# Relatório Semestral de Tendências e Riscos IBM X-Force 2011

*Setembro de 2011*

# Colaboradores

Produzir o Relatório de Tendências e Riscos IBM X-Force é uma dedicação em colaboração em toda a IBM  Gostaríamos de agradecer às seguintes pessoas por sua devotada atenção e dedicação para a publicação desse relatório.

| Colaborador | Cargo |
|---|---|
| Bryan Casey | Market Manager – IBM Security Solutions |
| Carsten Hagemann | X-Force Software Engineer, Content Security |
| David Merrill | STSM, IBM Chief Information Security Office, CISA |
| Dr. Jens Thamm | Database Management Content Security |
| Dr. Ashok Kallarakkal | Sr. Manager – Product Management and Beta Ops |
| Jason Kravitz | Techline Specialist for IBM Security Systems and E-Config |
| John Kuhn | Senior Threat Analyst, MSS |
| John C. Pierce | Threat Intelligence Analyst – AI, MSS |
| Jon Larimer | X-Force Advanced Research, Malware |
| Leslie Horacek | X-Force Threat Response Manager |
| Marc Noske | Database Administration, Content Security |
| Marc van Zadelhoff | Director of Strategy, IBM Security Solutions |
| Mark E. Wallis | Senior Information Developer for IBM Tivoli Security |
| Michelle Alvarez | Team Lead, MSS Intelligence Center (aka Eagle Eyes) |
| Mike Warfield | Senior Wizard, X-Force |
| Ory Segal | Security Products Architect, AppScan Product Manager |
| Patrick Vandenberg | Manager, Rational Security & Compliance Marketing |
| Pete Allor | Senior Cyber Security Strategist |
| Phil Neray | Data Security Strategy, InfoSphere Guardium & Optim |
| Ralf Iffert | Manager X-Force Content Security |
| Randy Stone | Senior Incident Response Analyst |
| Ryan McNulty | IBM Managed Security Services & SQL Querier Extraordinaire |
| Scott Moore | X-Force Software Developer e X-Force Database Team Lead |
| Scott Van Valkenburgh | Market Segment Manager, IBM Security Solutions |
| Tom Cross | Manager – X-Force Strategy and Threat Intelligence |
| Vidhi Desai | Product Marketing – IBM Security solutions |

**Sobre o X-Force**

As equipes de pesquisa e desenvolvimento IBM X-Force estudam e monitoram as mais recentes tendências em ameaças, incluindo vulnerabilidades, ataques ativos e de exploração, vírus e outros malware, spam, phishing, e conteúdo malicioso na web. Além de alertar clientes e o público em geral sobre ameaças emergentes e críticas, o X-Force também fornece conteúdo de segurança para ajudar a proteger os clientes IBM contra tais ameaças.

# Índice
# Seção I

# Índice
# Seção II, III e IV

# Navegando pelo Relatório

Bem-vindo. Este ano fizemos algumas melhorias de uso com relação ao formato e conteúdo do Relatório de Tendências. Essas melhorias foram projetadas para permitir que os leitores usufruam de aplicativos práticos com relação às constatações. Sabemos que a segurança de um computador e de sua rede tratam da conscientização de ameaças, além de ajudar a proteger os sistemas e as redes contra essas ameaças. Mas e depois? Assim como uma organização amadurece em sua posição em relação à segurança dos computadores e ameaças já conhecidas, como começar a desenvolver um foco maior em relação às melhorias?

Nos perguntamos e determinamos que a resposta é fornecer a nossos leitores um maior entendimento sobre o que vivenciamos e aprendemos em relação à amplitude de recursos que é o IBM Security Solutions.

Para este relatório dividimos o conteúdo em quatro seções.

- Ameaças
- Operando a Infraestrutura de Maneira Segura
- Desenvolvendo Software Seguro
- Tendências Emergentes em Segurança

Começaremos falando sobre as **Ameaças** que nossos sistemas e redes estão enfrentando, pois temos que começar a entender o problema com que estamos trabalhando para resolver. Uma vez que a ameaça é compreendida, podemos trabalhar em direção a controles tecnológicos realistas e percepção educacional para ajudarmos a proteger nossa corporação e sistemas. Nas seções **Operando a Infraestrutura de Maneira Segura** e **Desenvolvendo Software Seguro** discutiremos as ameaças e forneceremos conselhos lógicos sobre como ajudar a melhorar ou detectar essas ameaças em seu ambiente. Na seção **Tendências Emergentes em Segurança**, exploraremos e examinaremos as tecnologias emergentes que estão impulsionando discussões de preocupações futuras dos negócios.

O X-Force acredita que esse novo layout organiza melhor o material que desejamos apresentar, e ajuda a focar no que é mais importante para sua organização.

# Seção I
# Ameaças

Nesta seção exploraremos tópicos relacionados às ameaças e descreveremos os ataques às corporações que os especialistas em segurança enfrentam. Abordaremos a atividade maliciosa observada através de um espectro pela IBM e como podemos ajudar a proteger as redes contra essas ameaças. Também iremos atualizá-lo sobre as mais recentes tendências de ataque que a IBM identificou.

## Visão geral executiva

Algumas vezes, para encontrarmos o caminho correto, devemos observar a história recente para que possamos correlacionar, entender e assimilar as lições e tendências que encontramos.

No relatório de tendências lançado no final de 2010, começamos a discutir o que nós da IBM chamamos de Planeta Mais Inteligente.

*"Um mundo que é mais interconectado, inteligente e instrumentado. Por mais que muitas dessas inovações aumentem nossa eficácia e habilidade de nos conectarmos instantaneamente em uma escala global, os riscos e perigos de um mundo conectado também se tornam mais sofisticados e difíceis de serem contidos."*

Mal sabíamos que 2011 iria nos fornecer uma demonstração crítica e em primeira mão de como estamos interconectados, e como isso nos confronta em nosso dia a dia. As corporações e governos estão comprovando quase que diariamente como as decisões que tomamos no mundo virtual podem afetar nosso mundo físico.

Um número sem precedentes de violações de segurança de alto nível reportadas ao longo do primeiro semestre desse ano, demonstraram as falhas em potencial na tecnologia e o impacto que uma violação pode causar nas corporações. Cada nova violação reforça a percepção de que a segurança básica de rede não é apenas um problema técnico, mas um desafio complexo de negócios onde a exposição aos riscos, comunicação, educação ao usuário final e tecnologia devem ser consideradas em uma escala delicada.

Os invasores de redes e corporações também estão se ajustando e evoluindo de grupos razoavelmente indiscriminados que queriam invadir o maior número de redes possível usando ferramentas produzidas em série, para invasores sofisticados e com altos objetivos que estudam os alvos, aguardando pelo tempo exato para entrar nas redes e obter dados de alto valor. O hacktivismo político que relatamos em 2010 continua a evoluir. As ações testemunhadas por violações de segurança no primeiro semestre do ano estão ofuscando as barreiras entre valores políticos e padrões morais para simplesmente atacar as empresas com base em aparente tendência pessoal.

Como grandes operadores botnet foram derrubados e retirados por oficiais de segurança, verificamos uma tendência no declínio de spam e táticas tradicionais de phishing. Discutiremos o contínuo sucesso dos órgãos de direito interessados nessa derrubada de botnets e como essas ações estão mudando a forma com que os criminosos ganham dinheiro. Esses métodos em declínio agora estão forçando operadores maliciosos a considerar escolhas mais lucrativas como alvos específicos de spear phishing?

A jornada remota e de smartphone continua sua integração na corporação com alguns tópicos principais. Primeiro, relatamos que muitas corporações passaram das discussões iniciais sobre decisões básicas de ativação e agora estão lidando com uma nova geração de tópicos relacionados à segurança que discutimos no final do ano passado. A maturidade com que as grande corporações abordam essa jornada de ativação se torna mais importante conforme as políticas remotas baseadas em função são consideradas e implementadas. Segundo que as vulnerabilidades remotas, explorações e malware continuam a crescer rapidamente assim como as taxas de adoção do usuário decolam.

A discussão de segurança evolui para uma análise detalhada em direção ao entendimento de exposição de riscos, mitigação de desastres naturais (tais como no Japão) e como uma violação de segurança de alto nível pode afetar até a mais comum das empresas. Não se trata de questionar "Como eles nos atacariam?", mas sim de como cada empresa deve assumir sua responsabilidade ao declarar: "Estamos preparados para quando isso acontecer conosco?" A presunção de "Poderia acontecer?" se torna uma realidade de "Quando acontecer, como iremos responder?"

Acreditamos que esse relatório semestral ajudará as organizações a se prepararem melhor para as mudanças que enfrentamos.

# Destaques de 2011

## Ameaças

### Malware e a web maliciosa

- Uma explosão de violações de segurança aconteceu no início de 2011, e relatórios quase que diários continuam a marcar esse ano como o "Ano da violação da segurança" **Página 10**
- O SQL Injection continua a ser o vetor de ataque favorito entre os grupos maliciosos, conforme demonstrado pelos inúmeros ataques SQL Injection em massa que ocorreram nos últimos anos. **Página 23**
- As principais assinaturas de alto volume do IBM Managed Security Services (MSS) demonstraram que os métodos favoritos dos invasores são o SQL Injection e a retirada à força de senhas, bancos de dados e compartilhamentos do Windows que continuam a aparecer no topo do sensor de tráfego MSS. As pessoas estão na Internet procurando por serviços abertos e tentando invadi-los. **Página 25**
- O worm SQL Slammer, uma vez no topo do sensor de tráfego MSS, desceu na lista após um "desaparecimento" drástico que ocorreu em março de 2011. **Página 27**

### Conteúdo da web, spam e phishing

- No primeiro semestre de 2011, os proxys anônimos aumentaram progressivamente, mais do que quadruplicaram em número em relação a três anos atrás. Eles representam um tipo crítico de website para rastrear, porque permitem que as pessoas escondam intenções potencialmente maliciosas. **Página 34**
- Em 2011, os volumes de spam continuam a diminuir com a importante derrubada do botnet Rustock. **Página 40**
- Os principais países originários de spam mudaram esse ano. A Índia agora domina o topo da lista ao enviar praticamente 10% de todo o spam registrado atualmente. Atrás da Índia estão a Rússia, o Brasil e a Coreia do Sul, com a Indonésia fechando os cinco primeiros lugares. Os EUA, que estavam no topo da lista em 2010, estão na décima posição com menos de 3% de spam enviado. **Página 48**
- No primeiro semestre de 2011, spammers deram adeus ao tradicional phishing de email. Ao olhar a porcentagem de spam que é considerada como phishing semanalmente, medimos menos de 0,01% por semana. **Página 49**
- O principal país originário de phishing por email em 2011 é os EUA com 41,5%, seguido do Reino Unido com 6,8%. **Página 50**
- No primeiro semestre de 2011, as instituições financeiras continuaram a ser o principal alvo para tentativas de phishing, representando 69% dos segmentos atacados, um aumento desde o relatório do final de 2010, quando esse número era de 50%. **Página 51**
- Em 2011, conforme relatado previamente, a América do Norte permanece como a principal região para phishers por email. No entanto, no segundo trimestre, a Europa cresceu significativamente, alcançando quase 30%. **Página 52**

## Operando uma infraestrutura segura

### Vulnerabilidades e exploração

- No primeiro semestre de 2011, vimos um total inferior de divulgação de vulnerabilidade de segurança do que a vista no ano passado nesta época. O volume de divulgações de vulnerabilidade de segurança aparece a seguir em um ciclo alternado de dois anos. **Página 58**
- O ano de 2010 viu o maior número de divulgações de vulnerabilidade registradas, mais de 8500. Esse ano, aparecem um pouco mais de 7000 divulgações, uma diminuição significativa em relação ao ano passado, mas aproximadamente a mesma quantidade que foi vista em 2006. **Página 58**
- Nos últimos anos, aproximadamente metade das vulnerabilidades de segurança que foram divulgadas, eram vulnerabilidades em aplicativos da web. O número caiu para 37% este ano, com uma diminuição significativa no volume de vulnerabilidades SQL Injection em particular. **Página 59**
- Por enquanto, apenas 12% das vulnerabilidades que foram divulgadas viram lançamentos de exploração, enquanto nos anos anteriores, o número era próximo a 15%. **Página 61**
- As vulnerabilidades de segurança com um nível de 10 em 10 na escala CVSS (Common Vulnerability Scoring System) subiram 3% no ano e já excederam o total de 2010. Quase todas essas vulnerabilidades críticas representam um problema sério de execução de código remoto que afeta um importante produto de software corporativo. **Página 65**
- Duas áreas que tiveram aumentos significativos foram as vulnerabilidades em leitores de documentos e em tocadores de multimídia. Como o mercado de navegadores se tornou mais competitivo, os invasores se concentraram no software que os consumidores estão executando, independentemente do navegador de sua preferência – possibilitando a captura do maior número de vítimas com uma exploração específica. **Página 67**

## Desenvolvendo software seguro

### Vulnerabilidades em aplicativos da web

- O grupo de pesquisa IBM Rational Application Security testou 678 sites (os 500 da Fortune mais 178 sites populares na Internet.) Dos websites testados, 40% (271 sites) continham vulnerabilidades JavaScript no cliente. **Página 75**
- Dos aplicativos vulneráveis, 90% incluíam uma ou mais vulnerabilidades que foram apresentadas através de códigos JavaScript de terceiros, como campanhas de marketing, códigos que incorporam animações em flash e bibliotecas AJAX. **Página 77**
- Cross Site Scripting com base em DOM (3214 problemas de 3683) ainda representa o tipo de problema de segurança mais comum. **Página 78**
- Um novo tipo de vulnerabilidade foi detectado pela primeira vez: Mistificação de Atributo de email com base em DOM. Essa vulnerabilidade ocorre quando um aplicativo da web utiliza código JavaScript para produzir automaticamente um email para o usuário preencher e enviar, utilizando dados controlados pelo mesmo. Em tais cenários, um invasor poderia potencialmente manipular o conteúdo, assunto ou campos CC ou BCC do email, resultando no vazamento de informações privadas. **Página 78**

## Tendências emergentes em segurança

### Móveis

- O primeiro semestre de 2011 viu um aumento no nível de atividade de malware direcionada à mais recente geração de dispositivos inteligentes, e o número crescente de divulgações de vulnerabilidade e lançamentos de exploração destinados às plataformas móveis visto em 2010, continua em 2011, não mostrando nenhum sinal de diminuição. **Página 68**
- Os dispositivos móveis estão rapidamente se tornando a plataforma de malware do momento. Esse aumento de malware possui como base os serviços SMS premium que podem cobrar dos usuários uma taxa crescente por sua adoção e pelas vulnerabilidades sem patches nos dispositivos. **Página 79**
- Dois métodos populares de modelos de distribuição de malware estão a criar versões infectadas dos softwares existentes no mercado e a publicar softwares que pretendem ser crack, patch ou comandos de cheat para outro software. **Página 79**
- Além de enviar mensagens SMS, o malware de Android foi observado coletando dados pessoais do telefone e enviando-os de volta para um servidor central. Estas informações poderiam ser utilizadas em ataques phishing ou para roubo de identidade. Também vimos que o malware de Android pode ser controlado remotamente por um comando remoto e um servidor de controle – assim como um bot que infecta uma máquina com Windows. **Página 80**
- O gerenciamento de segurança corporativa de dispositivos de terminal remoto lutará para lidar com essa expansão massiva. Uma solução pode ser a convergência do gerenciamento de configuração de segurança de terminal para incorporar todos esses novos dispositivos. **Página 81**

### Segurança do banco de dados

- O velho princípio continua sendo verdadeiro – “Por que você rouba bancos? Porque é onde o dinheiro está...” Os dados de uma empresa devem estar continuamente conectados a seus clientes, parceiros e funcionários; porém, isso expõe dados confidenciais a ataques mais automatizados e direcionados do que nunca.” Por exemplo, estamos vendo inúmeros ataques que facilmente dispensam as defesas tradicionais de perímetro com a exploração de vulnerabilidades em aplicativos da web como SQL Injection, ou alavancam credenciais administrativas roubadas, para comprometer os bancos de dados backend. **Página 84**
- Os bancos de dados se tornaram um alvo importante para invasores. Dados críticos utilizados para administrar nossas organizações – incluindo informações financeiras/ERP, de clientes, de funcionários e de propriedade intelectual como novos projetos de produtos – são armazenados em bancos de dados relacionais. **Página 85**

## Colaboração de segurança IBM

IBM Security representa diversas marcas que fornecem um amplo espectro de competência em segurança.

- Enquanto as equipes de pesquisa e desenvolvimento X-Force estão ocupadas no trabalho de análise das mais recentes tendências e métodos utilizados pelos invasores, outros grupos dentro da IBM, trabalham para usar esses dados valiosos no desenvolvimento de técnicas de proteção para nossos clientes.
- A equipe de pesquisa e desenvolvimento IBM X-Force descobre, analisa, monitora e registra uma ampla gama de ameaças de segurança e vulnerabilidades do computador.
- O IBM MSS (Managed Security Services) é responsável por monitorar explorações relacionadas a terminais, servidores (incluindo servidores da web) e infraestrutura geral de rede. O MSS rastreia as explorações trazidas pela web, assim como outros vetores, como email e mensagens instantâneas.
- O IBM PSS (Professional Security Services) oferece uma ampla avaliação de segurança por toda a corporação, serviços de implementação e design para ajudar a desenvolver eficazes soluções de segurança da informação.
- Nossa equipe de segurança de conteúdo percorre e categoriza a Web, independentemente, através de crawling, descobertas independentes, e através dos feeds fornecidos pelo MSS.
- A IBM reuniu dados reais de vulnerabilidade dos testes de segurança realizados nos últimos anos com a equipe IBM Rational Services. Esses dados são uma combinação de resultados de avaliação de segurança de aplicativos obtidos do IBM Rational AppScan com testes e verificações manuais de segurança. A partir desses requisitos, através do design, código e produção, o IBM Rational AppScan fornece amplo gerenciamento contra vulnerabilidade de aplicativos por todo o ciclo de vida do aplicativo.
- O IBM Cloud Security Services permite que os clientes consumam recursos de software de segurança através de um modelo hospedado de assinatura que ajuda a reduzir custos, melhorar a entrega do serviço e aprimorar a segurança.
- As soluções de gerenciamento de identidade e acesso fornecem gerenciamento de identidade, gerenciamento de acesso e auditoria de conformidade de usuário. Essas soluções centralizam e automatizam o gerenciamento de usuários, a autenticação, o acesso, a política de auditoria e o provisionamento de serviços de usuários.
- As soluções de segurança de informações e dados IBM oferecem recursos para proteção de dados e gerenciamento de acesso que podem ser integrados para ajudar a abordar a segurança do ciclo de vida de informações em toda a corporação.
- As soluções de gerenciamento de terminal combinam o gerenciamento de segurança e de terminal em uma única oferta que permite que os clientes visualizem e gerenciem terminais físicos e virtuais – servidores, desktops, laptops em roaming, além de equipamento especializado como dispositivos de ponto de venda, caixas eletrônicos e quiosques de autoatendimento.
- O IBM InfoSphere Guardium fornece uma solução corporativa escalável para segurança e conformidade de banco de dados que pode ser rapidamente implementada e gerenciada com recursos mínimos.

## 2011 – Ano da violação de segurança

O primeiro semestre de 2011 foi marcado por uma série de significativas e amplamente relatadas violações de segurança de redes externas, que são conhecidas não apenas pela frequência, mas pela presumida competência operacional de muitas das vítimas. As perguntas que os executivos em todas os segmentos estão fazendo para suas equipes de segurança são: “O que está acontecendo?” e “Isso pode acontecer conosco?” Para responder a essas perguntas, alguém deve começar conhecendo os diferentes grupos responsáveis por esses ataques, suas motivações e recursos.

## Quem está atacando nossas redes?

Ameaças externas podem ser categorizadas de acordo com o foco dos ataques, assim como o nível de sofisticação operacional. Alguns invasores de redes são razoavelmente indiscriminados; eles desejam invadir o máximo de sistemas possíveis, independentemente de onde estejam. Outros são direcionados; eles possuem o interesse de invadir redes de vítimas específicas. Alguns operadores botnet carecem de habilidades técnicas sofisticadas, e principalmente, de saber como usar uma caixa de ferramentas de exploração e kits de malware que compraram. Outros trabalham em equipes bem organizadas e patrocinadas pelo estado, que descobrem novas vulnerabilidades e desenvolvem técnicas de ataque totalmente sem precedentes.

Por muitos anos, a ameaça mais comum de rede externa tem sido o malware e os desenvolvedores botnet motivados financeiramente – invasores que infectam milhões de computadores com software malicioso que rouba números de cartões de crédito, envia spam e lança ataques de negação de serviços. Esses ataques são amplamente direcionados e tendem a empregar técnicas de ataque conhecidas, produzidas em série. No passado, vimos novas vulnerabilidades dia-zero sendo utilizadas em conjunto com construção de botnet, mas parece que os vendedores dessas explorações no mercado negro estão atualmente sendo superados por compradores com diferentes tipos de aspirações.

Há uma excelente oportunidade de ganhar dinheiro com a atividade de botnet amplamente direcionada que tem atraído um grande número de pessoas do mundo todo. As estatísticas publicadas ao longo dos anos no Relatório de Tendências X-Force mostra os sinais. A atividade de ataque botnet amplamente direcionada é tão comum na Internet que aparece prominentemente nas estatísticas que publicamos. Também publicamos gráficos mostrando explorações maliciosas de kits de ferramentas, comandos de botnet e atividades de controle, e também os efeitos desses botnets, assim como o crescente volume de spam e ataques distribuídos de negação de serviços. Manter toda essa atividade fora da rede corporativa – suprindo-a com patches de vulnerabilidade e detectando ataques no perímetro – pode ser um desafio significativo, e o cenário de ameaças parece estar se tornando apenas mais complicado.

**Tipos e Técnicas de Invasores 1S 2011**


*Figura 1: Tipos e Técnicas de Invasores – 1S 2011*

## Ameaça avançada persistente

Apesar de as organizações governamentais sempre terem se preocupado com a ameaça de intrusos de computador patrocinados pelo estado, é evidente que grandes e pequenas corporações privadas também enfrentam esse tipo de ameaça. Uma série de violações proeminentes relatadas publicamente em 2010 e no início de 2011 parece comprovar essa ideia. Ataques sofisticados, com alvos específicos e patrocinados pelo estado (que algumas vezes são chamados de Ameaça Avançada Persistente) estão do lado oposto do espectro dos operadores botnet motivados financeiramente. Esses ataques geralmente possuem alvos específicos. Eles geralmente mostram evidências de coleta de inteligência pré-operacional extensiva e planejamento criterioso, ponderado e a longo prazo. E envolvem também vulnerabilidades nunca antes vistas e técnicas de ofuscação. A prescrição padrão de manter patches e executar produtos comerciais de segurança, tipicamente, não protege uma rede desse tipo de adversário.

Os Relatórios de Tendência e Risco IBM X-Force anteriores, assim como as publicações no **blog X-Force** investigaram a fundo o tópico de proteção contra invasores sofisticados. A abordagem é uma mudança de paradigma da abordagem usual "auditoria e patch" para segurança de rede, a qual envolve o desenvolvimento de garantias operacionais de que a rede não está vulnerável às técnicas conhecidas de ataque. Invasores sofisticados podem, algumas vezes, empregar técnicas de ataque desconhecidas que você não está preparado para evitar, então o foco deve mudar para detecção e análise.

Sua organização deve estar disposta a adotar abordagens para detecção que podem não ser 100% eficazes. Por exemplo, muitas organizações desistem do investimento pesado na educação de seus usuários finais sobre spear phishing, pois elas sabem que essa educação pode não ser completamente eficaz. No entanto, ela tem sua parcela de efetividade, e quando você está lidando com um invasor sofisticado e furtivo, essas detecções que você obtém de um processo de detecção parcialmente eficaz são detecções que você não obteria de outra forma. **Na próxima seção deste relatório, falaremos mais detalhadamente sobre as diferenças entre Phishing, spear phishing, ameaça avançada persistente e ataques direcionados a rede.**

Assim que houver a detecção de algo, o próximo passo é a análise judicial. A inclinação natural ao descobrir uma violação é removê-la, para que você possa seguir normalmente com os negócios. Ao lidar com um invasor sofisticado, pode ser melhor suprimir essa propensão. Você está executando a contrainteligência. Os ataques que estão sendo lançados contra você são desenvolvidos de maneira personalizada para alcançá-lo, e você precisa aprender sobre eles o máximo possível, mesmo que tenha conseguido detectá-los antes de serem bem-sucedidos. Você pode querer acompanhar seu desenvolvimento para observar o que acontece. Dessa maneira, a análise judicial se torna parte diária de sua abordagem operacional para a segurança.

Em outras palavras, ao lidar com APT (Ameaça Avançada Persistente), a prevenção irá falhar em algum momento – uma análise mais detalhada será necessária, então você deve estar à frente e ter condições de lidar com esses tipos de eventos. Você deve fazer isso com o entendimento de que a informação obtida através dessa análise pode fornecer uma prevenção bem-sucedida contra ataques futuros e ao mesmo tempo criar um ciclo de feedback para melhorias. As informações que você obtém de análises podem levar à detecção de outros comprometimentos dos quais ainda desconhece. É o feedback entre a detecção e a análise que ajuda você a estar à frente de seu adversário.

Para maior compreensão deste tópico, recomendamos que você faça **download dessa discussão sobre APT** do evento IBM Pulse 2011.

## Enfraquecendo práticas comuns de segurança

Muitas das violações mais proeminentes de 2011 foram realizadas por invasores que não se encaixavam em nenhuma das duas categorias anteriores. Grupos hacktivistas, como Lulzsec e Anonymous, não possuem a sofisticação técnica e operacional de invasores patrocinados pelo estado e não possuem a motivação financeira dos operadores botnet, mas foram muito mais bem-sucedidos com violações em redes e causando danos à reputação. Esses grupos se encaixam na categoria de invasores que cometem ataques com alvos específicos utilizando técnicas conhecidas e produzidas em série. É claro que também vimos ataques com motivação financeira que entram nessa categoria, como a série de violações atribuídas a Albert Gonzales.

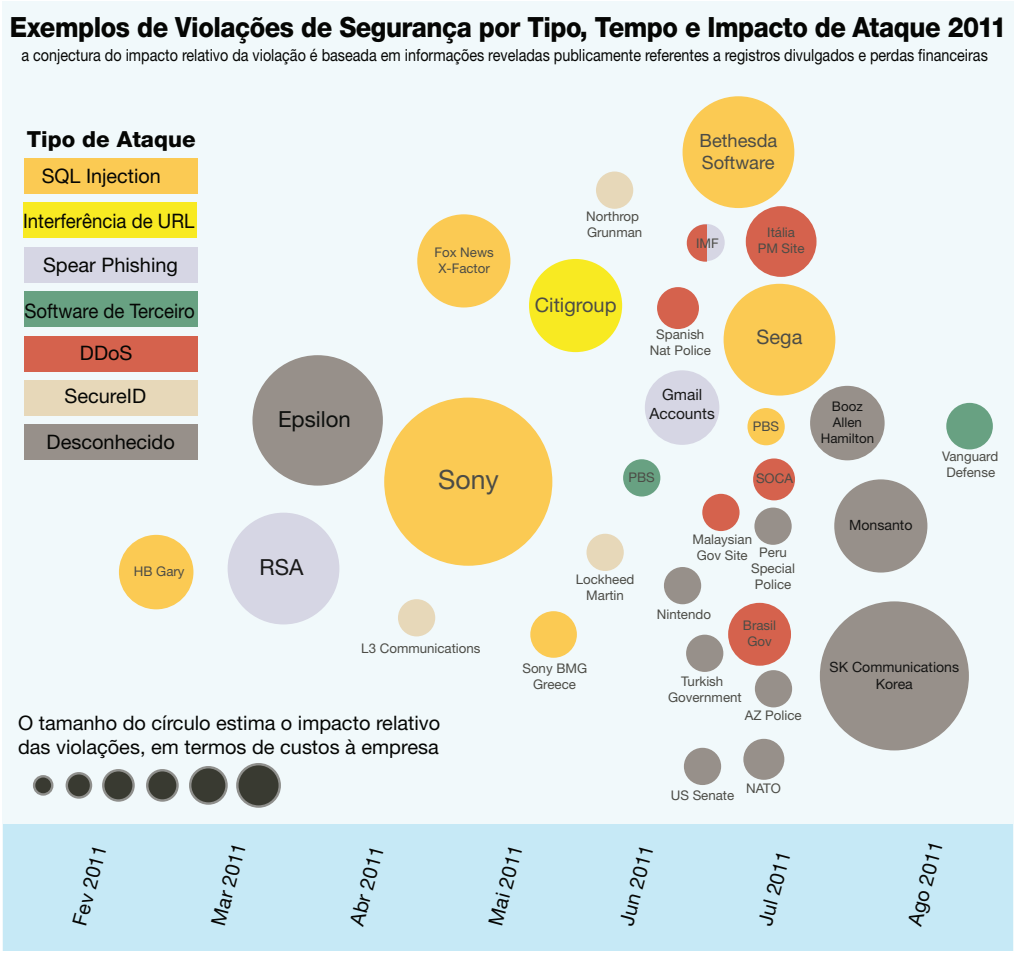



*Figura 2: Modelo de Violações de Dados por Tipo de Ataque, Tempo e Impacto 2011– 1S 2011*

Como ilustrado na Figura 2, muitas das violações de dados publicadas em 2011[1] foram bem-sucedidas apesar do fato de que técnicas bem conhecidas, como SQL Injection, eram muitas vezes um fator. Alguns desses ataques que podem não ter sido bem-sucedidos, tiveram como vítimas, organizações que seguiram melhores práticas de maneira consistente com relação à segurança de computadores.

## Pontos comuns de entrada

Há dois pontos comuns de entrada de TI em cada corporação. O primeiro e mais óbvio é o website público e os servidores de dados. Cada página e script em cada website público, assim como todos os outros serviços interativos da Internet, são uma oportunidade para que um indivíduo motivado encontre uma violação. O segundo ponto de entrada são estações de trabalho ou terminais de funcionários. Cada funcionário com acesso a uma rede corporativa é um alvo em potencial para um invasor.

O desafio de bloquear a presença pública de uma organização na Internet é complexo; grandes websites corporativos podem conter milhares de scripts, escritos por muitos departamentos diferentes. Uma simples página promocional temporária pode conter uma falha que pode levar a uma exploração em grande escala da rede interna de uma empresa.

1 Linha do tempo de Ciberataques (e Cibercustos) de 2011 (Atualizada):
http://paulsparrows.wordpress.com/2011/06/28/2011-cyber-attacks-and-cyber-costs-timeline-updated/
http://blog.thomsonreuters.com/index.php/cyber-attacks-timeline-graphic-of-the-day/
http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

Uma política de segurança eficaz para o que é colocado em um servidor público é um bom começo. Os scripts devem ser auditados com o uso do software de varredura de códigos da web, e cada formulário de entrada deve ser verificado regularmente em busca de Injection comuns e vulnerabilidades Cross Site Scripting.

Scripts e aplicativos de terceiros como software para blogs ou fóruns podem ser especialmente vulneráveis à problemas de segurança, já que aplicativos mais populares são usados por muitas empresas e os invasores podem utilizar uma única exploração em muitos sites diferentes. A maioria dessas violações pode ser varrida automaticamente e os invasores podem se concentrar então, nos servidores vulneráveis. Esses servidores, por outro lado, podem ser utilizados para explorar o negócio final, ou para injetar malware em páginas legítimas para infectar todos os visitantes dos sites.

Em muitos casos, uma pequena falha pode levar a novas oportunidades para que os invasores encontrem caminhos na rede. Por exemplo, em uma violação recente, um arquivo comum incluía vulnerabilidades que foram utilizadas, ao que consta, para acessar o sistema de arquivos em um servidor da web. Os invasores afirmam ter descoberto chaves SSH no servidor, permitindo a autenticação a outros servidores. Isso abriu caminho para a tomada total do controle da rede da empresa[2].

Em diversas violações, senhas fracas ou reutilizadas resultaram em uma exploração em escala ainda maior. Quando um usuário reutiliza a mesma senha em diversos locais, sua Intranet, seu email pessoal, sites de redes sociais, VPN corporativa e website da empresa, torna-se muito mais fácil obter um maior ponto de apoio em uma corporação, que poderia ter sido protegida de outra maneira. Utilização de senha forte é essencial com uma política contra reutilização de senha e execução periódica de validade.

O segundo ponto de entrada comum de TI é o terminal. Ao usar esses ataques de engenharia social com base em email, é possível persuadir as pessoas de uma organização a clicar em links maliciosos, permitindo que backdoors ou outro malware seja instalado no terminal. Isso pode propiciar um ponto adicional de lançamento na infraestrutura. O terminal pode ser o alvo de invasores de todas as classes, desde os invasores motivados financeiramente procurando desenvolver botnets até os sofisticados, patrocinados pelo estado realizando ataques cuidadosamente criados por engenharia social. Claramente, manter os terminais com patches e atualizados é uma tarefa crítica de segurança.

## Não é um problema técnico, mas um desafio de negócios

Nenhuma das recomendações acima deveria surpreender profissionais experientes de segurança da Internet. Testes regulares de invasão externa, testes de vulnerabilidade de aplicativos da web, firewall de aplicativos da web, políticas eficazes de senhas, educação do usuário final, cumprimento da política de rede, criptografia e prevenção contra invasões deveriam ter identificado e acabado com muitas das violações que serviram para violações importantes que ocorreram este ano. Então, por que isso aconteceu?

Porque, esse tipo de segurança básica de rede não é apenas um problema técnico, é um desafio de negócios. Grandes organizações possuem operações complicadas de rede e essas redes estão em constante mudança. Um esforço significativo geralmente é exigido para inventário, identificação e fechamento de todas as vulnerabilidades, e para mantê-las fechadas enquanto a rede cresce e muda. Esses esforços encontram resistência, não apenas financeira, mas também operacional. As empresas querem fazer negócios e não perder tempo colocando todos os pingos nos "i" e cortando todos os "t" na lista de verificação do auditor de segurança. Quanto investimento em tudo isso é suficiente?

A resposta para essa pergunta evolui ao longo do tempo, à medida que as violações proeminentes nos ensinam que ainda não encontramos o nível certo de investimento. Os programas de conformidade criaram um denominador comum útil e mais baixo para programas de segurança, mas a experiência demonstrou que as redes de conformidade, sistemas e infraestruturas ainda podem ter sérias falhas de segurança. O que aconteceria se você combinasse os sofisticados recursos técnicos e operacionais que associamos à Ameaça Avançada Persistente com o amplo foco de operadores botnet financeiramente motivados?

2 LulzSec contra Bethesda & Senate.gov: http://pastebin.com/i5M0LB58

Isso nos traz o cenário de ciberguerra que foi o foco de muitas "quedas de braço" nos círculos de política nos últimos anos. Definimos ciberguerra como invasores sofisticados que utilizam amplos ataques com base em computadores para obter vantagens táticas e estratégicas ao prejudicar a infraestrutura e os recursos de seus inimigos. Felizmente, não vimos muito desse tipo de atividade. Porém, o fato continua; se não conseguimos repelir um ciberexército de hacktivistas utilizando técnicas produzidas em série, não estaremos preparados para lidar com uma ameaça maior.

Evidentemente, há mais trabalho a ser feito em relação à segurança da rede externa. Realizar todo esse trabalho se resume a ter certeza de que você possui um conhecimento atualizado das falhas no perfil de segurança da rede externa. Com esse conhecimento, você pode comunicar de maneira mais eficaz os riscos associados a essas falhas para que os executivos tomem decisões dentro da organização. Você também pode desenvolver um plano para abordar essas falhas e obter os recursos necessários para executar o plano. No final, os eficazes programas de segurança de rede funcionam, pois eles têm o nível certo de suporte político dentro de uma organização. Considerando a abordagem adequada para desenvolvimento, esse suporte deve ser um diálogo contínuo dentro da comunidade de segurança.

## Principais lições aprendidas

Uma lição importante que a IBM aprendeu ao trabalhar com clientes neste problema é que faz sentido priorizar esforços que criam os resultados mais visíveis e demonstráveis com impacto mínimo nos processos de negócios existentes. Você deve desenvolver uma campanha de marketing para os esforços de segurança, enquanto se concentra no alcance de marcos significativos, e na comunicação com o negócio quando cada marco for alcançado, focando-se nos benefícios acumulados. Através de uma demonstração repetitiva de sucesso, você pode aumentar a conscientização e o suporte para seus esforços. Esse suporte é importante quando chega o momento de investimentos mais significativos ou quando alguma mudança problemática em um processo contínuo é necessária.

Nada disso acontece rapidamente e o tempo está passando. Quanto mais falhas existem nas defesas, maior é a probabilidade de comprometimento. É provável que a maioria das organizações que foram violadas nos últimos meses tivessem programas de segurança de rede reais e essenciais em vigor no momento em que foram violadas. E a corrida não terminou para nenhuma delas – ou para nós; a escala e a complexidade das ameaças enfrentadas por nossas redes cresce a cada ano que passa.

# SE O IBM X-FORCE ESTIVESSE ADMINISTRANDO O DEPARTAMENTO DE TI

Muitos leitores perguntaram: se o IBM X-Force estivesse administrando o departamento de TI e tivesse visto o que aconteceu este ano, o que você faria? Aqui estão dez ações além do básico que o X-Force executaria se nós administrássemos o departamento de TI.

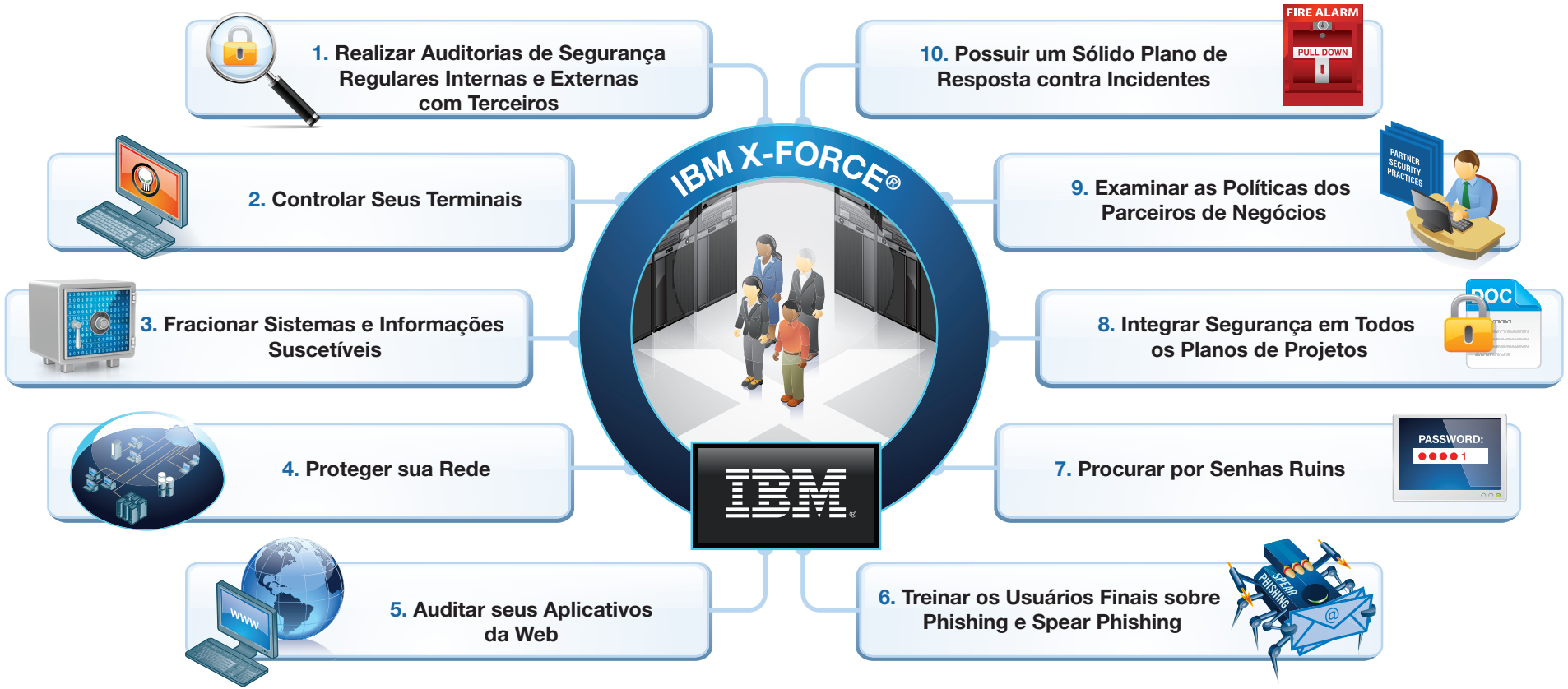



*Figura 3: Se o IBM X-Force estivesse comandando o Departamento de TI*

### 1. Realize auditorias regulares de segurança interna e externa de terceiros

Sua rede está em constante mudança. Quando novos problemas de segurança forem introduzidos, você precisa encontrá-los antes que os vilões os encontrem. Auditorias regulares de segurança de terceiros, em conjunto com constante avaliação de vulnerabilidades e varreduras são as melhores formas de garantir que você entenda a visualização completa da sua rede e onde as fraquezas estão localizadas.

