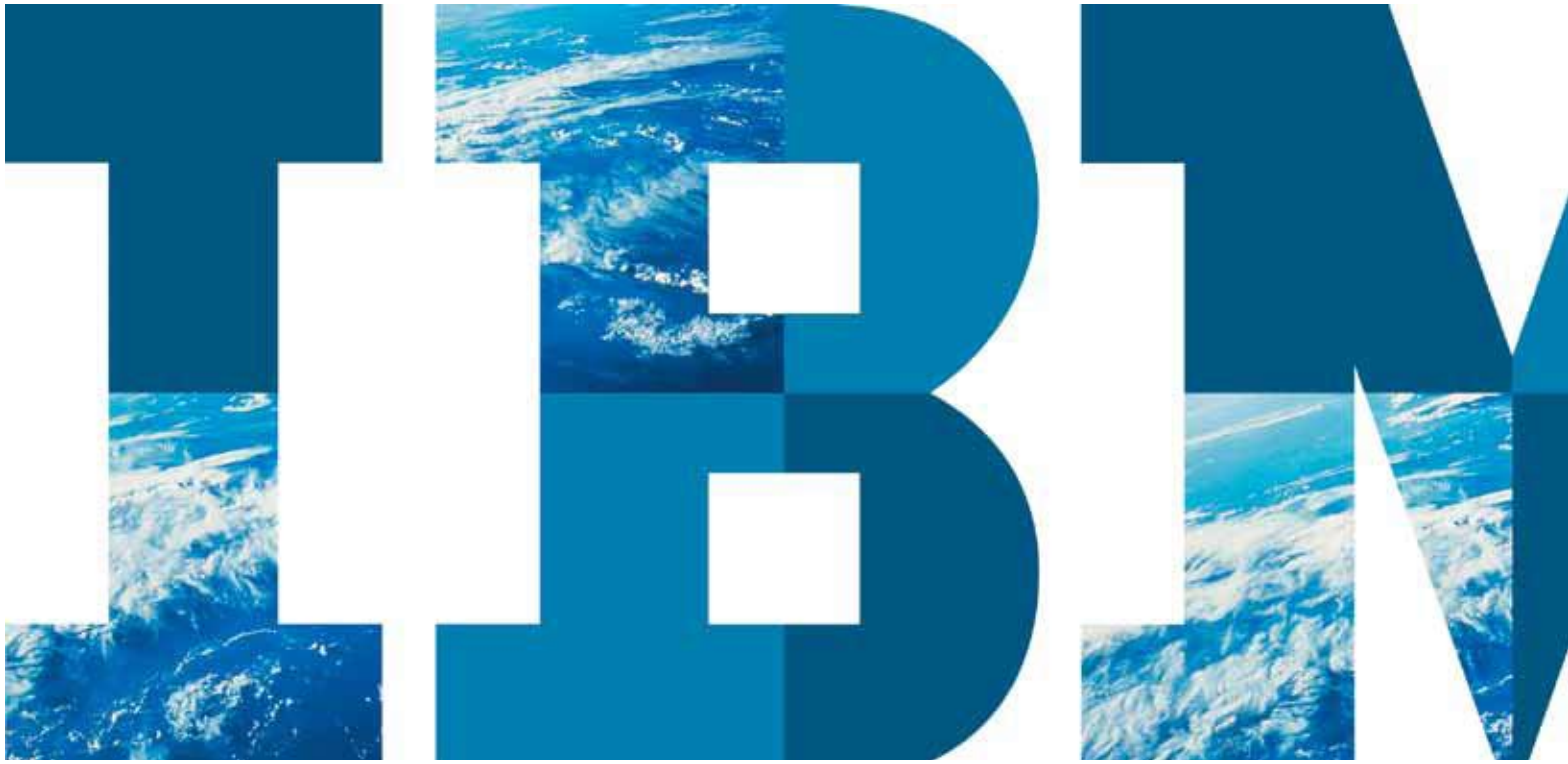
Relatório Semestral de Riscos e Tendências da IBM X-Force 2012

Setembro de 2012



Colaboradores

A produção do Relatório de Riscos e Tendências da IBM X-Force é uma dedicação em colaboração com toda a IBM.

Gostaríamos de agradecer às pessoas abaixo por sua atenção e contribuição na publicação deste relatório.

Colaborador	Cargo
Brian McGee	Visual Designer - User Experience Group/Usability
Bryan Ivey	Team Lead, MSS Cyber Threat and Intelligence Analyst
Carsten Hagemann	X-Force Software Engineer, Content Security
Chadd Horanburg	Cyber Threat Intelligence Analyst
Cynthia Schneider	Technical Editor, IBM Security Systems
David Merrill	STSM, IBM Chief Information Security Office, CISA
Dr. Jens Thamm	Database Management Content Security
Gina Stefanelli	X-Force Marketing Manager
Jason Kravitz	Techline Specialist for IBM Security Systems
Larry Oliver	Senior Cyber Threat/Security Intelligence Analyst
Leslie Horacek	X-Force Threat Response Manager
Marc Noske	Database Administration, Content Security
Mark E. Wallis	Senior Information Developer, IBM Security Systems
Mark Yason	X-Force Advanced Research
Michael Applebaum	Director of Product Marketing, Q1 Labs
Mike Warfield	Senior Wizard, X-Force
Nishad Herath	X-Force Advanced Research
Paul M. Sabanal	X-Force Advanced Research
Ralf Iffert	Manager X-Force Content Security
Randy Stone	Engagement Lead, Emergency Response Service
Rob Hall	Product Manager - Sterling Connect:Enterprise, Sterling Secure Proxy
Robert Freeman	Manager, X-Force Advanced Research
Rod Gifford	Product Marketing Manager, Sterling Connect:Enterprise, Sterling Secure Proxy
Scott Moore	X-Force Software Developer and X-Force Database Team Lead
Thomas Millar	Senior Incident Response Analyst

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

DEDICATÓRIA

O Relatório Semestral de Riscos e Tendências da IBM X-Force 2012 é dedicado à memória do nosso querido amigo e colega, ***Don Hall****. Director of Product Development for Advanced Threat Platforms no IBM Security Systems, Don supervisionava uma equipe mundial de engenheiros, incluindo as equipes de pesquisa e desenvolvimento da X-Force, que contribuem para a produção deste relatório.*
Um grande campeão para a sua equipe e um líder de tecnologia dedicado, as contribuições de Don feitas à segurança e à IBM farão muita falta.

Colaboração da IBM Security

A IBM Security oferece um grande espectro da competência de segurança.

- A equipe de pesquisa e desenvolvimento da IBM X-Force descobre, analisa, monitora e registra uma ampla variedade de ameaças de segurança a computadores, vulnerabilidades, além das tendências e dos métodos mais recentes utilizados por invasores. Outros grupos da IBM utilizam esses dados ricos para desenvolver técnicas de proteção aos nossos clientes.
- A equipe de segurança de conteúdo da IBM X-Force investiga e categoriza a web por meio de crawling, descobertas independentes e pelos feeds fornecidos pelos Serviços Gerenciados de Segurança da IBM (MSS - Managed Security Services).
- Os Serviços Gerenciados de Segurança (MSS) são responsáveis pelo monitoramento de explorações relacionadas aos terminais, servidores (incluindo servidores da web) e pela infraestrutura geral da rede. Os MSS controlam as explorações fornecidas pela web, além de outros vetores, como email e mensagem instantânea.
- Os Serviços Profissionais de Segurança da IBM (PSS - Professional Security Services) oferecem serviços corporativos de avaliação, design e implementação de segurança para ajudar a desenvolver soluções efetivas de segurança da informação.

- O Qradar Plataforma de Inteligência de Segurança, da Q1 Labs, uma empresa da IBM, oferece uma solução integrada para SIEM, gerenciamento de registros, gerenciamento de configuração e detecção de anormalidades. Ele oferece um painel unificado e informações em tempo real sobre riscos de segurança e de conformidade de pessoas, dados, aplicativos e infraestrutura.
- O IBM Sterling Secure Proxy é um proxy de aplicativo baseado em uma zona desmilitarizada (DMZ) que protege suas transferências de arquivo da internet pública. O IBM Sterling Connect:Direct® é uma das soluções líderes para transferências de arquivos de ponta a ponta seguras. Ele foi otimizado a fim de obter uma entrega de dados de arquivos confiável e de alto volume dentro das e entre as empresas e fornece automação, planejamento e notificações de alerta baseados em script para operações não assistidas que funcionem 24 horas por dia, 7 dias por semana.

Índice

Índice

Seção I – Ameaças

Nesta seção, exploramos tópicos relacionados a ameaças e descrevemos os ataques corporativos enfrentados por especialistas em segurança. Discutimos a atividade maliciosa observada pela IBM e como ajudamos a proteger as redes dessas ameaças. Também oferecemos atualizações sobre as tendências de ataques mais recentes identificadas pela IBM.

Visão geral executiva

No início de 2011, a IBM X-Force declarou aquele o ano da violação de segurança. Tanto grandes quanto pequenas empresas foram atingidas. Em 2012, a tendência continuou e o tópico de violações de segurança rapidamente surgiu como o principal assunto das listas de discussões de diretorias a blogs, até a grande mídia. Executivos que foram responsabilizados por dados importantes da empresa, do cliente, do funcionário, do investidor e/ou do parceiro desejavam reconciliar e entender se estavam indo bem nesse ambiente combustível de atividade de ataque. Continuaram fazendo perguntas difíceis sobre o nível de segurança de uma empresa interconectada em termos de tecnologias em nuvem, móveis e terceirizadas. Eles também perguntavam quem estava gerenciando a segurança de dentro da organização, a fim de que as etapas em direção a um plano de ação fossem tomadas.

Como uma organização de pesquisa de segurança, a IBM X-Force tradicionalmente visualizou violações de segurança com um foco técnico. No entanto, modificamos nossa visão dos ataques e violações ao longo do tempo para incluir um contexto de negócios mais abrangente. A tendência geral de violação continua em 2012, à medida que várias grandes empresas notórias tiveram que lidar com o efeito colateral adverso do vazamento de senhas, além de outros dados pessoais. O segmento de mercado de assistência média em particular parece ter sido severamente atingido.

Embora produtos e tecnologias de segurança pudessem ter mitigado muitos desses eventos infelizes, estamos observando, mais do que nunca, como a interconectividade dos sistemas, a fraca execução da política e o erro humano são muito mais influentes do que uma única vulnerabilidade de segurança.

Observamos várias notícias relacionadas a casos nos quais as identidades digitais foram dizimadas, não por meio de malware, criadores de registros importantes, quebra de senha ou mesmo acesso ao computador ou dispositivo da vítima. Em vez disso, os vilões realizam seus atos abomináveis descartando uma pequena quantidade de dados pessoais de fontes públicas, utilizando truques de engenharia social e dependendo de políticas vagas de um pequeno número de empresas a quem confiamos nossos dados privados. Agora, mais do que nunca, o equilíbrio delicado entre segurança, conveniência e privacidade assume o papel central.

Em um caso, os invasores escaparam da autenticação de dois fatores – comumente considerada praticamente à prova de falhas – simplesmente convencendo um provedor de telefones celulares a realocar a mensagem de voz de um usuário, oferecendo aos invasores os dados necessários para redefinir uma senha. Em outro, os últimos quatro dígitos do número de um cartão de crédito, que estava facilmente visível em um site, foi utilizado por outro serviço como uma peça importante dos dados de identificação, utilizados para redefinir a conta. Para cada um destes tipos de incidentes de alto nível, há violações semelhantes ocorrendo sob o radar.

Por meio da divulgação de violações em 2012, continuamos vendo uma SQL injection reinando como a principal técnica de ataque. Além disso, os invasores parecem se aproveitar das vulnerabilidades do cross-site scripting para os aplicativos da web. Mais de 51% das vulnerabilidades de aplicativos da web reportadas em 2012 são categorizadas como cross-site scripting.

Mesmo com toda essa atividade numerosa de ataque, também testemunhamos pontos positivos. Os níveis de spam e de phishing continuam baixos com o fim de botnets em 2011 e recentemente, em julho de 2012, testemunhamos outro fim de botnets com a remoção da Grum. Os dados claramente demonstram quedas dessa atividade. Tendências da web positivas continuam com a adoção da tecnologia IPv6. Atualmente, as empresas e os governos que aproveitam o IPv6 encontram menos atividades maliciosas, embora não saibamos quando os invasores decidirão adotar a tecnologia IPv6.

Em meados de 2012, vemos uma tendência de crescimento nas vulnerabilidades gerais, com uma possibilidade de grande alta até o final do ano. Mesmo assim, os dados da IBM X-Force continuam demonstrando quedas em explorações verdadeiras, com apenas 9,7% de todas as vulnerabilidade divulgadas publicamente sujeitas a explorações. Ao obter progresso em determinadas áreas, encontramo-nos em uma encruzilhada de mudança. As melhorias de design e tecnologia de softwares do passado combinam a adoção de novas tecnologias, como a combinação de dispositivos móveis pessoais e tablets, na empresa.

É necessária uma abordagem mais holística a todo o ecossistema. Os usuários devem estar mais cientes da visibilidade online de seus dados pessoais, de como acessá-los e de como eles podem ser utilizá-los contra eles. Isso afeta não somente suas redes sociais, como também suas escolhas de seleção e uso de aplicativos remotos. Como uma tendência crescente, os aplicativos remotos requerem uma quantidade significativa de permissões que diluem a capacidade dos usuários de discernirem uma possível intenção maliciosa. Além disso, à medida que os consumidores e as empresas movem dados importantes para a nuvem, é ainda mais importante auditar e entender como esses dados são acessados.

Mudamos do escritório para o perímetro da rede corporativa, para negócios ligados, um mundo de dispositivos e serviços interconectados. Um lapso na política ou na tecnologia em qualquer ponto do sistema pode e irá abalar a fundação. A IBM X-Force está confiante de que nosso Relatório de Riscos e Tendências da IBM X-Force ajudará a prepará-lo com a conscientização necessária para tomar as decisões certas para o seu negócio.

Agora, consideremos alguns dos destaques que ocorreram no primeiro semestre de 2012.

Destaques de 2012

Ameaças

Malware e web maliciosa

- Qualquer grande evento global, seja ele uma eleição ou uma catástrofe, levará a Otimizações do Mecanismo de Busca (SEOs) criadas por várias pessoas diferentes para uma variedade de objetivos, tanto genuínos quanto maliciosos. As notícias atuais oferecem excelentes fontes de "isca" a serem utilizadas em spams, ataques de SEO e phishing, ou campanhas de phishing. Elas também são excelentes oportunidades para que invasores em posse de um navegador da web explorem kits como o Buraco Negro. **(Página 11)**
- Um método de corromper completamente o computador da vítima é prover uma URL ou site confiável com uma carga útil maliciosa por meio de vulnerabilidades de cross-site scripting. Os websites de várias organizações bem-estabelecidas e confiáveis ainda são suscetíveis ao cross-site scripting não persistente. **(Página 11)**
- Desde o último relatório, observamos um crescimento contínuo na SQL injection, que está mantendo o ritmo com o aumento do uso dos comandos cross-site scripting e directory traversal, como os comandos HTTP "Ponto Ponto". Esses três tipos de exploração se tornaram bastante eficientes quando utilizados em conjunto. **(Página 11)**
- No final de 2011, discutimos como a emergência de novas variantes de malwares para Macs serão cada vez mais semelhantes à sua contraparte do Windows. Analisando o primeiro semestre de 2012, parece que estávamos certos. Nos últimos meses, observamos alguns grandes desenvolvimentos no mundo de malwares para Macs, incluindo o surto do Flashback e a descoberta de malwares para Macs de ameaça avançada persistente (APT). **(Página 29)**
- Em nosso último Relatório de Riscos e Tendências da IBM X-Force, mencionamos que a dificuldade técnica em explorar o software OSX é um grande fator na prevenção da exploração em massa. Infecções do Flashback contornam a segurança do S.O. utilizando explorações multiplataforma por meio de vulnerabilidades do Java. Isto é, a técnica de exploração e grande parte do código envolvido são os mesmos, independentemente se o alvo é o Windows ou o Mac. Alguns fornecedores de segurança definiram sumidouros para determinar o número de infecções do Flashback e as estimativas são de até 600.000 máquinas. **(Página 30)**
- Outro grande desenvolvimento em malwares para Macs no primeiro semestre do ano é a descoberta de malwares direcionados (APT para Mac). Algumas variantes iniciais utilizaram a exploração Java CVE-2011-3544 para espalhar. Essa exploração é a Vulnerabilidade do Mecanismo de Scripts do Java Applet Rhino – a mesma utilizada pelo Flashback. O objetivo desse malware direcionado é roubar os dados do usuário. **(Página 30)**

Tendências do conteúdo da web, spam e phishing

- O IPv6 Day foi realizado em 6 de junho de 2012, com várias organizações executando implementações permanentes do IPv6. Embora a adoção total ainda seja baixa, os dados da IBM X-Force demonstram que o Web 2.0 e sites legítimos são atualmente os mais prontos para IPv6. Websites com conteúdo, como sites de hackeamento, sites de drogas ilegais, proxies anônimos, pornografia e sites de jogos, foram mais lentos na adoção do IPv6. Isso pode ser devido aos esforços técnicos adicionais necessários para ser pronto para IPv6 ou possivelmente a fim de que eles possam continuar atingindo o máximo número possível de usuários. **(Páginas 31-33)**
- Os registros de proxies anônimos continuam estáveis no primeiro semestre de 2012, com três vezes mais proxies anônimos recém-registrados hoje do que no ano anterior. Mais de dois terços de todos os proxies anônimos eram executados no domínio .tk (o domínio de nível superior de Tokelau, um território da Nova Zelândia). **(Página 35)**
- Os Estados Unidos continuam sendo o principal host de links maliciosos, com a hospedagem de mais de 43% de todos os links de malware. A Alemanha ocupa a segunda posição, hospedando 9,2%. Completando a lista dos principais está a Rússia, em terceiro lugar pela primeira vez. A China caiu do topo da lista para a quarta posição. Aproximadamente 50% de todos os links de malware estão localizados em websites de pornografia ou jogos. **(Página 36)**

- No final de 2011, observamos o renascimento de spams baseados em imagens. Os spammers continuaram utilizando esse tipo de spam até o final de março de 2012. Ao mesmo tempo, mais de 8% de todos os spams continham um anexo de imagem. **(Página 39)**
- Outra nova tendência esteve relacionada ao tamanho do spam. Tradicionalmente, mensagens de spam eram propositalmente pequenas, a fim de assegurar que os spammers enviassem o máximo possível, considerando sua banda larga. Atualmente, observamos mensagens de tamanhos relativamente grandes, sendo grande parte de seu tamanho resultado de grandes seções de Folhas de Estilo em Cascata (CSS). Uma teoria atual é que os dados extras estão sendo utilizados como uma forma de escapar da detecção, já que eles não parecem afetar os dados ou a formatação da mensagem. **(Página 41)**
- A Índia continua sendo o principal país de distribuição de spams, dominando o topo da lista e estabelecendo um recorde constante, enviando aproximadamente 16% de todos os spams registrados atualmente. Os EUA, que caíram para menos de 3% no segundo trimestre de 2011, tiveram um crescimento no segundo trimestre de 2012. Eles atualmente representam mais de 8%, em terceiro lugar, seguidos do Vietnã. Completando os cinco primeiros estão a Austrália e a Coreia do Sul, com o Brasil logo em seguida, em número seis, responsável por 6% de todos os spams distribuídos no primeiro semestre de 2012. **(Página 44)**
- Em 18 de julho de 2012, testemunhamos o fim da botnet da Grum. A Grum preferia clientes dos EUA, Vietnã, Austrália, Alemanha e Brasil, sendo que esses países enviavam 29,9% dos spams mundiais antes do fim da botnet, mas apenas 22,5% depois disso. **(Página 47)**
- No final de 2011, começamos a observar o surgimento de emails parecidos com phishing, que levavam a websites que não necessariamente executavam um ataque de phishing. Em 2012, essa atividade continuou em locais nos quais serviços de encomenda eram amplamente utilizados para enganar usuários, atingindo mais de 27% de todo o volume de scam e phishing. Os phishers também voltaram sua atenção para organizações de fins não lucrativos, representando 66% e, em seguida, caindo para 7% nos dois primeiros trimestres de 2012. **(Página 49)**

Práticas operacionais de segurança

Vulnerabilidades e exploração

- No primeiro semestre de 2012, reportamos um pouco mais de 4.400 novas vulnerabilidades de segurança. Se essa tendência continuar ao longo do resto do ano, o total de vulnerabilidades previsto será um pouco maior do que o registro observado em 2010, alcançando um total de 9.000 vulnerabilidades. **(Página 58)**
- A queda de vulnerabilidades de SQL injection continuou em 2012, mas as vulnerabilidades de cross-site scripting aumentaram novamente, chegando a uma alta prevista constante. Cross-site scripting é um termo utilizado para descrever vulnerabilidades de aplicativos da web que permitem que invasores insiram scripts do lado do cliente em páginas da web visualizadas por outros usuários. Mais de 51% de todas as vulnerabilidades de aplicativos da web reportadas até agora em 2012 são categorizadas como cross-site scripting. **(Página 59)**
- A IBM X-Force classifica duas categorias de exploração. Fragmentos simples com código de prova de conceito são considerados explorações, mas programas totalmente funcionais que podem atacar um computador são categorizados separadamente como “explorações reais”. A redução da tendência de explorações reais continua em 2012, quando, com base nos dados dos seis primeiros meses, prevemos que apenas 9,7% de todas as vulnerabilidades divulgadas publicamente contêm explorações. **(Página 62)**
- A IBM X-Force observou que as vulnerabilidades no Office e em Portable Document Formats (PDF) diminuíram drasticamente. A IBM X-Force está confiante de que haja uma forte ligação entre a queda de divulgações de PDFs e o ambiente de simulação do Adobe Acrobat Reader X. **(Página 67)**

- A IBM X-Force tem visto grandes progressos na taxa de vulnerabilidades corrigidas dos dez maiores fornecedores, o que pode ser atribuído a práticas de desenvolvimento seguras e à implementação e melhoria contínuas dos programas da Equipe de Resposta a Incidentes de Segurança do Produto (PSIRT). Os dez maiores fornecedores têm uma taxa de recurso de correção de pouco mais de 94% de todas as vulnerabilidades divulgadas. **(Página 67)**
- A taxa de vulnerabilidades não corrigidas (com exceção dos dez maiores fornecedores) no primeiro semestre de 2012 foi a mais alta vista pela IBM X-Force desde 2008. Quarenta e sete por cento de todas as vulnerabilidades divulgadas este ano continuam sem um recurso, mas isso se deve principalmente a softwares não corporativos. **(Página 68)**

Práticas de segurança de desenvolvimento de softwares

Segurança da senha de emails

- A conexão entre websites, serviços baseados na nuvem e webmail fornece uma experiência inigualável de dispositivo a dispositivo, mas os usuários devem tomar cuidado com o modo como essas contas são conectadas, com a segurança de sua senha e com quais dados foram fornecidos para a recuperação de senhas ou redefinição da conta. **(Página 87)**
- Considerando a velocidade das ferramentas de recuperação de senhas, senhas fracas podem ser descobertas a partir de hashes vazados de bancos de dados em segundos. A melhor solução para desenvolvedores da web é utilizar uma função de hash desenvolvida para proteger o storage de senhas. Ela deve utilizar um salt e a própria transformação de hash deve demorar um tempo relativo, dificultando ainda mais a recuperação de senhas em texto simples. Um salt é apenas um elemento adicional, como uma sequência aleatória de texto combinada à senha antes de ser enviada à função de hash. **(Página 91)**

Tendências emergentes de segurança

Malware móvel

- No primeiro semestre de 2012, as vulnerabilidades e explorações de dispositivos móveis reportadas atingiram os níveis mais baixos desde 2008. A IBM X-Force acredita que haja vários motivos para isso. Em primeiro lugar, os desenvolvedores de sistemas operacionais de dispositivo móvel continuam investindo em descobertas internas de vulnerabilidades e em aprimoramentos em seus modelos de segurança para impedir a exploração das vulnerabilidades. Como é comum em uma área nova (como a de dispositivos móveis), observamos um padrão. Primeiro, há um pico inicial de descobertas, com a rápida descoberta de erros mais fáceis e, em seguida, sobram os mais difíceis de explorar. Geralmente, há um atraso entre as técnicas de descoberta dos pesquisadores e invasores para superar limitações percebidas anteriormente. **(Página 64)**
- O estado da segurança do dispositivo móvel está em evolução. Embora existam relatórios sobre malwares remotos exóticos, como TigerBot/ Android. Bmaster on Android e Zeus/ ZITMO em diversas plataformas remotas, a maioria dos usuários de smartphones ainda está em risco principalmente devido às falsificações de SMS comercial, entre outros. Essas falsificações funcionam enviando mensagens SMS automaticamente aos números telefônicos principais de uma variedade de países diferentes a partir dos aplicativos instalados. **(Página 98)**

Móvel – Traga Seu Próprio Dispositivo (BYOD)

- Para que o BYOD funcione, deve haver uma política em vigor completa e clara antes que o dispositivo de propriedade do funcionário seja agregado à infraestrutura da empresa. Essa política deve abordar todos os aspectos da ligação entre a empresa e o dispositivo do funcionário e incluir a adesão de todas as partes. **(Página 99)**
- À medida que os dispositivos móveis se tornam um dispositivo de computação importante para muitos – tanto em empresas quanto na internet como um todo – podemos descobrir que a correção de dispositivos vulneráveis se torna uma preocupação de segurança importante, pois essa área teve o menor progresso no último ano. **(Página 105)**

Serviços Gerenciados de Segurança da IBM – Um cenário global de ameaças

Os Serviços Gerenciados de Segurança da IBM (MSS) monitoram dezenas de bilhões de eventos por ano em mais de 130 países, 24 horas por dia, 365 dias ao ano. A presença global do IBM MSS oferece uma visão em primeira mão de ameaças atuais e nossos analistas utilizam essa riqueza de dados para obter uma compreensão do cenário de ameaças cibernéticas. Esta seção oferece atualizações sobre nossa visão das principais ameaças discutidas neste relatório. A identificação da tendência de ameaças é essencial para estabelecer futuras estratégias de segurança e entender o significado das ameaças para o nosso ambiente de computação.

Em conjunto: Cross-site scripting e SQL injection

Qualquer grande evento global, seja ele uma eleição ou uma catástrofe, levará a Otimizações do Mecanismo de Busca (SEOs) criadas por várias pessoas diferentes para uma variedade de objetivos, tanto genuínos quanto maliciosos. Temos visto o efeito em sites da mídia social toda vez que há um desastre, um evento de celebridade ou um escândalo.Este ano, testemunhamos muitos desses tipos de eventos, incluindo as eleições de 2012, as Olimpíadas de Londres e a Profecia Maia, bastante mencionada. Todos proporcionaram uma fonte excelente de "iscas" a serem utilizadas em spam, ataques de SEO e phishing, ou campanhas de phishing. Elas também são excelentes oportunidades para que invasores em posse de um navegador da web explorem kits como o Buraco Negro.

Um método de corromper o computador de uma vítima é fornecer uma URL que envie o usuário para um website vulnerável de sua confiança. Muitos websites de organizações conhecidas e confiáveis continuam suscetíveis a cross-site scripting não persistente, geralmente empregando uma URL criada especialmente para esse fim. Com o uso crescente do HTML5, agora a SQL injection no lado do cliente também é possível, pois o HTML5 se tornou o novo método de acesso à web de fato. Isso significa que os invasores podem acessar o storage local por meio de recursos espessos do HTML5 e, caso haja uma versão local de um banco de dados da SQL, a SQL injection se torna outro método válido de afetar o computador da vítima.

Desde o nosso último Relatório de Riscos e Tendências da IBM X-Force, continuamos vendo um crescimento contínuo na SQL injection, mantendo o ritmo do crescimento de cross-site scripting e de comandos de directory traversal, como comandos HTTP “Ponto Ponto”. Estes três tipos de exploração se tornam bastante eficientes quando utilizados em conjunto. Como já há muitas formas de misturá-los, não enumeramos todos os métodos em vigor atualmente.

No entanto, o que podemos afirmar é que a SQL injection e o cross-site scripting estão crescendo rapidamente como métodos de ataque preferenciais e que as nossas informações de tendência combinam com a asserção. Continuaremos observando todos os três eventos em busca de oportunidades para correlacionar e melhorar os relatórios sobre essa nova abordagem.

Ofuscação

No mundo das ameaças cibernéticas, a ofuscação é uma técnica para ocultar ou mascarar as fontes e métodos de um evento de segurança relevante. Novos métodos de ofuscação estão em desenvolvimento constante em uma tentativa de evitar sistemas de prevenção contra intrusão (IPS) e softwares antivírus. O IBM Security Network IPS possui algoritmos especiais de detecção que auxiliam no monitoramento dessas técnicas em todo o mundo. O tipo de ofuscação mais difícil de lidar é baseado em criptografia, pois ele limita o que pode ser determinado sobre as informações que estão sendo transmitidas. Por outro lado, as informações criptografadas que aparecem em locais inesperados são geralmente "delatoras" por elas próprias, pois identificam uma origem e um alvo suspeitos que requerem mais verificação.

Combinando Tendências Entre Eventos de Cross-site Scripting e Eventos de SQL injection
julho de 2011 a junho de 2012

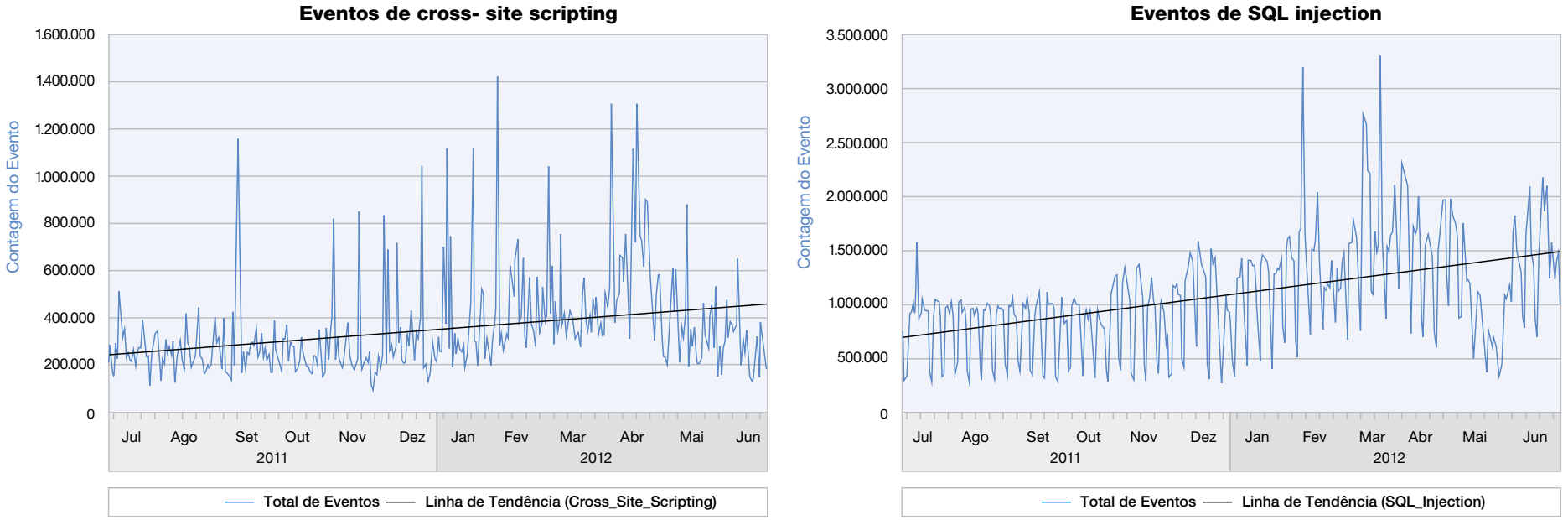


Figura 1: Combinando tendências entre Eventos de Cross-site Scripting e Eventos de SQL injection - julho de 2011 a junho de 2012

Estamos observando o crescente uso de criptografia por criminosos virtuais para esconder suas explorações e dificultar que os sistemas de segurança da rede as detectem. Isso inclui HTTPS, além de recursos de criptografia nativos, em vários formatos de documento e ofuscação utilizando linguagens de script. Conforme claramente demonstrado no gráfico, a presença e o volume do tráfego possivelmente ofuscado é extremamente variável e persistente. A imagem representa um composto de aproximadamente 30 heurísticas de ofuscação separadas. Esperamos que o uso de técnicas de ofuscação continue como tecnologias que identificam explorações, malware e à medida que o vazamento de dados melhore. Além disso, à medida que novos aplicativos são implementados e novas tecnologias (serviços em nuvem, aplicativos remotos, etc.) emergem e influenciam o modo como comunicamos utilizando a mesma internet, haverá mais motivos para ocultar possíveis ataques, aumentando o impacto diariamente.

Continuamos desenvolvendo e implementando técnicas para manter o ritmo do crescimento de técnicas de ofuscação e continuaremos atualizando nossos clientes com relação a essas tendências.

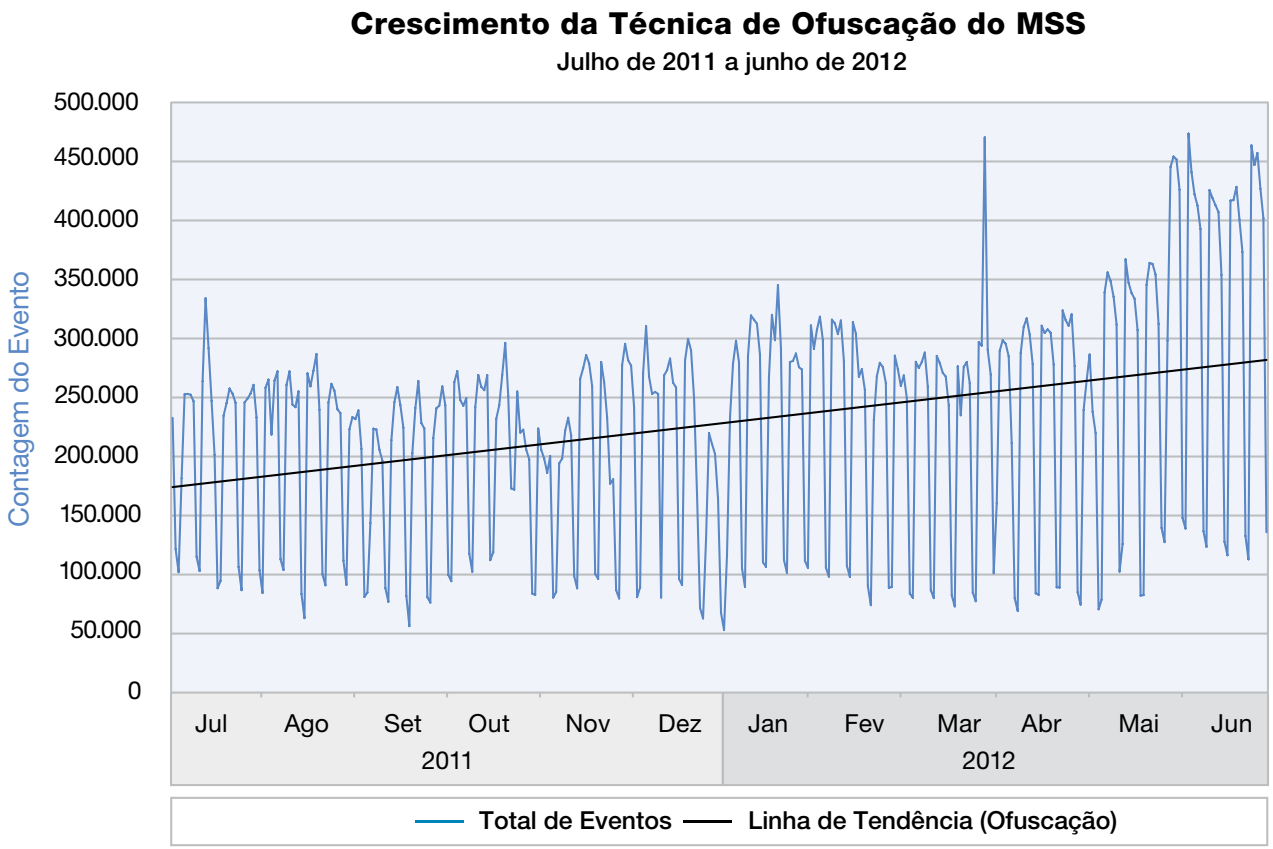


Figura 2: Crescimento da Técnica de Ofuscação do MSS - julho de 2011 a junho de 2012

MSS – Principais assinaturas de alto volume de 2012

Tabela 1: A tabela Principais assinaturas de alto volume do MSS mostra a localização relativa das dez assinaturas mais significativas do Managed Security Services e sua direção de tendência para 2012, conforme comparado com o final do ano de 2011 e 2010. Sete das principais assinaturas do final do ano de 2011 mantiveram um lugar na lista de meados de 2012. Primeiro, destacaremos algumas das mudanças significativas.

A trajetória de queda da assinatura SQL_Injection foi revertida em 2011 e continua aumentando, mantendo, assim, sua posição como a assinatura de maior volume.

A assinatura Worm SQL Slammer, SQL_SSRP_Slammer_Worm, estava em declínio durante todo o ano e pode inclusive cair da lista das dez principais durante a próxima iteração do relatório. Ainda não sabemos o motivo exato pelo declínio dramático e sustentado.

Ao mesmo tempo, a assinatura PsExec_Service_Accessed voltou para a fila de assinaturas de alto volume. Essa ferramenta popular de administração de sistemas está em terceiro lugar, após ficar fora da lista por um ano.

Como várias das demais assinaturas, o volume da assinatura HTTP_Get_DotDot_Data continua sua tendência crescente, subindo da quinta para a quarta posição.

Nome do Evento	Classificação de 2012	Tendência	Classificação de 2011	Tendência	Classificação de 2010	Tendência
SQL_Injection	1	Crescente	1	Crescente	2	Decrescente
SQL_SSRP_Slammer_Worm	2	Levemente Decrescente	3	Levemente Decrescente	1	Decrescente
PsExec_Service_Accessed	3	Levemente Crescente	3	Levemente Crescente		
HTTP_GET_DotDot_Data	4	Crescente	5	Crescente		
Cross_Site_Scripting	5	Levemente Crescente	6	Levemente Crescente		
SNMP_Crack	6	Decrescente	4	Decrescente		
SSH_Brute_Force	7	Levemente Crescente	7	Levemente Crescente	4	Levemente Crescente
HTTP_Unix_Passwords	8	Crescente	8	Crescente	6	Levemente Crescente
Shell_Command_Injection	9	Levemente Crescente	9	Crescente		
JavaScript_Shellcode_Detected	10	Crescente				

Tabela 1: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS - 1o Semestre de 2012

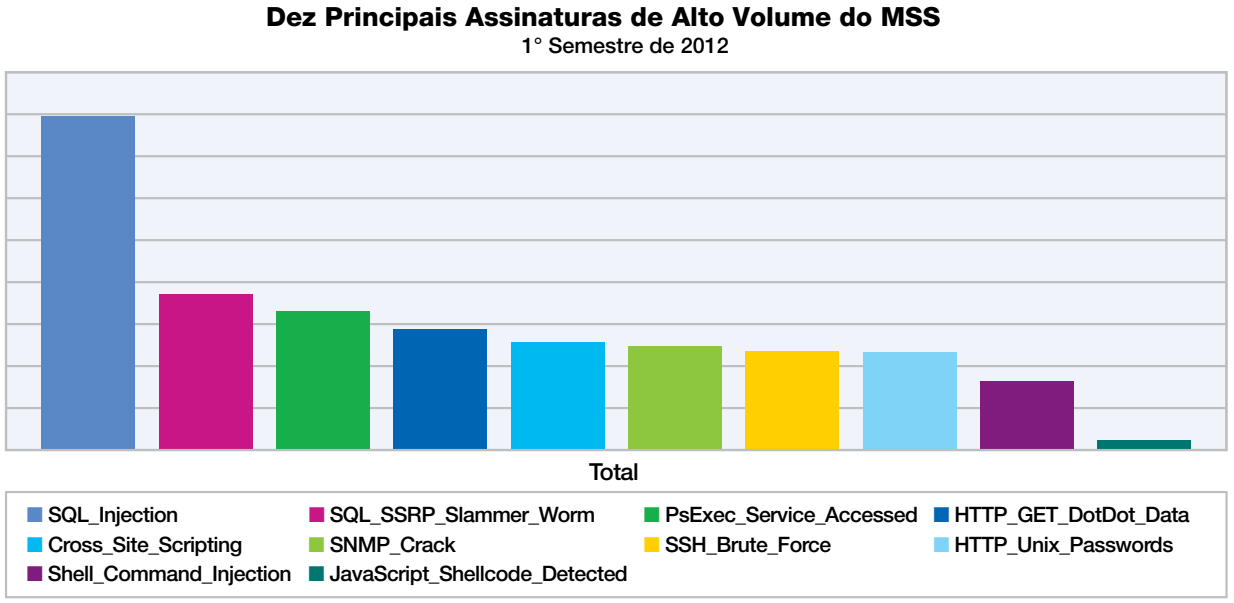


Figura 3: Dez Principais Assinaturas de Alto Volume do MSS - 1o Semestre de 2012

SQL injection

A assinatura SQL_Injection foi classificada em segundo lugar em 2010 e subiu mais em 2011, com uma indicação de uma tendência crescente contínua. 2011 foi um ano marcante para a exploração dos pontos fracos da SQL. No final do ano, a linha de tendência para a atividade de SQL injection começou a nivelar à medida que a atividade de ativistas hackers começou a se acalmar. Houve o salto usual perto dos feriados do varejo, em novembro e dezembro, mas a tendência era se acalmar.

Os grupos de ativistas hackers, Anonymous e Lulzsec, tiveram uma grande presença nas táticas de SQL injection no início de 2011 e continuaram a aprimorar suas habilidades com novos vetores de ataque de injeção. No entanto, os níveis de atividade entraram em uma breve calmaria que foi reconhecível.

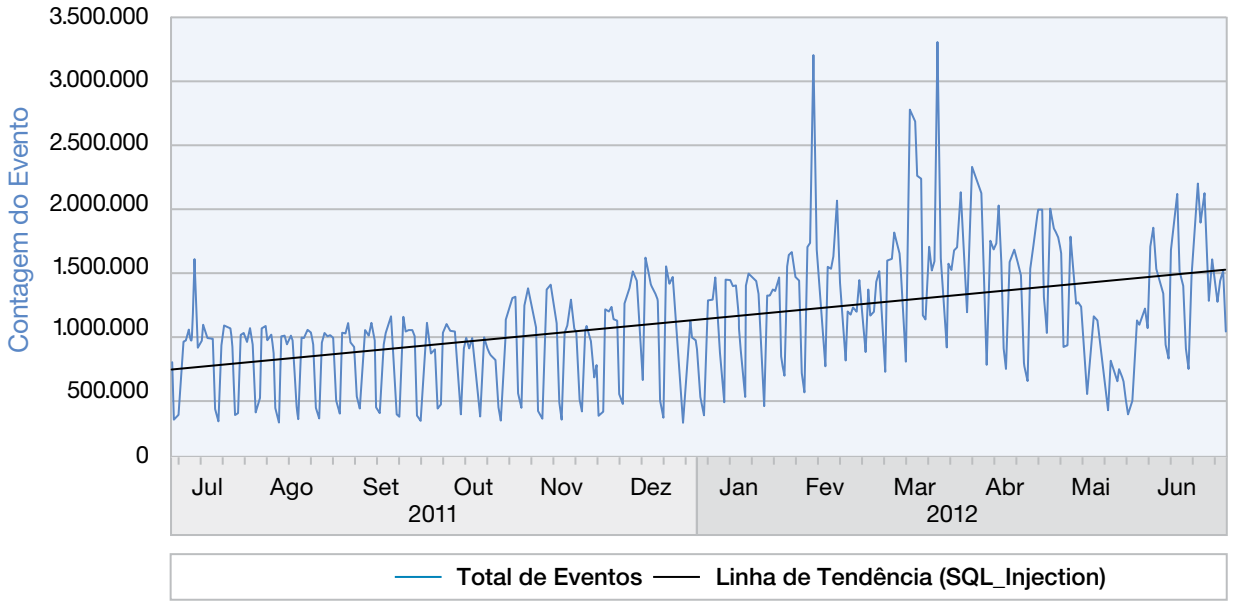
Utilizando ferramentas como LizaMoon, a comunidade de invasores tiveram progresso em 2011 na automação da identificação de possíveis sistemas fracos e continuou a aprimorar seus métodos de exploração.
Em 2012, estamos observando níveis ainda mais altos de tentativas de SQL injection e a taxa de expansão desse tipo de ataque parece ser maior do que no final de 2011. O resultado líquido de toda essa atividade manteve a SQL injection na posição mais alta no primeiro semestre de 2012.

O Relatório Anual de Riscos e Tendências da IBM X-Force contém uma seção, "A Ameaça Contínua da SQL injection", que oferece insight adicional à ameaça de SQL injection e identifica ações que podem ser tomadas para ajudar a se proteger contra ataques. Este artigo deve ser leitura necessária para qualquer pessoa que esteja familiarizada com esse ataque e seus mecanismos de exploração associados.

