visar aos plug-ins de navegadores de terceiros com mais frequência que ao próprio navegador.

Os leitores de documentos são um componente de terceiros preferencial dos invasores, à medida que os arquivos de documentos maliciosos podem ser usados nos cenários de acionamento por download, bem como anexos aos emails. Embora as vulnerabilidades dos formatos de documentos e as explorações tenham aumentado no ano passado, 2011 apresentou menos divulgações de vulnerabilidades e as liberações de explorações caíram para um nível não visto desde 2007. Isso representa um processo significativo.

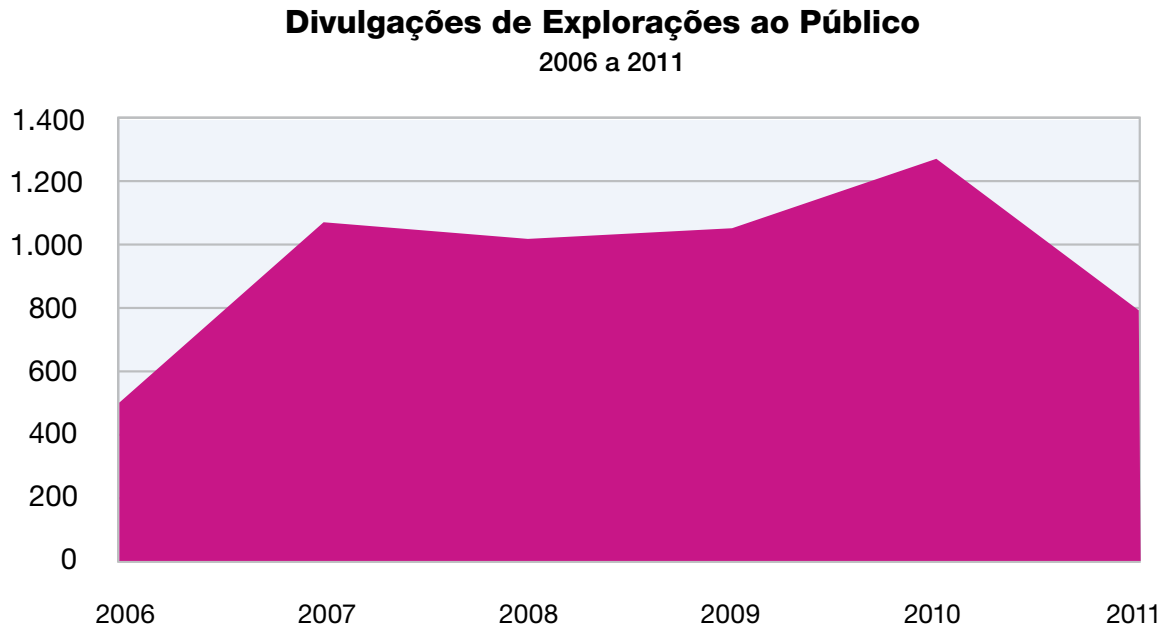


Figura 35: Divulgações de Explorações ao Público – 2006 a 2011

	2006	2007	2008	2009	2010	2011
Explorações ao público	504	1078	1025	1059	1280	778
Porcentagem do total	7,3%	16,5%	13,3%	15,6%	14,7%	11,0%

Tabela 4: Divulgações de explorações ao público – 2006 a 2011

A X-Force acredita que este progresso é resultado das mudanças arquiteturais que foram feitas aos softwares nos últimos anos, o que torna a exploração mais desafiadora. Os gerenciadores de memória dos sistemas operacionais contêm uma variedade de recursos que detectam a corrupção da memória e interrompem a execução com segurança. Muitos navegadores e leitores de documentos vêm com ambientes de simulação de execução que limitam o que as explorações bem-sucedidas podem fazer. O resultado é que as vulnerabilidades que no passado resultariam rapidamente em uma exploração difundida, agora, passam meses sem poder ser exploradas com êxito.

Mesmo assim, a exploração das vulnerabilidades não é impossível atualmente, apesar dos vários recursos de segurança. A X-Force Research publicou vários artigos que descrevem o processo de obtenção de execução de códigos em situações desafiadoras. Na Blackhat USA de 2012, os Pesquisadores da X-Force Mark Yason e Paul Sabanal apresentaram Playing in the Reader X Sandbox, que discutia maneiras pelas quais os códigos maliciosos podem operar em um ambiente de aplicativos simulado. Em 2011, Chris Valasek apresentou Understanding the Low Fragmentation Heap na Blackhat USA, que discutia abordagens para a obtenção de execução de códigos no Windows Heap bastante protegido.

No entanto, as técnicas descritas nestes artigos exigem bastante tempo, esforço e qualificação para serem aplicadas com êxito. Este ano, foi observado um número crescente de situações nas quais as vulnerabilidades críticas que foram exploradas em ambientes laboratoriais não foram visadas em campo. Antes, nós raramente podíamos dizer estes fatos, o que pode significar que estamos no auge de uma nova era de segurança de computadores.

Divulgações de Explorações de Navegadores ao Público
2005 a 2011

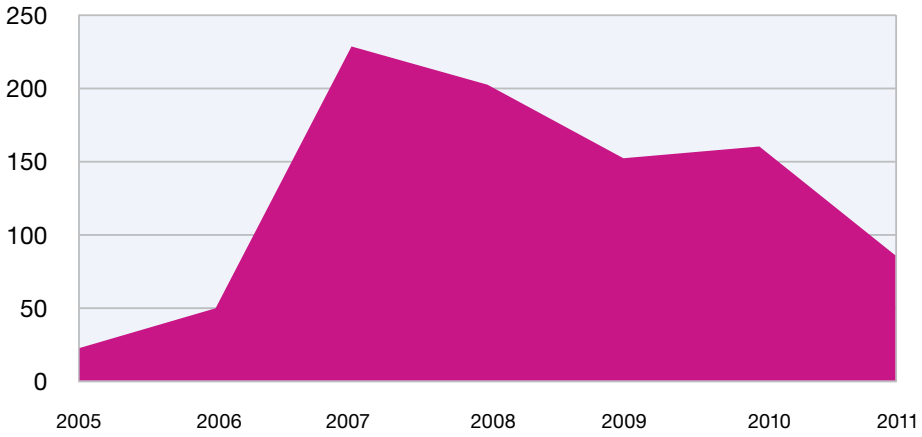


Figura 36: Divulgações de Explorações de Navegadores ao Público – 2005 a 2011

Vulnerabilidades Altas e Críticas de Navegadores da Web
2005 a 2011

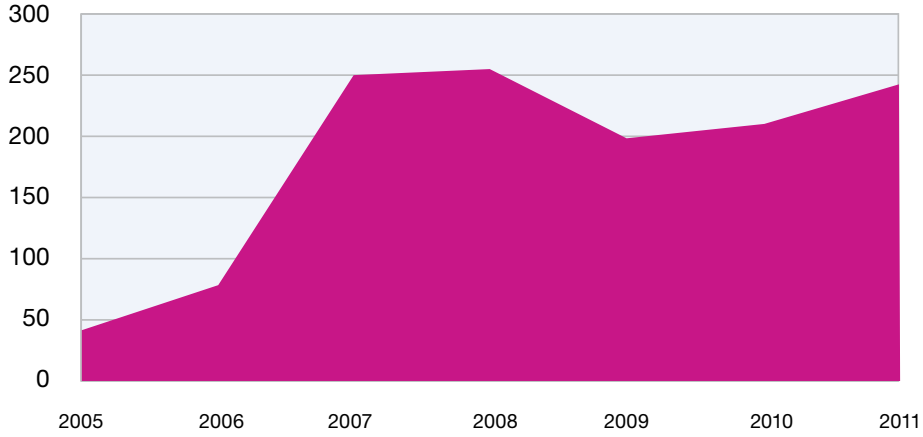


Figura 37: Vulnerabilidades Altas e Críticas de Navegadores da Web – 2005 a 2011

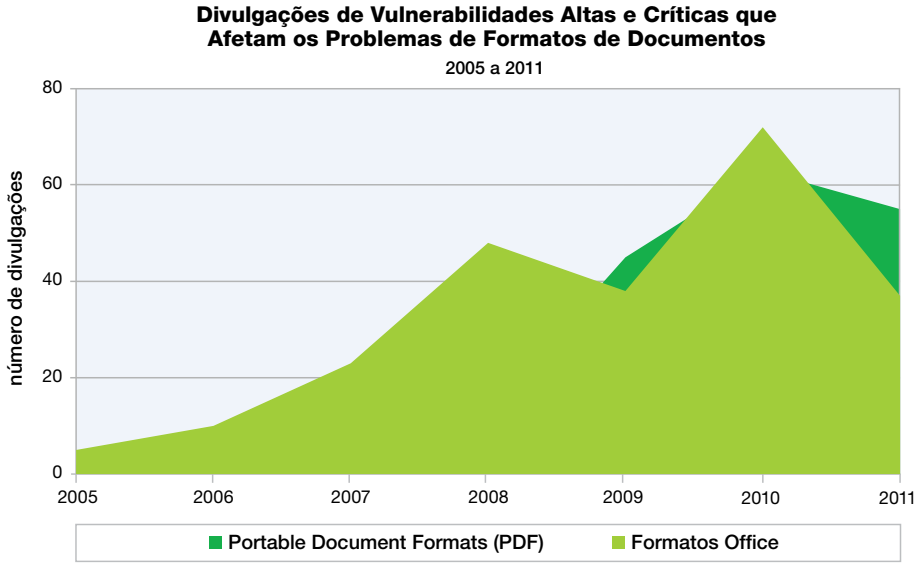


Figura 38: Divulgações de Vulnerabilidades Altas e Críticas que Afetam os Problemas de Formatos de Documentos – 2005 a 2011

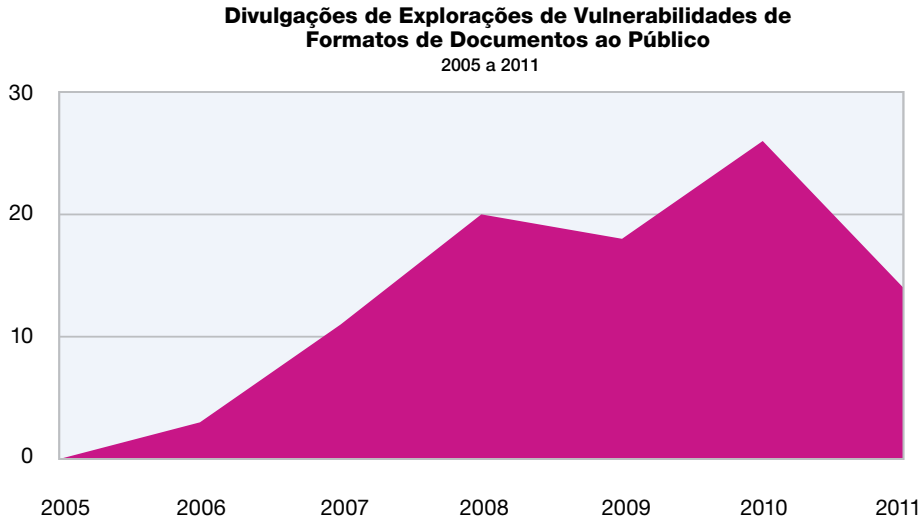


Figura 39: Divulgações de Explorações de Vulnerabilidades de Formatos de Documentos ao Público – 2005 a 2011

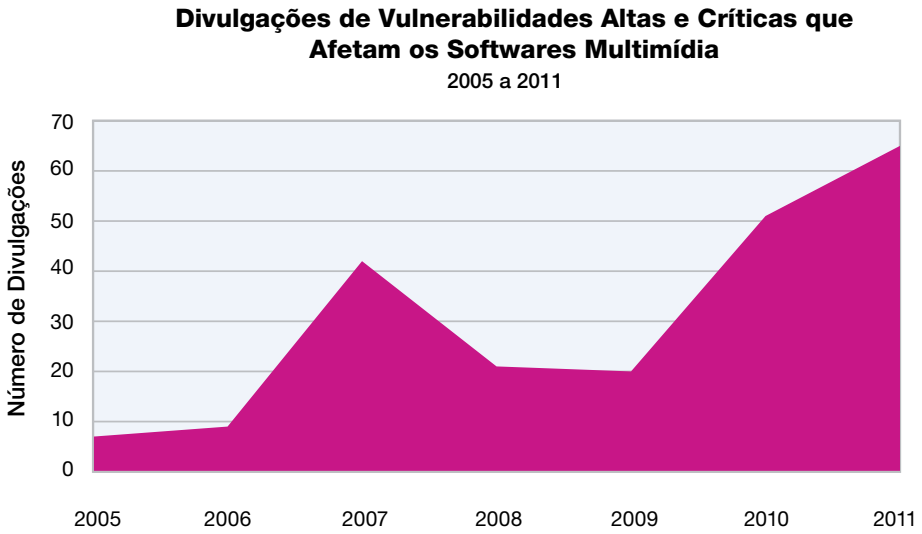


Figura 40: Divulgações de Vulnerabilidades Altas e Críticas que Afetam os Softwares Multimídia – 2005 a 2011

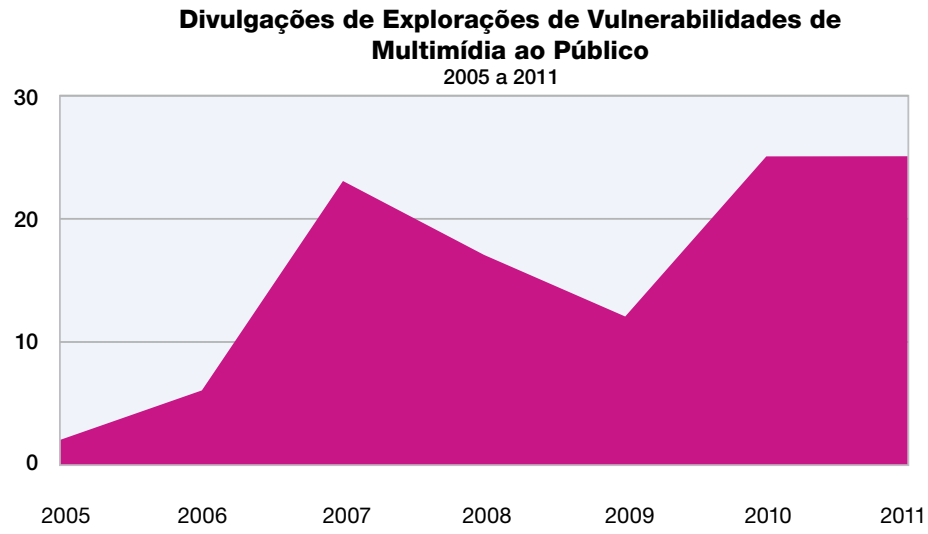


Figura 41: Divulgações de Explorações de Vulnerabilidades de Multimídia ao Público – 2005 a 2011

Invasores que mudam para novas áreas de foco

Obviamente, existem lacunas importantes que continuam sendo eliminadas. Continuamos a observar aumentos do número de vulnerabilidades sendo divulgadas nos players multimídia em 2011 equivalentes ao ano de 2010. Esta continua sendo uma área de foco para os invasores.

Durante a elaboração deste documento, diversas vulnerabilidades críticas de multimídia que foram divulgadas ao público no começo deste ano continuam a ser usadas em ataques direcionados e sofisticados associados às Ameaças Avançadas Persistentes. Estes arquivos maliciosos podem ser anexos aos emails, que são enviados aos alvos com um texto cuidadosamente criado e customizado à vítima visada. É fundamentalmente importante que os players multimídia sejam corrigidos de modo meticuloso ou completamente desativados em ambientes de alta segurança.

O domínio de dispositivos móveis é outra área que está ganhando importância. Existem muitas vulnerabilidades dos sistemas operacionais móveis sendo divulgadas e várias explorações destas vulnerabilidades sendo liberado ao público. O desejo de desbloquear ou disponibilizar os dispositivos móveis é um fator motivador que faz com que as pessoas postem os códigos de explorações móveis online. Obviamente, assim que o código é disponibilizado, ele pode ser usado para propósitos maliciosos em relação aos telefones não desbloqueados.

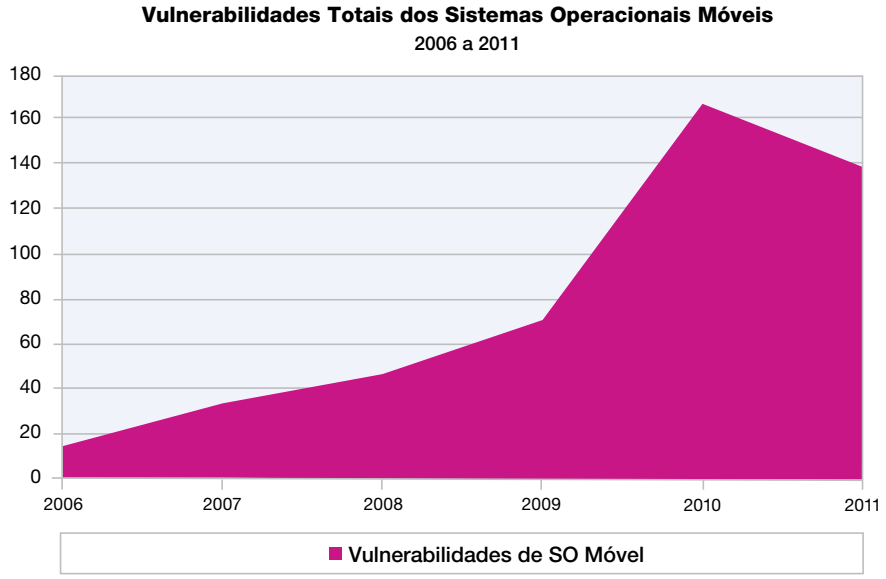


Figura 42: Vulnerabilidades Totais dos Sistemas Operacionais Móveis – 2006 a 2011

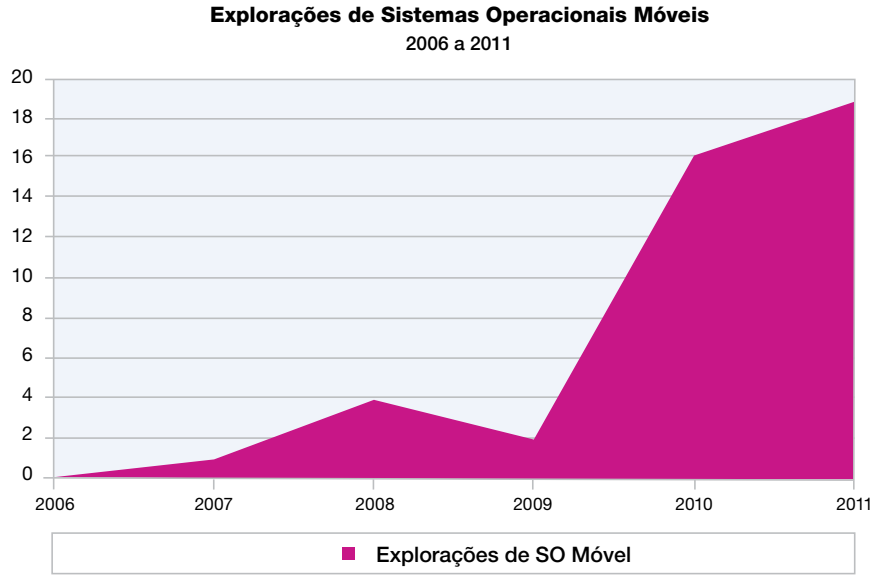


Figura 43: Explorações de Sistemas Operacionais Móveis – 2006 a 2011

Em 2011, foi observado um aumento das atividades maliciosas que visavam aos dispositivos móveis. Alguns aplicativos maliciosos usaram as explorações de desbloqueio disponíveis ao público para obter privilégios elevados dos telefones, assim que eles eram instalados. Devido ao relacionamento de duas camas entre o telefone e os usuários, as empresas de telecomunicação e os fornecedores de sistemas operacionais móveis divulgaram que as vulnerabilidades podiam permanecer não corrigidas nos telefones por um período estendido, fornecendo uma grande janela de oportunidades aos invasores. Esta situação é exacerbada pela proliferação de diferentes plataformas de hardware, bem como de exigências regulamentares. Hoje, a quantidade de atividades de ataques reais é muito pequena em comparação ao volume das atividades que visam às estações de trabalho tradicionais, mas espera-se que o interesse dos invasores nos dispositivos móveis aumente de modo linear no futuro. Começaram a aparecer grandes botnets de dispositivos móveis infectados e isso é apenas o começo.

2011 apresentou um aumento de 70% do número de vulnerabilidades críticas divulgadas em relação ao ano passado. As vulnerabilidades críticas são vulnerabilidades que têm uma pontuação Common Vulnerability Scoring System (CVSS) de 10 para 10. Embora esse aumento pareça ser alarmante, a opinião da X-Force é de que ele representa uma aberração dos dados e esperamos que o volume deste tipo de vulnerabilidade se estabilize em 2012.

