IBM X-Force Threat Intelligence Quarterly - primeiro trimestre de 2014

Explore as mais recentes tendências de segurança — desde a liberação de um malware até os riscos de dispositivos móveis — com base em dados do final do ano de 2013 e em pesquisas contínuas

IBM

Conteúdo

O que há de novo

Mais uma vez, chegou a hora de conhecer as últimas notícias da equipe de pesquisa e desenvolvimento do IBM® X-Force®, e gostaríamos de destacar algumas mudanças animadoras que fizemos no Relatório de Tendências e Riscos do IBM X-Force para 2014.

Formato trimestral

Anteriormente, a IBM produzia o relatório duas vezes ao ano, em formato longo. A partir do primeiro trimestre de 2014, a IBM produzirá o relatório em um formato trimestral, mais curto e mais ágil. Junto com o novo cronograma de publicação, vem também o novo nome, "IBM X-Force Threat Intelligence Quarterly", bem como atualizações no estilo e no formato.

Expansão da equipe: Apresentação da Trusteer

Com esta edição do relatório, estamos introduzindo dados coletados dos nossos colegas da Trusteer,[i] uma empresa IBM desde setembro de 2013.

Como fornecedora líder de softwares que ajudam a proteger as organizações contra fraudes e ameaças avançadas de segurança, a Trusteer oferece produtos utilizados por mais de 100 milhões de usuários, presentes em mais de 350 instituições financeiras em todo o mundo. As tecnologias e as pesquisas da Trusteer enfocam a prevenção da causa-raiz da maior parte das fraudes: ataques de "malware" e "phishing" que comprometem computadores e dispositivos móveis dos clientes.

Temos o prazer de dar à equipe Trusteer as boas-vindas à IBM. A combinação do conhecimento e da expertise dos pesquisadores do X-Force e da Trusteer continuará melhorando os futuros relatórios.

Visão geral executiva

Desde o final de 2010, o X-Force tem relatado aumentos anuais nas violações de segurança em todos os segmentos de mercado. No segundo semestre de 2013, os avanços nesses ataques continuaram aumentando. Neste relatório, explicaremos como mais de meio bilhão de registros de informações de identificação pessoal, como nomes, e-mails, números de cartão de crédito e senhas vazaram em 2013 — e como esses incidentes de segurança não mostram sinais de interrupção.

Pedimos aos novos pesquisadores de malwares do X-Force (Trusteer) para relatarem suas descobertas mais significativas no final de 2013, e eles responderam com um relatório sobre como os invasores continuam usando conteúdos como uma arma, com o objetivo de introduzir malwares no computador do usuário. Eles também relataram que as vulnerabilidades do Java da Oracle continuam sendo o principal ponto de entrada de muitos desses ataques de malware.

Para muitas organizações, a segurança de dispositivos móveis continua sendo uma área em constante mudança. Discuriremos como os riscos atuais associados ao crescimento do uso dos dispositivos móveis no local de trabalho não são tão simples como muitos acreditam — e como a mídia pode levá-lo a acreditar — e oferecemos um “insight”, bem como recomendaçoes sobre como as organizações podem proteger melhor seus ambientes móveis.

Por fim, encerraremos o relatório discutindo como o ano de 2013 terminou com o número de vulnerabilidades públicas pouco acima dos registros definitivos do final do ano de 2012. Ainda que as vulnerabilidades gerais tenham aumentado durante o ano passado, também vimos o declínio de algumas tendências em importantes áreas do relatório.

Resumo dos incidentes de segurança de 2013

Uma vez que a preocupação com a privacidade nunca foi tão grande — graças em parte à ampla cobertura da mídia sobre diversos ataques de grandes dimensões aos consumidores — os incidentes de segurança têm se tornado o assunto principal, desde a sala da diretoria até a sala de estar.

Ao longo dos anos em que a equipe do X-Force tem rastreado incidentes de segurança, as táticas e técnicas gerais de ataque não mudaram significativamente. No entanto, tem havido um marcante aumento no volume de todas as áreas. O número de incidentes gerais tem crescido, a quantidade de tráfego usado em ataques do tipo Distributed Denial of Service (DDoS) se multiplicou e o número de registros vazados tem aumentado de modo constante. Como você pode ver na Figura 1, que mostra os incidentes analisados pelo X-Force, a taxa de crescimento, a frequência e a dimensão de possíveis impactos financeiros têm estado em costante crescimento desde 2011.

Em 2013, os invasores continuaram usando métodos testados e comprovados para a extração de dados. Como se vê na Figura 2, eles conseguiram explorar aplicativos da web vulneráveis usando ataques como SQL injection (SQLi) e cross-site scripting (XSS), e também utilizaram uma combinação de kits de ferramentas sofisticados e facilmente acessíveis para obter pontos críticos de entrada. Essas ferramentas — que visam atingir terminais por meio de ataques de engenharia social contra funcionários, spear phishing e outras formas de instalação de malwares — criaram um grande desafio para as organizações que enfrentam a tarefa de proteger seus dados sensíveis.

A Figura 2 ilustra uma amostra dos incidentes de segurança de 2013. Os círculos maiores na segunda metade do final do ano representam várias importantes violações, com mais de meio bilhão de casos de vazamento de informações de identificação pessoal e números de cartão de crédito. A figura também ilustra o possível impacto financeiro de uma violação de dados em termos de multas, perda de propriedade intelectual, perda da confiança do cliente e perda de capital, que podem ser enfrentados por organizações de qualquer porte.