Conforme discutido anteriormente neste artigo, os invasores continuam combinando diferentes tecnologias, criando um ataque em camadas a partir do qual eles podem ter uma chance maior de sucesso e contra o qual pode ser difícil se defender. A SQL injection é uma das explorações mais comuns encontradas nesses kits de ferramentas, especialmente quando combinada a outras explorações comuns, como injeção de comando shell ou cross-site scripting.

Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (SQL_Injection)

Julho de 2011 a junho de 2012



Worm SQL Slammer

A segunda assinatura mais comum já vista está relacionada ao Worm SQL Slammer. O Worm SQL Slammer provou ser um dos exemplos mais duráveis de malware da internet. O final de janeiro de 2012 marcou o nono aniversário da liberação do Worm slammer. Mas o Slammer não parece estar desaparecendo. Conforme discutido no artigo do Relatório Semestral de Riscos e Tendências da IBM X-Force 2011, "O dia em que o SQL Slammer desapareceu", a atividade do SQL Slammer caiu precipitadamente em março de 2011. Desde então, o Slammer praticamente desapareceu. Embora esteja atualmente classificado no Relatório Semestral de 2012, ele pode desaparecer completamente até o lançamento do próximo relatório. Conforme previsto, a queda continua e será provavelmente removido da lista das Principais Assinaturas de Alto Volume no próximo relatório.

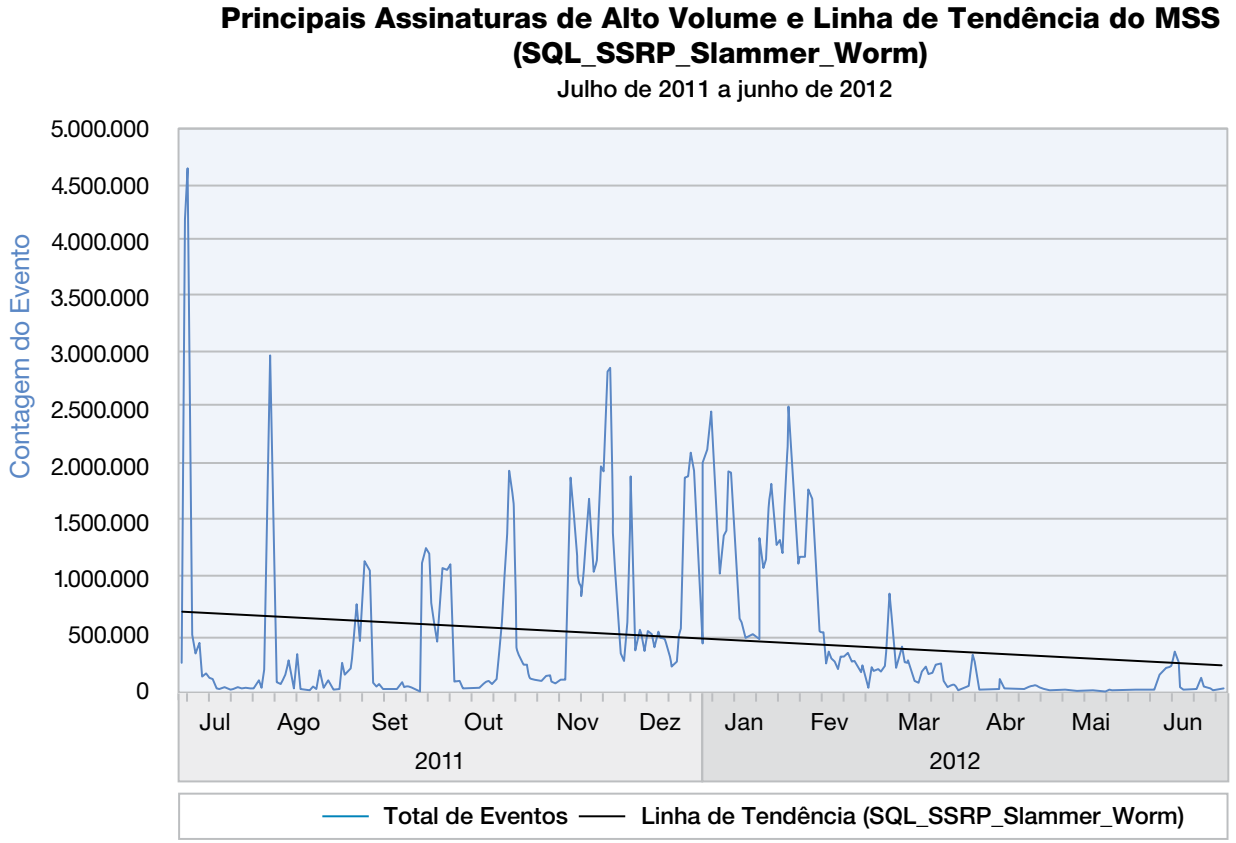


Figura 5: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (SQL_SSRP_Slammer_ Worm) - julho de 2011 a junho de 2012

PsExec_Service_Accessed

A assinatura em quarto lugar, PsExec_Service_Accessed, é uma espécie de "estalo do passado", pois foi classificada em terceiro lugar na lista de Assinaturas de Alto Volume no final de 2010.

Observe que o software PsExec faz parte de um legítimo pacote de aplicativos de propriedade da Microsoft e é suportado como parte do Windows Sysinternals. É uma ferramenta de administração remota baseada em uma linha de comando, mais parecida com uma versão leve da telnet, e funciona de forma adequada sem a instalação de nenhum código no sistema de destino. O PsExec manipula tudo.

No entanto, às vezes, worms e ameaças avançadas se aproveitam do PsExec. O worm "Here you are", por exemplo, inclui uma ferramenta que permite que ele seja copiado em outros computadores da rede. Caso o conjunto de softwares Sysinternals seja utilizado em sua organização, é preciso se certificar de que as melhores práticas sejam empregadas.

Nossa assinatura heurística detecta a invocação do manipulador do servidor do PsExec e reportará tentativas de utilizar a ferramenta. Isso nem sempre significa que um ataque ou um malware tenha sido detectado, mas sempre que essa assinatura aparecer, é melhor confirmar se o seu uso é apropriado.

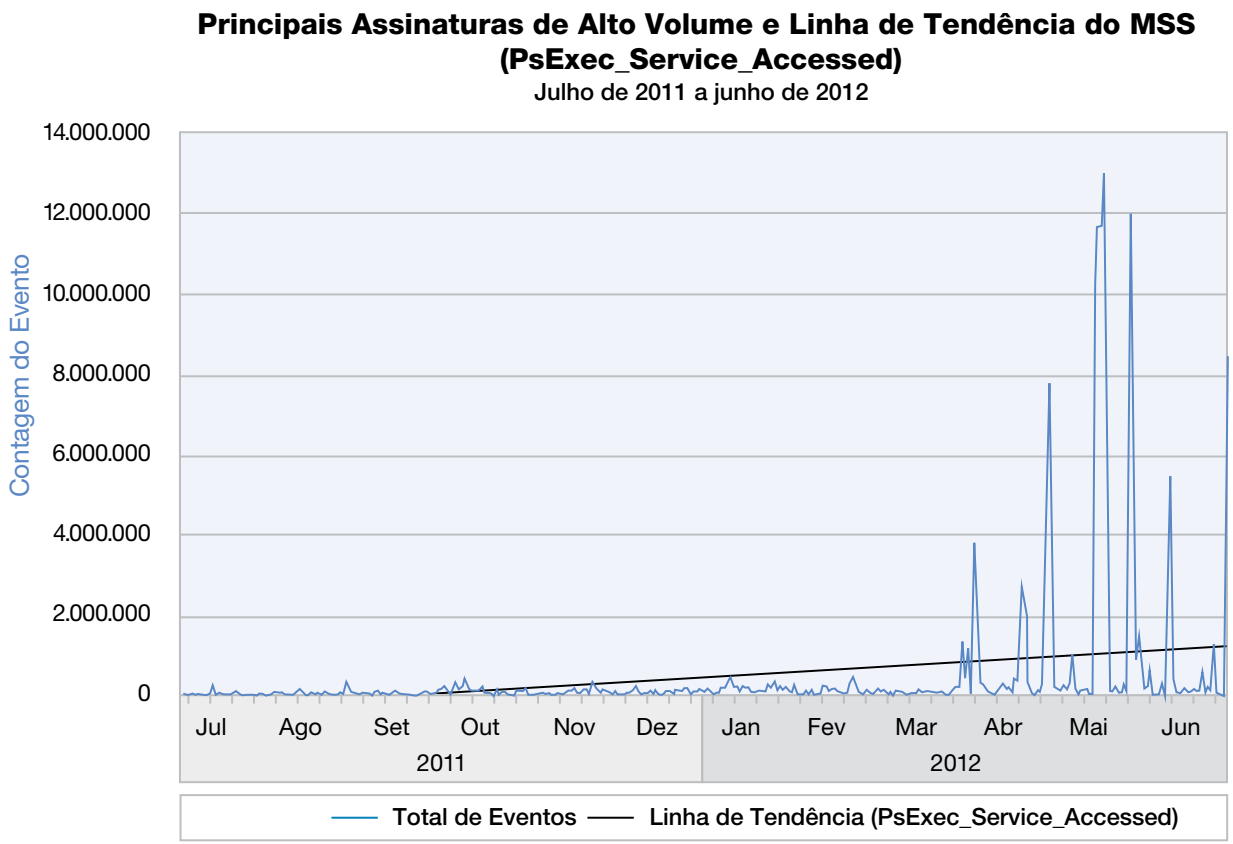


Figura 6: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (PsExec_Service_Accessed) - julho de 2011 a junho de 2012

Directory Traversal

A quarta assinatura mais comum vista é HTTP_GET_DotDot_Data e sua relação com o método de ataque directory traversal. Este é um método de ataque realmente antigo, mas ainda é efetivo, pois é baseado nos recursos persistentes de grande parte dos shells do sistema operacional.

Isso permite que um invasor atravesse diretórios em servidores da web vulneráveis. A capacidade de mover de diretório a diretório pode fornecer grandes informações para o invasor sobre a localização de programas no servidor.

A única defesa confiável contra essa técnica é filtrar a entrada do usuário para identificar e desativar habilidades indesejadas e restringir o nível de privilégio de acesso dos processos de serviços da web.

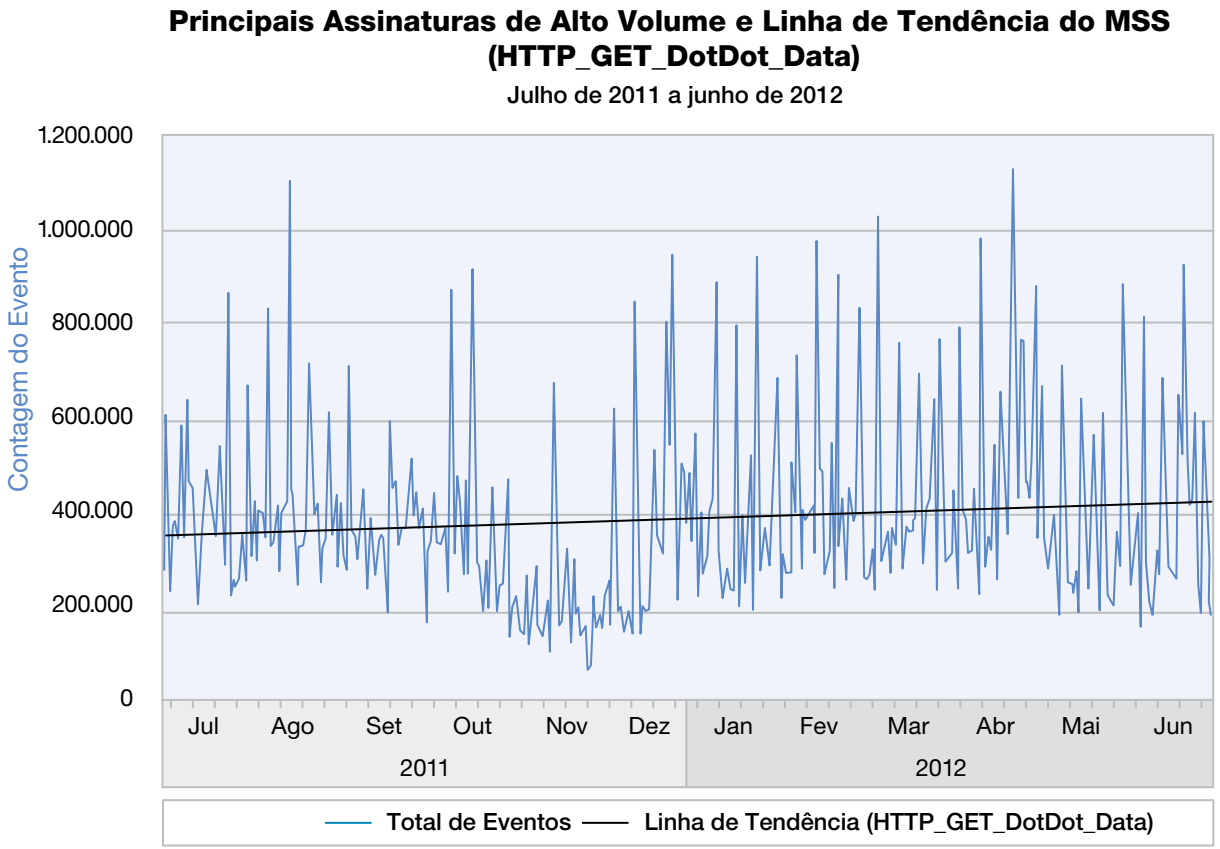


Figura 7: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (HTTP_GET_DotDot_Data) - julho de 2011 a junho de 2012

Cross-site scripting (XSS)

Cross-site scripting é uma das explorações mais persistentes da era da internet. Um ataque cross-site scripting injeta scripts do lado do cliente nas páginas da web, possivelmente corrompendo o computador do cliente. Esse ataque funciona em qualquer tecnologia de navegação da web, incluindo dispositivos móveis. Ele é extremamente popular e pode representar um risco de segurança significativo.

Documentado pela primeira vez em 1999, o cross-site scripting era originalmente um problema exclusivo do ambiente Unix. Antes do término do ano, uma segunda variante da exploração foi documentada. Nesse momento, há mais de 6.000 variantes dessa vulnerabilidade, com usos variando de interceptação de uma sessão de navegador a um controle total baseado no servidor da web do sistema.

A assinatura Cross_Site_Scripting encontra-se em quinto lugar em nossa lista das principais assinaturas controladas por volume. A redução da exposição a esse risco normalmente envolve uma validação cuidadosa do código do lado do servidor. Novas tecnologias do navegador mostram alguma promessa de redução da efetividade dessa vulnerabilidade e a educação do usuário com relação ao lado do cliente é fundamental.

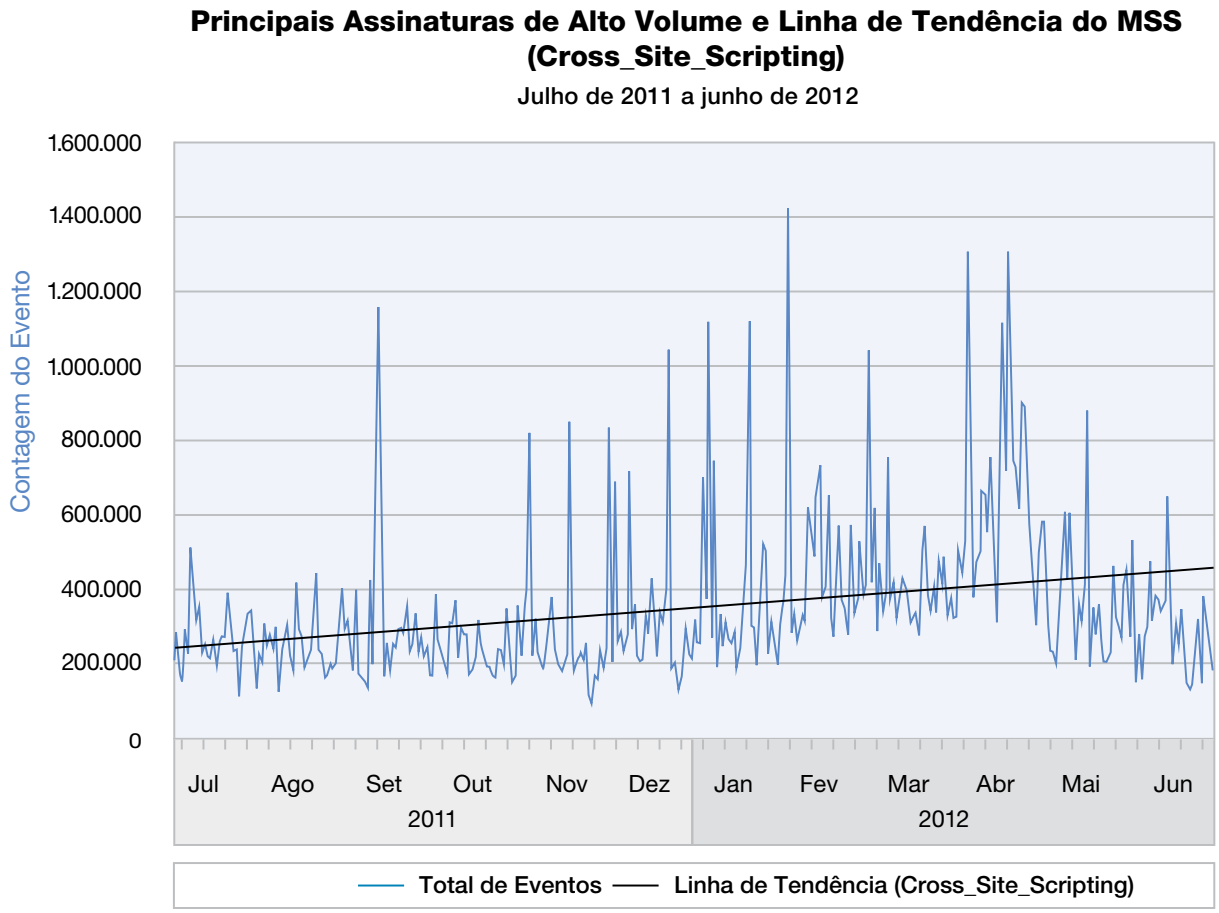


Figura 8: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (Cross_Site_Scripting) - julho de 2011 a junho de 2012

SNMP Crack

A assinatura SNMP_Crack é uma das várias assinaturas que são impulsionadas para detectar tentativas de força bruta contra a segurança bastante fraca. O Protocolo Simples de Gerenciamento de Rede (SNMP) foi desenvolvido para uso em um ambiente confiável e as sequências de comunidade visavam ajudar a manter as coisas resolvidas, não fornecer autenticação em redes públicas. Visando auxiliar os administradores da rede, o SNMP pode ser encontrado em sistemas operacionais, hubs, comutadores e roteadores em um ambiente de Protocolo da Internet.

A assinatura SNMP_Crack é acionada quando um grande número de mensagens de SNMP com diferentes sequências de comunidade são detectadas em um curto período. Essa é uma descoberta suspeita, que pode indicar um ataque de estimativa de sequência de comunidade de força bruta. Por uma questão de melhores práticas, o SNMP é normalmente proibido por meio de firewalls, a fim de evitar que uma entidade externa utilize-o para executar uma varredura de descoberta em sua rede protegida.

Como os serviços do SNMP são configurados com sequências de comunidade padrão, um possível invasor pode primeiro procurar por essas sequências de comunidade. Ao não obter informações utilizando sequências padrão, ele pode tentar uma procura de força bruta por sequências de comunidade válidas. A menos que seja absolutamente necessário, recomendamos que o SNMP seja bloqueado no perímetro externo. Também recomendamos que a necessidade do SNMP seja avaliada em sua totalidade e que a desativação do protocolo seja considerada caso ela não seja exigida. Caso seja realmente necessário, considere a migração para o SNMPv3 para uma autenticação mais forte.

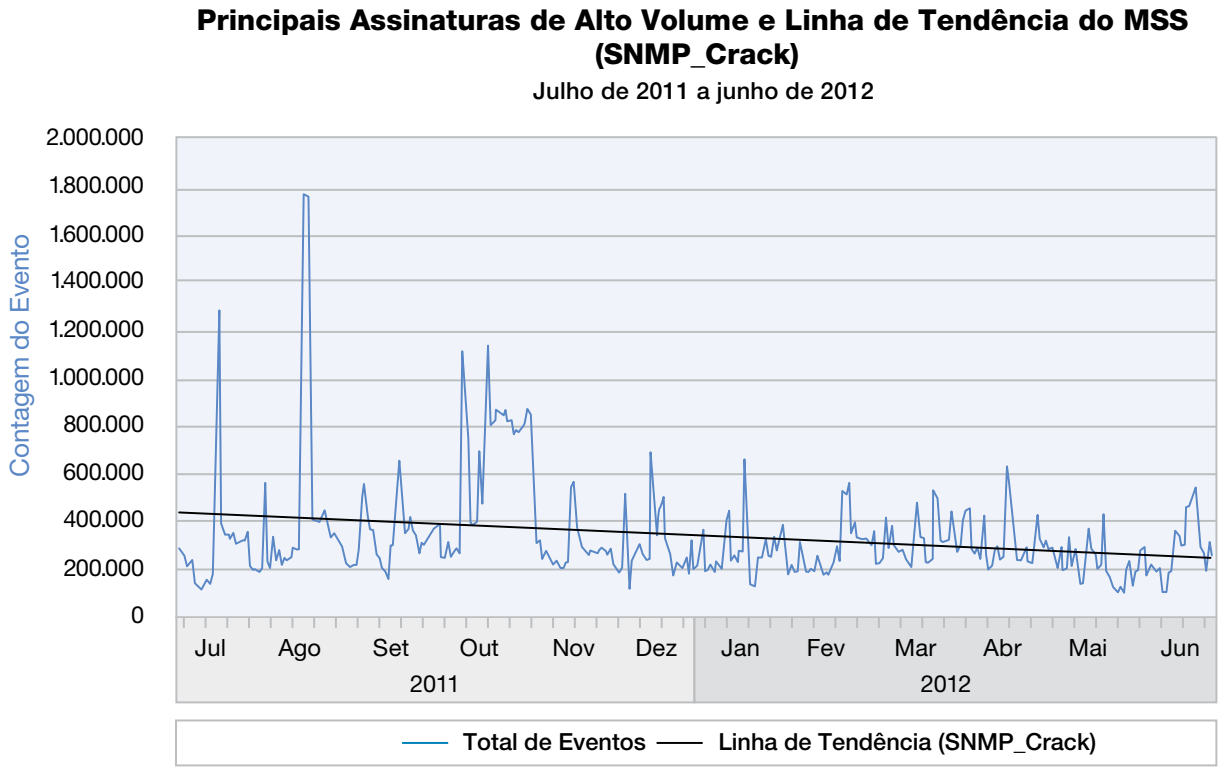


Figura 9: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (SNMP_Crack) - julho de 2011 a junho de 2012

Força bruta do SSH

Embora o crescimento desse evento tenha sido significativo no final de 2011, o nível de atividade parece ter alcançado um platô. Bastante semelhante à HTTP_Unix_Passwords, essa assinatura não é absolutamente indicativa de um ataque, mas requer atenção.

Devido à sua natureza, não é possível dizer se um ataque de força bruta ou estilo dicionário pode estar ocorrendo, pois todo o tráfego a ser examinado está criptografado. Portanto, essa assinatura está relacionada a um grande número de Identificações do Servidor de SHH ocorrendo em um curto período a partir de um endereço de origem específico. Dependendo da configuração, isso poderia ser um scanner de vulnerabilidade verificando um sistema, uma ferramenta verificando senhas fracas ou um ataque estilo dicionário de força bruta completo. Como não podemos ver dentro dos pacotes criptografados, não há nenhuma forma adequada de determinar a intenção de uma quantidade pequena de atividade. As contagens das solicitações de Identificação do Servidor tenderão a ser um indicador do tipo de comunicação sendo tentado, com altas contagens altamente suspeitas.

Nossas recomendações permanecem as mesmas: desative o login direto para contas privilegiadas, reforce a segurança da senha e do nome de usuário e considere a autenticação multifatores para sistemas particularmente sensíveis.

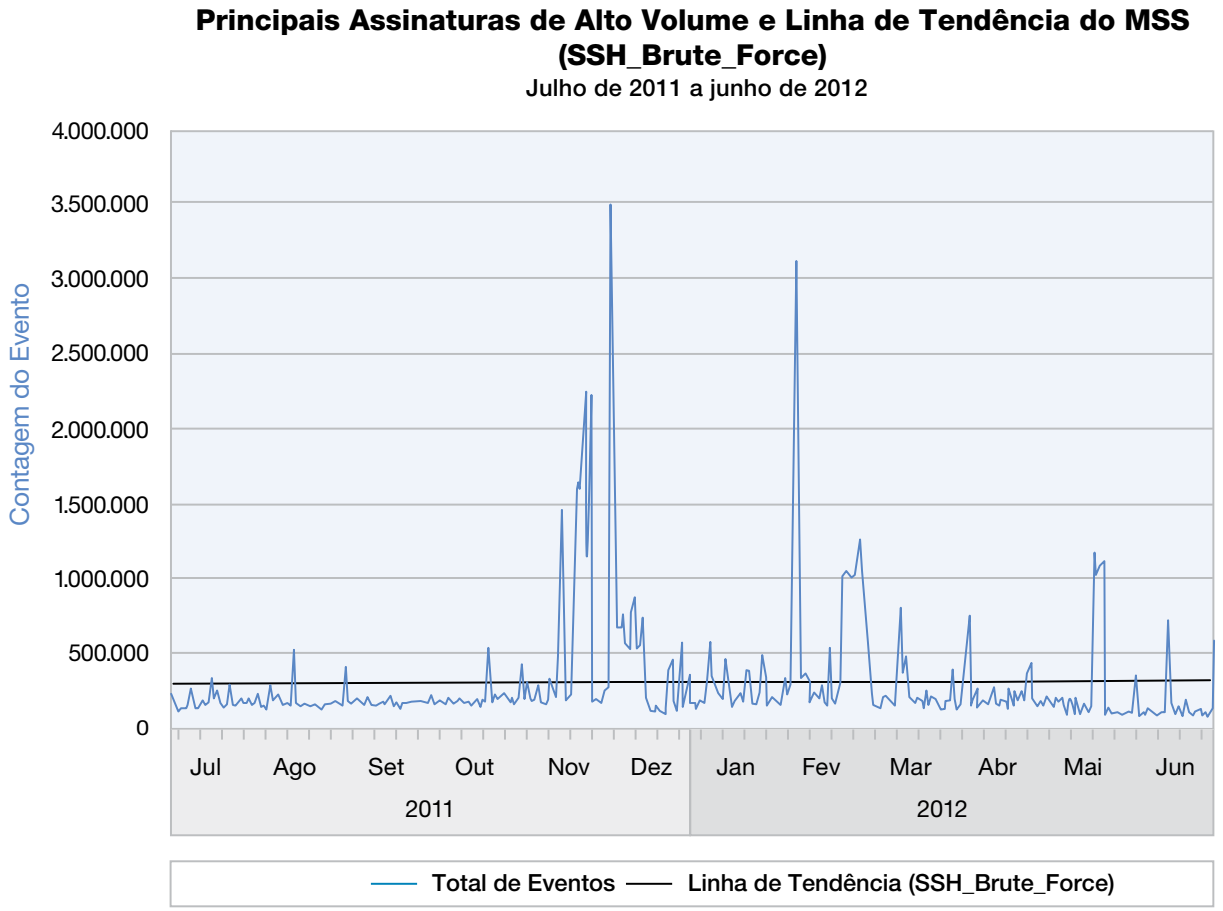


Figura 10: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (SSH_Brute_Force) - julho de 2011 a junho de 2012

Senhas Unix HTTP

A assinatura identifica as tentativas de acesso ao arquivo da senha (/etc/passwd e /etc/shadow) em sistemas Unix por meio do protocolo HTTP. Embora a assinatura HTTP_Unix_Passwords continue no topo da lista de alto volume, com uma tendência crescente, ela caiu da sexta posição em 2010 para a oitava em 2011. Permanece em oitavo lugar em 2012. Assim como em várias outras assinaturas, a contagem do evento continua crescendo, mas o número elevado de eventos adicionais de alto risco está ultrapassando essas assinaturas.

Relativamente falando, o ataque Senha Unix HTTP é antigo, mas continua sendo efetivo, que é parcialmente porque ele continua crescendo. As tentativas de obter acesso a /etc/passwd podem ser feitas por meio de vários protocolos, portanto, outras assinaturas, como HTTP_Unix_ Passwd_File_ Accessed ou FTP_Unix_Password_ File_Accessed, também podem estar presentes. Claramente, a obtenção de acesso aos arquivos de senha do sistema e a tentativa de romper essas proteções com ferramentas hash, rainbow tables ou ataques de força bruta ainda são consideradas buscas que valem a pena e resultam em resultados desejáveis para os invasores.

A assinatura HTTP_Unix_Passwords permanece no topo da lista de alto volume e continua sendo uma tendência crescente, atualmente em oitavo lugar.

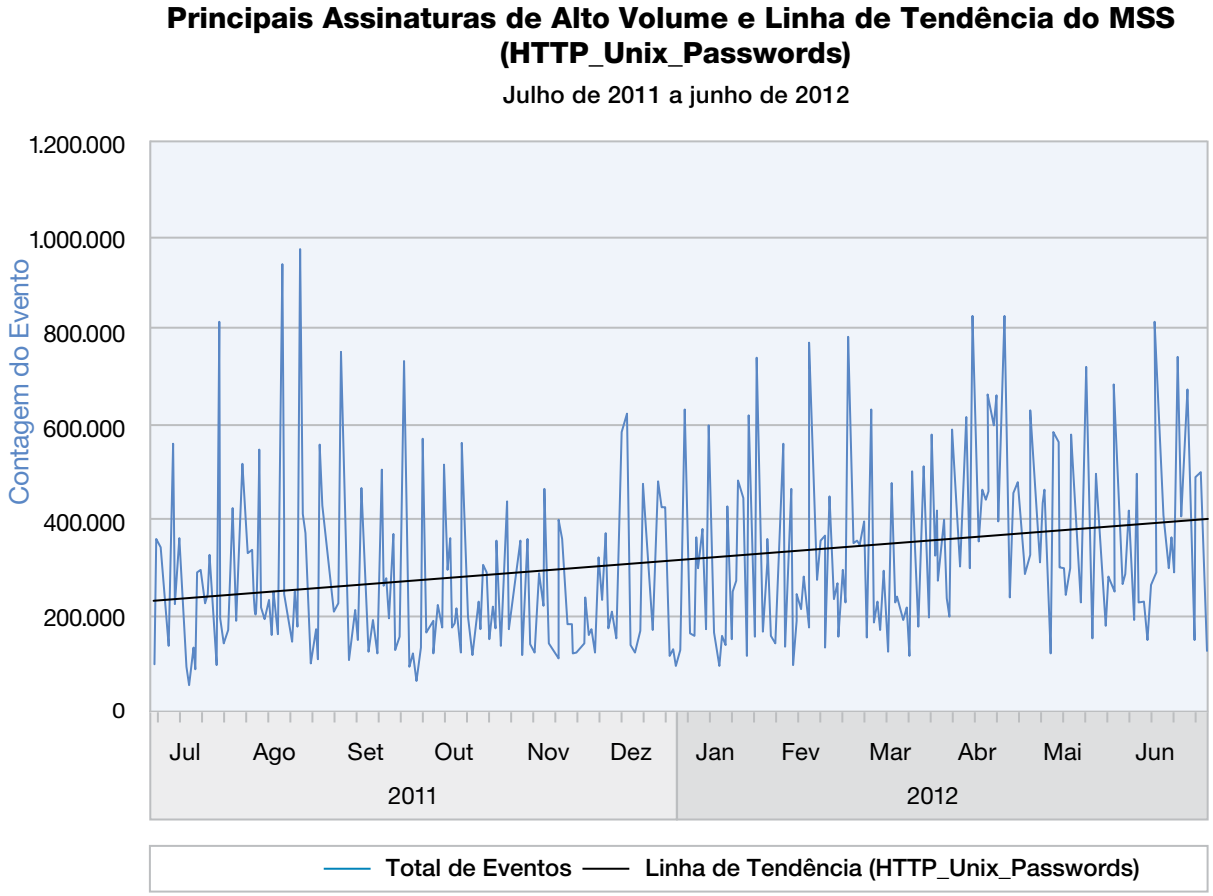


Figura 11: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (HTTP_Unix_Passwords) - julho de 2011 a junho de 2012

Injeção do comando shell

A Injeção do comando shell é uma forma de Execução de Comando Remoto (não deve ser confundida com a Execução de Código Remoto) que deve se tornar uma presença contínua em todos os tipos de clientes. Os Serviços Gerenciados de Segurança (MSS) estão observando um crescimento lento, mas bastante contínuo, dessas tentativas de ataque e antecipamos mais crescimento.

Assim como a SQL injection, essa é uma forma fácil de um invasor obter um ponto de apoio em um servidor. Assim que esse ponto de apoio for estabelecido, o invasor pode obter uma vantagem estratégica que fornece um ponto de partida para atacar outros sistemas de dentro das defesas do perímetro. A exploração é abrangente e frequentemente bem-sucedida. Máquinas já comprometidas executando PHP "falsos" (como o Shell C99) também tendem a serem expostas por meio da mesma heurística descrita abaixo. O C99 é uma ferramenta de administração remota que não é exclusivamente maliciosa, mas é frequentemente a preferida dos invasores, pois está prontamente disponível.

A assinatura Shell_Command_Injection é um conjunto de heurísticas para detectar tentativas de injeção do comando shell Unix classificando várias combinações de comandos e símbolos comumente utilizados ao executar comandos shell. Na configuração padrão, os comandos shell são classificados somente quando um parâmetro de ajuste for correspondente ou quando uma tentativa directory traversal for detectada. Nesses dois casos, uma tentativa é feita para classificar comandos shell e símbolos.

A principal defesa contra esse ataque é validar a entrada do usuário no servidor, eliminando comandos shell. A restrição ou a eliminação do acesso do software do servidor aos comandos shell (como wget, passwd, dir, ls, entre outros) também pode reduzir a efetividade desse ataque no caso de seu êxito.

Figura 12: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (Shell_Command_Injection) - julho de 2011 a junho de 2012

Retorno da exploração do navegador da web

Recentemente, identificamos um pico na exploração do navegador por meio do aumento de relatórios da assinatura JavaScript_Shellcode_ Detected. Essa assinatura detecta a transmissão do código da máquina codificado no JavaScript e considerado um código shell para explorar a vulnerabilidade que pode ou não já ser conhecida. Em outras palavras, isso faz parte da nossa abordagem "à frente da ameaça". Observamos números extremamente pequenos de falsos positivos com essa assinatura desde sua concepção, em 2006. O acionamento de um aumento dramático dessa assinatura se deve provavelmente a um crescimento nos kits de ferramentas de exploração do navegador da web. Por sua vez, isso pode ser devido a um aumento nas campanhas de ataque de aplicativos da web, procurando por servidores vulneráveis para servirem como links maliciosos e, em alguns casos, como o código malicioso real.

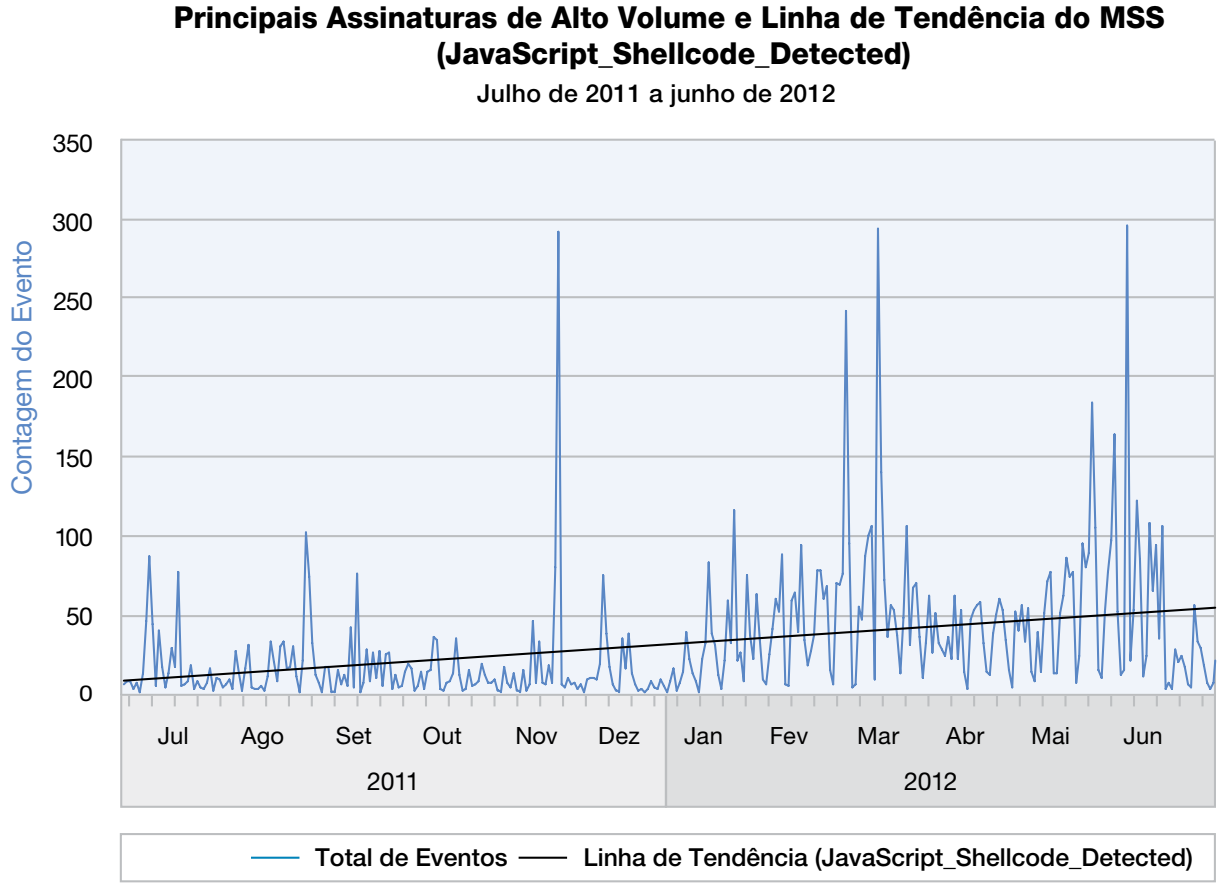


Figura 13: Principais Assinaturas de Alto Volume e Linha de Tendência do MSS (JavaScript_Shellcode_Detected) - julho de 2011

Evoluindo na escuridão – o brilho de um ataque?

Um dos vários recursos de dados que os analistas de segurança da IBM utilizam para determinar a tendência é uma darknet. Uma darknet é uma grande variedade de endereços IP na internet, nos quais nunca foram executados serviços. Uma darknet também é conhecida como uma rede de buraco negro ou um telescópio de rede. Nossa darknet possui uma abertura de 25.600 endereços. De um modo geral, não há motivo legítimo pelo qual os computadores na internet enviariam pacotes para abordar essa variedade, mas, na verdade, eles o fazem. O tráfego recebido nesse endereço é geralmente associado à atividade maliciosa. O espaço é continuamente monitorado e todo o tráfego recebido é captado em sua totalidade e armazenado para análise e arquivamento de longo prazo.

Ataques falsificados de negação de serviço

Ao observar os dados dos últimos anos, algumas tendências começam a emergir. A primeira tendência é o aumento gradual da atividade de retroespalhamento (Figura 14). O retroespalhamento é, na verdade, um efeito colateral dos ataques falsificados de negação de serviço (DoS). Invasores que lançam ataques de negação de serviço na internet geralmente inserem endereços de origem falsos nos pacotes enviados à vítima. Isso é conhecido como spoofing. Ao realizar o spoofing de endereços de origem selecionados aleatoriamente, o invasor dificulta que o sistema da vítima determine a origem de um ataque, a fim de bloqueá-lo de forma efetiva ou de distingui-lo entre os pacotes falsificados e pacotes legítimos de usuários reais. Isso é geralmente utilizado em ataques de negação de serviço e de negação de serviço distribuída (DDoS) para esconder a verdadeira origem de um ataque e evitar simples filtros de pacote. O sistema da vitima pode responder a esses pacotes falsificados como se eles fossem legítimos e enviar uma resposta aos endereços falsos, possivelmente mobilizando recursos em seus sistemas. Essas respostas são conhecidas como retroespalhamento. Se um invasor selecionar aleatoriamente um endereço IP em nossa variedade de darknet e a vítima responder, coletamos e arquivamos essa resposta. Ao estudar essas respostas e seus padrões, podemos aprender e controlar coisas sobre a atividade de negação de serviço na internet.

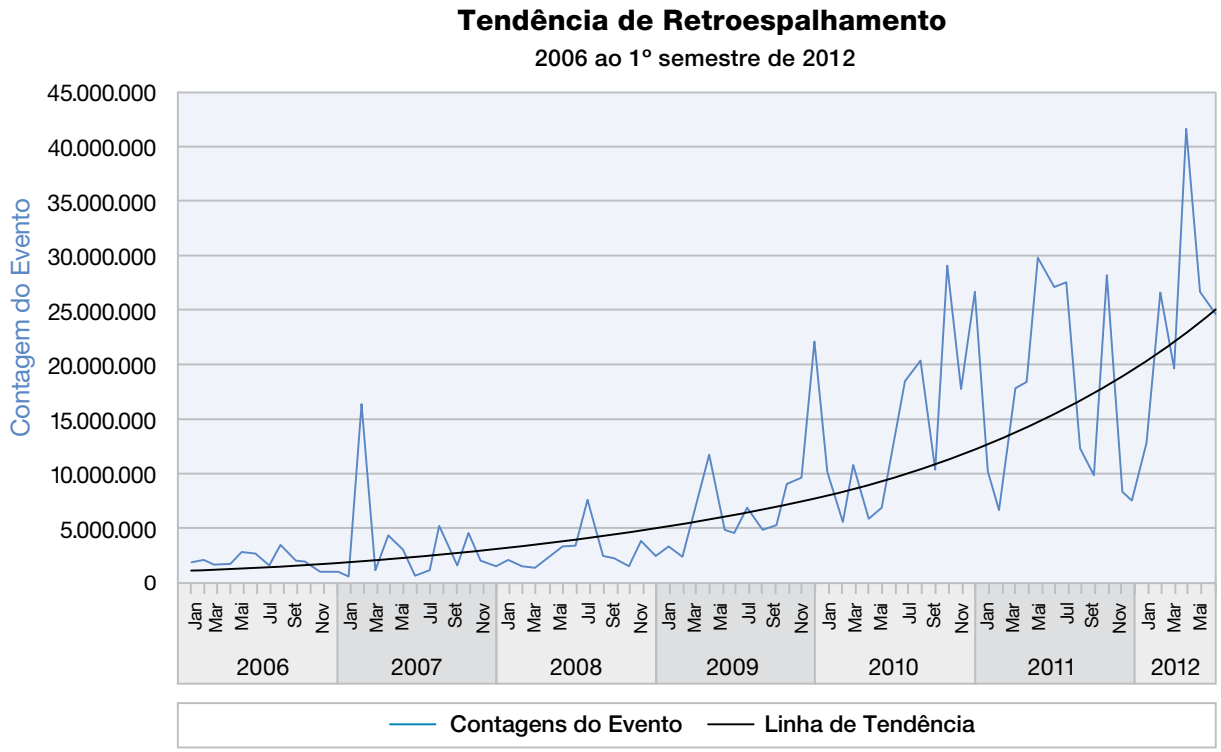


Figura 14: Tendência de Retroespalhamento - 2006 ao 1º semestre de 2012

Na darknet da IBM X-Force, cada pacote de retroespalhamento SYN-ACK (de resposta) recebido é provavelmente um indicador de que um invasor enviou um pacote SYN (de solicitação) falsificado a uma porta de serviço conhecida na máquina que está sendo atacada, falsificado a partir de um dos endereços da darknet da IBM X-Force. Embora tenha havido um aumento gradual da atividade de retroespalhamento desde 2006, houve um salto entre os anos 2008 e 2009. Parte desse aumento se deve a um pico significativo na atividade em 2009 – o maior, em termos de porcentagem, durante o período. Essa tendência de aumento do tráfego de retroespalhamento continuou em 2010 e em 2011, com outro grande salto em 2010. No fechamento do 2o trimestre de 2010, a contagem média do primeiro semestre de 2010 foi ligeiramente maior do que a média total para 2009, com um pouco mais de 16,5 milhões. No fechamento de 2010, observamos que esse número saltou para mais de 18 milhões. No primeiro semestre de 2011, observamos picos mensais de até 30 milhões. Embora o volume tenha caído um pouco no segundo semestre de 2011, 2012 vivenciou picos de retroespalhamento de até 42 milhões. A Figura 2 indica o aumento no volume anual de ataques falsificados de negação de serviço na internet de 2006 a 2011.