### 2. Controle seus terminais

Você sabe quais sistemas possui em sua rede, qual software está sendo executado, e que níveis de patch e configurações você tem? Até que ponto? O mais próximo que você pode chegar a uma consciência e controle total do terminal, mais segura sua infraestrutura deve se tornar. Você tem um ambiente dinâmico de TI que permite que você se mantenha atualizado com correções de segurança ou você luta para reparar os sistemas devido à falta de recursos, código legado ou códigos personalizados que são incompatíveis com as mais recentes tecnologias? Sistemas legados e ciclos longos de implementação de patches podem se tornar uma responsabilidade de segurança.

### 3. Informações e sistemas confidenciais de segmentos

Em ambientes onde pessoas trabalham com informações particularmente confidenciais, como os datacenters classificados, os funcionários tipicamente recebem sistemas separados de desktops para navegação na Internet e emails em relação ao verdadeiro trabalho. Você pode não estar trabalhando com informações classificadas em seu escritório, mas ainda faz sentido eliminar interconectividade desnecessária entre dados sensíveis e redes inseguras, particularmente se sua organização é alvejada por ataques sofisticados. É importante ter em mente que a interconectividade tem muitas formas, tais como tokens USB.

### 4. Proteja sua rede

Você precisa entender o que reside em sua rede, e você também precisa entender quem possui acesso. As violações geralmente ocorrem em áreas onde sistemas de prevenção contra invasões não foram implementados ou monitorados cuidadosamente. Quando as violações ocorrem, investigações bem-sucedidas dependem do acesso à informações sofisticadas de registros. Quanto mais você monitora sua rede e quanto mais você sabe sobre o que ocorreu no passado da sua rede, mais bem preparado você estará para as violações.


### 5. Realize a auditoria de seus aplicativos da web

As vulnerabilidades dos aplicativos da web continuam a ser uma falha comum que é alvejada por invasores de todas as motivações e níveis de habilidade. Se um aplicativo da web foi desenvolvido internamente, comprada de um fornecedor de software, ou feito download da Internet, se está sendo executado em sua rede, você precisa verificar suas vulnerabilidades. Se você não fizer isso, alguém fará por você.

### 6. Treine usuários finais sobre phishing e spear phishing

Muitos ataques sofisticados envolvem engenharia social ou um elemento de spear phishing. Ataques podem ter como alvo contas e sistemas pessoais e de negócios. Usuários astutos podem suspeitar que alguma coisa não está normal. Se sua organização sabe que ela pode ser potencialmente alvejada, os funcionários tem maior possibilidade de relatar algo suspeito ao invés de ignorá-lo.


### 7. Pesquise senhas ruins

Mesmo após décadas de experiência, senhas ruins continuam sendo uma falha comum de segurança. As auditorias de segurança podem fazer tentativas precipitadas de tentar encontrar senhas ruins, mas esforços constantes e proativos para descobrir senhas ruins de funcionários são muito mais amplos, particularmente quando agrupados com políticas eficazes e educação de usuário final. Para um exemplo de perspectiva inteligente com relação à políticas de senhas, veja essa animação recente: http://xkcd.com/936/


### 8. Integre a segurança em cada plano de projeto

A equipe de segurança não pode operar em uma condição em que tenham que constantemente perseguir projetos que “tenham ido para a produção” com introdução de massivas falhas de segurança na rede que parecem mostrar um relatório de avaliação de vulnerabilidades. A segurança deve ser aplicada em uma nova infraestrutura desde o início. Alcançar isso exige artifícios políticos – a organização de segurança deve ser ativada e não ser uma barreira burocrática. A equipe de segurança deve demonstrar constantemente seu valor para o restante do negócio em todos os níveis.

### 9. Examine as políticas dos parceiros de negócios

Neste mundo de computação em nuvem e complexos relacionamentos de serviços terceirizados, muitos dos sistemas pelos quais você é responsável podem ser operados por outras empresas. Muitos ataques "internos" vêm de funcionários que trabalham para os parceiros de negócios da empresa alvejada. Sua equipe de segurança fez auditoria das práticas de seus parceiros? As práticas deles são consistentes com as suas? Você está confiante na execução deles?


### 10. Tenha um sólido plano de resposta contra incidentes

Eventualmente, a prevenção falha. Gerenciar ataques sofisticados e com alvo específico é um processo contínuo que envolve não apenas ser capaz de identificar se uma violação ocorreu, mas ser capaz de responder e investigar, aprender e adaptar-se. Se você é um alvo estratégico importante e não está consciente de nenhuma violação, isso pode significar que você não está observando cuidadosamente.

# Phishing, spear phishing, ameaça avançada persistente e ataques com alvos em rede

## Introdução

No ano passado um grande incidente de ciberinvasão envolvendo o Google ocorreu e foi chamado de "Aurora". Antes do incidente Aurora, o termo "Ameaça Avançada Persistente" ou APT recebia pouco destaque nos círculos de cibersegurança e nas notícias em geral. O termo se originou com os militares anos antes e foi ocasionalmente mencionado e discutido em círculos profissionais e particulares, mas após o Aurora, ele apareceu em toda a imprensa e está nas notícias desde então, ligado a um número de invasões.

Por outro lado, o termo phishing tem sido comentado nas notícias sobre cibersegurança há muito tempo. Spear phishing também é um termo comum há alguns anos, embora não tenha sido tão utilizado quanto o mais comum phishing.

O termo spear phishing foi intimamente associado aos recentes incidentes de APT. O Google Aurora se tornou um incidente de APT bem comentado, que resultou de um ataque de spear phishing.

Esses termos estavam sujeitos a serem usados erroneamente na imprensa recentemente, e até mesmo em discussões profissionais, já que o significado de cada um tende a ser vago. Phishing soa muito parecido com spear phishing. O uso errôneo desses termos parecem estar aumentando. Porém, eles são bem diferentes um do outro e devemos prestar atenção ao uso, entendimento e reconhecimento correto de cada um.

Recentemente, alguns observadores introduziram o termo Ataques com Alvos em Rede como alternativa à Ameaça Avançada Persistente em uma tentativa de reduzir a confusão com relação à definição.

## Phishing

O nome phishing é derivado da analogia de pescar em um grande lago. Você joga a isca no lago e não se importa se há 10.000 peixes ali que não gostem dela. Você também não se importa se conseguir pegar o maior peixe do lago. Tudo que você quer é que meia dúzia ou alguns peixes razoavelmente grandes mordam a isca e se tornem o jantar. Seu jantar é quantidade, e não tamanho.

Phishing em geral, é o método de atacar usuários fingindo ser um site legítimo e confiável, como um banco, serviço de email ou alguma loja com que o usuário possa ter algum contato[3]. Alguns phishing podem levar a uma fraude bancária onde os invasores roubam a conta da vítima, enquanto outros podem levar a sites malware tentando comprometer ainda mais a vítima.

O phishing se baseia em emails em massa com relativamente pouca personalização, além de um endereço personalizado no campo "para" e talvez um nome no assunto e no corpo da mensagem. Eles geralmente são enviados em grande volume através dos botnets e envios de email em massa. O phishing pode parecer um pouco amador com grande quantidade de erros de ortografia ou gramaticais. Pode aparentar ser de uma instituição que o destinatário pode ter ou não uma relação comercial. Muitos desses detalhes podem servir como um aviso de que esse email não é legítimo. Geralmente, ataques de phishing levam os usuários à malware, como falsos Antivírus ou Trojans, ou URLs maliciosas executadas por invasores tentando captar conexões. Como são mensagens em massa, as várias organizações e serviços de segurança rapidamente coletam os sites maliciosos, as URLs, o software, e são rapidamente detectados. As pessoas por trás do phishing não passam muito tempo preparando essas mensagens e os sites podem funcionar por poucas horas antes de serem derrubados por organizações de segurança. Quem envia emails de phishing realmente não se preocupa se 99,99% das pessoas que recebem o email, enviam-no para a lixeira.

Enquanto o phishing originalmente se referia à atividade de email, desde então, evoluiu para a inclusão em mensagens instantâneas, páginas de redes sociais, e outros mecanismos de entrega pelos quais um usuário pode ser levado a visitar um site malicioso, disfarçado de algo que eles devam confiar.

3 Phishing: http://en.wikipedia.org/wiki/Phishing

## Spear phishing

Spear phishing é uma forma de phishing[4] mas, além de compartilhar parte de um nome e um paradigma básico, em pouco eles se parecem. Em contraste com o phishing comum, ele é altamente direcionado.

O spear phishing é altamente direcionado e possui como alvo poucos indivíduos, porém, muito específicos, dentro de uma organização. Ele é extremamente personalizado para aparentar ser proveniente de um amigo ou colega de trabalho. Os invasores conhecem bem os alvos e podem demandar tempo e esforço consideráveis estudando-os e planejando os ataques. Provavelmente, não parecerá ser uma mensagem genérica de uma grande instituição. Pelo contrário, parecerá ter vindo de um amigo ou colega com quem as conversas podem ser frequentes. Pode até ser relacionada com eventos ou atividades recentes que as pessoas têm conhecimento. A mensagem em si pode nem ser uma "fraude", mas pode realmente vir da conta comprometida de outra pessoa. O malware ou site malicioso que o email envia não terá sido enviado em massa, então as organizações de segurança e antivírus podem não estar cientes sobre os sites e software. Resumindo, essas pessoas escolheram os alvos e as ferramentas cuidadosamente. Os invasores decidiram que queriam você e fizeram um grande esforço para conseguí-lo. Consequentemente, deve valer a pena para os invasores. A porcentagem de rendimento deve ser muito maior, apenas 0,01% de sucesso não é possível. Os invasores exigem uma porcentagem significativa dos alvos para que caiam na armadilha. O valor do alvo também tem que ser muito mais alto, para fornecer um melhor "retorno sobre investimento".

Para ampliar a analogia com a pesca, aí é onde o pescador está em pé, com uma lança na mão, na água, em um deque, em um barco, observando o peixão que ele quer. Ele espera pacientemente enquanto assiste os movimentos do peixe e aprende sobre esses movimentos. Quando for o momento certo, o spear phisher age rapidamente e de modo decisivo quanto a pegar ou não o peixe. Se não quiser, ele pega outro peixe ou outra lança. Muito tempo e esforço é gasto nesse tipo de pesca. Seu jantar é muito mais sobre o tamanho do peixe do que a quantidade.

Como o phishing, o spear phishing pode acontecer em diversos canais e não apenas no email ou nas mensagens instantâneas.

Whaling, em relação ao spear phishing, é um termo usado ocasionalmente para descrever o spear phishing que tem como alvo específico os funcionários do mais alto escalão dentro de uma empresa. Eles têm como alvo os maiores "peixes" da organização. Esses podem não ser necessariamente os executivos de nível C com informações financeiras valiosas, mas podem ser pessoas com posição de autoridade ou pessoas com altos níveis de acesso a dados. O termo whaling não é tão popular quanto spear phishing e frequentemente você irá ouvir spear phishing relacionado com qualquer ataque, sendo a um executivo de alto nível ou a um funcionário comum.

Há mais de 2000 anos, Sun Tsu escreveu, em A Arte da Guerra "Ataque onde não há defesa. Defenda onde não há ataque". A primeira parte é fácil de entender e é a visão do agressor. Ataque onde você ver uma fraqueza e uma fraqueza é onde o defensor não está protegido. A segunda parte não é tão fácil de se entender e está sujeita a interpretações ao longo dos séculos. Uma das interpretações é que ele está meramente dizendo a mesma coisa do ponto de vista de um defensor, apenas contando para o outro que ele deve proteger as áreas frágeis que podem ser percebidas por um agressor e serem atacadas.

Podemos tomar esse conselho de nos defendermos contra o spear phishing, que pode ter como alvo qualquer funcionário, de alto ou baixo escalão dentro da organização. Não são apenas executivos de alto nível e alto valor que serão alvos, mas qualquer um que o invasor perceber em uma posição segura dentro da corporação e por trás de seus perímetros de segurança.

## Ameaças avançadas persistentes

Enquanto phishing e spear phishing parecem ser bem parecidos e utilizam algumas técnicas parecidas, eles possuem como alvo pessoas diferentes, possuem um perfil de ataque muito diferente, e vêm de uma classe de invasor muito diferente. Uma área em que o ataque de

4 Spear Phishing: http://www.webopedia.com/TERM/S/spear_phishing.html
5 Ameaças Avançadas Persistentes: http://en.wikipedia.org/wiki/Advanced_Persistent_Threat

spear phishing pode ser utilizado é nas atividades de abertura de uma Ameaça Avançada Persistente, APT[5]. Enquanto números precisos são impossíveis de serem analisados, acredita-se que sejam as grandes organizações por trás das APTs que devotem equipes significativas de invasores especializados e gastem tempo estudando um número de funcionários de todos os níveis de uma organização. Eles estudam a família, amigos e conhecidos profissionais do funcionário alvo procurando por fraquezas. Eles podem encontrar poucas, mas isso já é suficiente. Eles podem comprometer a conta de um amigo e estudar a correspondência anterior com o alvo escolhido para imitar o estilo e comportamento, ou talvez até participar de uma conversa real se essa oportunidade surgir. O real alvo recebe um email praticamente legítimo de um colega com a atualização de um arquivo que enviou recentemente ou algumas fotos das crianças ou algum vídeo que ambos estejam interessados em assistir. Nada como um email similar que a pessoa da mesa ao lado acabou de receber de um colega de trabalho com a conferência que ele participou há duas semanas. E pode nem ser um email. Pode ser um bate-papo com um amigo em mensagem instantânea. O invasor conhece os alvos bem o suficiente para imitar amigos. Nenhuma bandeira vermelha real até aqui. O comprometimento resultante começa muito pequeno e muito silencioso, baixo e lento, mas se expande, conforme as oportunidades surgem, para outros sistemas e outras pessoas na organização. O malware pode envolver vulnerabilidades de um ou mais dia-zero, desconhecido para a maioria da comunidade de segurança ou até mesmo a comunidade underground geral. O malware percorre distâncias significativas para não atrapalhar ou causar confusão ou até mesmo chamar atenção para si. Finalmente, após meses de preparação e de ter se espalhado em áreas essenciais da organização alvo, ele pode começar a exfiltrar dados e se sustentar contra esforços de erradicação, tornando-se uma ameaça persistente quando for descoberto. A essência desse trabalho são os primeiros ataques, até mesmo os que falharam, que não foram detectados ou relatados. As vítimas não sabem que foram atacadas.

Com as APTs, a detecção rápida é a melhor defesa, quanto antes melhor. Encontrar um ataque de spear phishing é desafiador até mesmo para quem está preparado. Até mesmo as diferenças entre phishing e spear phishing podem levar as pessoas a um falso senso de confiaça de que elas sabem como encontrar um ataque sofisticado de spear phishing. As pessoas devem verificar mensagens inesperadas, mesmo se for de um amigo ou membro da família, além de não confiar plenamente em URLs. Uma simples resposta para alguém dizendo "ei, obrigada pelo vídeo, foi ótimo" pode ser seguida de uma resposta "hein, que vídeo?" Esses tipos de resposta devem ser feitas "fora da banda" já que você não sabe se seria o invasor a ler e apagar aquela resposta. As pessoas devem ser treinadas para encontrar e relatar qualquer atividade suspeita como essa, até mesmo mensagens instantâneas peculiares com pessoas conhecidas. Se suspeitarem que algo está errado, encoraje-as a relatar essa atividade. Nunca penalize alguém por relatar que pode ter caído em uma armadilha. Toda a sua organização são seus olhos e ouvidos para esses tipos de ataques. Você não conseguirá confiar em seu antivírus para encontrar o malware ou em seu software antispam para bloquear o email. Após o comprometimento, podem ser alguns dos indícios mais sutis que podem levá-lo até ele, como atividades incomuns do DNS, que estão ilustradas em uma série focada no DNS nas **avaliações diárias do MSS (Managed Security Services)** do ano anterior. Mas, você tem que procurar por esses indícios para encontrá-los ou eles ficarão perdidos no meio das atividades diárias. Seja paranóico. Até os paranóicos têm inimigos.

## Ataques com alvos em rede

O termo Ameaça Avançada Persistente causou controvérsias no mundo da segurança. Uma das perguntas é se a APT é um nome próprio para um grupo específico de invasores ou uma descrição de um tipo de metodologia de ataque. Aqueles no campo "nome próprio" enfrentam o desafio de como se referir a ataques que possuem características similares, mas que tenham sido lançados por outros grupos de invasores com diferentes motivos. Geralmente corrigir atributos de ataques de Internet pode ser o próprio desafio. Situações complicadas podem surgir onde operadores botnet motivados financeiramente vendem acesso à uma rede comprometida para invasores mais sofisticados. Aqueles no campo "metodologia" enfrentam o desafio de descrever situações onde invasores sofisticados utilizam tipos diferentes de técnicas de ataque, que eles certamente possuem a capacidade de fazer. Além disso, a palavra "Avançada" causou discórdia no campo "metodologia" já que os profissionais de segurança

geralmente veem esse termo de uma perspectiva técnica ao invés de em termos de sofisticação operacional do invasor, e se a técnica específica é "Avançada" pode ser questão de opinião.

O termo Ataques com Alvos em Rede descreve uma tentativa dominante de manter o controle da rede de computadores de uma organização alvo, independentemente de quem está mirando ou porque. Ele fornece, portanto, uma forma de caracterizar a situação enfrentada por uma organização, independente de quem está lançando o ataque ou do "Avanço" que suas ferramentas e técnicas parecem ter. Se a adoção desse termo como uma alternativa mais neutra para "Ameaça Avançada Persistente" irá se consolidar nos círculos de segurança, precisa ser vista.

## "Não há patch para..."

Quando o assunto de phishing e spear phishing aparece, sempre haverá quem pergunte “como alguém foi tão estúpido?” Essa pergunta pode ser compreensível para phishing comum. Porém, não é tão aplicável para spear phishing e APTs. Spear phishing e APTs são altamente sofisticados. E não são tão fáceis de serem identificados.

Temos muito termos depreciativos utilizados em casos onde alguém erra e cai em armadilhas como "operador cabeça no espaço", "o louco que segura o teclado", "PEBKAC (Problema Existe Entre Teclado e Cadeira) ou "PICNIC" (Problema Na Cadeira, Não No Computador). Esses termos são resumidos em um comentário que vemos nos slides de apresentação quando um erro humano acontece – "Não há patch para estúpidos." Porém, esses termos podem desprezar a sofisticação de um número de ataques e fazer uma injustiça a alguns dos indivíduos enganados. Eles podem até estar piorando o problema.

Ao categorizar esses problemas como tais, nós podemos estar dando as pessoas o falso senso de confiança de que eles nunca cairiam em algo assim. Eles não serão estúpidos. Mas os invasores também não são estúpidos e estão escolhendo os alvos cuidadosamente e planejando os ataques. A pessoa que cair em um deles pode não ser estúpida, mas não estar preparada e pode estar despreparada por causa de referências excessivas a ser estúpida.

Ao categorizar esses problemas como tais, podemos colocar as vítimas na defensiva. Elas ouviram os comentários depreciativos e estão aqui ou suspeitam (mas não têm certeza) de que algo ruim pode ter acontecido com elas. Elas ousam contar a alguém e parecerem ridículas por cair em uma armadilha? Elas devem ser encorajadas a relatar qualquer coisa diferente do normal. Devemos ter cuidado com a terminologia e enfatizar que alguns desses invasores são bons e estão melhorando.

## Exemplos das notícias

**Google e Aurora**[6]

Quando o Google anunciou que havia descoberto uma grande invasão, o termo APT não se tornou tão comum quanto atualmente. Ao longo de semanas e meses, informações sobre a extensão da invasão e quanto tempo esteve presente junto com detalhes do malware, foram reveladas. Tornou-se mais aparente que esse ataque não foi comum. Finalmente, em junho de 2010, no Encontro Anual Geral do FIRST (Forum of Incident Response and Security Teams), Heather Adkins do Google fez uma apresentação excelente detalhando o ataque, sua descoberta, e a resposta seguinte ao incidente. Ela descreveu como ele foi apenas detectado pela extração de dados dos registros extensivos de DNS e que o malware, embora basicamente mundano, foi recompilado para evadir-se da detecção dos defensores de antivírus. Ela descreveu como eles utilizaram análise judicial e extração de dados adicional para trazer de volta o comprometimento original "paciente zero" e seguir ainda mais o ataque em relação às versões mais recentes de malware que foram reintroduzidas nos sistemas.

O ataque original foi um ataque com foco à Mensagem Instantânea. Os invasores haviam pesquisado bastante e comprometeram a conta de um amigo. A metodologia do ataque foi avançada em sua pesquisa, mesmo que o malware em si não fosse. Os invasores foram muito persistentes. Eles criaram todo um critério para uma APT.

6 Para o Google, a análise do registro do DNS essencial na investigação do ataque contra Aurora: http://searchsecurity.techtarget.com/news/1514965/For-Google-DNS-log-analysis-essential-in-Aurora-attack-investigation

**Stuxnet**[7]
Stuxnet é considerado por um número de profissionais de segurança a ser outro exemplo de APT, mas há alguma controvérsia sobre essa designação. Ele não parece ter sido ativado através de spear phishing. A metodologia de ataque foi avançada e os invasores fizeram muita pesquisa sobre seus alvos. Porém, o ataque de ativação (aparentemente infectaram chaves USB e possivelmente outros mecanismos) foi amplo e não foi focado em indivíduos específicos, apesar de o grande alvo ser muito específico. Uma vez que o ataque estava sendo preparado, porém, ele teve uma abordagem de infiltração "baixa e lenta" e uma comunicação silenciosa e de não causar nenhum dano enquanto estava sendo inserido na rede e procurando por dados a serem exfiltrados, e finalmente, a última missão de causar danos para certos sistemas de controles industriais. O malware foi atualizado várias vezes enquanto exibia uma persistência tenaz. Pareceria estar de acordo com o comportamento de uma APT, mas não envolvia spear phishing.

**RSA**[8]
O ataque contra RSA certamente parecia ser similar àquele contra o Google. Inicialmente, o RSA disse muito pouco sobre o comprometimento ou sobre a extensão do dano / penetração. Após algum tempo, eles anunciaram que haviam sido atingidos por um ataque de APT que havia sido percebido no início. Também relataram que os invasores utilizaram um ataque phishing com um anexo malicioso alvejando uma vulnerabilidade dia-zero, mas os emails que foram expostos publicamente não parecem ter sido alvejados cuidadosamente. Também foi relatado que os invasores utilizaram dados coletados do RSA em ataques contra outros alvos, incluindo alguns grandes contratantes do Departamento de Defesa. Esse foi um sério comprometimento que não impactou apenas o RSA, mas uma grande quantidade de outras organizações que dependem da tecnologia que o RSA produz para proteger suas próprias infraestruturas.

## Conclusão

Ataques de phishing, spear phishing, APTs e ataques com alvos em rede parecem ter chegado para ficar. Como explicado previamente, phishing e spear phishing são diferentes em escopo e execução. Spear phishing nem sempre indica uma APT, e ataques de APT nem sempre são sinônimos de ataques com alvos em rede. Entender as diferenças intrínsecas entre essas técnicas ajuda a fornecer melhor entendimento, educação e remediação.

O que é mais preocupante sobre esses tipos de ataque é que estamos testemunhando uma mudança nos paradigmas e uma agressão sem precedentes na questão da confiança. Essas séries de ataques contra cadeias físicas de fornecimento agora estão alvejando o intelectual, o e-commerce, assim como os softwares e firmwares que sustentam nossas redes.

Tudo que sabemos ou fazemos com relação à Internet é impactado como o elemento humano representa a força em ver o que pode ser feito, assim como o lado mais fraco e o ponto mais fácil a ser superado.

As organizações devem perceber que alguns, e não todos, dos nossos dados devem ser protegidos. Não apenas em tecnologias defensivas, mas também no monitoramento e revisão em todos os estágios dentro do ciclo de vida dos dados. Além disso, precisamos de estímulos dos outros para saber o que está acontecendo na Internet, para que possamos realizar rápidas modificações nas técnicas usando esses processos. Essa consciência nos permitirá monitorar melhor, caçar de forma judicial, e remover a quantidade de ameaças e ataques arraigados na organização em muitos terminais.

7 Como detetives decifraram o Stuxnet, o malware que mais ameaçou na história: http://arstechnica.com/tech-policy/news/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history.ars
8 RSA: Anatomia de um ataque: http://blogs.rsa.com/rivner/anatomy-of-an-attack/

## IBM Managed Security Services – uma visualização global de ameaças

O IBM MSS (Managed Security Services) monitora vários bilhões de eventos por dia em mais de 130 países, 24 horas por dia e 365 dias por ano. A presença global do IBM MSS fornece uma visão em primeira mão das ameaças atuais. Os analistas IBM utilizam essa riqueza de dados para apresentar uma compreensão única da visualização da ciberameaça. Essa seção é focada em SQL Injection, atividade JavaScript, ataques com força bruta, e varreduras entre outras ameaças que ainda serão discutidas neste relatório. A tendência dessas ameaças é essencial para determinar quais direções elas estão tomando e para entender seu significado em nossas redes.

### Atividade de ataque de SQL Injection em 1S 2011

Uma vulnerabilidade com injeção de SQL ocorre quando a entrada de um usuário é filtrada de maneira imprópria, permitindo que um invasor execute comandos SQL em um servidor alvo. Especificamente, se os caracteres de escape não forem filtrados, um invasor pode alterar uma consulta para produzir resultados indesejáveis. SQL Injections geralmente levam à revelação de informações ou a habilidade de alterar informações armazenadas no banco de dados.

O SQL Injection verificou uma tendência relativamente em alta durante 2011 (consulte Figura 4). É muito cedo para dizer qual será a tendência geral para 2011. E o SQL Injection continuará a ser um vetor de ataque favorito entre grupos maliciosos conforme demonstrado por inúmeros ataques em massa que verificamos nos últimos anos.

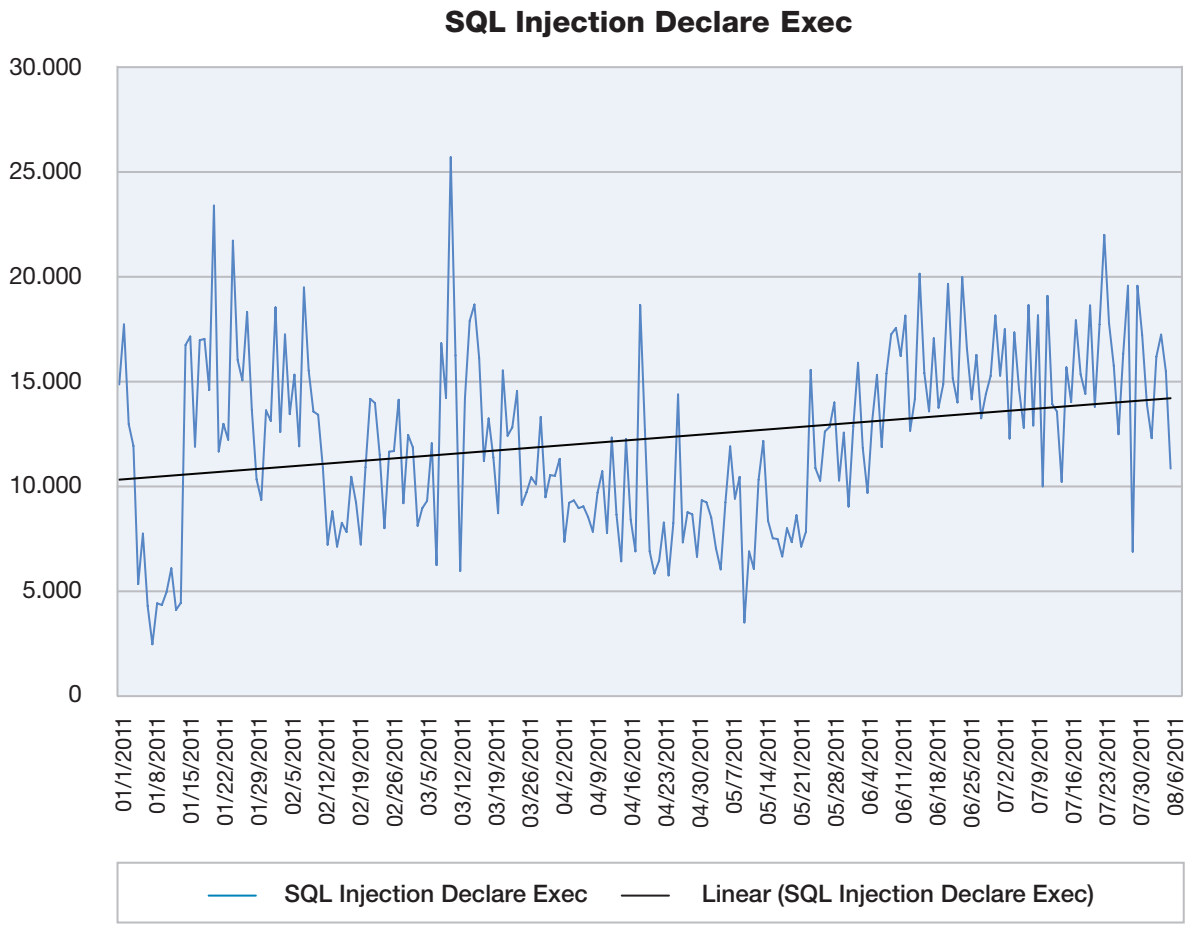



*Figura 4: SQL_Injection_Declare_Exec Activity January 2011 – Junho de 2011*

Porém, é possível que essa atividade se torne mais lenta ou diminua, resultando em uma tendência estabilizada ou em queda durante o ano todo.

Historicamente, ataques com alvo em SQL Injection se concentravam principalmente em dados – obtendo dados não autorizados ou alterando-os. Porém, no início de 2008, começamos a ver diversos comprometimentos em massa coordenados e simultâneos de dezenas de milhares de websites utilizando SQL Injection como vetor de ataque. Em vez de roubar dados, os invasores injetaram conteúdo HTML personalizado contendo iframes invisíveis que redirecionavam os usuários para sites que hospedavam explorações drive-by e outros conteúdos maliciosos. **O Relatório de Tendências e Riscos IBM X-Force 2010** destaca os diversos ataques em massa observados nos últimos três anos.

A tendência continua em 2011. Em março, o IBM Managed Security Services começou a rastrear um ataque em massa de SQL Injection chamado **LizaMoon** devido a uma URL que havia sido injetada nas tabelas SQL do site alvo. Enquanto este ataque alcançou níveis notáveis, não vimos nem de perto o volume de atividade que vimos com os ataques "Asprox" (2009) e "dnf666" (2010). Isso ocorreu porque os ataques pareciam ser a fonte de apenas alguns poucos endereços específicos de ID que se correspondiam com o site, sendo injetados no banco de dados da vítima. Contraste isso com o ataque SQL Injection Asprox que usou um botnet para fazer a injeção em massa, dando aos invasores muito mais alcance e largura de banda.

Um dos principais problemas para as organizações que estão tentando trabalhar com esse problema é que os invasores não estão explorando apenas as vulnerabilidades no software atual do servidor da web, como IIS e Apache. Isso não é suficiente para que os administradores do servidor da web fiquem atualizados com os patches dos fornecedores. Os invasores também estão analisando os pacotes dos aplicativos da web (escritos em .ASP, PHP, etc) executados no servidor da web para encontrar vulnerabilidades SQL Injection que possam explorar. Em alguns casos, uma vez que o aplicativo da web vulnerável tenha sido identificado, os invasores utilizam mecanismos de pesquisa para automatizar o processo para encontrar sites alvos que utilizam aplicativos vulneráveis.

Infelizmente, os invasores possuem muitas opções disponíveis para permanecer indetectáveis. Há diversas formas de disfarçar e ofuscar o ataque para evitar a descoberta. Para evitar SQL Injection, os aplicativos da web devem ser varridos ou auditados para locais onde a entrada do usuário pode passar infiltrada para o banco de dados. Isso inclui formulários da web, parâmetros de URL e valores de cookies. Onde possível, as afirmações com parâmetros SQL devem ser usadas para que o driver de banco de dados subjacente possa escapar os caracteres nocivos. Além disso, registros da web devem ser monitorados por tentativas de invasão como cadeias codificadas hexagonais ou palavras-chave SQL como DECLARAR, DIFUNDIR, CONVERTER, UNIR, INSERIR ou ATUALIZAR. Organizações que suspeitam que tenham sido vítimas de ataques recentes de SQL Injection devem automatizar a limpeza do banco de dados.

Além da auditoria aos aplicativos da web, os administradores devem revisar suas políticas de acesso remoto e verificar quais senhas reutilizáveis são proibidas em favor de mecanismos fortes de autenticação, como SSH "authorized_keys". Acesso remoto às contas administrativas devem ser desativados completamente com a possível exceção de aplicativos e chaves plenamente controlados. Para ajudar a minimizar o risco de ser infectado ao visitar sites comprometidos, os sistemas do cliente devem garantir que eles tenham aplicado os mais recentes patches de segurança para navegadores e plugins (Flash, Realplayer™, etc.). Adicionalmente, contas "fantasmas" (contas expiradas ou contas onde proprietários não estejam mais presentes), devem ser removidas.

A desfiguração pública, o vazamento de dados confidenciais e o comprometimento do servidor de banco de dados pode resultar desses ataques. Um comprometimento completo de sistemas vulneráveis de clientes também é possível. É imperativo que as organizações tratem as vulnerabilidades SQL Injection como uma ameaça séria e direcionem-nas corretamente.

# MSS – Principais assinaturas de alto volume de 2011

## Principais assinaturas de alto volume

Tabela 1, mostra a localização das assinaturas de alto volume no topo do MSS (Managed Security Services) e sua linha de tendência para a metade do ano de 2011 se comparada a 2010. O que é interessante é que as duas principais assinaturas foram revertidas na posição em nosso gráfico. O SQL_injection agora é o número um e verificando uma tendência crescente, o SQL_SSRP_ Slammer_Worm está em segundo lugar e continua a observar uma tendência à queda. Seis das dez principais assinaturas de 2010 conseguiram uma posição na lista semestral de 2011. Além disso, com exceção do SMB_ Empty_Password_Failed, a metade superior está formada das mesmas assinaturas; apenas sua posição mudou.

| Nome do Evento | Tendência | Rank Semestral de 2011 | Rank do Final de Ano de 2010 |
|---|---|---|---|
| SQL_injection | Para cima | 1 | 2 |
| **SQL_SSRP_Slammer_Worm** | **Para baixo** | **2** | 1 |
| SMB_Empty_Password_Failed | Relativamente para cima | 3 | |
| SSH_Brute_Force | Para cima | 4 | 4 |
| HTTP_Unix_Passwords | Para cima | 5 | 6 |
| **PsExec_Service_Accessed** | **Relativamente para baixo** | **6** | 3 |
| HTTP_DotDot | Para cima | 7 | |
| Shell_Command_Injection | Relativamente para cima | 8 | |
| MSRPC_RemoteActivate_Bo | Para cima | 9 | |
| SMB_Mass_Login | Para cima | 10 | 7 |

*Tabela 1: Principais assinaturas de alto volume MSS e linha de tendência – meio do ano de 2011 versus final do ano de 2010*

## SQL Injection – Maior tendência e volume mais alto

O SQL Injection continua a ser o vetor de ataque favorito entre os invasores. Nossa assinatura SQL heurística pulou para o primeiro lugar. Contribuindo para esse maior volume de atividade estão as campanhas de SQL Injection em massa que continuam a castigar os usuários, como discutido na seção **SQL Injection**. A tendência geral desde 2010 até a metade de 2011 foi crescente.

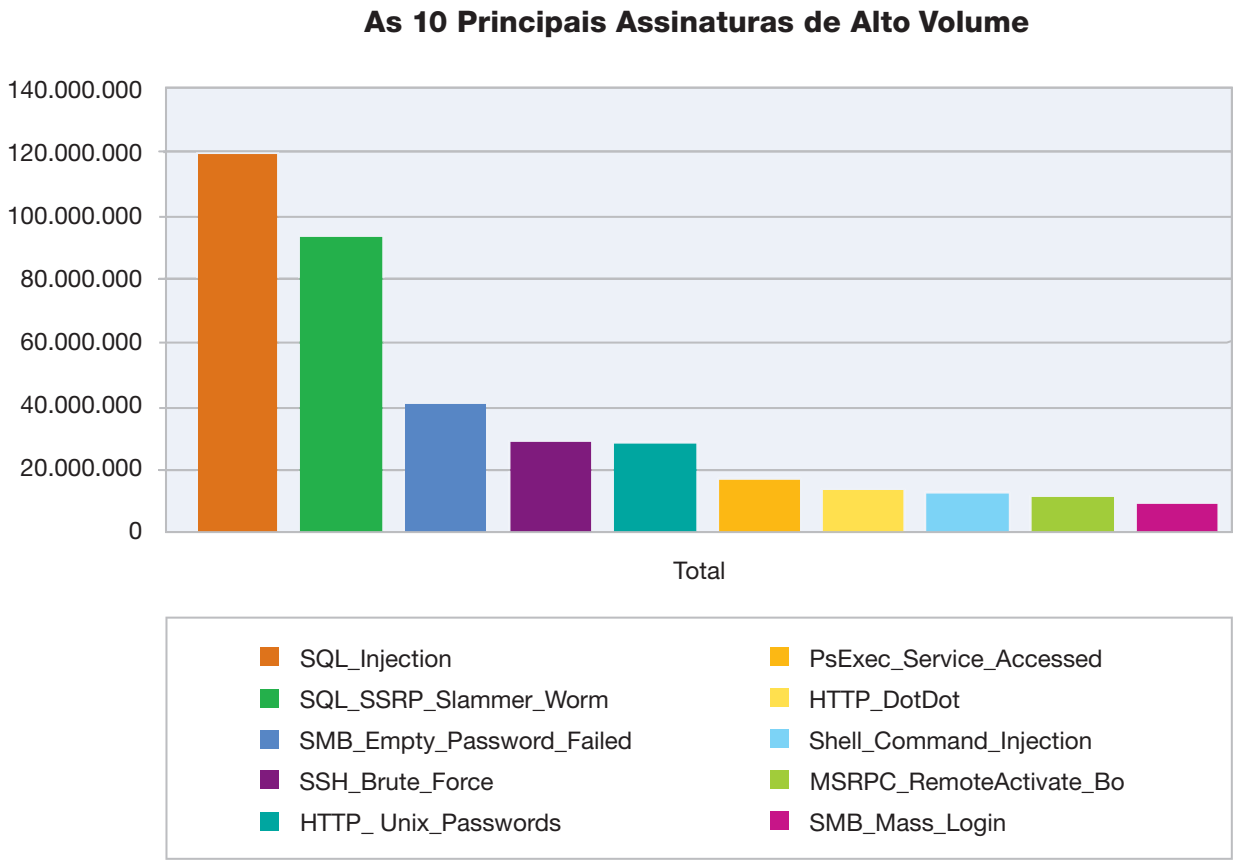



*Figura 5: 10 Principais Assinaturas de Alto Volume – 1S 2011*

## SQL Slammer – não mais o dominante

A principal assinatura de alto volume em 2010 foi SQL_SSRP_Slammer_Worm. Essa assinatura caiu para o segundo lugar em nossa tabela semestral de 2011. O SQL Slammer tem como alvo uma vulnerabilidade de estouro de buffer na instalações do Serviço de Resolução no Microsoft SQL Server 2000 ou Microsoft Desktop Engine (MSDE) 2000. A seção **"O dia que o SQL Slammer desapareceu"** destaca uma queda drástica na atividade do SQL Slammer em março, o que contribuiu para a queda na colocação dessa assinatura em nossa lista semestral de 2011.