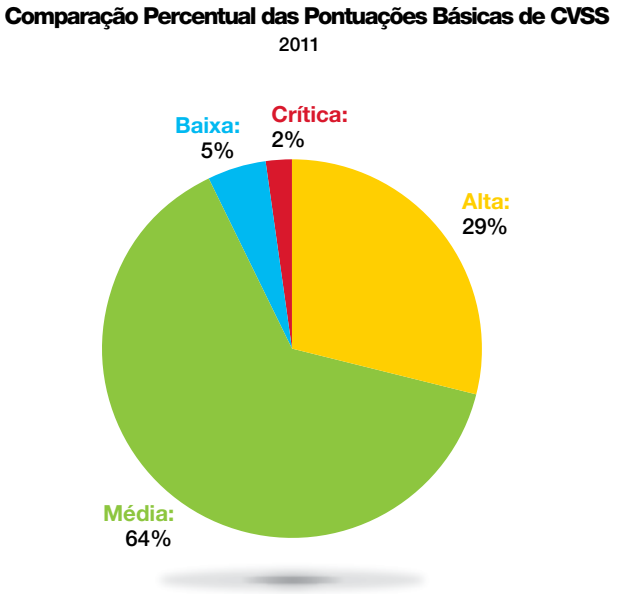


Figura 44: Comparação Percentual das Pontuações Básicas de CVSS – 2011

Pontuação de CVSS	Nível de Gravidade
10	Crítica
7,0-9,9	Alta
4,0-6,9	Média
0,0-3,9	Baixa

Tabela 5: Pontuação de CVSS e Nível de Gravidade Correspondente

"Desbloqueio" é um processo que permite instalar aplicativos não aprovados de terceiros em seu dispositivo. Muitas vezes, o desbloqueio envolve o uso de uma exploração de escalação de privilégios para obter acesso raiz aos telefones com base em sistemas operacionais de estilo Unix e, portanto, às vezes é denominado como "disponibilização" do dispositivo. Assim que é obtido o acesso disponibilizado, os controles de segurança que impedem a instalação de softwares não aprovados podem ser subvertidos.

Vulnerabilidades de softwares corporativos

Uma importante tendência de longo prazo é o aumento da porcentagem de vulnerabilidades sendo divulgadas pelos grandes fornecedores de software. Os dez principais fornecedores de software que divulgaram o maior número de vulnerabilidades de segurança também fornecem a maior variedade de softwares corporativos. Uma lista real dos dez principais também incluiria os fornecedores de sistemas de gerenciamento de conteúdo com base na web, mas excluímos estes produtos desta análise a fim de nos focar no impacto das vulnerabilidades sobre os produtos populares de softwares corporativos.

Estes dez principais fornecedores representaram uma porcentagem constantemente crescente do número total de vulnerabilidades divulgadas, de 19% em 2008 a 31% em 2011. Não acreditamos que isso é meramente uma medida de consolidação do segmento de mercado de software.

As práticas de desenvolvimento seguro se tornaram uma parte cada vez mais importante do ciclo de vida de desenvolvimento de software e, nos últimos anos, os fornecedores responsáveis realizaram etapas para melhorar sua capacidade de identificar e eliminar vulnerabilidades em seus códigos. Estas iniciativas estão produzindo aumentos nas divulgações públicas desses fornecedores, à medida que eles corrigem os códigos fornecidos e disponibilizam estas correções.

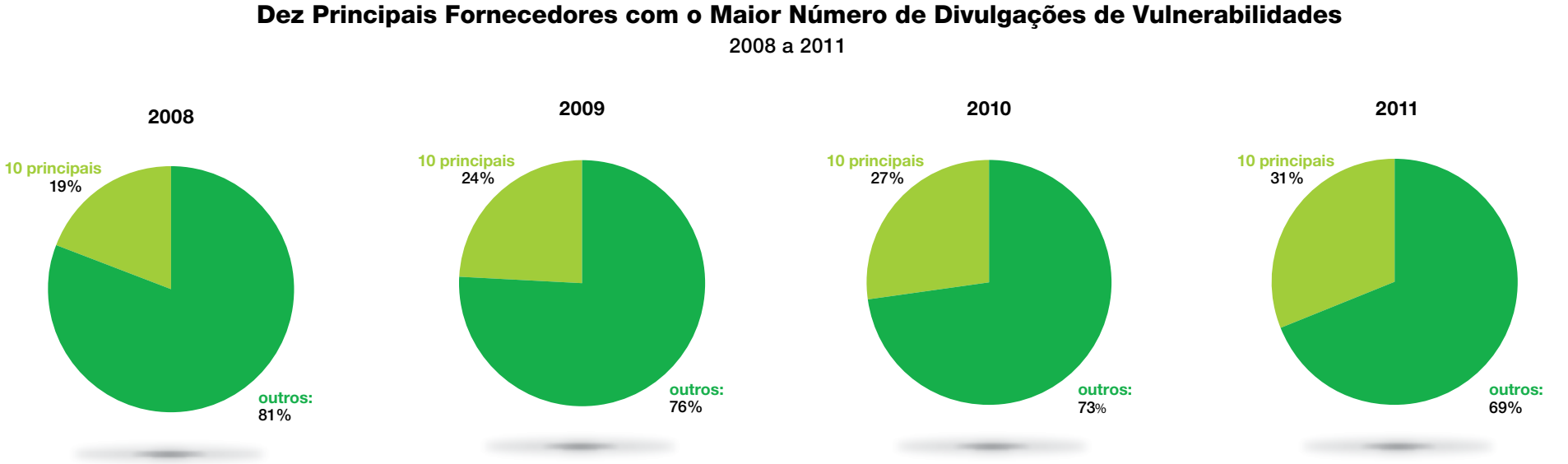


Figura 45: Dez Principais Fornecedores com o Maior Número de Divulgações de Vulnerabilidades – 2008 a 2011

Finalmente, este é um processo que está ajudando a contribuir para as reduções de liberações de explorações ao público observadas este ano. No entanto, em curto prazo, o aumento do número de vulnerabilidades que causam impacto sobre os softwares corporativos populares, bem como o aumento das vulnerabilidades críticas, significa que a equipe de TI responsável por corrigir e proteger as redes de computadores de produção tem muito mais trabalho a fazer para acompanhar essas divulgações em relação aos anos anteriores. O número real de vulnerabilidades dos dez principais fornecedores aumentou em 50% desde 2008. Este fato deve ser considerado ao planejar a capacidade da equipe de correção de vulnerabilidades.

As etapas que a equipe de TI deve realizar para proteger a rede contra as vulnerabilidades divulgadas ao público dependem do fato de haver ou não uma correção disponível e da rapidez com que a correção é disponibilizada. Felizmente, estão sendo observadas melhorias na disponibilidade das correções. Este ano, apenas 36% das vulnerabilidades divulgadas não tiveram correções relatadas ao público. Esta é uma melhoria significativa em relação aos anos anteriores, quando o número chegou a cerca de 45%.

Cerca de 91% das vulnerabilidades são corrigidas no mesmo dia de sua divulgação ao público, o que é a situação ideal. Mas e os outros 9%? A maioria é corrigida em algumas semanas, mas os piores cenários podem demorar muito tempo – às vezes, centenas de dias se passam entre a divulgação da vulnerabilidade ao público e a liberação da correção. Isso é verdadeiro até mesmo quando nos limitamos aos fornecedores de softwares corporativos populares ou às vulnerabilidades com explorações públicas. A X-Force contou apenas 29 casos em 2011 nos quais demorou mais de uma semana para que um principal fornecedor de software corporativo corrigisse uma vulnerabilidade divulgada ao público com uma exploração pública, mas basta uma dessas vulnerabilidades para que um invasor destrua uma rede de computadores.

	2006	2007	2008	2009	2010	2011
não corrigidas	46,6%	44,6%	51,9%	45,1%	43,3%	36,0%

Tabela 6: Porcentagem de correções informadas ao público – 2006 a 2011

Linha de tempo da correção	Todos	Principal fornecedor	Principal fornecedor e exploração pública
mesmo dia	4054	2263	138
semana 1 (1 a 7)	132	19	4
semana 2 (8 a 14)	55	15	5
semana 3 (15 a 21)	26	3	2
semana 4 (22 a 28)	27	10	2
semana 5 (29 a 35)	27	8	2
semana 6 (36 a 42)	33	7	1
semana 7 (43 a 49)	14	6	2
semana 8 (50 a 56)	9	2	1

Tabela 7: Tempo de liberação de correções de todos os fornecedores de software versus os principais fornecedores de software – 2001 Sem1

Estas lacunas não são necessariamente consequência de negligência dos fornecedores. Demora certo tempo para corrigir, empacotar e testar devidamente uma atualização de um aplicativo de software comercial. Em alguns casos, as preocupações de interoperabilidade complexa podem causar um efeito em cascata sobre os diferentes componentes de software, exigindo mudanças extensivas a fim de abordar um único problema de segurança. Portanto, culpar os fornecedores de software pode não ser a melhor maneira de abordar este problema. Inevitavelmente, haverá situações nas quais existirão lacunas entre a divulgação e a correção e os gerenciadores de rede precisarão de estratégias para proteger suas redes durante essas lacunas.

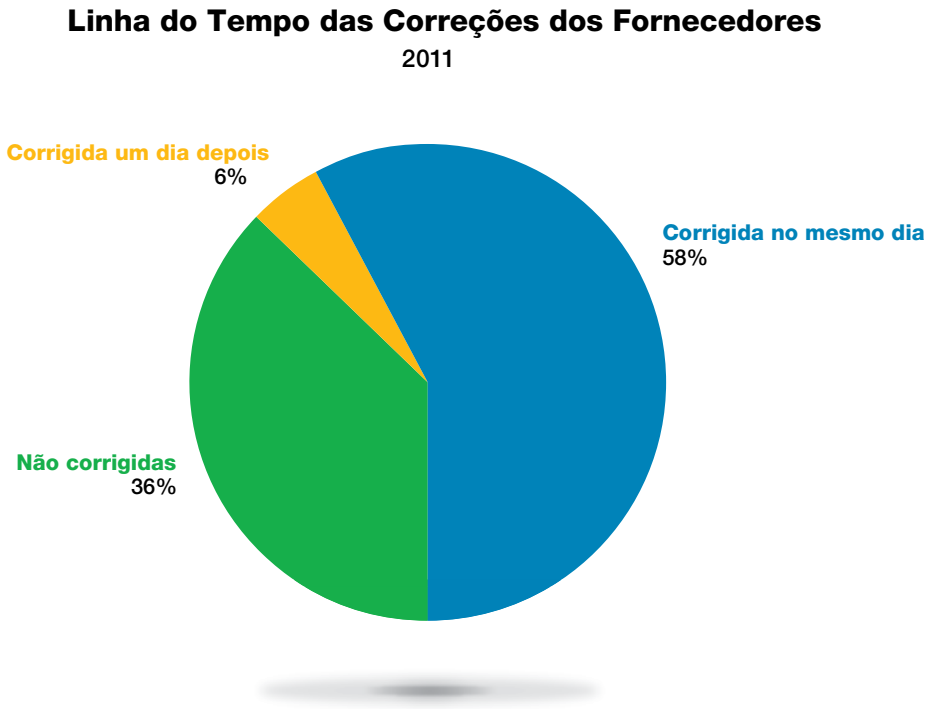


Figura 46: Linha do Tempo das Correções dos Fornecedores – 2011

Quando as vulnerabilidades mais sérias de segurança são divulgadas ao público, a X-Force emite alertas e consultorias. Como um recurso regular de nossos Relatórios de Riscos e Tendências, esses alertas e consultorias são colocados em um gráfico bidimensional, com base na dificuldade de exploração das vulnerabilidades e no valor que elas podem representar para um invasor. Estes fatores nos ajudam a entender quais vulnerabilidades têm mais probabilidade de ter uma exploração difundida na Internet.

A X-Force emitiu trinta e quatro alertas e consultorias em 2011. Dezesseis dessas vulnerabilidades se enquadram na categoria crítica, são fáceis de explorar e extremamente valiosas, o que representa um alvo fácil para as atividades maliciosas. Quase todas estas vulnerabilidades representam problemas de execução remota de códigos dos softwares de clientes, que são exploráveis por meio de acionamento por download ou anexos de email. Atualmente, a maioria está sendo explorada em campo.

Doze destas vulnerabilidades são categorizadas como valiosas, mas mais difíceis de explorar – já que os novos recursos dos sistemas operacionais dificultaram a obtenção com êxito da execução remota de códigos a partir das vulnerabilidades, a X-Force encontrou um número crescente de sérias vulnerabilidades que se enquadra nesta categoria.

Embora ainda exista a preocupação de que os invasores sofisticados podem ter explorações para algumas destas vulnerabilidades, não se espera que haja uma exploração difundida na Internet. O crescimento de vulnerabilidades neste quadrante, em oposição ao quadrante crítico, representa alguns progressos da luta contra os crimes de computadores.

Figura 47: Iniciativa de Exploração versus Recompensa Possível – 2011

Seis das vulnerabilidades para as quais a X-Force emitiu alertas em 2011 são problemas de negação de serviços. Embora essas vulnerabilidades sejam menos valiosas que os problemas de execução remota de códigos, existe um crescente interesse nelas nos últimos seis meses. Os grupos de atividades hackers possivelmente motivados, como o Anonymous, têm lançado ataques de negação de serviços contra as entidades corporativas e governamentais em todo o mundo, a fim de fazer diversas declarações políticas. A maioria dessas atividades envolve fluxos distribuídos de tráfego similar ao legítimo, que pode ser bem difícil de filtrar, ao contrário dos ataques que acionam vulnerabilidades específicas. No entanto, começamos a ver algum interesse desses invasores em vulnerabilidades que podem tornar seus ataques mais efetivos.

As ferramentas e técnicas que esses hackers desenvolveram também passaram às mãos de invasores motivados financeiramente, que parecem estar usando ataques de negação de serviços em contextos de negócios competitivos com uma frequência crescente. Com uma eleição política nos Estados Unidos este ano, juntamente com as controvérsias globais relacionadas às leis de propriedade intelectual, esperamos ver ataques de negação de serviços distribuídos mais proeminentes ao longo de 2012.

Engenharia social de mídia social: Como os invasores fazem isso?

Visão geral

Desde a adoção difundida da Internet, houve poucas inovações que causaram o mesmo impacto que a mídia social. A mídia social está mudando a maneira como a sociedade se conecta, se inter-relaciona e compartilha informações. O subproduto desta mudança é uma inundação de informações pessoais e privadas que anteriormente eram difíceis de reunir em um local central e arquivável – a saber, a Internet. Esta riqueza de informações é particularmente útil para as mentes maliciosas da invasão de computadores.

Nos últimos sete anos, a rede social passou por um passatempo alternativo à atividade online número um do mundo, obscurecendo até mesmo os mecanismos de busca. Até o ano de 2011, aproximadamente 80% da população global de usuários online (mais de um bilhão de pessoas) estava usando a mídia social[20]. Naturalmente, esta atividade concentrada representa um ambiente fértil para um invasor. As fraudes e scams que foram bem-sucedidos por email anos atrás encontraram vida nova nos fóruns de mídia social, bem como um novo grupo de possíveis alvos.

A vasta quantidade de informações privadas que os usuários estão colocando nas redes sociais mudou o paradigma da coleção de inteligência. A inteligência reunida dessas redes já começou a desempenhar uma função na pesquisa de pré-ataques relacionada à infiltração das redes da computação do setor público e privado. Como um resultado direto, alguns dos ataques de hackers de mais alto perfil de 2011 começaram com a coleção da Inteligência de Software Livre (OSINT) e/ou das explorações de engenharia social executada por meio da mídia social.

20 Fonte: Comscore It's a Social World Report, dezembro de 2011

Estes ataques exploram uma área obscura do perímetro organizacional, visando a um indivíduo e às informações que ele insere, geralmente, em um contexto não relacionado ao local de trabalho. Os indivíduos associados a uma organização visada podem inserir informações valiosas de modo inadvertido (ou proposital) ou introduzir malwares nos sistemas corporativos, o que resulta em roubo ou destruição dos ativos de dados corporativos.

Embora a estruturação de uma exploração bem-sucedida que se aproveita da mídia social possa ser desafiadora, foi comprovado que a taxa de sucesso dos ataques e as recompensas associadas valem o esforço. Esta seção exporá o impacto que a mídia social tem causado sobre a segurança, analisando particularmente as mudanças na coleção de inteligência e na anatomia dos ataques de engenharia social que se aproveitam das plataformas de mídia social. O objetivo desta seção é informar os leitores sobre as metodologias emergentes de ataque e seu possível impacto sobre as entidades de setor público e privado.

Coleção de inteligência

É geralmente aceito que a coleção de inteligência segue um ciclo relativamente simples que envolve o desenvolvimento de requisitos, planejamento e direção, coleção real, processamento, análise e disseminação, embora o número real de etapas do ciclo possa variar. Alguns tipos comuns da inteligência reunida neste processo são a Inteligência Humana (HUMINT), a Inteligência de Software Livre (OSINT), a Inteligência de Sinal (SIGINT), a Inteligência de Medição e Assinatura (MASINT) e a Inteligência de Imagem (IMINT).

Antes da mídia social, os métodos de coleção de cada um desses tipos de inteligência eram relativamente objetivos e, muitas vezes, exigiam um foco especializado em cada um deles. O surgimento da mídia social mudou as fontes da coleção de inteligência das áreas individuais em direção à OSINT.

A HUMINT não exige mais o contato físico para que exista o "contato interpessoal" e é muito mais pública que anteriormente. A SIGINT não exige mais a intercepção de sinais, já que a mídia é bastante compartilhada com o público pelas entidades e a inteligência de imagem é aprimorada pelos maiores repositórios de imagens do mundo (Fotki, Webshots, Facebook etc.).

Agora, a mídia social oferece aos coletores de inteligência um repositório de informações incomparáveis na história humana. Considere que uma pessoa que imediatamente adote a mídia social possa incluir não apenas artefatos de inteligências, mas também fornecer o contexto para esses artefatos específicos. Ao oferecer uma voz pública para as massas, a mídia social convida inerentemente a disseminação acidental ou proposital de informações secretas. Isso é evidenciado pelas diversas ocorrências nas quais os oficiais dos EUA postaram informações por engano sobre viagens confidenciais ou quando um congressista postou: "[de] volta a Washington. Recebendo grandes sínteses secretas de inteligência do Irã". No entanto, além do domínio da indiscrição descarada, os usuários muitas vezes postam informações benignas na mídia social, como endereços de email pessoal, cidade de residência atual e informações educacionais.

Coleção de inteligência de software livre

A quantidade massiva de inteligência pública ou de software livre (OSINT) que está disponível para coleção abriu um novo domínio de segurança de informações e ataques. A tendência de realização de buscas de inteligência de software livre cresceu rapidamente em 2011 e, provavelmente, continuará aumentando em 2012.

Este crescimento massivo gerou todo um domínio de ferramentas e técnicas de busca. Essas ferramentas incluem utilidades que são concentradas não apenas na busca real, mas também no mapeamento dos dados encontrados. As ferramentas mais utilizadas, como a Maltego, oferecem assistência à busca de informações e as representam de uma maneira facilmente utilizável. Enquanto isso, as ferramentas como a Foca auxiliam na busca de informações e as utilizam para reunir mais inteligência.

Tem sido amplamente divulgado que as organizações de cumprimento da lei não estão apenas aproveitando as ferramentas existentes para minar os dados públicos das redes sociais, mas também estão procurando novas ferramentas que são mais poderosas e granulares. Estas iniciativas são interessantes, já que mostram que a coleção de OSINT não é apenas uma crescente tendência para os invasores, mas também para os profissionais de segurança. De fato, a riqueza de informações é útil para determinar quem pode estar realizando ataques.

No contexto da invasão de computadores, as informações como essas são puro ouro para os ataques de engenharia social e ataques lógicos de autenticação, como as reconfigurações de senha que exigem informações pessoais. Os invasores foram bastante ativos ao explorar esses pontos fracos da mídia social para proteger os pontos de entrada nas organizações visadas. Devido ao sucesso de diversos ataques de alto perfil executados em 2011, os ataques de engenharia social por meio da mídia social é a tendência emergente das Ameaças Avançadas Persistentes.