O que podemos deduzir desse aumento gradual e, em alguns casos, dos grandes saltos da atividade de retroespalhamento? Grande parte dos dados de retroespalhamento resulta de ataques de negação de serviço (DoS), portanto, podemos especular que houve um aumento constante de ataques falsificados de DoS desde 2066. No entanto, o retroespalhamento está sujeito a um alto grau de variabilidade devido à natureza do que é coletado e do que está ocorrendo. Alguns períodos intensos de retroespalhamento podem ser o resultado de conflito destruidor dentro de e entre vários campos do invasor. Durante esse conflito, um grupo pode tentar bloquear ou assumir os recursos do outro grupo. Esses "resultados de bombardeios" entre campos de guerra podem resultar em um aumento repentino do tráfego e dos endereços de origem de retroespalhamento. Ele geralmente cessa de forma tão repentina quanto começa. Esse tipo de atividade muito provavelmente contribuiu para os picos dramáticos em fevereiro de 2007, dezembro de 2009 e, mais recentemente, em abril de 2012, conforme mostrado na Figura 15.

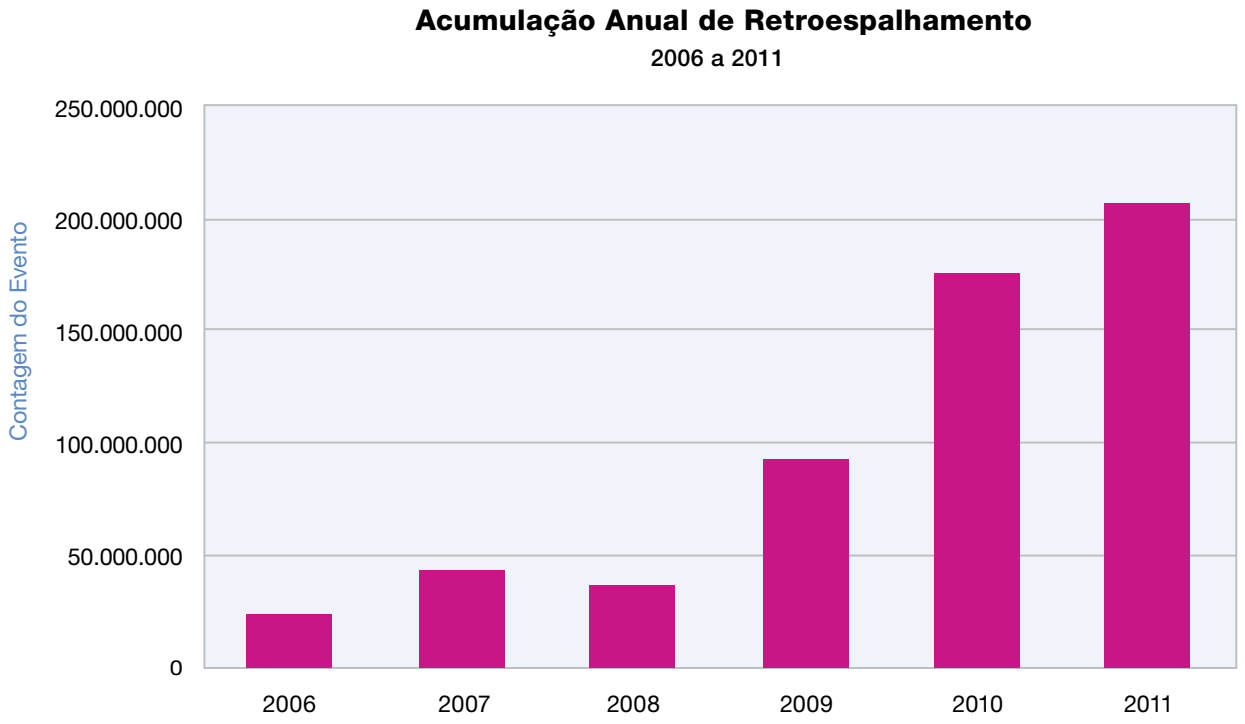


Figura 15: Acumulação Anual de Retroespalhamento - 2006 a 2011.

Alvos de ataques de negação de serviço

A natureza de um ataque falsificado de negação de serviço dificulta a determinação da origem do ataque. O invasor fabrica origens para as comunicações com o endereço IP da vítima. Essas conexões fabricadas podem, por sua vez, vir de uma série de endereços diferentes. Ao olhar para um retroespalhamento na darknet da IBM X-Force, é evidente que as origens do ataque são falsificadas, mas seu local-alvo pode ser determinado. A verificação das origens do retroespalhamento fornece informações sobre os alvos dos ataques falsificados de negação de serviço. A Figura 16 mostra os principais países-alvo que geraram retroespalhamento durante o primeiro semestre de 2012, conforme determinado utilizando o banco de dados WorldIP, que mapeia os endereços para os países.

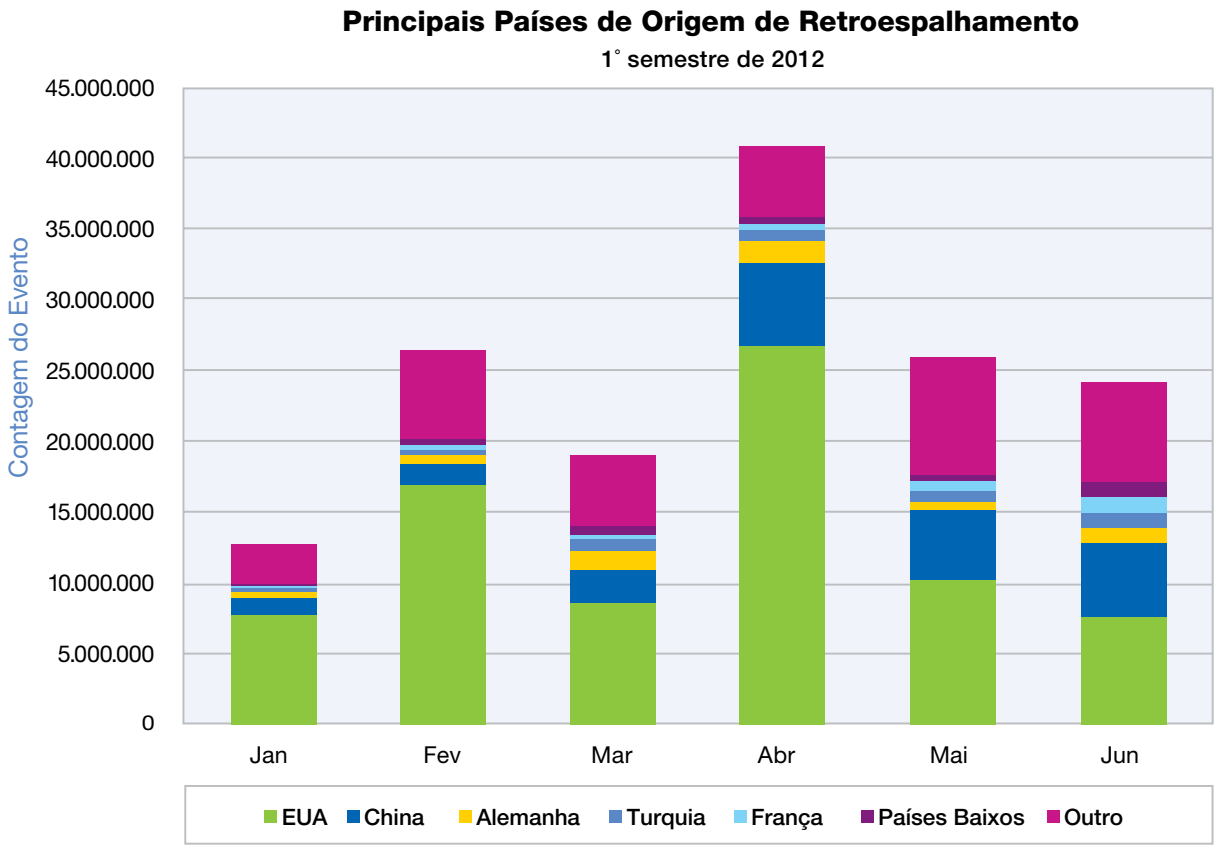


Figura 16: Principais Países de Origem de Retroespalhamento - 1o semestre de 2012

Há uma tendência bastante clara nos dados. Os Estados Unidos são, de longe, a principal origem; a China é a segunda e a Alemanha é um distante terceiro lugar. Outros países individuais estão ainda mais longe. Os Estados Unidos e a China possuem a primeira e a segunda maiores contagens de endereços IPv6 alocados, portanto, suas classificações como origens de retroespalhamento não são surpreendentes. Se qualquer endereço IP for tão provável de ser um alvo quanto qualquer outro, portanto, também seria esperado que Japão, Coreia do Sul e Reino Unido estivessem entre os cinco primeiros. No entanto, os ataques são altamente variáveis e podem ocorrer em qualquer lugar, como pode ser visto pelo grande número de ocorrências de "Outro", representando outros alvos que não sejam os principais países desse gráfico, e as contagens caem rapidamente depois dos EUA e da China.

Em muitos casos, a categoria "Outro" inclui países que podem ser determinados, mas que possuem contagens inferiores aos dos principais países, embora grande parte da categoria "Outro" contenha blocos de endereços para os quais informações precisas sobre o código do país não estão disponíveis. Vários endereços IPv6 na categoria "Outro" são endereços legados do início da internet, quando o rastreamento de dados não era tão limpo, mas que ainda representam uma parte considerável do espaço de endereços da internet.

Como a categoria "Outro" inclui o retroespalhamento coletado de todos os países, exceto os seis principais, identificados no gráfico, a altura total de cada uma das barras representa o tráfego de retroespalhamento total coletado. O grande pico em abril de 2012 claramente se destaca, juntamente com um pico menor em fevereiro de 2012. Esses picos são bem controlados por oscilações na atividade de retroespalhamento dos EUA, embora a correlação com o da China não seja tão clara, sendo que, em junho de 2012, os EUA e a China tiveram uma aproximação maior no tráfego de retroespalhamento.

Malware para Macs – grandes surtos e ataques direcionados

No último Relatório de Riscos e Tendências da IBM X-Force, discutimos a emergências de malwares para Macs. Também previmos que mais malwares para Macs surgiriam em 2012 e que eles serão cada vez mais semelhante à sua contraparte do Windows. Analisando o primeiro semestre de 2012, parece que estávamos certos.

Nos últimos meses, observamos alguns grandes desenvolvimentos no mundo de malwares para Macs: o surto do Flashback e a descoberta de malwares para Macs de ameaça avançada persistente (APT). Vamos dar uma olhada mais detalhada nesses desenvolvimentos.

Flashback

A primeira variante do Flashback foi descoberta em setembro de 2011. Várias variantes foram liberadas depois disso, mas as desse ano eram, de certa forma, especiais. Elas compartilham grande parte dos recursos das anteriores, mas o que as torna tão bem-sucedidas dessa vez é seu método de entrega.

Embora as variantes anteriores do Flashback dependessem de táticas de engenharia social para atrair os usuários a instalá-las, as mais recentes também utilizaram técnicas drive-by-download comuns no mundo de malwares para Macs. O Flashback alcançou isso por meio de sites de blog do Wordpress que foram modificados para hospedar links diretos que contêm as explorações.

No último relatório, mencionamos que a dificuldade técnica em explorar o software OSX é um grande fator na prevenção da exploração em massa. O Flashback resolve isso utilizando explorações multiplataforma por meio de vulnerabilidades do Java. Isto é, a técnica de exploração e grande parte do código envolvido são os mesmos, independentemente se o alvo é Windows ou Mac.

O Flashback utilizou duas explorações Java pela primeira vez em fevereiro, a CVE-2011-3544 (Vulnerabilidade do Mecanismo de Scripts do Java Applet Rhino) e a CVE-2008-5353 (Vulnerabilidade de Desserialização do Calendário do Java), mas essas explorações foram corrigidas na época e, portanto, essa variante nunca chegou a ser uma infecção generalizada. No entanto, as coisas mudaram quando, em março, o Flashback começou a utilizar uma exploração CVE-2012-0507 (Vulnerabilidade de Violação Tipo AtomicReferenceArray do Java). Essa vulnerabilidade já havia sido corrigida pela Oracle no mês anterior, mas a versão da Apple do Java ainda não havia sido atualizada, deixando muitas máquinas Mac vulneráveis a essa exploração. A infecção em massa resultante foi enorme e o Flashback se tornou o malware mais difundido para Macs até então. Alguns fornecedores de segurança definiram sumidouros para determinar o número de infecções do Flashback e as estimativas são de até 600.000 máquinas.

O surto do Flashback também esclareceu o principal objetivo desse malware, que é obter renda por meio de click-jacking. Depois de ser instalado, o Flashback é vinculado ao navegador e intercepta tanto um acesso de anúncio online quanto uma procura do Google. Caso um anúncio do Google seja acessado, os parâmetros de consulta são enviados ao servidor Command and Control (C&C), em vez de um servidor do Google. Caso uma procura do Google seja detectada, os parâmetros de procura são enviados ao servidor C&C, que responde com as próprias URLs pay-per-click do autor do Flashback, em vez dos resultados reais de procura do Google.

APT para Mac

Outro grande desenvolvimento em malwares para Macs no primeiro semestre do ano é a descoberta de malwares direcionados.

Primeiro, há o malware do Tibet, descoberto em março. As primeiras variantes utilizavam a exploração Java CVE-2011-3544 (Vulnerabilidade do Mecanismo de Scripts do Java Applet Rhino), também utilizada pelo Flashback, para espalhar. Seu principal objetivo é copiar e efetuar o download dos

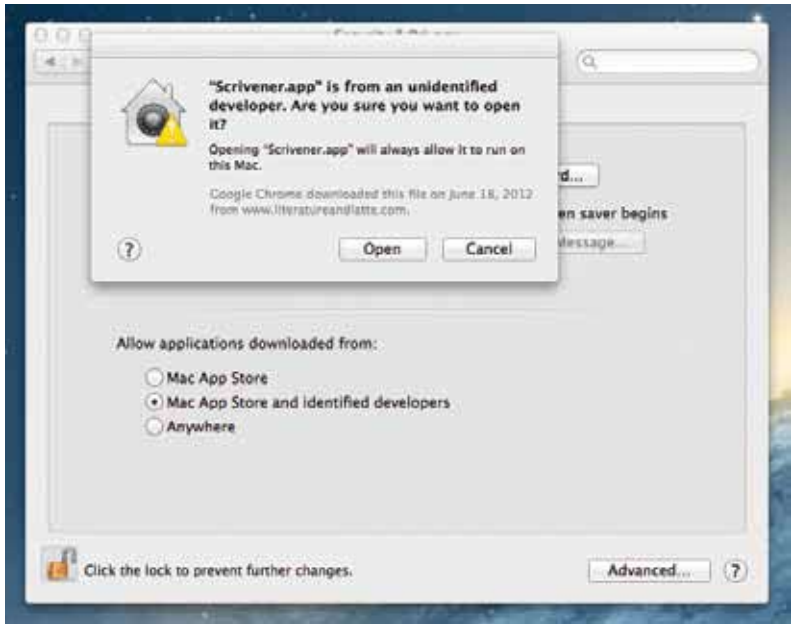
dados de um usuário. Foi espalhado por meio de links em emails que eram especificamente destinados a organizações não governamentais (ONGs) do Tibet. As próximas variantes utilizam um método diferente de entrega. Essas variantes utilizam uma vulnerabilidade do MS Word, a CVE-2009-0563 (Vulnerabilidade de Estouro de Buffer de Análise de Registros do MS Word). Essa vulnerabilidade foi corrigida em 2009. Ela afeta as versões 2004 e 2008 do Word para Mac, mas não afeta o Word para Mac 2011. Os arquivos de documento do Word continham textos que discutiam a situação política do Tibet, o que levou os pesquisadores a especularem o fato de que, assim como na primeira variante, seu alvo eram ONGs do Tibet.

Outro ataque de malwares direcionados é o backdoor SabPub, descoberto pela primeira vez em abril. A primeira variante não mostrou inicialmente nenhum sinal de que fosse um ataque direcionado, embora houvesse relatórios de emails apontando para URLs que a hospedaram. Esse malware utiliza a mesma exploração Java que o Flashback, a CVE-2012-0507 (Vulnerabilidade de Violação Tipo AtomicReferenceArray do Java). A vulnerabilidade já foi corrigida, portanto, ela não teve tanto impacto quanto a variante do Flashback, que utilizou a mesma exploração quando foi liberada pela primeira vez. A próxima variante é semelhante ao malware do Tibet, pois é enviada utilizando a mesma exploração do documento do Word. Quanto ao malware do Tibet, o documento do Word exibe o texto em tibetano.

Conclusão

O surto de malwares do Flashback definitivamente colocou um fim à antiga crença de que Macs não são suscetíveis a malwares. Chegamos a um ponto em que qualquer coisa que venha a seguir não será mais tão surpreendente. Na verdade, no momento da redação deste documento, um novo backdoor para Mac denominado Crisis havia acabado de ser descoberto e apresentava recursos antirreversão e de rootkit. O Crisis é o tipo de malware previsto em nosso último Relatório de Riscos e Tendências da IBM X-Force.

Recentemente, a Apple lançou o OS X Mountain Lion, que inclui recursos de segurança, como o Gatekeeper e atualizações de segurança automáticas. Desde junho de 2012, a Apple requer que todos os aplicativos enviados para a App Store do Mac tenham o ambiente de simulação capacitado. Essas são grandes etapas para ajudar a evitar a mesma infecção em massa que experimentamos com o Flashback, mas ainda veremos como essas melhorias impedirão malwares no futuro.



Tendências do conteúdo da web

O datacenter de conteúdo da IBM constantemente revisa e analisa os novos dados do conteúdo da web e analisa 150 milhões de novas páginas da web e de imagens por mês. O datacenter analisou 17 bilhões de páginas da web e de imagens desde 1999.

O banco de dados do filtro da web da IBM apresenta 68 categorias de filtro e 71 milhões de entradas com 150.000 entradas novas ou atualizadas incluídas por dia.

Esta seção oferece uma revisão dos seguintes itens:

- Metodologia de análise
- Implementação do IPv6 para websites
- Proxies anônimos
- Websites maliciosos

Metodologia de análise

A IBM X-Force captura informações sobre a distribuição de conteúdo na internet contando os hosts categorizados no banco de dados do filtro da web da IBM Security Systems. A contagem de hosts é um método aceitável para a determinação da distribuição de conteúdo e fornece uma avaliação realista.

Ao utilizar outras metodologias – como a contagem de páginas da web e de subpáginas – os resultados podem ser diferentes.

Implementação do IPv6 para websites

A fim de medir a implementação do IPv6 para websites, executamos solicitações de DNS (para verificar um registro AAAA no DNS) para milhões de hosts toda semana. À medida que o IPv4 fica sem espaço, esperamos que sites da internet mudem cada vez mais para o IPv6. Entretanto, quando observamos os números até maio de 2012, essa expectativa não foi alcançada. No entanto, em junho, observamos um aumento significativo e a porcentagem de domínios com no mínimo um host suportando o IPv6 chegou aos 3% pela primeira vez.

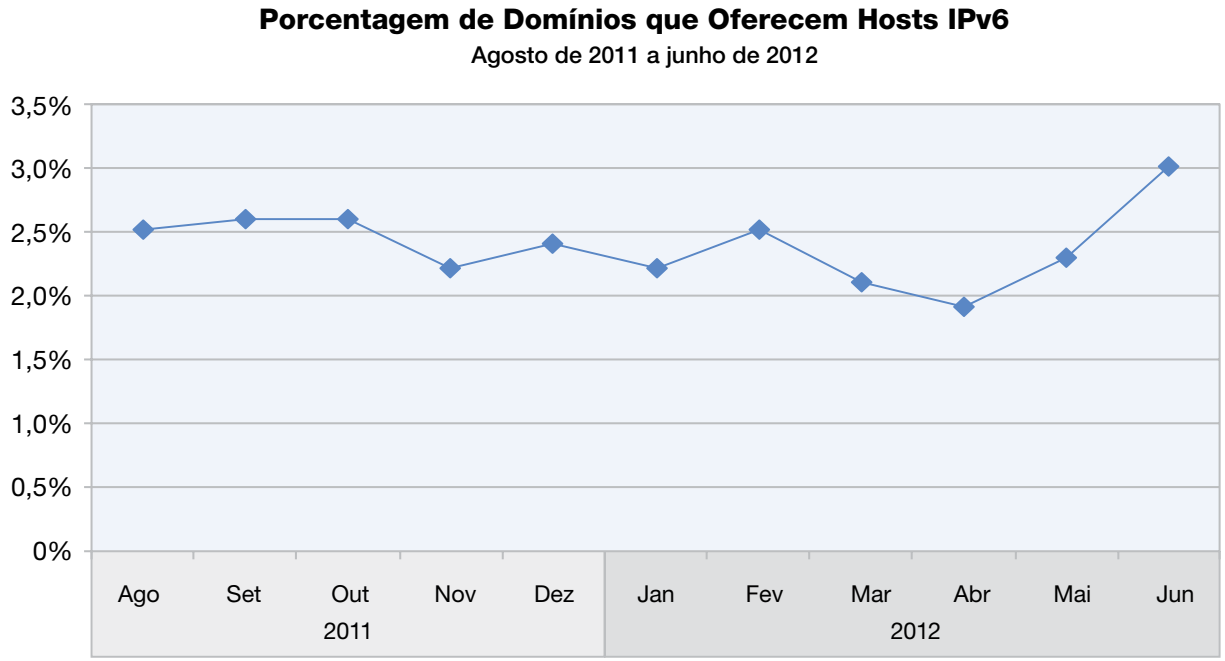


Figura 17: Porcentagem de Domínios que Oferecem Hosts IPv6 - agosto de 2011 a junho de 2012

A fim de analisar esse aumento, vamos dar uma olhada mais detalhada nos números de maio a junho de 2012.

A mudança ocorreu na semana 23. No meio dessa semana (6 de junho), foi realizado o 2012 IPv6 Day[1] . Neste ano, várias empresas e organizações executaram implementações permanentes do IPv6. A Figura 18 demonstra isso claramente.

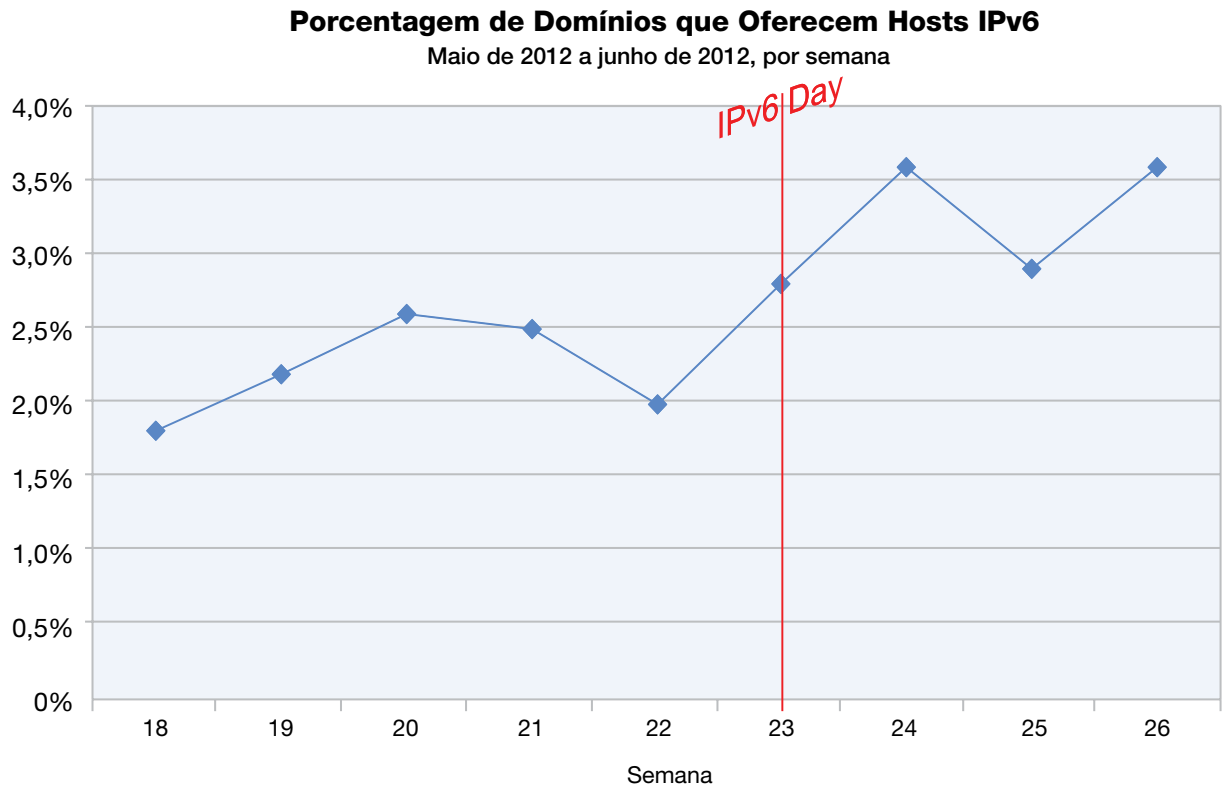


Figura 18: Porcentagem de Domínios que Oferecem Hosts IPv6 - maio a junho de 2012, por semana

1 Visite http://en.wikipedia.org/wiki/World_ipv6_day

Os domínios que fornecem no mínimo um host de apoio do IPv6 podem ser denominados "prontos para IPv6". Quando observamos os tipos de categorias[2] para websites prontos para IPv6, surge outra tendência interessante.

- Sites do Web 2.0, além de organizações governamentais, são as áreas mais prontas para IPv6 da internet.
- Muitas organizações não governamentais, mecanismos de busca, portais, sites de TI, sites de notícias e blogs são bem-preparados.
- Sites de consumidores, como correios da web clássicos, sites de esportes, de jogos de computadores, de compras e de encontros, ainda estão acima da média de 3% (a média em junho, de acordo com o gráfico).
- Websites com conteúdo, como sites de drogas ilegais, proxies anônimos, sites de pornografia e de jogos são particularmente não prontos para IPv6.
- URLs de spams representam a parte inferior da liga.

Disponibilidade Acima da Média	% de "prontos para IPv6"	Disponibilidade Abaixo da Média
Mídia Social	29,7%	
Redes Sociais	26,2%	
Organizações Governamentais	14,5%	
Storage da Web	9,3%	
Organizações Não Governamentais	9,3%	
Mecanismos de Busca / Catálogos da Web / Portais	9,3%	
Bate-papo	8,6%	
Software / Hardware	8,3%	
Notícias / Revistas	8,3%	
Blogs / Quadros de Avisos	7,5%	
Correio da Web	6,5%	
Educação	6,0%	
Esportes	5,7%	
Jogos de Computador	5,5%	
Compras	5,5%	
Encontros	4,8%	
	3,6%	Warez / Hackeamento / Crime de Computador
Financeiro	3,3%	
	2,8%	Drogas Ilegais
Negócios em Geral	2,5%	
Viagens	1,7%	
	1,4%	Atividades Ilegais
	1,3%	Proxies anônimos
	1,3%	Malware
	1,1%	Pornografia
	1,1%	Violência / Extremos
	0,8%	Jogos / Loteria
	0,5%	URLs de Spams

Tabela 2: Porcentagem de websites prontos para IPv6 por categoria - junho de 2012

2 Para uma descrição detalhada das categorias de website acima, visite http://filterdb.iss.net/categories/

Por que os maus elementos descartam a tecnologia IPv6? Uma resposta pode ser que muitos dos websites indesejados existem apenas durante algumas horas. Isso é principalmente verdade para URLs de spams, portanto, essas pessoas podem querer evitar qualquer esforço técnico adicional. Além disso, os spammers desejam alcançar o maior número de usuários possível, portanto, não há necessidade de suporte ao IPv6, pois todo mundo "entende a linguagem" do IPv4, mas somente alguns grupos conseguem "entender a linguagem" do IPv6.

Será interessante ver se há um aumento significativo no suporte ao IPv6 nos próximos meses e anos.

Proxies anônimos

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 nesses locais públicos cada vez mais acham necessário controlar os locais nos quais as pessoas podem navegar.

Um desses controles é um sistema de filtragem de conteúdo, que evita o acesso a websites inaceitáveis ou inadequados. Alguns indivíduos tentam utilizam proxies anônimos (também conhecidos como proxies da web) para evitar essas tecnologias de filtragem da web.

Os proxies da web permitem que os usuários insiram uma URL no formato da web, em vez de visitar o website-alvo diretamente. O uso do proxy esconde a URL-alvo de um filtro da web. Caso o filtro da web não esteja configurado para monitorar ou bloquear proxies anônimos, essa atividade (que seria normalmente interrompida) evita o filtro e permite que o usuário chegue ao website não permitido.

O crescimento de websites de proxy anônimo registrados recentemente reflete essa tendência.

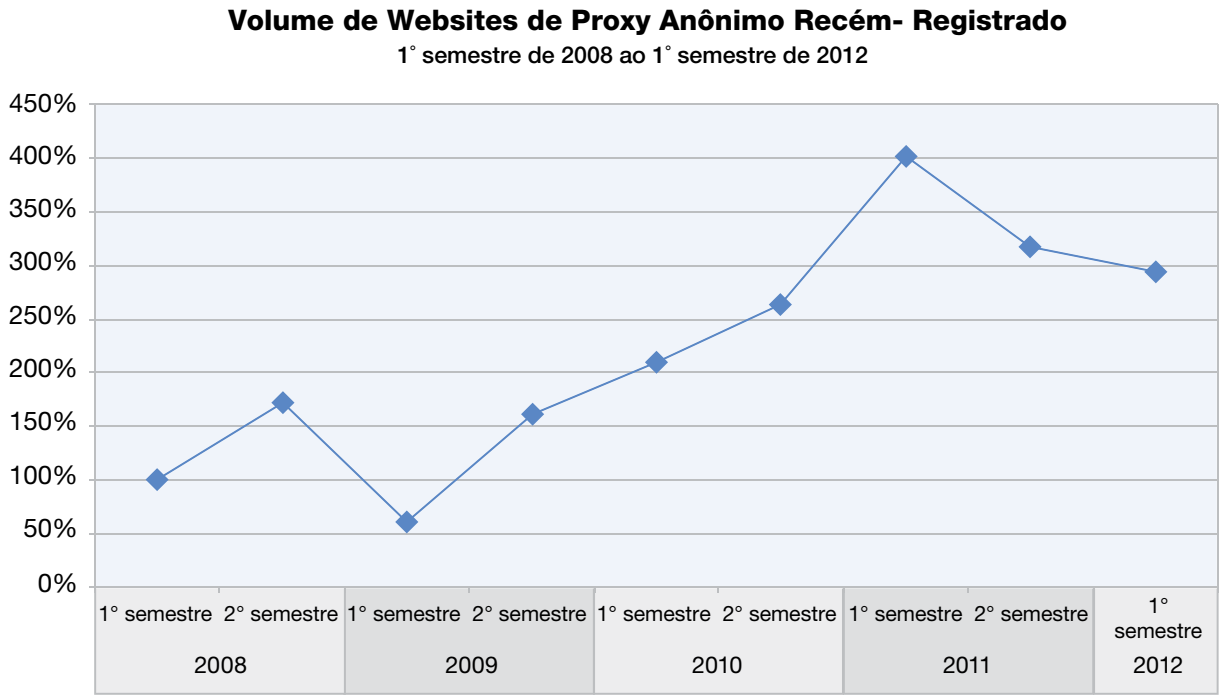


Figura 19: Volume de Websites de Proxy Anônimo Recém-Registrado - 1o semestre de 2008 ao 1o semestre de 2012

Foram registrados quatro vezes mais proxies anônimos no primeiro semestre de 2011, em comparação a três anos atrás. No segundo semestre de 2011 e no primeiro semestre de 2012, ainda houve cerca de três vezes mais proxies anônimos recém-registrados, em comparação a três anos atrás. Mais uma vez, não vimos outro aumento desse volume. Talvez as atividades da internet estejam mais focadas em redes sociais. Em vários casos, esses sites não são bloqueados no trabalho ou em escolas, portanto, as pessoas não precisam mais burlar o sistema de filtragem de conteúdo.

No entanto, o uso de plataformas de redes sociais gera um novo desafio, especialmente para empresas que precisam controlar quais informações são compartilhadas com outros usuários e que precisam impedir o compartilhamento de informações confidenciais. Portanto, muitas empresas estão começando a utilizar sistemas de controle de aplicativos da web, geralmente como parte da próxima geração de firewalls.

Proxies anônimos continuam sendo um tipo essencial de website a ser rastreado, devido à facilidade com a qual eles permitem que as pessoas escondam intenções possivelmente maliciosas.

Domínios de proxies anônimos de nível superior Há apenas um grupo de domínios de nível superior em uso por websites de proxies anônimos. Até o final de 2009, os domínios .com e .info eram dominantes, totalizando mais de 70% de todos os proxies anônimos. Isso mudou desde o final de 2009, quando o domínio .cc (o domínio de nível superior das Ilhas Cocos (Keeling), um território australiano) foi inserido no mercado e, em seguida, o domínio .tk (o domínio de nível superior de Tokelau, um território da Nova Zelândia) foi inserido no mercado no segundo trimestre de 2010.

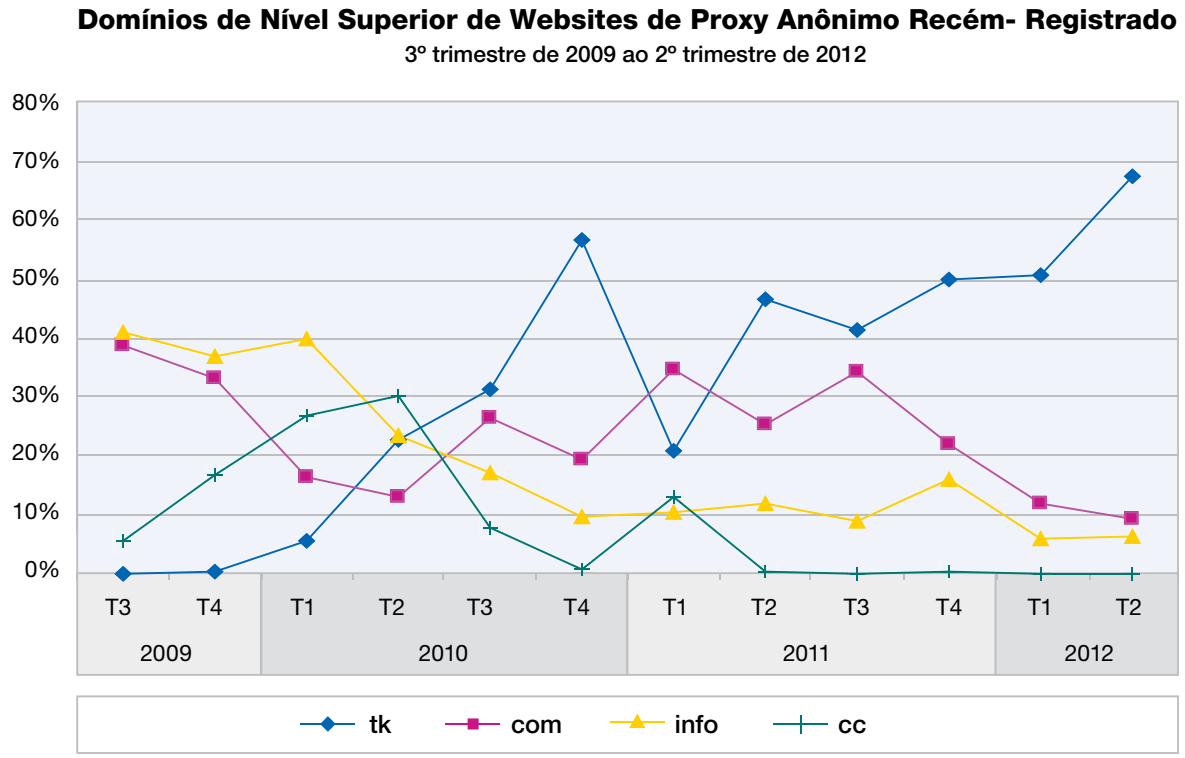


Figura 20: Domínios de Nível Superior de Websites de Proxy Anônimo Recém-Registrado - 3o trimestre de 2009 ao 2o trimestre de 2012

Conforme discutido no Relatório de Riscos e Tendências da IBM X-Force anterior, os domínios desses domínios de nível superior são gratuitos[3]. Portanto, hoje, observamos menos de 10% de todos os proxies anônimos utilizando o domínio .info. O mesmo é verdade para o domínio .com. No segundo trimestre de 2012, mais de dois terços de todos os proxies anônimos eram executados no domínio .tk.

Websites maliciosos

Esta seção discute os países que são responsáveis pela hospedagem de links maliciosos e também discute os tipos de websites que são geralmente ligados a esses websites maliciosos.

Localização geográfica de links da web maliciosos

Os Estados Unidos continuam sendo o principal host de links maliciosos. Mais de 43% de todos os links maliciosos são hospedados nos EUA. A Alemanha é o novo segundo lugar e hospeda 9,2%. A Rússia aparece entre os três primeiros pela primeira vez. A China era um dos dois principais até 2010, mas agora está em quarto lugar. A França hospeda 4% dos links de malwares. A Romênia teve dois anos fortes, em 2010 e 2011, quando chegou aos 8%, mas caiu para 1,1%.

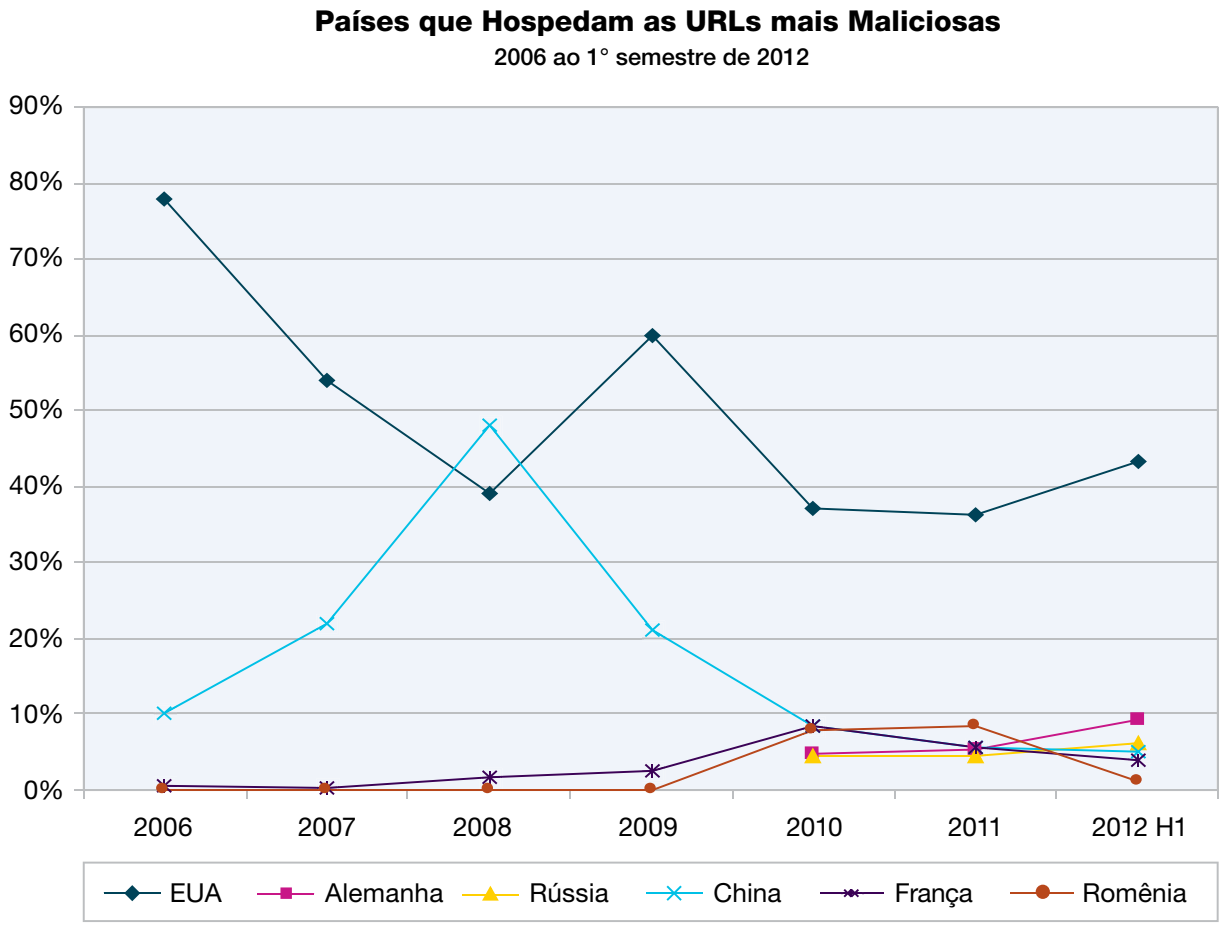


Figura 21: Países que Hospedam as URLs mais Maliciosas - 2006 ao 1o semestre de 2012

3 Visite http://www.co.cc/?lang=en and http://www.dot.tk/

Bons websites com links ruins

Conforme mencionado em vários pontos do nosso relatório e em relatórios anteriores, os invasores visam cada vez mais o uso do nome de websites confiáveis para abaixar a guarda dos usuários finais e esconder suas tentativas utilizando tecnologias de proteção. O uso de conteúdo da web malicioso não é diferente. A análise abaixo oferece uma visão sobre os tipos de websites que mais frequentemente contêm links para conteúdo malicioso e conhecido.

Algumas das principais categorias podem não ser surpreendentes. Por exemplo, pode-se esperar que pornografia e jogos estejam no topo da lista. Juntos, eles agora compõem aproximadamente 50% de todos os links maliciosos. No entanto, os candidatos da segunda camada se enquadram na categoria de mais "confiáveis".

Blogs, quadros de avisos, websites pessoais e mecanismos de busca se enquadram nessa categoria de segunda camada. Grande parte desses websites permite que os usuários efetuem o upload do conteúdo ou desenvolvam seus próprios websites. Em outras palavras, é improvável que esses tipos de websites estejam hospedando links maliciosos de forma intencional.

O gráfico abaixo mostra o histórico da distribuição de links de malwares.

Ao analisar os últimos três meses e meio, surgem tendências interessantes.

- Websites, como sites de pornografia e de jogos, foram claramente dominantes durante mais de um ano e distribuíram malwares de forma sistemática.
- Sites de pornografia eram um dos principais e representavam mais de um terço de todos os links maliciosos.
- Sites de jogos vivenciaram uma queda em malwares pela primeira vez, mas ainda representam cerca de 13% de todos os links de malware. Embora menos de 0,6% da população adulta tenha problemas com jogos[4], sites de jogos são um alvo popular para distribuidores de malwares.
- Blogs e quadros de avisos tiveram uma queda de 7,6% nos últimos seis meses.
- Páginas pessoais – os websites clássicos do Web 1.0 – continuaram perdendo espaço. Um motivo pode ser que as páginas pessoais saíram de moda devido a aplicativos Web 2.0, como perfis em redes sociais ou de negócios.
- Malwares de mecanismos de busca, catálogos da web e portais diminuíram para 5,1%.

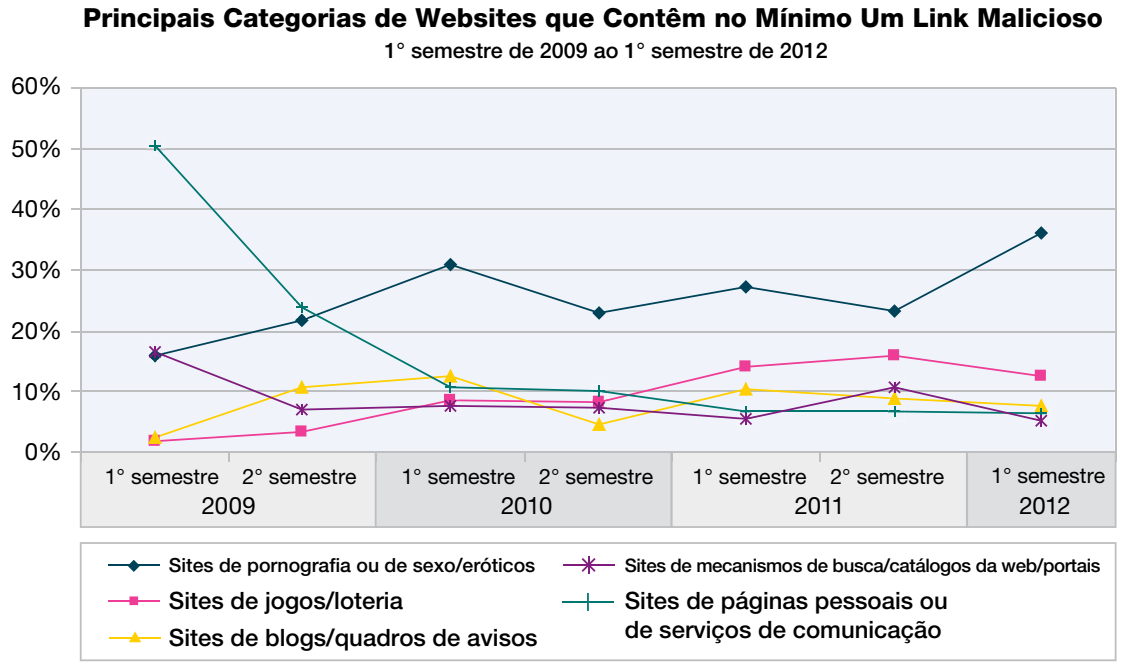


Figura 22: Principais Categorias de Websites que Contêm no Mínimo Um Link Malicioso - 1° semestre de 2009 ao 1° semestre de 2012

4 Visite http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence

Spam e phishing

O banco de dados de filtro de spams e de URLs da IBM oferece uma visão de abrangência mundial de ataques de spam e phishing. Com milhões de endereços de email sendo monitorados de forma ativa, a equipe de conteúdo identificou inúmeros avanços nas tecnologias de spam e phishing utilizadas pelos invasores.