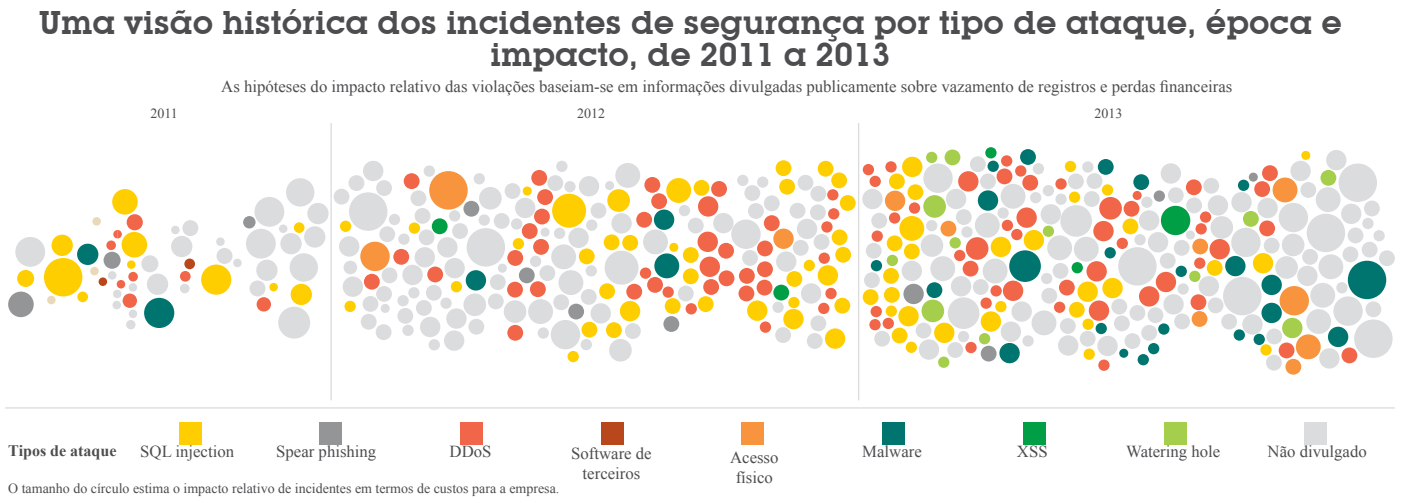
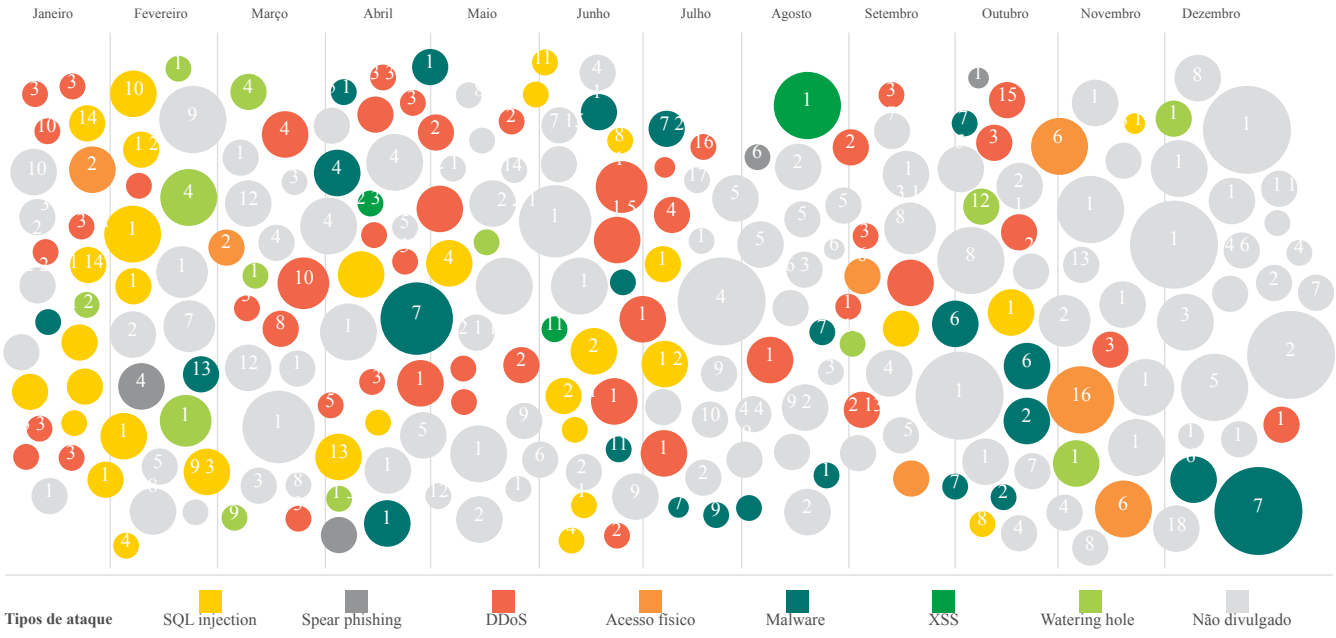


Figura 1. Uma visão histórica dos incidentes de segurança por tipo de ataque, época e impacto, de 2011 a 2013

Amostragem dos incidentes de segurança de 2013, classificada por tipo de ataque, época e impacto

As hipóteses do impacto relativo das violações baseiam-se em informações divulgadas publicamente sobre vazamento de registros e perdas financeiras

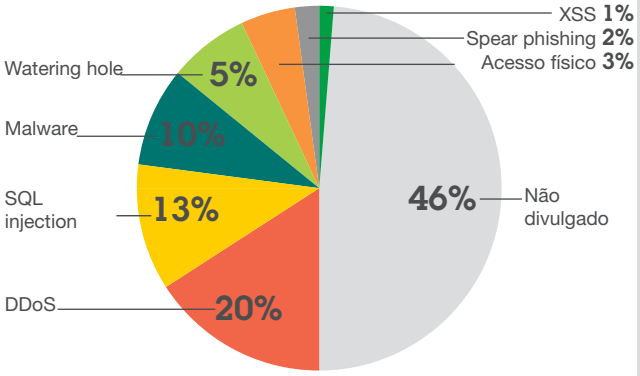


O tamanho do círculo estima o impacto relativo de incidentes em termos de custos para a empresa.