Como funciona? - Não é um bicho de sete cabeças

Por exemplo, esta exploração em particular é um ataque de três níveis que combina a engenharia social, spear phishing e execução repentina para concluir a agenda. Assim como

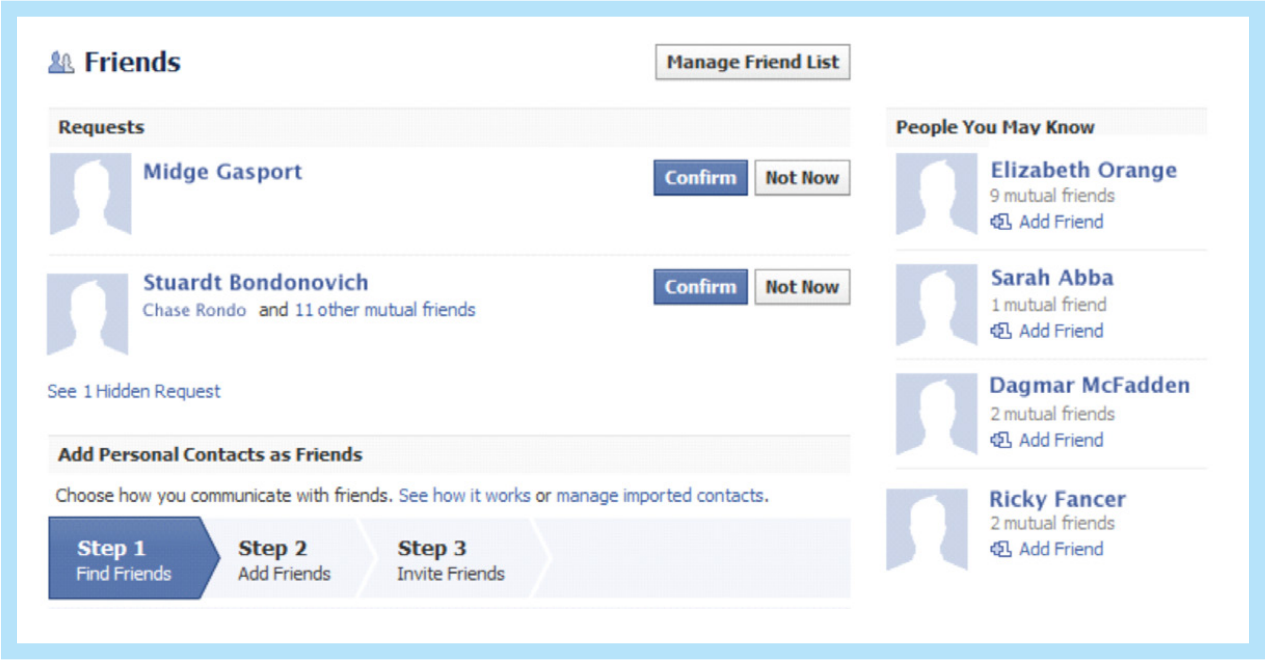


Figura 48: Exemplo de lista de possíveis contatos para fazer spear phishing 2011

trapaceiros andam pelos cassinos de Las Vegas procurando por jogadores fracos e as chitas andam pelo Serengueti tentando encontrar zebras machucadas, os invasores trapaceiam nas redes sociais procurando usuários finais com listas de amigos grandes e ativas.

Primeiramente, o invasor seleciona uma organização-alvo. Depois, ele cria uma conta em um fórum de mídia social, como o LinkedIn, e configura um apelido e um perfil que sugere uma afiliação com a organização, como um ex-funcionário. Em uma economia em baixa, em um segmento de mercado que passa por um alto nível de atividades de fusões e aquisições, disfarçar-se de um ex-funcionário do alvo pode fazer com que o apelido pareça plausível. Com a conta estabelecida, os fóruns como Facebook e LinkedIn sugerem aos invasores listas de possíveis conexões da organização visada.

Assim que o invasor sabe quem abordar, começa a fase de engenharia social. O invasor tenta fazer conexões com os funcionários atuais do alvo. As abordagens são simples, mas variadas – entrar em contato novamente após alguns anos, mudou de emprego e está procurando aumentar sua rede profissional, perdeu o emprego recentemente e está procurando voltar à empresa-alvo ou quer se conectar após terem se conhecido em um evento do segmento de mercado. Uma abordagem que contém palavras escolhidas com cuidado e, às vezes, informais, tem boas chances de sucesso se o invasor abordar um grande número de indivíduos. Fazer a primeira conexão é muitas vezes a etapa mais difícil. Às vezes, o invasor criará outra conta com o apelido da organização-alvo e relacionará as duas para criar credibilidade. Não há um mecanismo para vetar essas falas alegações e representações feitas nos fóruns de mídia social; portanto, a maioria das contas de usuário é considerada com valor nominal e tratada como legítima.

Assim que o invasor fizer uma conexão legítima com o alvo, fica mais fácil reunir outras. O LinkedIn, por exemplo, promove apresentações secundárias e terciárias dos membros, assim como o Facebook faz por meio de amigos de amigos. Além disso, a capacidade de relacionar contas entre os principais fóruns facilita que o invasor estabeleça contatos adicionais a partir de uma variedade de fontes por meio do relacionamento com um dois contatos individuais legítimos.

Depois, o invasor começa a analisar os perfis de cada um dos contatos legítimos, coletando informações pessoais, informações relacionadas à organização e até mesmo medindo as áreas de interesse para determinar a melhor abordagem a cada indivíduo. Estabelecer um nível básico de confiança com estes novos contatos é algo facilmente realizado – pedir simples informações ou encaminhar algumas

informações que podem ser interessantes. Isso permite que o invasor determine quais usuários finais são mais ativos e quais têm mais probabilidade para "auxiliá-lo" a acessar o alvo.

Finalmente, assim que o invasor preparou os indivíduos, pode começar a fase de spear phishing do ataque. Este ataque é mais bem-sucedido quando o invasor tem acesso às contas de email corporativo dos usuários finais. Até mesmo um ou dois emails corporativos permitem que o invasor entenda as convenções de nomenclatura e adivinhe as contas de email adicionais. Um email bem elaborado – um anúncio de vaga de emprego para um funcionário insatisfeito, um pesquisa profissional para uma pessoa que está procurando emprego, um link de um vídeo instrutivo para um indivíduo em transição na carreira – qualquer coisa que pareça legítima, possa estar fracamente associada ao trabalho e que tenha o potencial para atrair a atenção e aceitação de, no mínimo, um dos usuários finais do ambiente de computação corporativa do alvo. Geralmente, esses emails contêm uma carga útil, um link, um download ou um arquivo *.exe malicioso e é o usuário final que estabelece o estágio final do ataque em movimento.

Figura 49: Exemplo de email de spear phishing em 2011[21]

Assim, o invasor está "dentro do sistema" e o ataque repentino pode ser executado. A única coisa boa – a diferença entre um ataque com falha e um bem-sucedido – é o usuário final realizar uma ação para que a exploração seja ativada.

Etapas realizadas pelas organizações para mitigar os riscos da mídia social

Um estudo do Ponemon Institute[22] em setembro de 2011 indicou que somente 35% dos participantes tinham uma política escrita de mídia social. Dessas organizações, somente 35% aplicavam-na ativamente. O mesmo estudo indicou que os ataques de vírus e malware nos sistemas de computação corporativa aumentaram mais de 50% desde que seus funcionários começaram a usar a mídia social. Infelizmente, não há softwares ou conjuntos de produtos de terminal que possam ser implementados facilmente para realizar a defesa contra a engenharia social. Assim como ocorre com a maioria das ameaças visadas aos humanos, a melhor forma de gerenciar esses riscos é por meio de políticas e instrução.

21 Fonte: http://contagiodump.blogspot.com/2011/10/cve-2011-0611-pdf-2011-10-24-northkorea.html.
22 Fonte: http://www.ponemon.org/Global Survey on Social Media Risks September 2011. O estudo pesquisou 4.640 profissionais de TI e segurança de TI dos Estados Unidos, Canadá, Reino Unido, França, Alemanha, Itália, Austrália, Cingapura, Hong Kong, Índia, Brasil e México com uma média de 10 anos de experiência no campo.

Estas iniciativas podem ser divididas em duas áreas de foco específicas: ações para ambientes de negócios e ações para usuários. À medida que a mídia social vira quase uma experiência pessoal, encontrada principalmente fora do local de trabalho, os usuários são amplamente responsáveis por sua privacidade e segurança. No entanto, é obrigatório que os negócios criem políticas e procedimentos para auxiliar na orientação dos funcionários, bem como na proteção da marca e dos ativos da empresa. Estas iniciativas se parecem com os programas de "Reconhecimento de Segurança" do passado, mas devem conter exclusivamente orientações sobre as responsabilidades dos usuários finais, como:

Ativar as configurações de segurança e privacidade. Os principais fóruns de mídia social têm configurações básicas de privacidade para os usuários. É importante que os usuários finais entendam quais controles de segurança e privacidade estão disponíveis nos fóruns que usam regularmente, mesmo que eles não se considerem usuários ativos. Para reduzir a exposição aos spams, scams e invasores oportunistas, os controles de segurança e privacidade devem ser configurados aos níveis máximos.

Os usuários finais também devem entender que qualquer ação de segurança e privacidade realizada será minimizada aos menores níveis em seu círculo social do trabalho. Por exemplo, se um amigo usar somente as configurações mínimas de segurança e privacidade, ele cria uma avenida de exposição a todas as conexões de seu círculo, independentemente das maiores posturas de segurança adotadas por essas conexões. Em outras palavras, se o Amigo1 do Facebook limitar seus posts e contatos permitidos somente ao seu círculo de amigos, mas o Amigo2 disponibilizar posts e contatos a qualquer pessoa, qualquer coisa postada no mural do Amigo2 pode ser vista por qualquer pessoa do Facebook. Dependendo das configurações de privacidade do Amigo2, os posts podem até mesmo ser buscados na Internet.

Incentivar os usuários finais a adotar uma configuração "negar de modo padrão" em sua presença na mídia social parece ser algo antiético, mas é esse nível de reconhecimento de segurança que pode protegê-los contra os ataques de engenharia social.

Adicionar somente os amigos. Os ataques de engenharia social não seriam tão bem-sucedidos se eles não fossem tão inteligentes em alguns aspectos. Assim como acontece com os artistas do mundo real, os invasores de mídia social começam seus ataques tentando obter determinado nível de confiança de seus alvos. Fingindo ser um antigo colega de classe, um antigo colega, um amigo de um amigo ou um parente não é nada incomum. Fingir um relacionamento de trabalho via LinkedIn, por exemplo, oferece credibilidade quase instantânea ao status de LinkedIn do invasor na mídia social, como um fórum orientado aos negócios. Ainda assim, fazer conexões pelo LinkedIn usando falsas alegações de relacionamentos de trabalho anteriores ou de ter conhecido o alvo em uma conferência ou evento do segmento de mercado é plausível o suficiente para convencer o alvo a aceitar a conexão. Os usuários finais que procuram aumentar seu status online ou esfera de influência podem aceitar rotineiramente as solicitações aleatórias simplesmente para aumentar seus números.

Apesar dos vários incentivos e recompensas de ter várias e diversas listas de seguidores e amigos, é importante lembrar que este é exatamente o tipo de ambiente no qual o invasor procura se esconder. Os usuários finais devem considerar cuidadosamente as solicitações de amizade, aceitando-as com base em relacionamentos reais ou algum nível de confiança do fórum de mídia social, como comunidades patrocinadas por fóruns, interesses comuns etc. As solicitações aleatórias de amizade com base em conexões mútuas secundárias ou terciárias devem ser filtradas com cuidado. As comunicações e solicitações privadas em relação a informações pessoais detalhadas feitas por novos amigos, conhecidos do usuário final por mídia social, devem ser sempre vistas com cuidado, principalmente quando a solicitação envolve informações de contato reais.

Ter cuidado com links e downloads. Os links e downloads têm sido um veículo preferencial dos invasores para fornecer malwares aos seus alvos, já que os emails se tornaram obsoletos no final da década de 90. A tendência evoluiu constantemente nos fóruns de mídia social. Os usuários finais devem ter extremo cuidado e considerar cuidadosamente a fonte antes de clicar em quaisquer links ou fazer download de qualquer coisa (principalmente arquivos executáveis), de fontes desconhecidas ou não confiáveis. Muitos novos "amigos" podem tentar fornecer cargas úteis maliciosas por meio de mensagens pessoais que direcionam os usuários finais a vídeos hilários do YouTube, fundos de tela engraçados, fóruns falsos de fãs ou jogos gratuitos incríveis. Muitas vezes, os invasores aleatórios tentam fornecer cargas úteis maliciosas via spam. O Facebook e outros fóruns postam avisos rotineiramente quando são alertados sobre ataques difundidos. Os usuários finais devem assinar quaisquer serviços de alerta oferecidos pelos respectivos fóruns.

Tomar cuidado com competições, presentes, prêmios e ofertas especiais. "Você pode já ser um ganhador". Os scams de prêmios e outras ofertas especiais também existem desde os primeiros dias dos emails, mas continuam a ter um forte desempenho nos fóruns de mídia social. Os criadores de scam geralmente usam este tipo de oferta, por exemplo, "gift cards de alto valor gratuitos disponíveis aos membros do fórum", para direcionar os usuários finais a um website sem fim que carregará cookies ou mesmo spyware ou a websites que imitam negócios ou marcas legítimas e exigem que o usuário preencha inscrições ou pesquisas complexas para se qualificar à falsa competição. De qualquer forma, o criador de scam está coletando informações pessoais de seus alvos. O Facebook hospeda uma comunidade de usuários chamada Facecrooks, que alerta os membros sobre scams, fornecendo detalhes e informações de correções quando disponíveis. Os usuários finais devem assinar quaisquer serviços de alerta de scam oferecidos pelos seus respectivos fóruns de mídia social.

Considerar limitar as informações relacionadas ao trabalho. Os usuários finais devem sempre consultar as políticas de uso para mídia social adequadas dos empregadores ao comunicar informações sobre a organização, os colegas, os clientes, produtos, serviços e projetos nos quais eles estão envolvidos no momento. Além de informações específicas, os usuários finais podem considerar fazer referências ao seu segmento de mercado ou empregador apenas em termos gerais, a fim de evitar divulgações inadvertidas. A filtragem cuidadosa de informações relacionadas ao trabalho está se tornando cada vez mais importante à medida que mais usuários finais buscam oportunidades de contratação ou rede por meio da mídia social e à medida que mais empregadores escaneiam a mídia social para avaliar funcionários atuais ou possíveis[23].

Na ausência de uma política corporativa por escrito, o senso comum pode ser seu melhor guia em termos de postagem de informações relacionadas ao trabalho.

Às vezes, até mesmo uma referência descuidada pode revelar mais que a intenção original do usuário final. O melhor princípio básico relacionado a quaisquer posts nos fóruns de mídia social é que, apesar das configurações de segurança e privacidade e apesar das boas intenções e até mesmo dos acidentes, a rede social é desenvolvida para compartilhar informações globalmente pela Internet. Todos os posts devem ser considerados com cuidado, já que eles são publicados instantaneamente e, essencialmente, são irrecuperáveis.

Tendências futuras

Os ataques de mídia social continuarão a aumentar em influência e variação no futuro. Esta expansão inclui o empreendimento em tecnologias aparentemente não relacionadas. Por exemplo, os automóveis já estão ostentando interfaces com a Internet e interconexões por meio da mídia social. Com esta expansão, a mídia social continuará a evoluir e representar uma arena facilmente explorável para os invasores.

As organizações empresariais precisam desenvolver e aplicar as políticas e os usuários devem se tornar capacitados e experientes em sua própria proteção.

23 Apesar das reações negativas em 2011 a essa tendência, muitos empregadores usam a mídia social abertamente como parte do processo de contratação, incluindo verificações de histórico e crédito.

Dez principais erros comuns dos CSIRP

Os Planos de Resposta a Incidentes de Segurança de Computadores (CSIRP), uma pedra fundamental de qualquer ambiente com qualquer coisa mais avançada que uma calculadora cara, são absolutamente cruciais ao formular uma resposta aos incidentes de segurança que envolvem redes, computadores ou dados eletrônicos. Durante um incidente, um CSIRP é o mapa que guia as respostas.

Este artigo descreve diversos erros mais comuns que envolvem CSIRPs. A equipe de Emergency Response Services (ERS) da IBM está intimamente envolvida em planos CSIRP, já que a IBM responde frequentemente às emergências dos clientes e desenvolve planos CSIRP customizados para seus clientes. A ERS é muito precisa em observar o que funciona ou não. Neste artigo, serão descritas várias das desvantagens observadas mais comuns destes planos.

Nº 1 Criar um CSIRP muito complexo

Ao desenvolver seu CSIRP, é melhor ter em mente que o público estará lendo o documento durante uma crise e não relaxando em uma cafeteria com um copo e um salgado nas mãos, absorvendo lentamente o material enquanto ouve música clássica. Embora possamos sonhar com um incidente que envolva salgados quentinhos e um tempo ilimitado para digerir um plano, geralmente, isso não vai acontecer. Pode haver stress. Os indivíduos podem estar em pânico e preocupados com seus empregos. Os executivos que podem ou não entender os pontos técnicos reais do que está acontecendo podem estar nervosos porque a mídia de notícias local está fazendo perguntas. Depois disso, a solução seria apenas chorar e ficar em posição fetal... já se pode ter uma ideia.

Na situação descrita acima, há tempo para consultar um plano CSIRP grande e detalhado? Obviamente, não. Os CSIRPs devem ser precisos, claros e concisos. Caso um funcionário que não esteja familiarizado com o documento não possa examinar rapidamente os processos descritos no plano, entender a cadeia de comando e realizar as ações necessárias, ele pode ser muito complexo. Claramente, fazer um CSIRP muito simples também é uma armadilha; atingir o equilíbrio correto entre a brevidade e direções acionáveis é essencial a um CSIRP bem-sucedido.

Nº 2 Sobrecarregar os principais funcionários

Todas as organizações têm um José. O José conhece todo mundo e todos os sistemas, roteadores, cabos e as principais cafeteiras do prédio. Ele é a pessoa a quem todos recorrem durante um incidente. Sem dúvidas, José é a melhor pessoa no local para pequenos incidentes e pode manipulá-los do início ao fim. Quando desenvolvemos CSIRPs para nossos clientes, encontramos rapidamente o José da organização durante nosso questionamento-padrão: Quem é responsável pelos antivírus? José. Quem se comunica com os executivos? José. Quem planeja as festas da empresa? José.

José é fantástico no que faz das oito às cinco. No entanto, quando um incidente se prolonga por dias, ele não pode ser o responsável por 72 horas diretas. É necessário separar as obrigações durante um incidente e implementar backups anteriormente designados caso uma empresa não queira funcionários sobrecarregados e sonolentos planejando as festas em junho.

Nº 3 Tratar um incidente como um processo em série.
Durante um incidente de grande escala, multitarefar é essencial. Os Gerenciadores de Incidentes que somente analisam um incidente como um processo em série serão incapazes de resolvê-lo em tempo hábil. Embora cada incidente seja único, todos eles compreendem diversos objetivos de curto prazo. Apresentar assinaturas de antivírus, corrigir sistemas, liderar iniciativas investigativas, informar funcionários e clientes sobre seu status atual, buscar suprimentos adicionais de bebidas cafeinadas e outras tarefas importantes são todos processos únicos e devem ser tratados desta forma. Uma falha comum é quando uma empresa se concentra apenas em uma dessas tarefas em um momento e negligencia as outras tarefas importantes que podem ser concluídas paralelamente.

Nº 4 Não estabelecer linhas adequadas de comunicação
Ao responder a um incidente, diversos indivíduos e fornecedores podem ser solicitados a oferecer assistência. O gerenciador de incidentes – o indivíduo responsável pelo gerenciamento de "forças terrestres" – deve ser um principal comunicador. A comunicação deve ser ordenada, eficiente e seguir os canais adequados. Imagine uma sala de operações com 25 pessoas diferentes, na qual cada uma dessas pessoas receba ordens de 15 outras e não exista uma linha de comunicação adequada. O progresso está congestionado e um incidente que deveria ter sido resolvido há 24 horas é prolongado. As capacidades de comunicação podem ser tão importantes quanto as técnicas ao confrontar um incidente. Sem uma voz, uma visão e um orientador, muitas vezes o resto da equipe está fadado a falhar. Um CSIRP deve abordar e codificar as linhas de comunicação para assegurar que todas as informações estejam nas mãos das pessoas que precisam delas e não congestionadas em "feudos" compartimentados.

Nº 5 Concentrar-se no que é fácil, não no que precisa ser feito
Em cada incidente, surge o impulso de se concentrar nas tarefas fáceis e não nas que precisam ser feitas. Isso é parecido com completar o fluido de limpador de para-brisa de um carro quando o motor não funciona. Certamente, o fluido não precisa ser completado eventualmente, mas sem um motor funcional, seu carro é inútil. O mesmo vale para um incidente. Existem tarefas difíceis e fáceis, mas independentemente da dificuldade, algumas apenas precisam ser concluídas. Não concentrar sua energia nos problemas essenciais, sejam eles difíceis ou fáceis, pode causar dores de cabeça e incidente prolongados.