Atualmente, o banco de dados do filtro de spams contém mais de 40 milhões de assinaturas de spam relevantes. Cada parte do spam é dividido em várias partes lógicas (frases, parágrafos, etc.). Uma assinatura exclusiva de 128 bits é computada para cada parte e para milhões de URLs de spams. Todo dia, há aproximadamente um milhão de assinaturas novas, atualizadas e excluídas para o banco de dados de filtro de spams. As atualizações são fornecidas a cada cinco minutos.

Esta seção aborda os seguintes tópicos:

- Volume de spams estabilizado em um nível baixo
- Principais tendências de spam nos últimos 12 meses
- Domínios de nível superior comuns em spams da URL
- Tendências do país[5] de origem do spam
- Atividades de finais de semana de spammers
- Fim da botnet em julho de 2012
- Scam e phishing de emails

Volume de spams estabilizado em um nível baixo

No segundo e terceiro trimestres do último ano, observamos os mesmos níveis de spam que no início de 2009. Após um breve aumento em setembro de 2011, o volume diminuiu para os níveis do segundo trimestre de 2011. No primeiro semestre de 2012, não houve grandes mudanças e o volume de spams estabilizou nesse nível baixo.

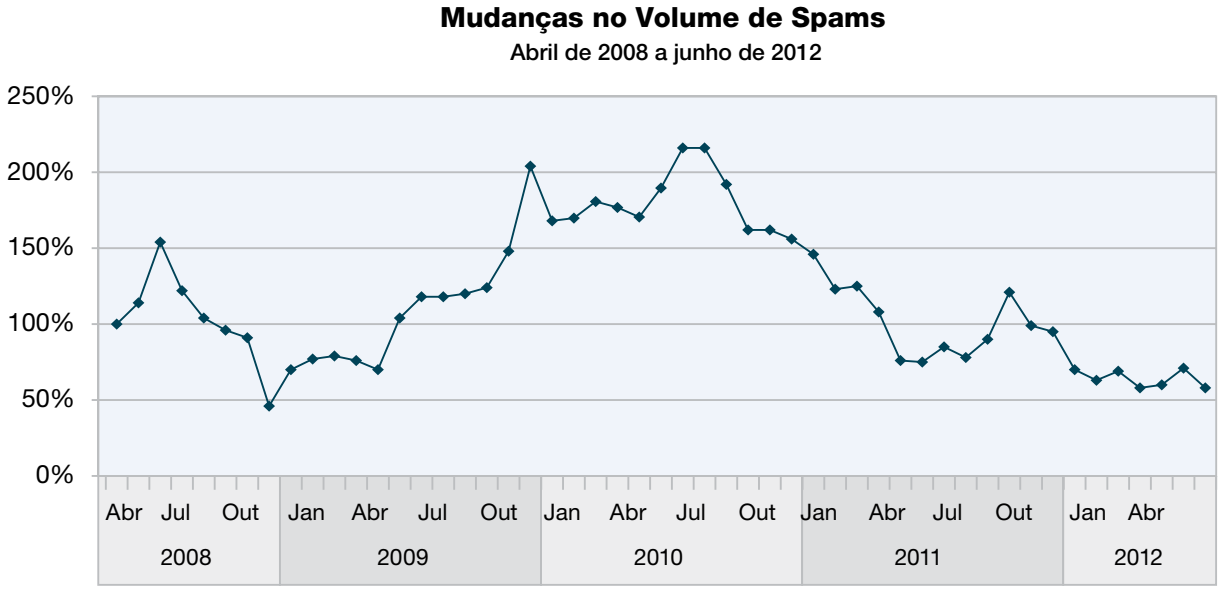


Figura 23: Mudanças no Volume de Spams - abril de 2008 a junho de 2012

5 As estatísticas deste relatório para spams, phishings e URLs utilizam o Banco de Dados IP-to-Country fornecido por WebHosting.Info (http://www.webhosting.info), disponível em http://ip-to- country.webhosting.info. A distribuição geográfica foi determinada solicitando os endereços IP dos hosts (no caso de distribuição do conteúdo) ou do servidor de envio de emails (no caso de spam e phishing) para o Banco de Dados IP-to-Country.

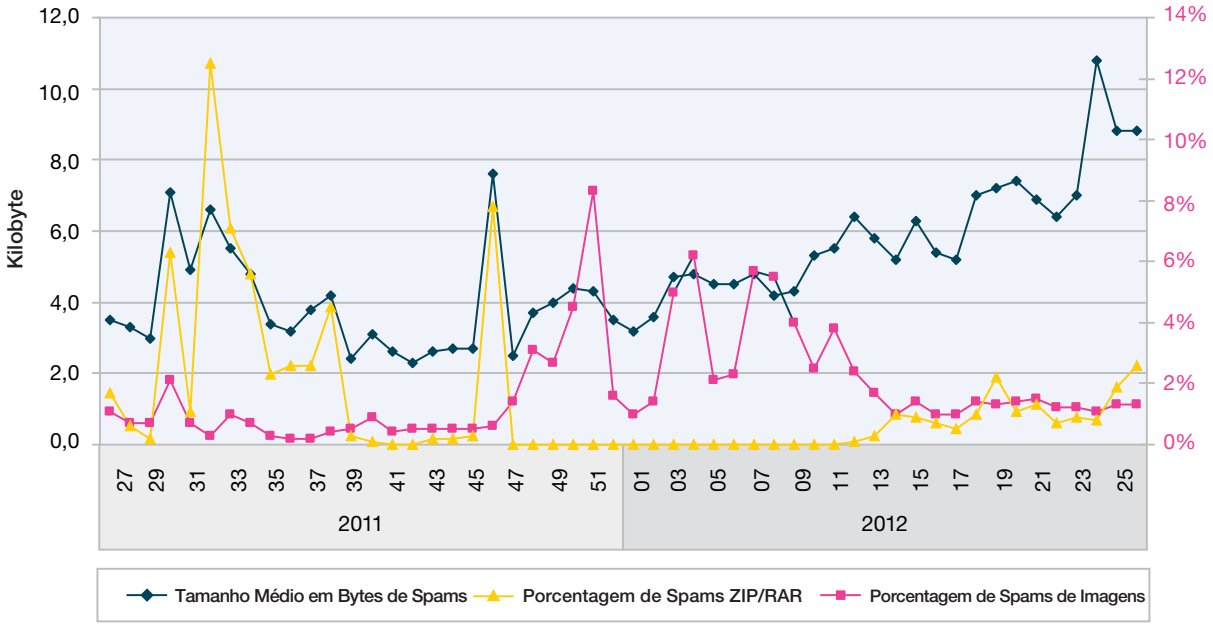
Principais tendências de spam nos últimos 12 meses

O gráfico abaixo resume as principais tendências de spam observadas desde julho de 2011, por meio de três parâmetros.

- **Spams de imagens:** No final de 2011, observamos o renascimento de spams baseados em imagens. Os spammers continuaram utilizando esse tipo de spam até o final de março de 2012. Às vezes, mais de 8% de todos os spams continham um anexo de imagem. Tecnicamente, não houve nenhuma mudança em comparação aos spams de imagens de dezembro de 2011.
- **Spams ZIP/RAR:** No segundo semestre de 2011, observamos várias ameaças de spams ZIP/RAR. Tantos os spams de imagens quanto os ZIP/RAR foram discutidos em detalhes no Relatório de Riscos e Tendências da IBM X-Force. No primeiro trimestre de 2012, não houve nenhuma ameaça. Elas voltaram a ocorrer em abril de 2012, mas em um nível bem mais inferior. Tecnicamente, não houve nada de novo nesses anexos ZIP ou RAR. Obviamente, eles substituíram os spams de imagens do primeiro trimestre.

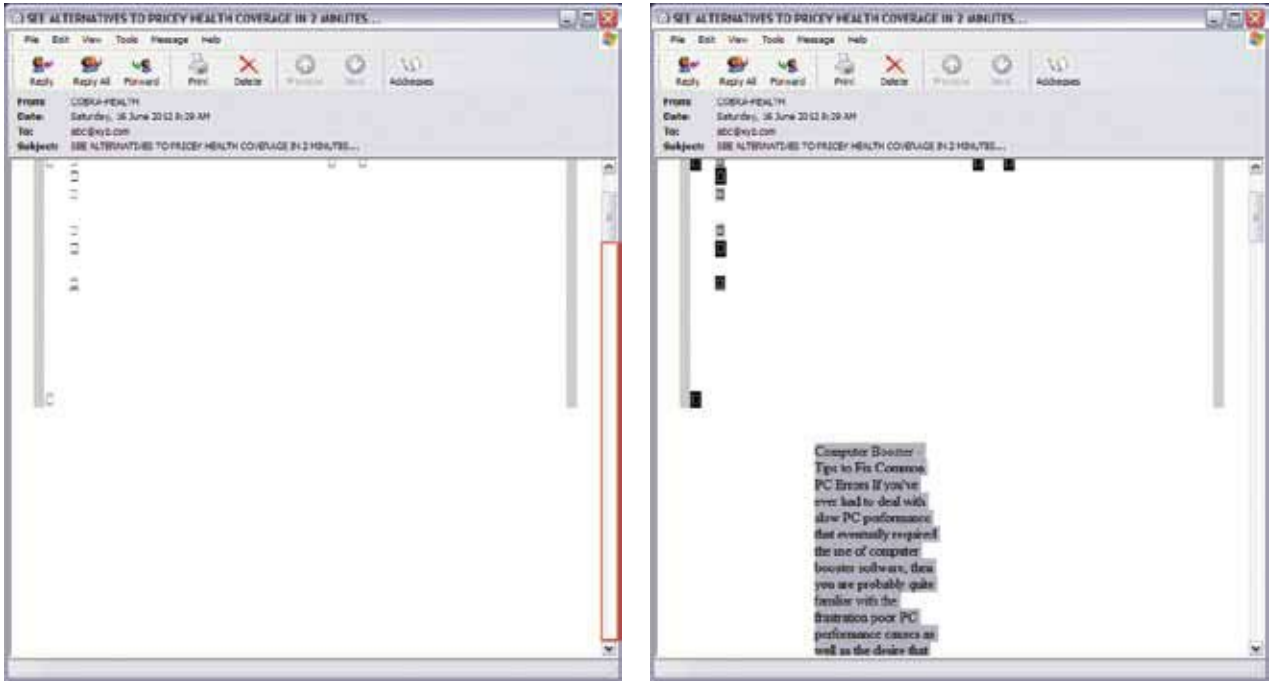
Tamanho Médio em Bytes de Spams *versus* Porcentagem de Spams de Imagens e ZIP/RAR

Julho de 2011 a junho de 2012 (por semana)



- **Tamanho médio em bytes de spams:** Desde meados de 2010, o tamanho médio de spams é normalmente cerca de três ou quatro kilobytes. No entanto, desde o início de 2012, observamos um aumento contínuo em seu tamanho. Em meados de junho de 2012, ele excedeu dez kilobytes. Os spammers acrescentaram conteúdo legítimo de websites escolhidos de forma aleatória para seus spams, a fim de confundir e passar por filtros de spam.

No exemplo à direita, o lado esquerdo mostra um email como seria visto por um usuário ao abri-lo (o download das imagens nesse ponto depende da configuração). Observe o enorme espaço na barra de rolagem. O mesmo email é mostrado no lado direito, mas quando o usuário pressionou [Ctrl]+A[6], o texto oculto se tornou visível. Este texto foi copiado de um website legítimo: http://ezinearticles.com/?Computer-Booster---Tips-to-Fix-Common-PC-Errors



Amostra de Spam com texto oculto escolhido a partir de um website legítimo - Acessado em junho de 2012

6 [Ctrl]+A: para S.O. Microsoft; e para S.O. Mac, [Comando]+A

Filtros de spams baseados no conteúdo (por exemplo, classificadores bayesianos ou abordagens baseadas em assinaturas de texto) podem ter problemas em detectar esses tipos de spam, devido à grande quantidade de texto legítimo. Em um cenário pior, os usuários teriam de desativar seu filtro de spams, devido ao grande número de combinações de falsos positivos, caso esses spams tenham sido incluídos em seus filtros.

No início de julho, começamos a ver outro encadeamento com grandes mensagens de spam com cerca de 700 Kb. Grande parte das pessoas adivinha ou supõe que esse imenso tamanho se deva aos anexos de imagens ou malwares integrados. No entanto, a verdade é completamente diferente.

Esses spams tinham uma parte HTML com um grande cabeçalho. O cabeçalho estava repleto de comandos CSS, que foram copiados de diversos sistemas de gerenciamento de conteúdo (como o Joomla, Wordpress, Typo3, etc.) e era completamente inútil para o resultado desse email.

É interessante ver spammers gastando sua banda larga dessa forma. Não muito tempo atrás, eles tentaram manter o spam pequeno, a fim de enviar o máximo possível. Até mesmo esse exemplo é extremo. Ele representa a tendência geral de aumento de tamanho dos spams.

Qual poderia ser a razão disso?

- O fim recente de botnets impactaram os spammers que estavam mais concentrados em spams menores. Como eles desapareceram, spams maiores se tornaram mais visíveis.
- O spammers não se preocupam tanto com a largura da banda mais, pois qualquer computador pessoal e dispositivo móvel possui uma rápida conexão com a internet.
- Agora, o mais importante é que os spammers não sejam sinalizados por ISPs, grupos de cumprimento da lei e empresas de TI. Portanto, há uma abordagem razoável para que os spammers enviem menos spams, mas certifiquem-se de que eles passem pelo filtro de spams. Alguns filtros podem ter limites que detectam um correio maior do que “tamanho X”, o que indicaria que ele não é um spam.

Outra visão sobre os últimos acontecimentos são as linhas de assunto mais usadas de spams.

Em resumo à tabela à direita, termos:

- Janeiro de 2012: Os spammers utilizaram linhas de assunto inócuas, como "RE:" e "Fw:", como resposta ou encaminhamento sem assunto.
- Fevereiro e março de 2012: Scams de emprego[7] foram as linhas de assunto mais utilizadas.
- Abril de 2012: O mês de scams Românticos[8]
- Maio e junho de 2012: Produtos médicos e acessórios de moda foram as linhas de assunto mais utilizadas.

A cada um ou dois meses, vemos outros tópicos dominando as linhas de assunto mais usadas de spams. Isso demonstra que, apesar da redução do volume geral de spams, os spammers não perderam sua habilidade de mudar os tipos de spam rapidamente.

Três Principais Linhas de Assunto	
Janeiro de 2012	**%**
RE:	0,83%
Fw:	0,83%
Fw: Re:	0,58%
Fevereiro de 2012	**%**
Oportunidade de Emprego	1,76%
Posição de Assistente Virtual	1.33%
Posição de Assistente Administrativo	1,32%
Março de 2012	**%**
Oportunidade de Emprego	1,04%
Vaga - inscreva-se online	0,76%
Anúncio de trabalho - veja detalhes! Enviado por meio de um mecanismo de busca	0,76%
Abril de 2012	**%**
todos querem você	0,37%
beleza real	0,37%
encontros reais	0,37%
Maio de 2012	**%**
Réplica de Relógios Chanel, Réplica de Sapatos, Bolsas, Réplica de Bolsas de Mão... nos especializamos em Réplicas de relógios, Réplica de bolsas de mão, Réplica de sapatos	0,66%
Compre Cialis Online de forma Segura a preços incrivelmente baixos. Comprimidos de bônus, descontos e ENTREGA GRATUITA. Peça Pílulas Cialis Baratas	0,51%
garota bastante bonita	0,50%
Junho de 2012	**%**
Compre Ciails e Viagra online!	2,01%
Re: viagra_sale	0,96%
Preços baixos e pílulas da mais alta qualidade aprovadas pela FDA. Mais de 75.000 clientes confiam em nós. Aceitamos Visa, Mastercard, AmEx e ACH	0,60%

Tabela 3: Três Principais Linhas de Assunto de Spams por Mês - 1o semestre de 2012

7 Visite http://en.wikipedia.org/wiki/Employment_scams
8 Visite http://en.wikipedia.org/wiki/Romance_scam

Domínios de nível superior comuns em spams da URL

O spammers possuem preferências bastante claras com relação aos domínios de nível superior registrados.

- Nos últimos dois anos, os dos domínios de nível superior mais preferidos foram .com e .ru (o domínio de nível superior da Rússia).
- Os domínios de nível superior bem-estabelecidos e de segunda camada são .info e .net.
- Há aproximadamente um ano, os recém-chegados .ua (Ucrânia) e .рф (o domínio de nível superior internacionalizado da Rússia) foram encontrados em vários spams.

Nos anos anteriores, houve outros domínios de nível superior do código do país entre os domínios mais usados, como Reino Unido, Países Baixos, Chile ou Áustria. Atualmente, esse é um caso bastante raro e, nesse contexto, parece ter ocorrido uma crise. Isso pode ser comparável aos domínios de nível superior de proxies anônimos, nos quais um ajuste no mercado, relacionado ao número de diferentes domínios de nível superior utilizados para proxies anônimos, também ocorreu.

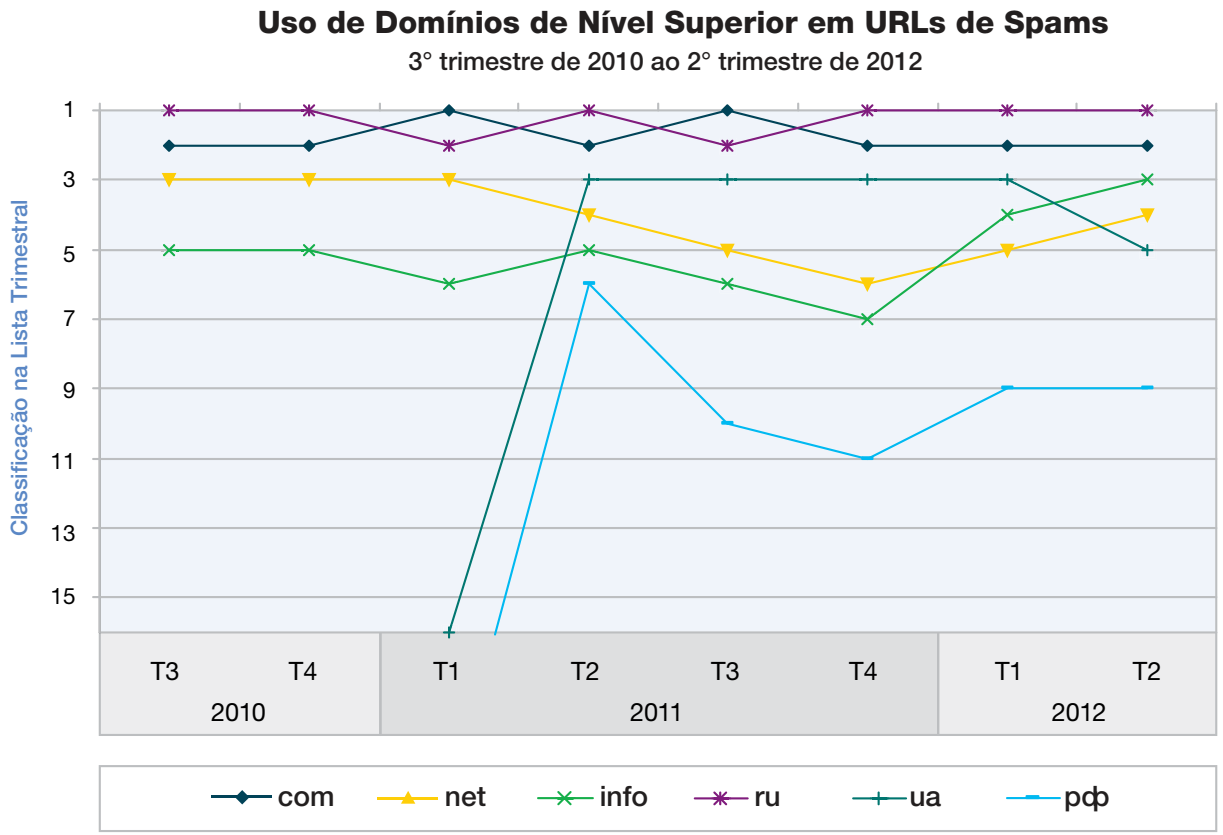


Figura 25: Uso de Domínios de Nível Superior em URLs de Spams - 3o trimestre de 2010 ao 2o trimestre de 2012

Tendências do país de origem do spam

Quando analisamos quais países enviaram mais spams nos últimos três anos, algumas tendências de longo prazo interessantes se tornam visíveis.

- A Índia demonstrou um crescimento praticamente contínuo (com uma grande queda no primeiro trimestre de 2012) e agora domina a cena com uma margem grande, enviando aproximadamente 16% de todos os spams. Isso pode ser o resultado de um crescimento de 25% nos usuários de internet do país ao longo dos últimos 12 meses[9]. É a primeira vez que um país representa cerca de 16% de todos os spams. O recorde anterior pertencia aos EUA, que representavam 15% em 2007.
- O Vietnã varia entre 4% e 10%, mas parece ter se estabelecido entre os países que mais enviam spams.
- Os Estados Unidos tinham a primeira posição em 2010 e, em seguida, caíram para menos de 3% no segundo trimestre de 2011. O país se recuperou desde o segundo trimestre de 2012 e atualmente representa mais de 8%.
- O Brasil caiu para menos de 6% pela primeira vez.
- A Austrália alcançou mais de 6% pela primeira vez.

Há uma queda interessante da Índia e do Vietnã no segundo trimestre de 2012. Embora os dois países juntos tenham totalizado aproximadamente 25% dos spams mundiais no quarto trimestre de 2011 e no segundo trimestre de 2012, no início deste ano, eles somaram menos de 14%. Durante esse período, os spammers obviamente encontraram suas vítimas em outros países, como Argentina, Itália e Romênia. Estes três países tiveram um primeiro trimestre forte em 2012, enviando mais de 10% de todos os spams.

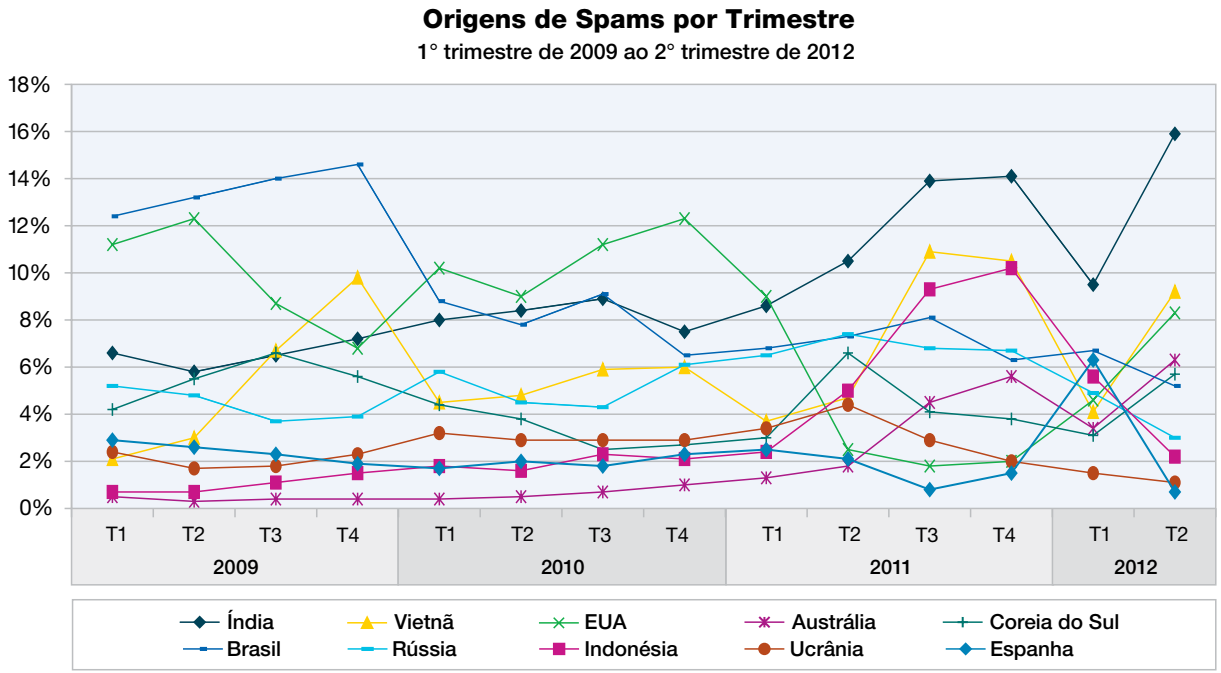


Figura 26: Origens de Spams por Trimestre - 1o trimestre de 2009 ao 2o trimestre de 2012

9 Visite http://www.bbc.co.uk/news/business-16354076

Atividades de finais de semana de spammers

Se os spammers enviaram seus spams de forma uniforme de segunda-feira a domingo, 14,3% de seu volume semanal foi enviado diariamente; portanto, 28,6% nos finais de semanas (sábado e domingo). No Relatório de Riscos e Tendências da IBM X-Force 2010, observamos que o volume de spams em russo nos finais de semana foi significativamente menor do que as atividades durante a semana, pois somente cerca de 10% dos spams russos foram enviados no sábado ou domingo. Em 2012, reconhecemos uma mudança significativa. No primeiro trimestre de 2012, mais de 14% dos spams russos foram enviados durante o final de semana. Ao mesmo tempo, o volume de spams não russos diminuiu para cerca de 22% no final de semana.

A pergunta é: por quê? As respostas podem ser as seguintes:

- Spammers russos automatizam cada vez mais o processo de envio de spams (que, é claro, já foi completamente automatizado por meio de botnets nos últimos anos) e continuam automatizando novas ameaças.
- Eles podem assumir que a oportunidade de contornar filtros de spams seja melhor do que em dias úteis, pois os funcionários de fornecedores antispam também aproveitam o seu final de semana
- Ao mesmo tempo, spammers não russos podem concluir que as ameaças de spams funcionam melhor em dias úteis, pois a primeira coisa que vários usuários fazem é limpar suas caixas de correio na segunda-feira de manhã e rapidamente descartam os spams enviados no final de semana.
- Poderia haver uma consolidação e uma crise, pois os spammers agora utilizam menos métodos para enviar spams. Isso é consistente com a queda do volume de spams ao longo dos últimos dois anos.

Será interessante observar se as atividades de finais de semana dos spammers russos e não russos continuam convergindo nos próximos meses e anos.

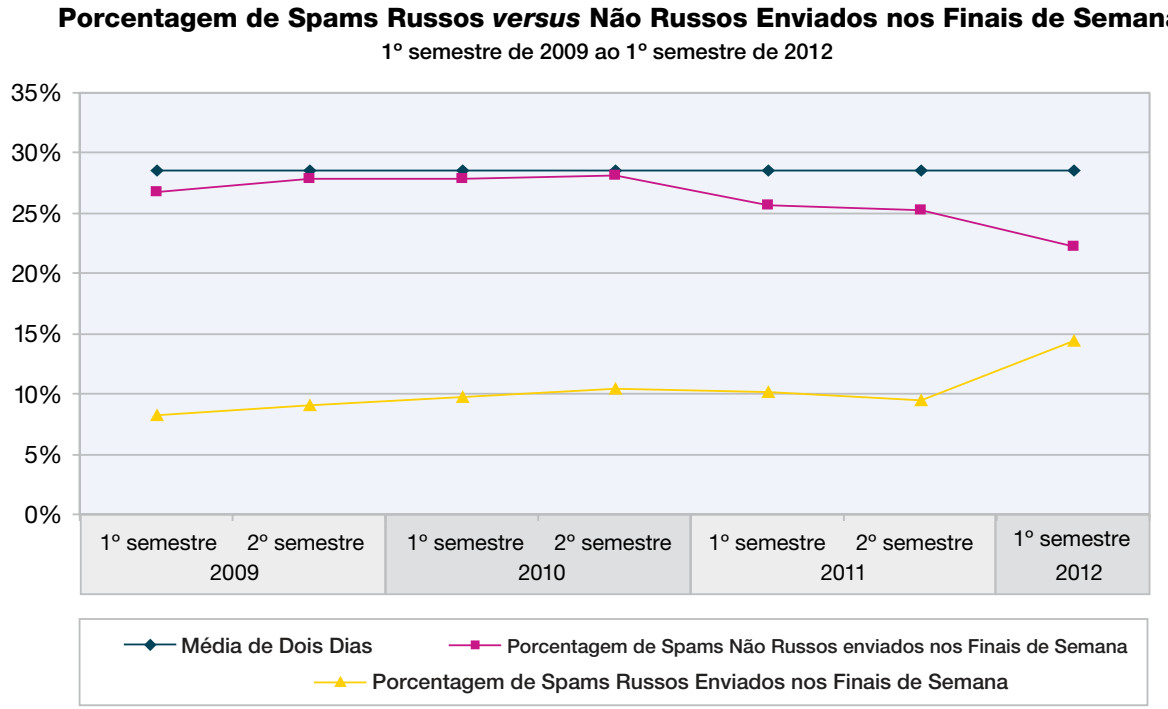


Figura 27: Porcentagem de Spams Russos versus Não Russos Enviados nos Finais de Semana - 1º semestre de 2009 ao 1º semestre de 2012

Fim da botnet em julho de 2012

Em 18 de julho de 2012, testemunhamos o fim da botnet da Grum[10]. Isso resultou em uma baixa anual no volume de spams.

Na semana do fim da botnet da Grum, observamos menos de 60% dos níveis de spam medidos no primeiro trimestre de 2012.

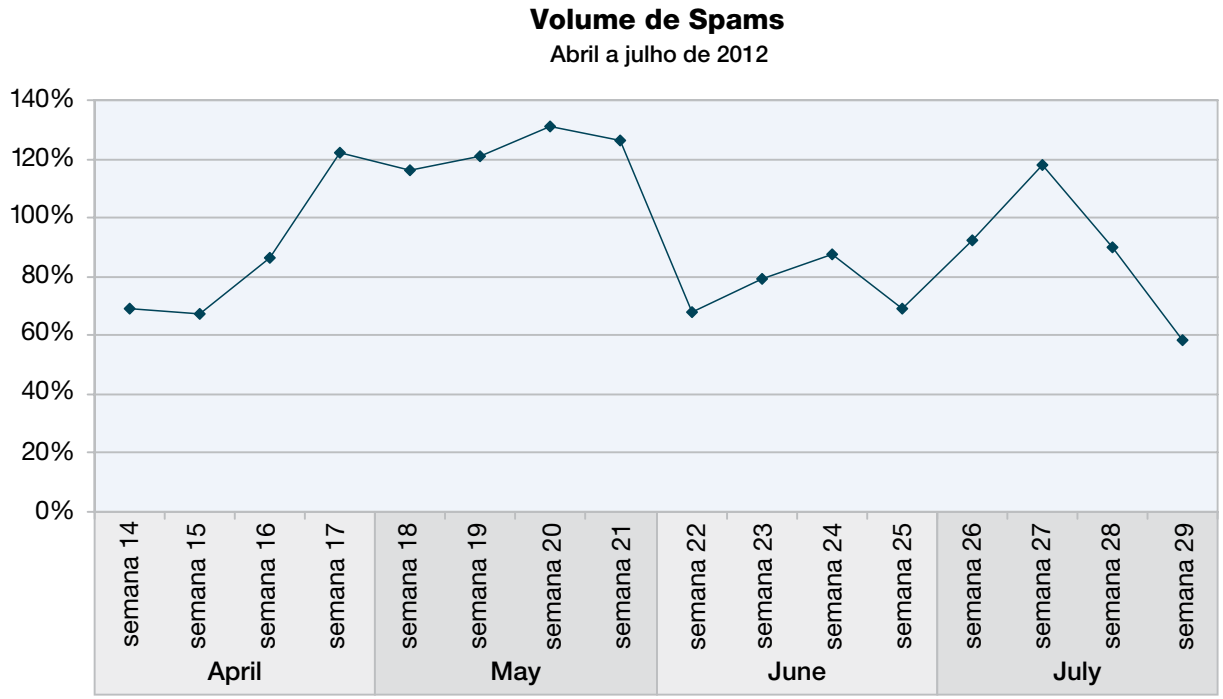


Figura 28: Volume de Spams - abril a julho de 2012

10 Visite http://en.wikipedia.org/wiki/Grum_botnet and http://blog.fireeye.com/research/2012/07/grum-botnet-no-longer-safe-havens.html

Quando observamos as origens de spams antes e depois do fim da botnet, outras tendências interessantes se tornam visíveis.

- A impressão era a de que a botnet da Grum evitava a infecção de computadores nos países da Índia, Arábia Saudita, Turquia e Reino Unido. Podemos chegar a essa conclusão, pois, desde o fim da botnet da Grum, esses quatro países reuniram 36,5% de todo o volume mundial de spams e, após o fim da botnet, eles acumularam 49,6%.
- A Grum direcionava várias de suas infecções em computadores baseados nos EUA, Vietnã, Austrália, Alemanha e Brasil. As melhorias nos dados demonstram que, antes do fim da botnet, esses países enviavam 29,9% de todos os spams mundiais, mas somente 22,5% depois disso.

Essa não é a primeira vez que a Índia foi afetada pela desativação de uma botnet. Quando a botnet Rustock[11] teve seu primeiro encerramento durante a época de férias de Natal de 2010, a Índia aumentou sua porcentagem do volume mundial de spams de 7,1% para 11,4%[12].

Origens do Spam Antes e Depois do Fim da Botnet
12 de julho a 25 de julho de 2012

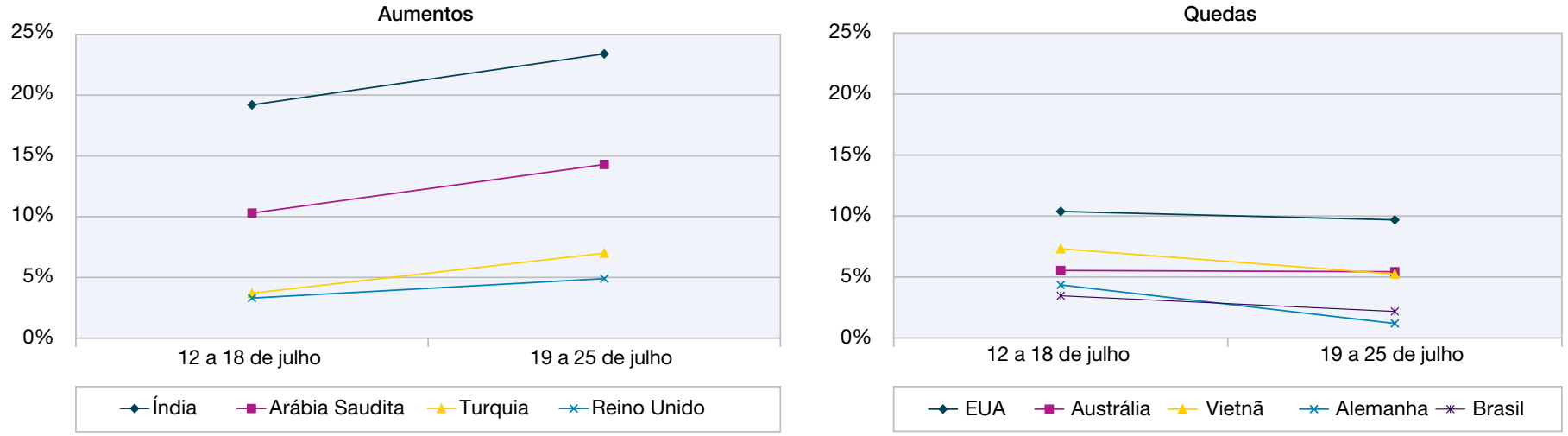


Figura 29: Origens do spam antes e depois do fim da botnet da Grum - 12 a 25 de julho de 2012

11 Visite http://en.wikipedia.org/wiki/Rustock
12 Visite http://blogs.iss.net/archive/2011spambotdecline.html

Scam e phishing de emails

Metodologia

A fim de determinar as tendências mais recentes em scams e phishing:

- As estatísticas são baseadas exclusivamente em scams e phishing implementados por email.
- Elas incluem todos os emails que utilizam o nome de marcas conhecidas, a fim de fazer com que os usuários cliquem em um anexo ou link, mesmo que eles não sejam relacionados ao phishing. Portanto, alguns dos emails incluídos são apenas parecidos com phishing.
- Elas não incluem nenhuma tentativa de phishing não relacionada ao email, como malwares fornecidos por uma unidade por meio de downloads e registros de pressionamentos de teclas.

Informações detalhadas sobre a metodologia das estatísticas de scam e phishing fornecidas são oferecidas na seção correspondente do Relatório Anual de Riscos e Tendências da IBM X-Force 2011.

Tendências mais recentes em scams e phishing de emails

Quando consideramos a metodologia mencionada acima, observamos algumas diferenças significativas entre o volume de spam e o volume de scams e phishing de emails do primeiro semestre de 2008 ao primeiro semestre de 2012 (primeiro semestre de 2008 = 100% base tanto para spam quanto para scam/phishing).

- De 2008 a 2010, o volume de spams praticamente dobrou.
- De 2008 a 2010, o volume de scam/phishing de emails diminuiu significativamente, chegando a menos de 20% dos níveis de 2008.
- De 2010 a 2012, o volume de spams diminui para cerca de um terço dos níveis de 2010.
- De 2010 a 2012, o volume de scam/phishing de emails praticamente quadruplicou, chegando a mais de 83% dos níveis de 2008 no segundo trimestre de 2012.

Concluindo, o volume de spams e de scams e phishing se comportam de forma contrária.

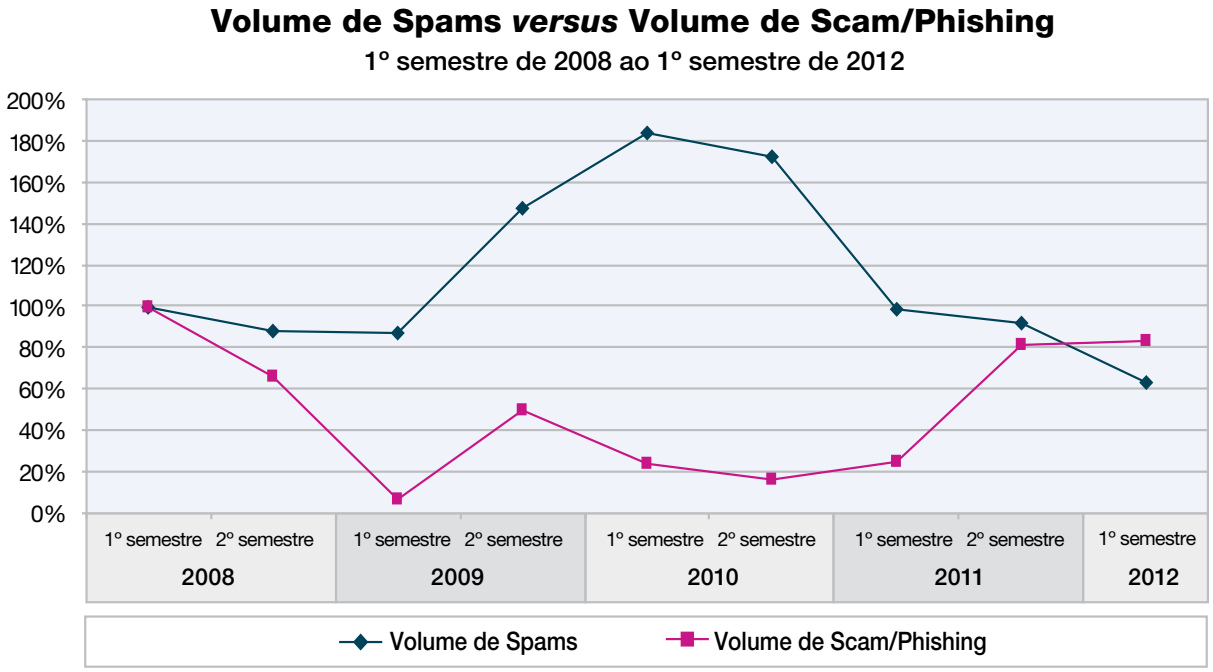


Figura 30: Volume de Spams versus Volume de Scam/Phishing - 1º semestre de 2008 ao 1º semestre de 2012

Quando observamos os tipos de scam e phishing de emails, algumas tendências interessantes se tornam visíveis.

- Até 2009, phishing tradicionais de emails cujo alvo eram instituições financeiras dominaram as estatísticas e representaram mais de 50% de todos os emails de phishing. Eles não dominam as estatísticas desde o início de 2010.
- Desde o início de 2010 – quando começamos a monitorar essa classe de emails – as redes sociais dominavam as estatísticas, estando presentes nas duas primeiras posições. No início de 2011, mais de 80% dos nomes de marcas legítimas foram utilizados em emails em redes sociais, permanecendo estabilizados em 43% durante o segundo semestre de 2011. Após um curto intervalo no início de 2012, agora eles representam mais de 31% de todos os scams e phishing.
- Serviços de encomenda foram amplamente utilizados para enganar os usuários durante o segundo semestre de 2010, quando atingiram cerca de 20% de todos os emails parecidos com scam/phishing. No segundo trimestre de 2011, mais de 50% desse tipo de spam utilizou o bom nome dos serviços de encomenda. Esse tipo praticamente desapareceu no final de 2010 e início de 2012, mas voltou no segundo trimestre de 2012, chegando a mais de 27% do volume de scam/phishing.
- No início de 2012, os phishers se concentraram em organizações sem fins lucrativos, representando 66% de todos os scams e phishing do primeiro trimestre, mas, em seguida, caíram para 7% no segundo trimestre de 2012.
- Scams varredores (como “Digitalize em sua impressora no. 6269319”) que incluem um anexo malicioso chegaram às três primeiras posições no segundo trimestre pela primeira vez e representaram mais de 13% de todos os scams e phishing.

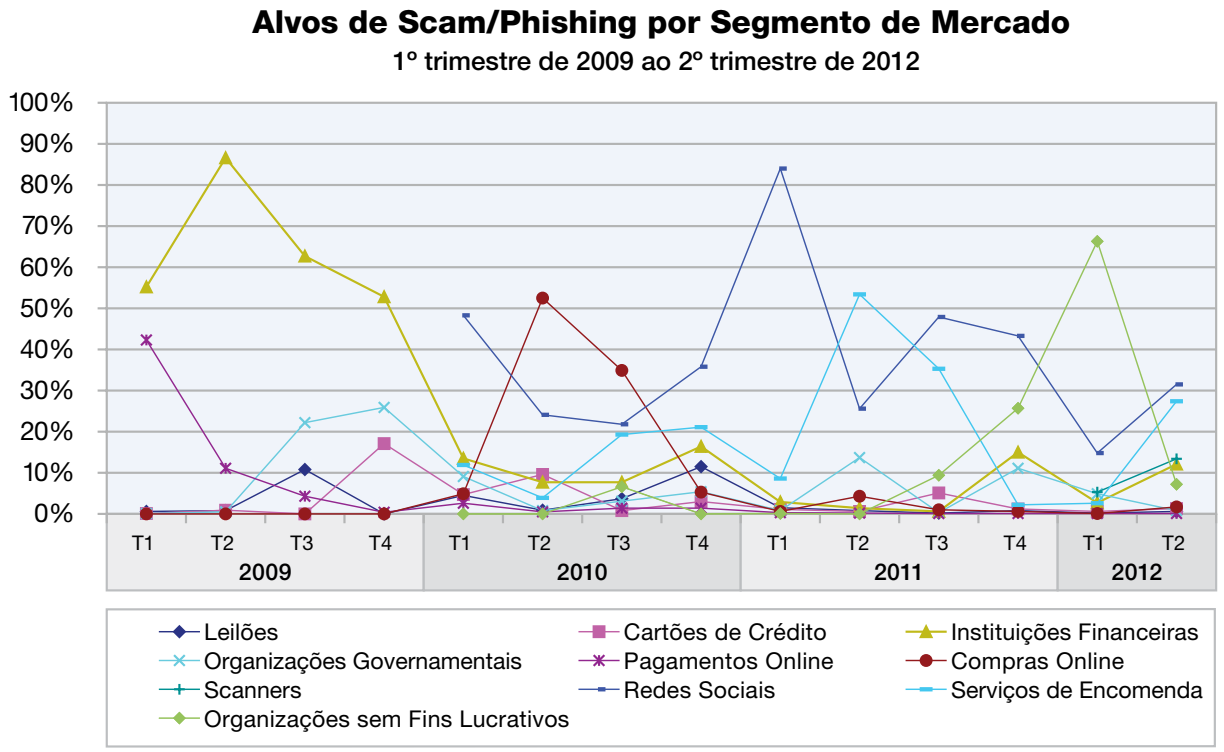


Figura 31: Alvos de Scam/Phishing por Segmento de Mercado - 1º trimestre de 2009 ao 2º trimestre de 2012[13]

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

Ao revisar os altos e baixos do gráfico anterior, podemos observar que os phishers estão repetindo os alvo abaixo para fazer com que os usuários cliquem nos links ou anexos. O método é o mesmo, mas o alvo é diferente.