Segmentos de mercado atacados mais frequentemente

- **28%** Serviços computacionais (1)
- **15%** Governo (2)
- **12%** Mercados financeiros (3)
- **9%** Mídia e entretenimento (4)
- **7%** Educação (5)
- **5%** Saúde (6), Varejo (7), Telecomunicações (8)
- **3%** Produtos ao consumidor (9)
- **2%** ONGs (10), Automotivo (11), Energia e serviços públicos (12), Serviços de assistência profissional (13)
- **1%** Produtos industriais (14), Viagens e transporte (15), Distribuição e serviços de atacado (16)
- **<1%** Espaço aéreo e defesa (17), Seguros (18)

Tipos de ataque mais comuns



Qual é o custo de uma violação de dados?

As violações de dados têm impactos financeiros em termos de

multas, perda de propriedade intelectual, perda da confiança do cliente e perda de capital

Em 2013, o Ponemon Institute estimou um custo de US$ 136 por registro de dados perdido, com base em dados reais.*

* "2013 Cost of Data Breach Study: Global Analysis", Ponemon Institute, maio de 2013.

Por exemplo:

- Um importante varejista com milhões de cartões de crédito vazados poderia se deparar com mais de US$ 1 bilhão em multas e outros custos associados.
- Uma universidade que teve o vazamento de 40.000 registros poderia se deparar com uma perda de US$ 544.000.

Figura 2. Amostragem dos incidentes de segurança de 2013 por tipo de ataque, época e impacto

Como um exemplo significativo, muita atenção tem sido dada ao uso de sistemas de processamento de cartão de crédito por parte do segmento de varejo. Esses sistemas, que são implantados em websites de e-commerce e dispositivos de ponto de venda (POS), muitas vezes executam versões embarcadas ou mais antigas do Microsoft Windows, o que os torna mais suscetíveis à exploração. Esses sistemas de processamento de cartão de crédito são um lucrativo alvo de coleta de dados para invasores, que utilizam malwares otimizados para arquivar números e dados da faixa magnética de cartões de crédito, além de outras informações confidenciais.

As ferramentas destinadas a atingir esses terminais geralmente funcionam por meio de algum tipo de tecnologia "RAM scraper", que pode ser usada para ler informações diretamente da memória durante a fração de segundo entre a chegada dos dados criptografados no sistema e validação do texto não criptografado das informações do cartão. Uma vez que os dados são coletados, eles podem ser enviados para um servidor comprometido dentro da empresa. Nesse ponto, os invasores podem manualmente exfiltrar tais dados para fora da rede. Em 2013, numerosos incidentes do segmento do varejo foram divulgados como tendo sido causados por esse malware otimizado.

Além disso, considerando-se a amostragem dos incidentes de segurança, informados pelo X-Force em 2013 e o país onde o alvo do ataque estava localizado, percebemos que mais do que 3/4 deles ocorreram nos EUA.

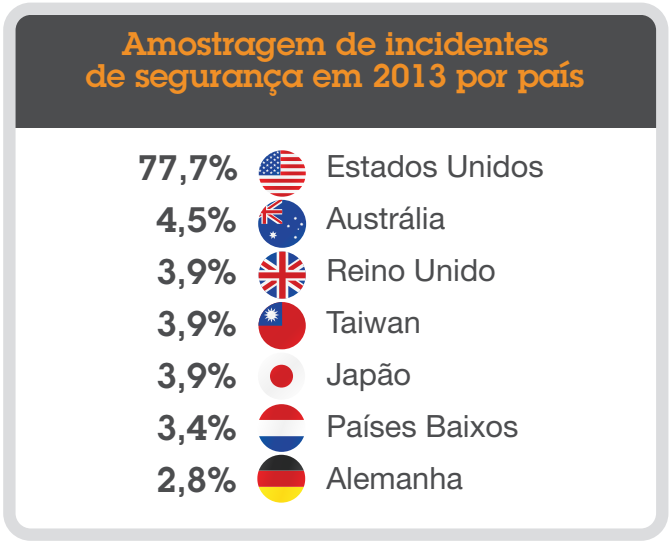


Figura 3. Amostragem de incidentes de segurança em 2013 por país

Alvos centrais estratégicos

No relatório do primeiro semestre de 2013, o X-Force identificou que os invasores estão, cada vez mais, buscando alvos estratégicos centrais como meio de otimizar seus esforços e aumentar o retorno da sua exploração. Essa tendência continuou no segundo semestre do ano. Exemplos importantes incluem vulnerabilidades em estruturas da web, como Ruby on Rails e Apache Struts, que fornecem aos invasores uma forma de comprometer milhares de websites. Uma vulnerabilidade no software do popular fórum vBulletim levou a uma violação de mais de 35.000 websites.[2] Além disso, alguns desses sites afetados têm bases de usuários muito grandes, com mais de uma milhão de registros vazados.[3]