Nº 6 Concentrar-se no que é estimulante, não no que precisa ser feito
Durante alguns incidentes, o respondente descobrirá algumas informações interessantes e se concentra na busca de uma toca de coelho que não tem a ver com o incidente em si. O item recém-descoberto pode ser extremamente cativante, mas não desempenha uma função material na resolução do incidente. Podem ser gastas horas intermináveis nesta toca de coelho, mas o coelho está de férias fora do país. Lembre-se, você está caçando coelhos e não observando as variações arquiteturais da toca.

Nº 7 Descartar o CSIRP
Ocasionalmente, surgirá um impulso para descartar o CSIRP, pois ele não aborda a situação específica em mãos. Existe um motivo para que o documento não aborde os vírus de email mais recentes. O CSIRP não é feito para ser um guia abrangente de como confrontar cada incidente específico. Em vez disso, o documento é um projeto para linhas de comunicação, funções, notificações necessárias e etapas a serem realizadas para responder ao incidente. Embora cada incidente seja único, o documento deve permitir que uma resposta seja formulada por meio de um entendimento rápido das identidades, funções e protocolos de comunicação dos principais responsáveis que devem ser incluídos. Com esta estrutura implementada, as etapas necessárias podem ser realizadas para abordar o incidente em mãos.

Nº 8 Criar uma política, não um plano

Lembre-se sempre de que o "P" em CSIRP significa "Plano" e não "Política". Ocasionalmente, a ERS revisa um CSIRP que é lido mais como uma política que um plano. Qual é a diferença? Um plano contém etapas e funções acionáveis, ao passo que uma política declara as diretrizes abrangentes a serem aplicadas na organização. Quando ocorre um incidente, você realmente quer ler uma política de empresa para formular um plano? É claro que não. Você gostaria de um plano bem pensado que te diga o que fazer.

Nº 9 Não atribuir um proprietário

Seu CSIRP pode ter muito em comum com seu gato. Os dois se desenvolvem com o tempo, exigem manutenção e atenção e devem ter proprietários responsáveis pelo seu bem-estar. Ocasionalmente, quando ocorre um incidente, os CSIRPs são obtidos das profundidades da rede, apenas para descobrir que o documento foi atualizado pela última vez quando o Vista era um sistema legal. Um a um, descobre-se que os números de telefone dos principais funcionários estão desconectados. Até mesmo a sala de conferência desenvolvida originalmente como uma sala de operações foi reconfigurada para o centro de supervisão da empresa. Não foi atribuído nenhum proprietário ao documento e, sem um responsável, o documento ficou desatualizado e teve seu valor diminuído.

Ao estabelecer um CSIRP, atribua um proprietário ao documento. Ele é responsável por atualizar o documento, assegurando que os procedimentos que ele contém ainda sejam relevantes e coordenando o teste anual. Sem um proprietário específico, o documento pode enfraquecer, ficar estagnado e causar um maior tempo de resposta aos incidentes.

Nº 10 Negligenciar a revisão após as ações

As lições mais valiosas de qualquer incidente podem ser aprendidas com a revisão após as ações. Até mesmo se parecer que tudo ocorreu conforme o planejado durante um incidente, é provável que uma revisão após as ações possa trazer possíveis melhorias à situação. Não há vergonha em apontar os erros ou problemas que precisam ser melhorados; quaisquer erros ou problemas podem fortalecer o CSIRP e são mais capazes de abordar suas necessidades durante os incidentes futuros.

Na conclusão de um incidente, os principais responsáveis devem se reunir e discutir a qualidade do desempenho do CSIRP. Infelizmente, na pressa para esquecer as dores de cabeça das semanas passadas, a revisão após as ações muitas vezes é uma etapa valiosa negligenciada no processo do CSIRP.

Resposta aos incidentes – preparando sua infraestrutura para respostas em escala

A resposta aos incidentes (IR) não é algo que a maioria dos funcionários de segurança pensa em suas tarefas diárias. Em vez disso, são pensadas as posições defensivas e ofensivas, o gerenciamento de identidade, a revisão de códigos e outras operações rotineiras. Mas o que acontece quando estes mecanismos falham de verdade? Como uma organização de recupera de uma invasão, um ataque de vírus ou um vazamento de dados sensíveis? A resposta aos incidentes deve ser um processo planejado, bem estabelecido com antecedência de sua necessidade, a fim de evitar rápidas decisões com pouca consideração sobre as repercussões. Em sua forma mais simples, o planejamento de IR envolve mais identificar os especialistas em resolução de problemas de sua organização que seriam melhores em identificar e erradicar sérios problemas de segurança. Estes indivíduos não precisam ser respondentes de incidentes dedicados, mas estariam disponíveis para envolvimento imediato. Neste tipo de cenário, geralmente a resposta aos incidentes não é sistemática. Os profissionais tendem a jogar um jogo, atingindo as infecções individuais com escaneamentos locais e resolvendo mais problemas com sneakernets e um CD de boot em vez de exercer um monitoramento disseminado e procedimentos de limpeza em massa.

Tudo o que a resposta aos grandes incidentes realmente exige é a capacidade de armazenar todas as coisas e dar a elas um sentido coerente.

Para as pequenas organizações, isso pode ser suficiente. Essa não é uma má abordagem, mas ela não realiza o escalamento para além de uma pequena quantidade de máquinas. Geralmente, as etapas que excedem isso exigem um investimento real em infraestrutura, configurando a equipe de resposta aos incidentes com ferramentas para capturar e analisar os dados da empresa. Com todas as plataformas de registro e análise e os dispositivos disponíveis atualmente, é fácil imaginar que a resposta escalável aos incidentes fica apenas a um dispositivo de distância.

A resposta aos incidentes não é fácil e exige a capacidade de armazenar todas as coisas e dar um sentido coerente a elas. Infelizmente, até mesmo esta abordagem pode falhar ao realizar um escalamento para além de umas duas máquinas. Assim que um incidente abrange mais de algumas dúzias de máquinas, os modelos mais simplistas de resposta aos incidentes exigem uma quantidade irregular de força para serem funcionais. Embora o truísmo "se a força bruta não está funcionando, isso significa que você não está usando força suficiente" possa ser aplicado, a maioria dos processos resultantes dela é cara e incômoda. Digamos, por exemplo, que seu plano de resposta aos incidentes dite que um sistema infectado com um vírus que rouba informações deve ser desativado e desenhado. Com qual qualidade (e rapidez) isso funciona para 50 máquinas? Para 1500? Como se determina quais máquinas estão infectadas quando faltam horas ou dias para o vírus ser detectado por sua solução antivírus? Este artigo tentará discutir algumas etapas básicas que achamos mais úteis para a preparação para lidar com esses tipos de cenários de uma maneira que realize um escalamento financeiro e temporário.

Preparação: A base sólida de todas as respostas aos incidentes

Embora o acrônimo específico varie, os destaques da doutrina tradicional de resposta aos incidentes sempre começa com "P", que representa "preparação". A resposta aos incidentes em escala envolve muito mais preparação que os ambientes menores, mas quando preparada devidamente, a iniciativa necessárias às etapas posteriores pode ser substancialmente similar. Felizmente, muitas (se não todas) etapas envolvidas na preparação para uma boa resposta aos incidentes são simplesmente boas práticas de infraestrutura em geral e, deste modo, já são componentes necessários de um ambiente bem gerenciado. De fato, boa parte da administração de sistemas pode ser considerada uma resposta aos incidentes de "menor nível". A autenticação centralizada, o gerenciamento de correções, o gerenciamento de inventário, o registro, o controle de acesso e a automação são componentes básicos da execução de uma infraestrutura computacional bem-sucedida e cada um deles tem implicações específicas sobre a resposta aos incidentes. Discutir todos eles está além do escopo deste artigo, mas dois deles em particular são incrivelmente importantes para escalar a resposta aos incidentes: registro e automação. Eles são dois principais fatores de sucesso nos quais os clientes falham periodicamente.

Não registrar causa mais danos

Uma das primeiras coisas que um respondente de incidentes experiente perguntará é "Onde estão seus logs?". Quando o respondente encontrar uma situação na qual a resposta for menos que desejável, ele fará o possível para ajudar, mas com o conhecimento de que suas chances de identificar com êxito o problema em mãos e disponibilizar a causa estão diminuindo rapidamente. Ele aprendeu que o sucesso da resposta aos incidentes não é a perfeição inatingível, mas um encerramento suficiente. O cliente pode ser prejudicado de forma a não poder identificar os indivíduos envolvidos em uma violação de dados muito mais do que ter permanecido "no sistema" durante um longo período, elevando a exposição a dúzias de milhões de registros.

O registro fornece ao respondente de incidentes e ao administrador do sistema a tração de conhecimentos fundamental para determinar o que aconteceu na infraestrutura em determinado momento, passado ou presente. Infelizmente, assim como no resto de um ambiente de segurança bem executado, o registro disseminado também tende a ser uma das primeiras áreas destacadas na infraestrutura contemporânea, já que ele consome preciosos recursos de sistemas, redes e financeiros para algo que é apenas necessário ocasionalmente. Os principais segredos para um registro bem-sucedido são a filtração e a centralização. É um ambiente atipicamente bem planejado que pode oferecer suporte ao registro completo de cada operação específica. Muitas vezes, os respondentes de incidentes devem trabalhar com os administradores de sistema para determinar a configuração mínima de registro necessária para fornecer respostas razoáveis, ao mesmo tempo em que evita o consumo de excessivo de recursos. O segredo é atingir um equilíbrio entre a retenção e o custo/desempenho. Para servir de exemplo, raramente é necessário (mas totalmente possível) registrar cada acesso a objetos de um sistema Windows, mas não registrar o uso privilegiado pode causar implicações críticas sobre a resposta e a administração. Imagine que em um domínio bem configurado, um administrador de domínios (que usa devidamente credenciais pessoais de poucos privilégios) eleva brevemente o seu privilégio para alterar uma configuração de DNS e acaba por quebrá-lo, acidentalmente. Nesta situação, os administradores podem ver rapidamente o que aconteceu, quem o fez e o que corrigir. Agora, imagine que a credencial de poucos privilégios não era realmente a do usuário, mas a de um invasor que comprometeu essas credenciais.

Assim que os logs são coletados, eles precisam ser armazenados e existem alguns lugares piores para seu armazenamento que o sistema que os gera. Os logs consomem um espaço em disco valioso, podem ser perdidos em uma falha do sistema ou até mesmo ser modificados por um invasor em caso de uma invasão. O armazenamento centralizado pode ajudar a mitigar ou, no mínimo, descarregar estes problemas a um sistema separado. A transferência de logs a um sistema central pode adquirir várias formas dependendo das necessidades da organização e de um cálculo dos riscos do que constitui uma perda de dados aceitável. Da perspectiva do respondente a incidentes, uma disposição ideal seria um fornecimento em tempo real com garantias de ponta a ponta por meio de um mecanismo como o Reliable Event Logging Protocol (RELP), que elimina efetivamente a janela de um invasor para alterar os logs. O RELP pode fornecer um registro confiável de eventos em toda a rede. Novamente, o segredo é o equilíbrio e não permitir que o melhor seja inimigo do bom. É mais valioso tem um sistema de coleção de logs insuficiente que pesquisa logs nos lotes dos sistemas do que não ter sistema nenhum.

Um princípio básico para determinar a frequência da pesquisa de logs é decidir por quanto uma janela seria aceitável para que um invasor consiga modificar logs e, depois, dividi-los em dois. Algumas organizações evitam o armazenamento central de logs porque ele parece caro, citando os custos de disco SAN rápido e os preços de hardware de servidor de aplicativos. O registro central não precisa ser tão caro. Além de serem autônomos e administrados separadamente do resto do ambiente (sem credenciais compartilhadas ou confiáveis) e a menos que a análise de logs esteja sendo realizada no sistema, os requisitos de hardware e disponibilidade não devem ser maiores que os de um servidor de arquivos típico.

A automação é sempre sua melhor amiga

A automação na administração de sistemas e na resposta aos incidentes é a diferença entre o beisebol de liga principal e o softball de sábado. É ela que permite que algumas organizações operem em uma proporção de servidor para administrador de mais de 1.000:1 e que os respondentes de incidentes lidem de modo cirúrgico com milhares de máquinas comprometidas de uma só vez. Felizmente, para a resposta aos incidentes, geralmente, a automação é, no mínimo, parcialmente integrada nos ambientes que compreendem mais que algumas máquinas, já que um administrador geralmente não escolherá instalar correções em mais de dois sistemas sem algum tipo de ferramenta de gerenciamento de correções para controlar o processo. Além disso, muitos ambientes têm "agentes" instalados para fornecer segurança de terminais, gerenciamento de ativos, gerenciamento de antivírus e uma variedade de outras funções administrativas rotineiras necessárias. Muitas vezes, a maior dificuldade enfrentada por um respondente de incidentes em relação a essas ferramentas é saber qual delas está disponível e como usá-las. Quaisquer ferramentas de automação podem ser usadas para fornecer ao respondente de incidentes consultas customizadas valiosas dos vários estados do sistema, mas devem ser selecionadas cuidadosamente de acordo com o seu período refratário e com sua capacidade de modificar um sistema.

Por exemplo, suponha que sua equipe de resposta aos incidentes identificou um novo vírus que ainda não é detectado pela solução antivírus, mas que é conhecido por criar arquivos que correspondem à determinada expressão regular de determinado conjunto de diretórios. As equipes de infraestrutura têm gerenciamento de correções, gerenciamento de ativos e ferramentas antivírus executadas em todos os sistemas possivelmente infectados. Uma solução pode ser fornecer um arquivo de lote que busque os arquivos indicadores dos sistemas por meio da ferramenta de correções e que os reporte por meio do upload de um arquivo de resultados em um servidor central. Em algumas situações, esta pode ser a única abordagem, mas ela modifica os sistemas possivelmente afetados e tende a deixar o processo de resposta mais aberto para interferências de uma parte maliciosa. No entanto, se a ferramenta de gerenciamento de ativos pode reportar os arquivos que correspondem a um padrão específico, ela pode ser preferível, já que não pode modificar o sistema final e pode parecer uma atividade normal a uma parte maliciosa. A eliminação de uma infecção pode ser feita pelo gerenciamento de correções ou pelos sistemas antivírus, dependendo da situação específica. O segredo é, primeiramente, estar ciente de quais ferramentas/recursos já estão disponíveis para o ambiente (ou trabalhar com as equipes de infraestrutura para implementar ferramentas mutuamente benéficas) e, depois, escolher a ferramenta certa para a tarefa.

Por último e, certamente, não menos importante que modo de automação é o scripting. Embora as ferramentas de automação muitas vezes tenham suas próprias linguagens de scripting que podem ser colocadas em bom uso, pouca coisa é mais efetiva e eficiente no processo de resposta aos incidentes que os respondentes de incidentes que podem escrever scripts em uma linguagem genérica como Python ou Perl para controlar as ferramentas de automação e preencher as lacunas que as ferramentas podem apresentar. Ter um programador experiente de administração de sistemas na equipe de resposta aos incidentes ou disponível imediatamente pode ser um ativo inestimável para a velocidade e completude das respostas.

Finalmente e mais importante: A autenticação

Um terceiro segredo crítico e, de certa forma, esquecido da resposta aos incidentes é a autenticação. É possível observar que muitos aspectos anteriores são (ou devem ser) caracterizados como tendo uma autenticação forte e centralizada. Sem a autenticação central, geralmente, o administrador e o respondente não têm como consultar os sistemas, aplicar correções ou lidar com os sistemas de modo eficiente sem recorrer às táticas brutais como reunir e armazenar as senhas por máquina. Alguns ambientes consideravelmente grandes se dão bem sem a autenticação centralizada e, em vez disso, contam com agentes remotos que executam scripts periodicamente sob privilégios administrativos, mas o tempo de resposta deste tipo de configuração pode impedir uma boa administração e a resposta aos incidentes e deve ser evitado com toda a diligência.

Trabalhe de modo mais inteligente e faça bons amigos

As boas práticas de infraestrutura devem ser traduzidas diretamente em uma boa resposta aos incidentes. As ferramentas e procedimentos necessários para aproveitar o desenvolvimento de uma infraestrutura computacional mais tolerante a falhas, reproduzível e escalável são as mesmas ferramentas e procedimentos que devem ser aproveitados para responder aos incidentes de modo estável e rápido. Cultive bons relacionamentos com as equipes de administração de sistemas e saiba quais ferramentas elas já implementaram, a fim de se certificar de que entende e sabe como operá-las. Desta maneira, a equipe de resposta aos incidentes pode oferecer suporte a elas quando necessário.

Segurança e privacidade de dados: entendendo as diferenças para ajudar a realizar a conformidade

As empresas dependem dos dados para oferecer suporte às operações diárias de negócios; portanto, é essencial assegurar a privacidade e proteger os dados, independentemente de onde eles residam. De acordo com o Relatório de Investigação de Violações de Dados da Verizon, os servidores de banco de dados são a principal fonte de dados violados, representando 92% dos registros comprometidos. Infelizmente, há uma grande disparidade no tempo necessário para que os invasores penetrem os bancos de dados em comparação ao tempo necessário para reconhecer uma violação e corrigi-la. Os invasores levam dias para penetrar nas defesas, mas, muitas vezes, as organizações levam semanas ou meses para descobrir como, onde e quando elas foram comprometidas e, depois, semanas ou meses para corrigir o problema.

A segurança e a privacidade de dados ficam ainda mais complexas por causa dos diferentes tipos de informações que têm requisitos diferentes de proteção e privacidade; portanto, as organizações devem adotar uma abordagem holística para proteger suas informações. Isso inclui:

- **Descoberta e classificação de dados –** As organizações precisam entender onde os dados estão na empresa e como eles são relacionados. Isso permite que elas classifiquem os dados sensíveis de modo adequado para obter o tratamento devido ao longo de todo o seu ciclo de vida.
- **Redação de dados –** Os dados sensíveis também residem nos documentos, formulários e imagens escaneadas. Proteger estes dados não estruturados exige que as políticas de privacidade redijam (removam) as informações sensíveis, ao mesmo tempo em que ainda permitem que os dados de negócios necessários sejam compartilhados. Estes documentos não estruturados podem ser anexos ao banco de dados.
- **Criptografia de dados –** Os bancos de dados de criptografia podem ser necessários por muitos mandatos regulamentares. As organizações precisam de uma solução única que seja escalada para ajudar a proteger os tipos dedados heterogêneos. Este pode ser um bom complemento ao monitoramento de atividades de bancos de dados, já que as organizações podem criar uma defesa em uma abordagem detalhada.
- **Mascaramento de dados estáticos –** Existe um grande foco nos ambientes de produção, mas a segurança dos ambientes não relacionados à produção não deve ser negligenciada. Desidentificar os dados sensíveis em bancos de dados não relacionados à produção, mas, ao mesmo tempo, manter a usabilidade do desenvolvimento, teste, processos de treinamento e trabalhos de QA de aplicativos não apenas ajuda a facilitar os processos de negócios, como também assegura o princípio de menos privilégios. As pessoas sem um negócio válido precisam saber que não devem ter acesso aos dados sensíveis.
- **Monitoramento –** Proteger e monitorar de modo contínuo o acesso aos bancos de dados, warehouses e compartilhamentos de arquivos oferece insights de quem, quê, quando e como as transações ajudam as organizações validar a integridade de dados.
- **Avaliações de vulnerabilidade –** Reforce os bancos de dados para ajudar a mitigar os riscos, como riscos de más configurações ou configurações-padrão.

Dando sentido à confusão: Por que há um crescente foco na proteção de dados?

De acordo com o relatório independente da Forrester Research de fevereiro de 2011, Forrsights: The Evolution of IT Security, 2010 To 2011, a segurança de TI permanece um ramo de atividade e crescimento, à medida que as empresas lutam com uma paisagem de ameaças mais capaz e ameaçadora, respondem a um corpo crescente de exigências regulamentares e de terceiros e se adaptam um nível sem precedentes de auge da TI. Boa parte deste foco está posicionado especificamente ao redor de alguns temas principais: novas ameaças de segurança cibernética, como Stuxnet e Aurora; alteração das arquiteturas de TI, como a virtualização de um datacenter e crescentes pressões acerca de mandatos de terceiros.

Nos últimos anos, de acordo com o relatório da Forrester, "a segurança aumentou sua visibilidade de modo estável, atingindo uma atenção e um suporte em relação a conselhos". Por exemplo, a pesquisa da Forrester indica que 54% dos Diretores Executivos de Segurança das Informações (CISOs) corporativos são subordinados a um executivo de nível C e 42% deles são subordinados a pessoas externas ao departamento de TI. Estas porcentagens refletem o aumento da relevância aos negócios que a segurança tem nas organizações de todos os tipos de diversos segmentos de mercado. O número de organizações que veem a segurança como uma prioridade alta ou crítica, agora, está em seu nível mais alto dos anos recentes.

Vamos nos aprofundar nos detalhes dos diversos fatores que estão incentivando o maior foco em segurança e privacidade de dados.