## Alvo nos servidores SMB (Server Message Block)

Duas das principais decodificações mais uma vez (duas) identificam ataques contra ameaças com alvo em servidores SMB (server message block) – SMB_Empty_Password_Failed (terceiro lugar) e SMB_Mass_Login (décimo lugar). Enquanto o SMB_Mass_Login já esteve em nossa lista de final de ano de 2010 (sétimo lugar), o SMB_Empty_Password_Failed é novo na lista.

SMB_Empty_Password_Failed detecta quando uma tentativa mal sucedida de login sem senha é feita a um servidor SMB. Se os invasores estão tentando se conectar a servidores SMB sem senha, isso significa que esse método de ataque continua a ser frutífero para eles. A assinatura SMB_Mass_Login detecta um número excessivo de sessões NETBIOS concedidas que possuem origem no mesmo endereço IP. Isso pode indicar uma conta roubada sendo utilizada em um ataque com scripts.

A existência dessas assinaturas na lista destaca uma possível falta de segurança básica com porções SMB. Ameaças recentes, como o malware Conficker e Stuxnet, utilizam porções SMB para se espalhar pelas redes.

## Ataques com força bruta e varreduras

SSH_Brute_Force é outra assinatura interessante nessa lista, ficando no quarto lugar. Um ataque com força bruta envolve um invasor tentando obter acesso não autorizado a um sistema através de diversas possibilidades de senha. Essa assinatura detecta um número excessivo de Identificações de Servidor SSH de um servidor SSH em um limite de tempo específico. Através desse tipo de ataque, um indivíduo malicioso pode ser capaz de visualizar, copiar ou deletar arquivos importantes no servidor acessado ou executar códigos maliciosos.

A queda na colocação desta assinatura na lista pode indicar um movimento em direção à mitigação de ataques de força bruta com a desativação do acesso direto a contas raízes e a utilizar nomes de usuário e senhas fortes. Por outro lado, essa atividade é uma tendência crescente, e poderemos ver essa assinatura subir novamente no final do ano de 2011.

Não se esqueça do UNIX. . . Diversas das assinaturas mencionadas anteriormente detectam ataques vulnerabilidades da Microsoft; porém, sistemas UNIX não estão imunes à ameaças. A assinatura HTTP_Unix_Passwords continua na lista principal de alto volume, mas subiu uma posição, do sexto para o quinto lugar. Essa assinatura detecta as tentativas de acesso ao arquivo /etc/passwd nos sistemas UNIX através de um servidor da web (HTTP). Embora essa atividade algumas vezes seja autorizada, também pode ser suspeita. Esse é um ataque muito antigo, mas ainda é bem-sucedido atualmente.

## PsExec – uma ferramenta de administração remota

Terceiro em nossa lista de 2010, o PsExec_Service_Accessed, caiu para sexto lugar no meio do ano de 2011. O PsExec é uma linha de comando com base em uma ferramenta remota de administração utilizada para propósitos legítimos. Porém, worms e ameaças avançadas também se aproveitam do PsExec. O worm "Aqui está", por exemplo, inclui uma ferramenta PsExec que permite que ele seja copiado para outros computadores na rede. Se este aplicativo está sendo utilizado em sua organização, você deve garantir que as melhores práticas de segurança sejam implantadas.

## Atravessando diretórios

A assinatura HTTP_DotDot detecta uma tentativa do invasor de burlar a segurança normal imposta pelo servidor da web e para acessar arquivos normalmente restritos. Um invasor pode atravessar diretórios em servidores da web vulneráveis com o uso das sequências "dot dot" (/../) em URLs, permitindo que o invasor leia qualquer arquivo no servidor alvo HTTP que pode ser lido no mundo todo ou lido pelo ID do processo HTTP. Por exemplo, uma URL da forma (http://www.domain.com/..\..) permite que qualquer um navegue e faça download de arquivos fora do diretório raiz de conteúdo do servidor da web. URLs como o nome de script (http://www.domain.com/scripts..\..\) podem permitir que o invasor execute o script alvo. Um invasor pode utilizar uma listagem desse diretório como informações adicionais para planejar um ataque estruturado, ou pode fazer o download de arquivos em qualquer outro lugar no sistema de arquivos.

## Comandos shell

Nossa oitava assinatura na lista, Shell_Command_Injection, não é nenhuma surpresa. Essa assinatura detecta uma tentativa de injeção de Comando Shell com pontuação de diversas combinações de comandos e símbolos utilizados ao executar comandos shell. Vimos um aumento de um ataque muito rudimentar com o uso de comandos shell que são injetados em entradas limpas. Por que um invasor faria isso? Porque funciona! Ao invés de tentar utilizar SQL Injection, o invasor executa o comando de código através da web.

## Alvo Microsoft

A assinatura MSRPC_RemoteActivate_Bo procura uma solicitação de ativação MSRPC Remota especialmente projetada, utilizada para realizar um estouro de buffer. O Microsoft Windows é vulnerável ao estouro de buffer na interface DCOM (Distributed Component Object Model) do serviço RPC (Remote Procedure Call). Ao enviar uma mensagem defeituosa para o serviço RPC, um invasor remoto pode estourar um buffer e executar um código arbitrário no sistema com privilégios de Sistema Local.

# O dia em que o SQL Slammer desapareceu

## Origem do worm SQL Slammer

Em 25 de janeiro de 2003, um worm agressivo que explorou um estouro de buffer no Microsoft Resolution Service começou uma infecção em massa de servidores conectados à Internet. Embora o worm não utilizasse uma vulnerabilidade SQL para se propagar, a grande maioria das infecções ocorreu em servidores executando Microsoft MSDE (Microsoft SQL Server Desktop Engine). O worm existe apenas para se propagar e imediatamente procurar infectar o maior número de máquinas possíveis ao atacar endereços de IP aleatórios. O worm é muito pequeno, com apenas 376 bytes, então é capaz de enviar uma cópia de si mesmo para uma máquina vulnerável em um único pacote UDP.

Embora a Microsoft tenha lançado um patch para a vulnerabilidade seis meses antes da primeira aparição do Slammer, havia um número suficiente de servidores exploráveis para que o crescimento fosse exponente. De acordo com a análise feita pela **CAIDA (Cooperative Association for Internet Data Analysis)**, 90% de todos os sistemas vulneráveis foram infectados nos primeiros dez minutos do lançamento do worm. Desde que o worm tenha como alvo endereços aleatórios de IP, até mesmo redes sem servidores vulneráveis ficaram de joelhos frente ao grande volume de tentativas de infecção. Como os servidores SQL eram as principais vítimas do worm e os quadros infectados estavam gerando ataques suficientes para surpreender a infraestrutura da Internet, ele foi chamado de worm SQL Slammer pelo então CTO de Sistemas de Segurança da Internet, Chris Rouland.

A velocidade da propagação do worm foi dada em grande parte ao seu pequeno tamanho, mas a limitação de tamanho significava que não seria fácil de se tornar persistente. Remover o worm era tão fácil quando reiniciar o servidor afetado, mas se tornaria rapidamente reinfectado se o patch correto não fosse aplicado. Dados seus efeitos e velocidade assustadora de propagação, ele se tornou uma grande história mesmo fora das comunidades de segurança e de TI. A Microsoft lançou uma campanha educacional para que os administradores de servidores aplicassem o patch e os meios principais de mídia dedicassem uma anormal quantidade de cobertura para uma infecção por malware. O aumento na consciência teve o efeito desejável; o conjunto de servidores vulneráveis diminuiu rapidamente. Combinado com o filtro pelos dispositivos de segurança e as mudanças do ACL (Access Control List) para roteadores, o tráfego reduziu o suficiente a intensidade de negativas de serviços pela Internet.

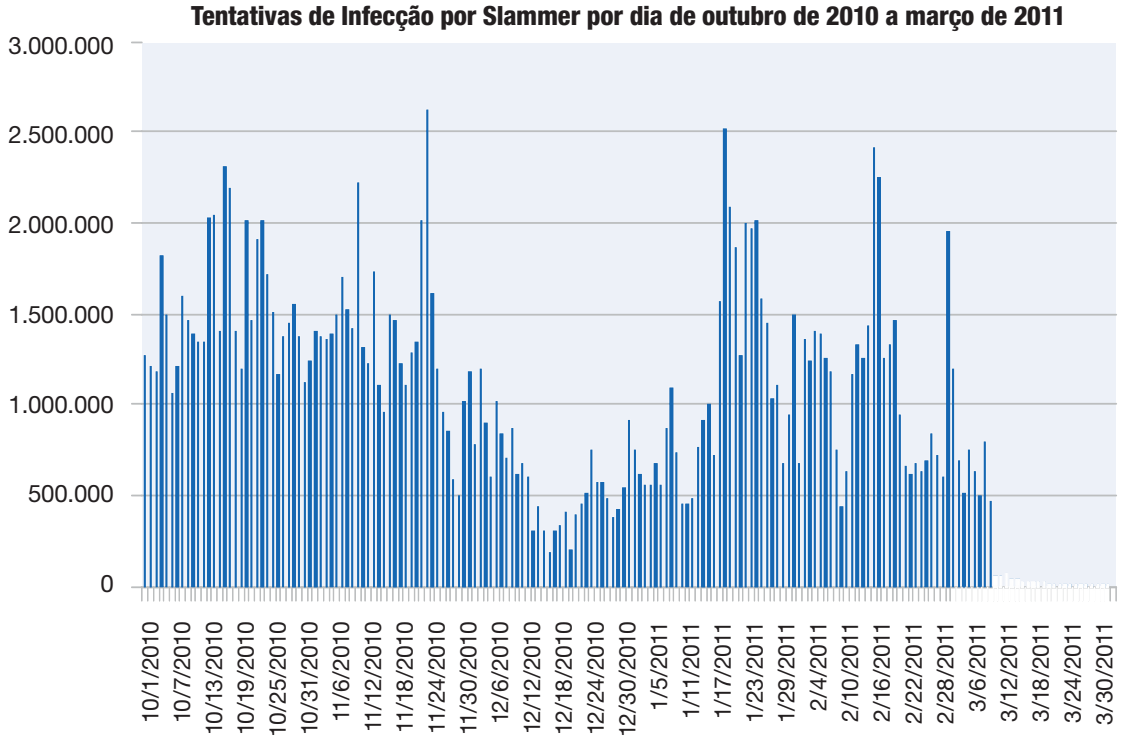



*Figura 6: Tentativas de Infecção do Slammer por dia, de outubro de 2010 a março de 2011*

O Slammer, porém, não desapareceu. Ainda no início de 2011, os pacotes de infecção por Slammer ainda são creditados para uma considerável porção de tráfego UDP na Internet. Para clientes IBM, isso se traduziu em tentativas de infecção medidas em centenas de milhares por dia. Tudo isso mudou nos dias 10 e 11 de março de 2011. Em um período de 24 horas, a taxa caiu para menos de 2.000 por dia, conforme exibido na Figura 6. Nós relatamos primeiramente este tópico no **blog Frequency-X em abril de 2011**.

## Análise da diminuição da atividade

Apenas os números diários já mostram que esse desaparecimento foi coordenado e possivelmente ativado por uma única causa. A queda drástica em um pequeno período de tempo não poderia ser um fenômeno natural, nem o desligamento de alguns servidores contam para tal declínio de tentativas de infecção. A equipe do IBM Managed Security Services decidiu descobrir o mecanismo pelo qual o Slammer tenha sido quase que universalmente desabilitado. O primeiro passo foi determinar como a janela de tempo afetada parecia ser de hora em hora.

Ao invés de uma queda abrupta ocorrer nas duas ou três horas seguintes (assinalando o uso de um estilo de comando e controle kill switch), vemos uma diminuição por fases, ocorrendo após um período de 20 horas (Figure 7). Esses dados apontaram para um desligamento com base no relógio causado pela mesma ativação por código em todos os servidores afetados. Para testar isso, utilizamos a localização geográfica dos endereços fontes de IP para esses ataques. A geo localização funciona com o uso dos registros do whois para endereços registrados e para identificar a localização geográfica desses endereços. O sistema não é perfeito – ele não pode lhe dizer a localização do espaço privado do endereço (10.x.x.x, 172.16.x.x, 192.168.x.x), nem todos os endereços reais possuem registros suficientes para identificar localizações físicas, e você não pode ter certeza se o servidor está com a informação correta de horário ou de fuso horário. Mas mesmo com esses avisos, nossos dados nos trouxeram alguns resultados interessantes.

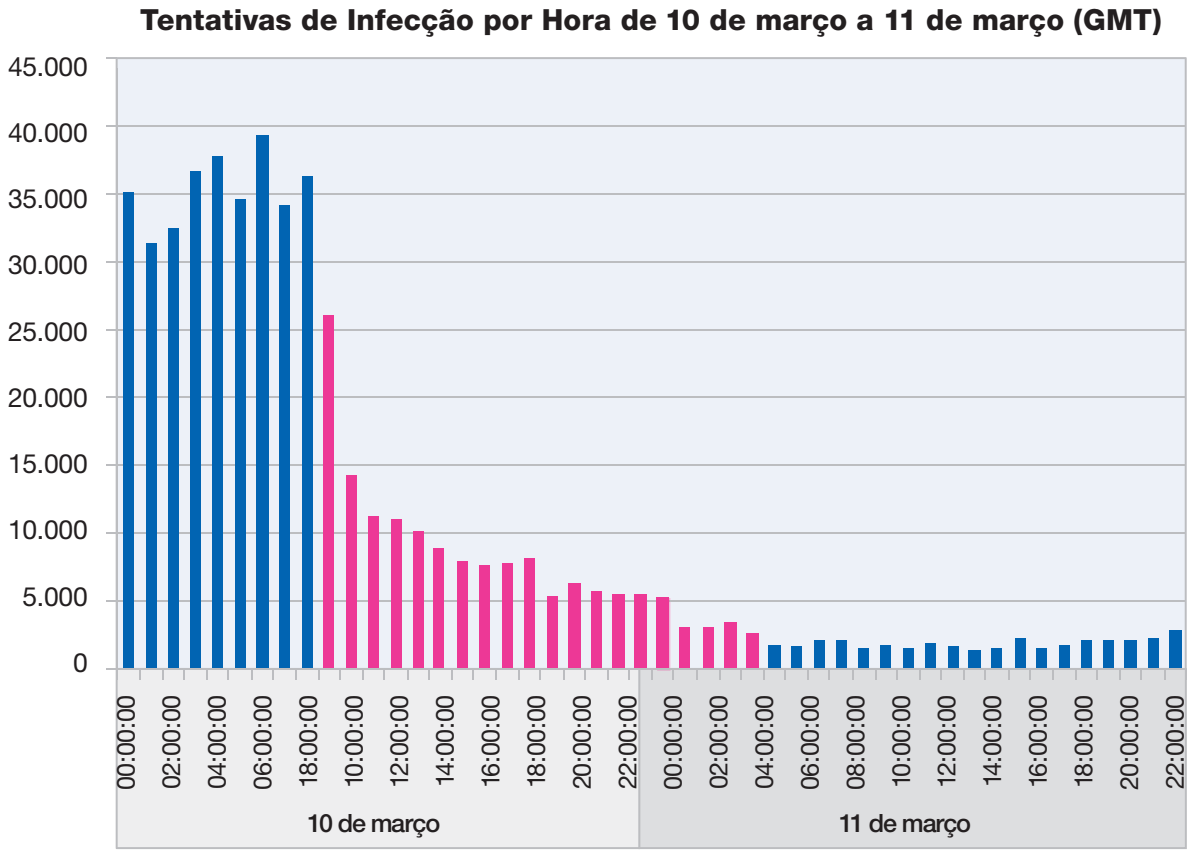



*Figura 7: Tentativas de infecção de hora em hora (GMT) de 10 a 11 de março*

Pegamos todos os endereços fontes de IP para os quais poderíamos obter bons dados de geo-localização e utilizamos os prováveis deslocamentos para observar as tentativas de infecção com base no local estimado do invasor. O que vimos foi uma queda de quase 50% entre 11h e 12h (horário local do invasor) em 10 de março de 2011 (Figura 8). Também vimos uma queda sustentada após às 12h desses endereços de IP. Embora não tenhamos visto uma queda completa no período de uma hora, o fato de que os dados ajustados caíram mais rápido do que os dados não ajustados é significativo. A diferença entre a redução gradual em 20 horas opostas a uma curva aguda ocorrendo em oito horas é um argumento bem convincente para que um conjunto de ativação ocorra entre 11h e 12h com base no relógio do servidor Slammer. Se não houvesse ativação com base no horário, a curva deveria ter sido rompida ao invés de clarificada com os ajustes com base no horário. Esperaríamos ver um gráfico mais irregular que não mais criasse um padrão discernível.

## Conclusão

Embora dados de geo-localização não sejam a metodologia perfeita, a correlação entre o horário local estimado do invasor e a queda nos eventos são fortes o suficiente para apontar para um desligamento automatizado ativado pelo relógio local de um único servidor. Embora esses dados suportem uma resposta plausível assim como “Como”, eles realmente não respondem “Porque”. Há duas teorias alternativas prováveis para o porquê. A primeira é que os pacotes de ataque gerados pelos servidores infectados deram um mapa para máquinas facilmente exploráveis. Um invasor

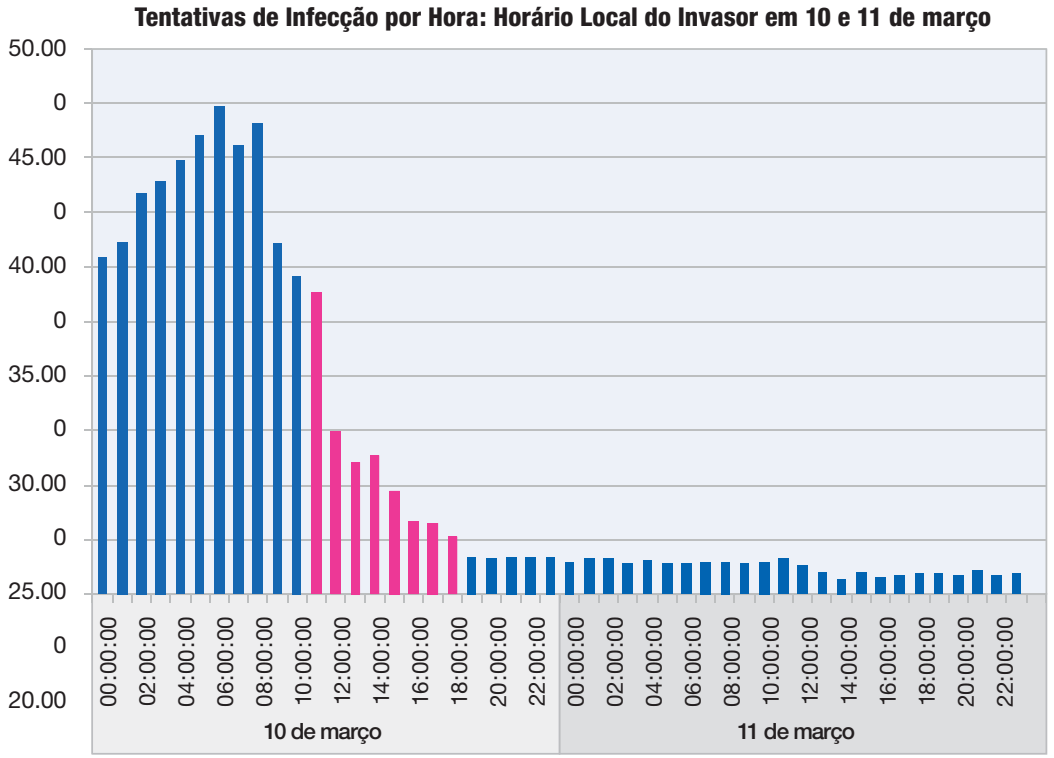



*Figura 8: Tentativas de Infecções por Hora: Horário Local do Invasor em 10 e 11 de março*

se comprometeu com todos esses servidores manualmente ou através de um processo automatizado e de um código botnet instalado neles. Uma vez que o invasor obteve controle dos servidores, ele estabeleceu um patch automatizado e reiniciou para que eles parassem de fazer concessões. A segunda é que o profissional de segurança White Knight decidiu se livrar do mundo do Slammer e fez exatamente a mesma coisa (esperançosamente sem o código botnet persistente.) Essas teorias atribuem dois motivos muito diferentes, mas a implementação é basicamente a mesma.

A coisa mais interessante sobre essa operação é o uso da ativação com base no tempo. Se os servidores tivessem tido um patch quando foram comprometidos, deveríamos ter visto uma redução mais gradual em um período de tempo mais longo ou uma redução aguda que teria ocorrido em uma ou duas horas após o início do patch. O fato de que eles utilizaram atrasos com base em tempo aponta para uma das três das possíveis motivações. Se fosse um botnet malicioso, o invasor poderia querer tempo suficiente para que a impressão digital saísse do roteador e dos registros de firewall para que ele não fosse rastreado. Se ele fosse um White Knight, ele ou ela podem ter desejado utilizar a ativação para saber se a metodologia foi efetiva. A terceira possibilidade é que, não importam os motivos que os invasores tiveram para fazer isso, a pessoa responsável queria obter a atenção da comunidade de segurança e, se essa era a motivação, o objetivo foi certamente atingido.

Verificamos tentativas de infecção subirem e caírem desde março, mas elas não chegaram nem perto ao volume que vimos antes de 10 de março (Figura 9). Considerando a vulnerabilidade que obteve patch por nove anos, parece improvável que esses eram novos sistemas que foram infectados naturalmente.

Os novos eventos formam um padrão de onda e começaram a aparecer em abril de 2011, logo após o fato de o desaparecimento do slammer ter ganhado uma atenção da mídia. É possível que muitos desses tenham sido infecções intencionais por membros da comunidade de segurança tentando responder “porque”.

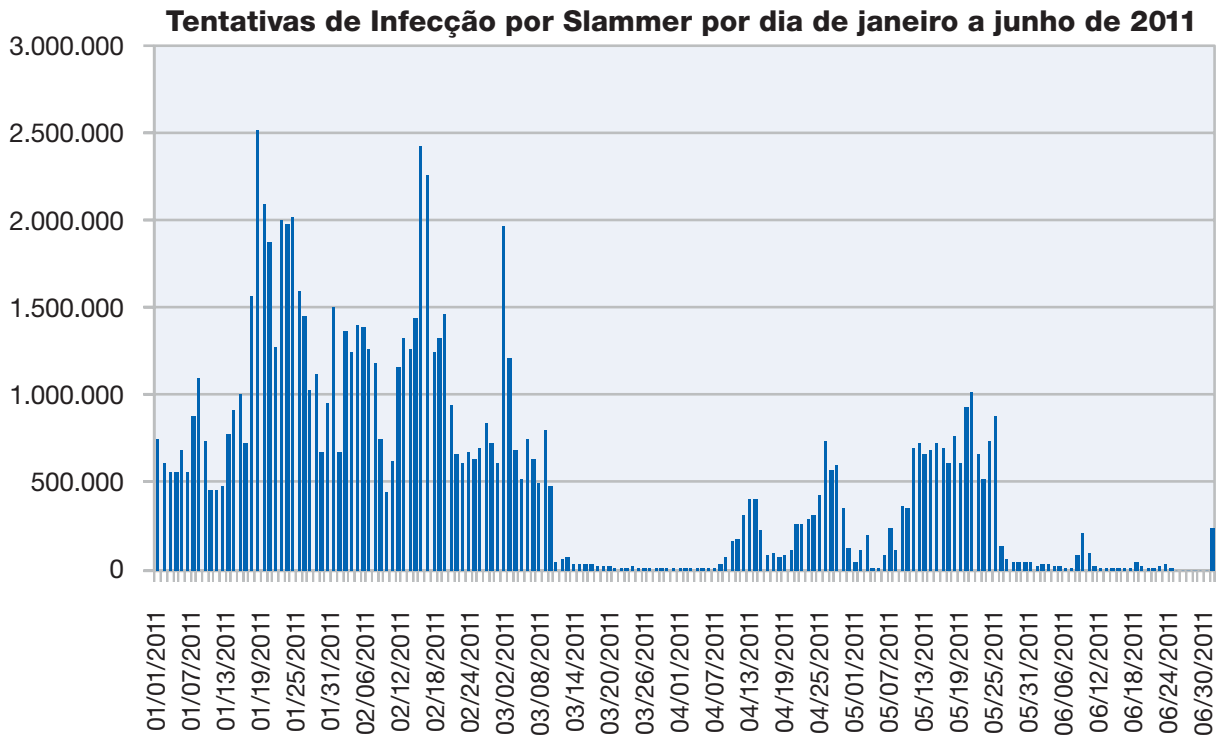



*Figura 9: Tentativas de Infecção do Slammer por dia, de janeiro de 2011 a junho de 2011*

# Tendências, Spam e Phishing do Conteúdo da Web

## Tendências de conteúdo da web

O datacenter IBM Content revisa e analisa constantemente novos dados de conteúdo da web e analisa 150 milhões de novas páginas da web e imagens por mês e já analisou 15 bilhões de páginas e imagens da web desde 1999.

O banco de dados de filtragem da web IBM possui 68 categorias de filtro e 69 milhões de entradas com 150.000 entradas novas ou atualizadas adicionadas por dia.

Essa seção fornece análise para:

- Metodologia de análise
- Domínios internacionalizados de alto nível
- Aumento na quantidade de proxys anônimos
- Domínios de alto nível de proxys anônimos
- Websites maliciosos

## Metodologia de análise

O X-Force captura informações sobre a distribuição do conteúdo na Internet com a contagem dos hosts categorizados no banco de dados de filtro da web do IBM Security Solutions. Contar os hosts é um método aceitável para determinar a distribuição de conteúdo e fornecer uma avaliação realista. Ao utilizar outras metodologias – como contar páginas e subpáginas da web – os resultados podem se diferenciar.

## Domínios internacionalizados de alto nível

Desde o início de 2010 é possível registrar domínios de alto nível com código internacionalizado do país[9]. Portanto, as URLs podem ser exibidas sem o uso de nenhum caractere ASCII. Os primeiros domínios foram registrados no alfabeto arábico ou cirílico. Porém, a quantidade de uso na Internet difere amplamente para línguas diferentes. Embora hajam apenas poucos websites arábicos usando esses novos domínios, há um aumento significativo desses domínios na Rússia.

Em abril de 2011, quase 5% dos novos domínios on-line russos eram domínios .рф[10]. Isso parecia ser algum tipo de promoção de primavera, já que em maio e junho eles caíram significativamente para 1%.

Na seção **Tendência reversa do volume de spam**, forneceremos mais informações sobre o uso desse novo domínio de alto nível.

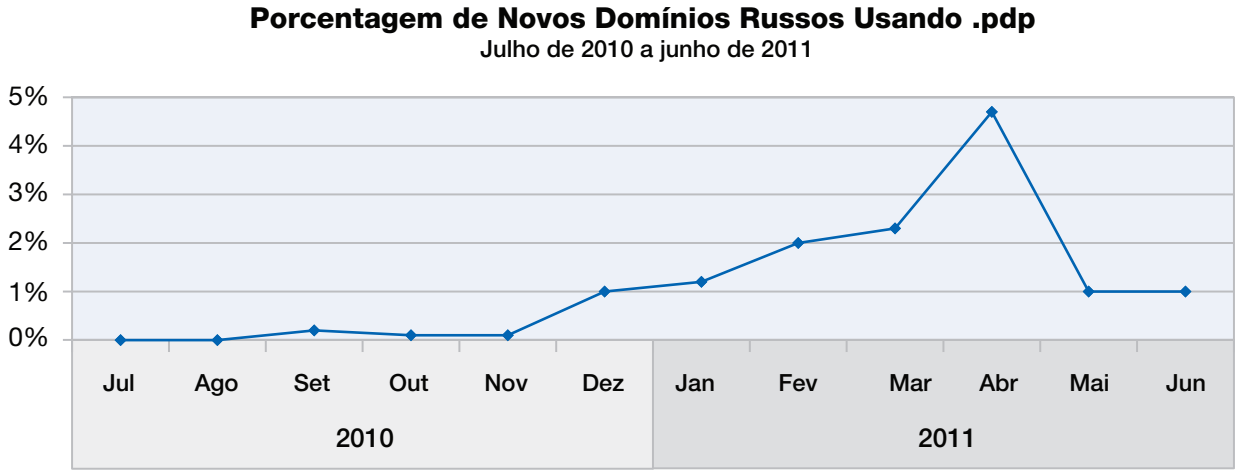



*Figura 10: Porcentagem de Novos Domínios Russos On-line Utilizando .рф – jullho de 2010 a junho de 2011*

9 Veja também: http://en.wikipedia.org/wiki/Internationalized_country_code_top-level_domain
http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains
http://en.wikipedia.org/wiki/Internationalized_domain_name

10 "**рф**" são as letras rf no alfabeto cirílico e significam "Federação Russa".

## Aumento na quantidade de proxys anônimos

Conforme a Internet se torna uma parte cada vez mais integrada de nossas vidas, não apenas em casa, mas também no trabalho e na escola, as organizações responsáveis por manter ambientes aceitáveis cada vez mais veem a necessidade de controlar onde as pessoas podem navegar em locais públicos.

Tal controle é um sistema de filtro de conteúdo que ajuda a evitar o acesso a websites inaceitáveis ou inadequados. Algumas pessoas tentam utilizar proxys anônimos (também conhecidos como web proxys) para contornar as tecnologias de filtro da web.

Os proxys da web permitem que usuários entrem em uma URL em um formulário da web ao invés de visitar diretamente o site alvo. Utilizar o proxy esconde a URL alvo de um filtro da web. Se o filtro da web não estiver configurado para monitorar ou bloquear proxys anônimos, então essa atividade (que normalmente teria sido parada) burla o filtro e permite que o usuário entre no site proibido.

O crescimento de novos sites de proxys anônimos registrados reflete essa tendência.

No primeiro semestre de 2011, havia quatro vezes mais proxys anônimos registrados do que havia há três anos. Proxys anônimos são um tipo crítico de website para rastrear, pela facilidade que os proxys fornecem em permitir que as pessoas escondam intenções potencialmente maliciosas.

Escolhemos nesse relatório fazer uma pequena mudança na metodologia em relação aos relatórios anteriores. No passado, sempre contamos o número total de websites de proxys anônimos. A desvantagem desse tipo de cálculo é que ele não demonstra a natureza dinâmica dessa atividade. Muitos desses proxys anônimos permanecem off-line e o mesmo número de proxys pode ficar on-line sem nenhuma mudança exibida no método anterior de gráfico. Portanto, decidimos mostrar uma nova maneira de apresentar os dados com a contagem dos mais novos proxys anônimos registrados de período em período.

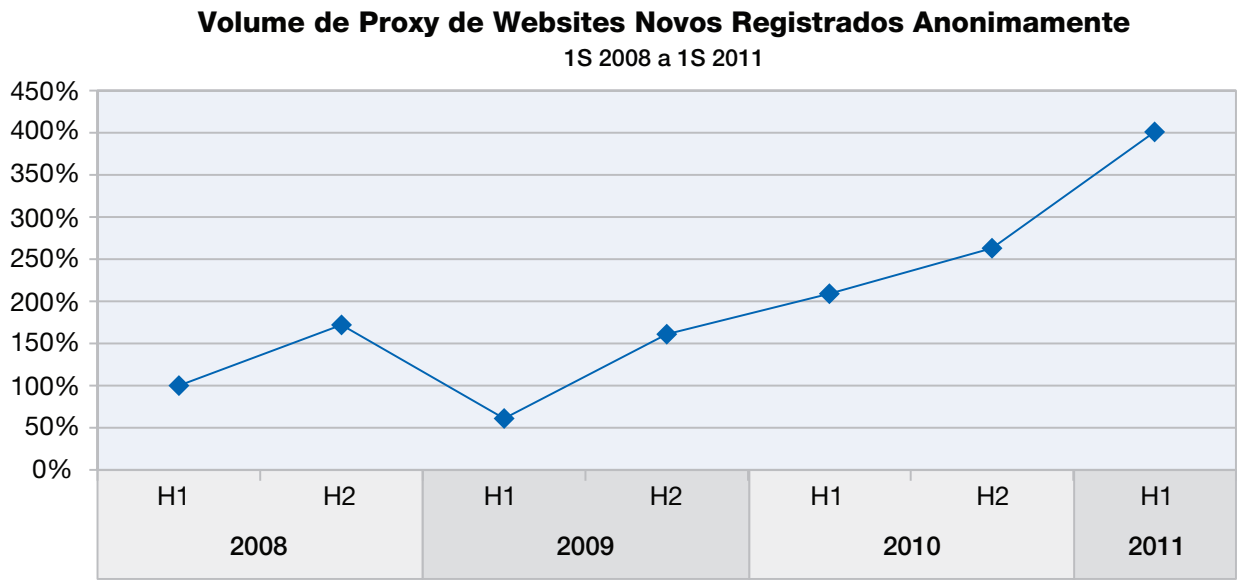



*Figura 11: Volume dos Mais Novos Sites de Proxys Anônimos Registrados – 1S 2008 a 1S 2011*

## Domínios de alto nível de proxys anônimos

A Figura 12 ilustra os domínios de alto nível (TLDs) dos mais recentes proxys anônimos registrados.

Em 2006, mais de 60% de todos os proxys anônimos mais recentemente registrados eram domínios .com, mas desde a metade de 2007, .info chegou ao topo no início de 2010 (enquanto .com ficou em 2º lugar na maior parte do tempo).

Mas porque o .info não está mais em 1º lugar? Parece ser um domínio de alto nível comprovado (TLD) para proxys anônimos por anos. A razão pode ser que .info, assim como .com, está ficando sem nomes. Portanto, a questão que surge é porque os proxys anônimos agora são fornecidos em domínios de alto nível .cc e .tk. Esses são os domínios das Ilhas Cocos (Keeling (.cc), um território australiano, e Tokelau (.tk), um território da Nova Zelândia. O domínio .cc é administrado pela VeriSign. Quase todos os sites de proxys anônimos .cc são registrados no domínio co.cc. Não há custos para registrar um domínio qualquercoisa.co.cc[11]. O mesmo é válido para .tk[12]. Portanto, é rápido e atrativo instalar novos proxys anônimos em .co.cc ou .tk

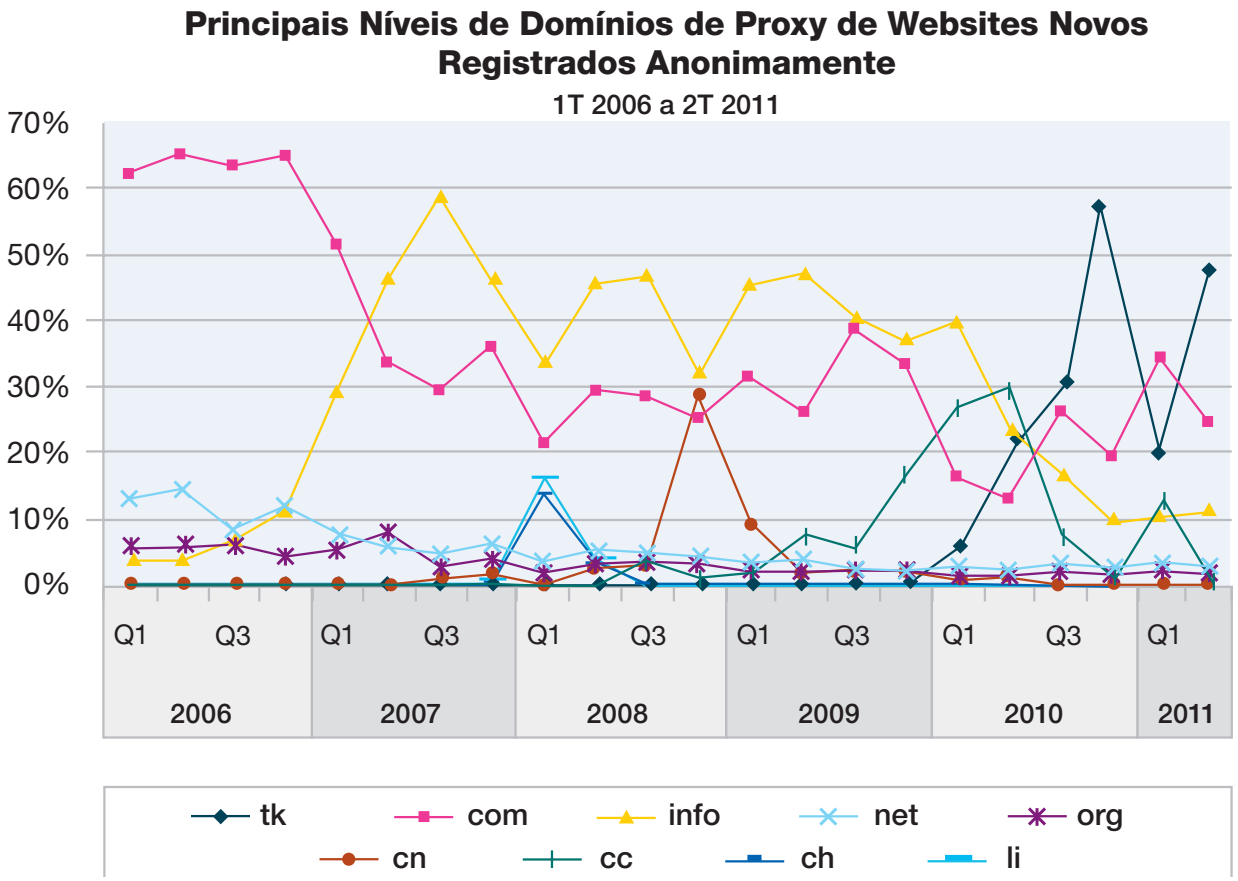



*Figura 12: Domínios de Alto Nível dos Mais Recentes Websites de Proxy Anônimo – 1T 2006 a 2T 2011*

11 http://www.co.cc/?lang=en
12 http://www.dot.tk/

**Tendências adicionais:**

- No início de 2008, os domínios de alto nível dos países vizinhos Suíça (.ch) e Liechtenstein (.li) juntos representavam quase 30% dos proxys anônimos recentemente registrados.
- No quarto trimestre de 2008, o domínio de alto nível da China (.cn) alcançou quase 30% dos proxys anônimos recentemente registrados.
- No final de 2009, .cc (Ilhas Cocos (Keeling)) começou a aumentar significativamente e até mesmo alcançar a posição de número 1 no segundo trimestre de 2010. Apesar disso, .cc ficou obsoleto no final de 2010 quase completamente, e teve um retorno rápido no primeiro trimestre de 2011.
- No segundo trimestre de 2010, outra nova estrela no céu dos proxys, .tk (Tokelau), alcançou quase 23% dos novos proxys anônimos. Ele dominou o resto do ano com quase 30 no terceiro trimestre e mais de 56% no quarto trimestre de 2010. No segundo trimestre de 2011, é o principal novamente com 46,5%.
- Durante o mesmo período de tempo, .info diminuiu drasticamente e caiu 10% pela primeira vez no final de 2010, recuperando apenas quase 12% no segundo trimestre de 2011.
- No primeiro trimestre de 2010, mesmo .com tendo caído significativamente para abaixo de 20% pela primeira vez, recuperar 26% no terceiro trimestre e 19% no quarto trimestre de 2010. No primeiro trimestre de 2011, ele dominou a lista pela primeira vez em quatro anos e terminou em segundo lugar no segundo trimestre de 2011.
- Ao observar os últimos 12 meses, .tk e .com estão claramente dominando o cenário.

Será interessante ver se .tk terá um destino similar ao .co.cc, sendo a estrela dos proxys anônimos por um ano e meio e depois cair na obscuridade.

Com relação ao .co.cc, há outra ação interessante: No início de julho de 2011, o Google anunciou que iria remover sites .co.cc do índice de pesquisa[13] para modificar o sistema de detecção de malware para identificar serviços de subdomínio que permitem que invasores registrem milhares de domínios. Alguém pensaria que tal sanção poderia ajudar a deter os proxys anônimos. Infelizmente, novos proxys anônimos são publicados de muitas outras formas incluindo listas de email e feeds do Twitter. Portanto, eles não precisam ser encontrados através dos mecanismos de pesquisa. Mesmo se não houvessem ações mais pesadas contra alguns domínios ou domínios de alto nível – talvez comparáveis às derrubadas de McColo ou Rustock (veja a **seção de volume de spam de tendência reversa**) – isso ajudaria apenas temporariamente. Parece possível que sempre haja alguns "registrar" soltos por aí que fornecem as portas abertas para proxys anônimos, porque o registro do domínio é uma questão que cada país lida de maneira diferente.