Provedores de DNS

Ao longo de 2013, os provedores de DNS foram alvos de diversas formas. Os invasores que desejam encerrar o acesso conseguiram realizar ataques DDoS em provedores de DNS o que, por sua vez, causou tempo de inatividade para os clientes que usavam esses serviços em sua infraestrutura de DNS. Em alguns casos, os invasores conseguiram atingir empresas que possuíam uma forte segurança interceptando

solicitações DNS no provedor de DNS. Isso permitiu que redirecionassem o tráfego que estava indo para o site legítimo. A partir daí, os invasores tinham diversas opções: podiam fazer algo razoavelmente benigno, como exibir uma versão deteriorada do website, algo um pouco mais traiçoeiro, como detectar cookies do usuário como um ataque do tipo indireto;[4] ou expor os terminais ao malware antes que alcançassem o site do host. Esses tipos de ataques afetaram diversos sites conhecidos de mídias sociais e de notícias.

Mídia social

As contas de mídia social que têm um grande número de seguidores serviram como mais um tipo de alvo central estratégico. Ao longo de 2013, os invasores conseguiram acesso às contas de grandes celebridades, veículos da mídia, empresas de tecnologia e pessoas de interesse público. Serviços da web que interagem com mídias sociais para programar posts e executar outras tarefas também se mostraram alvos úteis, devido ao modelo de confiança no qual operam. Geralmente, esses serviços são autenticados para o perfil do usuário por meio de uma interface de programação de aplicativos (API), dando aos invasores a capacidade de postar atualizações no feed a partir de milhares de contas comprometidas. Foi o que aconteceu com um popular serviço de gerenciamento de mídia social,[5] no qual os invasores aproveitaram sua base de usuários de mais de um milhão de contas para enviar spam sobre perda de peso aos seguidores do serviço.

Moeda virtual

A tecnologia de Bitcoins foi um tópico em destaque em 2013, graças ao aumento exponencial na valorização da sua moeda virtual. Conforme esperado, isso motivou os invasores a encontrar novas oportunidades de se beneficiar. Houve diversos tipos de ataques contra websites de Bitcoin, incluindo denial of service (DoS) contra bolsas nas quais os usuários compram e vendem Bitcoins. Esses tipos de ataques podem desestabilizar a moeda e também podem ser usados para encobrir roubos de carteiras eletrônicas digitais. Moedas virtuais armazenadas em carteiras eletrônicas digitais correm risco não apenas de roubo, mas também de corrompimento da mídia digital (travamento do disco rígido) e perda de credenciais, como senhas de criptografia. Em agosto, houve denúncias de que bitcoins foram roubados por invasores que criaram um malware personalizado para explorar uma vulnerabilidade no gerador de números aleatórios do sistema operacional (SO), que é usado por determinados aplicativos de carteira eletrônica de Bitcoin executados na plataforma Google Android.[6]

Evolução dos tipos de ataque

Outra forma pela qual os invasores obtiveram êxito em 2013 foi usando ataques do tipo "watering hole". Nesses tipos de ataques, o invasor compromete websites de interesse especial e injeta o malware nos visitantes por meio da exploração de vulnerabilidades do navegador ou do plug-in do navegador. Ataques "watering hole" mostraram-se eficazes para atingir grupos de usuários que frequentam determinados tipos de websites. Alguns bons exemplos incluem o PHP.net[7] — um website que fornece informações de referência para desenvolvedores da web que utilizam a linguagem de criptografia de websites de software livre PHP — e uma série de websites comprometidos nos segmentos de mercado de energia e serviços públicos, química e petróleo.[8]

De modo semelhante aos ataques "watering hole", o *malvertising* (publicidade maliciosa) está ganhando impulso.[9] A publicidade maliciosa ocorre quando os invasores miram redes de publicidade injetando anúncios com explorações maliciosas que levam a downloads do tipo drive-by. Esses anúncios maliciosos podem, em seguida, expor usuários vulneráveis nos muitos websites que exibem o conteúdo proveniente das redes de publicidade. A equipe de pesquisa da Trusteer recentemente publicou num blog um artigo detalhado sobre publicidade maliciosa[10], por meio da qual uma recente vulnerabilidade Java de dia zero (CVE-2013-0422) estava sendo explorada livremente. Essa campanha específica estava aproveitando kits de ferramentas de exploração de buracos negros, que utilizam essa vulnerabilidade para comprometer terminais do usuário.

Todos esses esforços permitem que os invasores se concentrem em um pequeno número de alvos críticos que, em seguida, fornecem acesso a milhares de outros.

Apesar de toda a divulgação e da cobertura em massa da mídia sobre o volume e o escopo das atuais violações de segurança, empresas e usuários ainda podem obter um considerável êxito na própria proteção se aplicarem melhores práticas de segurança básica para senhas, segmentação de rede e desenvolvimento seguro de softwares.

Malware: Entrega via explorações de aplicativos

Há muito tempo, sabemos que invasores exploram vulnerabilidades de aplicativos para fazer download de malware em terminais de usuários desavisados. Uma análise dos dados de inteligência de ameaças do X-Force durante o mês de dezembro de 2013 revela que em uma pesquisa com mais de um milhão de clientes bancários e corporativos da Trusteer, os aplicativos mais atingidos foram Oracle Java, Adobe Reader e navegadores populares.