A cada nova iteração de spam, eles encontram novas vítimas (isto é, novos usuários da internet) que caem em seus truques.

Também é interessante observar de quais países os emails parecidos com phishing estão sendo enviados.

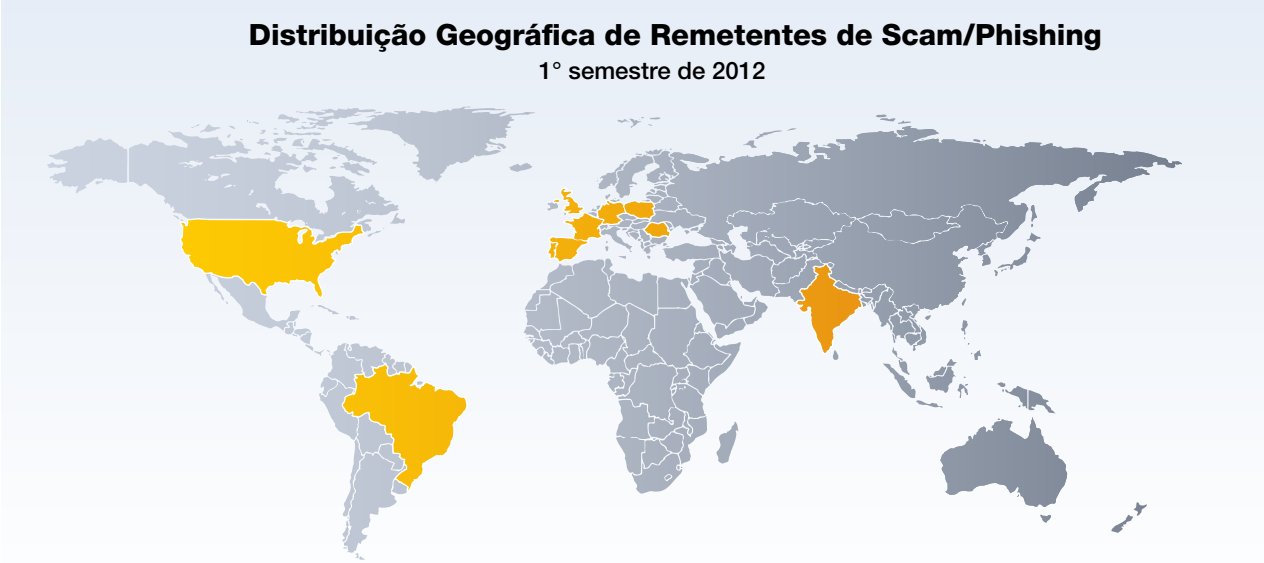


Figura 32: Distribuição Geográfica de Remetentes de Scam/Phishing - 1º semestre de 2012

País	% de phishing
Espanha	7,6%
Romênia	7,4%
Reino Unido	6,4%
Alemanha	5,5%
Brasil	5,0%

País	% de phishing
Índia	4,9%
Polônia	4,8%
França	4,4%
EUA	3,8%
Portugal	2,5%

Tabela 4: Dez Principais Países de Origens de Scam/Phishing - 1º semestre de 2012

As redes sociais foram os alvos dominantes de phishing de emails durante mais de dois anos, portanto, concluindo, vamos observar os países dos quais esse tipo de phishing de emails é enviado.

Mensagens enviadas dos EUA somam aproximadamente 15% de todos os scams/phishings de redes sociais. Em segundo lugar está a França, que representa cerca de 8% de todos os phishings de redes sociais. A distribuição desse país é significativamente diferente da distribuição geral de scam/phishing do país, que parece indicar que esse tipo de phishing não é proveniente das mesmas botnets que os demais tipos de spam e phishing.

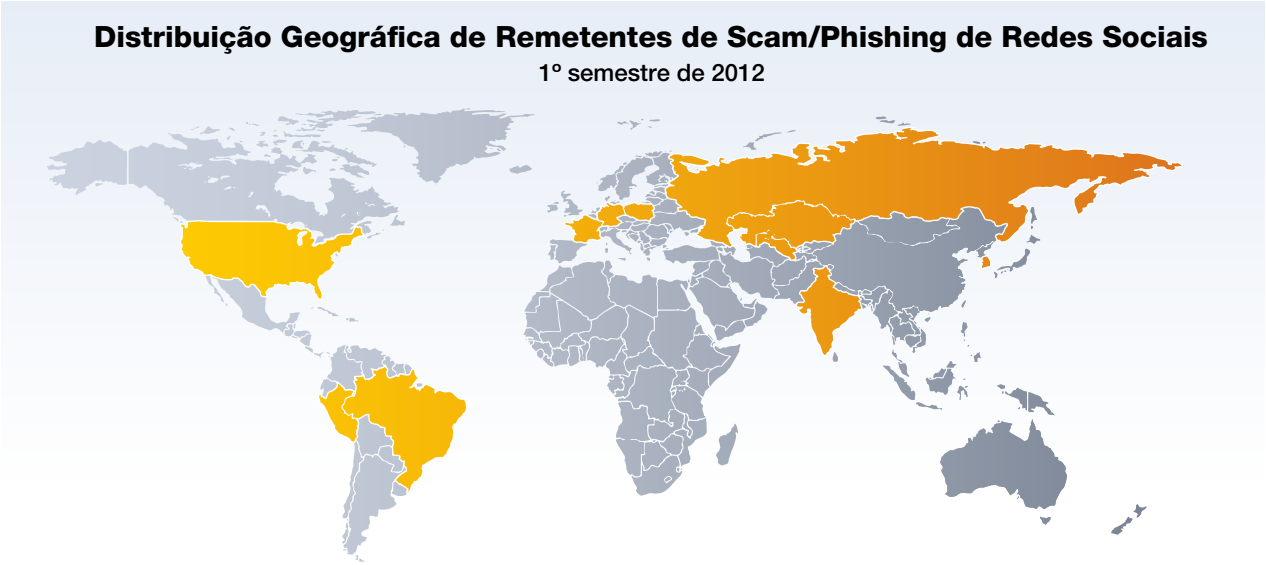


Figura 33: Distribuição Geográfica de Remetentes de Scam/Phishing de Redes Sociais - 1º semestre de 2012

País	% de phishing
EUA	14,7%
França	7,9%
Brasil	6,0%
Alemanha	5,3%
Coréia do Sul	4,5%

País	% de phishing
Russia	4,0%
Polônia	3,5%
Índia	3,3%
Peru	3,2%
Casaquistão	3,0%

Tabela 5: Dez Principais Países de Origens de Scam/Phishing de Redes Sociais - 1o semestre de 2012

Seção II
Práticas operacionais de segurança

Esta seção do Relatório de Tendências abordará tópicos relacionados aos pontos fracos de processo, software e infraestrutura visados pelas ameaças atuais. Serão discutidas melhores práticas de conformidade de segurança, ideias para a redução do custo operacional, inteligência e automação, custo de propriedade reduzido e consolidação de tarefas, produtos e funções. Também serão apresentados os dados rastreados dentro da IBM durante o processo de gerenciamento ou mitigação desses problemas.

Combatendo ameaças avançadas persistentes (APTs) com inteligência de segurança e detecção de anormalidades

As ameaças avançadas persistentes (APTs) tornaram-se um dos tópicos mais discutidos do segmento de mercado. Certamente, nem todas as violações de segurança resultam de uma APT – a maioria delas, na verdade. É evidente, porém, que algumas violações realmente resultaram dos esforços de equipes bem-organizadas que buscam alcançar objetivos específicos por meio de ataques pacientes e de longa duração, frequentemente usando malwares e táticas altamente customizados de acordo com a organização de destino e funcionários específicos. Em outras palavras, APTs.

O impacto de negócios das ameaças avançadas persistentes é surpreendentemente grande. Como mostrado no Relatório Anual de Riscos e Tendências da IBM X-Force 2011, empresas no mundo todo sofreram violações significativas – muitas causadas por APTs –, o que fez com que 2011 ficasse conhecido como o "Ano da Violação de Segurança". No início de 2011 e antes disso, empresas de grande porte (como RSA e Google, entre outras) enfrentaram comprometimentos generalizados que expuseram dados de cliente e usuário, além de propriedade intelectual sensível.

Em uma recente pesquisa de opinião do Enterprise Strategy Group feita com profissionais de segurança de organizações corporativas com sede nos Estados Unidos, 59% dos participantes disseram achar "altamente provável" ou "provável" que suas organizações tenham sido alvos de APTs. Além disso, 30% acreditam que suas organizações estão "muito vulneráveis" ou "vulneráveis" a um ataque de APT no futuro. Mesmo entre as organizações consideradas "mais preparadas para APTs", 46% dos participantes acreditam que estão "muito vulneráveis" ou "vulneráveis" a um ataque de APT no futuro[14].

A pergunta é: como as organizações podem se defender de adversários obstinadamente determinados, pacientes e criativos que sabem muito sobre seus funcionários e são, com frequência, bem-financiadas? Não é possível contar exclusivamente com abordagens preventivas, pois invasores avançados podem acabar violando suas defesas. Tampouco é possível contar apenas com tecnologias de detecção baseadas em assinatura, uma vez que tais ataques também conseguem enganá-las. Embora as detecções preventiva e baseada em assinatura sejam necessárias para a segurança corporativa, precisamos de mais proteção e devemos adotar novas estratégias. As abordagens de Inteligência de Segurança que incorporam detecção de anormalidades surgiram para complementar as soluções tradicionais e ajudar a proteger-se de ameaças avançadas persistentes.

Entendendo as ameaças avançadas persistentes

Apesar de o termo não possuir uma definição consensual, as APTs normalmente são descritas como algo que inclui noções de um esforço direcionado e com destino, um ataque persistente e possivelmente de longa duração e técnicas "avançadas" (em termos de sofisticação técnica e/ou operacional). Muitos executivos e líderes de segurança de informações admitem a existência das APTs, mas são poucos os que acreditam que suas próprias organizações podem ser alvos. Como não sou um órgão do governo nem uma corporação da Fortune 500 – raciocinam eles –, será que alguém realmente faria o esforço de atacar minha organização dessa maneira?

14 "U.S. Advanced Persistent Threat Analysis", Enterprise Strategy Group, outubro de 2011

Infelizmente, parece que a resposta é "sim". Um artigo recente sobre uma APT muito comum informou que os invasores haviam comprometido 72 partes diferentes, incluindo empresas de construção e indústria pesada, empresas imobiliárias e comitês olímpicos nacionais (ou seja, instituições que não parecem ser os alvos mais prováveis de uma APT)[15]. **Portanto, muitas organizações estão simplesmente pressupondo o pior – que o reconhecimento ou o ataque já começou.**

Em uma situação de APT verdadeira, considere que o invasor conseguirá penetrar suas defesas em algum momento. Isso acontece pelos motivos a seguir:

1. A dificuldade inerente de proteger todos os pontos de entrada. Isso inclui corrigir e proteger os recursos voltados ao público sempre que uma vulnerabilidade é descoberta, garantindo configurações seguras e assim por diante.
2. O desafio de proteger-se de ataques baseados em engenharia social, que podem resultar em comprometimento da conta ou podem neutralizar os recursos de prevenção.

Ou, como um analista observou recentemente:

"A maioria dos administradores de segurança e CISOs de empresas de grande porte entendem que **não é uma questão de se, mas de quando sua organização sofrerá uma violação** – algo que pode ser muito prejudicial para a organização como um todo. (...) Uma coisa está clara: quanto mais tempo um invasor furtivo permanecer indetectado na rede da empresa e em seus endpoints, mais dano ele poderá fazer" (Ênfase acrescentada pela IBM.)[16].

Vejamos alguns exemplos para entender as táticas utilizadas e as vulnerabilidades exploradas nos ataques avançados. Além de serem criativas e tecnicamente avançadas, a maneira como algumas dessas ações são orquestradas as torna mais efetivas que a soma de suas partes. É difícil combater as APTs em função de uma combinação de táticas (tais como as listadas abaixo) cuidadosamente coreografadas e que, às vezes, refletem meses de pesquisa e customização. Os exemplos extraídos de diversos ataques incluem:

- **Infiltrar um parceiro confiável.** Em um caso, os invasores comprometeram o provedor de software de terceiros confiável do alvo, inseriram um código de Troia no servidor de atualização de software e esperaram que o provedor de software atualizasse automaticamente esse código na rede do alvo.
- **Criar malware customizado.** Como acontece frequentemente em uma APT, o código de Troia do exemplo anterior foi feito para infectar apenas a organização de destino, mas nenhum dos outros clientes do provedor de software; isso impediu que o malware se espalhasse de modo generalizado e fosse identificado por fornecedores de antivírus antes de cumprir sua missão.
- **Usar pesquisa e engenharia social para comprometer contas de usuários.** Invasores pacientes e comprometidos realizam reconhecimento extensivo de alvos de spear-phishing e, em seguida, entram em contato com eles por meio de comunicações bastante críveis (email, IM ou mensagens de rede social), que podem demonstrar um conhecimento das atividades profissionais, colegas, amigos e da família do indivíduo. A mensagem de phishing pode incluir um link ou anexo que resulte na infecção do sistema do alvo, muitas vezes com malware customizado.

15 "Revealed: Operation Shady Rat", McAfee, 2011
16 Postagem em blog: "Okay, Breaches Are Inevitable: So Now What Do We Do?", por Paula Musich, Current Analysis, 20 de julho de 2012, http://itcblogs.currentanalysis.com/2012/07/20/okay-breaches-are-inevitable-so-now-what-do-we-do/

- **Explorar vulnerabilidades do dia zero.** Uma abordagem alternativa à engenharia social com o objetivo de violar o perímetro do alvo – além de uma tática usada para ampliar o alcance do comprometimento – é o uso de explorações do dia zero para ter acesso às contas de usuário e de administrador. Com a prosperidade dos mercados negro e comum em explorações do dia zero e tecnologias avançadas de implementação, os invasores não precisam descobrir as vulnerabilidades do dia zero nem preparar a exploração por conta própria. Em resumo, além de pragmática, a utilização desses mercados também é econômica.
- **Comunicar-se por canais ocultos**. Muitas vezes, os adversários usam malware para atrair uma máquina e uni-la a um botnet; mais tarde, comunicam-se com o comando do botnet e controlam o servidor por um canal oculto, como uma porta 80 ou 8080. Também é possível usar essa abordagem para exfiltrar dados da organização de destino.

Como APTs legítimas provavelmente conseguirão violar o perímetro do alvo mais cedo ou mais tarde, recursos efetivos de detecção e investigação são essenciais. Embora não se devam negligenciar os esforços de proteção e prevenção, o verdadeiro indicador das defesas de APT de uma organização é sua capacidade de detectar violações rapidamente e pesquisar com cuidado o alcance e o impacto dessas violações.

Inteligência de segurança: Equipada exclusivamente para se proteger contra APTs

Como introduzido no Relatório Anual de Riscos e Tendências da IBM X-Force 2011, a Inteligência de Segurança é uma nova classe de soluções que fornecem visibilidade unificada e analítica em tempo real no espectro de operações de segurança.

A Inteligência de Segurança (SI) é a coleta, normalização e análise em tempo real dos dados gerados por usuários, aplicativos e infraestruturas que afetam a segurança de TI e a conduta de risco de uma empresa.

Os dados coletados e armazenados pelas soluções de Inteligência de Segurança incluem logs, eventos, fluxos de rede, identidades e atividades de usuários, perfis e locais de acesso, vulnerabilidades, configurações de ativos e dados de ameaças externas.

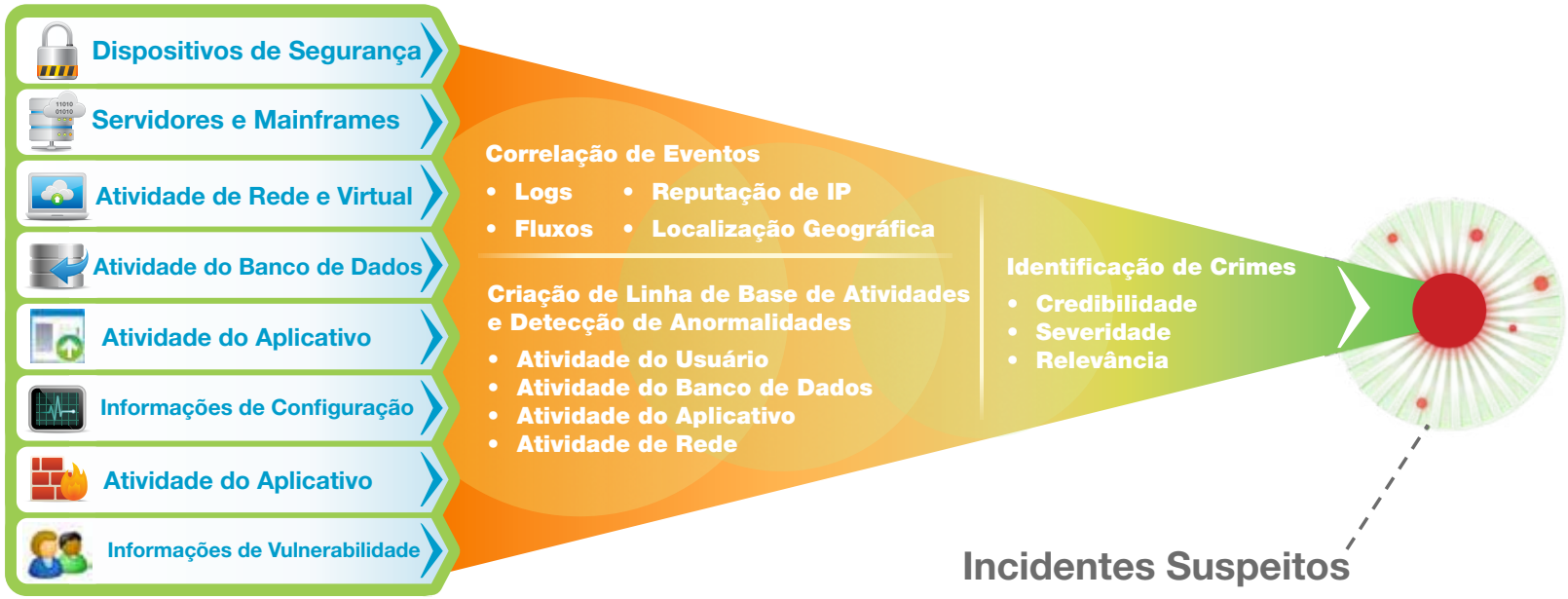
Diversos elementos fazem da SI uma abordagem ideal para ajudar a combater ameaças avançadas persistentes:

- **Consolidação de dados isolados para uma visualização de 360 graus.** Como a Inteligência de Segurança analisa um conjunto diferente de dados, ela pode ligar os pontos entre atividades aparentemente desconectadas ou benignas e, em última análise, gerar insights melhores para a detecção de APT.
- **Insights antes e depois da exploração.** Organizações usam a SI para reunir e priorizar informações sobre lacunas de segurança existentes que devem ser direcionadas (ajudando a impedir violações), bem como sobre o comportamento suspeito que já pode estar ocorrendo dentro da rede (ajudando a detectar violações).
- **Recursos de detecção de anormalidades.** Criar linhas de base das atividades atuais, identificar desvios do comportamento normal e, em seguida, determinar quais desvios são significativos é um aspecto fundamental da Inteligência de Segurança. Isso pode ser vital para detectar APTs em andamento.
- **Correlação e análise em tempo real.** As soluções de SI são capazes de correlacionar enormes conjuntos de dados em tempo real, usando métodos analíticos avançados e bancos de dados feitos sob medida. Isso permite uma detecção mais antecipada e precisa das APTs, ajudando a distinguir o sinal dos ruídos.
- **Ajudar a reduzir os positivos falsos.** Ao combinar todas essas abordagens analíticas, a SI consegue ajudar a detectar os comprometimentos mais rapidamente, além de remover a prioridade de atividades incomuns, porém benignas. A redução do tempo gasto na investigação de atividades anormais, mas inofensivas, pode

fazer uma grande diferença na capacidade da organização de priorizar os seus objetivos principais.

- **Recursos investigativos.** Após a descoberta de uma violação, a próxima etapa crucial é pesquisar exaustivamente o impacto causado por ela. A Segurança de Inteligência pode fornecer uma visualização de console único dos dados do log, tráfego de rede outras telemetrias de segurança em milhares de sistemas e recursos, diminuindo as tarefas da equipe de segurança e de rede, que precisa avaliar a violação com rapidez.
- **Flexibilidade.** Como o ambiente de TI interno e o cenário de ameaças externas podem mudar rapidamente, as abordagens de defesa de ATP precisam suportar mudanças frequentes. Normalmente, as soluções de SI modernas ajudam a incluir origens de dados, criar e ajustar a analítica, criar novas visualizações do usuário e relatórios e expandir e desenvolver a arquitetura de implementação geral.
- **Abordagem unificada.** As APTs costumam ser ataques complexos e a diversas frentes que envolvem dezenas – se não centenas de – sistemas de destino. Já que algumas soluções de Segurança de Inteligência são entregues por meio de uma plataforma unificada e modular, podem ajudar as organizações a percorrerem volumes de dados e realizarem um conjunto mais amplo de analítica e consultas ad hoc do que outras abordagens.

A Inteligência de Segurança correlaciona e analisa um conjunto diferente de dados relevantes à segurança



Detecção de anormalidades: O eixo central da inteligência de segurança dos esforços de defesa da APT

É possível que a principal arma fornecida pela Inteligência de Segurança para combater APTs seja a detecção de anormalidades. Uma vez que os adversários avançados utilizam estratégias de ataque criativas e direcionadas, frequentemente em combinação com explorações do dia zero, as defesas baseadas em assinatura tradicionais costumam ser insuficientes. As organizações precisam da capacidade de detectar atividades que são um pouco incomuns e, depois, enriquecê-las com o máximo de contexto possível para distinguir as anormalidades benignas das ameaças reais.

Os ataques de APT não vêm acompanhados por sinos ou luzes piscantes; eles se misturam ao seu ambiente na medida do possível. É necessário um monitoramento rigoroso, automatizado e contínuo – além de uso máximo dos dados – para ter uma chance de descobri-los antes que ocorram danos graves.

As tecnologias de detecção de anormalidades encontradas nas soluções atuais de Inteligência de Segurança têm origem no espaço de detecção de anormalidades no comportamento de rede (NBAD). Entretanto, expandiram seus recursos para além da NBAD tradicional com o objetivo de dar suporte à análise de dados do log, além da análise de fluxo de rede (tráfego de rede). Com a abordagem unificada da Inteligência de Segurança, as equipes de segurança podem realizar analítica em tempo real com uma combinação de fluxo de rede e dados do log de modo simultâneo, obtendo um insight melhor de possíveis ameaças e aprimorando o reconhecimento da situação.

A detecção de anormalidades ocorre por meio do monitoramento de atividades que não se encaixam no comportamento "normal". Ela determina os níveis de linha de base das atividades ao longo de dimensões de interesse e, em seguida, aciona alertas, conforme o caso. O ideal é que o período de aprendizado e o período do acionador possam ser ajustados facilmente – e que seja possível explicar a sazonalidade e as tendências de crescimento.

Os exemplos das muitas anormalidades que podem ser detectadas com a Inteligência de Segurança incluem:

- O tráfego de saída é enviado a um país em que a empresa não faz negócios e ao qual tráfego algum deve ser enviado.
- Um aplicativo conhecido (como um bate-papo de IRC) está usando uma porta não padrão (como uma porta 80).
- Tráfego de FTP é observado no departamento de Finanças, sendo que esse departamento nunca teve tráfego de FTP antes.
- Ocorre um surto de worm de autopropagação.
- Um serviço novo é iniciado em um host conhecido, possivelmente sinalizando uma violação.
- Um sistema host muda de funções – por exemplo, um servidor do Sistema de Nomes de Domínio voltado para fora é alterado, tornando-se também a retransmissão SMTP.
- Mudança no volume de tráfego de rede; o volume de tráfego para um host específico está 200% maior durante as últimas 24 horas em relação ao seu nível médio histórico nos últimos três meses, sem uma explicação sazonal clara para esse aumento.

Em resumo, a detecção de anormalidades pode fornecer uma base inteligente para descobrir violações de APT. Não exige um conhecimento avançado de como o ataque pode parecer, mas consegue monitorar automaticamente as atividades na rede em busca de desvios notáveis.

Melhores práticas para a detecção de anormalidades

Ao implementar recursos de detecção de anormalidades a fim de proteger-se de APTs, recomendamos as melhores práticas a seguir:

- **Monitorar a atividade do usuário, especialmente de usuários privilegiados**. Uma das táticas principais usadas na maioria dos ataques avançados é o controle das contas dos funcionários, especialmente de funcionários com acesso privilegiado. Depois que uma conta é comprometida, o adversário pode tentar acessar os aplicativos ou sistemas que não foram utilizados anteriormente pelo funcionário em questão ou acessar recursos em horários incomuns. Quanto mais inteligência sua solução consegue desenvolver acerca das atividades normais dos funcionários, mais efetiva ela será ao detectar um comportamento anormal significativo.
- **Monitorar o acesso a dados sensíveis.** Do mesmo modo, priorize a proteção dos dados que teriam mais valor para um invasor – dados do cliente, dados financeiros, propriedade intelectual e assim por diante. Desenvolva inteligência sobre os ritmos típicos de atividades envolvendo bancos de dados sensíveis e outros storages de dados, para que seja possível detectar irregularidades que talvez tenham significado. As soluções de segurança de banco de dados também podem fornecer telemetria de segurança de valor para a detecção de anormalidades. O ideal é combinar o monitoramento do acesso a dados com o monitoramento das atividades do usuário para ter uma detecção de ameaças mais precisa.
- **Monitorar o tráfego de saída para impedir a exfiltração de dados.** Aprimore seu monitoramento do tráfego de saída para poder detectar e interromper a exfiltração de dados sensíveis. Você saberia se começasse um tráfego para um país incomum com o qual não faz negócios ou se ele fosse enviado por uma porta incomum? Seria possível detectar o envio de tráfego por um canal oculto? Você saberia se um host interno iniciasse uma comunicação com um endereço com intervalo IP dinâmico?
- **Monitorar o acesso e o tráfego geográficos.** Mesmo se atuar em um ambiente global e fizer negócios em e com muitos países no mundo todo, provavelmente existe um conjunto finito de países em que o tráfego de rede de entrada e saída seria esperado. Quando o tráfego ocorre com outras geografias, talvez valha a pena investigar, especialmente se observar outros comportamentos suspeitos com usuários ou sistemas relacionados a essa atividade.
- **Utilizar a inteligência de ameaças com a detecção de anormalidades.** Muitos serviços comerciais e comunitários de inteligência de ameaças, incluindo os fornecidos pela IBM X-Force, fornecem insights ricos das atividades de ameaça e dos atores ruins, o que pode enriquecer ainda mais a detecção de anormalidades. Por exemplo, você deve saber se usuários ou sistemas interagirem com sites conhecidos como host de malware, comando de botnet e servidores de controle ou outras ameaças.
- **Coletar fluxos de rede para insights superiores.** Os dados do fluxo de rede – especialmente dados da camada sete com visibilidade de conteúdo – podem ser uma origem de dados extremamente útil para a detecção de anormalidades. Também podem fornecer informações de valor inestimável para confirmar ou contestar a existência de uma violação, além de determinar a extensão e o impacto de quaisquer violações.

Conclusão

Reconhecendo que as violações são praticamente inevitáveis, a prioridade de muitas organizações passou a ser a detecção. A Inteligência de Segurança surgiu como um importante candidato para combater APTs, utilizando a capacidade de coletar, normalizar e analisar conjuntos de dados grandes e variados. A detecção de anormalidades está no centro da Inteligência de Segurança, permitindo que equipes de segurança de informações identifiquem desvios significativos em relação aos ritmos normais de atividade. Por meio do uso de soluções e melhores práticas de Inteligência de Segurança, as organizações podem conseguir uma postura de segurança mais proativa.

Divulgações de vulnerabilidade no primeiro semestre de 2012

Desde 1997, a IBM X-Force faz o rastreamento de divulgações públicas de vulnerabilidades em produtos de software. A IBM X-Force coleta consultorias de software de fornecedores, lê listas de distribuição relacionadas à segurança e analisa centenas de páginas da web com vulnerabilidade em que dados, explorações e vulnerabilidade de recursos foram divulgados.

No primeiro semestre de 2012, foram reportadas mais de 4.400 vulnerabilidades de segurança novas. Se essa tendência continuar pelo restante do ano, as vulnerabilidades projetadas totais ficariam um pouco acima do recorde registrado em 2010, aproximando-se de um total de 9.000 vulnerabilidades.

Desde 2006 – e com a primeira queda nas divulgações de vulnerabilidade em 2007 –, o número total de vulnerabilidades sobe e desce a cada dois anos. Não existe um motivo definidor por trás da flutuação ano a ano. Porém, 2012 poderia muito bem ser um ano recorde para as divulgações de vulnerabilidades de segurança.

Aplicativos da web

A tendência contínua do número total de divulgações de vulnerabilidades de segurança também pode ser encontrada dentro da categoria de vulnerabilidades de aplicativos da web. Em 2011, houve uma queda nas vulnerabilidades de aplicativos da web,de 49% a 41%. No entanto, no primeiro semestre de 2012, as vulnerabilidades de aplicativos da web ressurgiram. A porcentagem projetada de vulnerabilidades de aplicativos da web para 2012 agora é de 47%, com mais de 2.000 reportadas até o momento este ano.

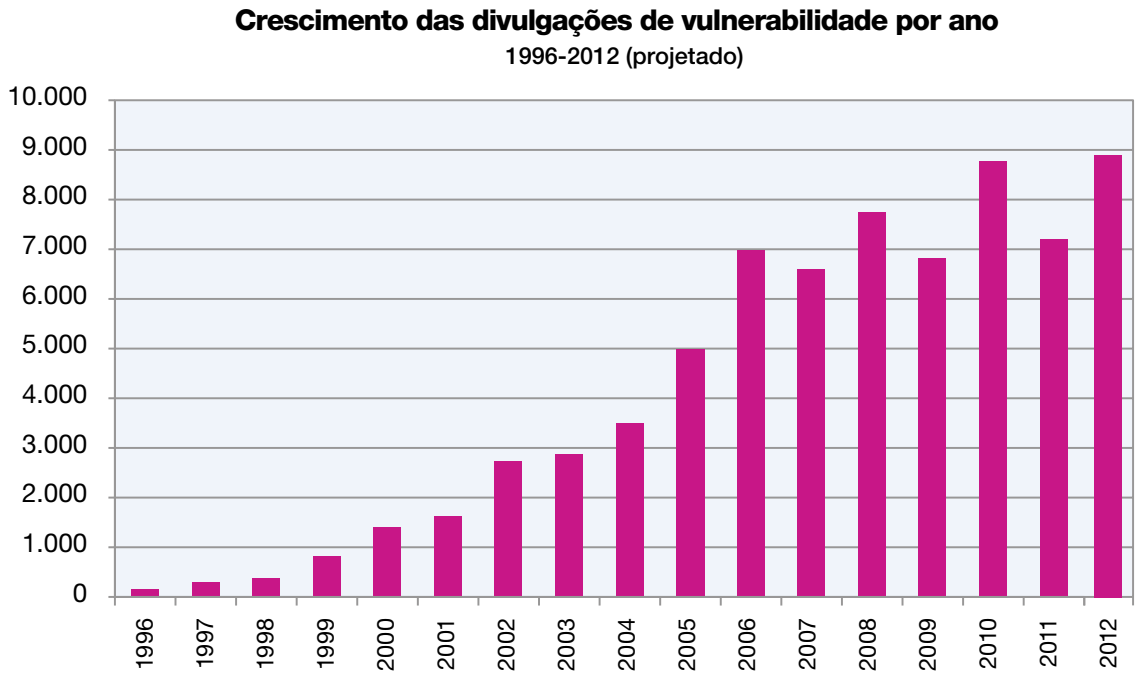


Figura 34: Crescimento das divulgações de vulnerabilidade por ano - 1996-2012 (projetado)

A queda de vulnerabilidades reportadas de SQL injection continuou em 2012, mas as vulnerabilidades de cross-site scripting voltaram a subir, chegando a uma alta projetada recorde. Cross-site scripting é um termo usado para descrever vulnerabilidades de aplicativos da web que permitem que os invasores injetem um script do lado do cliente em páginas da web que são visualizadas por outros usuários. Mais de 51% das vulnerabilidades de aplicativos da web reportadas até o momento em 2012 são categorizados como cross-site scripting. Trata-se de um fato perturbador, pois o cross-site scripting é um problema de segurança bem-conhecido e pesquisado. Nossos dados internos de resultados do IBM AppScan® OnDemand a partir de varreduras de vulnerabilidade de aplicativo da web on demand indicaram uma probabilidade superior a 40% de localizar uma vulnerabilidade de cross-site scripting nessas varreduras on demand ao longo de 2011.

Mais de 51% das vulnerabilidades de aplicativos da web reportadas até o momento em 2012 são categorizados como cross-site scripting.

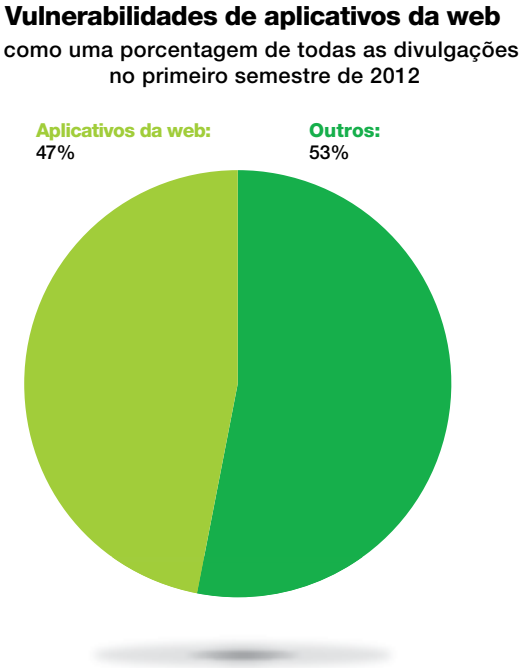


Figura 35: Vulnerabilidades de aplicativos da web como uma porcentagem de todas as divulgações no primeiro semestre de 2012

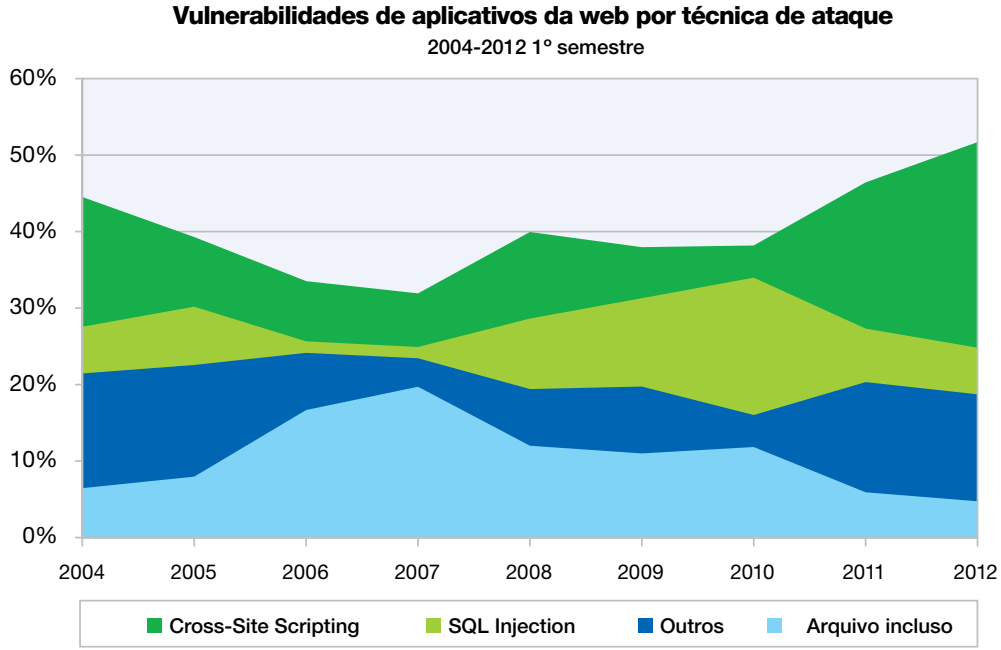


Figura 36: Vulnerabilidades de aplicativos da web por técnica de ataque - 2004-2012 1º semestre

A IBM X-Force constatou que uma grande quantidade das vulnerabilidades de aplicativos da web é divulgada em websites de uso público. Dentre esses aplicativos da web, muitos podem ser atribuídos a plug-ins contidos nos sistemas de gerenciamento de conteúdo (CMS) criados internamente, que são desenvolvidos por empresas de design de website. Com frequência, tais plug-ins não estão disponíveis para comprar separadamente. Todavia, após a ativação do website, o host passa a ser feito pelo consumidor em seu próprio hardware e redes. Diversas vulnerabilidades podem ser encontradas nesses websites de empresas de pequeno porte.

Também existem sistemas de gerenciamento de conteúdo amplamente usados na Internet. Esses principais programas de CMS baseados na web já têm um desempenho melhor ao notificar o público de que vulnerabilidades foram encontradas em plug-ins escritos por terceiros. Em tais programas de CMS, as vulnerabilidades são classificadas como problemas principais e plug-ins. Os problemas principais são corrigidos pela empresa produtora que fornece os sistemas, com uma taxa muito mais alta do que os plug-ins escritos por terceiros.

A Figura 37 demonstra as porcentagens de vulnerabilidades que são classificadas como problemas principais ou de plug-in.

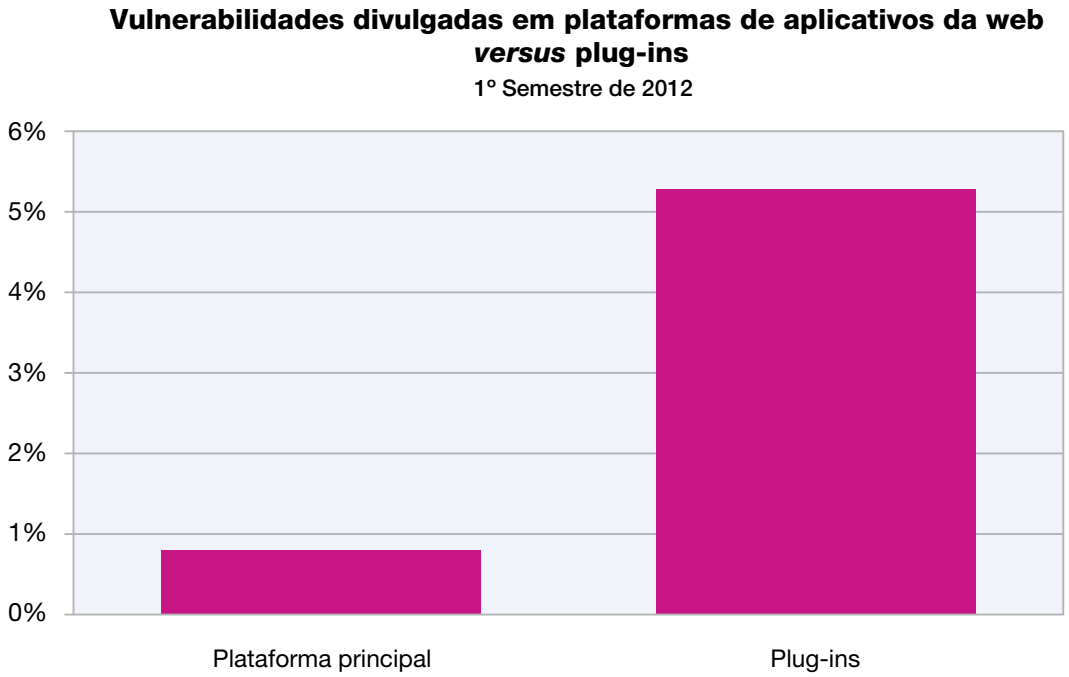


Figura 37: Vulnerabilidades divulgadas em plataformas de aplicativos da web versus plug-ins – 2012

Como é possível ver, menos de 1% de todas as vulnerabilidades de CMS é divulgado com relação aos principais líderes de mercado dos produtores de CMS. Dentre esses líderes, pouco mais de 5% das vulnerabilidades existe em plug-ins de terceiros.

As taxas de correção também são mais altas para as vulnerabilidades principais versus plug-ins. Muitos dos principais programas de CMS começaram a fazer o hosting de listas de extensão de terceiros vulneráveis para notificar usuários e desenvolvedores desses plug-ins de que pode haver um problema em um plug-in implementado por eles.

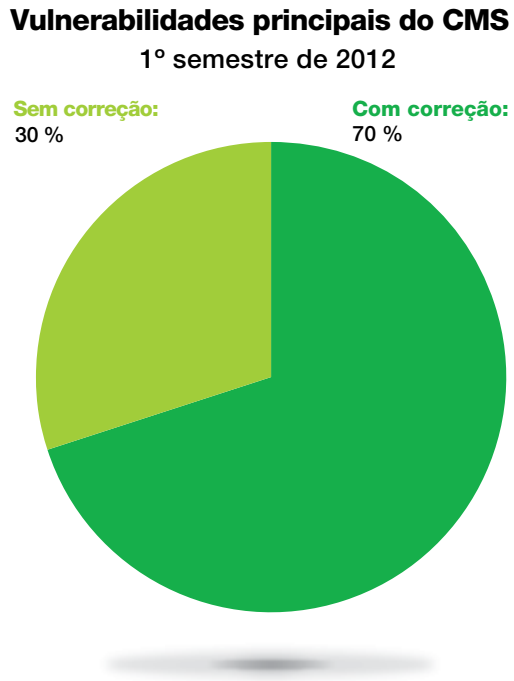


Figura 38: Vulnerabilidades divulgadas nos principais sistemas de gerenciamento de conteúdo – sem correção versus com correção –1º semestre de 2012

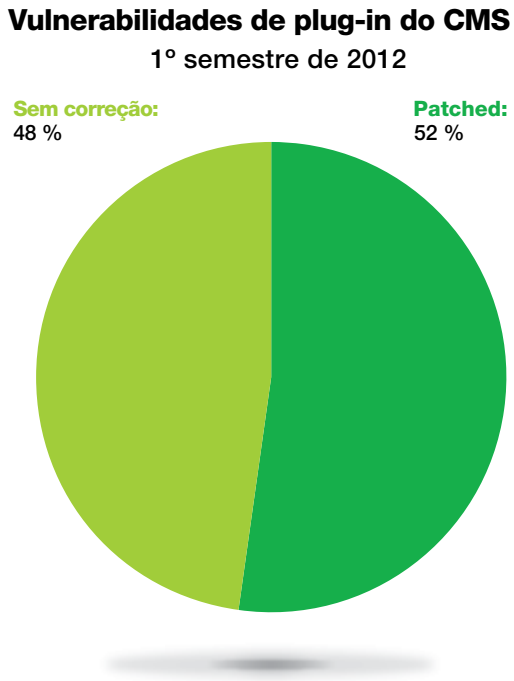


Figura 39: Vulnerabilidades divulgadas em sistemas de gerenciamento de conteúdo de plug-in – sem correção versus com correção –1º semestre de 2012

Queda contínua na contagem de exploração

Em 2011, a IBM X-Force percebeu uma queda significativa nas explorações liberadas publicamente. Duas categorias de explorações foram catalogadas. Os fragmentos simples com código de prova de conceito são contados como explorações, mas programas totalmente funcionais capazes de atacar um computador são categorizados separadamente como "explorações verdadeiras". Ao comparar o número de explorações verdadeiras com a porcentagem total de vulnerabilidades registradas no banco de dados, aparecem tendências interessantes.

Em 2009, a porcentagem de explorações verdadeiras chegou ao auge – quase 16% de todas as vulnerabilidades divulgadas publicamente. Desde então, tem-se observado uma queda nas vulnerabilidades gerais que fez com que o código de exploração verdadeira disponível caísse para quase 11% em 2011.

A tendência continua em 2012, pois, com base nos dados dos primeiros seis meses, projetamos que somente 9,7% de todas as vulnerabilidades divulgadas publicamente conterão explorações. Essas porcentagens não incluem muitas vulnerabilidades de aplicativos da web que podem ser exploradas por meio do uso da barra de endereço em um navegador da web padrão.

Olhando com mais atenção (figura 40, à direita), descobrimos que o número total de explorações verdadeiras é muito menor do que a alta de 2010, mas levemente superior ao total de 2011. Entretanto, se tomarmos as explorações verdadeiras como uma porcentagem do número geral total de vulnerabilidades (como mostrado na Tabela 6), veremos que a tendência é diminuir, aproximando-se da projeção de 9,7%. A IBM X-Force acredita que a queda nas explorações disponíveis publicamente é um resultado direto das mudanças arquiteturais que foram feitas nos softwares nos últimos anos, tornando a exploração dessas vulnerabilidades algo mais desafiador.