13 Consulte http://www.h-online.com/security/news/item/No-more-Googling-for-co-cc-domains-1274332.html.

## Websites maliciosos

Essa seção discute os países responsáveis por hospedar links maliciosos junto com os tipos de websites que geralmente têm link com esses websites maliciosos. Mais informações sobre websites maliciosos no contexto de exploração também podem ser encontradas na seção Esforço de exploração contra matrizes potenciais de recompensa.

### Localização geográfica dos links maliciosos da web

Os Estados Unidos continuam reinando como principais hospedeiros de links maliciosos. Mais de um terço de todos os links de malware estão hospedados nos EUA. O novo segundo lugar é agora a Romênia, hospedando 7,8%. A China era o principal há dois anos e meio, e agora está em terceiro lugar, com 7,2%. Isso é 1,4% a mais do que a França, conforme mostrado na Figura 13.

Os países de segundo nível também mudaram, mas essas mudanças estão abaixo de 1%.

### Bons websites com links ruins

Conforme será descrito mais tarde neste relatório, na página 58, discutiremos como o número total de vulnerabilidades está caindo. Independentemente disso, os invasores ainda se concentram no uso do bom nome de websites confiáveis para diminuir a guarda dos usuários finais e tentar ofuscar suas tentativas de tecnologias de proteção. O uso de conteúdo da web malicioso não é diferente. A análise seguinte fornece uma visão sobre os tipos de websites que mais frequentemente contém links para sites conhecidos e maliciosos.

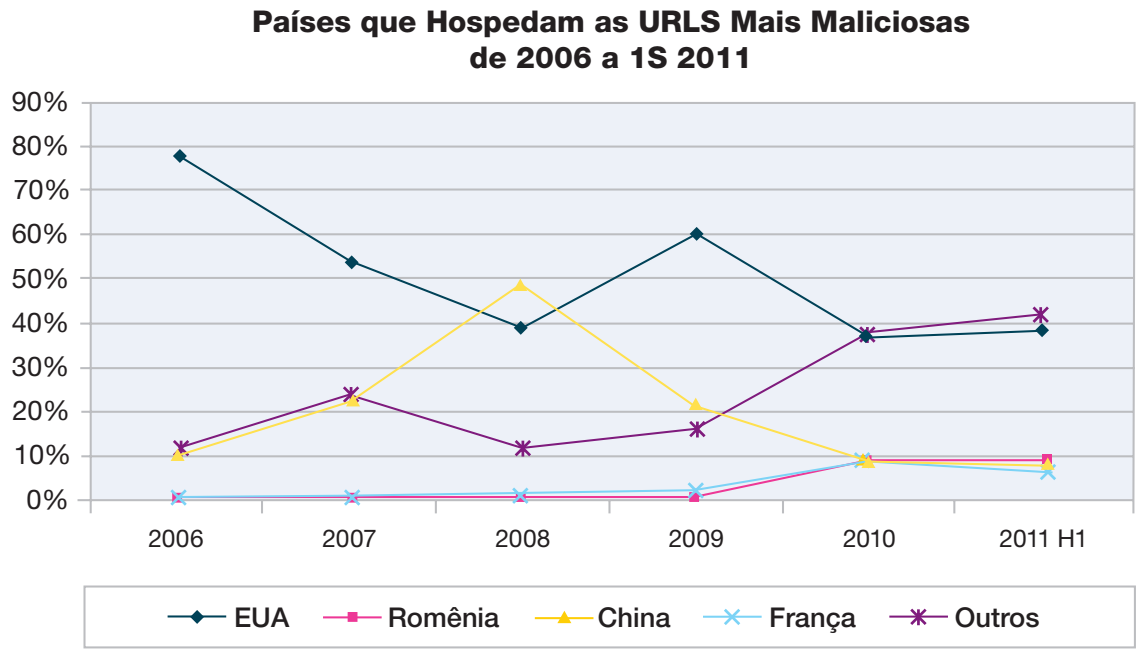



*Figura 13: Países que Hospedam as URLS Mais Maliciosas – 2006 a 1S 2011*

Algumas das categorias principais não são surpreendentes. Por exemplo, alguém pode esperar pornografia e apostas no topo da lista. Juntos eles hospedam mais de 40% de todos os links maliciosos. Porém, os candidatos de segundo nível caem na categoria mais "confiável".

Blogs, murais de notícias, websites pessoais, mecanismos de pesquisa, educação, sites de compras, revistas on-line e sites de notícias caem nessa categoria de segundo nível. A maioria desses websites permitem que os usuários façam upload de conteúdo ou projetem seu próprio site, como conteúdo pessoal em um website de uma universidade ou comentários sobre a compra em um site de compras. Em outras palavras, é improvável que esses tipos de site estejam hospedando intencionalmente os links maliciosos. A distribuição é provavelmente mais representativa dos tipos de websites que os invasores gostam de frequentar na esperança de encontrar uma violação de loop (como uma vulnerabilidade ou uma área que permite conteúdo fornecido pelo usuário) no qual eles podem incorporar esses links maliciosos na esperança de comprometer uma vítima que não suspeita de nada.

A Figura 14 lista os tipos mais comuns de websites que hospedam pelo menos um link que redireciona para um website malicioso conhecido.

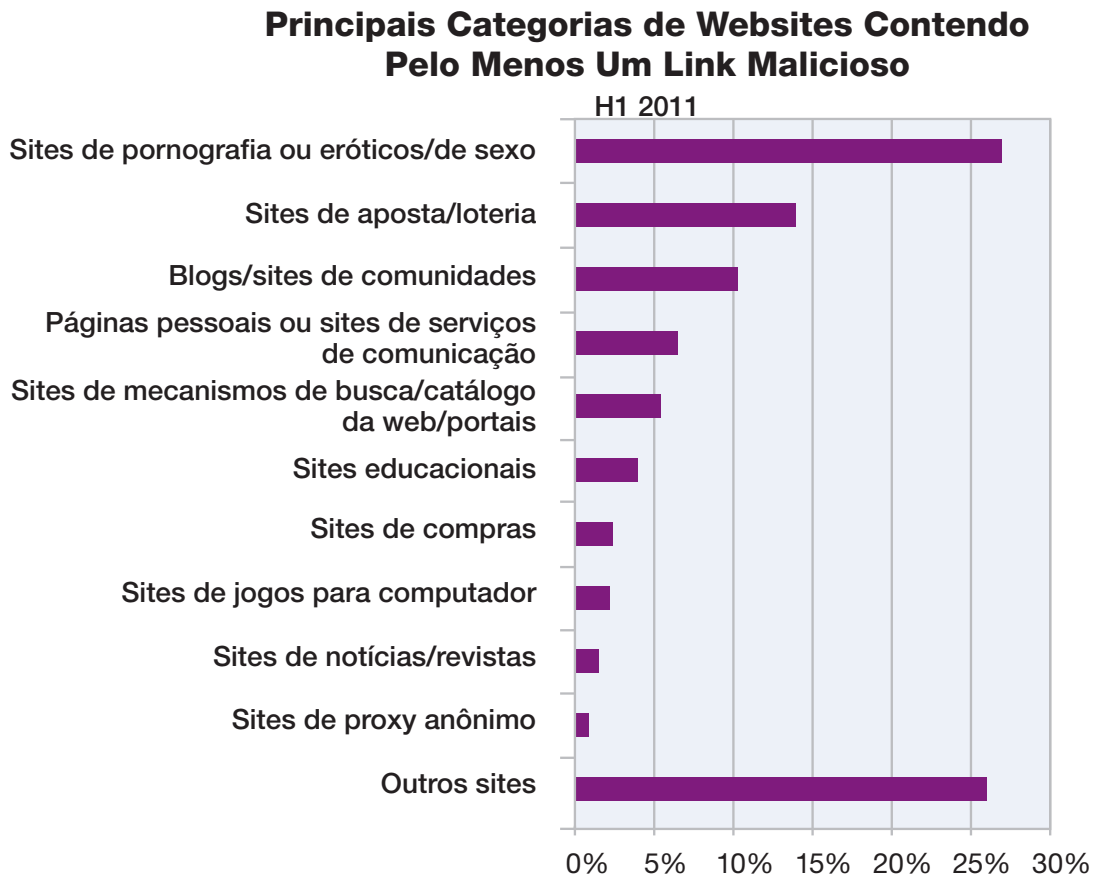



*Figura 14: Principais Categorias de Website Contendo pelo menos um Link Malicioso – 1S 2011*

A Figura 15 mostra a história dos principais jogadores.

Ao olhar para trás nos últimos dois anos e meio, algumas tendências interessantes aparecem.

- Os websites "ruins" profissionalmente como pornografia e apostas, agora dominam a cena para malware distribuído sistematicamente
- A pornografia está no topo e estabilizou-se em torno dos 25%.
- A aposta é a única categoria com um aumento significativo ano após ano. Contra um cenário de 0,6% da população adulta que possui problemas com apostas [14], esses sites são um alvo popular para distribuidores de malware.
- Blogs e murais de notícias estão praticamente no mesmo nível desde um ano atrás, em aproximadamente 10%.
- Páginas pessoais e mecanismos de pesquisa, catálogos da web e portais – os sites clássicos da Web 1.0 – perderam lugar significativamente. Uma razão pode ser que as páginas pessoais estão fora de moda em relação aos aplicativos da Web 2.0 como perfis em redes sociais ou profissionais.

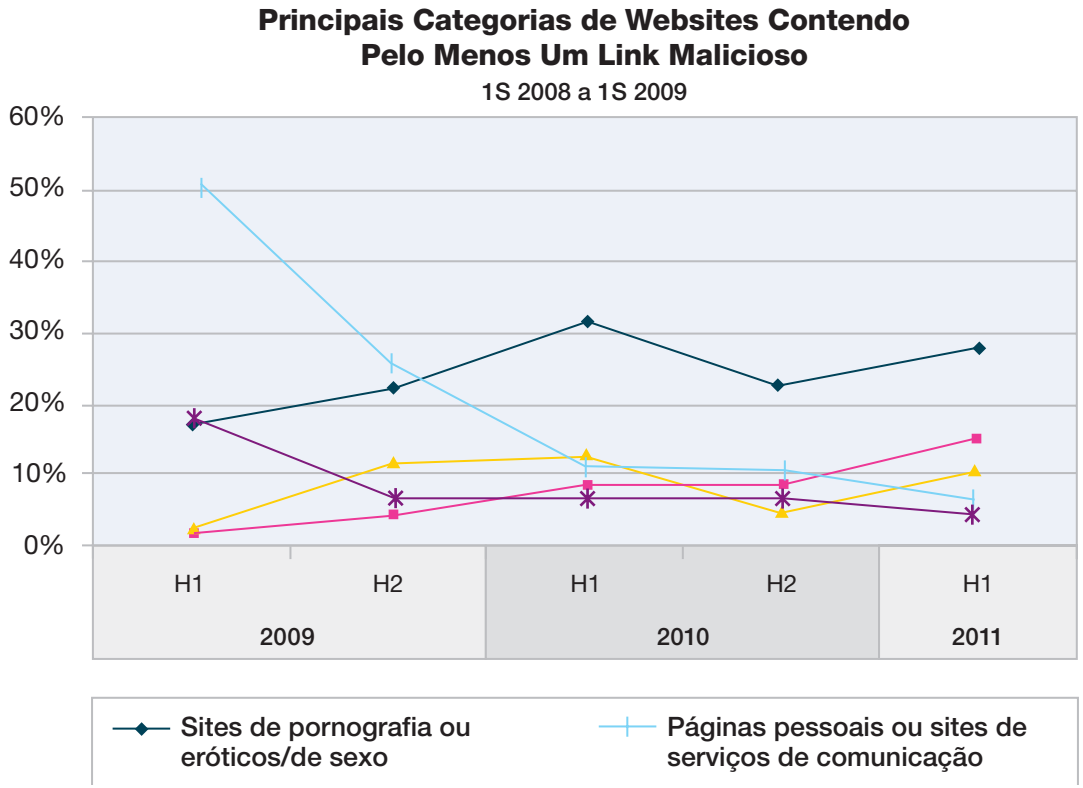



*Figura 15: Principais Categorias de Website Contendo pelo menos um Link Malicioso – 1S 2009 a 1S 2011*

14 Consulte http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence

## Tendência de reversão no volume de spam

O banco de dados de spam da IBM e de filtro de URL fornece uma visão global geral de spam e ataques phishing. Com milhões de endereços de emails sendo ativamente monitorados, a equipe de conteúdo identificou inúmeros avanços nas tecnologias de spam e phishing que os invasores utilizam.

Atualmente, o banco de dados do filtro de spam contém mais de 40 milhões de assinaturas relevantes de spam. Cada pedacinho de spam é quebrado em diversas partes lógicas (frases, parágrafos, etc.). Uma única assinatura 128 bits é computada para cada parte e para milhões de URLs de spam. Cada dia, há aproximadamente um milhão de assinaturas novas, atualizadas ou excluídas para o banco de dados de filtragem de spam.

Esta seção abrange os seguintes tópicos:

- Volume de spam e derrubada dos botnets
- Domínios comuns de alto nível em spam de URL
- Spam – tendências[15] do país de origem
- Phishing de email
- Perspectivas de futuro sobre spam

## Volume de spam e derrubada dos botnets

Após anos de crescimento significativo até meados de 2010 com apenas uma única retirada no final de 2008, vimos um declínio nos volumes de spam nos últimos 12 meses.

Uma história interessante discutida em círculos de spam desde o final de dezembro de 2010 é a "calma em atividade" no final do ano. Em uma postagem de janeiro do **blog Frequency-X** especulamos o porquê da diminuição repentina desses volumes. Os spammers entraram de férias? Os negócios "secaram"? Foi a primeira derrubada do botnet Rustock? Nós tinhamos mais perguntas do que respostas no mês de janeiro, mas desde então algumas notícias interessantes surgiram.

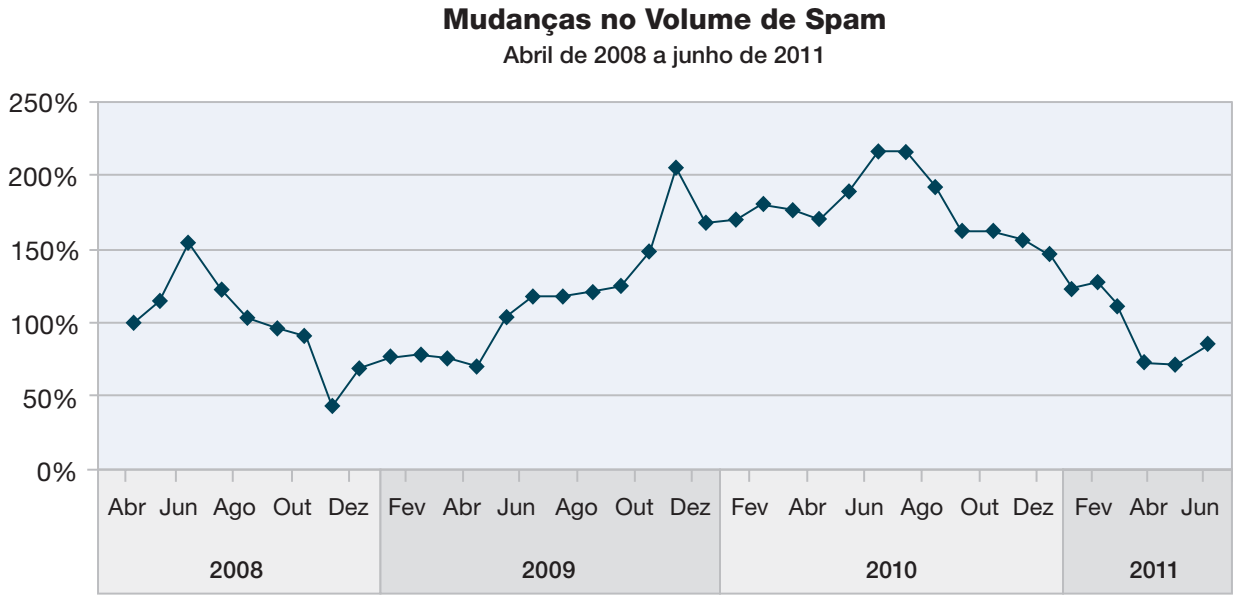



*Figura 16: Mudanças no Volume de Spam – abril 2008 a junho 2011*

15 As estatísticas deste relatório sobre spam, phishing e URLs usam o banco de dados IP-para-Países fornecido pelo WebHosting.Info (http://www.webhosting.info), disponível em http://ip-to-country.webhosting.info. A distribuição geográfica foi determinada com a solicitação de endereços de IP dos hosts (no caso de distribuição de conteúdo) ou do servidor que envia emails (nno caso de spam e phishing) para o Banco de Dados IP-para-Países.

Vamos observar mais de perto os últimos seis meses dominados por duas derrubadas Rustock em dezembro de 2010 e março de 2011.

- **Primeira derrubada Rustock** de 25 de dezembro de 2010 até 9 de janeiro de 2011: No início de janeiro, diversas agências de notícias, incluindo um **artigo do New York Times** começaram a relatar o declínio no spam enquanto o primeiro Rustock foi derrubado, e também relataram que os negócios principais na Rússia estavam "secando".

- **Segunda derrubada Rustock** desde 16 de março de 2011: Em março, ficou claro quando a Microsoft e o US Marshals foram capazes de derrubar os recursos de comando e controle do botnet, conforme relatado no **blog do site da Microsoft**. A diminuição dos volumes de spam foi pega pelas armadilhas de spam da IBM e pode ser vista na Figura 17.

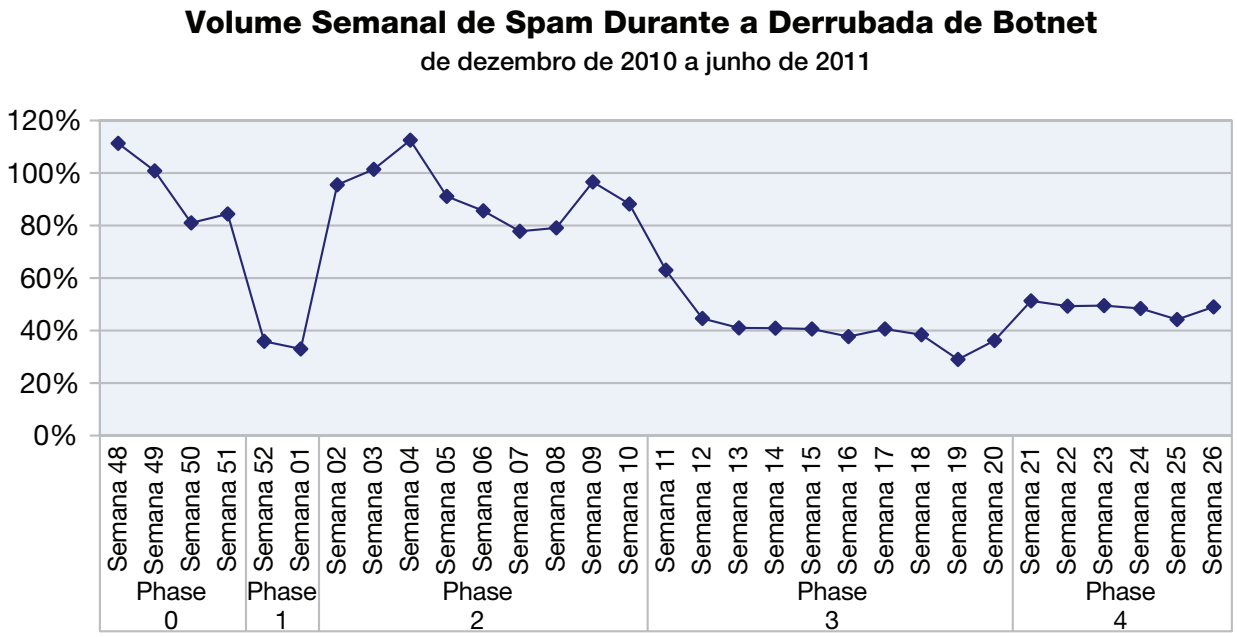



*Figura 17: Volume de Spam Semanal Durante Derrubada do Botnet – dezembro 2010 a junho 2011*

Com base nisso, pode-se derivar diversas mudanças com relação a outros aspectos do spam enviado até metade de 2011. Para destacar essas mudanças, definimos diversas fases:

- **Fase 0 – Situação inicial:**
  Início de dezembro de 2010
- **Fase 1 – Primeira derrubada do Rustock:**
  De 25 de dezembro de 2010 a 9 de janeiro de 2011
- **Fase 2 – Entre as derrubadas do Rustock:**
  De 10 de janeiro de 2011 a 15 de março de 2011
- **Fase 3 – Após a segunda derrubada do Rustock:**
  De 16 de março de 2011 a 18 de maio de 2011
- **Fase 4 – Primeira recuperação do volume de spam:**
  Desde 19 de maio de 2011

Primeiro olhamos para alguns dos principais jogadores com relação ao país de origem de spam. Índia, Indonésia e EUA eram os países que haviam mostrado maiores mudanças de fase a fase.

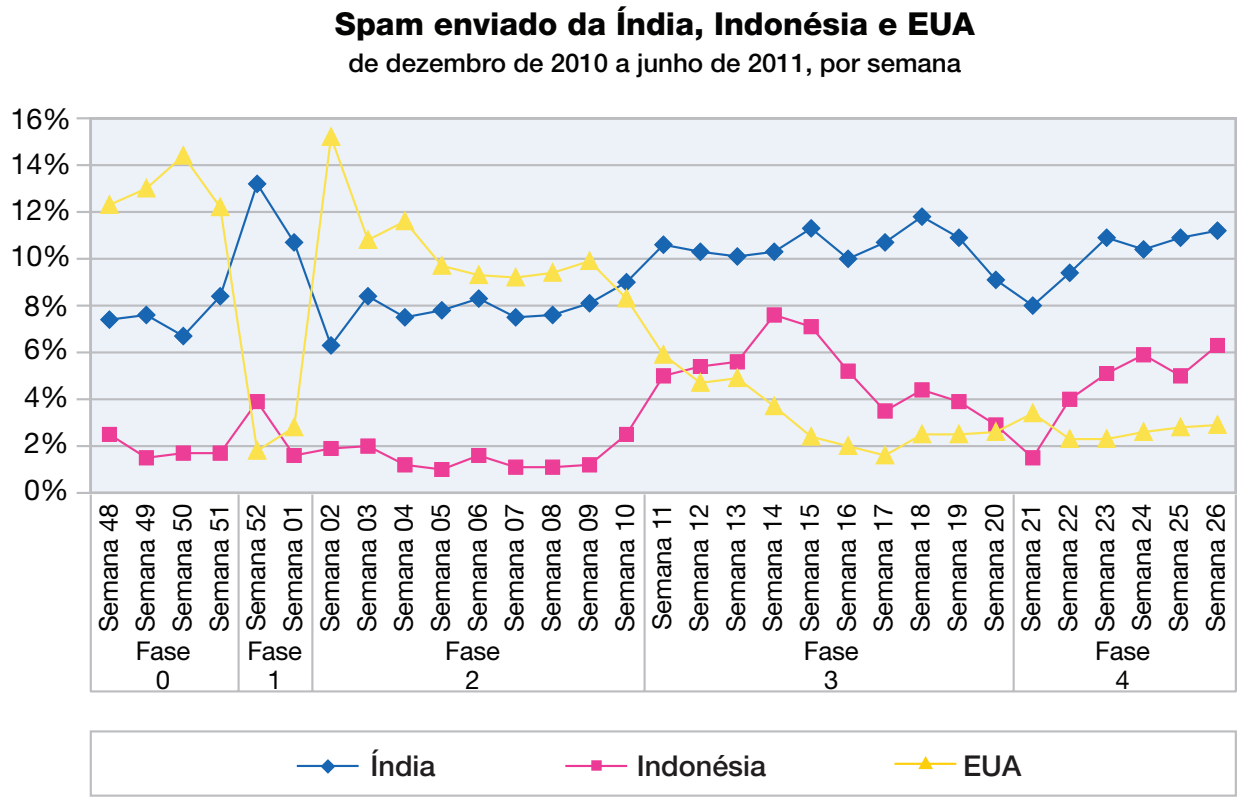



*Figura 18: Spam enviado a partir de Índia, Indonésia, EUA – dezembro 2010 a junho 2011, por semana*

Quando Rustock foi derrubado, o volume de spam enviado dos EUA ficou também, na maioria dos casos, abaixo de 3%. Ao mesmo tempo, a porcentagem de spam enviado da Índia aumentou para mais de 10% e o spam enviado da Indonésia aumentou para 4%. Quando o Rustock estava ativo (fase zero e dois), significativamente mais spam – mais de 9% na maioria dos casos – foi enviado dos Estados Unidos enquanto a Índia diminuiu para 8% e a Indonésia reduziu para 2%. Portanto, Rustock estava amplamente em uso nos computadores americanos, mas muito menos na Índia e na Indonésia. Na fase quatro, quando o volume de spam aumentou novamente, os níveis de spam enviados de computadores dos EUA não foram recuperados como antes. Parece que os novos clientes botnet são mais recrutados de fora dos Estados Unidos do que antes. Mas por que as infecções botnet evitam computadores dos EUA? Possível resposta: É muito mais fácil infectar computadores em outros países porque:

- As instalações Não Windows 7 em outros países são mais suscetíveis[16].
- As últimas duas derrubadas (McColo em novembro de 2008 e Rustock em março de 2011) foram direcionadas por organizações ou empresas com base nos EUA. Talvez os spammers estejam evitando essa área e se concentrando no restante do mundo.

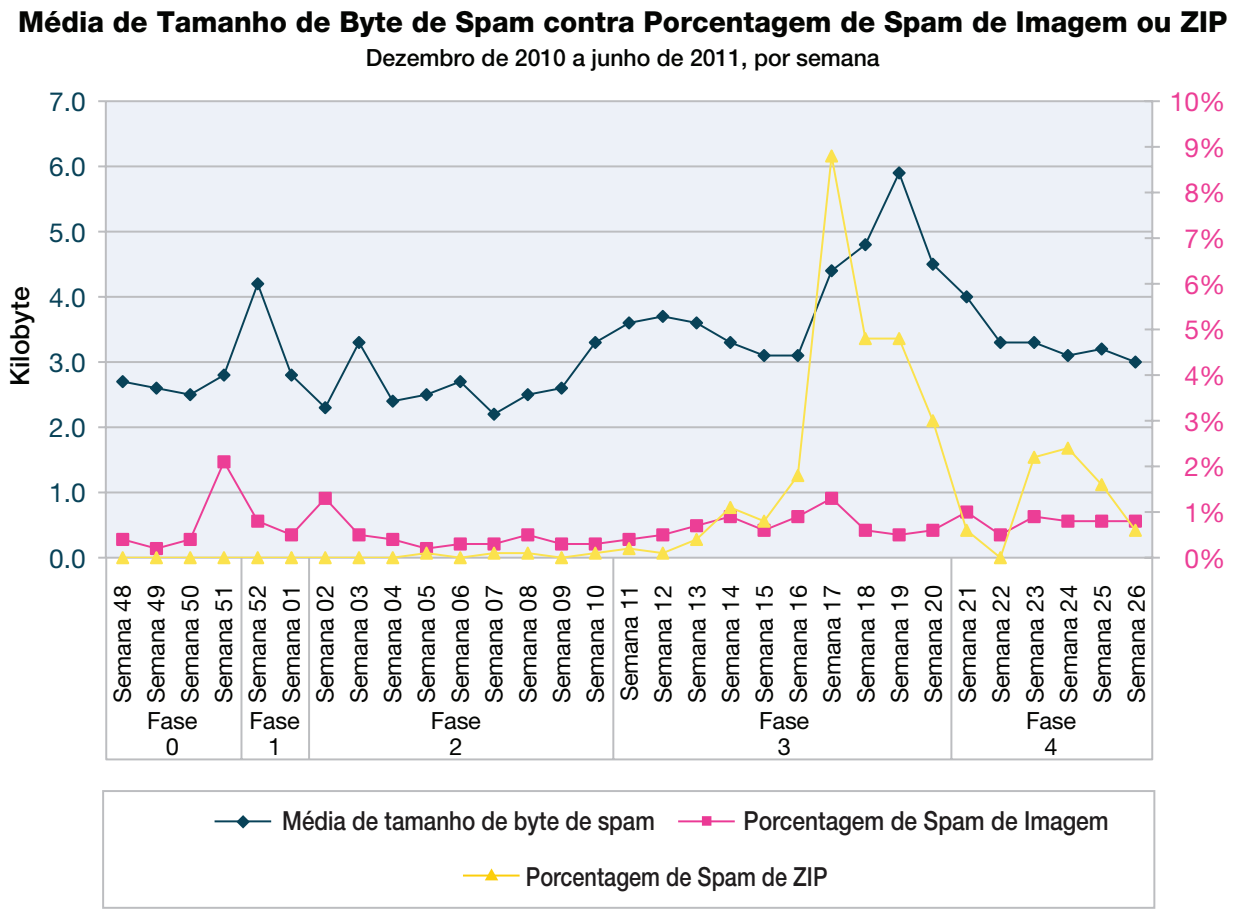



*Figura 19: Tamanho de byte médio de spam contra porcentagem de imagem e spam ZIP – dezembro 2010 a junho 2011, por semana*

16 De acordo com o StatCounter (http://gs.statcounter.com/) em junho de 2011, aproximadamente 35% de todos os computadores nos EUA estavam executando Windows 7, e apenas 29%, Windows XP. Na Índia, verificamos apenas 28% de Windows 7 e 64% de Windows XP. Isso é ainda mais significativona Indonésia onde temos apenas 21% de Windows 7 e 75% de Windows XP.

As características de conteúdo do spam são outra forma de analisar as mudanças.

- **Tamanho de byte médio de spam:**Quando o volume de spam aumenta e o Rustock está ativo (fases zero e dois) o tamanho de byte médio de spam é menor, geralmente menor do que 3 KB. Quando o volume de spam diminui (fase um e três) o tamanho de byte médio de spam é mais alto, maior do que 3 KB na maioria dos casos. O spam enviado por Rustock era pequeno em tamanho. Quando as ameaças de spam por anexo ZIP começaram em abril, o tamanho do spam aumentou significativamente conforme o esperado.
- **Spam baseado em imagem:** Como nos anos anteriores, esse tipo de spam não tem um papel significativo. Na maioria dos casos o volume é menor do que 1%.
- **Spam ZIP:** No primeiro trimestre, spam com anexos ZIP eram raramente vistos. Porém, desde meados de abril, temos visto diversas ameaças contábeis de 2% a 8% do volume de spam (medido semanalmente).

Ao observar os anexos ZIP de spam durante o início de maio desse ano, mais de 90% do spam continha o **TrojanDownloader:Win32/Chepvil.K**. Como um downloader Trojan, ele faz o download de malware, ao invés de ter recursos maliciosos intrínsecos. E, pode fazer o download não apenas de uma parte de malware, mas de diversos aplicativos malware com diferentes intenções.

Para convencer os usuários a abrirem o anexo ZIP, algumas variantes típicas são utilizadas.

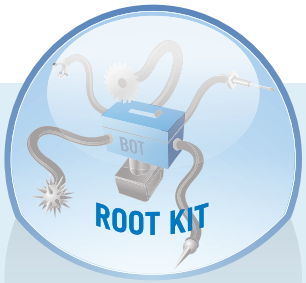
- Uma ordem falsa de confirmação incluindo a mensagem de que o cartão de crédito do usuário será taxado em mais de US$ 100 e de que o usuário pode encontrar detalhes no arquivo em anexo.
- Um email afirmando que o endereço IP do usuário esteve logado em diversos websites ilegais. O “emissário falso”, o FBI, solicita que o usuário responda perguntas em anexo.

Em outra ameaça durante o mês de maio, os emails continham o **TrojanDownloader:Win32/Ufraie.A**. Neste caso, os usuários foram convencidos a abrir um anexo ZIP anunciando que continha uma foto de alguém nu.

A derrubada do Rustock paralisou alguns dos maiores "canais de venda" dos spammers. A Figura 19 sugere que essas ameaças de spam em anexo ZIP são uma resposta a isso, porque, rapidamente após enviar essas ameaças de spam ZIP, o volume de spam começou a crescer (fase quatro), talvez com o envolvimento de novos clientes botnet que foram infectados dias antes do envio dos anexos ZIP. Porém, os níveis ainda estão 50% abaixo dos níveis do quarto trimestre do ano passado.

Pouco tempo antes da publicação deste relatório, verificamos um aumento significativo no volume de spam. O aumento foi iniciado por níveis mais altos de spam por anexo em ZIP. Em meados de setembro de 2011, o volume de spam alcançou 80% dos níveis que havia alcançado nove meses antes.

Estaremos fornecendo mais detalhes sobre a nova atividade de spam no **blog Frequency-X**.




## Há uma continuação da tendência das derrubadas de botnet em 2011?

No **Relatório de Risco e Tendência do IBM X-Force 2010** o grupo de Serviços de Segurança Administrado relatado em uma tendência ascendente na atividade de botnet Trojan durante 2010. Este crescimento foi significante pois, apesar dos crescentes esforços coordenados para fechar a atividade botnet (como visto com os botnets Mariposa e Bredolab), a ameaça pareceu ter ganhado força viva no momento.

No mesmo relatório, também discutimos os esforços da Microsoft para reprimir os botnets. Especificamente, a "Operação B49" da Microsoft, que derrubou o botnet Waledac no final de fevereiro de 2010.

Em 2011, esta tendência de tirar os operadores de botnet continua e questionamos, "A Segurança está avançando sobre as derrubadas de Botnet?" Dois outros exemplos surgiram no início de 2011.


**16 de março de 2011 – Botnet Rustock**
O botnet Rustock foi um dos mais problemáticos dos últimos anos. Era dedicado a enviar spam. Uma máquina infectada pelo Rustock enviava uma média de mais de 190 mensagens de spams. De acordo com o relatado, havia entre 150 mil e 2.400.000 de computadores infectados com Rustock. Em 16 de março de 2011, o botnet foi derrubado através de um esforço coordenado por distribuidores, pesquisadores e cumprimento da lei. Para mais detalhes consultar http://en.wikipedia.org/wiki/Rustock

**13 de abril de 2011 – Botnet Coreflood**
Desde o início dos anos 2000, o botnet CoreFlood tem sido utilizado para comprometer milhões de sistemas nos Estados Unidos e no mundo. Em um esforço para derrubar o botnet, o FBI executou a primeira operação do tipo que envolveu a criação de um comando personalizado e servidor de controle que emitia um comando de parada para o malware em execução no PC infectado. Além disso, a Microsoft adicionou à remoção do CoreFlood à sua Ferramenta de Remoção de Malware e ajudou na limpeza dos sistemas infectados. Como resultado desta violação, alegadamente, a atividade do botnet CoreFlood foi reduzida em 90% nos Estados Unidos e 75% no mundo todo.

**Referências 2011:**
1. Microsoft: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/04/13/fbi-and-doj-take-on-the-coreflood-botnet.aspx
2. US DOJ: http://www.justice.gov/opa/pr/2011/April/11-crm-466.html
3. http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/04/07/initial-revelations-and-results-of-the-rustock-takedown.aspx
4. http://www.computerworld.com/s/article/9216199/Feds_to_remotely_uninstall_Coreflood_bot_from_some_PCs
5. http://www.darkreading.com/database-security/167901020/security/client-security/229401635/coreflood-botnet-an-attractive-target-for-takedown-for-many-reasons.html

**Referências 2010:**
- Encerramento generalizado do botnet Mariposa – http://www.net-security.org/secworld.php?id=8962
- Encerramento do botnet Bredolab – http://nakedsecurity.sophos.com/2010/10/26/bredolab-botnet-shut/
- Quebrando os Botnets – http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx

## Domínios comuns de alto nível em spam de URL

### Código de país internacionalizado de alto nível domínios em crescimento

A Tabela 2 mostra os cinco domínios de alto nível (TLDs) mais frequentemente utilizados em spam por mês.

Semelhante a 2010, o primeiro semestre de 2011 foi dominado por .ru, alcançando a posição um ou dois a cada mês. Em março, o novato .me[17] chegou entre as primeiras cinco posições, causando um uso generalizado de serviço de publicidade zrink.me e alguns serviços de encurtamento de URL, tais como ino.me, shortn.me e widg.me.

Em abril deste ano, até a Rússia apareceu duas vezes, uma vez com seu domínio tradicional de alto nível .ru e uma segunda vez com seu domínio de alto nível de código de país internacionalizado .рф[18]. Este domínio de alto nível apareceu no final de 2010, e em menos de seis meses alcançou as primeiras cinco posições. Desde março de 2011, ele ficou entre as primeiras 15 posições, como mostra a Figura 20.

| Classificação | Janeiro 2011 | Fevereiro 2011 | Março 2011 | Abril 2011 | Maio 2011 | Junho 2011 |
|---|---|---|---|---|---|---|
| 1. | ru (Rússia) | com | com | ru (Rússia) | ru (Rússia) | ru (Rússia) |
| 2. | com | ru (Rússia) | ru (Rússia) | com | com | com |
| 3. | uk (Reino Unido) | net | me (Montenegro) | ua (Ucrânia) | net | net |
| 4. | net | nl (Holanda) | us (EUA) | рф (Rússia) | info | info |
| 5. | info | info | net | net | cl (Chile) | cl (Chile) |

*Tabela 2: Domínios de alto nível mais comuns com conteúdo real de spam, 1S 2011*

17 .me é o Domínio de Alto Nível de Montenegro que fazia parte da antiga Iugoslávia.
18 "**рф**" as letras rf estão em linguagem Cirílica e significa "Federação Russa".

Por causa do uso generalizado deste novo domínio de alto nível internacionalizado por spammers, vale a pena analisar mais detalhadamente ***como*** os spammers utilizam este domínio. Para este propósito, a Figura 21 mostra quanto tempo os spammers utilizam um domínio.

O mais tradicional dos domínios de spam .ru – quase 43% – são utilizados por mesmo de 24 horas. Apenas 12% são utilizado por um período maior que um mês. Em contraste, menos de um terço dos domínios de spam .рф são utilizados por apenas 24 horas ou menos (uma porcentagem significativamente inferior para os domínios clássicos .ru), mas também 32% dos domínios são utilizados por 30 dias ou mais (o que é uma porcentagem significativamente maior para os domínios clássicos .ru). Isso traz algumas conclusões interessantes:

- Os spammers utilizam imediatamente esta nova alternativa de domínio de alto nível.
- Um domínio internacionalizado é utilizado por tanto tempo quanto um domínio tradicional .ru. Pode ser por que os spammers esperam que estas URLs não sejam reconhecidos por alguns filtros de spam. Portanto, eles não precisam alterar com frequência as URLs.