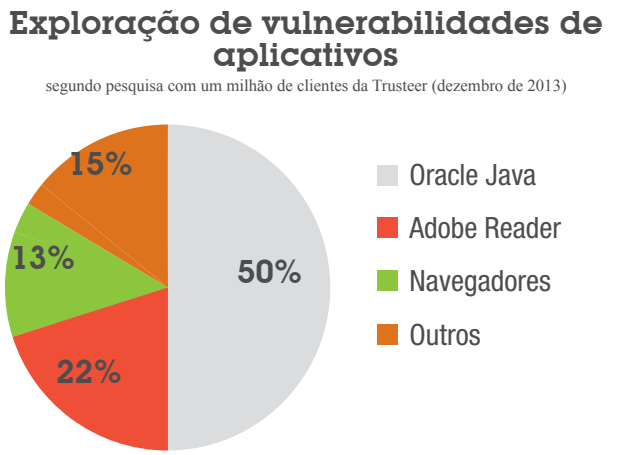


Figura 4. Exploração de vulnerabilidades de aplicativos,

Não é surpreendente que esses sejam os aplicativos de usuários mais visados. Afinal, todos esses aplicativos são encontrados na maioria dos terminais de usuário, todos eles têm vulnerabilidades que podem ser exploradas de modo a entregar malwares nas máquinas do usuário e todos eles podem receber e processar conteúdo externo. Isso significa que os invasores podem criar conteúdos que atuam como armas: arquivos ou documentos portadores de explorações que se beneficiam de vulnerabilidades no aplicativo. Os invasores usam mensagens de spear-phishing para levar os usuários a websites que contêm applets Java ocultos e maliciosos (sites de exploração). O conteúdo que serve como arma é geralmente entregue aos usuários por mensagens de spear-phishing ou sites de exploração. Assim que o usuário abre o arquivo ou o documento usando um aplicativo vulnerável, a exploração causa uma cadeia de eventos que termina com a entrega do malware na máquina do usuário e a subsequente infecção — tudo isso sem o conhecimento do usuário.

Java: Um aplicativo poderoso, mas vulnerável

O Java é um aplicativo de alto risco amplamente implementado que expõe organizações a avançados ataques. O número de vulnerabilidades do Java continuou aumentando ao longo dos anos, e 2013 não foi exceção. A quantidade de vulnerabilidades do Java saltou significativamente entre 2012 e 2013, mais do que triplicando.

Pesquisas indicaram que, com esse crescimento das vulnerabilidades, também houve um significativo aumento nas explorações de Java, conforme mostrado por metade dos clientes afetados da amostra observada. Isso foi o resultado das descobertas de novas vulnerabilidades de dia zero e do início da utilização de kits de ferramentas de exploração. Em relatórios anteriores de Tendências e Riscos do X-Force, discutimos como se descobriu que kits de ferramentas de exploração como *Blackhole* e *Cool* usavam vulnerabilidades Java não corrigidas para escapar do ambiente de simulação Java e instalar malwares nas máquinas das vítimas.

Durante o ano de 2013, essa popular tendência continuou.

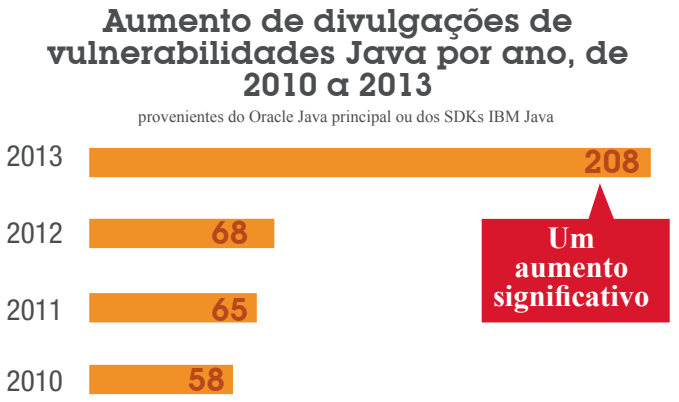


Figura 5. Aumento de divulgações de vulnerabilidades Java por ano, de 2010 a 2013

O uso de Java pode expor as organizações a avançados ataques, devido às numerosas vulnerabilidades do aplicativo. Tais vulnerabilidades podem ser exploradas a fim de entregar malwares e comprometer as máquinas do usuário. Uma vez em um terminal, é extremamente difícil impedir a execução maliciosa do malware Java. No entanto, os avançados recursos do Java continuam fazendo dessa uma plataforma popular para o desenvolvimento de aplicativos corporativos. Atualmente, é possível encontrar o Java em praticamente qualquer ambiente corporativo. Além disso, uma vez que as organizações são altamente dependentes de aplicativos Java, não é conveniente removê-lo desses ambientes (conforme alguns recomendam). Já que as organizações não podem eliminar o Java de seus ambientes, não surpreende que invasores usem código Java malicioso para se infiltrarem.

Explorações Java nativas versus explorações Java de aplicativo: Com as explorações de aplicativo à frente

As vulnerabilidades Java podem permitir dois tipos de explorações: nativas e de aplicativo. A maior parte das explorações que visam vulnerabilidades em aplicativos do usuário final, como navegadores ou aplicativos do Microsoft Office, são executadas de modo nativo. Uma exploração nativa resulta na execução do código shell nativo. Esse tipo e exploração é realizado por técnicas que incluem estouro de buffer, "use-after-free" e mais.