Alterações nos ambientes de TI e iniciativas de negócios em evolução

As políticas de segurança e tecnologias correspondentes devem evoluir à medida que as organizações adotam novas iniciativas de negócios, como terceirização, virtualização, nuvem, mobilidade, Web 2.0 e rede social. Esta evolução significa que as organizações devem pensar de modo mais amplo sobre onde residem os dados sensíveis e como eles são acessados. As organizações também devem considerar uma matriz mais ampla de dados sensíveis, incluindo informações sobre os clientes, segredos comerciais, planos de desenvolvimento e diferenciadores competitivos.

Invasores mais inteligentes e sofisticados

Muitas organizações estão lutando contra a crescente lacuna entre os recursos dos invasores e as defesas de segurança. A natureza em constante mudança, a complexidade e a maior escala de ataques externos são motivo de preocupação para as organizações. De acordo com o mesmo relatório da Forrester mencionado anteriormente, atualmente, os ataques de segurança causam um impacto de negócios mais prejudicial em comparação a dez anos atrás. Antes, a maior preocupação eram os ataques de vírus ou ataques curtos de negação de serviços, que criariam uma pausa temporária nas operações de negócios. Hoje, o roubo de dados dos clientes ou dados corporativos, como os segredos comerciais, pode resultar em bilhões de dólares de negócios perdidos, multas e processos judiciais, e danos irreparáveis à reputação de uma organização.

Mandatos de conformidade

O número e a variedade dos mandatos de conformidade são grandes e afetam as organizações de todo o mundo.

Juntamente com o crescente número de mandatos de conformidade, já a maior pressão para mostrar uma conformidade imediata. As empresas estão sob uma tremenda pressão de tempo e precisam mostrar um progresso imediato para o negócio e acionistas ou enfrentar danos à reputação e rígidas penalidades financeiras.

Explosão de informações

A explosão de informações eletrônicas é alucinante. A IDC estima que, atualmente, existem 45 gigabytes de dados para cada pessoa do planeta ou, no total, impressionantes 281 bilhões de gigabytes. Ao passo que meros 5% de dados terminarão nos servidores de dados corporativos, estima-se que esses dados aumentarão 60% ao ano, resultando em 14 exabytes de dados corporativos a partir de 2011. A explosão de informações disponibilizou o acesso às informações públicas e privadas como parte da vida diária. Geralmente, os aplicativos fundamentais dos negócios coletam essas informações para propósitos legítimos. No entanto, os dados sensíveis estão sujeitos a roubo e má utilização, em virtude da natureza interconectada da Internet e dos sistemas de informações, bem como os aplicativos corporativos de ERP, CRM e aplicativos de negócios customizados.

Ameaças internas

Uma alta porcentagem de violações de dados resulta de pontos fracos internos. Os exemplos variam de funcionários, que podem utilizar incorretamente os números de cartões de pagamento e outras informações sensíveis, a pessoas que salvam dados confidenciais em laptops que são roubados de modo subsequente. As organizações são responsáveis por proteger os dados, independentemente do local onde eles residam – incluindo dados guardados por parceiros de negócios, fornecedores ou outros terceiros.

Em resumo, as organizações estão se concentrando mais nas preocupações de segurança e privacidade de dados. Elas estão olhando para além das soluções pontuais em desenvolvimento para eventos específicos e em direção ao desenvolvimento de políticas de segurança, políticas de privacidade e procedimentos da empresa.

Entendendo a diferença entre segurança e privacidade

A segurança e a privacidade são conceitos distintos, mas relacionados. A segurança é o lockdown em relação à infraestrutura que impede ou concede acesso a determinadas áreas ou dados com base em autorizações. Em oposição, as restrições de privacidade controles o acesso aos usuários que são autorizados a acessar um conjunto de dados em particular. A privacidade de dados aborda as limitações ou restrições sobre as pessoas que têm um propósito de negócios legítimo para visualizar os dados. Geralmente, este propósito de negócios é definido pela função que, por sua vez, pode ser definida pela conformidade.

Alguns exemplos de soluções de segurança de dados são o monitoramento de atividades de bancos de dados e as avaliações de vulnerabilidades dos bancos de dados. Alguns exemplos das soluções de privacidade de dados são a redação e o mascaramento de dados. Em um caso recente que ilustra esta distinção, médicos da UCLA Medical Center foram pegos visualizando os registros médicos da celebridade Britney Spears. As políticas de segurança do hospital eram apreciadas, já que os médicos precisavam de acesso aos registros, mas surgiram preocupações de privacidade já que eles estavam acessando o arquivo por curiosidade e não para um propósito médico válido.

Os perigos são altos: Riscos associados à segurança e privacidade de dados insuficientes

De acordo com a pesquisa Ponemon de 2010, pelo quinto ano consecutivo, os custos de violação de dados continuaram a aumentar. O custo organizacional médio de uma violação de dados em 2010 aumentou para US$ 7,2 milhões, subindo 7% em comparação aos US$ 6,8 milhões de 2009. Os custos totais de violações de 2010 representaram para as empresas uma média de US$ 214 por registro comprometido, um aumento de até US$ 20 (5%) em relação a 2009.

A violação mais cara de 2010 estudada pela Ponemon precisou de US$ 35,3 milhões para ser resolvida, subindo US$ 4,8 milhões (15%) em relação a 2009. A violação de dados mais barata foi de US$ 780.000, uma alta de US$ 30.000 (4%) em relação a 2009. Como nos anos anteriores, os custos de violações de dados parecem ser diretamente proporcionais ao número de registros comprometidos.

Outros possíveis impactos negativos são as multas ou responsabilidades financeiras, a erosão do preço das ações causada pelas preocupações dos investidores e a publicidade negativa resultante de uma violação de dados. Quando uma empresa é identificada como não confiável, isso resulta em danos irreparáveis à marca.

Algumas fontes comuns de riscos são:

- **Privilégios excessivos e abuso de usuários privilegiados.** Quando os usuários (ou aplicativos) recebem privilégios de bancos de dados que excedem os requisitos de sua função, esses privilégios podem ser usados para obter acesso às informações confidenciais.
- **Elevação de privilégios não autorizados.** Os invasores podem aproveitar as vulnerabilidades dos softwares de gerenciamento de bancos de dados para converter os privilégios de acesso de baixo nível em privilégios de acesso de alto nível.
- **Injeção de SQL.** Os ataques de injeção de SQL envolvem um usuário que se aproveita das vulnerabilidades dos aplicativos de front-end da web e dos procedimentos armazenados, a fim de enviar consultas não autorizadas de bancos de dados, muitas vezes com privilégios elevados. Usando a injeção de SQL, os invasores podem até mesmo obter acesso irrestrito a todo um banco de dados.
- **Negação de serviços.** A negação de serviços (DoS) pode ser acionada por meio de várias técnicas. As técnicas comuns de DoS são estouros de buffer, corrupção de dados, sobrecarga de redes e consumo de recursos. Este último é único ao ambiente de bancos de dados e frequentemente é negligenciado.
- **Exposição dos dados de backup.** Alguns ataques recentes de alto perfil envolveram roubo de fitas e discos rígidos de backup de bancos de dados que não eram criptografados.

Aproveitando uma abordagem holística de segurança e privacidade de dados

As organizações devem adotar uma abordagem holística de proteção de dados. Esta abordagem deve proteger diversos tipos de dados de locais diferentes de toda a empresa, incluindo a proteção dos dados estruturados e não estruturados dos ambientes de produção e não relacionados a ela (desenvolvimento, teste e treinamento). Uma abordagem desse tipo pode ajudar a focar os recursos limitados sem processos adicionais ou maior complexidade. Uma abordagem holística também ajuda as organizações a demonstrar a conformidade sem interromper os processos de negócios fundamentais ou as operações diárias.

Para começar, as organizações devem considerar quatro perguntas principais, que são desenvolvidas para ajudar a focar a atenção sobre as vulnerabilidades dos dados mais críticos:

1. Onde os dados sensíveis residem na empresa?
2. Como o acesso aos bancos de dados de sua empresa pode ser protegido, monitorado e auditado? Como os dados podem ser protegidos contra acesso autorizado e não autorizado?
3. Os dados confidenciais dos documentos podem ser protegidos ao mesmo tempo em que permitem que os dados de negócios necessários sejam compartilhados?
4. Os dados de seus ambientes não relacionados à produção podem ser protegidos e, ao mesmo tempo, utilizáveis para treinamento, desenvolvimento de aplicativos e testes?

As respostas a essas perguntas fornecem a base para uma abordagem holística de proteção de dados. Elas ajudam as organizações a se concentrar nas principais áreas que podem estar negligenciando com as abordagens atuais.

1. As organizações não podem proteger os dados se não souberem que eles existem. Os dados sensíveis residem em formatos estruturados e não estruturados dos ambientes de produção ou não relacionados a ela. As organizações precisam documentar e definir todos os ativos e relacionamentos de dados, independentemente de sua fonte. É importante classificar os dados corporativos, entender os relacionamentos de dados e definir os níveis de serviço. O processo de descoberta de dados analisa os valores e padrões para identificar os relacionamentos que relacionam elementos de dados diferentes em unidades lógicas de informações ou “objetos de negócios” como clientes, pacientes ou faturas.

2. O Monitoramento de Atividades de Bancos de Dados fornece monitoramento de acesso privilegiado e não privilegiado a usuários e aplicativos, que é independente do registro de banco de dados nativo e das funções de auditoria. Ele pode funcionar como um controle compensador para os problemas de separação de obrigações de usuários privilegiados, por meio do monitoramento de atividades do administrador. A tecnologia também pode melhorar a segurança de bancos de dados detectando as atividades incomuns de leitura e atualização de banco de dados a partir da camada de aplicativos. A agregação, a correção e os relatórios de eventos de bancos de dados fornecem um recurso de auditoria de bancos de dados sem a necessidade de ativar as unções de auditoria de banco de dados nativo, que também fazem parte do monitoramento de atividades de bancos de dados. As soluções de monitoramento de atividades de bancos de dados devem conseguir detectar as atividades maliciosas ou o acesso inadequado ou não aprovado do administrador de bancos de dados (DBA).

3. A redação de dados pode remover os dados sensíveis dos formulários e documentos com base na função ou do propósito de negócios. Por exemplo, os médicos precisam visualizar informações sensíveis, como dados de sintomas e prognósticos, sempre que um funcionário de faturamento precisar do número de seguro e endereço de cobrança do paciente. O desafio é fornecer a proteção adequada e, ao mesmo tempo, atender as necessidades de negócios e gerenciar os dados conforme necessário. As soluções de redação de dados devem proteger as informações sensíveis dos documentos, formulários e gráficos não estruturados.

4. Desidentificar dados dos ambientes não relacionados à produção é o processo de remover, mascarar ou transformar de modo sistemático os elementos de dados que podem ser usados para identificar um indivíduo. A desidentificação de dados permite que os desenvolvedores, testadores e instrutores usem dados realistas e produzam resultados válidos, ao mesmo tempo em que cumprem as regras de proteção de privacidade. Os dados que foram limpos dessa maneira são geralmente considerados aceitáveis para uso em ambientes não relacionados à produção e ajudam a assegurar que até mesmo os dados roubados, expostos ou perdidos não tenham uso possível para qualquer pessoa.

Uma abordagem de três camadas para assegurar a proteção de dados holística

Entender e definir

As organizações devem descobrir onde residem os dados sensíveis, classificar e definir os tipos de dados e determinar as métricas e políticas para assegurar a proteção com o passar do tempo. Os dados podem ser distribuídos em diversos aplicativos, bancos de dados e plataformas com pouca documentação. Muitas organizações dependem muito de especialistas em sistemas e aplicativos para essas informações. Às vezes, as informações são integradas em lógica de aplicativos e podem ser aplicados relacionamentos ocultos por trás dos bastidores.

Encontrar dados sensíveis e descobrir relacionamentos de dados exigem uma análise cuidadosa. As origens e relacionamentos de dados devem ser claramente entendidos e documentados para que nenhum dado sensível fique vulnerável. Somente depois de entender toda a paisagem, as organizações podem definir políticas adequadas de segurança e privacidade de dados corporativos.

Proteger

As soluções de segurança e privacidade de dados devem abranger uma empresa heterogênea e proteger os dados estruturados e não estruturados dos ambientes de produção e não relacionados a ela. Elas devem ajudar a proteger os valores de dados sensíveis do banco de dados, em aplicativos de ERP/CRM e em ambientes estruturados como formulários e documentos. As principais tecnologias incluem o monitoramento de atividades de bancos de dados, o mascaramento de dados, a redação de dados e a criptografia de dados. Uma abordagem holística de proteção de dados ajuda a assegurar um lockdown de todos os dados organizacionais.

Dados estruturados: Estes dados são baseados em um modelo de dados e estão disponíveis em formatos estruturados como bancos de dados ou XML.

Dados não estruturados: Estes dados estão em formulários ou documentos que podem ser escritos à mão ou digitados, como documentos de processamento de texto, mensagens de email, fotografias, áudio digital e vídeo.

Dados online: Estes dados são usados diariamente para oferecer suporte ao negócio, como metadados, dados de configuração ou arquivos de log.

Dados offline: Estes dados estão em fitas de backup ou dispositivos de armazenamento.

Monitorar e auditar

Depois que os dados foram localizados e depois de seu lockdown, as organizações podem precisar comprovar a conformidade, estar preparadas para responder aos novos riscos externos e internos e monitorar os sistemas de modo contínuo. O monitoramento das atividades de usuários, criação de objetos, configuração de bancos de dados e autorizações ajudam os profissionais e auditores de TI a rastrear os usuários entre aplicativos e bancos de dados. Estas equipes podem configurar políticas ajustadas para comportamentos adequados e receber alertas caso elas sejam violadas. As organizações devem mostrar rapidamente a conformidade e possibilitar que os auditores verifiquem o status da conformidade. Os relatórios e aprovações de auditoria devem ajudar a facilitar o processo de conformidade, ao mesmo tempo em que mantêm os custos baixos e minimizam as interrupções técnicas e de negócios. Em resumo, as organizações devem criar trilhas de auditoria contínuas e ajustadas de todas as atividades de bancos de dados, incluindo "quem, o que, quando, onde e como" de cada transação.

Conclusão

Proteger a segurança e privacidade de dados é uma responsabilidade detalhada e contínua que deve fazer parte de todas as melhores práticas. As organizações devem considerar a segurança de dados e sua abordagem de privacidade fornecida por meio da estratégia de três camadas de Entender e Definir, Proteger e Monitorar e Auditar.

Seção III
Práticas de Segurança de Desenvolvimento de Software

Na seção de Práticas de Segurança de Desenvolvimento de Software deste relatório, são apresentados os processos e técnicas para abordar a segurança durante o desenvolvimento de software. Discutimos como as empresas podem encontrar as vulnerabilidades existentes e ajudar a impedir que novas vulnerabilidades sejam introduzidas. Caso os aplicativos da web ou em rede sejam usados para coletar ou trocar dados sensíveis, sua tarefa como um profissional de segurança é mais difícil agora do que nunca. São analisados os testes estáticos e dinâmicos de segurança realizados pelo grupo IBM AppScan em todos os estágios do desenvolvimento de aplicativos e são compartilhados os insights sobre as descobertas.

Conclusões das avaliações de aplicativos da web reais

Metodologia

O serviço IBM AppScan OnDemand é uma oferta baseada em nuvem que ajuda os clientes a identificarem e corrigirem as vulnerabilidades de aplicativos da web sem a necessidade de comprar e manter softwares ou contratar funcionários de segurança de aplicativos altamente qualificados e especializados. Os IBM Application Security Analysts usam o software IBM AppScan Enterprise Edition para analisar os aplicativos em relação às vulnerabilidades de segurança que, se não forem resolvidas, podem resultar em violações e possível perda de dados, como registros de clientes ou funcionários ou propriedades intelectuais corporativas. O software IBM AppScan Enterprise Edition testa as vulnerabilidades comuns dos aplicativos da web, incluindo scripting entre sites, estouro de buffer e escaneamentos de exposições de Web 2.0 e aplicativos flash/flex. Além disso, a oferta inclui a capacidade de escanear e detectar malwares integrados em propriedades da web, fornecendo proteção adicional contra ataques cibernéticos.

A IBM reuniu dados reais de vulnerabilidade de 237 testes de Segurança realizados em 2011, ao mesmo tempo em que realizou Avaliações de Segurança usando o IBM AppScan. Estas avaliações combinam os resultados das avaliações de segurança de aplicativos obtidos do IBM AppScan com teste e verificação manual da segurança. Em todos os casos, os falsos positivos foram removidos dos resultados e as vulnerabilidades foram mapeadas às dez principais categorias de OWASP (Open Web Application Security Project):

1. 1Injeção
2. Scripting Entre Sites (XSS)
3. Gerenciamento de Sessões e Autenticações Quebradas
4. Referências Inseguras de Objetos Diretos
5. Falsificação de Solicitações Entre Sites (CSRF)
6. Má Configuração de Segurança
7. Armazenamento Criptográfico Inseguro
8. Falha ao Restringir o Acesso à URL
9. Proteção de Camada de Transporte Insuficiente
10. Redirecionamentos e Encaminhamentos Não Validados

Para cada uma dessas categorias, foram calculadas duas métricas principais:

1. A chance percentual de encontrar no mínimo uma dessas vulnerabilidades na categoria
2. O número médio de vulnerabilidades com probabilidade de serem encontradas na categoria

Tendo já reunido dados similares desde 2007, a equipe também conseguiu fazer a tendência de resultados dos últimos cinco anos. Estes dados históricos também foram mapeados às dez principais categorias de OWASP de 2010 para rastrear esta tendência.

Pontos métricos

A equipe também analisou as métricas adicionais para ajudar a obter uma análise mais detalhada dos dados. Isso incluía:

Segmentos de Negócios para atribuir dados de teste a um dos seguintes:

- Finanças
- Indústria
- Tecnologia da Informação
- Logística
- Governo
- Outros

Ciclo de Teste de Segurança de Aplicativos, que representa o tipo de teste no qual o aplicativo estava envolvido:

- **Avaliação Única –** Aplicativos testados pela primeira vez
- **Avaliação Trimestral –** Aplicativos testados de modo contínuo e regular
- **Novo Teste –** Teste de acompanhamento para confirmar o encerramento das descobertas, geralmente a partir de uma avaliação única.

Observação: As informações somente foram categorizadas nesses grupos métricos nos quais o tamanho da amostra permitia dados adequados. Quando o tamanho da amostra foi considerado muito pequeno, os valores métricos foram ignorados. Portanto, nem todos os segmentos de negócios ou tecnologias são representados.

Tendências de vulnerabilidades dos aplicativos em 2011

O gráfico a seguir destaca a chance percentual de encontrar uma vulnerabilidade que corresponda a cada uma das dez principais categorias de OWASP em um teste de segurança de aplicativos.

O mapeamento das dez principais categorias de OWASP foi escolhido, já que permite uma avaliação mais focada e comparações com as melhores práticas do segmento de mercado. Quando as descobertas não foram mapeadas diretamente ao OWASP, elas foram capturadas em relação à categoria de má configuração de segurança e, portanto, os seus números são naturalmente superiores.

Vale a pena observar que estas avaliações são de organizações que parecem determinadas a mitigar os problemas de seus aplicativos. Elas podem já ter programas de segurança implementados ou podem ter tido violações no passado. Assim, esses dados não representam o estado dos aplicativos da web em geral ou dos aplicativos que nunca foram examinados. Existe uma tendência decrescente notável nos valores de algumas vulnerabilidades e, provavelmente, isso destaca o retorno sobre seus investimentos mais do que qualquer outra coisa.

Os problemas de Autenticação Quebrada e problemas relacionados com controle de são encontrados em quase oito de cada 10 testes. Muitos aplicativos testados falharam ao restringir a falsificação de sessões e foram expostos aos ataques ao estilo de fixação de sessões. Os problemas relacionados à finalização e reuso de sessões também contribuíram para esta alta estatística.

A Falsificação de Solicitações Entre Sites (CSRF) de 2011 foi encontrada em 28% dos testes realizados, mas este número foi reduzido em relação a 2010, quando a porcentagem era de 59%. Uma parte dessa redução parece ser devida ao maior reconhecimento deste tipo de vulnerabilidade e também às melhorias dos métodos usados para incluir tokens de CRSF.