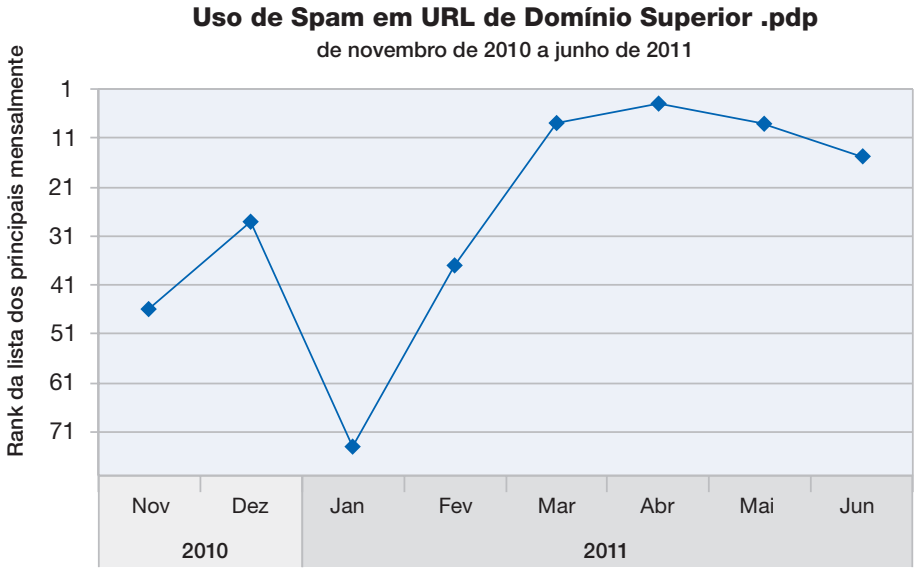



*Figura 20: Utilização de URL de Spam dos domínios de alto nível .рф – novembro de 2010 até junho de 2011*

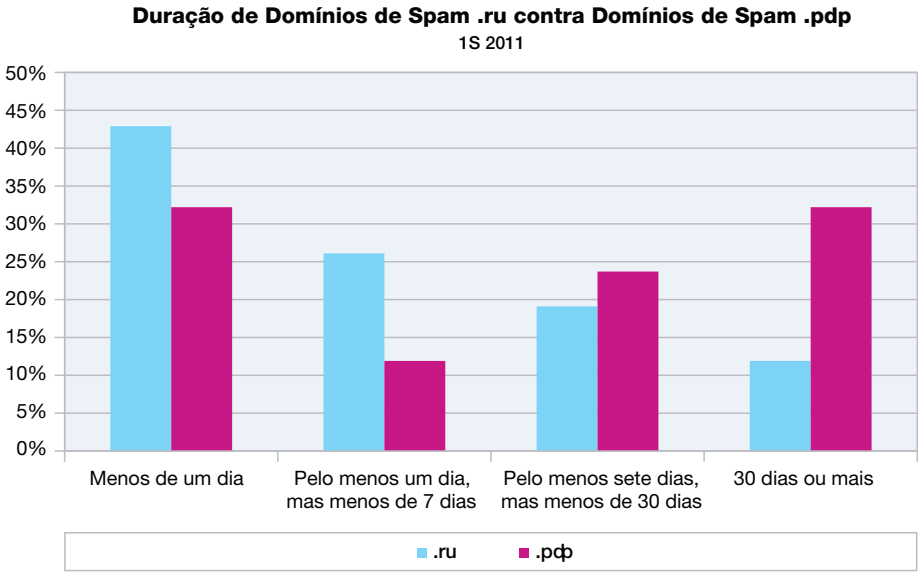



*Figura 21: A vida útil do Domínio de Spam .ru versus Domínios de Spam .рф – 1S 2011*

## Spam – tendências de país de origem[19]

Ao olhar para os países que enviam a maioria dos spams nos últimos 30 meses, algumas tendências interessantes de longa data tornam-se aparentes.

- Há dois anos e meio, o Brasil e os Estados Unidos dominavam o mercado.
- A Índia tem mostrado um crescimento contínuo e agora domina o cenário com grande margem, enviando mais de 10% de todos os spams.
- Os Estados Unidos possuíam a primeira posição em cada trimestre de 2010 e agora está em último, enviando menos de 3% do total de spams.
- O Vietnã era um grande fornecedor de spam em 2009, diminuiu significativamente no primeiro trimestre de 2011, mas se recuperou um pouco no segundo trimestre.
- O Brasil reduziu à metade sua porcentagem nos últimos 18 meses.
- A Indonésia, praticamente um novato, tem mostrado um crescimento contínuo por dois anos e meio e agora é responsável por 5% dos spams.

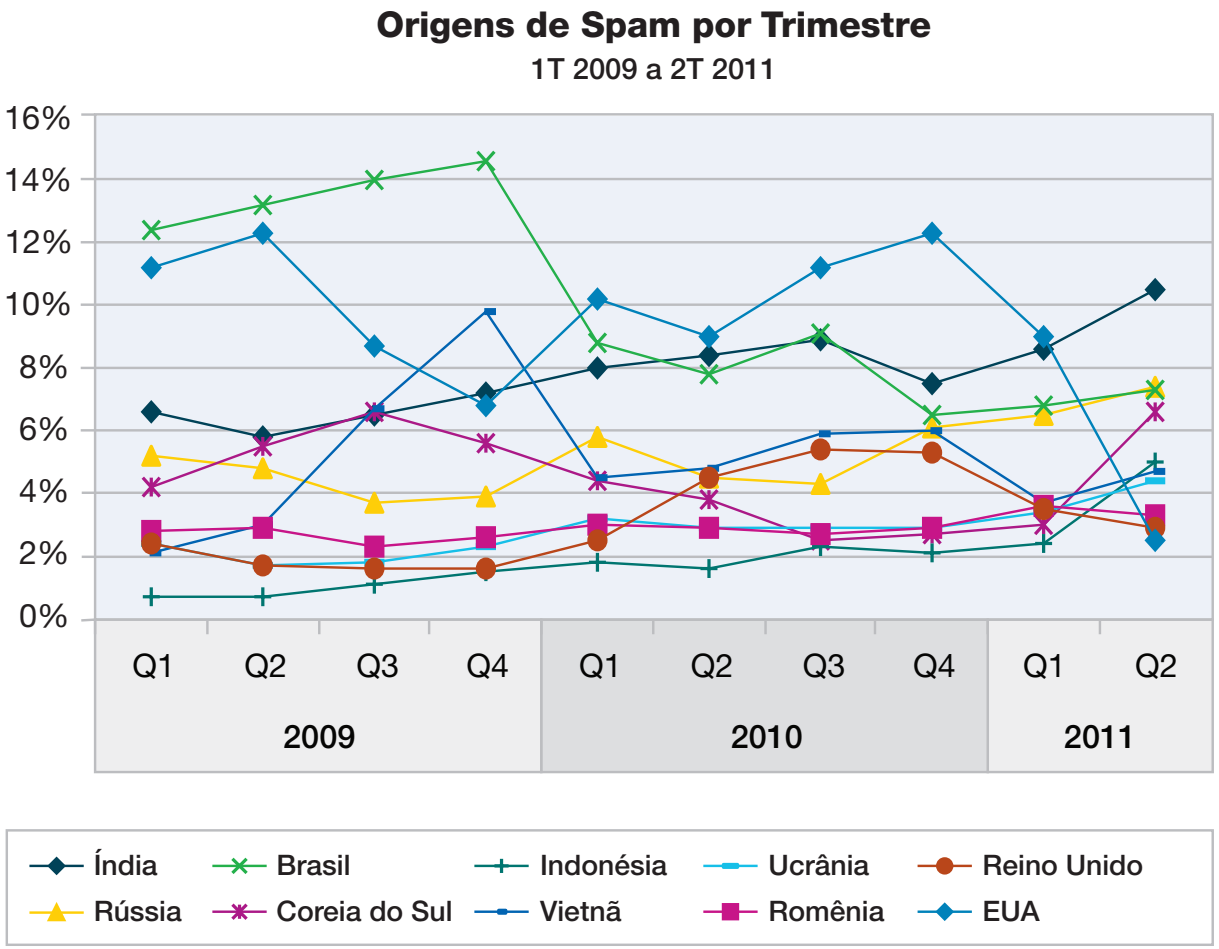



*Figura 22: Origens de Spam por Trimestre – T1 2009 até T2 2011*

19 O país de origem indica o local do servidor que enviou o email de spam. O X-Force acredita que a maioria dos emails de spam é enviada por redes de bot. Desde que os bots puderam ser controlados de qualquer lugar, a nacionalidade dos reais invasores por trás de um email de spam pode não ser a mesma de onde o spam foi originado.

## Phishing de email

No primeiro semestre de 2011, spammers deram adeus ao tradicional phishing de email. Ao olhar a porcentagem de spam phishing semanalmente, temos medido menos de 0,01% para cada mês.

A Figura 23 reflete a redução significante do tradicional phishing de email, particularmente em dois anos.

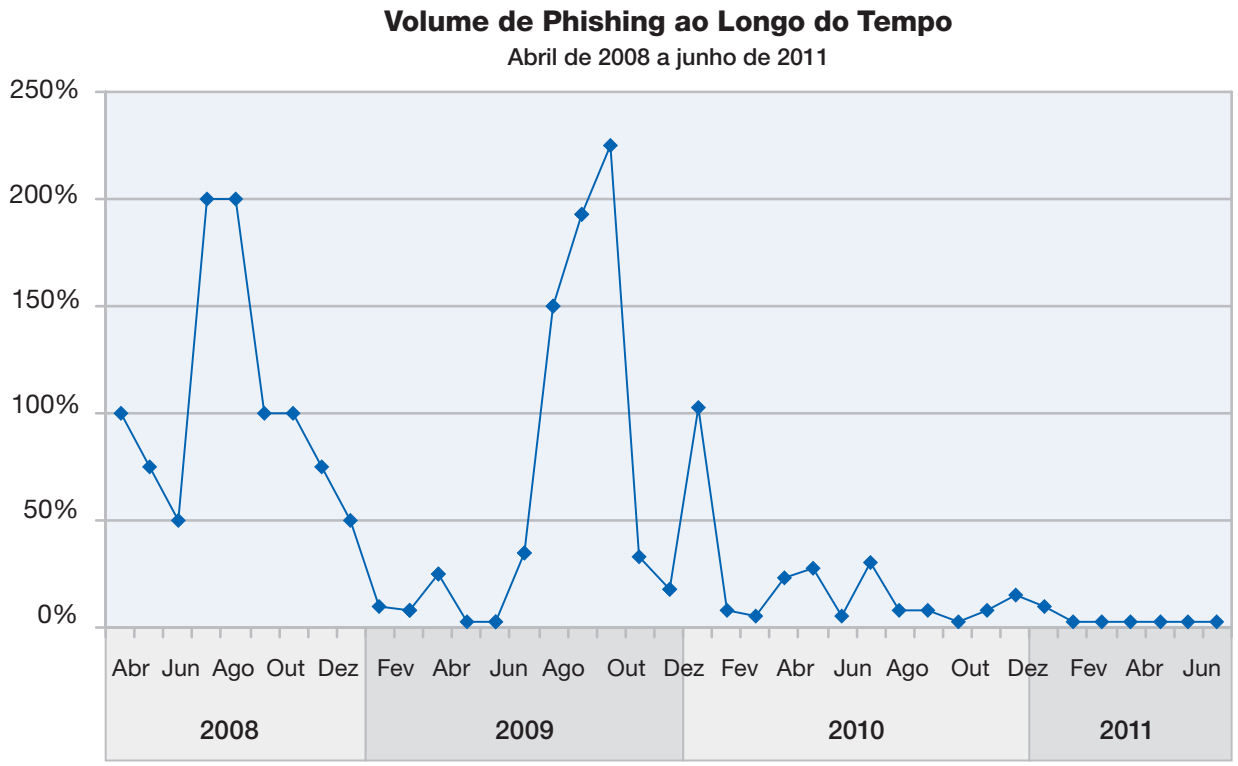



*Figura 23: Volume de Phishing ao Longo do Tempo – abril de 2008 até junho de 2011*

O momento em que observamos as grandes ameaças de phishing de email atraindo as pessoas para sites bancários falsos com um link em um email com aparência mais ou menos legítimas, parece ter passado. O mapa a seguir mostra de quais países os emails de phishing restantes são enviados[20].

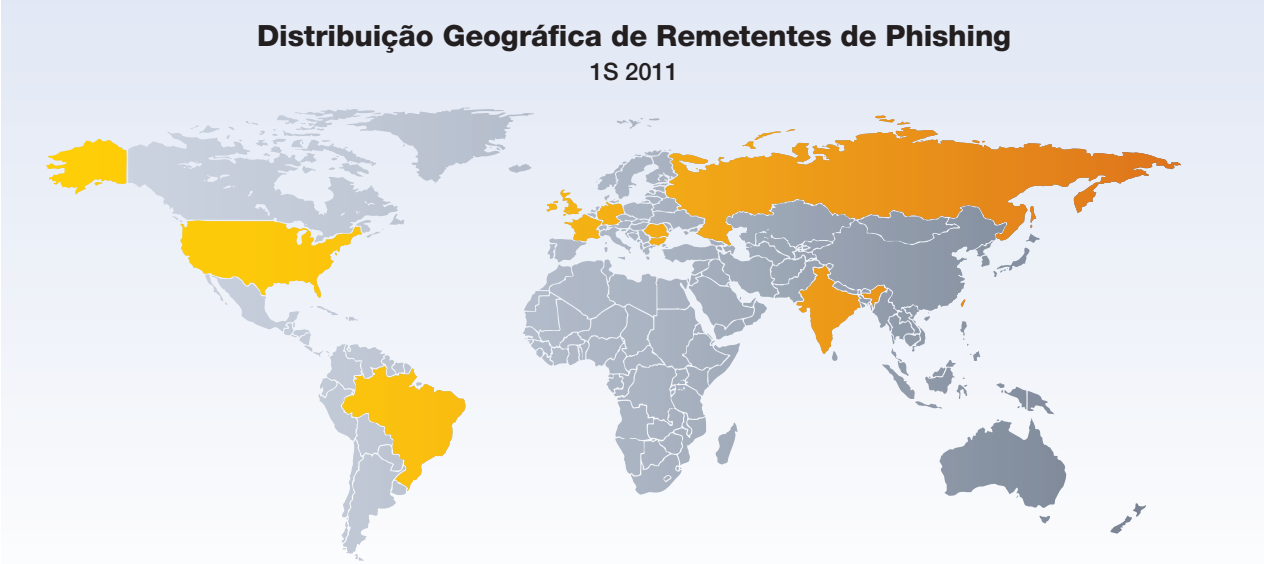



*Figura 24: Distribuição Geográfica de Remetentes de Phishing – 1S 2011*

| País | % de Phishing | País | % de Phishing |
|---|---|---|---|
| USA | 41.5 % | Índia | 3.0 % |
| Reino Unido | 6.8 % | França: | 2.9 % |
| Brasil | 3.5 % | Taiwan | 2.7 % |
| Bulgaria | 3.2 % | Alemanha | 2.7 % |
| Romênia | 3.2 % | Rússia | 2.6 % |

*Tabela 3: Distribuição Geográfica de Remetentes de Phishing – 1S 2011*

20 O país de origem indica o local do servidor que enviou o email de spam. O X-Force acredita que a maioria dos emails de phishing é enviada por redes de bot. Desde que os bots puderam ser controlados de qualquer lugar, a nacionalidade dos reais invasores por trás de um email de phishing pode não ser a mesma de onde o phishing foi originado.

O phishing de email ainda tem como alvo as instituições financeiras, que representam mais de 80% de todos os emails de phishing no primeiro trimestre e 31,1% no segundo trimestre. No segundo trimestre, o pagamento online atingiu a mais alta posição pela primeira vez em 31,7%. As lojas online chegaram a quase 19%, e os leilões a 13,5%.

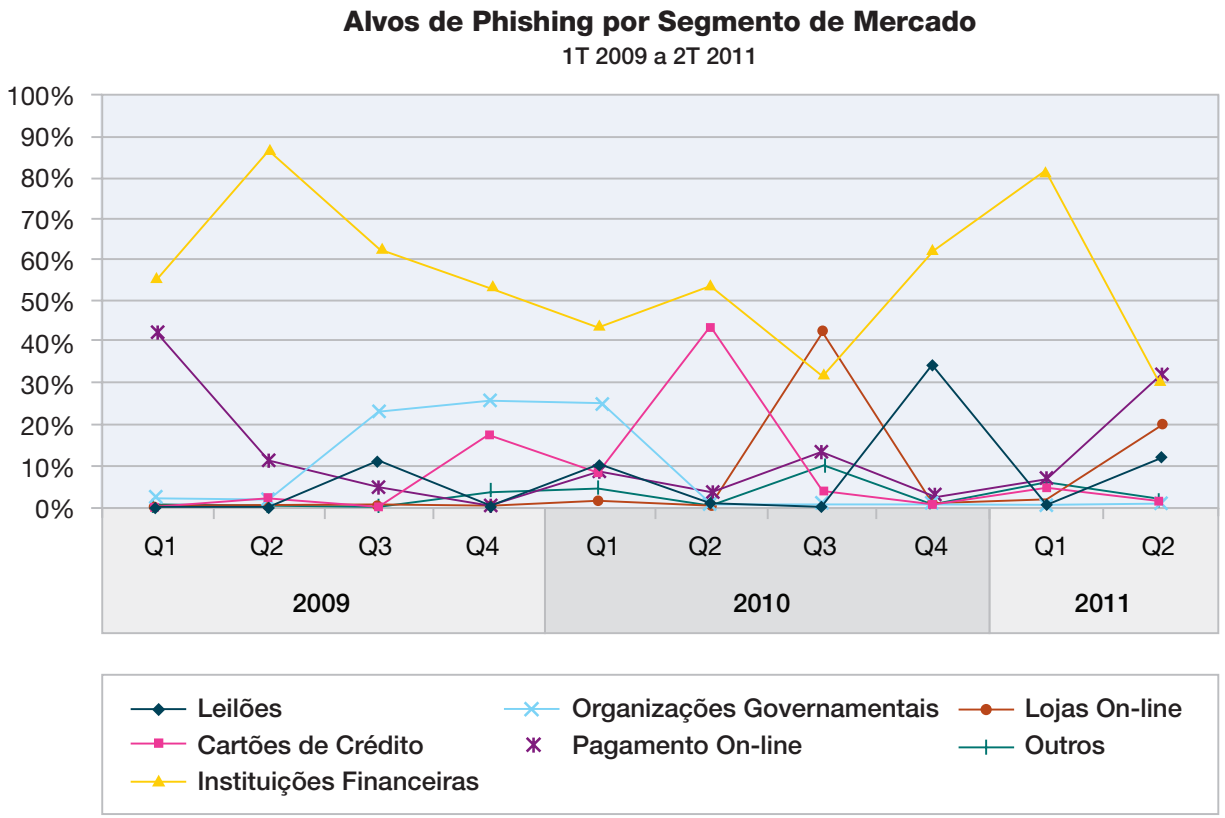



*Figura 25: Alvos de Phishing por Mercado – 1T 2009 até 2T 2011*

Figura 26 mostra a distribução geografica das instituições financeiras que são alvos de emails de phishing.

Como em 2010, a América do Norte é a principal região para phishers por email. No segundo trimestre, a Europa aumentou significativamente, alcançando quase 30%.

**Spear phishing**
Spear phishing é um phishing personalizado. Primeiramente, os phishers reúnem vários tipos de dados pessoais aplicando técnicas de engenharia social. Então, estes dados são utilizados para compor uma mensagem pessoal para a vítima. O conteúdo personalizado garante à vítima que a mensagem é legítima, daí, ela cai diretamente na armadilha. Para mais informações, consulte http://en.wikipedia.org/wiki/Spear_phishing#Phishing_techniques.

**Duplicação de cartões em caixa eletrônico**
Os duplicadores de cartões em caixas eletrônicos colocam um mecanismo sobre a abertura do cartão de um caixa eletrônico que lê a faixa magnética quando usuários desavisados passam seus cartões por ele. Mais informações sobre este assunto pode ser encontrado em http://en.wikipedia.org/wiki/Credit_card_fraud#Skimming.

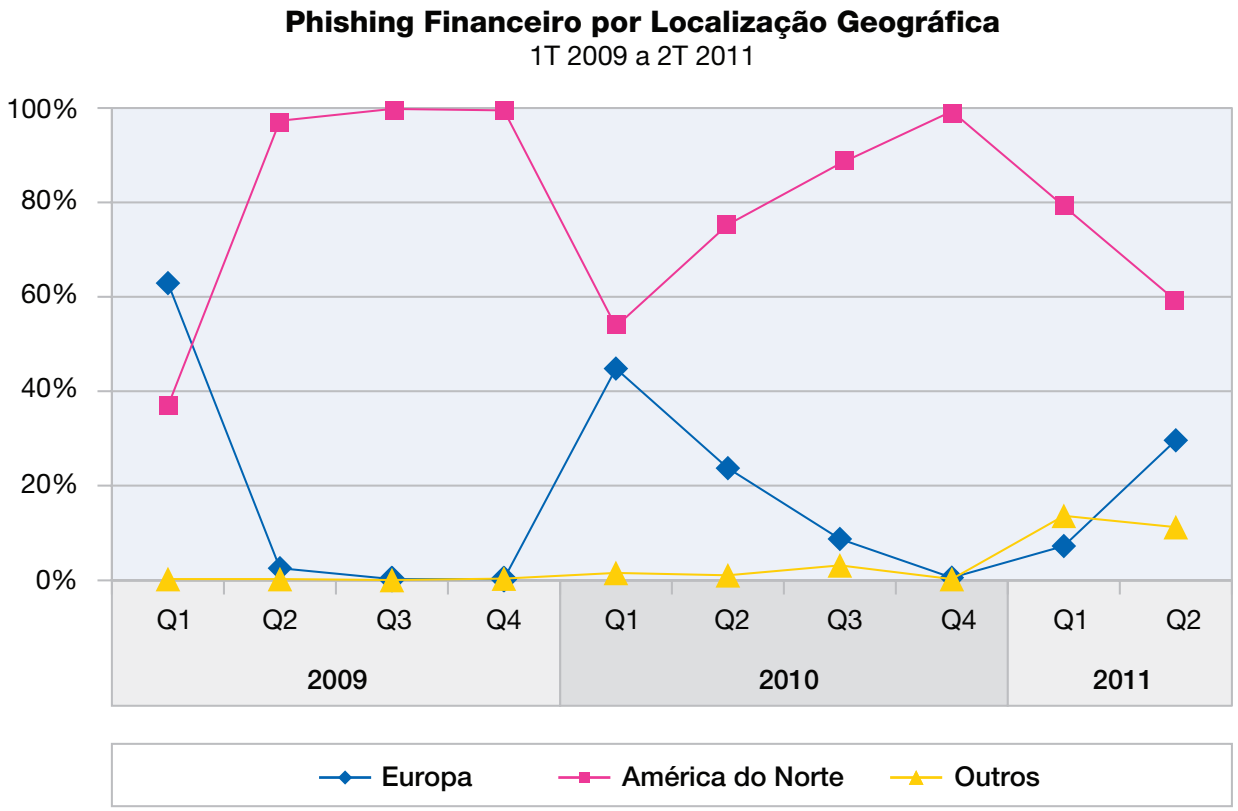



*Figura 26: Phishing Financeiro por Localização Geográfica – 1T 2009 até 2T 2011*

***Nota:*** *Estas estatísticas não apóiam a conclusão de que phishing por senhas e credenciais esteja acabado em geral. Simplesmente sugere que os phishers não confiam mais em simples phishing de emails. Parece razoável concluir que eles estejam focados em outras abordagens como spear phishing ou duplicação de cartões em caixas eletrônicos.*

## Perspectivas de futuro sobre spam

No primeiro semestre de 2011, vimos quedas significativas no volume de spam sem a recuperação que temos visto anos antes. O "ambiente de negócios" para os tradicionais spams de email mudou.

- As organizações ou empresas conseguiram derrubar botnets e infraestruturas utilizadas para distribuir spams, como visto nas derrubadas de McColo e Rustock.
- Os filtros de spams continuam melhorando.
- Outras abordagens parecem que afetam as atividades dos spammers, como percebido em "Trajetórias do Clique: Análise de Ponta-a-Ponta da Cadeia de Valor do Spam"[21]. O estudo afirmou que 95% dos pagamentos de produtos spamblicidade são manuseados por apenas três bancos. Os bancos de vítimas de spam podem bloquear o pagamento para esses três bancos.

Isto pode fazer com que os invasores concentrarem-se em outras áreas, tais como spam dentro de redes sociais ou realizar negação de distribuição de ataques de serviços. Há até mesmo spammers experientes que não consideram mais o negócio de spam atrativo[22]. Por outro lado, existem outros aspectos que podem enganar antigos e novos invasores a enviar mais spam.

- A quantidade de usuários da Internet está aumentando, consequentemente, há sempre novas vítimas de spam e ataques phishing, mesmo se apenas um de dez mil emails de spam chegar a uma caixa de entrada.
- A quantidade de máquinas disponíveis também ainda está crescendo permanentemente. Além disso, há um novo tipo de máquina para infectar: smartphones. E esses computadores portáteis têm outra vantagem sob a perspectiva dos spammers: Ao contrário dos computadores de mesa que são desligados quando não estão em uso, os smartphones estão sempre online. Atualmente, ainda temos limites de largura de banda no contexto de smartphone, pois a maioria dos usuários não tem uma taxa fixa para o uso da Internet móvel. Isto provavelmente irá mudar no futuro. Neste contexto, veja também a seção sobre **Vulnerabilidades móveis continua aumentando**.
- Sobre o tipo de conteúdo de spam, há algumas abordagens que os spammers ainda não usaram como documentos do Open Office como anexos de spam.
- IPv6 também pode fornecer muitas novas abordagens para os spammers incomodar os usuários e torturar os distribuidores de anti-spam, particularmente quando eles confiam exclusivamente em bloqueio de IP.

Portanto, há muitos aspectos que podem influenciar o desenvolvimento do volume de spam no futuro. Supondo que a quantidade de invasores não diminui, ficamos curiosos se eles ainda usarão spam para danificar ou se concentrarão em outras técnicas.

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

# Seção II
# Operando uma Infraestrutura Segura

Nesta seção do Relatório de Tendência, exploramos os assuntos sobre a fraqueza no processo, software e infraestrutura que são alvos das ameaças atuais. Discutimos as melhores práticas da conformidade de segurança, ideias de redução de custo operacional, automação, redução de custo de propriedade e a consolidação de tarefas, produtos e funções. Também apresentamos dados rastreados pela IBM durante o processo de administração ou mitigação destes problemas.

## Preparando para uma violação: abordagem de resposta a incidente (IRH)

*"Uma quantidade infinita de macacos com uma quantidade infinita de máquinas de escrever e uma quantidade infinita de tempo pode eventualmente escrever a obra de Shakespeare".*
*– O Teorema do Macaco Infinito*

Relatórios de Risco e Tendência do IBM X-Force anteriores discutiram vários mecanismos pelos quais uma rede ou seus usuários podem ser explorados e comprometidos. Recentes invasões e ataques de alto perfil demonstraram que é provável que sua organização precise realizar uma abordagem de resposta a incidente (IRH) para um incidente válido ou suspeito em algum momento no futuro. Algumas organizações possuem habilidades internas de realizar IRH enquanto outros realizam as primeiras etapas iniciais de resposta, e depois procuram por recursos adicionais de um fornecedor externo.

Para facilitar uma resposta inicial pelas primeiras respostas que ajudam a fornecer um bom ambiente de análise para respostas secundárias, o IBM Emergency Response Service (ERS) desenvolveu algumas sugestões para auxiliar com a resposta inicial.

**Ficar em pé, cair e rolar**
Cada organização deve ter um Plano de Resposta de Incidente de Segurança em Computadores (CSIRP) para implantar quando ocorrer um incidente de segurança nos computadores. Dependendo do tamanho da organização, seus recursos e a frequência com que ocorrem os incidentes, o CSIRP pode variar de algo tão simples como um número de telefone para uma organização, à qual foi terceirizada o suporte para executar totalmente seus próprios serviços de resposta a incidentes. Quando um incidente é declarado: *Planeje o trabalho. Execute o plano. Não fique dando voltas como se suas roupas estivessem pegando fogo*. O CSIRP existe para garantir que todos os aspectos do incidente sejam cobertos, que os tomadores de decisões sejam informados para que possam tomar decisões corretas e oportunas, e que o suporte possa ser fornecido ao mesmo tempo em que os erros são evitados. Pratique o CSIRP com antecedência para garantir que seja um bom plano e ofereça a estrutura necessária.

*"Uma quantidade infinita de hackers com uma quantidade infinita de teclados, uma infinita quantidade de cafeína, e uma infinita quantidade de tempo pode eventualmente comprometer uma rede".*
*– Corolário de Stone para o Teorema do Macaco Infinito*

**Treine as primeiras respostas**
Os primeiros entrevistados envolvidos no processo de IRH devem recebido treinamento suficiente para preencher a posição para a qual eles foram designados na equipe de resposta. Começando assim com suficiente consciência da situação das ameaças para reconhecer uma situação perigosa para sua rede. Os entrevistados devem ser treinados para reconhecer que há uma diferença no nível de preocupação entre um incidente com um único vírus e um incidente com várias contas de usuários fraudulentos criados juntamente com trojans, keyloggers e Zbot ou Zeus (que é um cavalo de tróia que rouba informações bancárias através de login pelo teclado.) A preocupação, as etapas corretivas e os avisos para os dois incidentes não seriam os mesmos.

**Mover esforços de peritos antecipadamente no processo**

Frequentemente, há um período de tempo entre o momento em que o incidente é reconhecido como evento e é designado como um incidente e o CSIRP é implantado. As ações durante este período crucial podem determinar se uma análise bem sucedida pode ser realizada. Tenha em mente que atividades como executar Anti-Virus e varredura de malware, correção, excluir logs e alterar configurações podem ter um impacto destrutivo sobre o sistema de arquivo além do objetivo de solucionar o problema. Por exemplo, parte do processo para incidentes com malware é desligar o sistema e excluir os pontos de restauração. É comum para dados relevantes ser recuperados a partir de pontos de restauração e excluir os pontos de restauração torna os dados indisponíveis para análise. Estes dados podem incluir cópias dos arquivos dropper iniciais, malware, registros inseridos pelo teclado, e outros arquivos para identificar o vetor de infecção inicial e conteúdo dos dados roubados. A medida em que o evento progride e começa parecer que é um incidente real, implante os procedimentos forenses no início do processo para captar os dados voláteis e conduzir as imagens. Caso contrário, você pode destruir dados valiosos para a análise.

**Saiba onde seu PI, PII, HIPAA e Fórmula Secreta residem**

**PI** significa Informação Pessoal

**PII** significa Identificação Pessoal Identificável

**HIPAA** significa Lei de Portabilidade e Responsabilidade de Seguros de Saúde. HIPAA é uma lei de privacidade criada em 1996 pelo Congresso dos Estados Unidos; seu único propósito é proteger os indivíduos e sua privacidade médica.

Os entrevistados incidentes devem conhecer os detalhes sobre a construção de sua rede, quais os dispositivos de rede que podem ter registros relevantes, e que tipo de dados confidenciais devem ou não ser encontrados em computadores analisados. Durante uma análise, podem ser recuperados os dados que apontam para endereços IP de outros computadores na rede como uma fonte ou alvo de tráfego malicioso. Deve-se poder localizar o proprietário e o local físico de um endereço IP rapidamente se um incidente estiver em andamento. Também, deve-se estar preparado para fornecer senhas e chaves de decriptografia para os dados criptografados.

**Deve-se ter um contato legal experiente e acessível**

Durante um incidente, várias questões legais podem surgir e que requeiram uma decisão do representante legal da organização. Estas questões podem variar de autoridade legal requerendo acesso a dispositivos de armazenamento pessoal de um funcionário até a legalidade de tomar tipos de dados específicos de um país estrangeiro. Além disso, se houver alguma participação do RH ou ação legal resultante do incidente, o conselheiro legal pode ter questões específicas que precisam ser respondidas. O conselheiro legal deve ter tido treinamento suficiente em questões legais de TI para oferecer respostas apropriadas. Elas também devem ser incluídas em discussões em pontos de decisão para ajudar a garantir que a empresa está tomando a ação legal correta.

**O representante do cliente deve ter a autoridade para fazer as coisas acontecerem**

O ponto de contato entre a organização e o grupo ERS de resposta deve ter autoridade suficiente para realizar as coisas, tanto organizacionalmente como na rede. Esta pessoa não tem que estar no topo da hierarquia do gerenciamento de CSIRP, mas deve ter conhecimento suficiente da organização e de rede para obter os recursos necessários. Além disso, o primeiro entrevistado deve ter privilégios de acesso suficiente à rede para executar ferramentas que captam dados voláteis e imagens forenses.

**Deve-se convidar alguém com um talão de cheque para a festa**

Muitas vezes, o processo de resposta a incidente envolve um custo monetário. Grande parte desta despesa é identificada e planejada se o suporte tiver de ser comprado. Frequentemente, o que não é planejado são os gastos do dia a dia no nível do entrevistado. Apesar de um contrato de vários milhares de dólares ser aprovado para o compromisso, o processo pode ser atrasado pela incapacidade de obter um disco rígido de armazenamento de dados de US$50 em menos de uma semana.

**Deve-se entender os recursos do malware**

Durante um incidente envolvendo malware, incorpore os recursos conhecidos do malware ao planejar e executar o plano de resposta. Por exemplo, o malware que é transmitido via autorun de USB é uma característica comum de muitos dos malwares de hoje. Por isso, o uso de drives USB para transferir ferramentas de correção ou capturas e registros de dados voláteis entre computadores contaminados e computadores entrevistados, frequentemente podem resultar em espalhar o malware de um computador contaminado para um não contaminado.

**Quarentena, não exclua**

Muitas atividades de resposta a incidente envolvem malware. Frequentemente, o malware é identificado por uma varredura do antivírus que pode tanto excluir ou colocar o malware em quarentena. Se o malware for excluído, não estará mais disponível para análise para determinar seus recursos e as datas e horários associados ao arquivo malware. Estas datas e horários podem ajudar a identificar as circunstâncias sob as quais ele foi instalado no computador e outras atividades do arquivo do sistema que ocorrem ao mesmo tempo, tais como a criação de arquivos de registro através do teclado.

**Configurações do Windows 7**

Para aquelas redes que migraram para o Vista e Windows 7 (ou estão em processo de), considere acionar a chave de atualização do último acesso no registro. No Windows 7, uma das datas que pode ser rastreada relacionada a um arquivo é a data que o arquivo foi acessado pela última vez. Esta pode ser a data que ele foi impresso, verificado pelo antivírus, copiado ou aberto. Para economizar tempo, uma instalação padrão do Windows 7 possui a "atualização" da última data de acesso e horário em que foi encerrado. Frequentemente, esta data e horário do último acesso é crítico durante a análise de um incidente para estabelecer uma linha de tempo para determinar quais dados foram roubados ou tocados.

**Registro – Sim/Não**

O registro padrão para o Windows XP não é configurado para auxiliar a maioria das empresas com análise pós-incidente. Alguns registros não são ativados, eventos apropriados não estão sendo registrados, e os tamanhos dos registros padrão são pequenos. Registros mal-configurados têm sido vistos para documentar pelo menos 52 minutos de atividade valiosa antes que o tamanho pequeno do registro faça com que entradas recentes substituam as mais antigas.

**Cafeteria boa companhia**

Enquanto que uma cafeteria boa companhia não é necessária, o ponto é que as funções de suporte ocorrem nos bastidores. Estas funções variam de suporte de alimentação local até um plano de rotação para o pessoal envolvido no processo de resposta e correção. Por exemplo, não é incomum para ERS responder a uma organização que está na metade da reposta e correção e descobrir que a equipe de resposta tem estado sem dormir por mais de 24 horas. Enquanto que às vezes é necessário alcançar as metas da operação, isto levanta várias preocupações:

- O planejamento e preparação pré-incidente não oferecia que mais de uma pessoa tivesse capacidade e habilidade para responder e corrigir o incidente. Planejar ter mais de uma pessoa com a capacidade apropriada.
- Os estudos mostram que após 24 horas sem dormir, o desempenho físico e cognitivo de uma pessoa é equivalente a estar legalmente intoxicado. Sua capacidade de tomar decisões é reduzida e o tempo que ela leva para tomar decisões é aumentado.
- A partir de uma perspectiva segura, a saúde dos entrevistados pode ser afetada pelo stress e longas horas de trabalho impostas pelo processo de gerenciamento de incidente. As operações de conduta militar ultrapassam 24 horas, mas eles são treinados para isso e o condicionamento físico dos soldados é comumente melhor do que o da equipe de TI. Os acidentes são mais prováveis de ocorrer quando a capacidade de tomar decisões diminui e o tempo de resposta aumenta.

Ao longo dos anos, as equipes policiais de rastreamento desenvolveram o conceito de "Espaço Tempo Distância" que compara a diferença de tempo que leva para uma pessoa em fuga percorrer uma distância comparada ao tempo que leva um rastreador a percorrer a mesma distância. Um criminoso em fuga pode correr 45 metros em segundos, mas o rastreador pode passar uma hora seguindo os mínimos sinais da passagem da pessoa pelos mesmos 45 metros. A resposta a incidentes sofre da mesma demora "Espaço Tempo Distância" para detectar o ataque, acumulando e analisando dados, e implementando defesas com base na análise. Os detalhes de dois minutos valiosos de atividades realizadas por um invasor pode levar horas ou dias para serem obtidos e analizados a partir de arquivos de registro, atrasando a implantação de defesas. Se a resposta a incidente for realizada no local ou não, cada um dos itens discutidos aqui tem a intenção de ajudar os entrevistados a reduzir o "Espaço Tempo Distância" em IRH para alcançar uma detecção, análise de dados e implantação de defesa mais rápidas.

| Fontes Potenciais de Dados para Análise IRH | |
|---|---|
| Diagrama de Topologia de Rede | Notas sobre as Primeiras Ações do Entrevistado (varreduras, atualizações) |
| Registros de Rede (Firewall, DNS, Proxy, IDS/IPS) | Imagem de Base (utilizada para excluir arquivos conhecidos) |
| Registros de Eventos IDS de Conectividade | Capturas de Pacote/Varreduras de Porta |
| Registros de Sistema Operacional | Registros de Aplicativos (WWW, FTP, VPN) |
| Registros de Banco de Dados | Backups de Sistema/Imagens Forenses |
| RAM e outros Dados Voláteis | Amostras de Arquivos Suspeitos Localizados |
| Entrevistas com Usuários | Registros de Evento de Antivírus |

*Tabela 4: Fontes de Dados Potenciais para análise de abordagem de resposta a incidente – 1S 2011*

## Pesquisa contra vulnerabilidades

Ataques em redes de computadores geralmente aumentam as vulnerabilidades no software executado nestas redes. Para operar as redes com segurança, deve-se estar consciente de tais vulnerabilidades e suas correções. Desde 1996, o Banco de Dados X-Force mantém um rastreamento de cada relatório público de uma divulgação ou correção de vulnerabilidade de segurança que pudemos ter acesso. Por anos, temos relatado sobre estes dados no Relatório Bianual de Tendência X-Force. Estes dados nos informam de um grande acordo sobre a natureza das questões de segurança que temos mitigado sobre nossas redes e como estas questões mudam com o passar do tempo.

Observe que em muitos gráficos sobre vulnerabilidade incluídos nesta seção, o total para 2011 é apresentado como projeções. É difícil comparar dados a partir da metade de um ano com tendências anteriores com base no total anual. Para facilitar as comparações, veja e entenda que, em alguns casos, dobramos a quantidade de vulnerabilidades que temos visto até 2011 para criar um total projetado para o ano todo que pode então ser comparado com o total do ano anterior todo e identificado como "P" nos gráficos. Claro que as tendências que temos visto no primeiro semestre de 2011 podem ou não se mater até o final do ano, então os gráficos finais que publicamos em nosso relatório de final de ano pode parecer diferente.

### Quantidade total de redução de vulnerabilidade – mas é cíclico

No primeiro semestre de 2011, vimos um total inferior de divulgação de vulnerabilidade de segurança do que a vista no ano passado nesta época. Isto pode não ser surpresa para aqueles que acompanham a divulgação de vulnerabilidade por muitos anos. O volume de divulgações de vulnerabilidade de segurança parece acompanhar o ciclo de alternância de dois anos. Em 2007, houve menos divulgações de vulnerabilidade do que em 2006, a quantidade aumentou novamente em 2008, e então voltou a reduzir em 2009, mas com o passar do tempo os totais parem estar se acumulando cada vez mais. No ano passado, 2010, viu-se o maior número de publicações de vulnerabilidade registrado, mais de 8.500. Este ano, estamos rastreando apenas 7 mil divulgações, uma redução significante desde o ano passado, mas cerca da mesma quantidade que vimos em 2006.