Diversas proteções nativas no nível do sistema operacional ajudam a proteger as organizações contra explorações nativas. Essas proteções incluem ASLR (address space layout randomization) e DEP (Data Execution Prevention), bem como proteções de segurança gerais que abrangem SEHOP (Structured Exception Handler Overwrite Protection), proteção contra heap-spraying (como NOZZLE), proteção contra Stack Pivoting e Export Address Table Access Filtering (EAF).

No entanto, uma observação mais atenta revela que o tipo mais comum de exploração Java é uma exploração de aplicativo (neste exemplo, explorações de camada Java). Diferentemente das explorações nativas, que visam a memória do aplicativo, o objetivo das explorações de aplicativo é violar o gerenciador de segurança Java, afetando aplicativos Java que são executados dentro de uma máquina virtual (JVM).

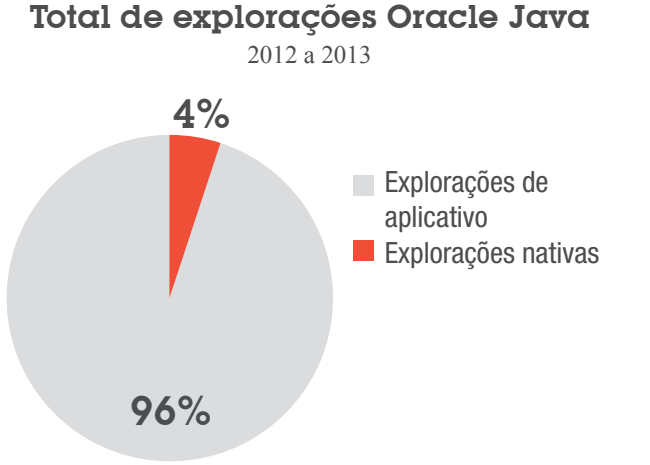


Figura 6. Total de explorações Oracle Java, 2012 a 2013

O gerenciador de segurança Java é uma classe que gerencia o limite externo da JVM, controlando como o código do applet Java que é executado dentro da JVM pode interagir com recursos externos à JVM. Explorações de aplicativo abusam das vulnerabilidades que rompem o modelo de segurança Java. Uma vez que o modelo de segurança é violado, nada impede que o applet Java execute operações críticas que não devem ser executadas.

A defesa contra explorações de aplicativo Java é mais difícil porque eles permitem que o applet ganhe privilégios irrestritos, o que faz com que as atividades maliciosas pareçam legítimas no nível do sistema operacional. Isso significa que, diferentemente de explorações nativas, as explorações de aplicativo Java ignoram totalmente as proteções nativas no nível do sistema operacional. Além disso, as explorações de aplicativo Java não geram estouro de buffer e, por isso, não são impedidas por métodos como DEP, ASLR, SEHOP e outros.

Recomendações

Como as organizações não podem eliminar o Java de seus ambientes, é importante que protejam esses aplicativos a fim de evitar a execução de código Java malicioso. No entanto, essas proteções nativas disponíveis atualmente têm recursos muito limitados, especialmente contra ameaças de dia zero.

Para ajudar a evitar explorações Java e infiltrações baseadas em malware, é importante restringir a execução apenas a arquivos Java conhecidos e confiáveis. As organizações que lutam para gerenciar e manter uma lista completa de todos os arquivos conhecidos e confiáveis devem, pelo menos, restringir a execução a arquivos que foram assinados por fornecedores confiáveis ou transferidos por download a partir de domínios confiáveis. De todo modo, arquivos Java não confiáveis não devem ter permissão para serem executados livremente dentro do ambiente corporativo. A restrição de arquivos Java não confiáveis permite que as organizações operem seus negócios com mais segurança, ao reduzir o perigo da exposição a arquivos de alto risco.

Ameaças de dispositivos móveis: percepção versus realidade

Apesar da preocupação dos executivos de que programas bring-your-own-device (BYOD) arriscam expor dados corporativos por meio da perda ou roubo de dispositivos móveis,[11] as divulgações públicas não relatam incidentes significativos que corroborem esse temor. Embora pesquisas na Internet mostrem muitos artigos e blogs anunciando os perigos de programas BYOD, os incidentes reais usados para justificar esses temíveis avisos geralmente envolvem laptops, pen drives ou cartões secure digital (SD) — não smartphones ou tablets.

Embora muitos de nós tratemos os smartphones e tablets como apêndices digitais (algumas pesquisas descobriram que quase metade dos usuários deixam os smartphones ao lado da cama por medo de perder chamadas, mensagens de texto ou atualizações das redes sociais enquanto dormem[12]), às vezes ainda os esquecemos em restaurantes, táxis ou eles são roubados (o que às vezes é chamado de *colheita da maçã* — em referência à Apple). Esses dispositivos órfãos, se usados para trabalho, podem conter informações protegidas relacionadas a prontuários de saúde, informações de identificação pessoal e/ou propriedade intelectual pertencente à organização, o que resulta no comprometimento dos dados.

Para fins de clareza e de acordo com a finalidade deste relatório, quando nos referirmos a dispositivos móveis e às novas ameaças que eles representam, limitamos o escopo aos smartphones e tablets. Deixamos os laptops de propriedade da empresa fora desse escopo porque eles já atuam como ferramentas de negócios básicas há décadas e, uma vez que executam sistemas operacionais de propósito geral como Windows, Apple OS X e Linux, trazem desafios de segurança diferentes daqueles representados por sistemas operacionais como Apple iOS e Android. Também excluímos pen drives, cartões SD, discos externos, fitas de backup e similares porque, embora tecnicamente sejam dispositivos móveis, eles simplesmente armazenam mídia. Assim como os laptops, esses dispositivos não representam uma nova tecnologia ou ameaça. Há anos as organizações já têm gerenciado exfiltração de dados em dispositivos de armazenamento.