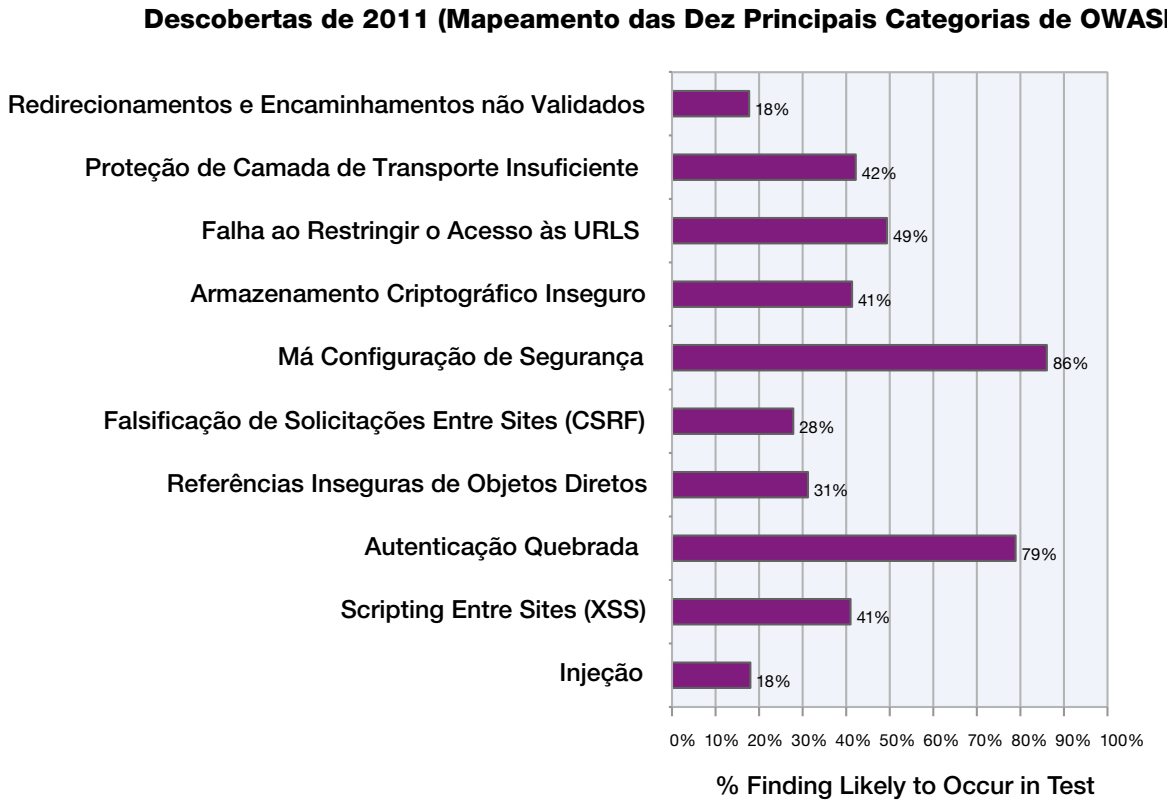


Figura 50: Descobertas de 2011 (Mapeamento das Dez Principais Categorias de OWASP)

Tendências anuais (2007 – 2011)

Desde que começamos a registrar as estatísticas de segurança de aplicativos em 2007, houve uma redução estável nas ocorrências de vulnerabilidades relacionadas ao controle de entradas, como scripting entre sites (XSS) e injeção de SQL. Em 2011, nossas estatísticas sugerem que a probabilidade de encontrar XSS em determinado teste continua a cair, mas mostram sinais de nivelamento com uma chance percentual de ocorrer de, aproximadamente, 40%. As vulnerabilidades de injeção e, especificamente, a injeção de SQL, parecem ter se nivelado com uma chance percentual de ocorrer de cerca de 20%.

Embora isso não esteja claro a partir das estatísticas, nossos testes encontraram que os aplicativos que usam as melhores práticas e protegem as práticas de codificação para filtrar as entradas inválidas tinham de pouca a nenhuma ocorrência de problemas relacionados às entradas, como XSS. O fato de que o XSS ainda é encontrado em mais de 40% dos aplicativos testados destaca que ainda há muitos aplicativos que não aderiram às práticas seguras de codificação. Não há dúvidas de que as coisas estão melhorando, mas isso não é motivo para ter calma. A probabilidade de 40% para vulnerabilidades de XSS ainda é alta, principalmente para algo que é tão facilmente entendido, tão facilmente demonstrado e tão facilmente corrigido. As vulnerabilidades dos aplicativos da web permanecem sendo o segredo para muitas violações de dados, que continuam a aumentar no primeiro semestre de 2011. Sendo assim, a X-Force declarou que 2011 foi o "Ano da Violação de Segurança".

Outro ponto de dados importante capturado é "o número médio de determinada descoberta por teste de segurança". O que se vê é uma redução de ocorrências do XSS quando esta vulnerabilidade é encontrada. Em 2009, o número médio era de 40, ao passo que em 2011, o número é um pouco superior a três. Agora, existe muito menos probabilidade de encontrar um aplicativo com absolutamente nenhum controle de entrada implementado. A maioria dos aplicativos nos quais o XSS foi encontrado agora parece vir de alguma forma de controle de entradas, mas houve vetores de ataques especializados que conseguiram contornar esses filtros/controles.

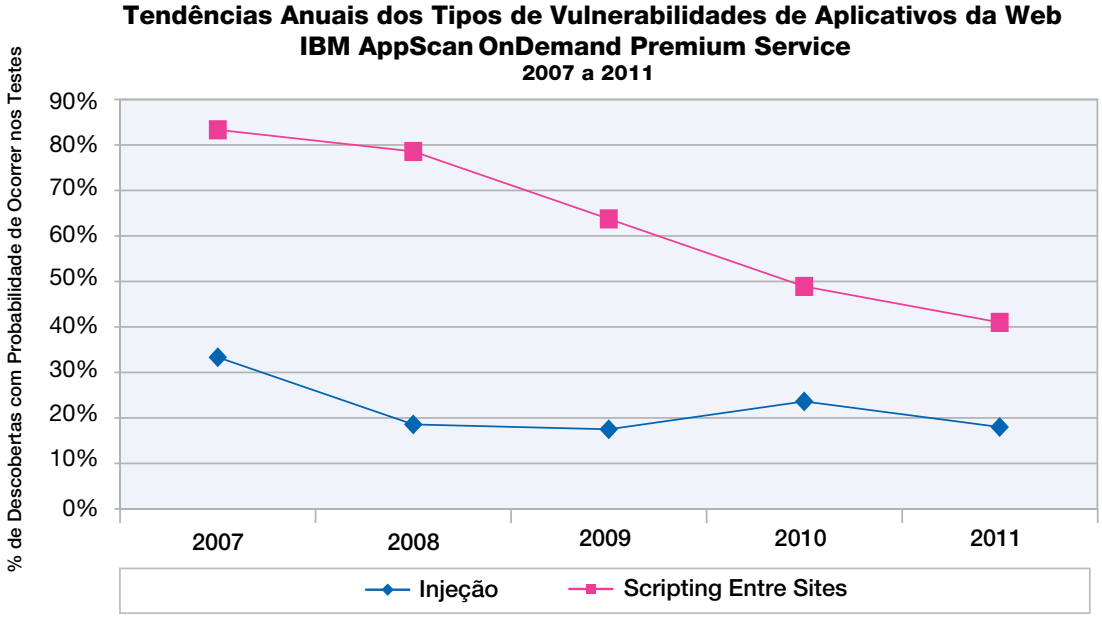


Figura 51: Tendências Anuais dos Tipos de Vulnerabilidades de Aplicativos da Web/ IBM AppScan OnDemand Premium Service/2007 a 2011

TENDÊNCIAS ANUAIS										
Tipo de Vulnerabilidade	**2007**		**2008**		**2009**		**2010**		**2011**	
	Vulnerabilidade média por teste	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**
Injeção	1,3	33%	5,3	19%	1,7	18%	2,3	24%	2,1	18%
Scripting Entre Sites (XSS)	12,7	83%	17,9	79%	40,8	64%	5,8	49%	3,3	41%
Autenticação Quebrada	11,2	83%	4,8	84%	3,2	65%	2,5	53%	9,7	79%
Referências Inseguras de Objetos Diretos	2,6	50%	3,2	54%	3,0	51%	1,9	33%	1,6	31%
Falsificação de Solicitações Entre Sites (CSRF)	1,9	22%	1,8	20%	7,9	59%	3,8	53%	2,0	28%
Má Configuração de Segurança	46,9	83%	22,6	74%	23,5	68%	15,3	56%	10,7	86%
Armazenamento Criptográfico Inseguro	21,7	38%	17,9	56%	29,1	38%	19,8	45%	11,9	41%
Falha ao Restringir o Acesso às URLs	7,2	13%	6,0	19%	9,7	13%	6,6	15%	5,0	49%
Camada de Transporte Insuficiente	7,3	28%	2,4	17%	2,5	35%	1,6	22%	9,8	42%
Redirecionamentos e Encaminhamentos Não Validados	1,7	7%	0,5	5%	0,1	3%	0,4	4%	0,3	18%

Tabela 8: Tendências Anuais dos Tipos de Vulnerabilidade de Aplicativos da Web, 2007 a 2011, IBM Rational IBM AppScan OnDemand Premium Service

Segmentos de negócios

Como foi feito em 2010, dividimos nossas estatísticas de 2011 por segmentos de negócios. Conseguimos dividir os dados em cinco segmentos, quando isso era permitido pelo número de pontos de dados.

Em 2011, os aplicativos financeiros foram novamente o segmento com melhor desempenho. O gráfico a seguir mostra como cada um dos cinco segmentos podia ser comparado em relação às vulnerabilidades de XSS, injeção e CSRF. Os aplicativos governamentais tiveram o pior desempenho em todas essas três categorias. Não está claro porque isso acontece, mas os danos às reputações podem ser um fator. As violações dos aplicativos governamentais têm menos probabilidade de acionar um investimento em mitigação de seguranças em relação aos aplicativos financeiros.

A CSRF é significativamente inferior para os aplicativos financeiros do que nos outros setores. É provável que esta forma de ataque seja levada muito mais a sério neste setor devido às consequências percebidas. O principal objeto deste tipo de ataque é defraudar a vítima, sendo provável que os aplicativos de comércio bancário e aplicativos que usam as transações financeiras sejam os principais alvos.

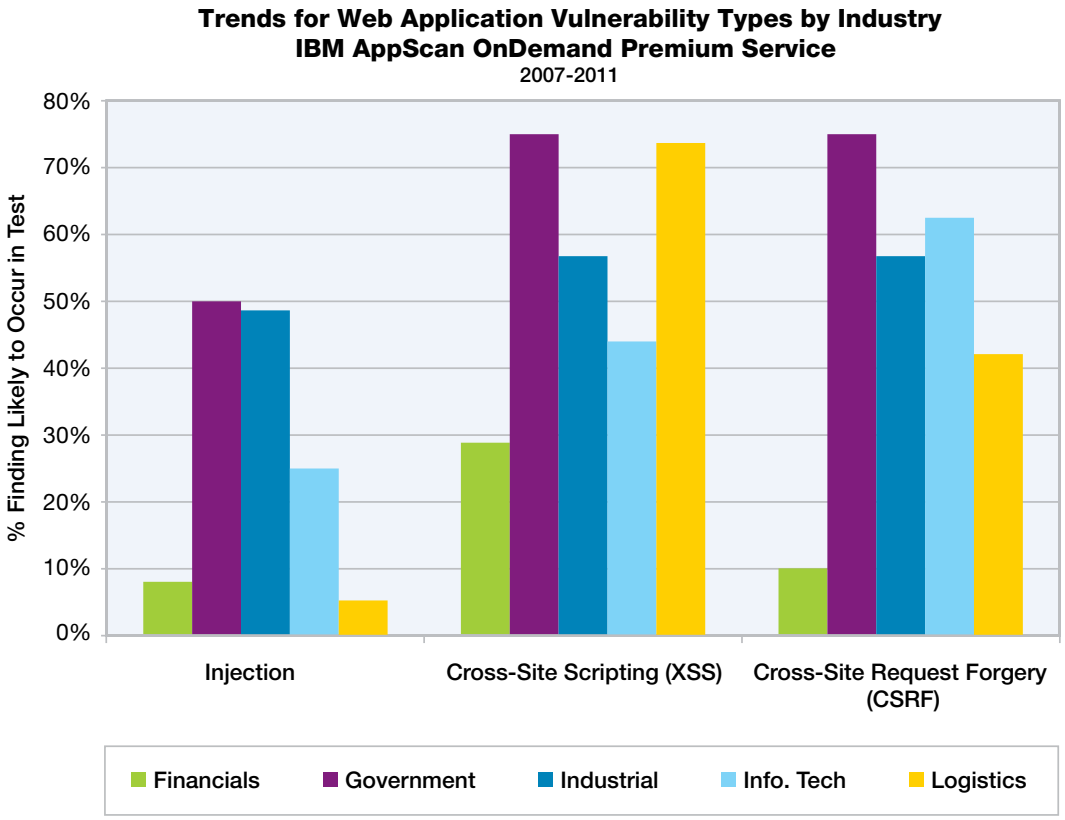


Figure 52: Trends for Web Application Vulnerability Types by Industry IBM AppScan OnDemand Premium Service – 2007-2011

SEGMENTO DE MERCADO										
Tipo de Vulnerabilidade	**Serviços Financeiros**		**Governo**		**Industrial**		**Tecnologia da Informação**		**Logística**	
	Vulnerabilidade média por teste	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**
Injeção	0,1	8%	3,5	50%	10,9	49%	0,6	25%	0,3	5%
Scripting Entre Sites (XSS)	0,4	29%	5,8	75%	13,2	57%	6,1	44%	2,5	74%
Autenticação Quebrada	5,1	73%	12,7	94%	4,8	84%	26,5	100%	38,9	84%
Referências Inseguras de Objetos Diretos	0,3	18%	5,6	94%	2,1	35%	4,8	63%	4,5	47%
Falsificação de Solicitações Entre Sites (CSRF)	1,1	10%	3,9	75%	3,0	57%	2,3	63%	5,7	42%
Má Configuração de Segurança	2,9	82%	18,9	100%	25,9	97%	39,7	100%	10,5	74%
Armazenamento Criptográfico Inseguro	4,8	22%	19,4	100%	12,3	51%	39,9	94%	37,1	79%
Falha ao Restringir o Acesso às URLs	1,0	44%	14,9	100%	0,9	19%	29,4	81%	15,2	79%
Camada de Transporte Insuficiente	3,8	25%	1,4	75%	13,6	59%	36,3	88%	34,3	79%
Redirecionamentos e Encaminhamentos Não Validados	0,2	14%	0,2	19%	1,1	46%	0,1	6%	0,0	0%

Tabela 9: Vulnerabilidades de Aplicativos da Web mais Prevalecentes por Segmento de Mercado, IBM AppScan OnDemand Premium Service

Ciclo de testes de segurança dos aplicativos

Na maioria dos casos, o serviço IBM AppScan no qual estes dados são coletados oferece uma opção de novos testes para qualquer aplicativo testado. Geralmente, estes novos testes ocorrem em até 60 dias após o teste inicial e nem sempre é possível encerrar todos os problemas neste intervalo de tempo.

Certamente, espera-se que os resultados obtidos de um novo teste de aplicativos sejam menores que os de um aplicativo que estivesse sendo testado pela primeira vez. Ao analisar o número médio de determinada descoberta de um teste, no entanto, esta diferença é altamente significativa. Para cada uma das dez principais categorias de OWASP, a diferença é mais que o dobro.

O gráfico a seguir destaca a diferença das descobertas médias feitas por teste entre uma avaliação única e um novo teste posterior.

Em geral, nossos clientes devem testar novamente os resultados para validar se as coisas estão corrigidas. Se o ato de teste inicial dos aplicativos foi suficiente, nossos resultados trimestrais produziriam resultados similares aos novos testes. Obviamente, este não é caso. Acreditamos que saber que o aplicativo será testado novamente deve funcionar como um motivador para a equipe de desenvolvimento; caso contrário, os resultados trimestrais pareceriam muito com os resultados do "novo teste". Outro fator é que os clientes que realizam testes trimestrais regulares podem estar motivados pelos fatores de conformidade e não pela necessidade urgente de mitigar as vulnerabilidades. Isso sugeriria que uma melhor prática seja sempre testar novamente os aplicativos para confirmar se os itens foram corrigidos. Para realizar isso com custo reduzido, os clientes devem considerar usar ferramentas e experiências internas.

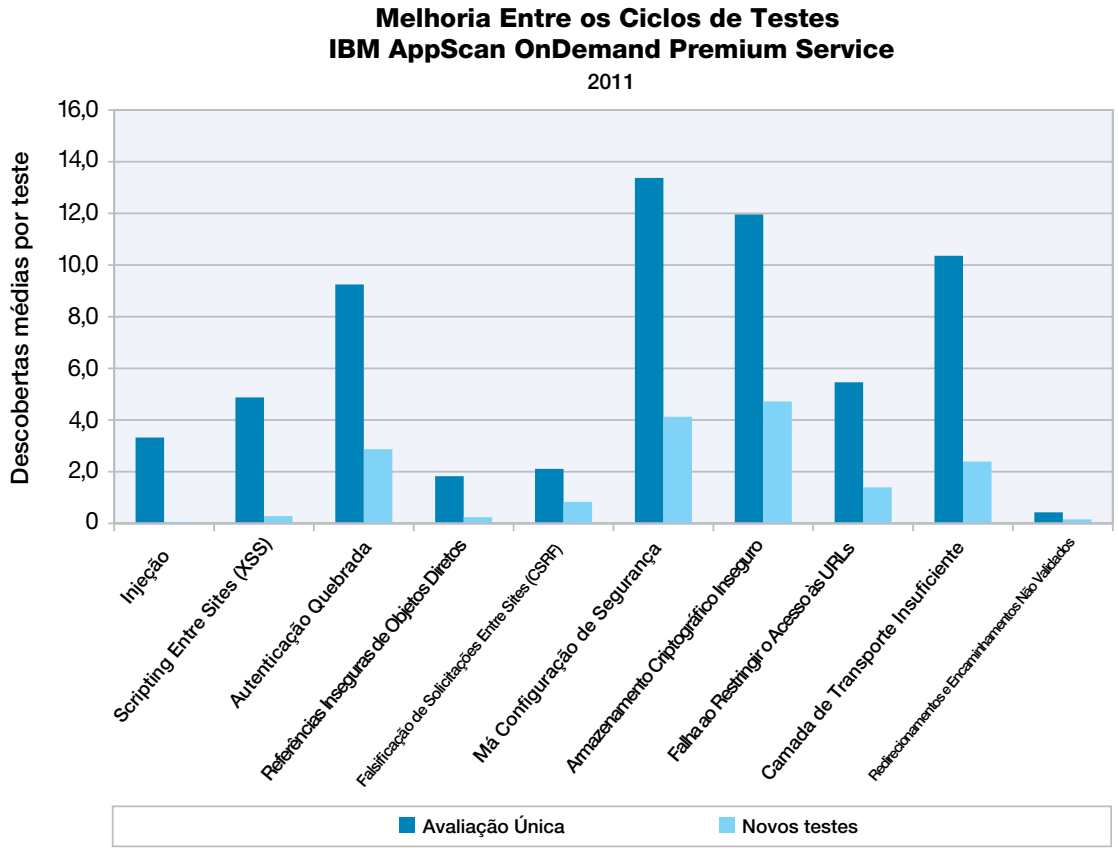


Figura 53: Melhorias Entre os Ciclos de Testes/ IBM AppScan OnDemand Premium Service – 2011

CICLO DE TESTES DE SEGURANÇA						
Tipo de Vulnerabilidade	**Avaliação Única**		**Avaliação Trimestral**		**Novos testes**	
	Vulnerabilidade média por teste	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**	**Vulnerabilidade média por teste**	**% de uma vulnerabilidade com probabilidade de ocorrer**
Injeção	3,3	27%	0,2	5%	0,1	4%
Scripting Entre Sites (XSS)	4,9	46%	3,0	76%	0,3	21%
Autenticação Quebrada	9,2	82%	36,3	86%	2,9	70%
Referências Inseguras de Objetos Diretos	1,8	37%	4,1	43%	0,2	15%
Falsificação de Solicitações Entre Sites (CSRF)	2,1	34%	5,5	43%	0,8	10%
Má Configuração de Segurança	13,4	91%	14,1	76%	4,1	79%
Armazenamento Criptográfico Inseguro	12,0	50%	35,7	76%	4,7	14%
Falha ao Restringir o Acesso às URLs	5,5	51%	13,9	76%	1,4	38%
Camada de Transporte Insuficiente	10,4	46%	31,0	71%	2,4	27%
Redirecionamentos e Encaminhamentos Não Validados	0,4	23%	0,0	0%	0,2	13%

Tabela 10: Ciclos de Teste de Segurança por Tipo de Vulnerabilidade, IBM AppScan OnDemand Premium Service 2011

Seção IV
Tendências Emergentes em Segurança

A seção de Tendências Emergentes em Segurança analisa a tecnologia de rápido desenvolvimento que pressiona as empresas a considerar se já é tempo de fazer investimentos nessas áreas futuras. São explicadas as ameaças e explorações que estão sendo usadas nessas adoções precoces de tecnologia e como as empresas podem permanecer focadas.