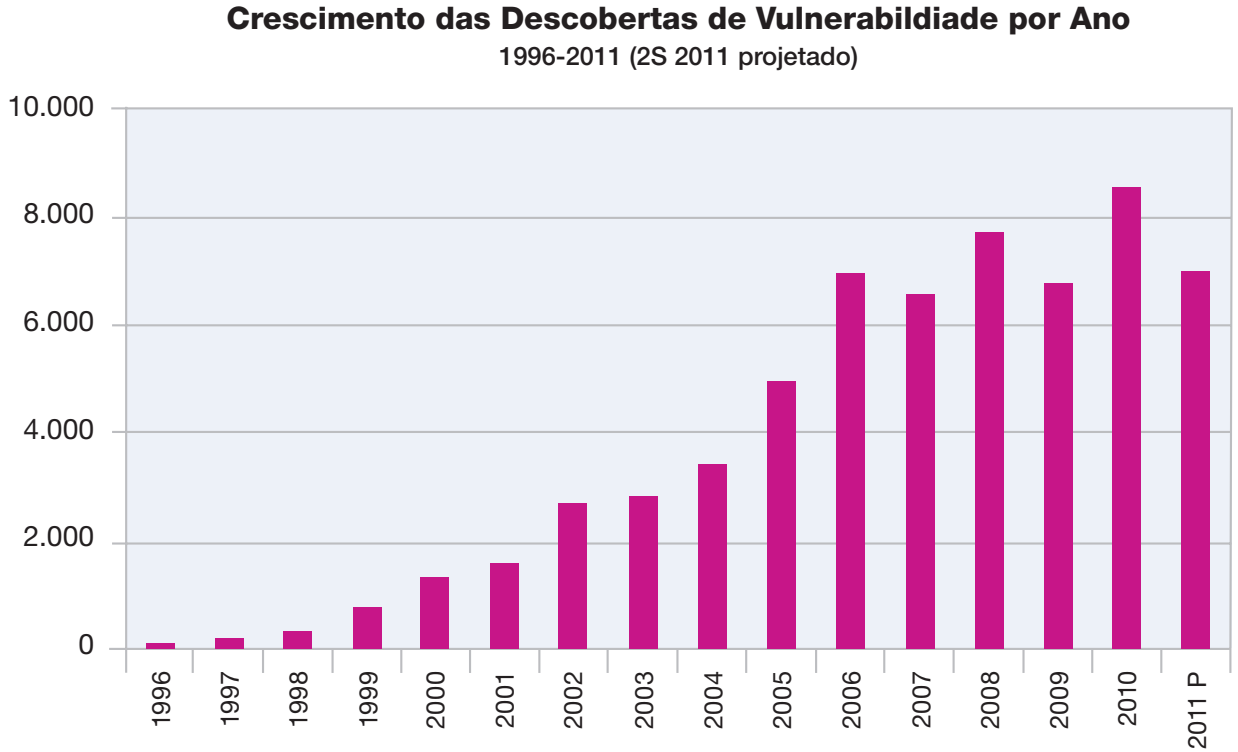



*Figura 27: Crescimento de Divulgações de Vulnerabilidade por Ano – 1996-2011 (2011 Projeção Semestral)*

Onde está a redução? Está principalmente nas vulnerabilidades de aplicativos da web. Nos últimos anos, aproximadamente metade das vulnerabilidades de segurança que foram divulgadas, eram vulnerabilidades em aplicativos da web. O número caiu para 37% este ano, com uma diminuição significativa no volume de vulnerabilidades SQL Injection em particular. Isto significa que podemos parar de nos preocupar com os problemas de segurança de aplicativos da web? Claro que não.

Ainda existe uma grande quantidade destas vulnerabilidades sendo divulgadas.

Na verdade, detestamos fazer previsões a longo prazo sobre esta categoria de questões de segurança. Uma redução este ano pode ser sinal de progresso – pode indicar que as vulnerabilidades de injeção de SQL estão ficando mais difíceis de serem encontradas – significando que os desenvolvedores de aplicativos da web estão escrevendo códigos melhores que são menos suscetíveis a eles. Ao longo do tempo, isto pode significar que a web se tornará mais segura. Entretanto, fizemos este tipo de previsão no passado em relação à redução de categorias de vulnerabilidades de segurança e então fomos surpreendidos quando a quantidade de divulgação subiu novamente. Vai levar mais tempo para uma tendência sustentada, antes de nos sentirmos confortáveis para fazer previsões.

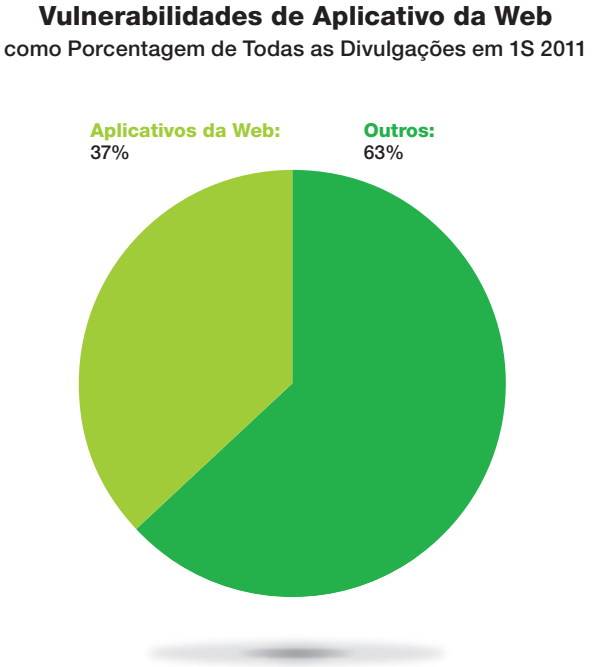



*Figura 28: Vulnerabilidades de Aplicativos da Webcomo uma Porcentagem de Todas as Divulgações em 1S 2011*

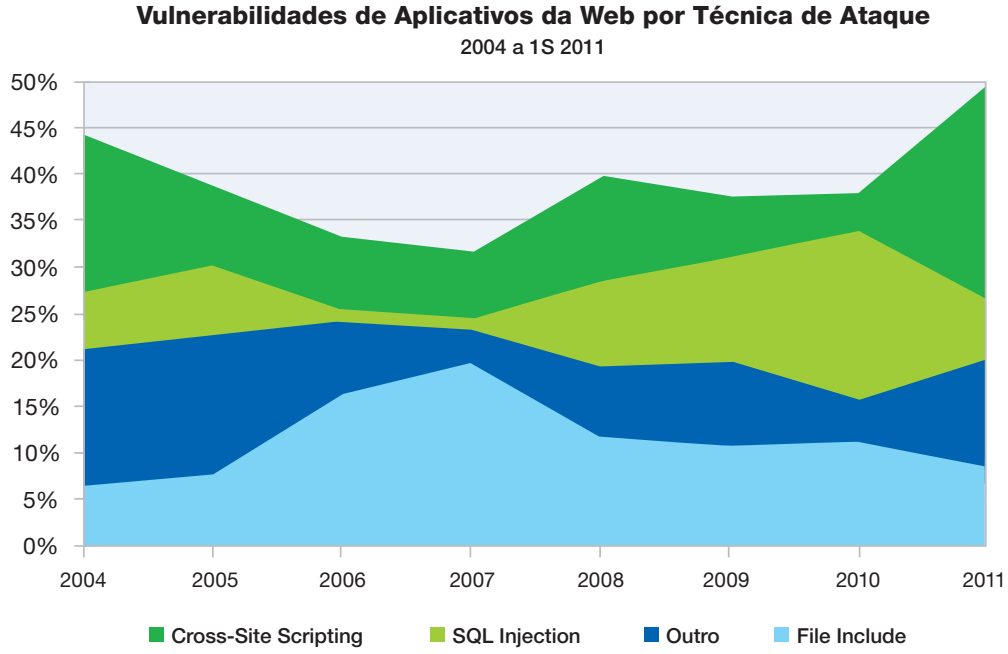



*Figura 29: Vulnerabilidades de Aplicativos da Web por Técnica de Ataque – 2004 a 1S 2011*

## Os navegadores da web estão mais seguros?

Por exemplo, em 2009, vimos as vulnerabilidades dos navegadores da web divulgadas menos altas e críticas do que em 2008. (Consideramos as vulnerabilidades altas e críticas como sendo aquelas que possuem uma pontuação CVSS (Common Vulnerability Scoring System) de 7,0 ou superior.) No momento isto parecia ser uma vitória. Há muita atividade de ataque almejando as vulnerabilidades dos navegadores de web, e então há a quantidade correspondente do foco de encontrar, divulgar e corrigir estas vulnerabilidades na esperança de reduzir a área de superfície do ataque do navegador. Quando vimos os números começarem a cair, pensamos, talvez já tenhamos ultrapassado isto. Talvez, realmente estejamos avançando em direção ao dia em que o navegador será mais seguro.

Infelizmente, a quantidade de vulnerabilidades altas e críticas do navegador subiu em 2010 e naquele ano, a quantidade total de vulnerabilidades de navegadores subiu significativamente. No primeiro semestre de 2011, a quantidade total ainda está crescendo, mas a quantidade de vulnerabilidades altas e críticas caiu para um nível que o segmento não via desde 2007. Quando você olha para a tendência decrescente em vulnerabilidades altas e críticas de 2009 até 2011 (projetada), parece haver uma redução constante. O segmento parece estar melhorando ao fazer software de navegadores mais seguros, mesmo que o mercado de navegadores esteja se tornando mais competitivo. Talvez, estes sejam os sinais do progresso.

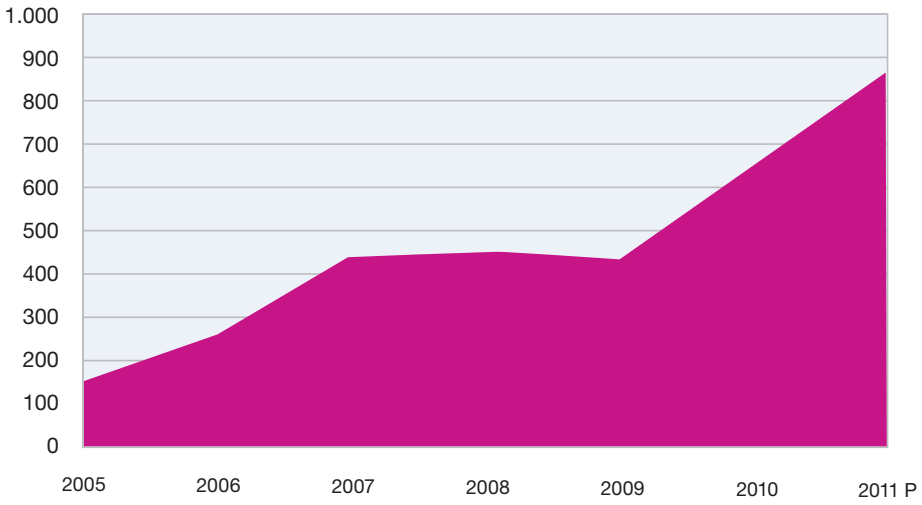



*Figura 30: Vulnerabilidades de Navegador da Web – 2005 – 1S 2011 (projetado)*

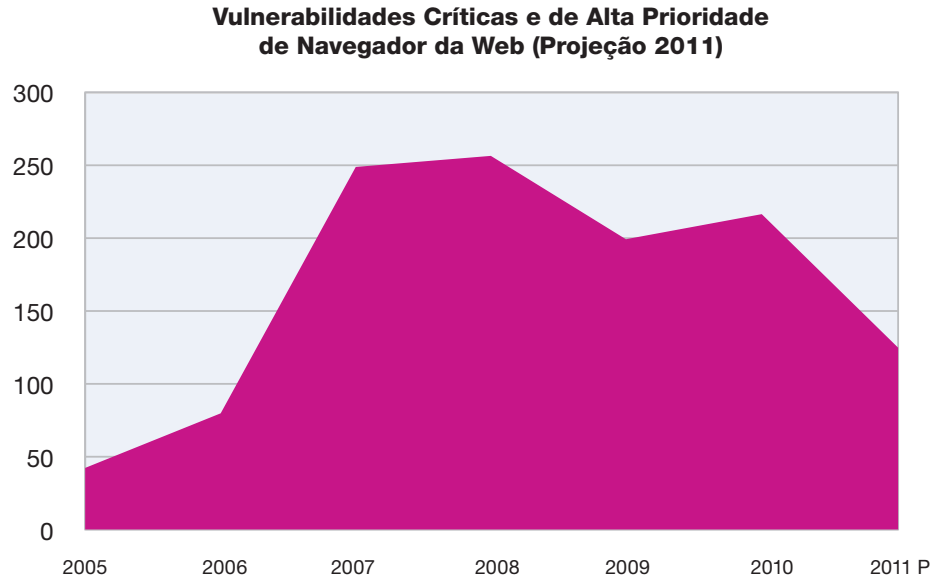



*Figura 31: Vulnerabilidades de Navegador da Web, Críticas e Altas – 2005 – 1S 2011 (projetado)*

Outra área, que viu um declínio significativo no primeiro semestre de 2011, foi o lançamento público das vulnerabilidades de segurança visando o código de exploração. Vimos menos explorações reais lançadas até este ano desde 2006. Embora, podemos apenas especular as causas, o declínio ocorrido tanto em termos reais como em base percentual versus a quantidade total de vulnerabilidades divulgadas. Até agora cerca de 12% das vulnerabilidades que foram divulgadas viram lançamentos de exploração real, considerando que no ano anterior a quantidade estava próxima a 15%.

Há uma janela de oportunidade que um invasor tem para almejar uma vulnerabilidade de segurança. Essa janela abre quando a vulnerabilidade acaba de ser descoberta, e fecha quando a vulnerabilidade é finalmente corrigida em um sistema vulnerável. O período de tempo entre a divulgação de vulnerabilidade e o lançamento da correção constitui uma parte desta janela, e a outra parte é o período de tempo que leva para uma pessoa instalar tal correção nos sistemas vulneráveis em suas redes.

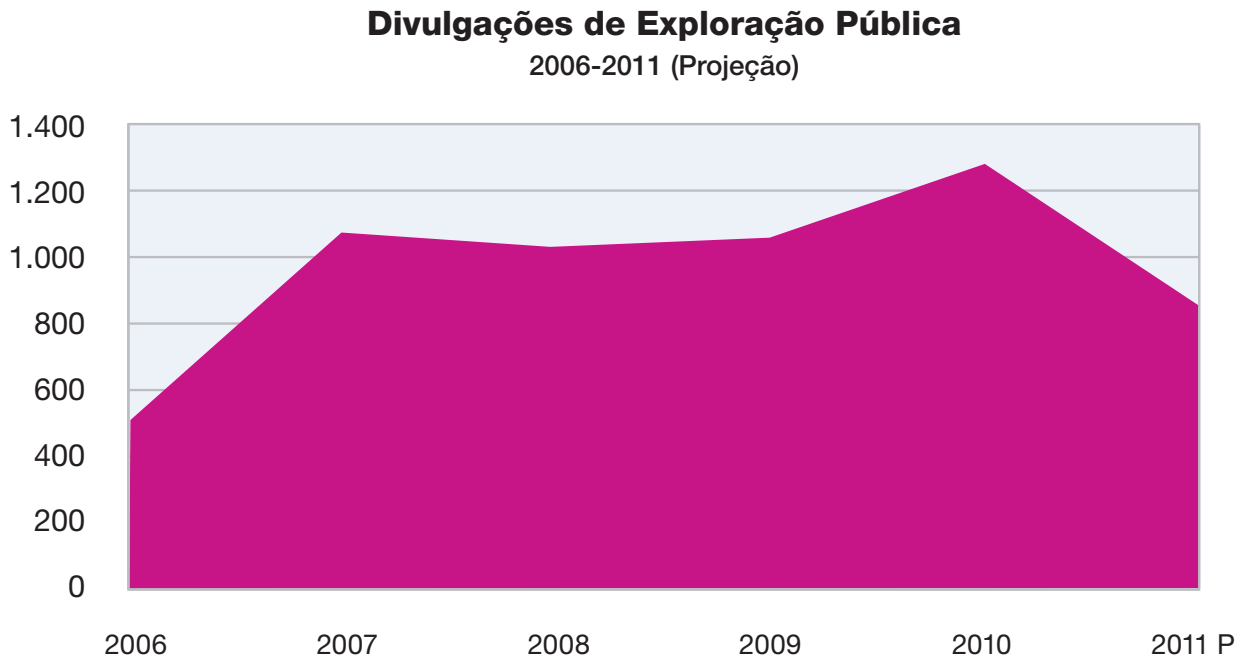



*Figura 32: Divulgações de Exploração Pública – 2006-2011 (Projetado)*

| Exploração Real | 2006 | 2007 | 2008 | 2009 | 2010 | Projeção de 2011 |
|---|---|---|---|---|---|---|
| Porcentagem do Total | 7,3 % | 16,5 % | 13,4 % | 15.7 % | 14,9 % | 12,0 % |

*Tabela 5: Divulgações de Exploração Pública – 2006-2011 (Projetado)*

Cerca de 58% das vulnerabilidades que foram divulgadas no primeiro semestre de 2011 tiveram uma correção disponível no mesmo dia em que foram publicamente divulgadas – o que é um caso ideal. Por outro lado, cerca de 37% não tinha correção disponível no momento deste relatório. Esta é uma melhora considerável desde os anos anteriores – a quantidade de vulnerabilidades não corrigidas tem caído abaixo de 44% do total pelos últimos 5 anos. Os outros 5% restantes representam os casos intermediários onde uma correção foi disponibilizada em algum momento após a divulgação pública da vulnerabilidade. O pior caso em nossos dados foi de 171 dias. Felizmente, há apenas uma minoria de vulnerabilidades de software corporativos com alta gravidade que se encaixam nesta categoria intermediária.

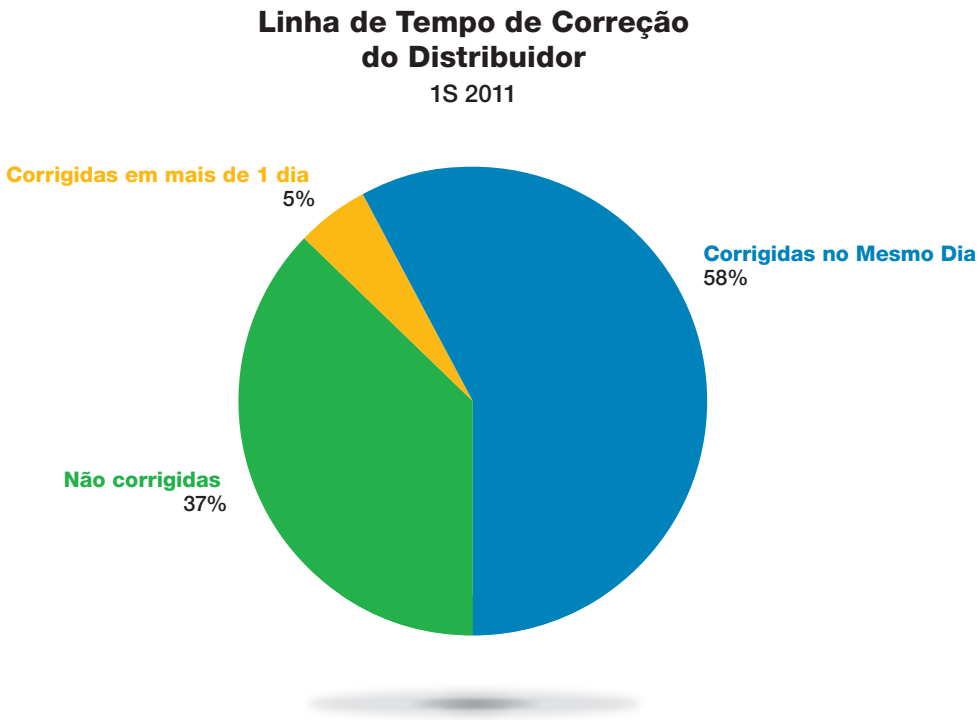



*Figura 33: Linha de Tempo de Correção do Distribuidor – 1S 2011*

Assim que uma correção é disponibilizada, os administradores de rede devem instalá-la de maneira oportuna. Não temos uma fonte de dados direta para medir a quantidade de tempo que leva para corrigir as redes, mas há um modo indireto de medir esta janela. Como afirmado anteriormente, o código de exploração foi lançado publicamente para cerca de 12% das vulnerabilidades que foram divulgadas este ano. O tempo destes lançamentos de exploração é interessante. Geralmente as explorações são lançadas no mesmo dia ou logo após uma vulnerabilidade ser divulgada, mas em alguns casos muitas semanas ou meses se passam antes do surgimento do código de exploração. Parte deste tempo de atraso pode representar situações onde o código de exploração está sendo utilizado para visar as redes vulneráveis e apenas uma vez, as superfícies publicamente têm seu valor reduzido, pois as vulnerabilidades foram finalmente corrigidas.

Embora uma quantidade das estatísticas de vulnerabilidades diminua durante o primeiro semestre deste ano, há áreas importantes de aumento. Nosso banco de dados de vulnerabilidades de segurança engloba vulnerabilidades de todos os tipos diferentes de produtos de software corporativos desde os softwares corporativos mais críticos até os pacotes de softwares menores com uma minoria de usuários. Uma redução na quantidade geral de vulnerabilidades de segurança pode não ter um impacto sobre a carga de trabalho experimentada pelas operações de TI da corporação a menos que a redução esteja focada nas vulnerabilidades que impactam o software corporativo. De fato, até este ano temos visto mais vulnerabilidades de segurança divulgadas nos principais pacotes de software corporativos que vimos nos anos anteriores, significando que os profissionais de segurança de TI podem tem mais trabalho para corrigir e remediar estas vulnerabilidades do que já tiveram no passado.

| Linha de Tempo de Correção | Distribuidores de Software | Principais Distribuidores de Software |
|---|---|---|
| Mesmo Dia | 2058 | 1229 |
| Semana 1 | 72 | 9 |
| Semana 2 | 30 | 6 |
| Semana 3 | 7 | 0 |
| Semana 4 | 14 | 5 |
| Semana 5 | 15 | 0 |
| Semana 6 | 11 | 4 |
| Semana 7 | 5 | 2 |
| Semana 8 | 2 | 1 |

*Tabela 6: Tempo de lançamento de correção de todos os distribuidores de software versus principais distribuidores de software – 1S 2011*

| Tempo de Exploração | 0 dias | 1 mês | 2 meses | 3 meses | 4 meses |
|---|---|---|---|---|---|
| 0 dias | 854 | 308 | 23 | 12 | 6 |

*Tabela 7: Tempo de Divulgação de Exploração Pública por Semanas – 1S 2011*

As empresas que enviam muitos softwares tendem a estar sujeitas a mais divulgações de vulnerabilidade de segurança. Ao olharmos para os dez distribuidores de software com o maior número de divulgações de vulnerabilidade, excluindo os sistemas de gerenciamento de conteúdo da web, temos uma lista das maiores empresas de software corporativos que são justamente consistentes ano após ano. Em 2009, este grupo representava 24% e em 2010 este grupo representava 25% do número total de divulgações de vulnerabilidades de segurança. Este ano, tal número subiu para 34% à medida que o número de divulgações de vulnerabilidades diminuiu.

Em 2010, o número de vulnerabilidades divulgadas por este grupo de dez distribuidores de software aumentou em uma média de 66% desde 2009, com 8 dos 10 maiores distribuidores comprovando os aumentos. Este aumento parece ter se mantido em 2011 apesar do declínio geral em divulgações de vulnerabilidade. Durante o primeiro semestre de 2011, vimos outro aumento médio de 28,6% desde grupo, com metade do grupo aumentando e a outra metade diminuindo. O resultado é que a equipe de TI da corporação está passando muito mais tempo, ou tempo demais, para instalar as correções este ano do que no passado.

**Os Dez Principais Distribuidores de Software com o Maior Número de Divulgações de Vulnerabilidade**
2009 – 1S 2011

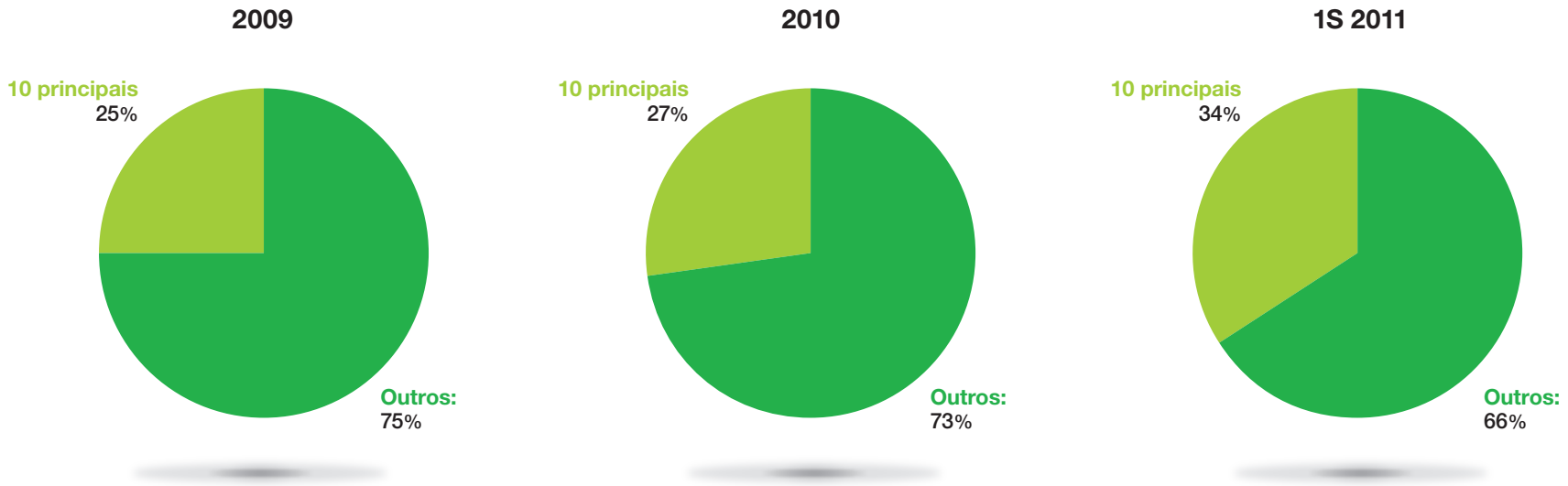



*Figura 34: Os Dez Principais Distribuidores de Software com o Maior Número de Divulgações de Vulnerabilidade – 2009 – 1S 2011*

## Vulnerabilidades críticas estão crescendo

Outra variável que está aumentando substancialmente é a quantidade de vulnerabilidades críticas. Estas são as vulnerabilidades de segurança com uma Pontuação CVSS (Common Vulnerability Scoring System) de 10 de 10. Para os dois últimos anos aproximadamente 1% das vulnerabilidades que foram divulgadas tiveram esta pontuação, mas até agora em 2011, o número está acima de 3%, e já ultrapassou o total para 2010. Quase todas essas vulnerabilidades críticas representam um problema sério de execução de código remoto que afeta um importante produto de software corporativo. Esta é outra razão pela qual houve pouco descanso para os profissionais de segurança de TI este ano.

| Pontuação CVSS | Nível de Gravidade |
|---|---|
| 10 | Crítico |
| 7.0-9.9 | Alto |
| 4.0-6.9 | Médio |
| 0.0-3.9 | Baixo |

*Tabela 8: Pontuação CVSS e Nível de Gravidade Correspondente*

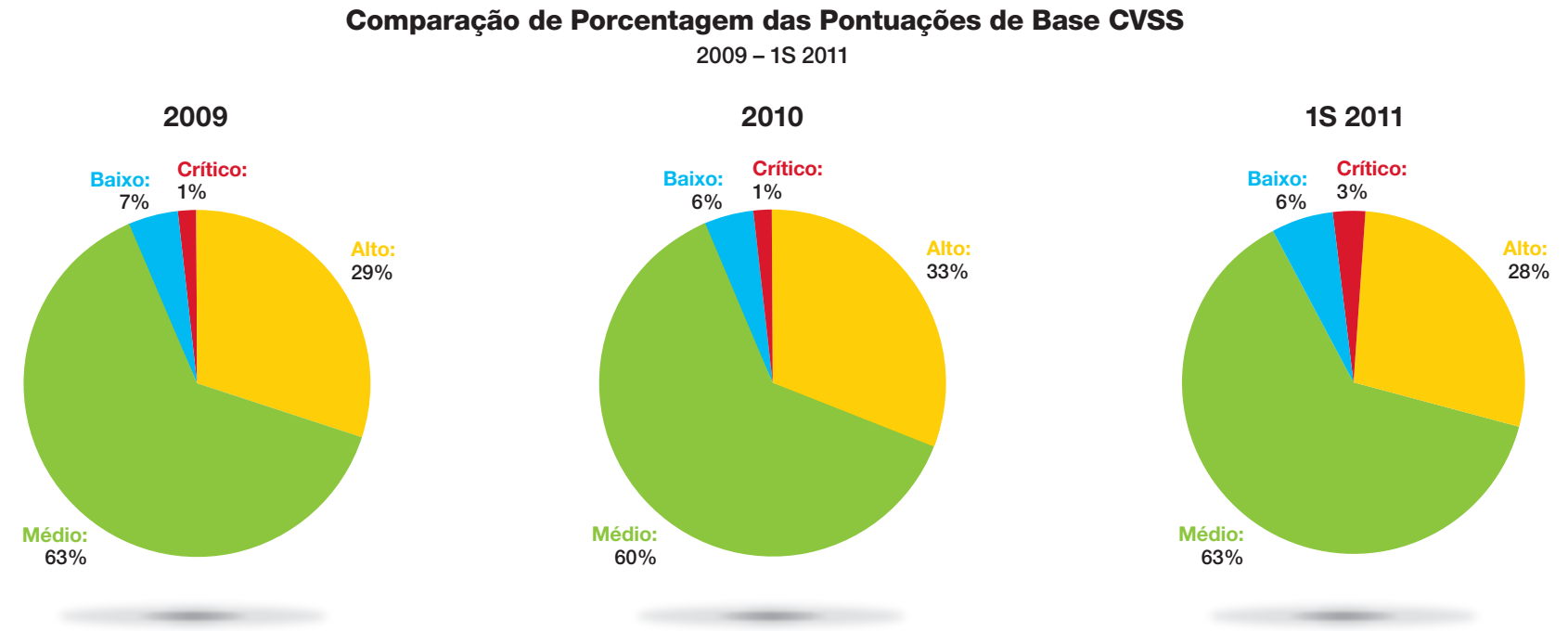



*Figura 35: Comparação de Porcentagem das Pontuações de Base CVSS – 2009 – 1S 2011*

## Alterações do cliente, multimídia e leitores de documentos

Em 2005 e antes do tipo mais comum de vulnerabilidade do cliente havia a vulnerabilidade no sistema operacional de desktop. Na verdade, as vulnerabilidades do sistema operacional de desktop eram um vetor de ataque muito importante durante o período em que alguns eram explorados por worms da Internet. Na última metade da década passada, as melhores práticas de segurança mudaram o foco do SO para o navegador. Entretanto, até 2011, temos visto uma grande quantidade de vulnerabilidades de SO de desktop, com vulnerabilidades altas e críticas de sistema operacional de desktop ultrapassando as vulnerabilidades altas e críticas divulgadas em navegadores. Estas vulnerabilidades se enquadram em várias categorias diferentes. Na teoria, algumas delas podem ser exploradas por worms, mas na prática isso não tem acontecido. Os recursos avançados de segurança nos modernos sistemas operacionais tornaram a exploração de algumas destas vulnerabilidades mais desafiadoras do que eram anos atrás, e até agora parecem ter tido um impacto positivo.

Os principais tipos de vulnerabilidades que afetam os clientes continuam a cair em uma das quatro principais categorias mostradas na Tabela 9.

| Categoria | Descrição |
|---|---|
| Navegador | Software e plug-ins de navegador de cliente da web. |
| Leitor e Editor de Documento | Software que permite aos usuários criar ou visualizar documentos, planilhas, apresentações e outros tipos de arquivo que não sejam imagens, músicas ou filmes. |
| Multimídia | Software que permite aos usuários criar ou visualizar músicas e filmes. |
| Sistema Operacional | O sistema operacional de base, excluindo aplicativos que estão nas outras três categorias. |

*Tabela 9: Principais Categorias de Vulnerabilidade Relativas às Divulgações de Vulnerabilidade de Cliente em 2011*

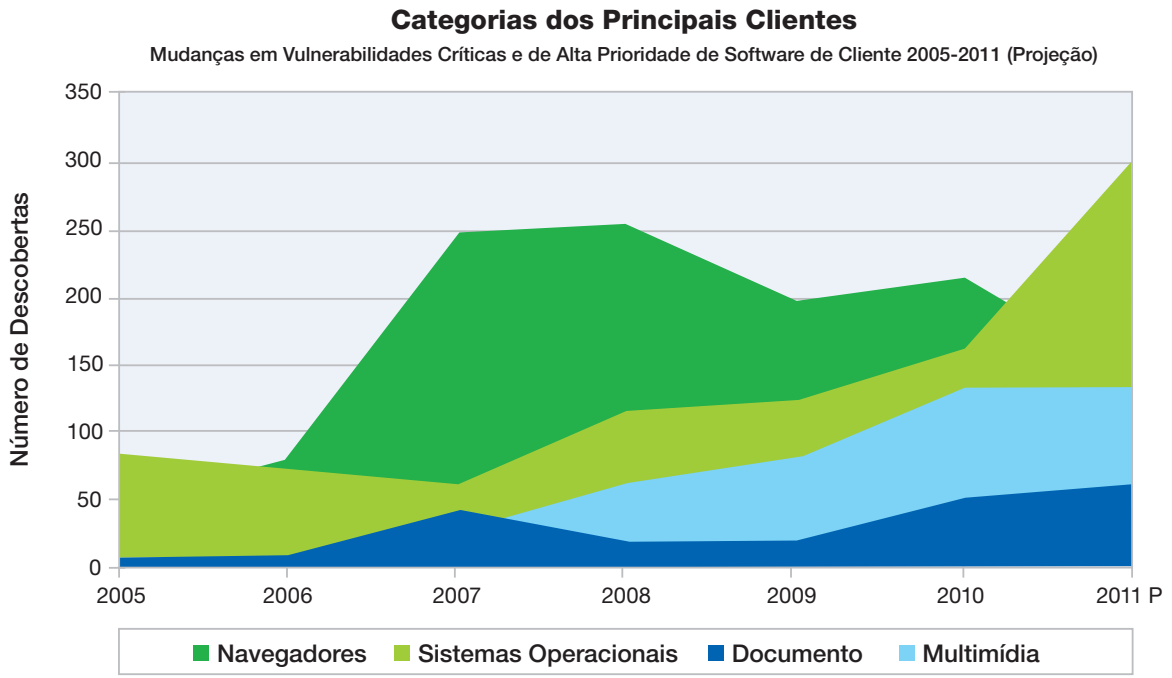



*Figura 36: Categorias dos Principais Clientes – Mudanças em Vulnerabilidades Críticas e de Alta Prioridade de Software de Cliente, 2005-2011 (Projetado)*

Duas outras áreas que viram aumentos significantes foram as vulnerabilidades em leitores de documentos e tocadores multimídia. Como o mercado de navegadores se tornou mais competitivo, os invasores se concentraram no software que os consumidores estão executando, independentemente do navegador de sua preferência – possibilitando a captura do maior número de vítimas com uma exploração específica. Esforços recentes para proteger alguns destes aplicativos devem forçar os invasores a mudar de estratégia, mas a tecnologia sandbox não é perfeita. Este assunto foi submetido a uma apresentação pelos Pesquisadores do X-Force, Mark Yason e Paul Sabanal, em Blackhat, EUA, 2011.

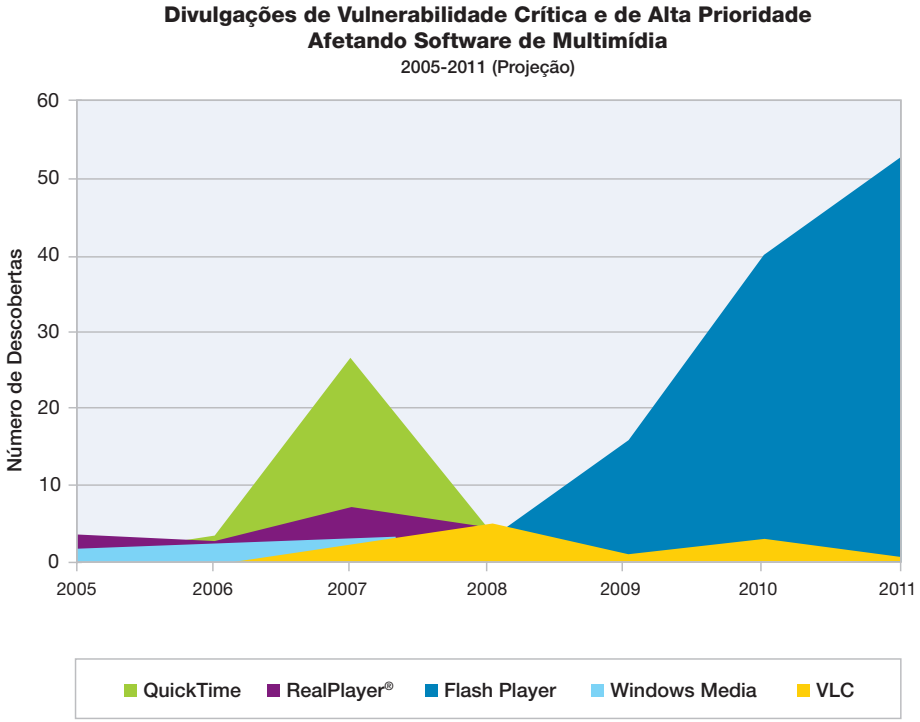



*Figura 37: Divulgações de Vulnerabilidade Críticas e de Alta Prioridade que Afetam Software de Multimídia – 2005-2011 (Projetado)*

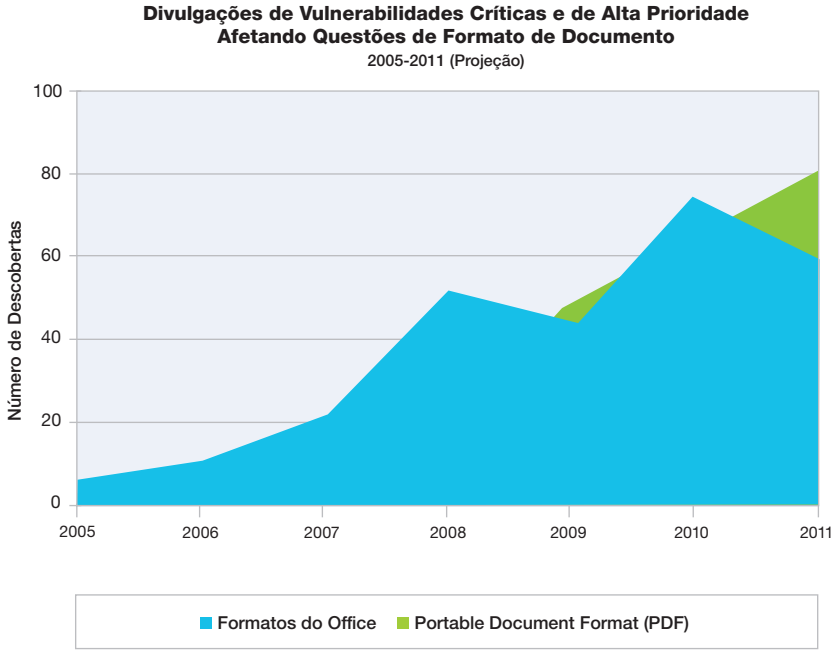



*Figura 38: Divulgações de Vulnerabilidade Crítica e de Alta Prioridade que Afetam Questões de Formato de Documento – 2005-2011 (Projetado)*

## Vulnerabilidades remotas continuam a crescer

Temos visto um interesse contínuo pelas vulnerabilidades remotas enquanto os usuários corporativos trazem smartphones e tablets para o local de trabalho. O primeiro semestre de 2011 viu um aumento do nível da atividade de malware visando a última geração de dispositivos inteligentes, enquanto que, finalmente, os invasores estão se aquecendo para as oportunidades que estes dispositivos representam. O aumento de quantidade de divulgações de vulnerabilidades e lançamentos de exploração visando estas plataformas que vimos em 2010, foi sustentado em 2011, e não mostra sinal de redução.