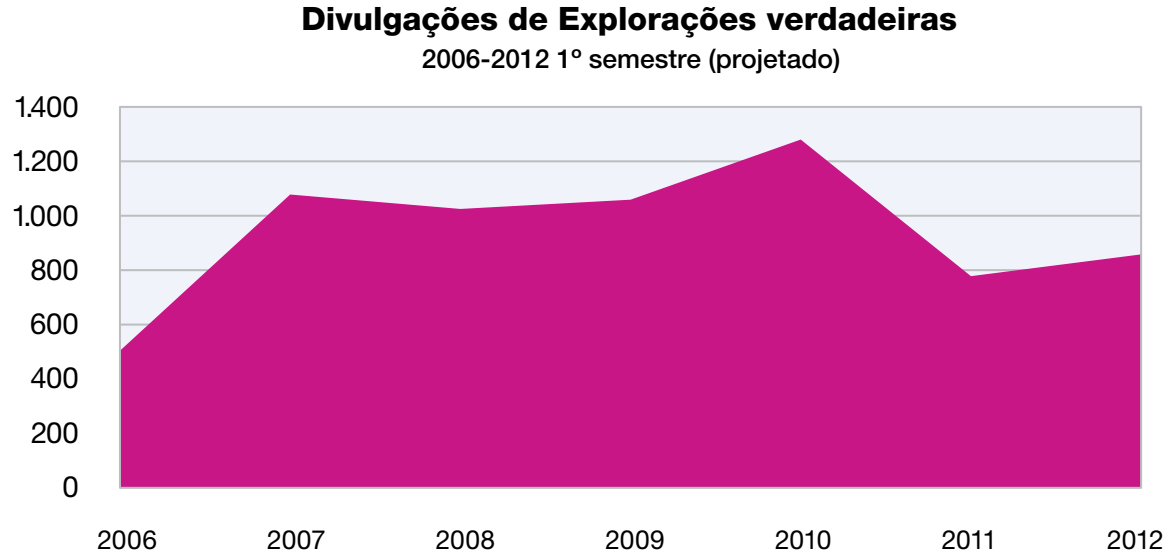


Figura 40: Divulgações de explorações verdadeiras - 2006-2012 1º semestre (projetado)

	2006	2007	2008	2009	2010	2011	2012
Explorações verdadeiras	504	1078	1025	1059	1280	778	858
Porcentagem do total	7,3%	16,5%	13,3%	15,7%	14,7%	10,9%	9,7%

Tabela 6: Divulgações de explorações verdadeiras - 2006-2012 1º semestre (projetado)

A IBM X-Force também percebeu que o número de explorações baseadas em multimídia permaneceu igual aos anos anteriores.

Na área de sistemas operacionais de dispositivo móvel, foi observada uma queda significativa nas explorações disponíveis publicamente. Cada vez mais, os dispositivos móveis se tornam uma parte do nosso dia a dia. Uma preocupação crescente entre os usuários de dispositivos móveis é a segurança desses dispositivos. A IBM X-Force constatou que, no primeiro semestre de 2012, as vulnerabilidades e explorações de dispositivos móveis reportadas chegaram aos níveis mais baixos desde 2008. A nosso ver, muitas coisas estão acontecendo. Em primeiro lugar, os desenvolvedores de sistemas operacionais de dispositivo móvel continuam investindo em descobertas internas de vulnerabilidades e em aprimoramentos em seus modelos de segurança para impedir o sucesso das vulnerabilidades. A seguir, como é comum em uma área nova (como a de dispositivos móveis), costumamos observar um pico inicial de descobertas; porém, à medida que os erros mais fáceis desaparecem e sobram os difíceis de explorar, ocorre um atraso entre os momentos em que os pesquisadores e os invasores descobrem técnicas para superar limitações percebidas anteriormente. Por exemplo, a aplicação da técnica "heap spray" ao cenário de vulnerabilidades do navegador por volta de 2005 permitiu que as vulnerabilidades de distorção de memória alcançassem uma exploração confiável do lado do cliente, uma vez que o spray normalmente garantia que o código de exploração chegasse a locais na memória que, até então, não podiam ser controlados por métodos não programáticos. Apesar disso, ressaltamos que o "heap spray" não era um conceito inteiramente novo.

Divulgações de exploração pública para o navegador
2005-2012 1º semestre (projetado)

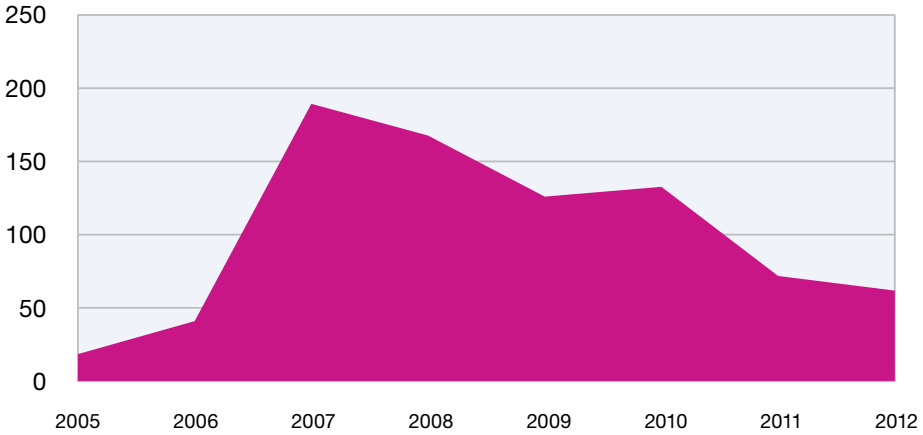


Figura 41: Divulgações de exploração pública para o navegador – 2005-2012 1º semestre (projetado)

Divulgações de exploração pública para multimídia
2005-2012 1º semestre (projetado)

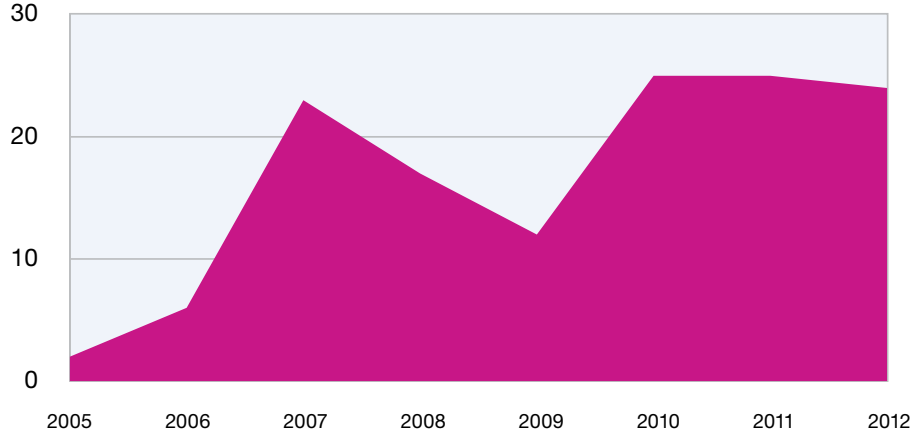


Figura 42: Divulgações de exploração pública para multimídia – 2005-2012 1º semestre (projetado)

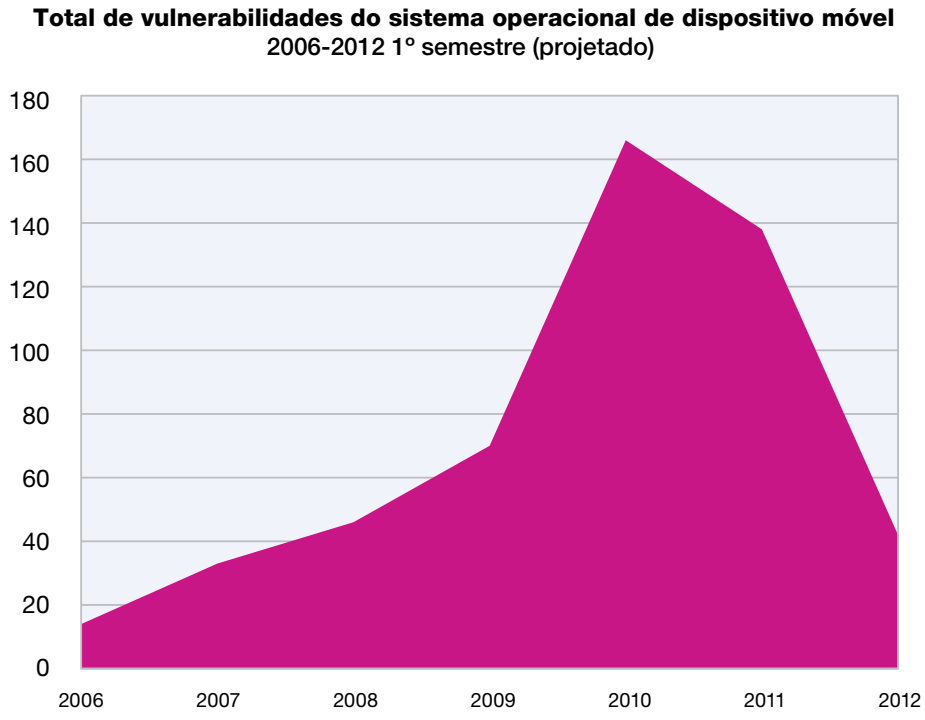


Figura 43: Total de vulnerabilidades do sistema operacional de dispositivo móvel – 2006-2012 1º semestre (projetado)

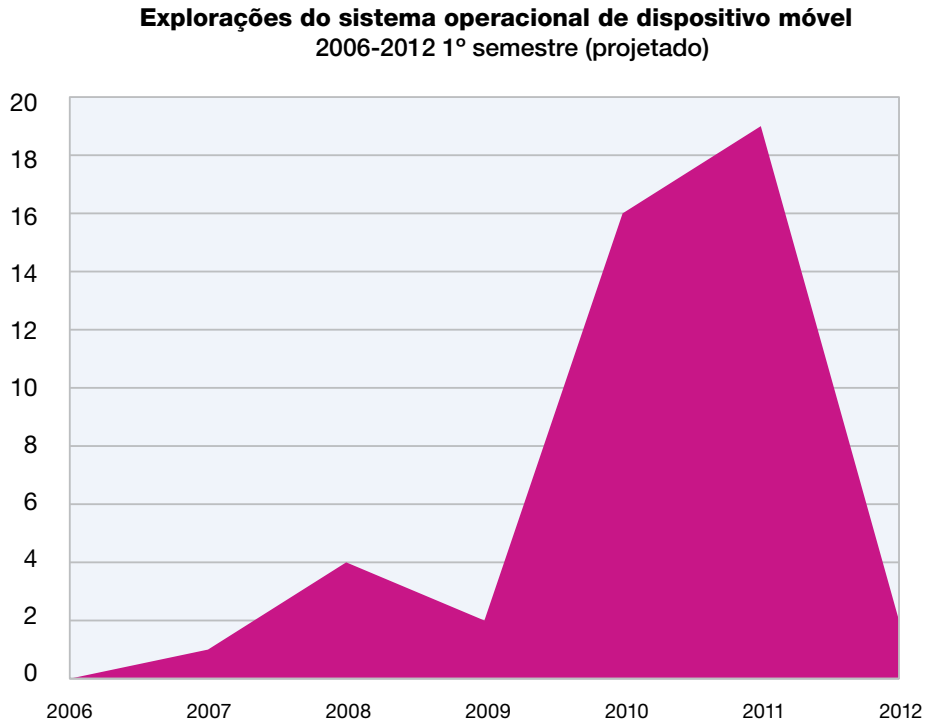


Figura 44: Explorações do sistema operacional de dispositivo móvel – 2006-2012 1º semestre

Pontuação CVSS

A IBM X-Force atribui uma pontuação a quase todas as vulnerabilidades que pesquisamos. Para tanto, utiliza o Sistema de Pontuação de Vulnerabilidade Comum (CVSS), baseado na severidade. Atribuímos uma pontuação às vulnerabilidades a partir de três perspectivas diferentes: como um banco de dados de vulnerabilidade que acompanha divulgações de vulnerabilidade de terceiros, como uma organização de pesquisa de segurança que descobre novas vulnerabilidades e como um grande fornecedor de software que precisa ajudar os clientes a avaliarem com precisão a severidade das vulnerabilidades dentro dos seus produtos. Atualmente, a IBM X-Force está trabalhando junto com outras organizações para desenvolver o novo CVSS versão 3 padrão. Na pontuação de vulnerabilidades para o primeiro semestre de 2012, constatamos que a maioria dos problemas está no intervalo médio, com 27% de todas as vulnerabilidades classificadas como críticas ou de severidade alta.

Pontuação CVSS	Nível de severidade
10	Crítico
7,0-9,9	Alto
4,0-6,9	Médio
0,0-3,9	Baixo

Tabela 7: Pontuação CVSS e nível de severidade correspondente

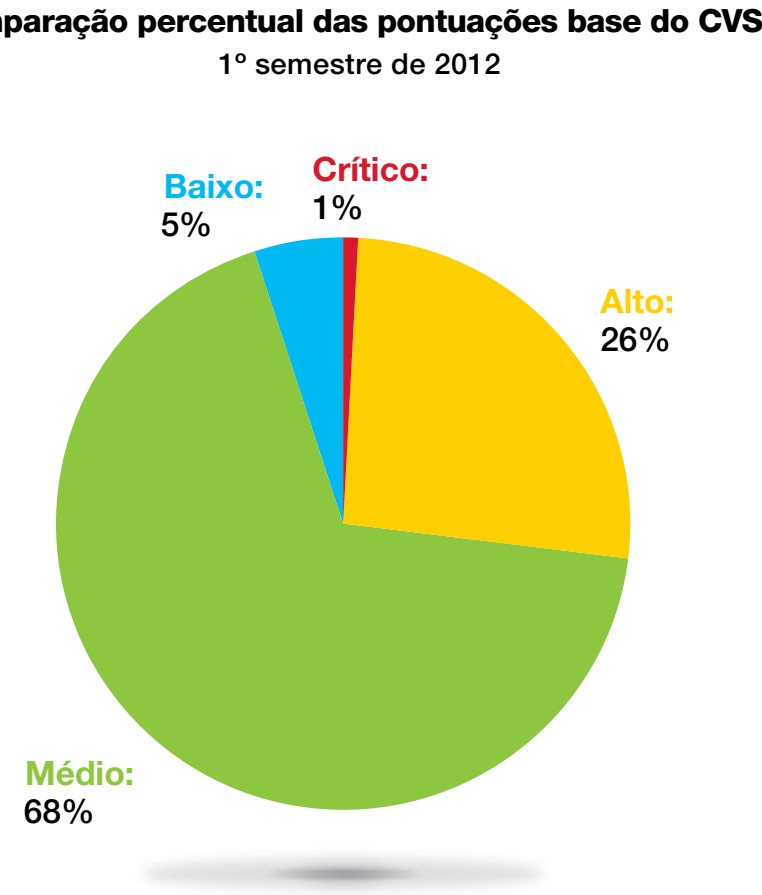


Figura 45: Comparação percentual das pontuações base do CVSS – 1º semestre de 2012

Vulnerabilidades no software corporativo

Ao examinar tendências no software corporativo, a IBM X-Force estuda os principais fornecedores de software que criam a maior variedade de softwares corporativos. Percebemos que, dentre milhares de fornecedores, essas empresas divulgam consistentemente um número significativo de vulnerabilidades de segurança. Tais fornecedores foram categorizados em um grupo com os dez maiores, deixando de fora as vulnerabilidades de CMS, pois a maioria destas está em plug-ins e complementos de terceiros, não sendo amplamente usadas como software corporativo. Desde 2007, temos visto que os dez maiores estão aumentando como porcentagem das vulnerabilidades divulgadas gerais, com até 30% de todas as divulgações feitas em 2011 vindo dos maiores fornecedores de software corporativo. No entanto, no primeiro semestre de 2012, percebemos umaqueda para 22% na porcentagem total de vulnerabilidades divulgadas por essas empresas.

Será uma tendência interessante para acompanharmos até o final do ano, já que o número de vulnerabilidades divulgadas no segundo semestre de 2012 determinará se estamos testemunhando uma tendência descendente notável ou se permanecerão relativamente inalteradas.

Os dez maiores fornecedores de software com o maior número de divulgações de vulnerabilidade

2011-2012 1º semestre

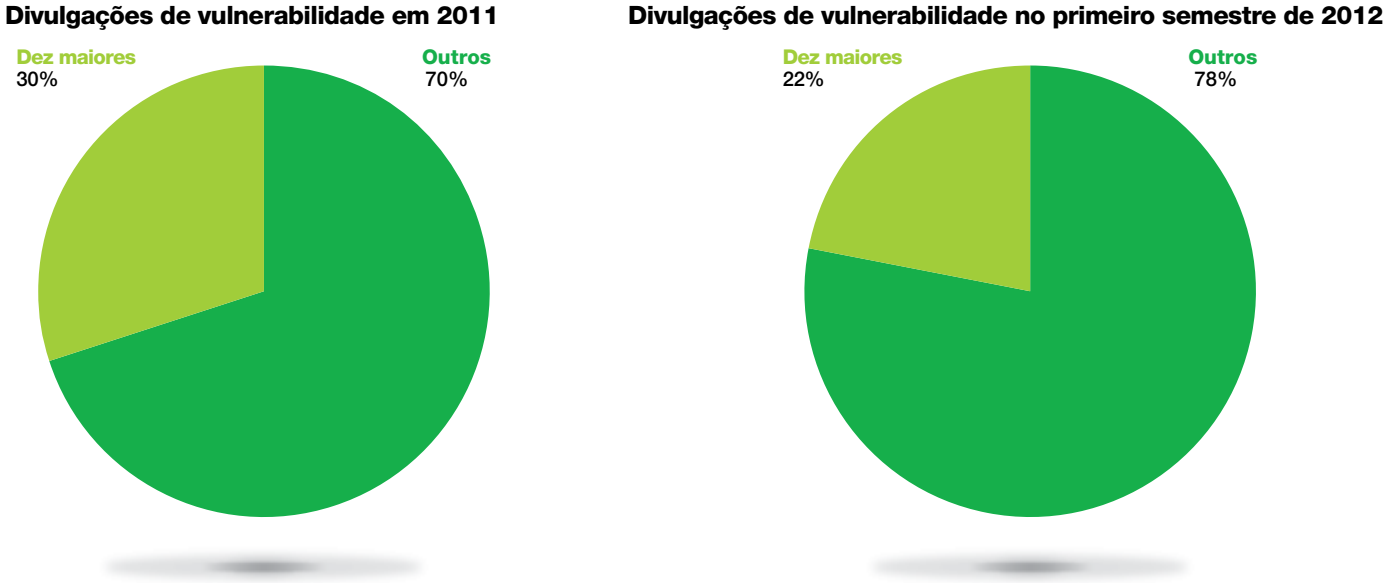


Figura 46: Os dez maiores fornecedores de software com o maior número de divulgações de vulnerabilidade – 2011-2012 1º semestre

A IBM X-Force fez uma descoberta significativa no primeiro semestre de 2012: as vulnerabilidades no Office e Portable Document Format (PDF) diminuíram consideravelmente. Estamos certos de que existe uma forte relação entre a queda de divulgações de PDF e o ambiente de simulação Adobe Acrobat Reader X. Em primeiro lugar, o ambiente de simulação deve aumentar drasticamente a complexidade de criar uma exploração confiável – retornaremos a isso em breve. Por causa da maior dificuldade de criar uma exploração confiável, vulnerabilidades de PDF simples se tornam menos interessantes para os invasores, que optam por não dedicar tempo à descoberta de novas. Os ambientes de simulação podem fornecer esse tipo de benefício ao ecossistema de segurança porque foram criados para diminuir as permissões que os invasores e pesquisadores conseguem obter nos sistemas afetados. Consequentemente, a IBM X-Force prevê a adoção contínua de ambientes de simulação de software para ajudar a desencorajar os invasores e mitigar muitos dos ataques existentes – senão todos.

As vulnerabilidades de navegador da web diminuíram levemente no primeiro semestre de 2012, porém, a uma taxa não tão alta quanto a de problemas no formato de documento. A IBM X-Force espera que o número de vulnerabilidades baseadas no navegador da web permaneça praticamente igual no decorrer de 2012.

A IBM X-Force tem visto grandes progressos na taxa de vulnerabilidades corrigidas dos dez maiores fornecedores, o que pode ser atribuído a práticas de desenvolvimento seguras e à implementação e melhoria contínuas dos programas da Equipe de Resposta a Incidentes de Segurança do Produto (PSIRT). Os dez maiores fornecedores têm uma taxa de recurso de correção de pouco mais de 94% de todas as vulnerabilidades divulgadas.

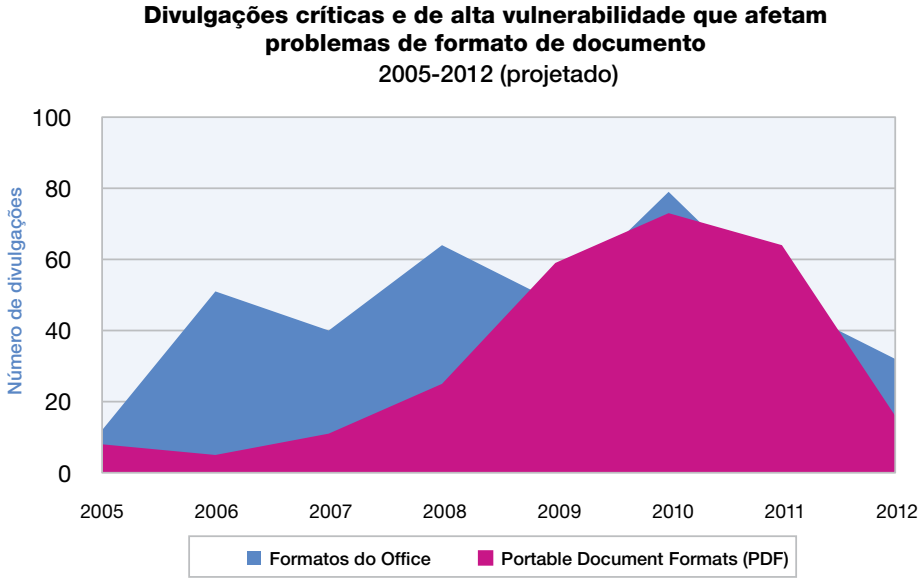


Figura 47: Divulgações críticas e de alta vulnerabilidade que afetam problemas de formato de documento – 2005-2012 (projetado)

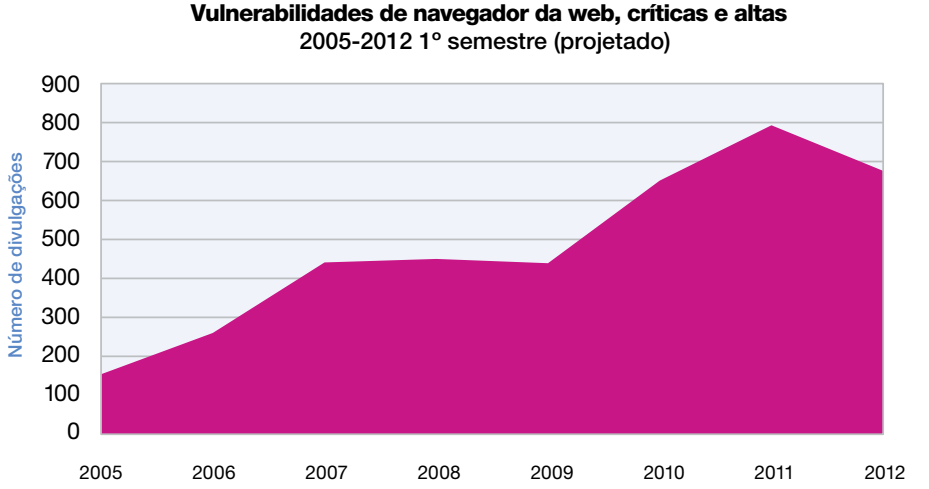


Figura 48: Vulnerabilidades e navegador da web, críticas e altas – 2005-2012 1º semestre (projetado)

São boas notícias para os dez maiores fornecedores de software; no entanto, não podemos dizer o mesmo sobre o restante do mundo da vulnerabilidade. A taxa de vulnerabilidades não corrigidas no primeiro semestre de 2012 foi a mais alta vista pela IBM X-Force desde 2008. Quarenta e sete por cento de todas as vulnerabilidades divulgadas este ano continuam sem um recurso.

A IBM X-Force não acredita, necessariamente, que o aumento de vulnerabilidades sem correção é um mau sinal. Os principais fornecedores de software corporativo estão fazendo um trabalho muito melhor hoje do que faziam cinco anos atrás. Achamos que o aumento das vulnerabilidades em aplicativos da web pequenos – e softwares obscuros feitos por pessoas ou empresas minúsculas – é responsável pelo aumento em 2012. Muitas dessas vulnerabilidades provavelmente ficarão sem correção ou sem suporte ao longo do tempo de vida do produto.

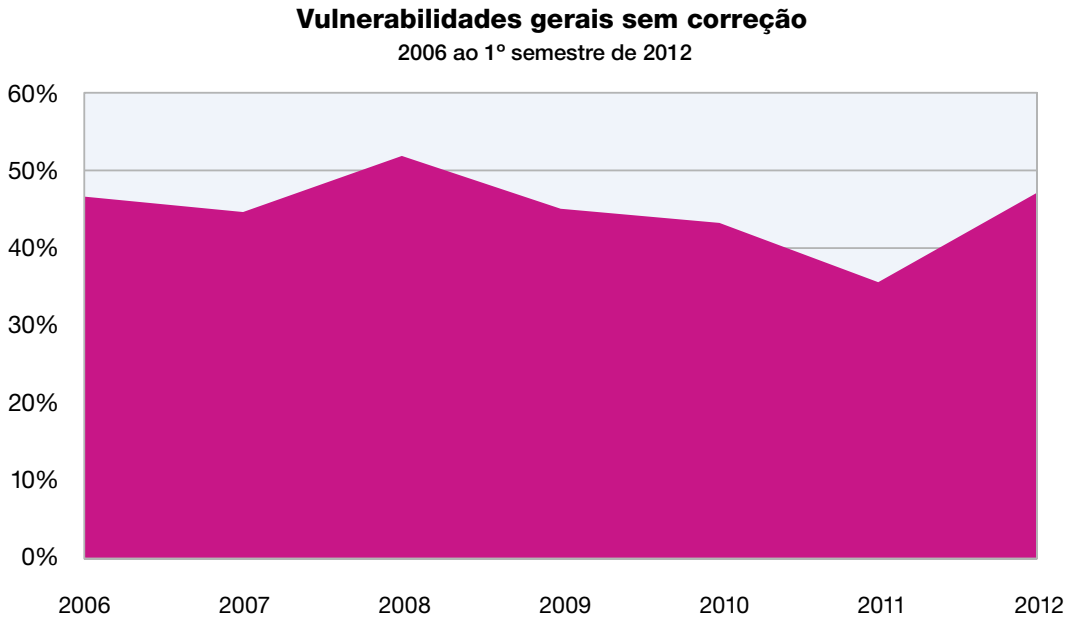


Figura 49: Vulnerabilidades gerais sem correção – 2006 ao 1º semestre de 2012

Conclusão

Em comparação com o último relatório, ocorreram descobertas surpreendentes em apenas algumas áreas principais. Como foi dito, a porcentagem de vulnerabilidades sem correção aumentou, mas com a ressalva de que são softwares mais obscuros, dificilmente encontrados em uma empresa. Em segundo lugar, houve uma queda drástica nas vulnerabilidades e explorações direcionadas à plataforma móvel. Novamente, a IBM X-Force vê vários motivos diferentes para isso, mas recomendamos que os leitores permaneçam vigilantes em relação aos seus dispositivos móveis – sejam próprios ou gerenciados pelo empregador. Sugerimos isso porque, com todas as distrações de trabalhar em movimento, podemos esquecer facilmente de aplicar os mesmos processos de pensamento centralizados na segurança. Por exemplo, você pode não aplicar o mesmo rigor aos emails de phishing recebidos no seu dispositivo móvel ou prestar atenção às permissões de segurança que um aplicativo remoto exige. Os ataques mais simples serão, portanto, os que têm maior probabilidade de ocorrer em 2012 – e falaremos mais sobre isso na seção de segurança de dispositivos móveis deste relatório.

A terceira área de tendência interessante está relacionada à efetividade dos ambientes de simulação de software em termos de mitigação de ataques e de desencorajar os pesquisadores e invasores de descobrir e divulgar vulnerabilidades que não conseguem passar pelas permissões reduzidas do ambiente de simulação. Para que esses ataques sejam realizados com sucesso, é necessário implementar diversas vulnerabilidades – normalmente, desativando o ambiente de simulação ou encontrando uma vulnerabilidade no ambiente de simulação de forma que o cenário de exploração se torne um processo duplo de explorar uma vulnerabilidade exposta pelo software e, depois, utilizar outra vulnerabilidade com relação ao ambiente de simulação para elevar os privilégios de alguém a ponto de comprometer o sistema. Algumas vulnerabilidades com relação aos ambientes de simulação de software foram reportadas por pesquisadores, como os Pesquisadores da IBM X-Force em 2011 e 2012, e provavelmente usadas em ataques avançados e direcionados. Os ambientes de simulação de software são uma área empolgante para fornecedores de software, pesquisadores de segurança e profissionais de segurança. Já falamos sobre a queda nas vulnerabilidades e na exploração de PDF com base nas contramedidas fornecidas pela Adobe. Agora, passaremos ao entendimento da tecnologia de criação de ambiente de simulação.

Ambientes de simulação: Outra linha de defesa

O que é um ambiente de simulação?

Imagine receber um alerta de que um assaltante conseguiu entrar na sua casa ou escritório. Naturalmente, uma das suas primeiras preocupações será o que fazer. Mas há outra pergunta igualmente importante: "o que será roubado e quais danos serão causados?". O assaltante tem acesso total a todas as suas posses – joias, produtos eletrônicos, documentos de negócios importantes ou propriedade intelectual. Também está livre para fazer o que bem entender na sua casa ou escritório, inclusive destruir propriedades. E se o assaltante for contratado por um concorrente? Pode instalar equipamentos de vigilância ocultos no seu escritório?

Agora, imagine a mesma situação – porém, em vez de sua casa ou escritório, o assaltante é um invasor remoto que conseguiu entrar no seu computador. A principal tarefa de um ambiente de simulação é limitar o que esse invasor remoto pode fazer ou acessar depois de infiltrar seu sistema.

Como os ambientes de simulação funcionam

Os ambientes de simulação isolam um aplicativo do resto do sistema fazendo com que, no momento em que ele é comprometido, o código do invasor executado em seu interior fique limitado com relação ao que pode fazer ou o que pode acessar.

A criação de ambiente de simulação pode acontecer de várias maneiras. Veja a seguir alguns métodos usuais para isolar um aplicativo do resto do sistema:

1. **Virtualização de recursos –** Envolve fornecer a um aplicativo (ou a um sistema operacional por inteiro) um conjunto de recursos virtuais, tais como discos virtuais, para que as mudanças nesses recursos virtuais não afetem os recursos reais. Um exemplo é a virtualização de recursos feita por um software de virtualização como Xen e VirtualBox.
2. **Redução de privilégio –** Envolve a redução dos privilégios e recursos de um aplicativo usando mecanismos existentes que são fornecidos pelo sistema operacional. Os exemplos incluem o ambiente de simulação do Google Chrome, o ambiente de simulação do Adobe Reader X e as implementações diferentes do ambiente de simulação do Adobe Flash Player.

3. **Execução controlada –** O aplicativo é executado em um ambiente controlado em que não há acesso direto ao sistema operacional. É necessário usar interfaces específicas para poder executar ações privilegiadas. Um exemplo é o ambiente de simulação do Java.

Os aplicativos com ambiente de simulação usam os serviços expostos por um aplicativo de privilégio superior (normalmente chamado de broker) para executar ações privilegiadas. Por outro lado, o broker consulta um conjunto de políticas para determinar se a ação privilegiada será permitida ou recusada.

Os ambientes de simulação podem ajudá-lo

Dependendo de como o ambiente de simulação foi implementado e quais políticas estão em vigor, um ambiente de simulação pode oferecer as proteções a seguir:

- Ajuda a prevenir a instalação de malwares persistentes no seu sistema, porque o acesso de gravação a recursos importantes não foi aprovado. O invasor não será capaz de modificar partes críticas do seu sistema e não conseguirá instalar um malware que possa sobreviver a uma reinicialização do sistema.
- Ajuda a prevenir a divulgação de informações, porque o acesso de leitura a recursos importantes e o acesso à rede não foram aprovados. O invasor não será capaz de acessar seus arquivos pessoais ou de enviá-los a um local remoto.
- Ajuda a prevenir danos ao seu sistema, porque a modificação de partes críticas do sistema e mudanças na configuração do sistema não foram permitidas.

Como nem todas as implementações de ambiente de simulação são iguais, é muito importante entender os recursos e limitações da implementação de ambiente de simulação que será utilizada. É possível consultar as publicações fornecidas pelo fornecedor e as pesquisas feitas pelos pesquisadores de segurança que observaram e avaliaram o ambiente de simulação, como a pesquisa do ambiente de simulação do Adobe Reader X[17] ou a pesquisa do ambiente de simulação do Adobe Flash Player[18].

O que pode ser feito agora

Uma maneira relativamente discreta de aproveitar os benefícios de um ambiente de simulação é determinar se os aplicativos usados pela sua organização têm versões com ambiente de simulação mais recentes e, em caso afirmativo, testá-las, implementá-las e utilizá-las.

Para começar, é possível observar os aplicativos que consomem conteúdo da Internet, tais como leitores de documentos, visualizadores de mídia, navegadores e plug-ins de navegador. Felizmente, alguns fornecedores já oferecem versões com ambiente de simulação dos seus produtos. Alguns exemplos de aplicativos com ambiente de simulação para a plataforma Windows são:

- Para Conteúdo da Web
  - — Google Chrome
  - — Internet Explorer 7 e versões mais recentes no Windows Vista e sistemas operacionais mais recentes
- Para Conteúdo de PDF
  - — Adobe Reader X (também conhecido como Adobe Reader 10) e versões mais recentes
  - — Visualizador de PDF integrado no Google Chrome
- Para Conteúdo de Flash
  - — Adobe Flash Player 11.3 e versões mais recentes (atualmente com ambiente de simulação no Firefox no Windows Vista e sistemas operacionais mais recentes apenas)
  - — Visualizador de Flash integrado no Google Chrome (também conhecido como Pepper Flash)
- Para Documentos
  - — Microsoft Office 2010 (no modo de Visualização Protegida)

Lembre-se de que existem ataques oportunistas direcionados a versões de aplicativos mais antigas e sem ambiente de simulação e que um ambiente de simulação age como mais uma linha de defesa contra tais ataques.

17 https://media.blackhat.com/bh-us-11/Sabanal/BH_US_11_SabanalYason_Readerx_WP.pdf
18 https://media.blackhat.com/bh-us-12/Briefings/Sabanal/BH_US_12_Sabanal_Digging_Deep_WP.pdf

O que podemos esperar

A implementação de um ambiente de simulação customizado é cara. Os custos incluem pesquisa, desenvolvimento, teste e manutenção. Acreditamos que os recursos de criação de ambiente de simulação para a maioria dos aplicativos de prateleira que precisam deles serão fornecidos pelo próprio sistema operacional. Atualmente, isso é feito como parte do recurso AppContainer no Windows 8 e do recurso App Sandbox no OS X. Espera-se que existam casos em que o ambiente de simulação oferecido pelo sistema operacional não forneça controle granular suficiente para alguns aplicativos. Nesses casos, ainda haverá espaço para ambientes de simulação customizados.

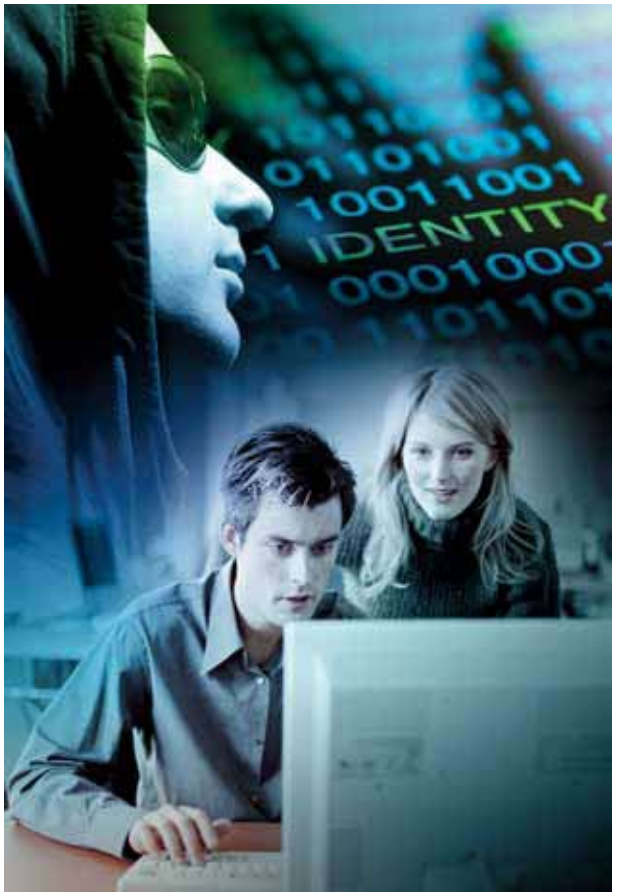
De qualquer modo, os sistemas operacionais provavelmente serão atualizados de forma contínua para incluir mecanismos adicionais que restrinjam os privilégios e recursos de um aplicativo. A maioria dessas restrições será aplicada por padrão, pois, se pensarmos bem, todo aplicativo executado não precisa realmente de acesso aos seus documentos pessoais.

Os invasores se adaptarão

À medida que os fornecedores continuam integrando recursos de criação de ambiente de simulação aos seus produtos, os invasores precisarão de uma vulnerabilidade separada para comprometer um sistema totalmente. Para o invasor, isso significa custos mais elevados no desenvolvimento de um ataque completo – e que as vulnerabilidades de escape do ambiente de simulação terão um valor maior. É provável que os invasores se adaptem alocando investimentos adicionais para descobrir e/ou adquirir vulnerabilidades de escape do ambiente de simulação.

Ideias finais

Naturalmente, a tecnologia de criação de ambiente de simulação não é infalível e um invasor motivado com recursos suficientes pode encontrar maneiras de escapar de um ambiente de simulação. Por isso, ainda precisamos ser vigilantes. A complacência pode causar problemas – mesmo se nos derem um capacete e um colete à prova de balas, não significa que podemos correr em uma linha de tiro, sentindo-nos invencíveis. Reduza a superfície de ataque desinstalando ou desativando aplicativos, recursos e plug-ins de navegador não utilizados, além de manter seu software atualizado. Também é uma boa ideia educar os usuários quanto aos perigos de abrir conteúdo não solicitado.



Auditoria facilitada com o registro histórico de data e hora do shell do UNIX

Para analistas de computadores, saber o horário em que os eventos ocorreram é um grande desafio ao investigar um incidente de segurança. O UNIX fornece um sistema de auditoria útil na forma do arquivo histórico do shell. Por padrão, esse arquivo não está sempre configurado para fazer um registro de data e hora junto com o comando, o que dificulta correlacionar eventos a uma linha de tempo.

Os analistas dos Serviços de Resposta a Emergências IBM (ERS) que executaram análises póstumas computadorizadas detalhadas de dezenas de casos UNIX/Linux perceberam que somente alguns pareciam ter os valores HISTIMEFORMAT configurados. A IBM X-Force acredita que tal configuração ajuda a entender o horário em que os comandos foram emitidos pelos usuários do sistema UNIX/Linux.

Por exemplo, o arquivo histórico do shell pode registrar uma instância em que um usuário digitou **`ping 192.168.100.10`**, mas, se não houver um packet sniffer ou uma entrada de log do firewall, não ficará aparente exatamente quando o comando foi digitado.

Os analistas de ERS que trabalham com UNIX – especificamente Linux, para os fins deste artigo – apoiam a importância de incluir registros de data e hora no arquivo histórico. Nosso objetivo é conscientizar sobre a implementação dessa técnica em servidores de produção para analistas de segurança e administradores de sistema.

Shells de comando do UNIX, como shell C (csh), shell Korn (ksh) e Shell Borne Again (bash), fornecem uma "instalação histórica" que é mantida como um relato de atividades individuais. Basicamente, mantém um registro de cada comando digitado (e digitado incorretamente, em caso de erro) no ambiente de linha de comandos por um usuário que efetuou login.

Os analistas de computador podem usar o conteúdo do arquivo histórico (.bash_history) para acompanhar atividades sempre que uma intrusão na conta do computador possa ter ocorrido ou quando eventos suspeitos semelhantes estão sendo investigados.

Entretanto, são muitos os problemas possíveis. Os dados contidos nos arquivos históricos que pertencem a uma conta do usuário não são imutáveis e podem ser alterados ou destruídos.

Além disso, um recurso para colocar os registros de atividades em uma linha de tempo precisa raramente é usado.

Considere o usuário hipotético Joe Black, que digita os comandos a seguir enquanto trabalha na empresa fictícia Acme.

```
telnet fs1.acme.com
```

Ao acessar o recurso fs1.acme.com, Joe emitiu estes comandos de acordo com seu arquivo histórico:

```
mail bigcheese SUBJ: Resignation
rm -rf *
```

A presença desses comandos sugere que Joe Black efetuou login no FileServer1, comunicou ao chefe algo relacionado a uma demissão e emitiu um comando de destruição de dados. Porém, sem os registros de data e hora, não é possível saber quando essas atividades ocorreram – o que é um fator crítico para explicar aos funcionários e à equipe quando a análise é realizada e colocada em termos significativos. Vamos examinar uma solução possível.

Para os objetivos desta discussão, examinaremos uma interação de sistema de computador host Linux e linha de comandos com o Shell Borne Again (bash). Ao examinarmos a configuração do perfil dos usuários, podemos introduzir um recurso para instituir o registro de data e hora de uma forma que seja útil para o examinador, bem como para os gerentes e administradores de sistema do host Linux.

A linha de código a seguir – que pode ser acrescentada ao arquivo /etc/profile – coloca a mudança em vigor:

```
export HISTTIMEFORMAT="%s %T%z
%d/%b/%y "
```

Essencialmente, isso atribui um registro de data e hora a cada comando inserido, enquanto um usuário efetua login no shell e interage com ele. Além disso, a configuração de data permite que os horários sejam inseridos como Horário Unix Epoch, o que pode simplificar a análise desses arquivos históricos e coloca o horário em termos legíveis. O horário Unix Epoch é o número de segundos transcorridos desde 00:00 (UTC) em 01 de janeiro de 1970. Os espaços na linha de comandos acima melhoram a capacidade de leitura da saída.

A saída também informa o fuso horário em vigor quando a entrada foi feita, ajudando a confirmar a configuração ou a detectar qualquer configuração incorreta. Isso é importante, pois os profissionais de TI precisam saber qual fuso horário está ativo ao examinar os registros.

É necessário considerar uma ressalva importante durante essa configuração. Você precisa armazenar os arquivos históricos existentes se fizer a configuração em um sistema que já tem um histórico estabelecido. Se isso não for feito, todos os eventos anteriores ao momento em que o comando 'export=HISTTIMEFORMAT' foi inserido no perfil estarão com a data incorreta. Sem dúvida, pode ser um problema grave.

Antes de configurar o HISTTIMEFORMAT, lembre-se de fazer backup e armazenar todos os arquivos .bash_history existentes. Uma abordagem é usar um loop 'for-do' que procura e localiza além dos arquivos .bash_history e, em seguida, os armazena em um arquivo tar-gz (usando o shell bash no Linux).

```
$ sudo tar -czvf `date "+%d%e%Y"-
history.tar.gz ` $find( -f /home -type
f -name '*history')
```

O resultado é a criação de um arquivo 'tar.gz', com a data do backup dos arquivos históricos. Após executar esse comando, é possível limpar o arquivo .bash_history (renomeando-o, o que pode ser revertido sempre) e depois implementar um registro de data e hora chamando o seguinte:

```
$ mv ~/.bash_history ~/.OLD_bash_
history

$ echo export HISTTIMEFORMAT="%s
%T%z%d/%b/%y " >> ~/.bash_profile

$ history -c && exit
```

Ao chamar o histórico (com o comando 'history'), você verá entradas semelhantes às mostradas aqui:

```
$ history
1 1341870050 14:40:50-0700 09Jul2012
history
```

Isso significa que o arquivo .bash_history mantém registros de registros de data e hora no arquivo real. O próprio arquivo manteria um registro do registro de data e hora junto com o comando, o que é mostrado aqui:

```
#1341870056 exit

#1341870112
tcpdump -i eth0 host 192.168.100.12
-s 0 -w ./PacketCapture.pcap

#1341870112
tcpdump -n -r PacketCapture.pcap

#1341870452
history
```

Se chamar o registro de histórico (inserindo o comando 'history' no shell), você verá o tipo de exibição a seguir, porque o shell bash usa o formato da variável HISTTIMEFORMAT para apresentar os dados de uma forma útil para o usuário, como mostrado aqui:

```
1 1341870056 14:40:56-0700 09Jul2012
exit

2 1341870112 14:41:52-0700 09Jul2012
tcpdump -i eth0 host 192.168.100.12 -s

0 -w ./PacketCapture.pcap

3 1341870274 14:44:34-0700 09Jul2012
tcpdump -n -r PacketCapture.pcap

4 1341870452 14:47:32-0700 09Jul2012
history
```

Além de fornecer um entendimento rápido dos comandos que foram inseridos e da ordem em que isso aconteceu, também fica evidente o fuso horário em que o host está.