Segurança móvel e a empresa – um ano em revisão

A ativação móvel e a segurança relacionada foi um item de foco principal para quase todas as empresas. Elas estão sendo desafiadas a adotar níveis crescentes de mobilidade devido ao fato de a inovação tecnológica ter ajudado a gerar recursos que permitem aumentos em eficiência e permitem que praticamente qualquer negócio aumente seu ritmo por meio do local de trabalho constantemente conectado acionado pela mobilidade. As melhores práticas de auxílio à proteção de dispositivos móveis estão apenas começando, embora estejam sendo feito progressos na área.

A falta de clareza acerca das melhores práticas de auxílio à proteção de dispositivos móveis também é responsável por muitas empresas que estão adotando ou, no mínimo, promovendo os programas "Traga Seu Próprio Dispositivo" (BYOD), que anteriormente nunca permitiram ou ofereceram suporte a esses modelos. Devido ao aumento da predominância de funcionários que têm esses dispositivos, os executivos seniores e funcionários similares estão interessados em fazer este programa funcionar e, muitas vezes, o CISO da empresa é o principal obstáculo devido às preocupações de segurança. Embora muitos CISOs continuem a dizer "não" em vez de "como", há indicações de que esta abordagem pode resultar em diversos projetos para detectar e impedir que os funcionários encontrem maneiras de contornar a infraestrutura existente. Obviamente, esta não é uma posição favorável para as empresas e a abordagem é adotada para ativar e controlar os usos limitados de dispositivos móveis com um foco na classificação de elementos de dados.

Uma sólida análise dos requisitos existentes de segurança associada aos elementos de dados em discussão para ativação oferece alguma clareza para as empresas que lutam com quais controles são necessários. Esta abordagem orientada aos dados aproveita os padrões existentes de segurança e, eventualmente, resultará em melhores práticas de segurança móvel. Em muitos casos, esta é apenas uma abordagem de senso comum de proteção de dados em qualquer dispositivo computacional – e, certamente, todos nós reconhecemos que os smartphones e tablets atuais são apenas dispositivos computacionais.

Para alguns segmentos de mercado, isso pode significar que as abordagens de BYOD que resultam na presença de alguns elementos de dados nos dispositivos móveis de propriedade pessoal podem não ser adequadas. Isso realmente é uma questão de se concentrar nos dados em consideração para ativação e, depois, aplicar os controles necessários associados.

Certamente, a visibilidade de malwares móveis aumentou no ano passado. É importante analisar isso no contexto da paisagem geral de ameaças com a qual as empresas lidam. Houve muitos artigos de imprensa de TI de mainstream que destacavam os ataques de malware específicos aos dispositivos móveis que fariam com que uma pessoa acreditasse que eles ultrapassaram a paisagem tradicional de ameaças de Windows XP. Obviamente, isso não pode ser verdade, mas fornece um bom ponto de dados no sentido de que os malwares móveis estão em alta e de que deve ser planejado um programa de segurança para esse desafio.

Os malwares relacionados aos dispositivos móveis não são a única coisa que aumentou no ano passado. Certamente, as novas soluções de gerenciamento de mobilidade (geralmente, chamadas de soluções MDM ou de Gerenciamento de Dispositivos Móveis) parecem estar aumentando a cada semana. Isso já é esperado e, assim como boa parte das inovações tecnológicas, o foco é o espaço móvel, o que deve causar uma maior necessidade e oportunidade para essas soluções. As escolhas e a concorrência são sempre boas para o cliente e aumentam a probabilidade de que todos os requisitos de controles de segurança necessários às empresas serão abordados em uma escolha de soluções com um preço competitivo. Ultimamente, também houve aumentos nos números de soluções de isolamento ou separação segura. Algumas vezes, elas são chamadas de soluções de Vazamento de Dados, embora no contexto móvel elas sejam muito diferentes das soluções tradicionais de DLP que existem para as estações de trabalho. Embora essas soluções forneçam a promessa eventual de conseguir abordar melhor os dados e aplicativos corporativos que residem nos dispositivos de propriedade dos funcionários de um programa BYOD, atualmente, a maioria delas é relativamente limitada e imatura.

Perspectiva de malwares móveis

À medida que analisamos as mudanças na paisagem de ameaças de malwares móveis do ano passado, ela recebeu mais visibilidade como uma área de interesse. De alguma forma, isso tem sido benéfico, fazendo com que os executivos de TI ficassem cientes sobre as possibilidades reais do que esperar e permitindo que as empresas planejassem os controles adequados. Os leitores dos Relatórios de Riscos e Tendências da X-Force anteriores podem observar que a IBM esteve se preparando e antecipando esses aumentos.

Vale a pena mencionar a natureza das ameaças de malwares móveis que foram expostas no ano passado. Quase em todos os casos, elas existiram e foram fornecidas aos dispositivos nas lojas de aplicativos consideradas legítimas associadas à plataforma móvel. Também vale a pena observar que isso ocorreu em todas as principais plataformas móveis e que as lojas não são confinadas exclusivamente a uma só. Isso é importante por vários motivos. À medida que a seleção de aplicativos explodiu em quase todas as lojas de aplicativos, a eficácia de revisão dos envios não aumentou (com exceção do mercado de trabalho dos Aplicativos Google destacado a

seguir) e os resultados disso começam a ser vistos. O outro aspecto importante é que a maioria dos proprietários de dispositivos (e funcionários corporativos) espera que o confinamento dos downloads de aplicativos apenas que apenas legitima as lojas de aplicativos proteja-os contra aplicativos maliciosos. Isso não é verdade.

Na verdade, os curadores das lojas de aplicativos populares certamente respondem de modo reativo à presença de um aplicativo malicioso e o removem, mas, muitas vezes, isso ocorre muito depois de o seu download já ter sido feito por muitos usuários, sendo algo puramente reativo. Também é uma orientação de melhores práticas evitar a maioria das lojas de aplicativos de terceiros, que não podem revogar os aplicativos existentes. Faz sentido que a probabilidade de encontrar um aplicativo malicioso aumente à medida que a supervisão diminui. Não há um modelo válido para oferecer reconhecimento ao curador a partir dos pesquisadores de segurança, já que isso não fornece um método para monetizar sua pesquisa. Infelizmente, o usuário e a empresa são os reais perdedores, devido à suposição de confiança implicada pelo modelo da loja de aplicativos.

Para auxiliar as empresas com esse problema, há uma crescente seleção de abordagens de prevenção contra malwares disponibilizada pelos fornecedores de segurança. Embora muitas empresas tenham negligenciado essa necessidade, cada vez mais empresas aceitaram a realidade de que os malwares móveis continuarão a aumentar e fornecer a empresa criminosa que aciona a maioria dos malwares em uma maior oportunidade (e ameaças à empresa). Estas soluções estão disponíveis para a maioria das plataformas e a cobertura de plataformas fica cada vez mais fácil à medida que o mercado determina quais plataformas sobreviverão.

Sem a presença ou necessidade de detecção, alguns aplicativos maliciosos podem não ser detectados pelo usuário do dispositivo. É preciso enfatizar alguns deles, já que os outros existem unicamente para realizar transações fraudulentas que devem ser detectadas pelo usuário mediante revisão de sua fatura mensal. Como acontece com os malwares de computadores pessoais, os ataques monetários permanecem sendo um principal foco e os dispositivos móveis que oferecem suporte a SMS são um alvo muito atrativo.

Outro exemplo prático observado, que é único de certa maneira em virtude da natureza dos dispositivos móveis (porque, geralmente, eles têm hardware de GPS com serviços de voz, mensagens e dados), é a presença detectada de aplicativos spyware que monitoram diversos aspectos do comportamento de seus usuários – incluindo localização de registros, mensagens, emails e chamadas de voz ao seu invasor para revisão. Isso é particularmente desconcertante quando é comparado aos tipos de ataques vistos nos computadores pessoais. Já que os dispositivos móveis podem se tornar “seu escritório em seu bolso”, eles fornecem uma ampla oportunidade para um ataque de spyware.

Recentemente, o Google divulgou a implementação de um recurso de revisão de aplicativos que inicia o processo de supervisão de segurança em todos os aplicativos aceitos e mantidos em seu App Marketplace. Isso é notável principalmente porque é uma etapa proativa em direção à melhoria da segurança de aplicativos de sua loja e um exemplo a ser seguido pelos outros curadores de lojas de aplicativos. Embora se espere que isso não seja perfeito e que, provavelmente, seja um exercício de “gato e rato” entre o Google e as pessoas que procuram enviar aplicativos maliciosos, a implementação é claramente uma declaração de ação e da necessidade de proteger usuários contra aplicativos maliciosos. O tempo dirá se os outros proprietários/curadores de lojas de aplicativos a seguirão de modo adequado.

Em relação aos malwares móveis, uma área de risco que deve ser de interesse é o uso dos sistemas operacionais móveis. Embora não tenha havido ataques de malware amplamente disseminados que se autorreplicaram em um sistema operacional móvel e que ocorreram como resultado da vulnerabilidade de uma plataforma subjacente, é provável que seja apenas uma questão de tempo antes que isso ocorra e, certamente, algumas plataformas estão em uma melhor posição para abordar essa situação que as outras. De uma perspectiva puramente corporativa, quase todas as soluções de MDM disponíveis permitem a capacidade de controlar a sincronização das informações corporativas com base na versão do sistema operacional (o que permite que a empresa interrompa o suporte de versões vulneráveis de sistemas operacionais não corrigidos). Provavelmente, isso causará a frustração dos funcionários corporativos, que podem estar presos no meio deste problema de suporte com sua operadora (principalmente nos programas BYOD, nos quais os modelos e operadoras muitas vezes podem ser completamente gerenciados como nos programas fornecidos pelas empresas com controles contratuais). Pode chegar um momento, em um futuro não muito distante, em que os funcionários e proprietários de dispositivos fiquem presos com seus dispositivos vulneráveis e sua única opção seja o upgrade do dispositivo antes da conclusão de seu contrato atual,

quando os modelos de contratos subsidiados foram populares. Muitos suspeitam que os OEMs de hardware tenham deixado os dispositivos para trás intencionalmente, a fim de fazer com que os proprietários façam upgrades com mais frequência. Este problema em particular pode ser um desafio em termos de aceitação dos consumidores em algum momento, já que é bem diferente do modelo aceito para outros dispositivos computacionais dos consumidores, como laptops.

BYOD e o isolamento seguro

Como destacado anteriormente, um dos desenvolvimentos mais recentes deste ano foi o maior interesse em fornecer a capacidade de separar os aplicativos e dados corporativos dos aplicativos e dados pessoais dos funcionários. Obviamente, o principal acionador deste desenvolvimento foi, especificamente, a natureza e o interesse disseminado dos programas BYOD. Embora algumas soluções existissem antes deste ano, a seleção era esparsa e a maioria das soluções era limitada em função e usabilidade. No ano passado, as soluções desta área surgiram como flores na primavera. Espera-se que a maioria delas seja de trabalhos em andamento e que, talvez, tenha suas próprias limitações, costumes de usabilidade e obstáculos à implementação, mas essas soluções são um sinal de que o reconhecimento desse problema e da necessidade corporativa esteja sendo ouvido e ganhando evidência no segmento de mercado. Este é um progresso significativo em relação ao ano passado, quando essas soluções eram um nicho usado por segmentos de mercado específicos, já que as empresas relacionadas tinham dados regulamentados muito específicos que podiam achar um caminho em direção aos dispositivos móveis dos funcionários.

À medida que este segmento de mercado melhora e se desenvolve, esperamos ver as soluções se enquadrarem em algumas categorias diferentes. No espaço Android, existem atividades e obras coletivas em andamento voltadas a abordagens que usam virtualização com base em hardware. O progresso dessas abordagens é limitado à extensa adoção deste recurso de nível de chips e, depois, à adoção e ao suporte correspondentes entre grandes números de dispositivos diferentes que são executados em uma matriz de operadoras globais, o que não as tornar abordagens efetivas para grandes empresas multinacionais. Embora isso possa levar de 24 a 36 meses para acontecer, a "movimentação" claramente está em andamento, à medida que os fabricantes de chips, OEMs de hardware e operadoras reconhecem este requisito corporativo e a oportunidade do mercado correspondente. No futuro, veremos se esta abordagem se torna disseminada o suficiente para funcionar em programas BYOD de grandes empresas.

Enquanto isso, diversas soluções que permitem a separação – por meio de um contêiner, um contêiner virtual ou abordagens de gerenciamento de ativos – estão preenchendo a lacuna para os novos adotantes. Essas abordagens fornecem um nível de separação e controle adicional que as empresas podem expressar nos dispositivos de funcionários sem continuar a controlar todo o dispositivo, mas ainda são necessários trabalhos ativos para determinar quais controles são necessários no nível de um dispositivo para confiar nele como um host da solução de separação. Embora esta mesma preocupação se aplique às abordagens de virtualização mencionadas anteriormente, um contêiner de aplicativo ou abordagem de separação da mesma instância do sistema operacional móvel apresenta mais riscos de existência de malware ou aplicativos maliciosos. Este é outro caso no qual a melhor prática ainda será definida, mas à medida que as empresas adotam essas soluções e que os testes técnicos de segurança necessários são realizados, provavelmente surgirão as práticas aceitas.

Importância da convergência do gerenciamento de dispositivos nas empresas com base em funções

À medida que a utilização de dispositivos móveis continua a explodir na empresa – independentemente de dispositivos de propriedade da empresa, dos funcionários ou de uma mistura dos dois – a necessidade de gerenciá-los no contexto do gerenciamento de riscos corporativos aumentará em importância. Isso será particularmente verdadeiro à medida que os rivais da adoção usarem outros dispositivos computacionais, como laptops. Provavelmente, não será incomum se a proporção de usuários para dispositivos for de dois ou três dispositivos por funcionário, incluindo laptops, tablets e smartphones. Isso significará que a distribuição de dados corporativos, provavelmente, continuará a aumentar e desafiar o uso de perfis de segurança com base em funções e o uso de gerenciamento de riscos corporativos.

À medida que as empresas procurarem abordar os perfis de segurança de usuários com base em recursos que são customizados à função e aos tipos de dados aos quais as funções de usuários específicos estão associadas, esta abordagem se

tornará cada vez mais difícil, enquanto o gerenciamento de dispositivos é disseminado entre as diversas soluções de gerenciamento de dispositivos. De fato, à medida que as empresas saem dos programas em que um tamanho se adapta a todos, que existem nos programas fornecidos de computação puramente corporativos, para confiarem no gerenciamento de uma matriz mais ampla de plataformas operacionais comuns nos programa BYOD, provavelmente esta capacidade de acionar o gerenciamento de dispositivos em uma única plataforma se tornará o principal fator que permite o BYOD com um custo razoável. Para as empresas homogêneas menores, isso pode ser evitado por causa da ausência de números significativos de diferentes funções ou do uso das mesmas classificações de dados entre a maioria de sua população. Elas podem conseguir se virar com poucas soluções (talvez uma para ativos computacionais-padrão e uma para ativos móveis, como smartphones e tablets), mas, para as empresas maiores, provavelmente isso seja uma grave limitação que termine como um comprometimento insatisfatório. Imagine uma empresa de grande porte tendo que proteger todos os ativos, móveis ou outros, para atender o nível mais alto de segurança necessário aos contratos, clientes ou projetos particularmente sensíveis porque não conseguem implementar efetivamente diversas funções entre os diferentes tipos de dispositivos usados por seus funcionários. No final, a perda de eficiência e a incapacidade de oferecer suporte ao melhor fator de forma de dispositivo para diferentes funções realmente aciona a necessidade de procurar uma plataforma uniforme para gerenciar todos os dispositivos de terminais.

O segundo motivo, e igualmente importante, para convergir o gerenciamento de todos os dispositivos de terminais é o desejo de visibilidade coletiva e de gerenciamento de riscos corporativos. Embora certamente seja possível tentar relacionar os diferentes sistemas de gerenciamento em um único console de riscos corporativos, é bem mais fácil e mais provável obter êxito se isso puder ser suportado por uma única tecnologia de estruturas. É muito mais provável conseguir integrar esta plataforma única em uma análise e resposta de ameaças avançadas persistentes (APT).

Fundamentalmente, para a maioria das empresas preocupadas com as ameaças avançadas persistentes, relacionar a análise operacional e a analítica para incluir o status, as informações e a capacidade dos terminais de interagir com os sistemas de terminais em tempo real se torna fundamental à capacidade de fornecer um ecossistema fechado de detecção/resposta. Gerenciar todos os terminais de modo consistente e programático com políticas controladas e bem definidas de segurança deve ser realizado facilmente com a seleção das tecnologias corretas de gerenciamento de segurança, juntamente com o fornecimento de eficiência e supervisão para melhorar toda a paisagem de segurança corporativa, concentrando-se na população de terminais.

Uma análise retrospectiva do estado da segurança na nuvem

Muitas coisas têm sido ditas sobre o estado da segurança nos ambientes em nuvem e as organizações têm procurado respostas ao tentar entender como adotar as soluções em nuvem e garantir a sua segurança. À medida que cada vez mais organizações buscam adotar a nuvem, a segurança permanece sendo a principal prioridade. Muitas organizações permanecem hesitantes em mudar os aplicativos fundamentais ao negócio às nuvens públicas e, em muitos casos, escolhem aproveitar as nuvens privadas. Este pensamento é similar a quando a Internet estava no início e muitas organizações estavam hesitantes em mover os aplicativos fundamentais ao negócio a esta "nova" rede e, em vez disso, confiaram nas redes privadas (muitas vezes baseadas em linhas fixas). Assim como as economias de escala eventualmente colocaram alguns dos aplicativos de negócios mais fundamentais na Internet, a mesma transformação está ocorrendo na computação em nuvem. A questão não é se a nuvem é mais ou menos segura, mas quais controles e processos de negócios específicos devem ser usados para ajudar a reduzir os riscos e ajudar a assegurar a segurança em um ambiente em nuvem. É importante que qualquer organização que esteja buscando uma adoção mais difundida de infraestruturas baseadas em nuvem entenda a função da organização em relação à do provedor de serviços de nuvem, em termos de segurança e mitigação de riscos.

Assim como acontece com qualquer aplicativo ou serviço fundamental ao negócio, a organização de negócios deve assegurar o alinhamento entre os riscos específicos à organização e as políticas e procedimentos fornecidos pelo provedor de serviços.

As melhores práticas de segurança devem ser aderidas ao adotar qualquer nova tecnologia de Internet e, com a computação em nuvem, isso não é diferente. Ao considerar qualquer implementação de nuvem, é preciso pensar sobre a segurança em todas as fases.

Desenvolver

Segurança pelo Design
Foco em desenvolver a segurança na estrutura da nuvem.

Implementar

Acionamento pela carga de trabalho
Proteger os recursos de nuvem com base nos requisitos de segurança de cada carga de trabalho

Consumir

Ativação pelos serviços
Controlar a nuvem por meio de operações e fluxos de trabalho contínuos de segurança

Adotando segurança para a nuvem

Uma pergunta que muitas organizações têm é se os aplicativos e serviços baseados em nuvem são mais seguros que os aplicativos tradicionais de Internet e intranet. Embora nenhum cenário único de implementação ofereça uma segurança mais inerente, uma observação comum é que a segurança é uma grande área de foco ao considerar as implementações baseadas em nuvem. Muitas vezes, há mais confiança na implementação de aplicativos e serviços de uma organização quando eles são considerados internos ao perímetro do limite de confiança da organização. É óbvio que apenas uma conversa sobre segurança não cria mais segurança, mas já que ela é um tema central e principal ao considerar as implementações em nuvem, é muito mais comum ver controles, processos e procedimentos rígidos de segurança em muitos aplicativos e contratações de serviços de nuvem.

Considerações sobre o design

As práticas de desenvolvimento de segurança corporativa devem ser implementadas e aderidas. Ao considerar os provedores terceiros de aplicativos em nuvem, é importante se certificar de que seus padrões e práticas de desenvolvimento seguro atendem ou excedem os de sua empresa.

As proteções adequadas de segurança de terminais e redes devem estar implementadas. Em um ambiente com diversos ocupantes, é importante se certificar de que os aplicativos sensíveis e fundamentais não estejam compartilhando o mesmo hypervisor sem zonas adequadas de segurança e processos implementados de segregação de dados.

Entender os requisitos de segurança de dados. Muitos aplicativos que aproveitam as informações sensíveis e privadas têm requisitos rígidos de segurança impostos pelas organizações, governos, padrões e regulamentos aplicáveis. É preciso assegurar que o provedor de serviços de nuvem possa abordá-los de modo adequado.

Considerações sobre a implementação

Gerenciar os terminais virtuais do mesmo modo que os terminais não virtuais. É importante que as bibliotecas e catálogos virtuais não sofram com os "desvios de segurança", em termos de gerenciamento de correções e configurações.

Aplicar os controles de segurança de modo consistente nos ambientes em nuvem ou outros. Certifique-se de que os aplicativos implementados nos ambientes virtuais recebam o mesmo escrutínio de segurança que os aplicativos públicos de Internet – principalmente nos ambientes de desenvolvimento e teste que, muitas vezes, não têm controles básicos de segurança.