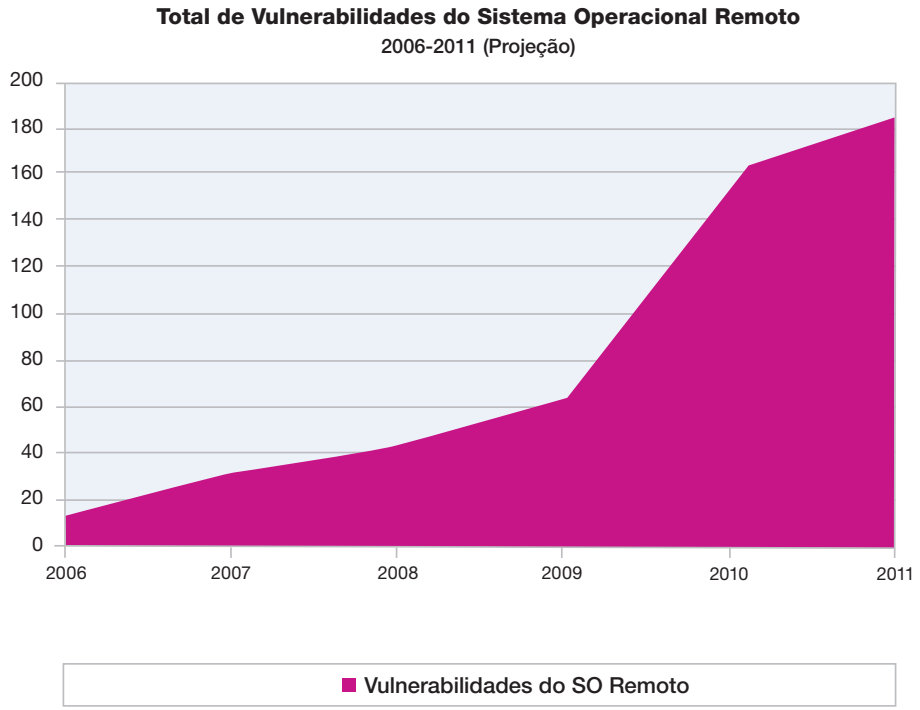



*Figura 39: Total de Vulnerabilidades do Sistema Operacional Remoto – 2006-2011 (Projetado)*

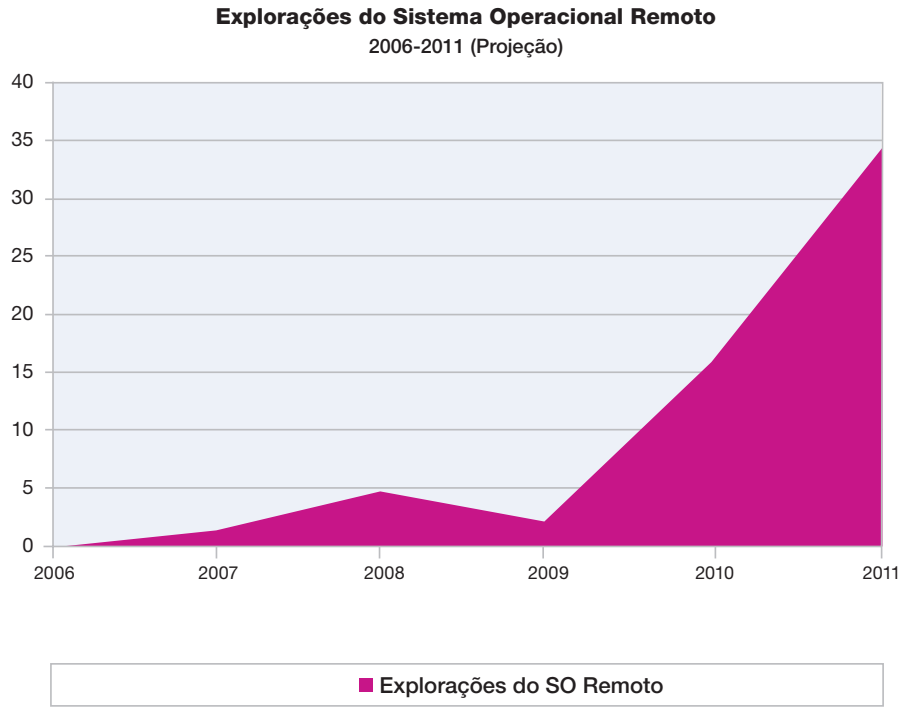



*Figura 40: Exploração do Sistema Operacional Remoto – 2006-2011 (Projetado)*

## Esforço de exploração versus matriz de recompensa potencial

Todos os dias, enquanto o X-Force rastreia as divulgações de vulnerabilidade, nós decidimos sobre quais vulnerabilidades necessitam uma investigação mais profunda com um olho na direção da abrangência do produto e quais as vulnerabilidades são menos prováveis de serem exploradas livremente. A matriz de probabilidade de exploração oferece uma abstração da linha de pensamento que aplicamos ao fazer estas escolhas. Isso funciona tentando mapear a oportunidade que cada vulnerabilidade representa para os invasores a partir de uma perspectiva financeira. No eixo X, mapeamos o custo associado com a exploração de vulnerabilidade, forçando-o a cometer um crime na rede. Vulnerabilidades que se encaixam facilmente em um processo existente e que os invasores possuem por invadir sistemas de computador de alta pontuação nesta dimensão. As vulnerabilidades que são difíceis de explorar ou que requerem que os invasores desenvolvam novos processos ao redor delas têm pontuação baixa. No eixo Y, mapeamos a oportunidade geral que uma vulnerabilidade representa para os invasores que a exploram – quantos sistemas na Internet estão vulneráveis e quais os tipos de dados que eles hospedam? Qual valor pode ser extraído pela exploração desta vulnerabilidade?

Um gráfico destes dois eixos é dividido em quatro quadrantes. O primeiro quadrante representa as vulnerabilidades que são relativamente baratas para explorar e representam uma grande oportunidade para os invasores. Estas representa exatamente o tipo de vulnerabilidade que provavelmente são vistas em explorações predominantes. O segundo quadrante representa as vulnerabilidades que têm valor alto, mas são difíceis de explorar – casos que podem ser visados por invasores mais sofisticados, mas menos prováveis de se ver em uma exploração predominante. O terceiro quadrante representa vulnerabilidades de valor baixo e custo alto que são improváveis de serem visadas amplamente. O quarto quadrante representa as vulnerabilidades de valor e custo inferiores, que são algumas vezes visados se forem fáceis o suficiente para os invasores.


*Figura 41: Esforço de Exploração versus Recompensa Potencial – 1S 2011*

No primeiro semestre de 2011, o X-Force publicou 24 **alertas e relatórios** de vulnerabilidade, destacando as mais críticas divulgadas durante este período a partir de nossa perspectiva. Colocamos 12 destas vulnerabilidades no primeiro quadrante – vulnerabilidades de valor alto que são baratas de serem exploradas. De fato, há explorações publicamente disponíveis para nove destas 12. Quase todas estas vulnerabilidades representam vulnerabilidades de execução de código remoto de software de cliente que são exploráveis por servidores de web maliciosos através do navegador ou pelo ambiente do navegador. Estas vulnerabilidades se enquadram diretamente na abordagem conduzida por download atraindo as vítimas para websites maliciosos que têm sido o padrão de um grande acordo de atividade de ataque nos últimos anos. Uma exceção interessante é uma vulnerabilidade de cross-site scripting do lado do cliente no Internet Explorer (**CVE-2011-0096**) que poderia ser utilizado para roubar os cookies necessários para acessar websites seguros mesmo se esses próprios websites não tiver uma vulnerabilidade inerente de cross-site scripting.

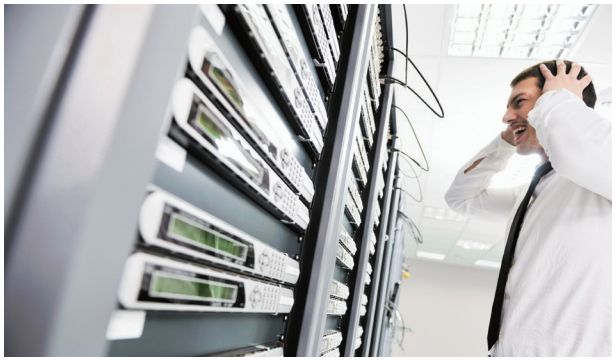
Colocamos nove vulnerabilidades no segundo quadrante – mais difícil de explorar e com alto valor. Esta porcentagem é raramente alta versus publicações anteriores de matriz de probabilidade de exploração. Duas destas são as vulnerabilidades do Adobe Shockwave (**CVE-2010-4306** e **CVE-2010-4307**) – exploráveis com um website malicioso, que foi descoberto por pesquisadores X-Force. Esperemos que a nossa descoberta precoce e coordenação dessas vulnerabilidades com o distribuidor tenha desencorajado os invasores de tê-los como alvo. Quatro dos nove estão nesta categoria por envolverem a definição de servidor malicioso que não é um servidor da web (como um servidor DNS ou servidor de arquivo). Pode ser relativamente fácil conseguir que as vítimas acessem vários tipos de servidores maliciosos incorporando as solicitações em conteúdo HTML que as vítimas estejam acessando. Isto é um pouco mais complicado do que simplesmente hospedar um conteúdo malicioso em um servidor web e a principal atividade de ataque favorecer o modelo em seu lugar.

As outras três vulnerabilidades no segundo quadrante são graves, as vulnerabilidades de execução de código remoto do lado do servidor que poderiam ter sido exploradas por worms auto-replicante da Internet. Não temos visto explorações públicas surgirem por qualquer destas três vulnerabilidades, apesar de seu valor extremamente alto. Sabemos de uma exploração privada para uma destas vulnerabilidades que foram desenvolvidas por dois ex-Pesquisadores X-Force, mas não foi divulgado publicamente, e a dificuldade técnica associada à execução do código de alcance neste caso foi relativamente alto. (Consulte o trabalho de Chris Valasek **Entendendo o Agrupamento de baixa Fragmentação** de Blackhat 2010.) Ao longo dos últimos anos, os desenvolvedores de sistema de gerenciamento de memória criaram uma ampla gama de recursos de prevenção de exploração que protegem graves vulnerabilidades de serem exploradas. Embora alguns dos melhores pesquisadores de vulnerabilidade do mundo encontraram modos de passar por estes mecanismos de proteção, o fato que vulnerabilidades de valor extremamente alto como estas podem agora permanecer meses sem as explorações publicamente emergentes provavelmente significa que estes recursos de segurança de gerenciamento de memória estão tendo um impacto mensurável sobre a segurança da Internet.

Colocamos três vulnerabilidades no quarto quadrante, as vulnerabilidades que são facilmente exploradas além de ter valor baixo. Todas essas são vulnerabilidades de negação de serviço nos serviços da Internet. Ataques de negação de serviço podem ter um impacto grave sobre as operações da rede, então é apropriado publicar alertas sobre estas questões. Entretanto, elas são obviamente menos valiosas para os invasores do que as vulnerabilidades de execução de código remoto, e então as classificamos adequadamente. Na verdade, descobrimos que a maioria das negações de atividade de serviço na Internet envolve tráfego distribuído em demasia em vez da exploração de vulnerabilidades específicas.

## Gerenciamento dos terminais: visibilidade e conformidade contínuas de patch

Os ataques de malware continuam rapidamente a explorar sistemas de computador vulneráveis antes que as correções sejam publicadas por distribuidores de software e aplicados pelos clientes. Estes ataques podem causar a perda da produtividade corporativa, risco de perda de dados confidenciais, e possível litígio e multas, custando à economia dos EUA uma estimativa de 266 bilhões de dólares anualmente, de acordo com o Instituto de Segurança Cibernética, um grupo de advogados com base em Washington, D.C.



Embora, geralmente o distribuidores estejam atentos para fornecer as correções e estejam emitindo mais e mais correções para tratar das vulnerabilidades, a maioria das organizações levam semanas ou até meses para desenvolvê-las por todo o ambiente. De acordo com algumas estimativas, as organizações podem levar até quatro meses para obter uma taxa de 90 a 95% de conformidade de correção.

Apesar dos riscos, algumas organizações são lentas para fazer as correções devido à grande complexidade e as barreiras que encontram ao implantar práticas de gerenciamento de correção eficaz. O tempo e o trabalho envolvido, falta de visibilidade, impacto do negócio potencial, restrições de largura de banda da rede, falta de gerenciabilidade, longas horas de correção, questões de escalabilidade, ambientes heterogêneos e terminais em roaming são apenas alguns dos obstáculos que podem ser encontrados.

Com software e as ameaças contra tais softwares em constante evolução, as organizações devem ter um modo eficaz de avaliar, implantar e gerenciar um fluxo constante de correções para diversos sistemas operacionais e aplicativos em seus ambientes heterogêneos.

### Alterando o paradigma de gerenciamento de correção

Enquanto não há uma única prática oficial melhor para gerenciar uma correção, a abordagem geral engloba um processo de ciclo fechado com seis etapas básicas: pesquisar, avaliar, corrigir, confirmar, reforçar e relatar. Historicamente, muitas destas etapas foram implementadas via tecnologia separada não integrada, tornando virtualmente impossível criar um processo de gerenciamento de correção de ciclo fechado em tempo real.

**Passo 1: Pesquisa**

A primeira etapa no processo de gerenciamento de correção envolve a descoberta de quais correções estão disponíveis e então avaliar e testá-las para compatibilidade dentro do ambiente organizacional. Se não automatizado, este processo pode consumir uma quantidade significativa de tempo e recursos. Aceitar as atualizações automáticas do distribuidor sem testá-las pode colocar as organizações em grande risco, desde que não há controle corporativo em relação a tempo ou relatório. Confiar nos usuários para aplicar as atualizações pode ser arriscado e não confiável.

As soluções de gerenciamento de correção que adquirem, testam e distribuem automaticamente as correções de distribuidores de sistema operacional, anti-malware e aplicativos terceirizados diretamente para que os clientes possam remover a pesquisa extra de gerenciamento de correção. Quando as novas correções são recebidas, elas devem ser analisadas e implantadas de acordo com políticas altamente granulares que contém informações como dependências, sistemas aplicáveis e nível de gravidade das correções. A implantação deve visar perfis específicos de máquinas, para que as correções específicas sejam enviadas apenas para os terminais que precisam delas.

**Passo 2: Avaliar**

Para cada correção identificada, a organização de TI deve determinar a aplicabilidade e criticidade da atualização. Desde que muitas correções são urgentes, e o processo de avaliação de risco e a prioritização de correção deve

acontecer o mais rápido possível, é importante para as organizações terem acesso aos ativos correntes e completos e ao conjunto de dados de configuração para quantificar o escopo e o impacto das correções pela organização. Existem ferramentas que podem ajudar a adquirir os dados, mas podem levar dias ou semanas para coletar os dados após varrer cada terminal.

A monitoração contínua dos terminais e relatórios sobre seus estados, configuração e estado de conformidade com as políticas definidas como níveis obrigatórios de correção e configurações padrões são altamente recomendados. Esta informação é especialmente crítica durante cenários de correção de emergência quando um distribuidor lança correções de alta prioridade entregues fora da programação regular e as organizações precisam responder rapidamente.

Assim que a quantidade total de correções é mapeada para os terminais que precisam delas, e o nível crítico do negócio é definido, a organização de TI pode dar prosseguimento à etapa de correção.

**Passo 3: Corrigir**
Geralmente, a correção é difícil de ser concluída rapidamente em escala organizacional devido a muitas razões. Entre algumas destas razões estão os pré-requisitos determinantes de correção, que garantem que a correção é segura, a capacidade da rede e pular inadvertidamente certos terminais, tais como aqueles que, atualmente, não estão ligados à rede corporativa Todos estes fatores podem resultar em taxas baixas de correção no primeiro acesso.

Além disso, muitas ferramentas não fornecem controles com base em políticas refinadas para implantar com eficiência correções para todos os terminais afetados. Controles como janelas de instalação de tempo de correção, se um usuário deve estar presente ou não, opções de reinicialização, método de distribuição, tipo de sistema, e as opções de notificação do usuário devem ser entradas disponíveis para o processo de atualização automática.

Um relatório abrangente pode ajudar as organizações determinarem quais os terminais que precisam ser atualizados. Os operadores podem então determinar quando a correção deve sair, qual notificação exibir para os usuários finais (caso houver), se permitir ou não aos usuários atrasar uma implantação de correção e por quanto tempo, e se forçar (ou atrasar) as reinicializações.

Uma vez determinado que a correção é aplicável a um terminal em particular, pode ser baixada e aplicada enquanto relata o sucesso ou falha. Com as soluções de gerenciamento de terminal que podem facilmente alcançar os dispositivos conectados à Internet, a carga da rede pode ser significantemente reduzida e as taxas de sucesso no primeiro acesso podem melhorar 95%.

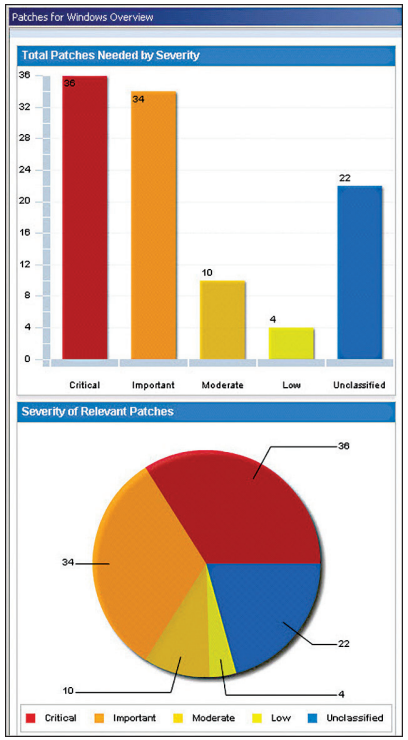
Para ajudar a garantir uma maior segurança, deve-se empregar apenas identidades criptografadas. Isto ajuda a garantir que apenas administradores autorizados possam criar e distribuir as correções.

**Passo 4: Confirmar**
Após a aplicação das correções, deve-se confirmar a instalação bem sucedida em todos os terminais para que TI saiba quando o ciclo de correção está completo. Estes dados devem ser comunicados a um sistema de relatório central que atualiza a equipe sobre o processo, incluindo exceções, em tempo real. Esta etapa é crítica nos requerimentos de conformidade de suporte, que necessitam de uma prova definitiva da instalação da correção e para encerrar o ciclo do gerenciamento da correção.

**Passo 5: Reforçar**
Se uma correção não for instalada por alguma razão (os usuários intencional ou acidentalmente desinstalam correções, novos aplicativos ou correções que corrompem as atualizações existentes, malware que deliberadamente removem as correções), a política pode especificar que a correção deve ser automaticamente reaplicada aos terminais conforme necessário. Em caso de problemas com uma correção, os administradores devem rápida e facilmente emitir um retorno aos terminais. Se o estado de conformidade do terminal for relatado em tempo real, os administradores de TI podem facilmente controlar e monitorar o estado de todos os terminais gerenciados.

### Passo 6: Relatório

O relatório é um componente crítico do processo de gerenciamento da correção. As políticas corporativas e de conformidade geralmente necessitam de painéis atualizados e altamente detalhados e relatórios que indicam a posição de risco da organização e o estado de gerenciamento da correção para vários consumidores, incluindo auditores de conformidade, executivos, gerência e até mesmo usuários finais.




*Relatórios mostram o progresso do gerenciamento de correção em tempo real*

## Implementação do IBM CIO da solução de gerenciamento de correção

A IBM precisa proteger sua infraestrutura interna, que abrange mais de 425 mil funcionários, exatamente como qualquer outra organização atualmente. Ao mesmo tempo, os modelos de negócio em evolução da IBM têm aumentado o desafio de manter os terminais e infraestruturas da UIBM, e a quantidade de terminais atípicos da IBM.

A IBM começou uma implantação mundial interna do Tivoli Endpoint Manager. Ao mesmo tempo que este documento era publicado, a IBM implantava o Tivoli Endpoint Manager para mais de 550 mil terminais em seis meses, de um total de 750 mil terminais Windows, Mac e Linux com objetivo de implantação até o final de 2011. A IBM estimava que pode reduzir os problemas de segurança de estações de trabalho por 50% no primeiro ano, uma economia de 10 milhões de dólares.

## Resumo

As abordagens do gerenciamento tradicional de correção que utilizam os processos manuais e varredura confusa – e mecanismos com base em pesquisa geralmente não são mais rápidas e econômicas o suficiente para cumprir os requerimentos regulatórios e de negócios, deixando as organizações com inaceitáveis riscos e custos altos. Quando os distribuidores apresentam ciclos regulares de lançamento de correção, os invasores aproveitam a oportunidade para explorar os terminais não corrigidos sem ter de trabalhar para revelar novas vulnerabilidades.

Soluções eficazes que automatizam as tarefas de gerenciamento de correção e suportam um processo de ciclo fechado podem ajudar as organizações a aumentar drasticamente as taxas de sucesso de correção, melhorar a conformidade regulamentar e reduzir os gastos.

## Acesso de usuário e ameaça interna

Quanto mais e mais aplicativos de negócios adotam a Web como plataforma preferida e como os usuários na web crescem cerca de 35 a 45% ano após ano, os riscos de seguranças expostos pelos aplicativos de web podem assumir proporções não vistas até aqui no mundo atual. Enquanto as altas ameaças de risco na forma de SQL Injection e cross-site scripting levam às vulnerabilidades de Aplicativos Web, alguns estudos associam as vulnerabilidades comuns às ameaças internas como arriscadas. As vulnerabilidades com base interna incluem vulnerabilidades relacionadas à "Autenticação Quebrada e Gerenciamento de Sessão", especialmente a partir de interações e compartilhamento de computador entre internos (funcionários) tendem a ser muito mais predominantes do que usuários externos. Estes casos onde usuários ou anônimos alavancam falhas na autenticação de usuário ou capacidades de gerenciamento de sessão de aplicativos alvo para representar os usuários genuínos e roubar ou modificar dados críticos de negócios.

### Causa primária

Muitas organizações tendem a ter aplicativos web com autenticação personalizada e capacidades de gerenciamento de sessão construídos como funções internas pelos próprios desenvolvedores de aplicativos. Geralmente, tais desenvolvedores de aplicativos não são especializados em soluções de segurança e por esta razão os módulos de segurança e acesso nestes aplicativos podem conter falhas/vulnerabilidades em áreas críticas tais como gerenciamento de senhas, gerenciamento de política de segurança, interrupções e gerenciamento de sessão. Desde que, frequentemente, as estruturas, os métodos e as tecnologias utilizadas em implantações de segurança diferem de aplicativo para aplicativo, testar e revisar os códigos que falham com frequência na detecção de muitas vulnerabilidades associadas a eles.

### Cenário típico de ataque

Considere um aplicativo que não possui uma capacidade de intervalo de sessão adequado. Se um usuário utilizar um computador compartilhado para acessar o aplicativo e deixá-lo sem fazer o logout adequado, os próximos usuários podem ser capazes de utilizar a sessão para realizar transações adicionais. O que fica agravado se a sessão permanece aberta por longos períodos na ausência de uma interrupção de sessão por inatividade adequada.

Considere um aplicativo online que suporta URL re-escrita, incluindo assim a sessão de ID na URL. Se um usuário, após uma transação específica, compartilhar o link, o destinatário poderia fazer mau uso do ID da sessão realizando transações adicionais.

### Soluções típicas adotadas por corporações

Considerando a gravidade das vulnerabilidades relacionadas à Autenticação Quebrada e ao Gerenciamento de Sessão e a enormidade das perdas associadas aos negócios, as organizações de hoje em dia atribuem grande importância para permitir mecanismos de segurança sólida e controle de acesso para seus aplicativos web. Apesar disto, a categoria de vulnerabilidade de aplicativo web subiu quatro posições no relatório OWASP (Open Web Application Security Project) 2010 das dez maiores vulnerabilidades em comparação com sua edição anterior.

Uma abordagem comumente utilizada para combater isto é externalizar o acesso e as funções de gerenciamento de sessão a partir de aplicativos web e o uso de uma solução especializada para manusear estas funções para todos os aplicativos web utilizados pela organização. Estas soluções especializadas em acesso web seriam construídas por peritos em segurança ou adquirido de distribuidores competentes. Os recursos adicionais como gate-keeping centralizado e Single Sign-On ajudam a reduzir as ameaças internas.

# Seção III
# Desenvolvendo Software Seguro

Na seção Desenvolvendo Software Seguro do relatório, os dados são apresentados em processos e técnicas para a criação de software seguro. Discutimos como as empresas podem encontrar as vulnerabilidades existentes e ajudar a evitar que novas sejam apresentadas. Se você utiliza aplicativos web ou em rede para coletar ou trocar dados confidenciais, seu trabalho como profissional de segurança agora é mais difícil do que jamais foi. Damos uma olhada nos testes de segurança estático e dinâmico feitos pelo grupo Rational AppScan em todos os estágios de desenvolvimento de aplicativos e compartilhamos os detalhes do que descobrimos.

## Mais detalhes sobre a análise híbrida do código JavaScript do lado do cliente

No primeiro semestre de 2011, o IBM's Rational Application Security Group continuou aprimorando, evoluindo e focando suas pesquisar na predominância das vulnerabilidades do JavaScript do lado do clienente em aplicativos Web 2.0. Esta pesquisa tem como base uma tecnologia única chamada **JavaScript Security Analyzer (JSA)**, que está disponível como parte de **IBM Rational AppScan Standard Edition**. A JSA realiza análise híbrida do código do lado do cliente, aplicando análise estática sobre os códigos JavaScript e HTML coletados de páginas web e extraídos por um processo profundo de rastreamento web automático (análise dinâmica).

Semelhante à pesquisa anterior, utilizamos um conjunto de amostra de 678 websites, incluindo os websites da Fortune 500, e uma lista dos 178 websites mais populares como redes sociais e sites de mídia. A pesquisa utilizou uma versão recente da tecnologia JSA, que inclui algoritmos superiores de análise e aprimoramento para reduzir a suscetibilidade para resultados com ruídos. Podendo resultar em uma taxa inferior de falso positivo. O resultado da pesquisa mostrou um aumento dramático na quantidade de vulnerabilidades que poderiam ser detectadas.

**Realizando a revisão manual de código para JavaScript moderno não é uma tarefa simples!**

Desde a realização desta pesquisa com os mesmos dados de website que a pesquisa anterior, a diferença nos resultados pode ser atribuída a uma precisão mais alta no aprimoramento dos algoritmos JSA. Tabela 10 mostra a descoberta de nossa atual pesquisa de que de 678 websites, 40% (271 sites) contém vulnerabilidades JavaScript do lado do cliente.

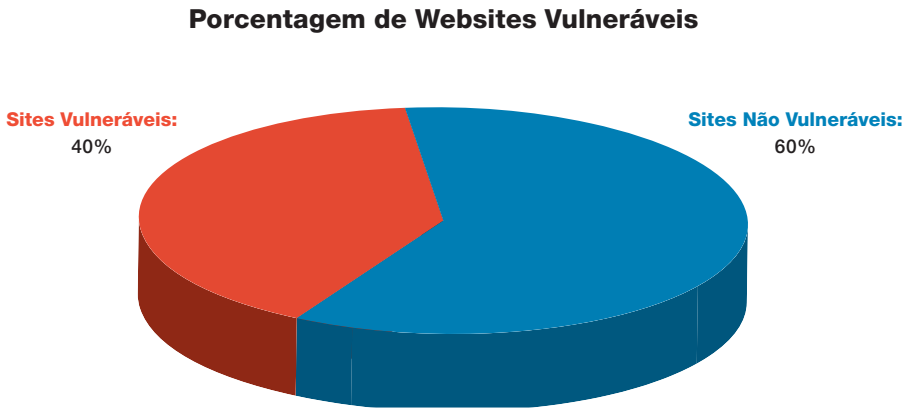



*Figura 42: Porcentagem de websites vulneráveis*

| | |
|---|---|
| **Total de Sites Examinados** | 678 |
| **Total de Problemas Encontrados** | 3683 |
| Sites vulneráveis (quantidade) | **271** |
| Sites vulneráveis | **40%** |
| Sites não vulneráveis | **60%** |
| Sites não vulneráveis (quantidade) | **407** |
| Aplicativos com problemas no código externo | 90% |
| Aplicativos com problemas apenas no código interno | 10% |
| Sites vulneráveis para XSS com base em DOM | 252 |
| Total de problemas encontrados de XSS com base em DOM | 3214 |
| Sites vulneráveis para Redirecionamento Aberto | 226 |
| Total de problemas encontrados de Redirecionamento Aberto | 266 |
| Sites vulneráveis à mistificação de Atributo de email com base em DOM | 5 |
| Total de problemas encontrados com Mistificação de Atributo de email com base em DOM | 203 |

*Tabela 10: Detalhamento do total de sites examinados*

| Tipos de Problemas | Sites Vulneráveis | Total de Problemas |
|---|---|---|
| XSS com base em DOM | 252 | 3214 |
| Redirecionamento Aberto | 226 | 266 |
| Mistificação de Atributo de email com base em DOM | 5 | 203 |
| **Total de Problemas Encontrados** | | **3683** |

*Tabela 11: Visão geral do total de problemas descobertos*

Na Figura 43, vemos que, dos aplicativos vulneráveis, 90%* incluiam uma ou mais vulnerabilidades que foram introduzidas por código JavaScript de terceiros, como campanha de marketing, código que inclui animação em Flash, e bibliotecas AJAX.

*** Observação:** As estatísticas na Figura 43 (Porcentagem de sites que incluem uma vulnerabilidade no código terceirizado do lado do cliente) são diferentes das estatísticas apresentadas nos resultados de nossa pesquisa anterior, que contava a quantidade de problemas de terceiros a partir dos tipos de problemas totais.

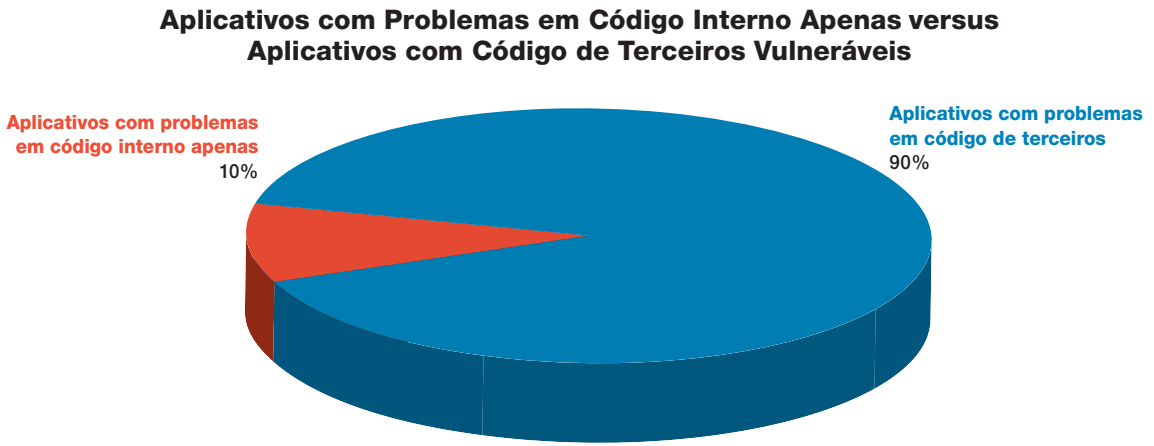



*Figura 43: Aplicativos com Problemas Apenas para Códigos Internos vs. Aplicativos com Código de Terceiro Vulnerável*

Figura 44 mostra que cross-site scripting com base em DOM (3.214 problemas de 3.683) ainda é o principal tipo de problema de segurança mais comum. Parece que a quantidade de sites vulneráveis ao cross-site (252) scripting com base em DOM e sites vulneráveis para redirecionamento aberto do lado do cliente (226) são bem semelhantes.

Além disso, um novo tipo de vulnerabilidade foi detectado pela primeira vez: Mistificação de Atributo de email com base em DOM. Esta vulnerabilidade ocorre quando um aplicativo web utiliza código JavaScript para criar automaticamente um email para o usuário preencher e enviar, utilizando dados controlados pelo usuário. Em tais cenários, um invasor poderia potencialmente manipular o conteúdo, assunto ou campos CC ou BCC do email, resultando no vazamento de informações privadas.

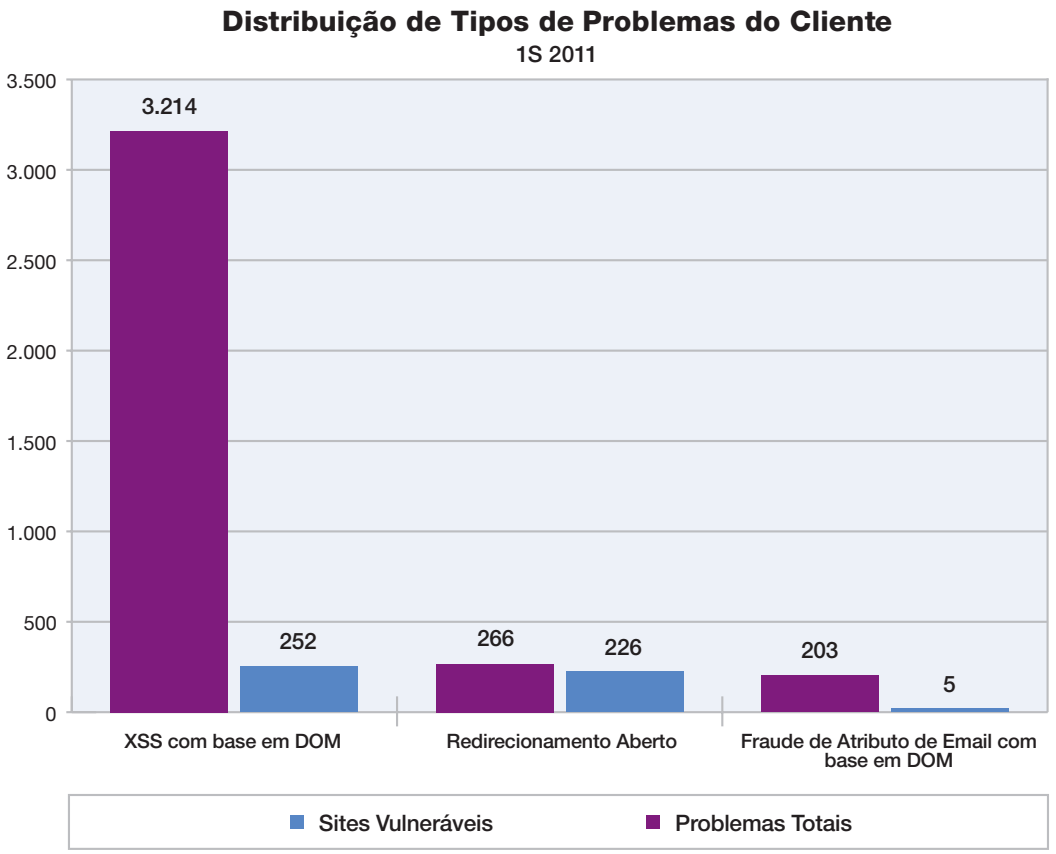



*Figura 44: Distribuição de Tipos de Problemas do Lado do Cliente – 1S 2011*

# Seção IV
# Tendências Emergentes em Segurança

A seção Tendências Emergentes em Segurança dá uma olhada na tecnologia de rápido desenvolvimento que exige que as empresas considerem se é momento de investir nestas áreas futuras ou não. Explicamos onde as ameaças e explorações estão sendo utilizados nessas adoções precoces de tecnologia e como as empresas podem ficar focadas.

## Malware de móvel

Os sistemas operacionais móveis, tais como o Google's Android, estão se tornando um alvo popular para os autores de malware. Entretanto, o malware móvel não é um fenômeno novo. Acredita-se que o primeiro malware de telefonia móvel seja o Cabir, que foi descoberto em 2004 e afetou telefones que executavam o SymbianOS. O Android OS estreou em 2008, e o primeiro malware Android conhecido foi descoberto em 2010. Este malware, duplicava FakePlayer, fazendo com que os telefones infectados enviassem mensagens SMS com cobranças em dinheiro para o usuário. Em 2011, o malware DroidDream foi a primeira infecção difundida hospedada no próprio mercado de aplicativos Google. Como os smartphones estão se tornando cada vez mais onipresentes, esperamos que a ameaça de malware móvel aumente.

## Dispositivos móveis como plataforma de malware

Os telefones celulares são uma plataforma atraente para os desenvolvedores de malware por várias razões. Primeiro por que é fácil rentabilizar uma infecção de telefone celular. Os distribuidores de malware podem configurar serviços premium de SMS que cobram dos usuários que enviam mensagens SMS para um número específico. A maioria dos malwares que vimos no Android e outras plataformas móveis aproveitam-se disto e enviam mensagens SMS a partir de um telefone infectado. Segundo, os celulares geralmente possuem vulnerabilidades não corrigidas. Enquanto que a segurança é um foco principal para o Android, várias vulnerabilidades de intensificação de privilégios foram descobertos que podem conceder um acesso raíz para aplicativos maliciosos. Até mesmo quando a vulnerabilidade é encontrada e corrigida, ainda existem dispositivos livres e não corrigidos. Muitos distribuidores de celulares não forçam as atualizações de segurança para seus dispositivos. Terceiro, os celulares são um alvo atraente por causa do tamanho grande da base do usuário. No final de junho de 2011, o Google alegou que havia 500 mil novas ativações de dispositivos Android por dia.

## Modelo de distribuição de malware de Android

Um dos mais populares e eficazes modos de distribuir malware de Android é através dos mercados de aplicativos. Além do próprio mercado oficial do Google, há muitos mercados não oficiais de terceiros. Há mas duas técnicas diferentes que os autores de malware utilizam para convencer as pessoas a baixar seus aplicativos. O primeiro método, utilizado pelo malware DroidDream, é criar versões infectadas de softwares existentes no mercado. Então, estas versões infectadas são enviadas com um nome muito parecido ao do software original, e os usuários baixam e instalam inadvertidamente a versão infectada. Outro truque para atrair as vítimas é publicar software que alega ser um crack, correção ou dica para outro software. Uma família de malware apelidada de Plankton utilizou este método; estava disfarçada como uma dica para o jogo Angry Birds.

Embora, os mercados de aplicativos não serem o único caminho para distribuir malware Android. Temos visto aplicativos infectados em redes ponto a ponto, hospedados em websites e até mesmo em Usenet. Geralmente, estes aplicativos de fora do mercado visam pessoas que procuram por versões piratas de aplicativos comerciais Android.

## Recursos de malware de Android

Uma vez que o malware estiver instalado em um celular, muito dano pode ser feito. Um explorador de raiz poderia ser utilizado para aumentar os privilégios e darem ao malware total acesso ao telefone. Mesmo sem o acesso raiz, o malware é capaz de fazer qualquer coisa dentro dos limites de permissões que o usuário conceda a ele.

Quando um aplicativo Android é instalado por um usuário final, as permissões necessárias são exibidas para o usuário poder verificar o que o aplicativo faz. Por exemplo, se um aplicativo precisa enviar mensagens SMS ou ler contas armazenadas no celular, o usuário pode decidir dar a permissão antes da instalação. Caso o usuário não queria conceder tais permissões, o aplicativo não é instalado. Se um usuário não é cuidado ao verificar as permissões, pode-se instalar aplicativos fraudulentos que necessitam de mais permissões do que o aplicativo original precisaria – como a capacidade de enviar mensagens SMS. O malware GoldDream, descoberto pelos pesquisadores na Universidade do Estado da Carolina do Norte em julho de 2011, foi distribuído como versões de cavalos de tróia de jogos existentes em mercados não oficiais de aplicativos chineses. Supunha-se que um exemplo em particular era de um jogo chamado "Blood vs Zombie" que na realidade era uma cópia de um

jogo real, “Draw Slasher”, mas incluia uma grande quantidade de permissões extras que permitiam o roubo de informações do usuário. Em comparação com as permissões necessárias entre o jogo infetado pelo malware e o legítimo, consulte as Figuras 45 e 46 abaixo.

Além de enviar mensagens SMS, o malware de Android foi observado coletando dados pessoais do telefone e enviando-os de volta para um servidor central. Estas informações poderiam ser utilizadas em ataques phishing ou para roubo de identidade. Também vimos que o malware para Android pode ser controlado remotamente por um comando remoto e um servidor de controle – assim como um bot que infecta uma máquina com Windows.

Como as plataformas móveis se tornaram mais poderosas, elas começa a ganhar recursos de computador desktop. Estes recursos ajudam a tornar as plataformas móveis um pouco mais atraentes para autores de malware.