O motivo de vermos somente a entrada de horário Unix Epoch no próprio arquivo histórico 'raw' em vez de vermos o horário Unix Epoch e a entrada legível (14:47:32-0700 09Jul2012) não é relevante. Depois que o shell percebe que o valor HISTIMEFORMAT foi configurado, os registros são armazenados no arquivo da maneira mais exata possível (horário Unix Epoch) e a exibição renderiza uma conversão simples, o que a torna significativa para aqueles que revisam os registros de histórico. Também é útil para membros da equipe de ERS, pois podem facilmente procurar em um sistema de arquivos quaisquer entradas excluídas e recuperar aquelas que parecem ter a estrutura de dados com registro de data e hora depois de aprenderem que um sistema havia capacitado os valores HISTIMEFORMAT.

Considere logs de eventos correlatos, registros de data e hora de arquivos ou capturas de pacotes de rede que registram quando a entrada de log foi feita, o horário em que um arquivo foi acessado ou modificado ou o horário em que os pacotes foram transferidos. Assim, fica mais fácil atribuir ações e observações com o histórico do comando do shell.

Para ilustrar a simplicidade desse histórico com registro de data e hora em ação, segue uma lista de eventos que ocorreram durante a correlação de registros e arquivos de captura de pacotes de rede, sendo executados por uma ferramenta de software livre conhecida pela análise da linha de tempo dos artefatos.

Nas listas a seguir, pegamos os arquivos .history do usuário raiz a partir de um servidor designado como 'VICTIMSRV' e os integramos nos arquivos de log de eventos do syslog, atributos de registro de data e hora das atividades do arquivo (tais como modificado, acessado, criado e entrada atualizada) e capturas de pacote. Os valores dessas quatro origens de dados díspares esclarecem a ordem dos eventos, assim como os comandos emitidos pelo usuário raiz.

```
Tue Jul 10 15:02:17 2012 Z
PCAP  192.168.100.10    - -   ICMP
packet 192.168.100.10 ->
192.168.100.12|PST8PDT|File: KSServer.
pcap.pcap inode:1872361
HISTORY VICTIMSRV root - ping
192.168.100.10

Tue Jul 10 15:01:58 2012 Z
LOG   VICTIMSRV   - - (Linux Syslog
Log File) [Entry written] [passwd]
log event on [victimsrv] by [pam_
unix(passwd:chauthtok)] : "password
changed for tmillar "|PST8PDT|File:
secure inode:11334
FILE  VICTIMSRV   - MA.E      /etc/
shadow

Tue Jul 10 15:01:32 2012 Z
HISTORY VICTIMSRV root - passwd
tmillar
```

É evidente quando a raiz do ID do usuário alterou a senha para o ID do usuário tmillar. Além de uma entrada de log que respalda essa asserção, o arquivo /etc/shadow mostra que uma modificação foi feita naquele horário. Ademais, o comando emitido a partir do arquivo histórico mostra que o comando foi emitido momentos antes das mudanças. É fácil perceber que o usuário digitou o ping 192.168.100.10 e essa entrada de registro correlaciona-se muito bem com a da entrada com registro de data e hora dentro de uma captura de pacote realizada na rede usando outro host.

A inclusão de um registro de data e hora no histórico do shell é capaz de reunir muitas informações díspares em uma linha de tempo de eventos sucinta.

É possível que isso já esteja ativado em hosts UNIX/Linux, especificamente em servidores críticos. Do contrário, considere nossas recomendações.

Como analistas investigativos, é importante saber como ativar os registros de data e hora nos arquivos históricos. O ideal seria implementar isso antes de tentar investigar um incidente. Ao estabelecer o valor HISTTIMEFORMAT, deve ser mais fácil relembrar rapidamente os comandos usados para manter o sistema ou até mesmo identificar ocorrências incomuns quando acontecerem.

Avaliando o terreno cibernético com o OCOKA

Com discussões de ciberguerra, invasores e defensores, é necessário ter a capacidade de avaliar uma rede como um terreno em que uma batalha será travada. Trata-se de uma batalha entre o invasor – que está tentando ganhar acesso, roubar dados, destruir informações ou cometer crimes – e os defensores, que tentam proteger suas redes dos invasores. As redes podem ser vistas como um terreno se considerarmos as semelhanças: perímetros, pontos de acesso (gateways), desafio e senha (nome de usuário e autenticação de senha), terreno principal (contas, servidores e dados sensíveis), postos de observação (IDS/IPS) e aqueles que ocupam e defendem o terreno (usuários, segurança).

O exército tem um processo para quase tudo que faz e um desses processos consiste em avaliar o terreno que a unidade irá defender ou percorrer. Esse mesmo processo de avaliação – conhecido pelo acrônimo OCOKA (Observação [*Observation*], Encobrimento [*Concealment*], Obstáculos [*Obstacles*], Terreno Principal [*Key Terrain*] e Vias de Abordagem [*Avenues of Approach*] – pode ser usado para avaliar o terreno do seu ambiente de rede pela perspectiva do defensor e do invasor.

O	Observação
C	Encobrimento
O	Obstáculos
K	Terreno Principal
A	Vias de Abordagem

O Observação

Observação é a capacidade dos defensores da rede de observarem as atividades do invasor e a capacidade do invasor de visualizar e obter dados sobre a rede e a partir dela. Os métodos de observação costumam incluir:

Defensor

- Logs de rede – firewall, Detecção de Intrusão / Sistema de Prevenção (IDS/IPS), VPN e Proxy
- Arquivos de log do servidor – DNS, Controlador de Domínio e console de rede de antivírus
- Arquivos de log do host – logs de eventos do Windows, logs de varredura de AV, logs de firewall e logs de acesso do Linux
- Logs do aplicativo – web, email, SharePoint e FTP
- Treinamento de reconhecimento do usuário que cria uma cultura de "chamada de emergência" para suspeitas de eventos de segurança

Invasor

- Reconhecimento para identificar exposições de sistema e de dados. As informações recuperadas por esse processo podem variar da descoberta de portais de acesso e aplicativos remotos que não exigem autenticação a relatórios de varredura de vulnerabilidades expostas.
- Capturas de pacote de rede e amostras usando tcpdump, sn.exe ou programas similares são utilizadas para tentar capturar dados ou identificar segmentos de rede que têm dados de cartão de crédito ou outros dados sensíveis.
- Nmap e outras varreduras das redes externas e internas podem ser utilizadas em um esforço para identificar as principais áreas da rede a serem atacadas.
- O acesso físico às instalações pode ser utilizado para obter informações sobre a rede.
- Monitorar e comprometer as contas de email de executivos e respondentes a incidentes. Isso pode ser feito de modo muito simples, como uma regra de encaminhamento de conta para emails.
- Uso da conta do administrador local para ocultar a utilização da conta dos esforços de observação de rede.

Recomendações

Valide e monitore os sistemas de observação defensivos. Para serem efetivos, os mecanismos de observação de defesa precisam estar funcionando adequadamente e serem monitorados. É necessário tratar os alertas com uma resposta planejada apropriada. Não raro, durante a investigação de um incidente, respondentes a incidentes, como os Serviços de Resposta a Emergências IBM (ERS), descobrem que os mecanismos de criação de log não estavam funcionando adequadamente (tamanho de log inadequado, resultando na rolagem frequente de logs ou criando logs apenas para eventos de sucesso). Indicações extensivas de atividades maliciosas podem estar presentes nos logs, mas, como o monitoramento dos logs não foi realizado, a intrusão passou despercebida. Com recursos de observação monitorada suficientes, as chances de detectar um ataque aumentam. Com poucos ou nenhum recurso de observação ou com recursos que não são monitorados nem recebem resposta, a probabilidade de ataques não detectados e bem-sucedidos aumenta.

Obtenha um reconhecimento situacional das ameaças. Apesar de não ser diretamente um método de observação, os defensores devem participar de organizações como a IBM X-Force Threat Analysis Service (XFTAS), FIRST e Infraguard para obter uma compreensão das ameaças atuais e tendências de ataque. Isso fornece um reconhecimento situacional das tendências atuais de ataque e ajuda a reconhecer melhor os indicadores de ataque quando os observar.

Treine e forneça. Treine equipes de segurança para examinar logs, avaliar conteúdo para indicadores de atividade maliciosa e responder a eventos e incidentes. Forneça-lhes recursos de observação adequados para uma observação de segurança, não apenas para observação de desempenho. Providencie uma equipe de segurança para monitorar logs de eventos de segurança dentro da rede.

C Encobrimento

Encobrimento refere-se à capacidade dos defensores da rede de ocultarem a arquitetura e os dados da rede, especialmente partes da rede ou de dados de alto risco, de invasores. Também inclui a capacidade do invasor de esconder suas ações maliciosas dos defensores. Várias técnicas de encobrimento incluem:

Defensor

- Criptografia para proteger dados de acesso não autorizado exigindo uma chave para ter acesso aos dados, seja em repouso em uma unidade ou em movimento em uma rede.
- Implementar "segurança pela obscuridade" com o uso de convenções de nomenclatura não previsíveis para nomes de host e nomes de contas de usuários.
- Usar a conversão de endereço de rede (NAT) para dificultar a identificação de hosts dentro de uma rede a partir da Internet.
- Limitar a quantia de dados que estão publicamente disponíveis em sites corporativos e de rede social que podem ser usados para exploração por esforços de Inteligência de Software Livre (OSI).

Invasor

- Comprometer e usar contas de usuários legítimas para misturar atividades legítimas e maliciosas.
- Canalizar o tráfego malicioso por túneis criptografados, frequentemente até portas de destino comuns, como a porta 80, para dar-lhe uma aparência de tráfego legítimo.
- Exfiltrar dados usando arquivos compactados transferidos por upload para sites públicos de compartilhamento de arquivos na Internet.
- Acessar a rede de destino a partir de diversos endereços IP de origem para ocultar a origem real do ataque.
- Usar contas do administrador local para ocultar a observação de uso da conta no nível da rede.
- Desativar o software antivírus durante ataques e atividades maliciosas.

Recomendações

Realize sua própria coleta de dados de OSI. Procure dados relacionados à sua organização em redes sociais e em outros sites. Os itens que devem ser procurados incluem: postagens de funcionários em fóruns técnicos que fornecem informações sobre a estrutura e a configuração da rede interna; informações em sites em que dados relacionados a vulnerabilidades, informações de inteligência e senhas e contas comprometidas são postados; e postagens de funcionários sobre atividades da empresa que podem fornecer informações úteis para ataques de phishing.

Desenvolva a capacidade de identificar comunicações não autorizadas. Tente identificar conexões criptografadas com uma porta de destino que normalmente não está associada a comunicações criptografadas, como a porta 80, ou um protocolo SSH destinado a portas normalmente associadas com SSL.

Desenvolva a capacidade de monitorar o uso de contas de administradores locais: Como os invasores preferem ocultar suas atividades para que não sejam observadas por meio do uso de contas de administradores locais, desenvolva métodos para coletar e monitorar tais informações dos hosts. Isso pode ser feito por gerenciamento de informações e eventos de segurança (SIEM), um syslog ou tendo um script para coletar tais informações dos sistemas. Tente identificar padrões de uso da conta do administrador local que não estejam de acordo com a quantidade e a duração normais de uso da conta.

Desenvolva a capacidade de identificar o uso normal da conta que está ocorrendo fora do horário comercial normal. Muitos invasores são de um fuso horário diferente em relação aos sistemas invadidos. A utilização das credenciais de conta roubadas durante o horário "comercial" normal do invasor (devido às mudanças de fuso horário) pode ocorrer fora do horário comercial normal do defensor. Tente estabelecer um padrão de atividade normal e, depois, observe se há desvios significativos em relação a ele.

O Obstáculos

Com frequência, defensores e invasores de rede colocam **obstáculos** no caminho do outro para impedir ou obstruir a capacidade de defensor ou atacar a rede com sucesso. Alguns desses obstáculos incluem:

Defensor

- Senhas complicadas ou autenticação de dois fatores.
- Listas de Controle de Acesso à Rede.
- Criptografia de dados em repouso e de dados em movimento.
- Treinamento de reconhecimento do usuário.
- Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS).
- Antivírus e outros scanners de malware.
- Sistemas de integridade e monitoramento de arquivos.

Invasor

- Exclusão de arquivos de log.
- Rotinas de limpeza dentro dos seus ataques – arquivos em lote que limpam chaves de registro, excluem arquivos buscados previamente, excluem e substituem malwares e arquivos de exfiltração para atrapalhar os esforços de determinar os recursos de malware e o conteúdo de dados extrafiltrados.
- Roubo e uso de credenciais de rede legítimas para misturar as atividades do invasor com atividades legítimas e atrapalhar os esforços de detecção e investigação.
- Uso de contas de administradores locais para realizar atividades que provavelmente não serão visíveis no nível da rede.
- Desativar o software antivírus durante a execução do ataque e durante a instalação do malware.
- Exclusão de sistemas de arquivos por inteiro.

Recomendações

Implemente obstáculos defensivos. A cobertura de obstáculos defensivos deve se sobrepor, criando várias camadas de obstáculos que o invasor terá de superar antes de obter acesso. Os invasores contam com a falha dos obstáculos defensivos para lhes fornecer acesso – frequentemente, um usuário executa o malware anexado ao email em um sistema em que as senhas estão armazenadas com um hash fraco, permitindo a determinação fácil de senhas. Isso fornece acesso a uma rede sem segmentação interna ou listas de controle de acesso e a dados sensíveis que não estão criptografados.

Antecipe e prepare-se para obstáculos de invasores. Dentro da sua equipe de resposta a incidentes de segurança de computador (CSIRT), pratique com situações de jogos de guerra em que se pergunta: "O que faríamos se o invasor...?". Priorize não apenas o "o que", mas também o "como" da resposta. Se sua ação for "obter esses logs" – você sabe quem deve chamar para obtê-los, quem deve chamar se estes estiverem de férias e será que essa pessoa tem o acesso e a qualificação necessários para obter o que você precisa? Caso o invasor tenha excluído logs do host local, sua organização tem criação de log em uma localização central? Sua CSIRT tem o acesso e as qualificações necessários para obter esses logs? Se um invasor cometer o ataque por meio do uso extensivo de contas de administradores locais, existe uma maneira de identificar um pico no número de contas de administradores locais dentro de partes da rede? Sua CSIRT tem visibilidade quando uma conta do usuário desativa o software AV? Em caso afirmativo, que acompanhamento é realizado para determinar se houve uma atividade legítima ou se foi uma ação de um invasor? São exemplos de alguns problemas que precisam ser reconhecidos e tratados durante um ataque.

K Terreno Principal

Terreno principal refere-se a áreas dentro da rede que contêm alvos de perfil alto, valor alto ou pagamento alto. O terreno principal pode incluir servidores, contas e indivíduos. Um exemplo de alvo de perfil alto seria um servidor da web direcionado ao público para um hacktivista que deseja envergonhar a organização ou usá-lo como uma plataforma para fazer uma declaração pública. Os alvos de valor alto podem incluir o comprometimento de contas relacionadas a altos executivos ou sistemas utilizados para folha de pagamento e outras transações bancárias e financeiras. As áreas dentro da rede que podem ser consideradas alvos de pagamento alto incluem redes que contêm bancos de dados de cartão de crédito, informações pessoais úteis para cometer roubo de identidade ou informações médicas úteis para cometer fraude.

Recomendações

Identifique seu terreno principal e certifique-se de que está protegido adequadamente e é bem-monitorado. Desenvolva uma lista de inventário com todos os terrenos principais para a sua organização. Podem ser alvos de valor alto típicos, como um controlador de domínio, mas também podem incluir alvos de pagamento alto, como gerência da organização, folha de pagamento, recursos humanos, departamento jurídico corporativo e localizações de propriedade intelectual confidencial.

Desenvolva um processo de avaliação de danos. Em caso de comprometimento do terreno principal, é necessário identificar o conteúdo que foi exposto ou comprometido, a natureza dos dados, uma avaliação de risco resultante da exposição e uma lista de ações mitigadoras que podem ser realizadas para reduzir o risco. As estratégias de mitigação devem ser designadas a ficar sob a responsabilidade de indivíduos para assegurar que as ações sejam concluídas. Essa avaliação de danos pode assumir a forma dos exemplos fornecidos na tabela a seguir:

Nome do arquivo	Natureza do conteúdo	Conteúdo	Risco	Estratégia de mitigação	Risco residual
Vuln_scan.txt	Segurança de rede	Varreduras de vulnerabilidade de 2010	Médio	Verificar se as vulnerabilidades foram reparadas	Baixo
Payroll.xls	RH	Lista de funcionários e contas bancárias	Alto	Notificar funcionários	Alto
Vacations.doc	RH	Planejamento de férias dos funcionários	Baixo	Nenhuma	Baixo
Passwords.xls	Operações de rede	Lista de senhas para dispositivos de rede	Alto	Alterar senhas dentro de 8 horas; aumentar o monitoramento	Médio

A Vias de Abordagem

Frequentemente chamadas de vetor de ataque, as **vias de abordagem** identificam o mecanismo por meio do qual um ataque pode ser realizado. Entre outras coisas, essas vias de abordagem costumam incluir:

- Email de engenharia social contendo malware ou links para websites maliciosos.
- Ataques de dicionário e de força bruta contra webmail acessível pela Internet ou outros logins remotos.
- Ataques de vulnerabilidade do aplicativo (configurações incorretas, estouros de buffer, etc.).
- Acesso físico à rede, como uma equipe de limpeza usando CDs de boot para descobrir as senhas.
- Sinais wireless corporativos acessíveis a partir de empresas vizinhas ou do estacionamento.
- Pontos de acesso wireless falsos instalados.
- Ataque de negação de serviço distribuído (DDOS).

Recomendações

Implemente soluções técnicas. Apesar de invasores determinados frequentemente atacarem a partir de diferentes vias de abordagem de modo simultâneo ou separado, invasores não relacionados podem atacar a partir de várias vias de abordagem ao mesmo tempo. É possível abordar esses ataques por meio de um treinamento rigoroso de reconhecimento de segurança, senhas complicadas e avaliações de vulnerabilidade. As vias de abordagem podem ser interditadas com soluções técnicas suficientes (correção de atualização, software AV e senhas robustas armazenadas usando métodos seguros).

Implemente soluções de usuários individuais. As soluções técnicas podem ser contornadas pelo usuário que executar o malware anexado ao email, fornecendo acesso remoto ao invasor. Isso pode ser abordado com a implementação de um bom programa de treinamento de reconhecimento de segurança. O objetivo do reconhecimento pode ser desenvolver uma cultura de "chamada de emergência" (de maneira semelhante a telefonar para o departamento de bombeiros ao ver uma fumaça), na qual os usuários são incentivados a chamar a segurança quando suspeitam de um incidente de segurança. Sua organização também pode rastrear usuários que são "viajantes frequentes" em busca de alertas de AV ou problemas de segurança e optar por adotar medidas contra eles por causa de ações inseguras. Essa ação pode ir da transição para um sistema operacional diferente menos sujeito a malware até – e incluindo – ações disciplinares para a exposição frequente da rede a invasores devido às suas atividades de computação inseguras.

Os defensores da rede devem identificar estratégias defensivas dentro das categorias de OCOKA e antecipar e preparar-se para ações dos invasores em cada uma delas. Todos os aspectos de OCOKA são afetados pelas ações do usuário. Uma recomendação comum entre várias áreas de OCOKA é o treinamento do reconhecimento do usuário para desenvolver e promover uma cultura de reconhecimento de risco e um sistema de gerenciamento, preparando os usuários para reconhecer, reportar e responder apropriadamente às ameaças de segurança. Para um defensor de rede, o OCOKA pode ser uma ferramenta de valor para ajudar a avaliar o terreno da rede. Com base nos resultados de uma avaliação do terreno da rede usando o OCOKA, os administradores de segurança podem obter um reconhecimento situacional mais amplo dos recursos de defesa de suas redes, ajudando-os a se preparar para, defender-se de, responder a e recuperar-se de um ataque.

Utilizando a segurança do perímetro para eliminar o risco de transferências de arquivos

Mais do que nunca, a segurança dos dados está em posição de destaque para o grande público. Nos últimos 18 meses, aconteceram muitas violações de dados de alto nível de muitos setores, incluindo governo, assistência médica e serviços financeiros. Até junho de 2012, foram 214 violações documentadas com mais de 8,5 milhões de registros expostos[19]. Tais violações são muito conhecidas por causa do impacto direto nos consumidores, mas esses dados não conseguem mostrar a situação completa da violação de dados.

Realizado pelo Ponemon Institute e patrocinado pela Symantec, o 2011 Cost of Data Breach Study reporta que o custo de uma violação de segurança de dados nos Estados Unidos foi de US$5,5 milhões, representando uma queda de 24% em relação ao custo de 2010, que era de US$7,2 milhões por violação[20]. As organizações estão cientes da segurança geral, mas e quanto aos seus arquivos? Será que estão seguros?

As empresas precisam lidar com essas perguntas diariamente. Como irei proteger a minha empresa? Qual parte da minha empresa precisa de proteção? Um firewall é suficiente? Varreduras de vírus nas nossas máquinas são suficientes?

Existem muitas perguntas sobre segurança, mas apenas recentemente os CIOs e profissionais de segurança corporativa tomaram conhecimento de Business to Business (B2B) e segurança de transferência de arquivos.

Todo dia, bilhões de arquivos são enviados pela Internet sem pensar na segurança. As pessoas enviam emails com informações confidenciais diariamente. As corporações enviam dados sensíveis por suas redes internas e fora da empresa sem se preocupar com os possíveis problemas que poderiam enfrentar.

19 Identity Theft Resource Center, 2012 Data Breach Stats, 03 de julho de 2012, http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf
20 Ponemon Institute, 2011 Cost of Breach Study United States, março de 2012, patrocinado pela Symantec, http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

Há mais de 40 anos, alguma forma de Protocolo de Transferência de Arquivos (FTP) tem sido um meio padrão para enviar arquivos de uma pessoa à outra ou de uma empresa à outra. Ele foi criado antes do TCP/IP e ainda hoje é usado em sua forma original, praticamente inalterada. O FTP deu às pessoas uma maneira de transferir arquivos de um ponto a outro ou de uma máquina à outra. Porém, 40 anos atrás, não nos preocupávamos tanto com a segurança. É fato que o protocolo não é seguro, porque envia senhas e dados em texto simples pela rede.

Além dos problemas com o protocolo propriamente dito, muitos servidores de arquivo ficam sem proteção e são vulneráveis a ataques. Nos últimos 40 anos, aconteceram muitos progressos no espaço de Transferência de Arquivos com a inclusão do SFTP (FTP usando SSL), FTP/S (FTP sobre SSH), HTTP, HTTPS (HTTP usando SSL) e muitos outros sistemas de mensagens e protocolos de transferência de arquivos – proprietários e abertos. Mesmo com o surgimento desses protocolos mais seguros, existem problemas de segurança.

Até 2015, os analistas preveem que o mercado B2B será de US$2,22 bilhões[21] e a Transferência de Arquivos Gerenciada (MFT) de US$2,48 bilhões[22] em termos de renda anual. As empresas estão se adaptando aos novos tempos, mas o mundo também. Conforme um número cada vez maior de corporações tenta bloquear suas transferências de arquivos, a necessidade de uma forte estratégia de segurança de transferência de arquivos se torna vital. Com milhões de arquivos entrando nas empresas e milhões de arquivos deixando-as anualmente, é importante ter uma estratégia em vigor para certificar-se de que os dados estão seguros.

O crescimento do mercado de MTF vem acompanhado por novos meios de transferir arquivos e dados de forma *ad hoc*. Hoje em dia, um espaço de destaque para a transferência de arquivos *ad hoc* são provedores de storage de arquivos em nuvem, como o Dropbox. Os serviços de nuvem pública são uma maneira de as pessoas compartilharem arquivos por meio do simples upload de um arquivo em uma pasta virtual abrigada em um datacenter maior. Embora a conveniência possa ser o maior motivador desses serviços, a segurança costuma deixar a desejar para os padrões corporativos.

Muitos fornecedores começaram a lidar com o problema ad hoc como se fosse uma tarefa, fornecendo soluções ad hoc corporativas com uma segurança equivalente à de soluções de transferência de arquivos gerenciada mais tradicionais. Estão surgindo novos produtos que se integram com outros aplicativos de segurança corporativa e transferência de arquivos gerenciada para fornecer uma segurança de perímetro bem-definida.

Protegendo o seu perímetro

Apesar de não ser um conceito novo, a segurança do perímetro ainda não foi amplamente implementada. Os resultados da pesquisa de opinião Best Practices in Data Protection do Ponemon Institute mostraram que 55% dos 718 profissionais de TI e de segurança responderam que não têm uma estratégia formal para controlar a segurança da transferência de dados[23].

Trata-se de uma estatística impressionante se considerarmos os provavelmente milhares de parceiros comerciais que enviam e recebem emails de uma organização maior. É provável que a maioria dos outros 45% de participantes seja organizações de serviços financeiros que enfrentam requisitos de segurança muito rigorosos, apesar de não serem o único segmento de mercado que lida com informações confidenciais.

O perímetro da sua organização é seguro ao lidar com arquivos e informações confidenciais? Você tem uma estratégia? O que você pode fazer a respeito?

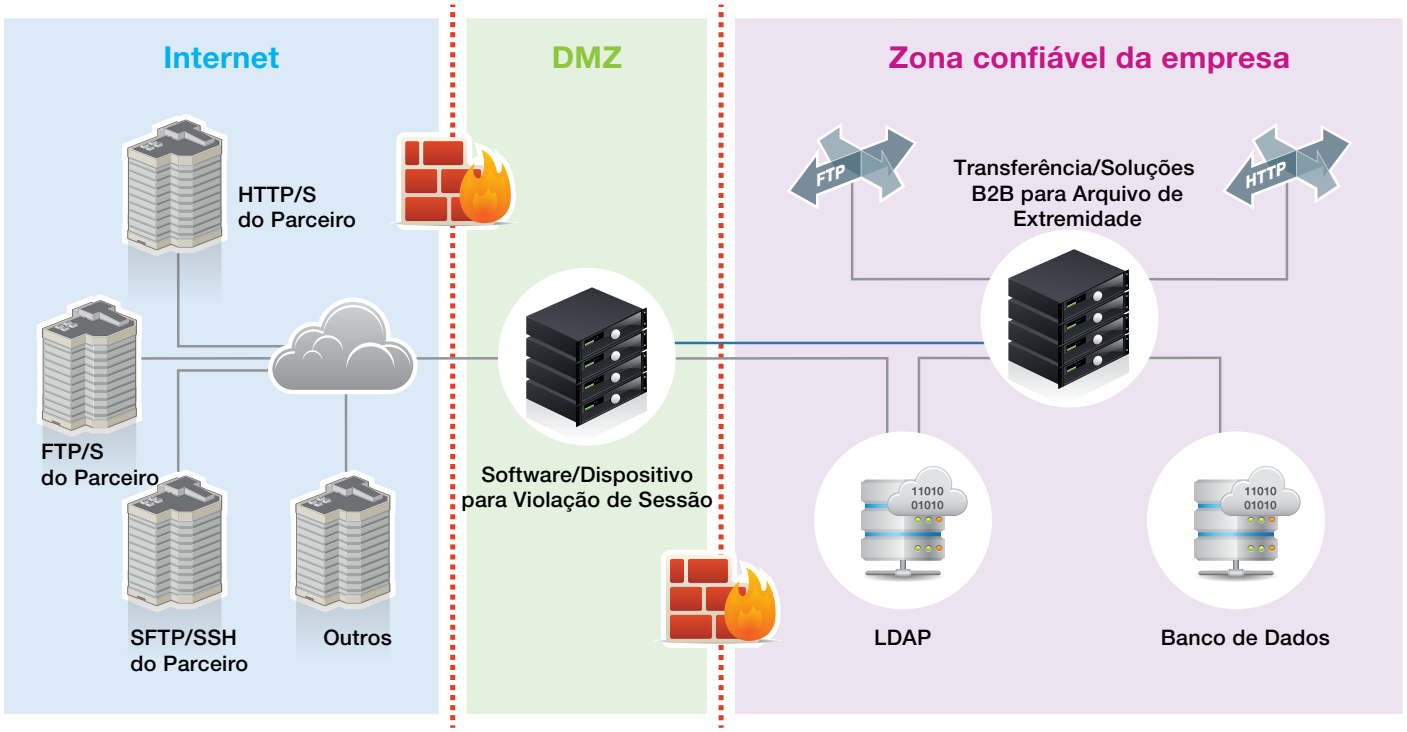
Sua empresa tem uma estratégia relacionada à segurança do perímetro? Em caso negativo, por que não? Quais são as próximas etapas? É necessário responder a essas perguntas para determinar o que deve funcionar para a sua empresa e o seu segmento de mercado. Aquilo que funciona para uma organização pode não funcionar para a sua.

21 IDC, Worldwide Horizontal Business-to-Business Middleware 2011-2015 Forecast, agosto de 2011
22 Ken Vollmer, Forrester Research, Market Overview: Managed File Transfer Solutions, julho de 2011
23 Ponemon Institute, Best Practices in Data Protection: Survey of U.S. IT & IT Security Practitioners, outubro de 2011, patrocinado pela McAfee, http://www.mcafee.com/us/resources/reports/rp-ponemon-data-protection-full.pdf

Seu tráfego é composto principalmente por arquivos grandes ou você recebe quantidades grandes de arquivos menores que devem ser transmitidos em tempo real? Trabalhar com suas equipes de segurança e governança de TI para determinar seus requisitos de transferência de arquivos é o primeiro passo para definir quais recursos são necessários e que tipo de implementação você deve investigar.

Existem muitas definições diferentes do tipo de segurança que deve ser implementado ao lidar com transferências de arquivos, mas a maioria dos fornecedores concorda que simplesmente enviar arquivos, independentemente do protocolo, deixou de ser suficiente. Há opiniões diferentes sobre as melhores práticas de segurança do perímetro e Zona Desmilitarizada (DMZ). Alguns fornecedores oferecem violações de sessão IP e autenticação/autorização na zona confiável, enquanto outros oferecem dispositivos fortalecidos com bancos de dados que permitem a varredura de vírus na DMZ. Independentemente do mecanismo de implementação, é vital ter proxies baseados em DMZ para reduzir o número de portas abertas até a zona confiável da empresa.

Exemplo de implementação de melhor prática



Melhores práticas

Não existe uma solução perfeita para cada empresa, mas há muitos recursos que devem ser examinados ao pesquisar soluções de proxy baseadas em DMZ. Algumas soluções são otimizadas em busca de transferências de alta velocidade e baixa latência, enquanto outras são otimizadas visando a transferências de arquivos grandes. Independentemente dos seus requisitos de transferência de arquivos e casos de uso, considere estas melhores práticas:

Proteção de dados

- Use protocolos de Secure Sockets Layer (SSL) e de Segurança da Camada de Transporte (TLS).
- Não armazene dados na Zona Desmilitarizada (DMZ).
- Entenda as diretrizes e requisitos legais e de segmento de mercado referentes à criptografia, além de seguir tais diretrizes e requisitos.
- Use Módulos de Segurança de Hardware (HSMs) para o storage de chave criptográfica.

Segurança do perímetro

- Use um proxy baseado em DMZ para encerrar as sessões IP e SSL na DMZ, o que bloqueia o acesso direto à porta da Internet pública a uma zona confiável.
- Minimize o acesso à porta do firewall de entrada e saída.
- Implemente uma solução de Prevenção de Perda de Dados (DLP).
- Implemente em uma estrutura de DMZ com multicamadas.
- Forneça varredura de vírus in-line ou Protocolo de Adaptação do Conteúdo da Internet (ICAP).

Autenticação

- Autentique na DMZ, mas não na zona confiável.
- Use a autenticação com multifatores.
- Forneça acesso baseado na função.

Cada melhor prática supramencionada é uma peça necessária para fornecer segurança de perímetro completa.

Os fornecedores estão desenvolvendo ativamente novos métodos de implementação, melhorando a amplitude dos seus protocolos suportados e oferecendo aos clientes a capacidade de conectarem-se a parceiros comerciais de forma segura. Eles estão fazendo o possível para criar as melhores soluções para proteger o perímetro. Contudo, os firewalls não são mais suficientes – e uma varredura de vírus na sua máquina evidentemente não é o final para a proteção corporativa.

Nenhuma solução de proxy de perímetro consegue fornecer, sozinha, todos os recursos da lista de melhores práticas fornecida. À medida que o mercado de trabalho continua exigindo mais segurança, os fornecedores estão melhorando suas ofertas, mas ainda existem lacunas. A segurança do arquivo deve ser a maior prioridade, pois é o ponto mais vulnerável em função da natureza das suas conexões com diversos fornecedores e com a Internet pública. Cabe a você determinar os pontos fracos do seu plano de segurança corporativa a fim de definir quais soluções podem proteger melhor a segurança do seu perímetro.

Seção III
Práticas de segurança de desenvolvimento de softwares

Esta seção apresenta processos e técnicas para abordar a segurança durante o desenvolvimento de softwares. Falamos sobre como as empresas podem localizar vulnerabilidades existentes e ajudar a prevenir a introdução de vulnerabilidades novas. Se você utiliza aplicativos em rede ou da web para coletar ou trocar dados sensíveis, sua tarefa como profissional de segurança está mais difícil do que nunca.

Senha do email – as chaves para a sua identidade online pessoal

Qual é a importância da sua senha do email?

Para todos que usam a web hoje em dia, o endereço de email é uma parte crucial da identidade online. Isso significa que sua caixa de entrada é muito mais do que um baú do tesouro cheio de emails, fotos e informações pessoais que você não deseja compartilhar com o mundo. É um gateway para a sua identidade online. Ao inscrever-se em um website, seu endereço de email se torna um dado crítico, assim como sua senha. Se uma pessoa maliciosa conseguir as duas informações, pode causar problemas para um usuário sem suspeita. Hoje em dia, a grande maioria dos usuários da web simplesmente não percebe o perigo e deixa de adotar medidas básicas para se proteger. Além disso, o webmail e outros portais online usam técnicas antigas para permitir a recuperação de senha – os invasores as utilizaram recentemente e de modo contínuo.

Novamente dentro da brecha

Como a sua senha chega à Internet, ficando à vista de todos? É um resultado direto de todas as violações de segurança das quais ouvimos falar diariamente. Tornou-se um hábito, entre os invasores, roubar o máximo de nomes de usuário e senhas de um website que conseguirem e os postarem publicamente. Apenas nos últimos seis meses, milhões de endereços de email e senhas chegaram a sites públicos.

Após o vazamento, até mesmo senhas que foram criptografadas com uma função hash podem frequentemente ser convertidas em texto simples – seja por métodos de força bruta baseados em dicionário ou consultas a tabelas preexistentes de senhas comuns e valores do hash.

Por que isso é importante?

Dados de violações recentes mostraram que um alto número de usuários da Internet reutiliza senhas em diversos websites. Portanto, quando um website aleatório é comprometido, os invasores costumam vazar uma lista com todos os endereços de email e senhas que conseguem encontrar. Isso já é ruim quando o endereço de email termina com gmail.com, yahoo.com ou hotmail.com. O que acontece quando o endereço de email em questão pertence a um domínio .gov ou à sua própria empresa? Você se sente confortável sabendo que, em caso de vazamento do email e senha de um usuário final, é realmente possível que se trate da mesma senha usada para os seus recursos corporativos?

Provavelmente, você também reutiliza senhas para tipos diferentes de recursos corporativos e pessoais. Ter senhas múltiplas é aconselhável, mas ainda pode causar problemas se a senha não for complexa o suficiente ou se estiver armazenada em formato não criptografado.

O que vem depois?

Depois de serem postados publicamente, seu endereço de email e senha ficam abertos para que qualquer indivíduo comece a tentar efetuar login na sua conta de email usando a senha listada. Muitos dos sites mais populares não se esforçam para prevenir esses ataques de força bruta. Quando alguém encontra uma senha que funcione, o que pode acontecer depois depende daquilo que está vinculado à conta em questão. Pode ser algo simples, como ler todos os seus emails privados e ver suas fotos ou utilizar sua conta para enviar spams a terceiros. Mas também pode custar caro: podem conseguir ter controle dos seus serviços bancários online, contas de lojas ou cartões de crédito. Podem descobrir onde você mora, qual é o seu banco e o que compra online. Há informações suficientes para alguém cometer fraude de identidade.

Esqueceu sua senha? Clique aqui para redefini-la

A maioria dos websites baseados no usuário tem algum tipo de mecanismo de recuperação de senha em vigor. Em geral, uma técnica comum é enviar um link por email para que você clique nele e inicie a mudança de senha. Se um invasor já tiver acesso à sua conta de email, será um risco de segurança enorme. Pense em todos os serviços associados àquele endereço de email: e-commerce, serviços financeiros e redes sociais. A lista é longa. Qualquer um desses sites lhe enviaria um email com um link para alterar sua senha. Alguns sites criaram etapas adicionais para dificultar a mudança de senha, mas a maioria pede apenas para clicar em um link. Tendo acesso à sua conta, uma pessoa maliciosa pode fazer com que você perca dinheiro de verdade. Muita gente já armazenou os dados do cartão de crédito em um site de e-commerce, por exemplo, para simplificar a compra de itens. Com alguns serviços online, um invasor poderia configurar um banco adicional para o qual transferir fundos. É verdade que o serviço pode lhe enviar um email avisando que alguém adicionou uma conta nova – mas de que serve isso se sua conta já foi comprometida e alguém pode simplesmente excluir esse email?

"Não use a mesma senha em sites diferentes"

Todos nós já ouvimos este conselho antes: nunca reutilizar nossas senhas. Algumas pessoas sugerem ter uma senha diferente para cada site, usando uma ferramenta de gerenciamento de senhas. Outros dizem que o ideal é usar uma senha para sites seguros, como serviços bancários online, e uma senha diferente para sites menos seguros. São sugestões excelentes, mas dificilmente seguidas. Embora a fraude financeira seja extremamente inconveniente para o usuário final, não se esqueça de que muitas pessoas reutilizam senhas pessoais para sistemas corporativos. Pense na escala da perda, pois seus negócios poderiam ser afetados pelo roubo de propriedade intelectual devido, simplesmente, à reutilização de credencial. Nessa situação, evidentemente, a IBM X-Force recomendaria uma abordagem de segurança em camadas para mitigar e/ou minimizar possíveis danos.

Regras e regulamentos versus o mundo real

Não importa se as políticas de segurança corporativa são rigorosas com relação às senhas: com frequência, a maioria dos usuários faz o mínimo exigido para a conformidade. É comum pessoas mudarem sua senha para não terminarem com um 1 (e sim com um 2 ou um 3) quando são forçadas a fazer uma alteração. Está na natureza humana: se não entendermos o motivo por trás de algo, é menos provável que o façamos. Use o tempo necessário para mostrar aos usuários como é fácil para um invasor mexer com suas finanças pessoais; assim, eles podem se mostrar mais cuidadosos em relação às suas senhas. O resultado final pode ser usuários que levam sua segurança um pouco mais a sério no futuro, o que é bom para todos.

O que é uma senha segura?

Pergunte a uma dúzia de profissionais de segurança o que constitui uma senha forte e eles lhe darão uma dúzia de respostas diferentes. A tendência crescente (que apoiamos) é usar senhas muito longas, normalmente chamadas de passphrases. Uma passphrase é simplesmente uma combinação de palavras ou uma frase inteira. Basicamente, quanto maior a senha, mais difícil descobri-la. Em termos estatísticos, uma senha de 10 caracteres – independentemente de quantos caracteres especiais estão inclusos – não é tão segura quanto uma senha de 30 caracteres composta por palavras aleatórias. O uso de uma passphrase também é muito mais fácil de lembrar-se do que uma mistura complicada de letras, números e caracteres especiais. Não é muito mais fácil lembrar-se de

"AgoraMinhaSenhaESuperSegura" em comparação com "4K4$!lvabQ!"? Uma senha longa da qual você certamente se lembrará costuma ser melhor do que qualquer senha mais curta. Se você precisar anotar suas senhas em uma nota adesiva para conseguir se lembrar delas, chegou a hora de alterar sua abordagem com relação às senhas. Crie uma variação do título da música favorita da sua infância, combine algumas palavras aleatórias que façam sentido para você ou apenas invente uma frase aleatória. Use alguns minutos para incluir alguns caracteres aleatórios (coloque alguns símbolos na mistura), utilize algumas letras maiúsculas, insira um ou outro número e você terá uma senha bastante segura e fácil de lembrar.

Um exemplo

Um exemplo desse processo vem da letra de música "One Eyed One Horned Flying Purple People Eater". É uma frase bastante longa, mas fácil de lembrar. É possível abreviar, se quiser, substituindo "one" por "1", o que resultará em "1eyed1hornedflyingpurplepeopleeater". Você pode substituir "purplepeopleeater" por "PPE" e chegará a "1eyed1hornedflyingPPE". Para criar uma visão realmente assustadora, é possível acrescentar um "!" no final, intensificando o efeito (e a segurança). O resultado final – "1eyed1horendflyingPPE!" – tem 22 caracteres e mistura letras maiúsculas e minúsculas, números e símbolos.

Lembrando as suas senhas

Se realmente desejar usar uma senha diferente para cada conta online (como deveria), você precisa de uma maneira de rastrear todas elas – e não me refiro a anotar tudo em um pedaço de papel. Uma ferramenta de gerenciamento de senha pode ser muito útil. Existem muitas disponíveis. Algumas delas podem manter suas senhas criptografadas em um arquivo local que somente sua senha principal é capaz de desbloquear. Outros serviços levam isso para a nuvem, onde plug-ins do navegador podem ajudar a simplificar a tarefa. Independentemente do método usado, certifique-se de que a ferramenta suporta uma forma forte de criptografia (como AES-256) e que sua senha principal realmente seja uma "passphrase" longa. Utilize as etapas acima para criar essa passphrase segura e você terá um método seguro para gerar senhas aleatórias para todo website em que efetuar login.

Perguntas de segurança

Há outro risco de segurança relacionado ao seu email: as perguntas de segurança. Com o objetivo de aumentar a segurança, muitos websites acabaram enfraquecendo-a com perguntas de segurança – muitas vezes, um campo obrigatório. Muitas dessas perguntas têm uma resposta que qualquer invasor poderia descobrir depois de cinco minutos de pesquisa. O mascote da sua escola, sua cidade natal e sua data de nascimento são perguntas de "segurança" ruins. Se quiser proteger suas coisas, o ideal é respondê-las com dados falsos. Conte com uma senha segura e um gerenciador de senhas para rastrear todas as suas senhas, mas não com perguntas de segurança falsas.

Autenticação de dois fatores

Embora as etapas acima contribuam muito para manter seu email em segurança, se desejar segurança adicional, encontre um provedor de email que ofereça alguma forma de autenticação de dois fatores. Alguns serviços oferecem um aplicativo de smartphone que gera um código de seis dígitos que é obrigatório para finalizar o processo de login. Outras ofertas podem enviar um código por SMS ao seu telefone. De qualquer modo, o resultado final é uma segunda informação que existe, somente no seu telefone, para acessar seu email. Também oferecem a capacidade de lembrar-se do computador em que você está, para que não seja preciso inserir seu código sempre que efetuar login. Isso significa que o código será solicitado sempre que efetuar login a partir de um novo computador – um computador que nunca havia sido usado para acessar seu email. Tais restrições ajudam a assegurar que acessar seu email a partir de um computador doméstico seja algo seguro e fácil, enquanto acessá-lo de um computador desconhecido –e possivelmente malicioso – exige o código de segurança adicional.

Juntando tudo

Já falamos sobre a importância da sua caixa de entrada, como é fácil para os invasores obterem acesso a ela e os problemas que podem causar depois de acessá-la. Em um mundo ideal, todo mundo usaria uma senha aleatória para cada website em que efetuar login.

Existem muitas ferramentas que podem transformar isso em realidade para quem estiver disposto. Para os demais, dediquem cinco minutos do seu tempo para criar uma passphrase longa. Utilize essa passphrase exclusivamente para o seu email. Ou, se optar por usar um gerenciador de senhas, utilize essa senha como senha principal e, em seguida, use o gerenciador de senhas para gear uma senha longa e complexa apenas para o seu email. Se quiser segurança adicional, procure um provedor de email que suporte a autenticação de dois fatores. Acostume-se com a ideia de não saber qual é a senha do seu email: utilize um gerenciador de senhas para rastreá-la.

Hashing de senha segura – quando o mais rápido nem sempre é o melhor

Quando o mais lento é o melhor

Com o ritmo intenso do ciclo tecnológico, somos levados a acreditar que o mais rápido sempre é o melhor. Em muitos casos, isso é verdade. Todavia, existe um caso de uso computacional em que ser lento é, além de preferível, mais seguro. Trata-se da forma de verificar e armazenar senhas em bancos de dados.

Continuamos vendo manchetes sobre a violação da empresa X e a postagem pública de milhares (ou milhões) de endereços de email e senhas de usuários. Felizmente, essas senhas vazadas costumam estar em hash, não sendo salvas como texto simples. Desse modo, em vez de vermos um monte de senhas reais, cada uma aparece como uma longa sequência codificada.

Tal abordagem parece muito mais segura do que apenas armazenar senhas em texto simples – certo?

Não exatamente.