Escanear regularmente todos os aplicativos em nuvem. Aproveitar o código-fonte e os serviços dinâmicos de aplicativos para limitar a exposição de segurança de qualquer aplicativo implementado na nuvem.

Considerações sobre o consumo

Gerenciamento adequado de identidade e acesso. Aplicar os direitos de identidade e acesso de modo adequado, considerando a federação de identidade em relação aos serviços de SaaS de nuvem de terceiros.

Gerenciamento de logs e eventos de segurança. Tenha um gerenciamento efetivo de logs e eventos de segurança de dispositivos virtuais.

Perícia de dados. Ao considerar um terceiro, entenda como a perícia de dados é gerenciada em caso de um incidente de segurança.

Seguir uma abordagem de proteção por design é a melhor maneira de ajudar a realizar uma maior segurança e a reduzir os riscos de passagem a uma infraestrutura baseada em nuvem. A movimentação à nuvem envolveu novamente muitas organizações de TI e, por causa da falta de controle, existe uma maior ênfase sobre a segurança. Em muitos casos, esta maior atenção à abordagem dos desafios envolvidos na proteção de um ambiente que não é 100% controlado resulta na realização de uma maior segurança. Embora os detalhes da infraestrutura sejam menos transparentes e até mesmo obscuros, isso pode resultar em maior segurança.

Melhorando a segurança da nuvem por meio de ANSs

Introdução

2011 foi um grande ano de violações de dados na nuvem. Muitas organizações de grande porte e alto perfil foram exploradas e milhões de registros dos consumidores foram colocados em risco. A violação de uma única entidade de nuvem em grande escala no 1o trimestre de 2011 iniciou uma reação em cadeia, afetando os bancos de dados dos varejistas e instituições financeiras, cujos registros financeiros de consumidores foram expostos. 2011 foi considerado pela IBM X-Force como o Ano da Violação de Segurança e levou muitas organizações a questionar se a computação em nuvem poderia ser protegida de modo razoável.

O sucesso de uma computação em nuvem segura é mais que uma questão de simples gerenciamento de contratos, embora este possa ser fundamental ao sucesso da implementação da nuvem. Geralmente, os contratos e Termos de Serviço (TOS)-padrão são escritos para benefício do provedor da nuvem, a fim de definir os serviços básicos e limitar a exposição e a responsabilidade. É extremamente incomum que o fornecedor de nuvem altere seu contrato-padrão a fim de acomodar as necessidades das organizações de clientes. O Acordo de Nível de Serviço (ANS) é o documento mais flexível que permite que a organização do cliente defina requisitos únicos às suas exigências de modelo de negócios, legais e regulamentares ou outras considerações. Infelizmente, é a natureza da computação em nuvem – sua flexibilidade, escalabilidade e recurso de implementação rápida – que pode dificultar bastante a estruturação e manutenção de um ANS significativo.

Problemas a serem considerados

Devido ao impacto limitado que a organização pode exercer de modo material sobre o ambiente de computação em nuvem, o meio mais efetivo para gerenciar a segurança das informações pode ser o ANS. Portanto, é importante que a organização seja proativa nesta abordagem e adote a visão em longo prazo mais razoável possível para cada um de seus projetos de computação em nuvem. Muitos adotantes iniciais adotam uma visão de curto prazo, preocupando-se principalmente com a seleção do fornecedor e o lançamento do serviço, desconsiderando o gerenciamento de ciclo de vida e a estratégia alternativa.

A resiliência está no centro da maioria dos ANSs de nuvem e, muitas vezes, no foco adotado pelos fornecedores de nuvem em suas declarações-padrão de serviços. A resiliência inclui garantias de tempo de atividade, desempenho e resposta, tempo de correção de erros, entre outros. Algumas podem incluir problemas como segmentação e isolamento em situações de ocupação diversa ou alterar políticas e procedimentos de gerenciamento. Com muita frequência, os ANSs-padrão incluem somente representações gerais em relação à segurança das informações. A organização deve analisar com cuidado as políticas, procedimentos e medidas de controle oferecidas como serviços-padrão e, depois, criar requisitos customizados para cada carga de trabalho específica, conforme acionado pelos dados que cada uma processa, transmite ou armazena.

Para um gerenciamento efetivo da segurança de informações em longo prazo, a organização deve considerar o seguinte ao elaborar ANSs:

- **Propriedade.** A organização deve escanear os contratos-padrão, TOS, ANSs e outros do provedor de nuvem em relação à propriedade conjunta ou absoluta de aplicativos, funcionalidades, conjuntos de dados ou produtos de trabalhos relacionados resultantes da contratação da nuvem, antes de colocar quaisquer dados, processos ou propriedades intelectuais sensíveis ou fundamentais nas mãos do provedor. A organização deve assegurar por escrito que detém a propriedade dos dados ou ativos que expõe ao provedor de nuvem, a fim de promover a transferência do ativo a outro provedor de serviços ou trazê-lo de volta às suas instalações. Isso é particularmente importante para as organizações que usam Qualquer Coisa como Serviço (XaaS) baseado em nuvem. Os softwares e processos proprietários de um fornecedor de nuvem podem não ser replicados facilmente caso a organização precise trazer o projeto às suas instalações ou transferir o projeto a outro provedor. Descobrir posteriormente que a organização cedeu direitos parciais ou integrais de seus ativos como uma condição de serviço pode complicar ainda mais uma situação difícil.
- **Gerenciamento de acesso.** Assim como a organização estabelece os limites dos usuários autorizados de dados sensíveis ou fundamentais internamente, ela deve supervisionar as políticas e mecanismos de gerenciamento de acesso implementados em um ambiente de nuvem. Os requisitos específicos de gerenciamento de acesso dos funcionários do provedor de nuvem aos dados da organização devem ser acionados pelas demandas únicas da carga de trabalho. No entanto, em geral, a organização deve ter um bom entendimento de como o princípio de menor privilégio é aplicado ao(s) ambiente(s) ativo(s) de produção do provedor. Isso é completamente fundamental em um ambiente de nuvem pública de ocupação diversa. Assim como a implementação de cada ocupante deve ser isolada no ambiente compartilhado de hospedagem, o acesso deve ser restrito (na medida razoável possível) a um conjunto de funcionários técnicos designados a prestar serviços à organização do cliente. Isso depende do modelo de negócios do provedor, mas a organização deve entender precisamente como ele gerencia o acesso físico, lógico, remoto e emergencial aos dados e ambientes dos ocupantes. A organização deve avaliar as exigências legais e regulamentares para dados da carga de trabalho e certificar-se de que o provedor de nuvem entenda e possa atender essas exigências e fornecer evidências demonstráveis das iniciativas de boa fé correspondentes. O Gerenciamento de Acesso é discutido em mais detalhes na seção a seguir.
- **Governança.** Como o provedor de nuvem faz representações relacionadas à sua postura e recursos de segurança de informações deve ser um fator principal para a organização ao determinar o tipo de nuvem e provedor adequado à carga de trabalho. A organização deve examinar quaisquer documentos disponibilizados pelo provedor em relação aos seus recursos de segurança de informações, incluindo relatórios ou resumos auditados redigidos (como um relatório SSAE 16 SOC 2 ou selo SOC 3), certificações (como um registro ISSO 270001 do ambiente de produção) ou outros documentos de adesão aos padrões de conformidade, como AUP ou COBIT de BITS Shared Assessments. A organização deve declarar sua necessidade de ter acesso a essa documentação do provedor, a fim de satisfazer quaisquer exigências legais e regulamentares. Ela deve negociar em seu ANS com o provedor de nuvem:
  - A verificação de treinamento e reconhecimento de segurança para os funcionários técnicos.
  - O acesso às informações de registro e monitoramento diretamente relacionadas aos ambientes dos ocupantes.
  - A responsabilidade documentada de segurança e em caso de violação de dados. Isso é particularmente fundamental quando existem ANSs compostos.

  - O acesso às informações forenses relacionadas às violações de dados para propósitos de notificação aos consumidores e de investigação pelo cumprimento da lei.
  - A documentação que destaca como o provedor de nuvem responderá às solicitações de informações, investigações, intimações, entre outras, de cumprimento da lei.

- **Rescisão.** A maioria dos contratos e declarações de TOS-padrão dos provedores de nuvem contém disposições relacionadas à rescisão com causa pelo provedor (como não pagamento) ou pelo cliente (como não atendimento as garantias de tempo de atividade). Além disso, a organização deve inspecionar estes documentos-padrão em busca de quaisquer outras condições de violação de contrato e deve definir claramente uma estratégia alternativa com antecedência às alterações materiais aos serviços oferecidos ou às capacidades do provedor, alterações ao seu próprio modelo de negócios ou simplesmente devido à falha do projeto de nuvem. A organização deve reter o direito razoável de rescindir seu contrato com o provedor sem imposição de penalidades não razoáveis, como:
  - Alterações no modelo de negócios do provedor de nuvem, como a introdução de ANSs compostos após o início da contratação, sem aviso suficiente ou oportunidade de devida diligência pela organização.
  - Alterações na propriedade do provedor de nuvem, como fusão ou aquisição.
  - Alterações substanciais das comissões sem aviso suficiente.
  - Cancelamento ou alterações significativas aos serviços sem aviso suficiente.

De modo ideal, a organização deve se planejar para a rescisão de seu serviço de nuvem com tempo suficiente para implementar um plano de transição. Isso obviamente pressupõe que a organização tenha um plano de transição por escrito implementado. Os motivos para isso podem variar dependendo da carga de trabalho, do tipo de nuvem e do desempenho do provedor, mas as implementações de nuvem podem falhar por muitos motivos o as economias de custos previstas nunca se materializaram de modo realista, o projeto era muito difícil de gerenciar em uma situação terceirizada, o produto ou serviço falhou etc. Qualquer que seja o motivo da organização, ela deve ter uma estratégia alternativa que planeje a necessidade de mover o projeto a outro provedor terceirizado ou retornar as funções às próprias instalações. Um plano de transição documentado deve incluir:

- Motivos para a rescisão documentados para benefício do provedor de nuvem.
- Tempo suficiente para transição nos casos em que a função ou o serviço não foi desenvolvido originalmente para ser completo.
- Assistência à transição, incluindo o formato dos dados e a transferência do provedor à organização.
- Retorno de todos os dados e ativos que pertencem à organização, incluindo os backups.
- Descarte e/ou destruição segura dos dados residuais do ambiente de nuvem, incluindo backups.
- Contingência para complicações criadas pela criptografia dos dados.

Obviamente, este não é um conjunto abrangente de problemas que a organização deve considerar. Os requisitos específicos de carga de trabalho permitem que a organização escolha o tipo de nuvem mais adequado (pública, privada, híbrida ou gerenciada) e o fornecedor mais adequado para prestar os serviços de nuvem. Estas considerações variam de acordo com o tipo de modelo de nuvem implementado pela organização.

Conclusão

A computação em nuvem está mudando rapidamente de uma tecnologia emergente para mainstream e este rápido crescimento é antecipado para o final de ano de 2013. Existem valiosas lições a serem aprendidas com os adotantes iniciais da tecnologia de nuvem, principalmente em relação à segurança de informações. Adotar uma visão de longo prazo para qualquer projeto proposto de computação em nuvem e revisar com cuidado os requisitos de serviço e segurança ditados pela carga de trabalho permite que a organização selecione um modelo e um provedor de nuvem adequado.

Negociar ANSs fortes e favoráveis pode ser fundamental ao sucesso da missão e gerar benefícios a todas as partes envolvidas. Este exercício exige planejar-se com cuidado e evitar os contratos "pegar ou largar" com termos-padrão e não negociáveis. Se o provedor de nuvem não estiver disposto a negociar o ANS, ele pode não ser o provedor certo para a implementação. Os ANSs devem ser específicos em termos e escopo, alterados somente com aviso adequado, e devem reconhecer os requisitos específicos de segurança de informações e de negócios da organização. Eles podem parecer uma ferramenta passiva, mas podem ser o meio mais efetivo de gerenciar e manter uma postura efetiva de segurança em um ambiente terceirizado.

Gerenciamento de identidade e acesso na nuvem

Desafios de segurança nos ambientes de nuvem

Com sua flexibilidade, eficiências de custos e modelo escalável "sob demanda", a computação em nuvem se tornou cada vez mais popular. A capacidade de compartilhar serviços e informações com diversos departamentos, parceiros e clientes é uma vantagem principal da computação em nuvem. Como um benefício adicional, ela pode aprimorar a experiência dos usuários, sem aumentar em complexidade. Os usuários não precisam saber nada sobre a tecnologia subjacente ou as implementações.

Embora os benefícios da computação em nuvem sejam claros, também é a necessidade de desenvolver uma segurança adequada nas implementações de nuvem. À medida que cada vez mais organizações adotam ou consideram a computação em nuvem, elas também se preocupam com os riscos de segurança associados. Uma Pesquisa de Riscos Globais realizada pelo Institute for Business Value da IBM descobriu que a computação em nuvem gerava sérias preocupações sobre o acesso, uso e controle dos dados: 77% dos respondentes acreditavam que adotar a computação em nuvem dificulta a proteção da privacidade; 50% estavam preocupados com uma violação ou perda de dados e 23% se preocupavam com um enfraquecimento da segurança da rede corporativa.

Muitas vezes, os dados e aplicativos são hospedados em domínios públicos e, portanto, o gerenciamento de acesso se torna uma preocupação. A computação em nuvem será tão segura quanto o datacenter? O que acontece quando as unidades de negócios começam a usar serviços de nuvem pública em conjunto com o datacenter ou uma nuvem privada? Como se pode ter certeza de que somente pessoas autorizadas estão acessando seus dados e aplicativos sensíveis? O seu provedor de nuvem consegue fornecer relatórios de auditoria para demonstrar sua conformidade com os regulamentos governamentais e do segmento de mercado? Abordar os problemas levantados por essas perguntas é fundamental à segurança bem-sucedida da nuvem.

As organizações devem equilibrar a proteção, privacidade, governança e acessibilidade aos principais recursos – independentemente de eles estarem no datacenter tradicional, na nuvem privada ou na nuvem pública. A computação em nuvem exige um equilíbrio delicado entre o requisito de compartilhamento de recursos e a necessidade de protegê-los contra acesso não autorizado, vazamento de dados e outras exposições. É óbvio que não se deseja que indivíduos não adequados tenham acesso aos dados e aplicativos privados de sua organização. Para ajudar a assegurar que os recursos de TI de sua empresa estejam seguros independentemente de sua localização e sempre que necessário, o gerenciamento de identidade e acesso deve ser integrado à estrutura de sua nuvem.

A necessidade de segurança na nuvem não deve ser negligenciada ou "engarrafada" posteriormente durante a transição, mas deve ser integrada aos planos gerais de implementação de nuvem. Estes planos podem precisar incluir atualizações aos processos de negócios e políticas, à medida que a segurança da nuvem exige mais que apenas tecnologia. Assim como nos ambientes de segurança tradicional, as organizações devem concordar em documentar e executar mandatos de segurança para que o ambiente de nuvem atenda seus objetivos regulamentares e de negócios. Estes mandatos podem incluir acordos de nível de serviço com o provedor de nuvem, a separação dos requisitos de obrigações dos vários grupos de usuários de nuvem e a criação de "zonas de confiança" para isolar seus dados dos outros clientes que compartilham o mesmo hardware físico.

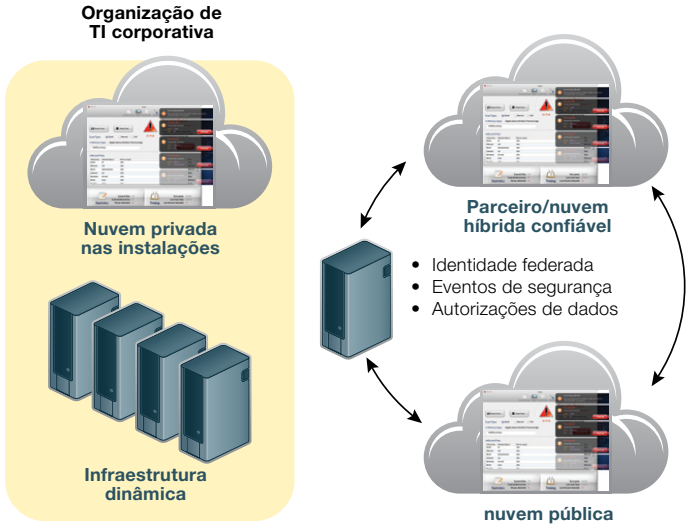
Soluções de Gerenciamento de Identidade e Acesso (IAM) para a nuvem

Independentemente dos aplicativos ou informações que forem movidos à nuvem, uma sólida solução de gerenciamento de identidade e acesso (IAM) pode liderar o caminho. Ela pode abranger os ambientes de computação tradicional e em nuvem para que não seja preciso gerenciar dois conjuntos de credenciais. O objetivo principal é ajudar a assegurar que os usuários autorizados tenham acesso aos aplicativos, dados e ferramentas quando necessário e, ao mesmo tempo, bloquear o acesso não autorizado. Com sua capacidade de limitar o acesso somente aos usuários autorizados e adequados, as soluções de IAM são um componente inestimável de qualquer plano de segurança da nuvem.

Com uma solução de IAM, é possível configurar e aplicar políticas às pessoas que podem acessar as informações a partir de determinados locais e o quanto elas podem acessar em um período determinado. É possível usar a solução para reconfirmar as autorizações com o passar do tempo e revogá-las imediatamente conforme necessário. Também há ferramentas disponíveis para monitorar, relatar e impedir violações de políticas de modo proativo.

Como nos ambientes tradicionais de TI, uma solução de IAM para a nuvem deve incorporar os recursos a seguir: o fornecimento de usuários (incluindo separação de obrigações, controles de acesso com base em funções e autorizações ajustadas), gerenciamento de senhas, sign on único federado e da web, registro e relatórios de auditoria. Finalmente, o gerenciamento de identidade privilegiada é especialmente fundamental por causa dos danos catastróficos que os detentores de informações privilegiadas podem causar, intencional ou inadvertidamente.

Protegendo o acesso aos serviços e aplicativos baseados em nuvem



Com as soluções de Gerenciamento de Identidade e Acesso (IAM), a organização pode controlar de modo central o acesso de grandes números de usuários aos seus serviços baseados em nuvem hospedados por provedores externos, como salesforce.com.

A nuvem estende os serviços, aplicativos e recursos a uma comunidade grande e diversa de usuários que pode incluir funcionários, clientes e parceiros de negócios provenientes de locais externos confiáveis e não confiáveis. As organizações devem relacionar os aplicativos com base em nuvem aos aplicativos internos e permitir que os usuários os acessem com facilidade com um sign on único. A federação de identidade e os recursos de rápida integração devem estar disponíveis para coordenar a autenticação e a autorização com os sistemas de backend e de terceiros. O gerenciamento de identidade federada fornece uma abordagem para gerenciar identidades e acesso em uma nuvem e nas infraestruturas tradicionais de computação. Ele também pode simplificar o fornecimento do ambiente de autoatendimento da nuvem. Um recurso com base em padrões e com sign on único simplifica os logins dos usuários finais para aplicativos hospedados internamente e para a nuvem, permitindo que eles aproveitem os serviços de nuvem de modo fácil e rápido.

Em um cenário típico, a autenticação do usuário ocorre fora da nuvem. Então, a identidade do usuário é federada na nuvem. O processo como um todo é transparente ao usuário. Os recursos de sign on único permitem que o usuário acesse diretamente os aplicativos e informações com base em nuvem sem precisar gerenciar as identidades na nuvem.aproveitem os serviços de nuvem de modo fácil e rápido.

Em relação à conformidade, as organizações devem ter recursos para toda a empresa que ajudem a assegurar que o acesso interno e externo seja controlado por uma autenticação efetiva, para monitorar a autorização e o tráfego da rede e para oferecer suporte ao sistema com recursos abrangentes de auditoria e relatórios. Independentemente do tipo de usuário, a solução deve aprimorar a segurança ajudando a preencher as lacunas nas medidas de segurança. Ela deve mitigar o risco de ameaças, como fraudes, roubos de propriedade intelectual ou perda de dados dos clientes. Ela também deve ajudar a reduzir os custos otimizando os processos de negócios e de TI que concedem acesso dos usuários aos recursos.aproveitem os serviços de nuvem de modo fácil e rápido.

Em resumo, o gerenciamento de identidade e acesso oferece os benefícios operacionais tangíveis de maior produtividade dos usuários, ao mesmo tempo em que reduz o risco de violações de segurança. Uma solução automatizada de gerenciamento de identidade e acesso (IAM) pode abordar os desafios de segurança da nuvem e abranger os ambientes de computação em nuvem e tradicionais.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 EUA

Produzidos nos Estados Unidos da América
Março de 2012

Recicle

WGL03012-USEN-00