Os fatos

A fim de validar a falta de incidentes envolvendo a exposição de dados sensíveis em dispositivos móveis, escolhemos um conjunto de dados de amostra para analisar: as divulgações públicas monitoradas pelo Escritório de Direitos Civis (OCR) do Departamento de Saúde e Serviços Humanos dos Estados Unidos.[13] A pesquisa do X-Force revelou que não houve relatos de incidentes de roubo de informações protegidas relacionadas a prontuários de saúde em dispositivos móveis. Descobrimos que laptops e documentos em papel estão mais frequentemente envolvidos nesses incidentes, enquanto pen drives e roubo a partir de servidores (em alguns casos, o próprio servidor foi roubado) ocupam o terceiro lugar.[13]

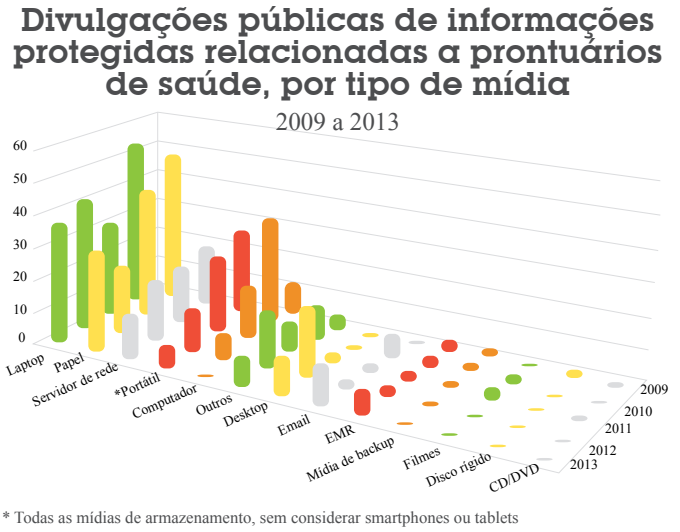


Figura 7. Divulgações públicas de informações de saúde eletrônicas protegidas, por tipo de mídia, de 2009 a 2013

De modo geral, nossa pesquisa mostra que aplicativos corporativos que permitem acesso a dados organizacionais através de dispositivos móveis não armazenam quantidades significativas de registros em dispositivos móveis. Devido à necessidade de acesso em qualquer lugar, os dispositivos móveis se desataram da empresa e oferecem apenas interface ao usuário — no entanto, a maior parte dos dados é armazenada na nuvem. Geralmente, os aplicativos remotos conectam-se a armazenamentos de dados por meio de portais publicamente acessíveis e funcionam por transação, interagindo com um registro por vez ou com pequenos lotes armazenados em cache, para fins de desempenho.

Isso não quer dizer que dados sensíveis corporativos nunca são armazenados em dispositivos móveis. Um repositório de destaque é o e-mail, que muitos usuários consideram um sistema de arquivos alternativo para compartilhar e armazenar tudo e qualquer coisa, desde correspondências com membros da família até negociações para fusões corporativas. Além disso, alguns dispositivos móveis podem ser usados como dispositivos de armazenamento em massa, semelhantes aos pen drives.

Ainda assim, a ausência de evidências divulgadas publicamente sobre violações de grande escala envolvendo dispositivos móveis não é prova de que a ameaça não é real. Não vamos nos esquecer de que muitas empresas têm resistido a transferir dados corporativos para dispositivos móveis por puro receio.

Portanto, qual é a ameaça real e quão ampla é a exposição?

A ameaça real

O resultado é que, embora algumas informações organizacionais possam estar presentes em dispositivos móveis, percebemos que o maior risco para a empresa não são os dados contidos nesses dispositivos, são as credenciais.

É mais eficiente para os invasores atacarem diretamente o portal ao qual o aplicativo remoto se conecta e obter acesso ao repositório de dados corporativos inteiro, do que "bater carteira" em uma infinidade de dispositivos móveis. Muitas vezes, tudo o que é necessário é um nome de usuário e uma senha (que podem ser roubados de um único dispositivo móvel usando um criador de logs de teclas digitadas), redirecionar o acesso ao portal por meio de um site intermediário onde as credenciais são capturadas ou apossar-se de uma carteira eletrônica digital e executar o crack dela off-line.

Os dispositivos móveis também podem conter uma coleção de informações pessoais, o que permite à engenharia social montar ataques novos ou mais avançados contra a empresa.

Outra grande ameaça dos dispositivos móveis são aplicativos que foram submetidos a crack e redistribuídos por meio de lojas de aplicativos piratas. A Arxan, um Parceiro de Negócios IBM, descobriu que, dos 100 principais aplicativos pagos em Android, 100% deles têm variantes hackeadas por aí. No caso do iOS a história é um pouco melhor, com apenas 50% dos aplicativos tendo alternativas piratas.[14] E, conforme apontamos no Relatório Semestral de Tendências e Riscos do X-Force para 2013, atualmente, o setor móvel abrange 4% de todas as vulnerabilidades. As ameaças estão por aí e já residem em centenas de milhares de dispositivos móveis. O fato de até agora não termos visto violações significativas de dados corporativos em smartphones e tablets não significa que o futuro continuará sendo tão bucólico.

Recomendações

Embora os dispositivos móveis possam certamente representar novas ameaças a dados corporativos, essas ameaças podem ser diferentes do que esperamos. É importante compreender as prováveis vias de ataque e proteger-nos contra elas, em vez de ver toda a questão da mobilidade como uma ameaça geral. A especificidade faz parte da segurança.