Um hash é uma criptografia unidirecional. Se você passar uma sequência de texto como uma senha para a função hash, ela lhe devolverá uma sequência nova, praticamente exclusiva, que é uma representação matematicamente transformada do texto original. Unidirecional significa que não é possível pegar o hash final e retroceder ao texto original.

Os desenvolvedores da web são orientados a utilizarem as melhores práticas de segurança, como fazer o hashing de senhas antes de armazená-las nos bancos de dados e assegurar que os hashes recebam o "salting" adequado. Falaremos mais sobre o salting de senhas ainda neste artigo. Fazer o hashing de senhas em geral acrescenta uma camada de segurança que faz com que até mesmo os proprietários do website não consigam ver facilmente as senhas dos seus usuários em texto simples. Isso é essencial para pessoas que usam a mesma senha em diversos sites, pois significa que alguém que esteja xeretando o banco de dados não pode pegar uma senha e endereço de email e usá-los para obter acesso a outros sites usando a mesma senha.

Vamos considerar um exemplo de uma senha bastante ruim, como 12345.

Se calcularmos o hash usando a função PHP MD5 (uma ferramenta de hashing popular e fácil de usar para armazenar senhas de usuários), receberemos este hash MD5:

```
827ccb0eea8a706c4c34a16891f84e7b
```

Parece bastante complexo e certamente não revela, de forma alguma, o texto original. No entanto, como uma procura simples na web pode comprovar, o texto original da senha é exibido diretamente nos resultados.

Em caso de violação de segurança, se um website estiver usando hashes MD5 e um usuário tiver essa senha, o texto será descoberto em segundos com uma procura simples na web.

É um exemplo simplista. Entretanto, hashes reais de violações públicas recentes mostraram que pessoas ainda utilizam senhas como essa para proteger o acesso a serviços da web.

Pode ajudar se o website ou serviço pedir que os usuários utilizem senhas mais complexas, mas, apesar de ser uma boa prática, ela não será efetiva como uma solução única. Até mesmo textos e hashes complexos podem ser recuperados rapidamente; isso é limitado apenas pela velocidade do hardware usado para adivinhar as senhas em relação ao tempo necessário para executar a função hash.

Considere as opções

O que os desenvolvedores da web podem fazer para ajudar a garantir que os hashes de senha sejam armazenados com mais segurança?

Seguem algumas estratégias possíveis:

- Executar a mesma função hash várias vezes.
- Tornar a senha / texto de origem mais complexo.
- Usar uma função hash mais lenta.

Um hash de um hash

Executar a criptografia diversas vezes é uma maneira de ofuscar a senha original e dificultar a reversão.

Retornando à senha 12345, calculamos o hash MD5 (827ccb0eea8a706c4c34a16891f84e7b) e, depois, executamos a função MD5 novamente para obter o hash dessa sequência, que agora é

`1f32aa4c9a1d2ea010adcf2348166a04.`

Isso parece acrescentar uma nova camada de segurança, mas, novamente, uma procura rápida nos leva direto ao 12345.

Na teoria, poderíamos repetir isso várias vezes, em vez de uma vez adicional, mas, apesar de ser uma estratégia efetiva nas circunstâncias certas, há outros problemas a considerar.

O primeiro tem a ver com o conceito de colisões, que significa que duas sequências de origem diferentes criam o mesmo hash. Embora seja uma possibilidade (teoricamente e comprovado com algumas funções hash), está fora do escopo desta discussão.

Além disso, calcular o hash de uma sequência de hash pode ser mais limitador em termos matemáticos do que calcular o hash de uma senha de texto. Na criptografia, isso é chamado de entropia de senha. Quando falamos sobre entropia de senha, consideramos o comprimento da senha, bem como a variedade de caracteres, números e símbolos que podem ser usados. Portanto, uma estratégia que faz hashing de um hash limita-se a uma entropia fixa, independentemente de quantas iterações estão envolvidas.

Há muitos recursos excelentes online que explicam como calcular a entropia de senha[24]. A ideia central é que, quanto mais bits de entropia houver em determinada sequência de origem, mais tempo será necessário para adivinhar aleatoriamente cada combinação possível.

Um hash MD5 composto por 32 caracteres hexadecimais tem 128 bits de entropia. Mesmo com o poder computacional atual, seria preciso muito tempo para adivinhar cada combinação. Contudo, o hash está sempre fixado em 128 bits, enquanto uma senha ou passphrase de origem pode ter uma entropia superior à do hash. Pressupondo que a velocidade do hardware continuará crescendo, o que reduzirá o tempo necessário para adivinhar cada combinação, a capacidade de aumentar a entropia com o tempo é a melhor solução.

A próxima conclusão lógica é exigir que as senhas sejam muito longas, assegurando uma alta entropia.

24 Password entropy: http://pthree.org/2011/03/07/strong-passwords-need-entropy/

Senhas mais complexas

Muito esforço foi feito para orientar as pessoas sobre como escolher uma senha segura. Leia "Qual é a importância da sua senha do email?" para mais informações Muitas empresas e websites tentam impingir uma forte política de senha. Apesar de ser uma boa prática, especialmente para impedir que se adivinhem senhas comuns, não se trata de uma solução perfeita.

Do lado do software, outra prática de segurança recomendada é incluir um valor salt em uma senha antes de fazer o hashing e armazená-la no banco de dados. Um salt é apenas um elemento adicional, como uma sequência aleatória de texto combinada com a senha antes do envio para a função hash.

Incluir o salt aumenta a entropia da senha (tornando-a mais longa e mais aleatória), além de limitar o uso de bancos de dados de consulta pré-calculados chamados Rainbow Tables. Infelizmente, ocorreram violações no ano passado em que o salting de senhas não foi usado de modo generalizado em registros de usuários.

Uma procura por um hash na web já é um tipo de consulta de Rainbow Table (mais especificamente, índices e links para sites que mantêm Rainbow Tables grandes de palavras e frases comuns). Criar Rainbow Tables é tão fácil quanto executar o algoritmo hash para milhões e milhões de combinações de senhas possíveis e armazenar o resultado para uso posterior. Para senhas de baixa entropia como seis letras minúsculas, é possível criar uma tabela de consulta para cada hash possível em minutos. Assim, recuperar um hash é apenas uma questão de verificar se ele existe na tabela de consulta.

A inclusão de algum texto aleatório (o salt) a cada senha reduz a probabilidade de que haja uma Rainbow Table existente com esse valor.

Usando o exemplo anterior da senha 12345, podemos incluir uma sequência salt aleatória:

```
'12345'
+'GlpQclJDRqYGeHi5PeRbg0oMHFlhNnBa'
```

que resulta em um hash MD5 de

```
09f60edb0aa088d50d0482c7ba745059.
```

Procure esse hash em qualquer consulta de Rainbow Table disponível; ele dificilmente será encontrado.

É improvável que Rainbow Tables pré-calculadas existentes tenham um hash armazenado para essa sequência. No entanto, se um banco de dados for violado e o valor salt estiver armazenado dentro do hash ou como uma coluna separada, a capacidade de recuperar a senha com o salt ainda será limitada apenas pela velocidade do hardware com relação à velocidade da função hash.

Em uma recente violação de alto nível realizada este ano, 6,5 milhões de hashes foram postados publicamente. Esses hashes foram gerados com o algoritmo SHA-1, sem qualquer salt adicional. Em poucas semanas, pesquisadores conseguiram recuperar 90% das senhas.

O motivo pelo qual foram capazes de atingir uma taxa de recuperação tão alta baseia-se em vários fatores e mostra como os hardwares de hoje são rápidos ao recuperar senhas.

O primeiro era que as senhas de origem não tinham uma entropia muito alta ou baseavam-se em palavras e frases comuns que podem ser adivinhadas facilmente com um grande conjunto de palavras de origem. Nem mesmo usar uma passphrase mais longa com multipalavras, composta por mais de 20 caracteres, era suficiente se a frase fosse o título de uma canção, uma letra de música, uma citação famosa ou qualquer outra frase "conhecida". Todas essas coisas podem ser acrescentadas ao conjunto de adivinhações e, com tempo suficiente, descobertas.

Os pesquisadores mencionaram[25] que, se a empresa tivesse acrescentado salt às senhas, o processo ficaria consideravelmente mais lento. Isso não é uma solução por conta própria, pois o maior fator contribuinte foi o fato de que a função hash SHA-1 é muito rápida em comparação com outras funções hash. Usando uma ferramenta grátis e um servidor inicial, os pesquisadores conseguiram adivinhar impressionantes 15 bilhões de combinações de SHA-1 por segundo.

Imagine qualquer palavra do dicionário ou senha simples comum – e provavelmente seria recuperada instantaneamente. Mesmo se os pesquisadores se concentrassem em uma senha única com um salt conhecido, ainda poderiam tentar bilhões de combinações em um período curto. Adicionar salt é uma melhor prática, mas, em função da velocidade do hardware atual, não é suficiente.

Vá devagar

Como os hardwares continuam ficando mais rápidos e enormes sistemas computacionais paralelos são baratos e adequados para adivinhar senhas, parece que a melhor solução é desacelerar o algoritmo hash. Se é necessário um segundo para calcular 15 bilhões de hashes SHA-1, uma função diferente deve ter uma magnitude mais lenta.

O SHA-1 não foi criado para fazer o hash de senhas. Idealmente, deve haver funções hash que são capazes de acompanhar o aumento da velocidade e do poder computacionais, ajustando-se de acordo.

Uma técnica tem a ver com o conceito de hash do hash, no qual o número de iterações – dependendo da função – pode escalar para bilhões. Executar a mesma função muitas vezes certamente desaceleraria o tempo necessário para calcular, o que também desaceleraria o tempo necessário para adivinhar as combinações.

SHA512crypt é uma dessas funções hash de senha que pode ser configurada para iterar milhares de vezes ou mais. No caso das pesquisas que recuperaram senhas de SHA-1 a 15 bilhões por segundo, com tipos parecidos de hardware, elas conseguiram adivinhar apenas 11.405 por segundo usando uma função SHA512crypt configurada para 5.000 iterações.

A Password-Based Key Derivation Function 2 (PBKDF2) é outra função criptográfica criada especificamente para direcionar o problema de velocidade da recuperação de senha e também pode ser configurada para executar diversas iterações.

Bcrypt é uma função hash criptográfica criada especificamente para senhas e baseia-se na cifra Blowfish. A Bcrypt usa salts internos para randomizar o hash resultante, dificultando a criação de Rainbow Tables. Ela também fornece suporte à configuração para várias iterações, embora a função propriamente dita seja mais lenta, o que significa que menos iterações são necessárias para desacelerar as coisas em comparação com uma função como SHA512crypt.

Scrypt é outra função dedicada com derivação de chave que pode ser utilizada para hashing de senhas. Uma das vantagens que diferencia o uso da Scrypt é que cada cálculo foi desenvolvido para utilizar uma grande quantia de memória, o que pode intensificar o consumo de recursos para adivinhar senhas paralelas com GPUs ou FPGAs (veja a barra lateral na página 96).

Considerando essas opções de hashing de senhas "lentas" existentes, por que mais desenvolvedores da web não as usam na prática?

25 Recuperação de senha do LinkedIn: http://securitynirvana.blogspot.co.uk/2012/06/final-word-on-linkedin-leak.html

São muitos os motivos possíveis. O primeiro é que funções como MD5 e SHA são bem-documentadas e fáceis de usar em linguagens do lado do servidor, como PHP e Java. Por muitos anos, pareceram ser soluções viáveis para a segurança de senhas e funcionavam de modo fácil e eficiente. Bibliotecas que fornecessem funções hash lentas não eram implementadas de forma tão tranquila nem ficavam disponíveis imediatamente. Hoje em dia, existem muitas ferramentas disponíveis e melhores práticas recomendadas para implementação.

Outro motivo provavelmente está na educação. À medida que o hardware necessário para descobrir bilhões de senhas por segundo se torna comum, um número cada vez maior de desenvolvedores passa a acreditar que algo melhor é necessário.

Aplicativos da web seguros são o primeiro nível de defesa. Em primeiro lugar, não se deve fazer o dump de bancos de dados cheios de hashes de senhas. No entanto, como acontece com qualquer melhor prática de segurança, múltiplas camadas de defesa são sempre recomendadas. Usar um algoritmo hash mais lento – criado para o storage seguro de senhas – é uma maneira extremamente efetiva de ajudar a assegurar a integridade dos dados de clientes.

Mais rápido, mais barato e eficientemente paralelo

Alguns anos atrás, CPUs (unidades centrais de processamento) multicores possibilitaram que se adivinhassem hashes de senhas em lotes cada vez mais rápidos por segundo.

Ao mesmo tempo, as demandas de jogos em 3D resultaram na necessidade de cartões gráficos de processamento dedicados mais rápidos e potentes.

Recentemente, fabricantes de cartões gráficos liberaram APIs de alto nível que permitem que os programadores gravem mais facilmente aplicativos que serão executados em paralelo, diretamente na GPU (unidade de processamento gráfico). São notícias excelentes para aplicativos científicos e médicos, processamento de áudio e vídeo e outros usos matemáticos intensos, que podem utilizar a força dessa plataforma multicore para um bem maior. Entretanto, no caso de algoritmos criptográficos que são apenas tão fortes quanto a velocidade na qual se submetem à força bruta, isso representa um problema.

Enquanto uma CPU de área de trabalho atual pode ter aproximadamente 2-16 núcleos, um cartão de GPU do consumidor pode ter algo entre algumas centenas até alguns milhares de núcleos. Considerando que cada núcleo é capaz de manipular tarefas em paralelo, uma tarefa repetida várias vezes, como executar uma função hash para cada combinação possível de letras e números de uma senha fica muito mais rápida.Acontece que renderizar os quadros de um jogo de tiro na primeira pessoa não é muito diferente da matemática necessária para fazer cálculos criptográficos avançados.

Enquanto a CPU é uma espécie de curinga, responsável por manipular uma variedade de tarefas e cálculos diferentes, a GPU se supera em termos de compactar lotes enormes de números repetidamente em rápida sucessão.

A adivinhação de senhas já chegou "à nuvem". Usando um provedor de serviços de nuvem, é relativamente barato alugar uma matriz de GPUs para compactar uma tarefa por algumas centenas de dólares por hora. Esses tipos de cálculos escalam muito bem em paralelo.

A utilização da GPU para adivinhar hashes de senhas ainda é uma operação de software, sendo limitada, portanto, pela velocidade da execução do software em um disco em um sistema operacional.

Outra ferramenta, no campo emergente dos "sistemas de recuperação de senha", são as Field Programmable Gate Arrays (FPGA), baseadas em hardware. As FPGAs assumem a forma de um dispositivo que contém vários cartões, sendo capaz de executar uma tarefa como calcular um hash de senha a uma velocidade impressionante. No momento, são mais caras do que usar CPUs ou GPUs, mas não fornecem aumentos significativos na velocidade. Segundo um fornecedor de FPGA[26], o dispositivo é capaz de adivinhar 1.756.800 senhas de wireless WPA-PSK por segundo versus 103.800 adivinhações/segundo em uma AMD GPU versus 30.000 /segundo em uma Nvidia GPU versus 4.000/ segundo em uma Intel I7 CPU.

26 http://vr-zone.com/articles/pico-fpga-hardware-beats-gpgpu-in-password-cracking/16705.html#

De HASHES a CINZAS

Não deixe o vazamento de senhas destruir tudo

Como
eles fazem isso ?

Rainbow Tables pré-calculam hashes de senhas e os armazenam eficientemente para consultas futuras. Com o tempo, podem incluir um grande número de combinações de senhas.

Os ataques de dicionário adivinham senhas usando um arquivo muito grande de palavras, frases e citações conhecidas, além de outras regras usadas na criação de senhas, como substituir um 3 pela letra E ou usar a inicial maiúscula.

A força bruta tenta todas as letras, números e símbolos possíveis. Usando hardwares modernos e uma função hash rápida, todas as combinações de uma senha com 6 caracteres podem ser adivinhadas em segundos.

O que
você pode fazer?

Como um usuário

- Não reutilize senhas em diversos sites
- Não use truques comuns estabelecidos para as senhas
- Não use palavras do dicionário ou frases conhecidas
- Use a autenticação de dois fatores, se disponível
- Use um gerenciador de senhas

Como um desenvolvedor da web

- Use uma função hash lenta feita para senhas
- Audite o código em busca de vulnerabilidades de XSS e SQLi
- Use IPS, Firewall de Aplicativo da Web ou algo parecido

Após o vazamento dos hashes, é possível recuperar rapidamente o texto da senha por meio de vários métodos, usando ferramentas disponíveis gratuitamente.

Cartões gráficos em 3D (GPU) podem executar funções hash muito rapidamente em paralelo. Em alguns casos, adivinhando bilhões de senhas por segundo. Hardwares especializados, como serviços de FPGA e nuvem, aumentaram drasticamente as velocidades de descoberta.

MD5 ou SHA-1
BILHÕES DE ADIVINHAÇÕES POR SEGUNDO

SHA512CRYPT
ALGUNS MILHARES DE ADIVINHAÇÕES POR SEGUNDO

BCRYPT ou SCRYPT
ALGUNS MILHARES DE ADIVINHAÇÕES POR SEGUNDO

Diminua a velocidade

Por causa do design, algumas funções hash podem ser calculadas rapidamente. Elas não são indicadas para armazenar senhas, pois os invasores conseguem adivinhar muitas combinações por segundo.

É melhor usar uma função hash lenta, que reduz consideravelmente o número de adivinhações por segundo, tornando o processo de recuperação muito mais difícil.

Após a recuperação de senhas, os invasores usam o endereço de email e as senhas de texto simples vazados para tentar acessar webmail, redes sociais e outros sites comuns.

Usuários que reutilizam senhas normalmente não sabem que uma violação em um site pode dar acesso a muitos outros.

As senhas são vazadas quando um invasor obtém acesso a um banco de dados por SQL injection, XSS ou outra vulnerabilidade.

Com frequência, as senhas são armazenadas como um hash, uma representação criptografada do texto.

Em um estudo recente* descobriu-se que

59%

dos usuários utilizavam a mesma senha para vários sites, incluindo suas contas de webmail.

*http://www.troyhunt.com/2012/07/what-do-sony-and-yahoo-have-in-common.html

Seção IV
Tendências emergentes de segurança

Esta seção examina tecnologias que se desenvolvem rapidamente e desafiam as empresas que tentam determinar o momento de fazer investimentos nessas áreas futuras. Explicamos onde ameaças e explorações estão sendo usadas nas primeiras adoções de tecnologias e como as empresas podem continuar priorizando sua proteção.

Influências do "Traga Seu Próprio Dispositivo" (BYOD) em grande parte das empresas

A capacitação remota na maioria das empresas ainda é um desafio à segurança. Uma transformação revolucionária é a legitimação dos programas "Traga Seu Próprio Dispositivo" (BYOD). Muitas empresas não reconheciam nem suportavam dispositivos de computação pessoal de propriedade pessoal antes; por isso, a implementação de um programa BYOD para dispositivos móveis (como smartphones e tablets) é realmente uma transformação considerável que deve incluir a elaboração de políticas e governança para dar suporte ao seu uso. Trata-se de um acréscimo aos controles de segurança obrigatórios e tecnologias correspondentes.

A importância de políticas de BYOD apropriadas – elaboradas de uma maneira multidisciplinar que inclua a contribuição e a orientação dos recursos humanos e do departamento jurídico, além de, talvez, a contribuição de funcionários – é fundamental. No caso das empresas com programas BYOD existentes que já suportam dispositivos de computação tradicionais, talvez seja indicado revisar a política existente para determinar se mudanças são necessárias na expansão para dispositivos móveis (uma vez que os dispositivos móveis podem resultar em um uso significativamente mais alto de dispositivos de propriedade pessoal em comparação com os dispositivos de computação pessoal de propriedade pessoal).

Estado de segurança

O estado da segurança dos dispositivos móveis está em fluxo. Apesar dos relatórios de malwares remotos, tais como TigerBot/Android.Bmaster em Android e Zeus/ZITMO em diversas plataformas móveis, a maioria dos usuários de smartphones corre riscos por causa de falsificações com SMS, entre outras coisas. Essas falsificações funcionam enviando mensagens SMS automaticamente aos números telefônicos principais de uma variedade de países diferentes a partir dos aplicativos instalados. Existem diversas abordagens de infecção de falsificações sobre esse respeito: 1) um aplicativo que parece legítimo em uma App Store, mas tem apenas uma intenção maliciosa; 2) um aplicativo que é um clone de um aplicativo real, mas com um nome diferente e algum código malicioso; 3) um aplicativo real que foi quebrado por um código malicioso e normalmente é apresentado em uma App Store alternativa. Isso coloca em destaque outro ponto interessante: as App Stores principais têm fortes incentivos de marca e iniciativas de segurança conhecidas para identificar os aplicativos falsos que são enviados, mas isso nem sempre acontece com as App Stores alternativas. Embora a liberdade de escolha seja benéfica para o ecossistema, ela agrega muita complexidade ao paradigma de segurança e, posteriormente, se torna menos benéfica para empresas e uma seção cruzada significativa de usuários finais que não participam de ambientes de App Stores alternativas por inúmeros motivos. Há um fato que aumenta a complexidade do BYOD e complica a aplicação de melhores práticas ao dispositivo móvel da própria pessoa: vários aplicativos populares exigem permissões extensivas, chegando a um ponto em que até mesmo usuários experientes podem se tornar menos vigilantes e descuidados com relação às permissões para aplicativos novos que podem ser arriscados ou desnecessários.

Por que o SMS? Na realidade, o SMS/texto é importante para gravadores de malwares remotos, seja para uma falsificação direta de SMS ou para algo indireto, como o Zeus. As mensagens de texto podem ser utilizadas para direcionar o comando e controle de um botnet (até o momento, na plataforma móvel, de forma centralizada); são usadas por alguns bancos no mundo todo para autenticação de dois fatores em transferências bancárias/eletrônicas; podem ser enviadas aos números principais no mundo todo, onde pessoas mal-intencionadas (e organizações desonestas) podem tirar dinheiro diretamente da sua companhia telefônica[27]. Como a operadora móvel manipula o faturamento automaticamente, é um caso único no mundo do endpoint, pois vincula diretamente um dispositivo a algum nível automático de risco financeiro ou acesso – dependendo do ponto de vista. Além disso, as mensagens de texto estão tão onipresentes na sociedade que até mesmo mensagens sem supressão de e para o malware podem passar despercebidas.

A questão da autenticação de dois fatores por texto de SMS é interessante, uma vez que expõe algo que, no início, parecia ser uma abordagem excelente à segurança. Porém, embora certamente tenha reduzido o risco para organizações financeiras, o número de sistemas operacionais de dispositivo móvel que o dispositivo móvel Zeus (ZITMO) suporta indica que, com o passar do tempo, ele pode se tornar cada vez mais ineficaz, sem acrescentar complexidade alguma à transação.

Bombas de código? Existem muitos programadores de aplicativos remotos para contratar e empresas de desenvolvimento terceirizadas. Embora seja fácil testar a qualidade geral do aplicativo no momento da entrega, poucos fazem a auditoria do código que apresentação em uma App Store em busca de códigos ilícitos. Ainda não vimos uma marca de grande porte ser afetada por um desenvolvimento de software com código de Troia, mas são poucas as coisas que impedem que isso aconteça em algum momento. Organizações que terceirizam o desenvolvimento de aplicativos remotos precisam tomar muito cuidado caso seus aplicativos manipulem dados pessoais ou financeiros sensíveis.

27 http://www.guardian.co.uk/technology/2012/may/25/android-users-angry-birds-malware

Com relação aos ataques direcionados, apesar das muitas histórias que a IBM X-Force ouviu de fontes respeitadas, acreditamos que o custo de fornecer explorações direcionadas aos usuários remotos é muito alto, colocando em risco somente possíveis vítimas que comprovadamente têm dados úteis em formato consumível. Em outras palavras, ataques direcionados a dispositivos móveis provavelmente existirão em todos os principais sistemas operacionais de dispositivo móvel, mas a probabilidade de alguém ser visado é, no geral, extremamente baixa.

Para reiterar, a IBM X-Force acredita que o cenário de ameaças à segurança dos dispositivos móveis está em fluxo. Os modelos de segurança de software de plataformas móveis distintas, como Android e iOS, são diferentes do endpoint típico e têm algumas diferenças entre si que serão exploradas em outro momento. Embora existam alguns ataques exóticos de certa escala, os principais riscos de segurança de dispositivo móvel estão relacionados a aplicativos falsos ou simulados que podem custar dinheiro para o usuário final ou para a empresa por meio de mensagens SMS. À medida que criminosos encontram maneiras de tirar proveito disso, poderemos ver mais bots remotos, como o Android(dot)Bmaster. Agora, falaremos sobre o escopo do tópico BYOD e as melhores práticas conhecidas.

Fazendo o BYOD funcionar

Para que o BYOD funcione, deve haver uma política em vigor completa e clara antes que o dispositivo de propriedade do funcionário seja agregado à infraestrutura da sua empresa. Essa política deve abranger todos os aspectos do relacionamento entre a empresa e o dispositivo do funcionário, além de ter a adesão de todas as partes. Sugerimos que as áreas a seguir sejam cobertas por essa política:

- Identificação e autenticação
- Autorização de acesso
- Proteção de informações
- Integridade dos serviços
- Garantia
- Resposta a incidentes

A maioria das empresas já tem políticas em vigor que abrangem essas áreas para a proteção dos seus equipamentos. Tais políticas devem ser aplicadas a dispositivos de propriedade de funcionários, mas usados em um modelo BYOD. Em quase todos os casos, os controles necessários devem assegurar o mesmo nível de segurança esperado para proteger dados.

Identificação e autenticação

Os requisitos de controle para classificações de dados cuja capacitação em um programa BYOD é considerada devem permanecer alinhados com os requisitos de autenticação existentes. No contexto do dispositivo móvel, isso significa ajudar a assegurar senhas gerenciadas e impingidas apropriadamente, que cumpram os requisitos de complexidade e sintaxe obrigatórios. É necessário estender os bancos de dados de ativos para ajudar a assegurar a identificação do inventário de ativos de propriedade pessoal em uso, além de gerenciar adequadamente o licenciamento de qualquer software fornecido pela empresa como parte do gerenciamento de ciclo de vida do dispositivo. Deve haver uma política de licenciamento de software claramente definida em vigor para ajudar a assegurar que os funcionários usem apenas softwares licenciados adequadamente ao utilizarem seus dispositivos no contexto corporativo.

Autorização de acesso

As empresas que se aproximam do BYOD pela primeira vez provavelmente têm programas de acesso remoto e ao aplicativo existentes. Sugerimos que o uso da infraestrutura, tecnologias e processos existentes seja estendido aos dispositivos de BYOD. Em primeiro lugar, isso ajuda a assegurar que o acesso ocorra dentro dos requisitos de controle existentes. É improvável que os dados associados a esse acesso mudem em termos de classificação e controles correspondentes; portanto, tal abordagem contribui para a consistência. Em segundo lugar, essa abordagem provavelmente tem mais custo reduzido do que a implementação de acesso BYOD ad hoc e específico para o dispositivo, em especial porque é difícil que se limite a gateways de acesso remoto, incluindo, também, controles de acesso ao aplicativo.

A exceção óbvia a essa recomendação são as empresas que optaram por fornecer programas de acesso BYOD completamente exclusivos. Em alguns segmentos de mercado, o acesso totalmente virtualizado por dispositivos BYOD também promove métodos de acesso exclusivos que não devem ser ignorados.

Proteção de informações

A segurança das informações e dados corporativos em dispositivos pertencentes a funcionários é extremamente importante para a empresa. Normalmente, os requisitos de proteção de informações são bem-definidos e estão alinhados com classificações de dados específicas. Devem ser aplicados de modo consistente em um programa BYOD. Uma opção que a empresa pode exigir na sua política de BYOD é a criptografia de dados. Essa opção deve estar alinhada com os requisitos existentes, mas, evidentemente, precisa ser compreendida e definida de acordo com os sistemas operacionais de dispositivo móvel em uso.

Muitos dispositivos usados atualmente oferecem a opção de criptografar todo o storage disponível para o dispositivo e exigir que o usuário insira uma passphrase no tempo de inicialização antes de permitir o acesso.

Em caso de perda ou roubo do dispositivo, o storage criptografado oferece certo nível de proteção. Todavia, com o poder crescente das Unidades de Processamento Gráfico (GPUs), é concebível que a criptografia seja quebrada, havendo tempo suficiente. Uma área que tem preocupado é a disponibilidade futura de processamento de GPU na nuvem – possivelmente, com uma redução de custo significativa e benefícios para os invasores. Uma sugestão para uma boa política é uma "cláusula de limpeza". Em caso de ausência de um dispositivo, isso permite que a empresa envie um comando de limpeza capaz de excluir todos os dados contidos no dispositivo assim que este acessar uma rede.

Integridade do sistema operacional e de aplicativos

Como os servidores e estações de trabalho de propriedade da empresa, os dispositivos que se qualificam para o status de BYOD têm sistemas operacionais e aplicativos. No caso de smartphones e tablets, o nível de maturidade do software é bem inferior ao dos servidores e estações de trabalho tradicionais. Por esse motivo, tais dispositivos se tornam alvos de ataques. Uma boa política de BYOD deve levar isso em consideração e exigir um nível de requisitos de correção igual (ou superior) ao dos dispositivos tradicionais. No momento, pode significar uma identificação clara da versão de firmware adequadamente atualizada e o uso de tecnologias para ajudar a assegurar que somente dispositivos com as versões apropriadas possam acessar informações corporativas. A fragmentação

de dispositivos – mais prolífica dentro da comunidade de dispositivos Android – cria desafios adicionais, como dispositivos mais antigos que não podem receber atualizações de firmware mesmo sendo relativamente novos em relação a uma política de atualização corporativa.

Os dispositivos também precisam executar um aplicativo antivírus que foi aprovado pela empresa. Isso oferece um nível de proteção contra malwares e websites maliciosos.

Smartphones e tablets oferecem menos do que acesso total ao dispositivo e precisam passar por um processo de "rooting" (Android) ou "jail breaking" (Apple iOS) para obter um nível de acesso superior. Quanto mais elevado o nível de acesso de um usuário, maior se torna o risco caso o dispositivo seja atacado. Como as práticas de jail breaking e rooting essencialmente contornam controles de segurança – por exemplo, a criação de ambiente de simulação do aplicativo – dentro do sistema operacional de dispositivo móvel, as empresas devem assegurar que tais dispositivos não sejam usados dentro de programas BYOD.

As empresas também devem restringir os sites em que é possível fazer o download ou comprar aplicativos para sites do fornecedor específicos do dispositivo, Os sites do fornecedor normalmente oferecem algum nível de controle de qualidade sobre software que distribuem.

Garantia

Como acontece em qualquer programa existente de segurança corporativa, a garantia de que os controles necessários foram implementados e são monitorados é um elemento essencial. O mesmo nível de garantia deve ser estendido para incluir todos os dispositivos com acesso às informações corporativas em um programa BYOD. Uma vez que os dispositivos pertencem aos funcionários, é importante que os elementos monitorados sejam claramente explicados e entendidos por eles antes de decidirem incluir seus dispositivos voluntariamente.

Resposta a incidentes

Embora um processo de resposta a incidentes bem-definido possa parecer óbvio, trata-se de uma parte importante e obrigatória de qualquer programa BYOD. Como os dispositivos móveis (em especial, os smartphones) são perdidos e roubados com muito mais frequência do que dispositivos de computação tradicionais, orientar os funcionários sobre como reportar uma perda ou roubo – e também com relação ao processo apropriado para limpar o dispositivo remotamente – pode ser vital. No programa de segurança ideal, isso está integrado ao processo de resposta a incidentes existente a fim de determinar o grau de perda, gerenciar possíveis ações de mitigação e ajudar a assegurar que as informações expostas sejam identificadas.

Definição e revisão do programa BYOD

Uma política de BYOD é um contrato voluntário entre a empresa e o funcionário. Por ser um contrato, precisa passar certos critérios antes de ser apresentado ao funcionário.

Naturalmente, o departamento jurídico da empresa precisa assinar a política. Os recursos humanos talvez tenham de participar, aprovando determinados aspectos dela. A política também precisa seguir as leis locais dos países em caso de implementação mundial (ou ser desenvolvida apropriadamente para seguir os regulamentos locais).

Também sugerimos a educação estendida do usuário. Para que uma política de BYOD funcione bem, os funcionários devem entender, aceitar e seguir todos os seus aspectos. Talvez seja necessário entrar em detalhes, como "por que" certos elementos da política foram colocados em vigor. Um funcionário bem-informado está menos apto a infringir a política. Do mesmo modo, uma política excessivamente restritiva pode resultar em sua infração ou algo pior – a desativação e/ou remoção dos sistemas de segurança e controle de acesso do dispositivo.

Com um planejamento cuidadoso, a empresa e o funcionário podem desfrutar dos benefícios de uma implementação de BYOD bem-sucedida.

Melhores práticas de segurança em dispositivos móveis

Apesar de desejarmos mencionar melhores práticas de segurança bem-estabelecidas para dispositivos móveis (tablets e smartphones), tal formulação e maturidade ainda estão em desenvolvimento. Embora existam algumas diretrizes de segurança publicadas que são específicas dos governos, ainda há práticas variadas em termos de requisitos reais de controle necessários nos programas de dispositivo móvel das empresas.

Como discutido em edições anteriores do Relatório de Riscos e Tendências da IBM X-Force, os programas de controle de segurança dos dispositivos móveis devem ser baseados em requisitos existentes de proteção e controle de dados que correspondam aos dados e informações capacitados nos dispositivos móveis. Embora essa abordagem pareça ser direta e possivelmente simples, na prática, aquilo que vimos funcionando com centenas de clientes varia de forma significativa. Boa parte dessa variação resulta da propriedade dos dispositivos. Isso não existia nos programas de computação de muitas empresas e, consequentemente, vemos que um segmento delas não está necessariamente retrabalhando requisitos de controle existentes, mas sim criando novos para dados corporativos em dispositivos de propriedade pessoal. Considerando a maturidade da tecnologia de controle de segurança para dispositivos móveis, não devemos nos surpreender com essa abordagem fraturada, mas isso pode se tornar um problema tático conforme os sistemas operacionais de dispositivo móvel continuam evoluindo e aumentando os controles possíveis via APIs.

Percebemos uma tendência definitiva rumo ao alinhamento da força das credenciais de acesso com os requisitos de controle existentes. Isso pode ocorrer utilizando-se abordagens baseadas em certificado; o controle do acesso de dispositivo aos dispositivos gerenciados pela empresa por meio de um PIN numérico está diminuindo rapidamente. Muitas empresas também reconhecem a necessidade de prevenção de malware e/ou alguma forma de detecção de comprometimento.

É possível resumir a aceitação de um grau de consistência em controles à medida que avança em direção às melhores práticas. No entanto, muita coisa precisa ser feita antes que as melhores práticas de segurança de dispositivos móveis se igualem às encontradas em outras áreas da computação corporativa.

Estado das tecnologias de segurança de dispositivos móveis

As tecnologias de controle de segurança estão evoluindo em um ritmo rápido. Os fornecedores de plataformas continuam incluindo controles que são acessíveis a todos os fornecedores de produtos por meio de APIs. As empresas recebem controles em maior número e mais profundos a cada revisão; às vezes, não com a rapidez desejada, mas o progresso ocorre de qualquer forma. O acesso a esses recursos incluídos via API é fundamental para sua inclusão nas soluções de gerenciamento de dispositivos móveis (MDM) disponíveis no mercado de trabalho. No espaço de MDM, o mercado de trabalho continua a evoluir, reduzindo o número de participantes conforme muitos dos principais fornecedores de segurança adquirem empresas novas de MDM para incluir em seu portfólio. Muitos acreditam que esse mercado de soluções se tornará uma mercadoria nos próximos anos, o que resultará em uma evolução maior do mercado de trabalho. Esperamos que isso aconteça, como é o caso de qualquer tecnologia emergente que se desenvolve e se torna parte daquilo que seria considerado convencional, passando a receber suporte de todos os fornecedores principais.

Percebemos uma mudança nas tecnologias de dispositivo móvel emergentes à medida que ocorrem alterações nas soluções de MDM. O número de fornecedores que oferecem tecnologias de "separação" ou "isolamento" está crescendo. Essas soluções têm como prioridade permitir que as empresas separem seus aplicativos e os dados associados dos aplicativos existentes e dos dados pertencentes aos funcionários em situações de BYOD. Tal abordagem parece ser um bom equilíbrio de controle nos programas corporativos de dispositivo móvel, nos quais há uma utilização intensa de dispositivos de propriedade pessoal. Também representa alguns meios-termos.

Muitas dessas soluções são desenvolvidas a partir dos principais sistemas operacionais (normalmente iOS e Android), embora existam muitas soluções para apenas uma das plataformas no momento, com roteiros para direcionar a outra. Elas vêm acompanhadas por um conjunto de limitações que podem diminuir seu valor, dependendo das metas corporativas de capacitação de dispositivo móvel. As duas limitações principais comuns nessas soluções são a perda de funcionalidades nativas (porque podem substituir os clientes da plataforma por itens como correio, calendários e contatos) e a ausência da capacidade de aplicar facilmente essa separação a todo e qualquer aplicativo que possa ser executado no dispositivo. A incapacidade de direcionar tal separação fora de um escopo limitado frequentemente exige que as empresas recompilem aplicativos para serem usados dentro da solução de separação. Isso é possível em alguns casos, tendo a empresa desenvolvido seu próprio aplicativo, mas, muitas vezes, o código fonte não está disponível para a empresa, o que transforma essa abordagem em uma limitação.

Conforme surgem soluções de "separação" para dar suporte a iOS e Android, é necessário observar que essa função já faz parte do sistema operacional na liberação atual do Blackberry (como "tecnologia Blackberry Balance"). Sendo uma tecnologia integrada ao sistema operacional, ela direciona as limitações encontradas em soluções de terceiros no iOS e no Android e, novamente, suporta a necessidade de uma tecnologia de separação no nível do sistema operacional, totalmente integrada ao seu funcionamento. Como a Research In Motion conduziu fornecedores de plataformas móveis de modo consistente até a introdução dos controles de segurança necessários para direcionar os requisitos de segurança corporativa, os outros fornecedores podem alcançá-los e começar a incluir tal requisito em seus sistemas operacionais. Devemos considerar, pelo menos, que um investimento em tecnologias de separação é visto como um investimento tático. Estrategicamente, os fornecedores do mercado de trabalho de plataformas móveis podem incluir sistemas operacionais que oferecem esse equilíbrio para que seus dispositivos sejam facilmente adotados por consumidores e empresas.

Até que a inclusão desse recurso de separação ocorra dentro dos sistemas operacionais de dispositivo móvel populares, muito se falará sobre essa abordagem, uma vez que, mesmo com o uso de tais tecnologias, a maioria dos especialistas em segurança ressalta a necessidade de confiar no dispositivo em que os aplicativos são executados – sendo esse um requisito fundamental para confiar na segurança da solução.

Tendências de abordagem pelo segmento de mercado

Embora estabelecer melhores práticas de segurança para a segurança de dispositivos móveis continue sendo um trabalho em andamento, começamos a observar algumas tendências que correspondem aos segmentos de mercado. É preciso ressaltar que ainda estão longe do tipo de tendências e abordagens encontradas em outros segmentos da computação por causa da falta de maturidade das melhores práticas, controles remotos específicos, etc. O uso da tecnologia de separação ou virtualização identificou algumas distinções em certos segmentos de mercado. Com frequência, vemos empresas dos segmentos de assistência médica, financeiro, comércio bancário e do governo optando por utilizarem alguma forma de abordagem de virtualização ou separação. Em alguns casos observados, isso é apoiado por uma tendência a não autorizar a presença de dados sensíveis em dispositivos de propriedade pessoal. Nessas situações, o resultado é o uso de virtualização (para dispositivos de computação tradicionais, como laptops) ou de virtualização de aplicativo (para dispositivos móveis). Embora as abordagens de virtualização possam impedir a presença de dados corporativos, não recomendamos o uso dessa abordagem tecnológica porque ela depende da presença de um host confiável para acomodá-la, o que geralmente significa algum nível de gerenciamento de dispositivo para estabelecer até mesmo um nível de confiança fundamental. Para conseguir um host confiável, as abordagens de virtualização devem ser utilizadas com alguma forma de gerenciamento de dispositivo de modo a assegurar a integridade do dispositivo.

Fora desses segmentos de mercado, temos visto a adoção de soluções de MDM, usando uma abordagem baseada em controles de segurança mais tradicional. Apesar das discussões sobre coisas como a força das senhas dos dispositivos, geralmente não se fala sobre a necessidade de utilizar uma senha (apenas sobre o comprimento, composição e reutilização da senha específica). Na maioria desses casos, o dispositivo inteiro é gerenciado e a participação na maioria dos programas costuma ser voluntária. Embora o BYOD seja frequentemente discutido como uma substituição para os dispositivos fornecidos pela empresa (devido à economia), na prática, poucas empresas migraram para um programa totalmente involuntário e suprido pelo funcionário – por vários motivos. O BYOD é oferecido e suportado, em grande parte, para os funcionários que não se qualificam nem precisam do uso constante da capacitação móvel para realizarem seu trabalho, apesar de poderem se beneficiar do acesso ocasional para aumentar a eficiência e melhorar o equilíbrio entre a vida profissional e a pessoal.

Gerenciamento de vulnerabilidade da plataforma móvel

Apesar de continuarmos vendo mudanças significativas em áreas como tecnologias de controle de segurança, dispositivos e recursos correspondentes, uma constante encontrada no cenário da segurança de dispositivos móveis é o comprometimento de praticamente todos os sistemas operacionais de dispositivo móvel em cada versão liberada. Na verdade, o jail breaking ou rooting de novas versões de liberação frequentemente ocorre dias ou horas depois de serem liberados. Isso é consistente em quase todos os sistemas operacionais de dispositivo móvel. E é especialmente ruim por alguns motivos. Alguns sistemas operacionais de dispositivo móvel foram desenvolvidos com modelos de segurança fortalecidos (por exemplo, criação de ambiente de simulação do aplicativo); portanto, a natureza da facilidade e rapidez com que foram comprometidos afeta a inclusão de itens como a criação de ambiente de simulação. Em segundo lugar, muitas vulnerabilidades de segurança ficam sem correção por semanas e até mesmo meses na maioria dos

sistemas operacionais de dispositivo móvel hoje em dia. Esse segundo item é o problema que mais deve preocupar as empresas estrategicamente, em especial nos casos discutidos anteriormente de fragmentação do dispositivo e seu suporte.

A aplicação rápida de correções para fechar as vulnerabilidades descobertas é uma prática fundamental usada para ajudar a assegurar a integridade de dispositivos de computação corporativos. Trata-se de um requisito básico que sabemos ser essencial para um programa de segurança de qualidade. Na realidade, a falta de boas práticas de correção tem sido um motivo principal para alguns dos problemas de segurança maiores e mais prejudiciais já enfrentados pela Internet. Em problemas mais específicos e menos invasivos, as vulnerabilidades não corrigidas fornecem uma superfície de ataque fundamental em muitas das ameaças avançadas que vemos atualmente. A tendência é que as ameaças avançadas migrem para os sistemas operacionais de dispositivo móvel conforme estes se tornam os dispositivos de computação principais de muitas empresas.

É apenas uma questão de tempo para que a correção de dispositivos móveis se torne um requisito principal. Hoje em dia, para a maioria dos sistemas operacionais de dispositivo móvel, isso não é possível. As empresas não têm a capacidade de corrigir dispositivos e, na prática, as infraestruturas dos sistemas operacionais não estão fazendo um bom trabalho nessa área. Infelizmente, é provável que tal problema deixe a empresa com poucas opções. Portanto, as empresas podem controlar essa preocupação bloqueando os dispositivos que considera arriscados demais em função da presença de vulnerabilidades não corrigidas. Com essa abordagem, quem sai perdendo são os funcionários, pois precisam se contentar com os dispositivos vulneráveis que o fornecedor, OEM ou provedor não está pronto para ou disposto a corrigir.

Muitas plataformas operacionais de dispositivos móveis não têm a noção de uma correção, contando somente com upgrades de firmware que fornecem uma imagem do sistema operacional totalmente nova aos dispositivos. Em alguns ecossistemas, isso se soma à presença de diversas camas de controle de firmware entre o fornecedor da plataforma, OEM de hardware e provedor, normalmente resultando em uma espera de vários meses ou mais para os dispositivos receberem os upgrades de que precisam. O comum é um modelo de obsolescência. Em vez de atualizarem os dispositivos para o nível de firmware atual, os provedores e OEMs tentam vender dispositivos substitutos. Apesar de ser uma solução econômica para o fabricante que promove a fragmentação com relação à arquitetura e implementação, a obsolescência não é desejável de um ponto de vista corporativo. A IBM X-Force acredita que muitas organizações terão essa dor de cabeça conforme o ecossistema de dispositivos móveis evolui.

À medida que os dispositivos móveis se tornam o dispositivo de computação primário para muitos (tanto em empresas quanto na Internet), poderemos constatar que a correção de dispositivos vulneráveis está se tornando a principal preocupação de segurança, pois se trata da área que menos progrediu no último ano, aproximadamente.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produzido nos Estados Unidos da América
Setembro de 2012

Recicle

WGL03014-BRPT-02