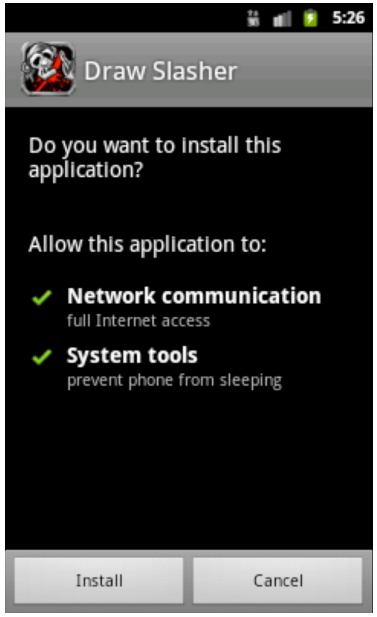



*Figura 45: Draw Slasher, um jogo legítimo que necessita de permissão mínima*

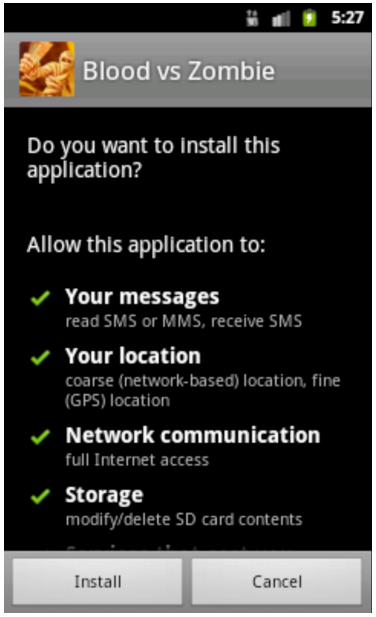



*Figura 46: Blood vs Zombie, uma cópia maliciosa de Draw Slasher que contém mais permissões do que um jogo deveria precisar – incluindo acesso de GPS e SMS.*

## Protegendo-se contra malware de Android

É possível evitar infecção com malware de Android pelo bom senso ao instalar os aplicativos. Primeiro, fiquei com um mercado de aplicativos de boa reputação, como o Google Market oficial ou o mercado de aplicativos Android da Amazon. Ainda é possível que os malware entrem em um mercado oficial, então seja cuidadoso com os aplicativos que instalar. Verifique duas vezes as permissões e assegure-se de que está confortável com o nível de acesso que está dando aos aplicativos. Um jogo não deve exigir acesso de GPS ou SMS. Tenha cuidado, também, com o tipo de software que instalar. Tentar obter uma cópia gratuita de um aplicativo pago é um caminho certo para ser infectado. Outra dica é instalar apenas aplicativos que possuem um grande número de instalações (100 mil ou mais) com uma quantidade alta de comentários.

Certifique-se de executar um software de segurança no seu celular, independente de qual sistema operacional que ele possui. A maioria dos principais distribuidores de software de antivírus possuem versões móveis de seus produtos que podem protegê-lo de muitos tipos de malware.

## Transformação na corporação com dispositivos terminais móveis

Ao longo dos dois últimos anos, muitas empresas têm continuado apenas com os tradicionais Blackberries, principal ou exclusivamente programas de smartphones de empresas confiáveis para aquelas onde pelo menos um número limitado de smartphones e tablets estão executando sistemas operacionais não-Blackberry com diferentes níveis de acesso da empresa. Em muitos casos, esta progressão tem ocorrido em resposta a uma combinação das necessidades de executivos e funcionários, combinadas com percepção de que a tendência é cada vez mais cara para evitá-la ao invés de adotá-la. Pelo menos algumas das principais plataformas de smartphones de consumidores amadureceram para incluir pelo menos uma segurança mínima e funcionalidade de gerenciamento necessária para permitir esta progressão na empresa.

Esta tendência de transformação varia significativamente por vários setores do mercado. As corporações com requisitos de aplicativos combinados com requisitos de dados de aplicativos que se estendem para dados regulamentados ainda são desafiados pelos controles de segurança em alguns sistemas operacionais móveis. Contudo, para as corporações com quantidades limitadas de dados regulamentados, a transformação claramente está em andamento.

Com esta tendência, tem se tornado cada vez mais importante planejar estrategicamente expansões crescentes pois o modelo de computação "normal" está obscurecendo a diferença entre smartphones, tablets e computadores pessoais. Enquanto eles podem parecer diferentes e separados agora, o gerenciamento de segurança corporativa lutará para manejar a expansão com a convergência do gerenciamento da configuração da segurança do terminal.

Atualmente, na maioria das empresas, o gerenciamento de configurações de segurança de computadores pessoais (geralmente laptops e desktops com uma pequena quantidade de tablets com base Windows) são completamente separados e diferentes dos smartphones. Principalmente por ter como base o legado dos Blackberry Enterprise Servers como plataforma de gerenciamento exigida nos celulares corporativos existentes. Enquanto tudo funcionava em um modelo de terminal simples que incluía apenas PCs e Blackberries, este modelo provavelmente se tornará pesado à medida que mais plataformas de smartphone são suportadas. Embora muitas das soluções MDM de smartphones atualmente sejam plataformas cruzadas, ainda há espaços enquanto os tablets entram em uso juntamente com os Blackberries. Além disso, a maioria dos programas de smartphones não Blackberry são relativamente limitados e pequenos em comparação aos programas de computadores pessoais. Se as tendências atuais continuarem, será comum para a maioria dos funcionários também utilizarem um smartphone e tablet quando estiverem longe de suas mesas. Neste modelo de computação corporativa, os funcionários terão vários dispositivos com uma mistura de responsabilidade de financiamento através do espectro.

Esta tendência transformacional deve conduzir a importância da convergência conforme aplica o gerenciamento de dispositivos de computação terminal. Provavelmente tudo variará de corporação para corporação, dependendo do apetite pelo risco, orçamento operacional e setor de negócios. Mas para quase tudo, esta diversidade e sobrecarga de tecnologia de gerenciamento apresenta um desafio.

## Convergência de gerenciamento de segurança de terminal

Quase todas as corporações serão afetadas por alguma forma de diferenciação de dispositivo de terminal, que continuará a conduzir a necessidade de convergência de gerenciamento de segurança.

Independentemente do apetite pelo risco, as corporações cada vez mais perseguirão um gerenciamento de segurança com base em funções. Esta necessidade dentro da corporação varia dependendo da diversidade de funções dentro da empresa bem como a variedade de classificações de dados de função para função. Em grandes corporações típicas, a maioria de dados confidenciais está sempre limitado a apenas quem necessita acessá-los (privilégio menor) e esta própria limitação pode levar a uma variação de segurança pelas funções. Idealmente, isto faz sentido – por que uma "segurança extra" para alguns dispositivos quando não é necessário. Segurança com base na função é um condutor primário em direção à convergência do gerenciamento de segurança dos terminais.

Derivado de um conjunto de papéis, cada um com requisitos de segurança que tem como base as classificações de dados associados com a função, esta abordagem é muito mais facilmente aplicada a uma mistura de dispositivos em um ambiente de convergência. Sem isso, a replicação do gerenciamento de funções é necessária por cada uma das infraestruturas de gerenciamento dos smartphones, tablets, e computadores pessoais correspondentes. Um sistema adequado de gerenciamento com base nas funções poderia orientar a instalação dos funcionários para dispositivos com configuração de segurança correspondente e todos os agentes de segurança necessários Isto pode ajudar a garantir que os funcionários não instalem aparelhos que não suportem os requisitos mínimos de proteção de dados associados com sua função. Tudo se torna ainda mais importante em um cenários de dispositivos de propriedade pessoal pois alguns dos dispositivos de funcionários podem não ser adequados para suportar os controles necessários para a função do funcionário. Neste caso, o funcionário e o dispositivo não devem ser instalados nos dados corporativos.

A complexidade de gerenciamento de dispositivos e custo é outra das forças condutoras em direção da convergência do gerenciamento de segurança. Enquanto, geralmente, as corporações estavam dispostas em investir em tecnologias diferentes para fornecer um uso seguro de smartphones, conforme se expande para incluir a maioria dos funcionários em toda a corporação usando aumento na quantidade de plataformas, a expansão da tecnologia associada pode se tornar inviável. Se não for acessível, certamente pode se tornar mais caro do que a seleção de tecnologias de gerenciamento de plataforma cruzada, convergente e estratégica. Idealmente, a empresa pode selecionar as tecnologias que melhor integram-se a seus serviços de diretório com base em funções, alavancando uma abordagem com base nas funções.

Custo de lado, a convergência do gerenciamento de segurança de terminal permite o gerenciamento uniforme de risco corporativo, bem como aumentou a disponibilidade de auditoria. Quanto menos ferramentas, consoles e relatórios necessários para ser bem gerenciado, mais provável que poderia resultar em eficiência. Isto é apenas bom senso: a expansão e a complexidade da tecnologia tornam mais difícil garantir que tudo é como deveria ser. Operacionalmente, a convergência simplifica a quantidade de esforços e conhecimentos necessários para manter tudo funcionando. A seleção de uma única ferramenta convergida deve melhorar a oportunidade da empresa para manter as habilidades profundas em nível de conhecimento que levam a uma implantação de auditoria pronta e melhor do tipo.

Um outro benefício para tudo isso, é fácil de desinstalar. Quando todos os dispositivos desde smartphones até tablets e computadores pessoais são gerenciados por uma única solução, tanto o processo de instalação como de desinstalação são simplificados e são mais prováveis de ocorrer como pretendidos. Isto estende-se a facilidade de integração para automatização se a empresa quer um processo de desinstalação automatizado.

Espera-se que as diferenças reais entre estes dispositivos de computação continuem a obscurecer até que se tornem uma continuidade da funcionalidade de seu bolso até seu desktop.

## Isolamento/separação de aplicativos e dados corporativos e de funcionários

Atualmente, muitas corporações permitem o uso de aparelhos de propriedade do funcionário e de responsabilidade financeira (onde o funcionário é responsável financeiramente pelo dispositivo versus a corporação). Isto não se estende a todas as corporações, particularmente aquelas nos setores financeiros e de saúde. A vontade de adotar os dispositivos de funcionários contrasta com o apetite por risco da organização, mas, ao invés de gastar dinheiro evitando o uso incorreto, as corporações deram um passo à frente para gerenciar os dispositivos dos funcionários de modo que cumpram com os requisitos de segurança corporativos.

Comumente, isto significa que os requisitos de segurança corporativos têm sido aplicados nos dispositivos de funcionários. Exemplos incluem o uso de uma senha corporativa compatível e limpar tentativas de acesso mal-sucedidas. Enquanto que inicialmente alguns funcionários recusavam, há casos de uso em que o gerenciamento corporativo de dispositivos de propriedade pessoal no modelo atual pode ser dominante. Sejamos realistas, inserir uma senha alfanumérica para pausar a música ou acessar um aplicativo pedômetro pressiona os limites com os quais os funcionários podem estar dispostos a conviver em termos de segurança corporativa em seu smartphone pessoal. Enquanto a recusa de hoje em dia vem de uma minoria de funcionários (enquanto que o modelo de consumerização se expande para incluir a maioria dos funcionários) se tornará uma necessidade estratégica para claramente separar o acesso dos aplicativos corporativos, dados associados e requisitos de controle de segurança de dados pessoais e aplicativos do funcionário.

Atualmente, muitas corporações financeiras e de saúde evitam o suporte de dispositivos de propriedade de funcionários por diversas razões. Estas razões vão desde a incapacidade de acessar os controles necessários nos dispositivos até preocupação em relação ao gerenciamento de ciclo de vida dos dados e até gerenciamento de incidente. Em alguns casos, as corporações precedem buscando soluções móveis virtualizadas para que os dados da corporação jamais acabem nos dispositivos. As soluções remotas de virtualização geralmente possuem seus próprios desafios como a necessidade de uma conectividade contínua e robusta.

Independente do setor do mercado (e o apetite por risco associado), a área em que praticamente todas as corporações possuem o mesmo objetivo são as soluções que permitem às corporações assegurarem dados e aplicativos corporativos, ao mesmo tempo em que permite ao funcionário determinar a segurança dos dados e aplicativos pessoais. Provavelmente, as abordagens irão variar do uso de contêineres criptografados seguros nos quais residem os dados e aplicativos corporativos até uma variedade das abordagens de virtualização local e remota. A virtualização pode incluir a capacidade de executar uma máquina virtual dedicada à corporação ou a extensão do desktop virtual atual ou abordagens de fluxo de aplicativos para tablets e smartphones.

Pelo fato deste ser um espaço totalmente aberto de solução para smartphones e tablets, devemos esperar ver uma variedade de abordagens. Da perspectiva de uso do funcionário, a solução de tecnologia subjacente é secundária; eles simplesmente querem determinar os controles de segurança para seu correio, fotos, música, vídeo e outros conteúdos pessoais. Enquanto que as corporações podem ver este requisito como sendo mais para a satisfação do funcionário que ajuda a possibilitar a consumerização (e a economia de custo da empresa), estas abordagens também devem melhorar muito o processo de desinstalação. Estas abordagens devem permitir a remoção dos dados e aplicativos corporativos sem destruir os arquivos do funcionário. A corporação não deve se preocupar em excluir fotos "únicas" que podem residir em um dispositivo do funcionário. Isso pode ser uma vitória tanto para o funcionário como para a corporação.

As soluções que permitem o isolamento e/ou separação ainda estão relativamente restritas e imaturas, mas o amadurecimento deve ocorrer rapidamente, tanto quanto aconteceu com as soluções MDM móveis nos últimos três anos. As corporações devem se esforçar para serem cuidadosas ao desenvolver a estratégia de como conseguirão esta separação. Isto pode facilitar uma identificação eficaz das soluções potenciais para piloto e teste.

## Superando a violação: tendências na segurança e conformidade do banco de dados

A vida para os profissionais de segurança costumava ser mais simples. Era possível impedir que estranhos acessassem seus dados estabelecendo defesas de perímetro como sistemas de firewalls e antivírus, e restringindo o acesso físico às máquinas que os processa. É possível ter guardas de segurança no local e verificação de identidade na entrada de seu datacenter corportativo.

No mundo interconectado de hoje, esse não é mais o caso, pois as fronteiras de nossa infraestrutura de negócios estão constantemente sendo ampliadas pela emergência de nuvem, mobilidade, negócios sociais, grandes dados e mais.

Para ser útil, os dados de uma empresa devem estar continuamente conectados aos seus cliente, parceiros de negócios e funcionários. O que pode expor dados confidenciais a ataques mais automatizados e visados do que antes. Por exemplo, agora estamos vendo vários ataques que facilmente contornam as defesas tradicionais de perímetro explorando as vulnerabilidades de aplicativos web como SQL Injection, ou alavancando credenciais administrativas para comprometer bancos de dados back-end. Apesar de mais atenção ser dada para assegurar as práticas de codificação, SQL Injection continua sendo o vetor de ataque favorito entre os grupos maliciosos como demonstrado pelos inúmeros ataques SQL Injection em massa que ocorreram nos últimos anos.

As defesas de perímetro também são ineficazes contra pessoas do grupo como funcionários descontentes ou fraudulentos, pois eles já estão "atrás do firewall". Nos mais atuais ambientes de TI, os usuários privilegiados como DBAs, desenvolvedores e pessoal terceirizado possuem acesso sem restrições à dados confidenciais, com pouco nenhum controle de monitoramento em relação às suas atividades.

De acordo com um grande estudo de violação, 92% de todos os registros comprometidos são roubados de servidores de banco de dados[23] – superando de longe outras fontes de vazamentos de dados confidenciais, tais como laptops roubados ou roubo de dados via email ou drives USB.

Não é surpresa de que os bancos de dados se tornaram um alvo importante para os invasores. Dados críticos utilizados para administrar nossas organizações – incluindo informações financeiras/ERP, de clientes, de funcionários e de propriedade intelectual como novos projetos de produtos – são armazenados em bancos de dados relacionais. Todos os principais aplicativos corporativos como SAP, PeopleSoft, Siebel e Cognos possuem sistemas comerciais DBMS em seu núcleo.

## O panorama de segurança de dados

De acordo com Forrester Research, mais de 75% das empresas não possuem um plano de segurança de banco de dados no local. A Forrester também estima que atualmente os DBAs passam menos do que 5% de seu tempo na segurança de bancos de dados.

Confrontando com estas realidades, muitas organizações agora estão vendo aumentar o foco nível C em controles apertados em relação às infraestruturas de aplicativos e bancos de dados. Em nossas conversas com clientes, vemos cinco dos principais condutores por trás destas iniciativas:

**Invasores** são altamente motivados em comprometer os bancos de dados com defesas fracas, com sindicatos do crime dispostos a pagar dinheiro vivo para obter informações pessoais roubadas de bancos de dados de cliente.

**Cyber-espionagem** visa propriedade intelectual (PI) como novos projetos de produtos, algoritmos, planos estratégicos e informações sobre recursos estratégicos como petróleo, energia e infraestrutura.

**Hacktivismo** é um fenômeno em que sites são atacados por razões políticas em vez de ganho financeiro. Ataques cibernéticos patrocinados pelo Estado também podem ser utilizados para apoiar objetivos políticos como obter informações pessoais para suprimir a dissidência interna.

**Ameaças internas** geralmente são consideradas a maior ameaça, pois os funcionários podem facilmente explorar o acesso legítimo para cometer fraude, baixar grandes quantidades de dados confidenciais ou proprietários, ou cometer atos de vandalismo como inserir bombas lógicas em bancos de dados críticos. O risco é especialmente alto para "superusuários" como administradores.

Requisitos de **Conformidade** estão em constante evolução e aumentando na complexidade, especialmente para organizações globais. Como resultado, reduzir custos através da simplificação dos processos de conformidade é um importante condutor financeiro para implantar novas tecnologias de segurança de banco de dados. Em particular, muitas organizações agora estão procurando substituir suas coletas ad hoc atuais de processos de conformidade manual com um conjunto único de controles centralizados, padronizados e automáticos para todos os seus principais aplicativos e mandatos de conformidade.

23 2010 Relatório de Investigações de Violação de Dados da Verizon Business.

## Dez melhores práticas para segurança e conformidade de banco de dados

Com base em nossos compromissos com as 1000 organizações Globais, as seguintes melhores práticas surgiram do fortalecimento da segurança e conformidade de banco de dados em ambientes corporativos:

**1. Descoberta.** Os dados não podem estar seguros se você não souber primeiramente que ele existe. É importante descobrir as localizações de dados confidenciais e ter um bom mapeamento dos ativos sensíveis. Incluindo exemplos de bancos de dados fraudulentos, dados confidenciais em bancos de dados, e relacionamento entre elementos de dados que podem torná-los mais confidenciais (como uma associação entre "Sobrenome" e Número de Inscrição na Previdência Social).

Também, não se esqueça dos dados não regulamentados como propriedade intelectual corporativa (PI) incluindo planos estratégicos, projetos de produtos, algoritmos e análises M&A que podem ser interessantes para invasores.

Finalmente, automatizar o processo de descoberta e executá-lo regularmente, pois a localização de dados confidenciais muda constantemente.

**2. Avaliar as vulnerabilidades e configurações.** É importante avaliar as configurações de acesso de bancos de dados para garantir que eles não possuem violações de segurança. Há muitas listas de verificação de melhores práticas para realizar tudo isso, como **Referências de Servidor de Banco de Dados CIS** e os **STIGs (Security Technical Implementation Guides) para bancos de dados** desenvolvidos pela DISA (U.S. Defense Information Services Agency).

Este processo inclui a verificação tanto do modo como o banco de dados é instalado no sistema operacional (por exemplo, verificar os privilégios de arquivo para arquivos e executáveis de configuração de banco de dados) e as opções de configuração dentro do próprio banco de dados (por exemplo, quantos logins incorretos resultam em bloqueio de conta ou permissões de verificação de várias funções no próprio banco de dados). Note que estas avaliações específicas do banco de dados não são comumente realizadas pelas soluções de avaliação de vulnerabilidade de rede. Verificar, também, se versões antiquadas de banco de dados com vulnerabilidades conhecidas não estão sendo executadas.

**3. Dificultar o banco de dados.** O resultado da avaliação de vulnerabilidade é geralmente um conjunto de recomendações específicas de configuração para serem consideradas como a próxima etapa. Outros elementos para dificultar, incluem a remoção de todas as funções de banco de dados e opções que não são utilizadas.

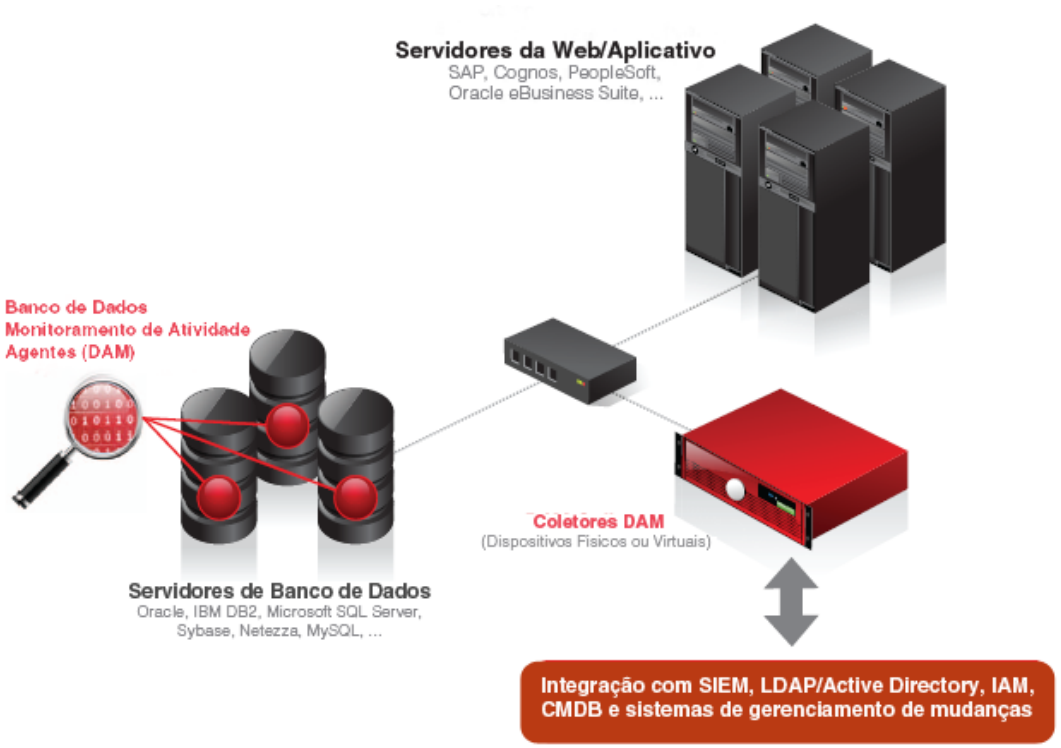
**4. Alterações de configuração de auditoria.** Uma vez estabelecida a configuração de dificuldade, é importante continuar a monitorar para ajudar a garantir que a configuração "de ouro" não seja alterada. O que pode ser feito com a alteração de ferramentas de auditoria que comparam capturas instantâneas das configurações (tanto em nível de sistema operacional e em nível de banco de dados) e então alertar imediatamente quando for feita uma alteração de configuração que possa afetar sua postura de segurança.

**5. Implantar Monitoração de Atividade de Banco de Dados (DAM) e Auditoria de Banco de Dados.**
Monitoração contínua e em tempo real (ver diagrama abaixo) é crucial para detectar rapidamente atividade não autorizada ou suspeita – tal como representante de serviço ao cliente baixando centenas de registros de dados confidenciais em um único dia – e restringindo a exposição de ataques e uso indevido.

É importante por que, de acordo com uma pesquisa recente de profissionais de banco de dados, 75% de organizações não consegue evitar que usuários privilegiados leiam ou adulterem os dados em seus bancos de dados, e quase metade disse que o usuário final com desktop comum ou ferramentas ad hoc poderiam tanto obter acesso direto não autorizado às informações confidenciais (ou não tinham certeza sobre isso).

Monitorar os usuários privilegiados também é importante para detectar invasões externas, desde que os ataques cibernéticos como SQL Injection frequentemente resultam no invasor obtendo controle de contas privilegiadas. O DAM também é um elemento essencial de avaliação de vulnerabilidade, pois vai além das avaliações estáticas tradicionais para incluir "vulnerabilidades comportamentais" ou dinâmicas enquanto que os usuários compartilham contas de serviços genéricos e outras credenciais privilegiadas.

Auditar o banco de dados permite que as organizações gerem uma trilha de auditoria não repudiável para todas as atividades de banco de dados que impactam a postura de segurança (como a criação de novas contas), integridade




**Tecnologias DAM (Database Activity Monitoring)** monitoram e auditam continuamente todo o tráfego do banco de dados para identificar rapidamente atividades suspeitas ou não autorizadas na camada do banco de dados.

**Os agentes DAM** residem em servidores de banco de dados e são utilizados para capturar todo o tráfego do banco de dados, incluindo atividades por usuários privilegiados como DBAs, desenvolvedores e equipes terceirizadas.

**Os coletores DAM** são utilizados para avaliar políticas de segurança de banco de dados em tempo real, armazenar uma trilha de auditoria segura do tráfego capturado, executar perícias de segurança em dados auditados e gerar relatórios de conformidade, relatórios de exceções de segurança e alertas em tempo real.

As soluções DAM podem fornecer recursos relacionados como bloqueio, avaliação de vulnerabilidade de banco de dados (p. ex., identificar sistemas não corrigidos, privilégios com configuração incorreta e contas padrão), descoberta de dados confidenciais, auditoria de configuração, relatório de autorização e monitoramento de camada de aplicativo para identificar fraude de usuário final em aplicativos corporativos multicamadas como SAP e Peoplesoft.

*Figura 47: Implantar Monitoração de Atividade de Banco de Dados (DAM) e Auditoria de Banco de Dados.*

de dados (como alteração valores ou esquemas de dados financeiros), ou privacidade e confidencialidade de dados (como visualizar Informações Identificáveis Pessoalmente ou PII). Além de ser um requisito importante de conformidade, as trilhas de auditorias granulares são importantes para as investigações forenses.

**6. Autenticar e controlar o acesso e gerenciar autorizações.** Autenticar, controlar o acesso e gerenciar as autorizações é essencial para ajudar a garantir totalmente os privilégios de gerenciamento e responsabilidade para limitar o acesso aos dados. Tais privilégios devem ser reforçados, mesmo para os principais usuários privilegiados de banco de dados. Recomenda-se também que revise periodicamente os relatórios de autorizações (também chamados de relatórios Certidão de Direito do Usuário) como parte de um processo de auditoria formal.

**7. Monitorar a camada de aplicativo.** As bem projetadas soluções DAM podem associar transações específicas de banco de dados realizadas pelo aplicativo com contas específicas do usuário final, para identificar deterministicamente os indivíduos que estão violando as políticas corporativas.

Além disso, combinando as informações da auditoria do banco de dados com os registros tradicionais de outros aplicativos e sistemas (como Windows, UNIX/Linux e firewalls) através de um sistema SIEM (Security Information and Event Management) para ver tudo o que o usuário tem feito, também pode fornecer informações críticas para investigações forenses.

**8. Criptografar.** Usar a criptografia para renderizar dados confidenciais ilegíveis, para que um invasor não obtenha acesso não autorizado aos dados de fora do banco de dados. Isto é mais facilmente obtido através da criptografia de dados em nível de arquivo, via sistema operacional, para evitar alterações caras e demoradas no aplicativo necessárias para encriptar em nível de campo na camada de banco de dados. A criptografia em nível de arquivo, quando combinada com monitoração granular em tempo real e controle de acesso na camada do banco de dados, é geralmente aceita como uma alternativa prática para a codificação em nível de coluna e um controle compensador para o Requisito 3.3 do PCI-DSS.

**9. Mascarar dados de teste.** De acordo com uma pesquisa recente da indústria, cerca de duas de cinco das organizações enviam dados de produção ao vivo para equipes de desenvolvimento e externas. Mascarar é uma tecnologia importante de banco de dados que de-identifica os dados de produção, substituindo-os com dados reais mas fictícios que, então, podem ser utilizados com o propósito de testar, treinar e desenvolver, pois é contextualmente apropriado para os dados substituídos da produção.

**10. Automatizar e padronizar os processos de conformidade.** As leis e regulamentações podem exigir a implantação de medidas de segurança de dados e provisões para ajudar a reduzir os riscos e vulnerabilidades para um nível razoável e apropriado. Obter a conformidade não é importante apenas por que ninguém gosta de falhar em uma auditoria, mas também fornece validação externa de que sua organização tenha implantado os controles adequados para ajudar a garantir a confidencialidade, integridade e disponibilidade de seus dados. Automatizar e padronizar os processos de conformidade é essencial para ajudar a reduzir os custos de conformidade, minimizar os exercícios de incêndio de auditoria de último minuto em sua organização e tratar das regulamentações em constante mudança.

## Por que as tecnologias de segurança existentes são insuficientes

As tecnologias de segurança tradicionais são blocos de construção essenciais para uma defesa por camadas, mas ao contrário das tecnologias específicas para banco de dados como DAM, elas não foram projetadas com conhecimento embutido sobre protocolos de banco de dados, estruturas, padrões de atividades e contexto que permitiriam que eles identificassem facilmente as atividades de banco de dados não autorizadas ou suspeitas. A seguir exemplos específicos.

**Firewalls,rede IDS/IPS e Firewalls de Aplicativos Web (WAFs)** tem limitado a compreensão das construções de banco de dados e comandos SQL. Mesmo os WAFs necessitam apenas compreensão de 10 ou mais construções HTTP, enquanto que analisar o tráfego de banco de dados exige uma compreensão de mais de 350 comandos SQL bem como de uma linguagem completa de programação (PL-SQL). Por exemplo, essas tecnologias não foram concebidas para identificar um DBA fraudulento que usa comandos DDL (Data Definition Language) para modificar os esquemas de banco de dados, que é um requisito importante para conformidade SOX. Similarmente, eles não são concebidos para identificar um invasor que tenha comprometido o servidor de aplicativo para obter acesso ao servidor do banco de dados, ou está utilizando credenciais roubadas para ler o conteúdo completo de um banco de dados confidencial.

Além disso, geralmente, os sistema tradicionais de segurança de rede não são projetados para lidar com grandes quantidades de dados de auditoria de banco de dados gerados pelos aplicativos da empresa, como Oracle EBS, PeopleSoft e SAP. Isso exige uma arquitetura escalável para uma coleta armazenamento e análise eficazes dos dados de auditoria do banco de dados, incluindo uma grande inclusão de dados da empresa toda por todos os vários servidores e localizações. Dispositivos IDS de rede tradicional – que são otimizados para monitoramento de pacote de rede em vez de registros de auditoria – podem ser ineficazes para monitorar continuamente e auditar os ambientes de bancos de dados em tempo real, pois isto exige algoritmos de armazenamento inteligente e ferramentas de banco de dados relacionais avançadas para extrair as informações críticas exigidas para as análises de auditorias e judiciais.

**Instalações e acionadores de registro de auditoria de DBMS nativo e outras abordagens residentes no DBMS**, combinadas com scripts próprios para analisar dados de auditoria, geralmente, são o primeiro caminho para que as organizações procurem monitorar as atividades de banco de dados, mas elas podem sofrer de várias desvantagens importantes, principalmente por que o registro DBMS nativo foi originariamente desenvolvido para realizar ajustes e propósitos de recuperação em vez de segurança e conformidade.

A desvantagem principal é que as instalações de registro de auditoria nativa são controladas pelas mesmas equipes DBA que os auditores estão procurando monitorar, assim criando uma separação importante de conflitos de obrigações (SoD). Como resultado, DBAs e outros usuários privilegiados podem desabilitar o registro ou violar os registros de auditoria para "cobrir seus rastros". Igualmente, os invasores que comprometem os bancos de dados através de SQL Injection ou credenciais roubadas geralmente obtém super privilégios de usuários o que permite que desabilitem os registros (conhecido como antiforense).

Uma segunda desvantagem é que as instalações de registro de auditoria nativa impõe um alto nível de desempenho extra nos sistemas de banco de dados, particularmente, quando utilizavam para captar um alto volume de atividades, como capturar todo o acesso aos dados confidenciais (como exigido pelo requisito 10 PCI-DSS, por exemplo).

Terceiro, os aplicativos corporativos multicamadas, como SAP e PeopleSoft, utilizam contas de serviço genéricas para acessar a camada de banco de dados, ocultando assim a identidade dos usuários finais do aplicativo que iniciam transações na camada do aplicativo. Como resultado, as tecnologias de registro de auditoria de banco de dados nativas podem não ser suficientes para detectar fraude de usuário final e outras ações suspeitas realizadas por usuários finais autorizados, pois elas associam todas as transações do banco de dados à conta de serviço genérica ao invés das IDs específicas do aplicativo.

Quarto, abordagens com base em script próprio que dependem de funções de auditoria residente em DBMS são difíceis de desenvolver e manter em ambientes DBMS heterogêneos, pois cada plataforma DBMS realiza o registro de auditoria de forma diferente. Isto pode levar a ferramentas únicas estocadas e processos para cada ambiente DBMS, com políticas e relatórios de auditoria inconsistentes. Também pode tornar muito mais difícil a criação de visões totalmente corporativas das informações de auditoria para conformidade, analítica e forense do banco de dados.

Finalmente, as instalações de registro de auditoria nativas são controles de detecção "posterior" que não fornece controles preventivos, pró-ativos em tempo real como alertas e bloqueios.

**SIEM (Security Information and Event Management)** confia na coleta de registros de auditoria de DBMS nativos e, portanto, pode sofrer das mesmas desvantagens descritas acima (falta de separação de obrigações, extras, etc.). O mesmo pode ser dito de outras soluções que dependem da coleta de registros de auditoria nativa, como cofre de dados de auditoria ou soluções de repositório de auditoria. Finalmente, os sistemas SIEM geralmente não fornecem qualquer proteção em tempo real, e falta relatório e análise focados no banco de dados.

As tecnologias **DLP (Data Leak Prevention)** são um elemento importante de uma estratégia de defesa profunda, mas não são utilizadas para proteger dados confidenciais na fonte – isto é, no datacenter – que é o foco da maioria dos ataques. Ao contrário, estas tecnologias são desenvolvidas para captar dados confidenciais assim que saem do perímetro da rede via email, ou quando saem do terminal via drives USB – após serem extraídos dos bancos de dados confidenciais. Por exemplo, por não monitorarem a atividade de acesso do banco de dados, as tecnologias DLP não seriam utilizadas para identificar um analista que acabou de lançar uma consulta SQL para acessar 1.000 registros de um servidor de banco de dados de documentos da empresa, sistema CRM, sistema de processamento de cartão de pagamento ou sistema CAD.

**Criptografia do banco de dados** é uma tecnologia importante para proteger os arquivos de banco de dados e mídia (como as fitas de backup) de roubos e snooping, mas não fornece recursos de monitoração para identificar ou evitar atividades não autorizadas por usuários não autorizados. Além disso, não é possível proteger contra invasores que sequestram servidores de aplicativos para obter acesso criptografado aos bancos de dados de backend, nem é possível se defender de administradores e desenvolvedores com acesso às chaves de criptografia. A criptografia de banco de dados também não é eficaz como o mecanismo de controle de acesso granular, pois ele pode levar anos para modificar as arquiteturas de aplicativos existentes para suportar a criptografia em nível de campo na camada de banco de dados (por exemplo, para endereçar o impacto de desempenho de campos indexados e criptografados).

## Visão geral das tecnologias de segurança de banco de dados

Ao longo dos últimos anos, a indústria de segurança respondeu com novas tecnologias desenvolvidas especificamente para tratar da segurança de bancos de dados e os desafios de conformidade. Estas novas tecnologias tratam das limitações das soluções de segurança existentes descritas acima, oferecendo os seguintes recursos.

**DAM (Database Activity Monitoring).** Monitoração contínua e em tempo real e auditoria para todas as atividades de banco de dados, incluindo a criação de uma trilha de auditoria granular de todas as atividades dos usuários privilegiados ou todos os acessos às tabelas confidenciais, com impacto mínimo sobre o desempenho. As regras com base na política são utilizadas para identificar rapidamente as atividades suspeitas ou não autorizadas, por ambientes DBMS heterogêneos (Oracle, DB2 e SQL Server), com alertas em tempo real e relatórios de exceção. As principais melhores soluções tem como base as arquiteturas escaláveis e multicamadas com gerenciamento de política centralizada, bem como agregação centralizada de dados de auditoria para relatórios de conformidade, analítico e jurídico de toda a corporação.

**Avaliação de Vulnerabilidade e Configuração (VA).** Bibliotecas de testes automáticos para encontrar vulnerabilidades específicas de bancos de dados como senhas padrão de distribuidores, privilégios e funções desconfigurados, arquivos de configuração de banco de dados desprotegidos e correções ausentes.

**Alteração e Configuração de Auditoria.** Identifica as alterações críticas nos bancos de dados como alterações de esquema, bem como alterações de configuração que pode impactar a postura de segurança como alterações nos arquivos e permissões de configuração de banco de dados, variáveis de registros, variáveis de ambiente e scripts.

**Descoberta.** Descoberta automática de banco de dados para identificar bancos de dados novos e fraudulentos, combinados com tecnologia de descoberta e classificação de dados para localizar dados confidenciais em seus bancos de dados como números de cartões de crédito e números de CPF.

**Controle de Acesso Refinado e Bloqueio.** Bloqueio com base na política de atividades de banco de dados não autorizadas, geralmente utilizado para bloquear transações por usuários privilegiados como DBAs terceirizados. As regras podem ser baseadas em consultas recebidas (usuários, atividades realizadas, objetos de banco de dados, horário, localização ou aplicativo fonte), bem como conjuntos de resultados em andamento como número anormalmente alto de registros confidenciais sendo devolvidos para o cliente.

**Automação do Fluxo de Trabalho de Conformidade.** Os auditores querem saber que as organizações não estão simplesmente gerando relatórios de acesso de banco de dados, mas que elas também possuem um processo formal de supervisão para tratar de exceções e violações das políticas corporativas. As principais melhores soluções DAM automatizam o processo de supervisão de conformidade, incluindo a distribuição de relatório, desconexão eletrônica, comentários e escalações. Geralmente, tudo combinado com as bibliotecas de relatórios e políticas de conformidade de melhores práticas.

**Mascarar.** De-identifica os dados confidenciais para uso em ambientes de desenvolvimento e teste.

**Criptografia.** Criptografa os arquivos de base de dados e mídia como fitas de backup para evitar roubo ou transgressões de dados confidenciais.

**Integração com Infraestruturas de TI Existente.** As organizações estão procurando por suporte DBMS heterogêneo amplo (Oracle, SQL Server, DB2, Sybase, Informix, MySQL, Teradata, Netezza e PostgreSQL) em todas as principais plataformas OS (Linux/UNIX, Windows e z/OS) bem como integração dos principais componentes de infraestrutura como LDAP/Active Directory, SIEMs, CMDBs, sistemas de alteração de registro, e assim por diante.

## Segurança de dados, virtualização e nuvem

Apesar da agilidade, escalabilidade e custo benefício de mudar para a nuvem, muitas organizações estão hesitantes em adotar serviços de computação em nuvem, geralmente citando a segurança de dados como preocupação. Entretanto, certos modelos de implementação de nuvem como Nuvens Privadas, bem como os modelos de serviço de nuvem como Infraestrutura como um Serviço (IaaS), permite que organizações garantam níveis mais altos de segurança de dados implementadas pelas mesmas. O mesmo é verdade para organizações com infraestruturas virtualizadas.

Aqui estão algumas questões para considerar ao migrar as tecnologias de segurança de dados esixtentes para infraestruturas virtualizadas ou nuvem.

**Abordagem de Monitoração.** A solução monitoração com base em software que automaticamente se muda com a instância do banco de dados enquanto ele migra para a infraestrutura virtualizada ou nuvem, ou depende do acesso físico para os recursos de rede tradicionais como portas SPAN ou TAPs? Geralmente, estes recursos não estão disponíveis em ambientes virtuais ou nuvem, pois a comunicação ocorre sobre painel traseiro de hardware em vez de redes tradicionais.

**Dispositivos virtuais.** A solução pode ser implantada como dispositivos virtualizados, ou dependem de dispositivos de hardware que moram "fora" do ambiente nuvem ou virtual?

**Gerenciamento com base na Web.** A solução pode ser gerenciada a partir de qualquer dispositivo que utilize um navegador padrão?

**Solução única tanto para infraestruturas físicas e virtuais ou nuvens.** É possível utilizar uma solução única que abrange ambos os ambientes, ou é dedicado a um ou outro?

IBM Brasil Ltda.
Rua Tutóia, 1157
CEP 04007-900
São Paulo – Brasil

O site da IBM pode ser encontrado em:
**ibm.com**



Por favor, recicle