Os dispositivos móveis causaram uma o renascimento de uma nova forma de pensar em segurança: criação de ambiente de simulação, conteinerização e transações confiáveis são tecnologias emergentes que prometem oferecer proteção aprimorada e revelam o desejo dos executivos de segurança e de TI de capacitar ainda mais os aplicativos remotos na mão de obra.

Uma estratégia viável para a proteção de dispositivos móveis tem três componentes-chave:

- Proteção do dispositivo — uso de tecnologias como Mobile Device Management (MDM) e Enterprise Mobility Management (EMM)
- Proteção do aplicativo — utilizar criação de ambiente de simulação, conteinerização e segurança no nível do aplicativo para separar dados pessoais de dados corporativos
- Proteção das transações — nem todas as interações móveis envolvem aplicativos, e nem todos no ecossistema farão parte da sua estrutura de MDM ou EMM. Assim, é importante garantir que as transações com clientes, parceiros e trabalhadores temporários também possam ser protegidas contra dispositivos desbloqueados ou submetidos a jailbreak, fraudadores e malwares de dispositivos móveis

Em última análise, a equipe do X-Force acredita que essas descobertas embasam nossa previsão apresentada no Relatório de Tendências e Riscos do X-Force para 2012: até o final de 2014, os dispositivos computacionais móveis deverão ser mais seguros do que os dispositivos tradicionais.

Divulgações de vulnerabilidade e explorações em 2013

O X-Force tem documentado divulgações públicas de vulnerabilidades de segurança desde 1997. Dezessete anos depois, armazenamos um banco de dados de informações sobre mais de 78.000 vulnerabilidades. Incontáveis horas são dedicadas à pesquisa de vulnerabilidades e ameaças de aplicativos, bem como à realização de buscas na Internet, a fim de pesquisar dados para o banco de dados de vulnerabilidades do X-Force.

Desde 2006 e desde o primeiro declínio no número de vulnerabilidades divulgadas, em 2007, temos visto o número total de vulnerabilidades crescer e diminuir, ano sim e ano não. No entanto, ao final de 2013, observamos o primeiro ano em que esses totais cíclicos não alternam entre as sequências anuais mais alta e mais baixa vistas ao longo dos últimos sete anos.
Como um percentual das divulgações gerais, o número de vulnerabilidades de aplicativos da web caíram nitidamente em comparação ao observado em 2012.

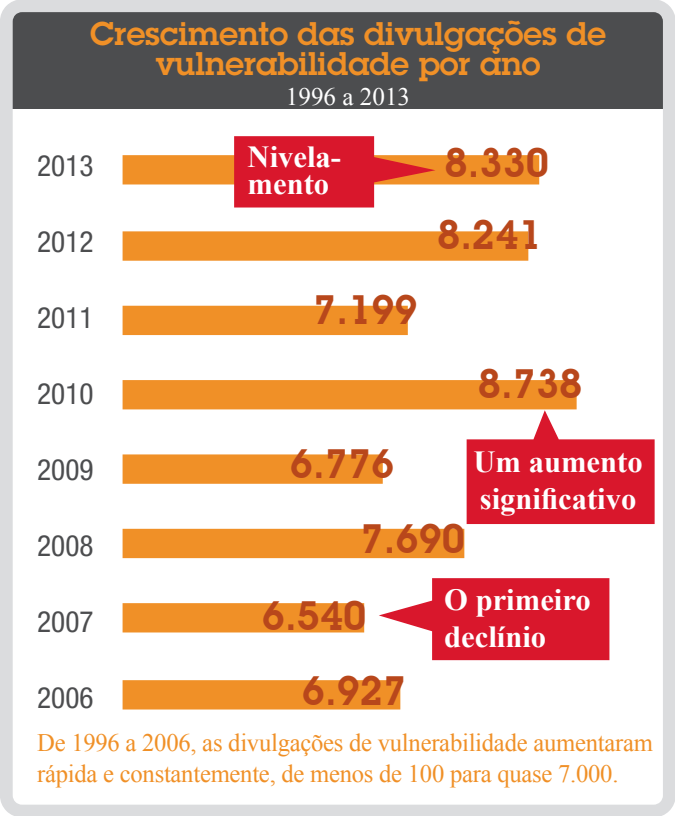


Figura 8. Aumento de divulgações de vulnerabilidades por ano, de 1996 a 2013

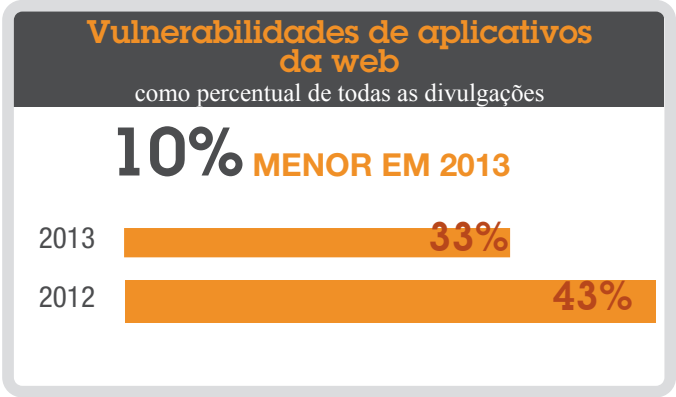


Figura 9. Vulnerabilidades de aplicativos da web como percentual de todas as divulgações, de 2012 a 2013

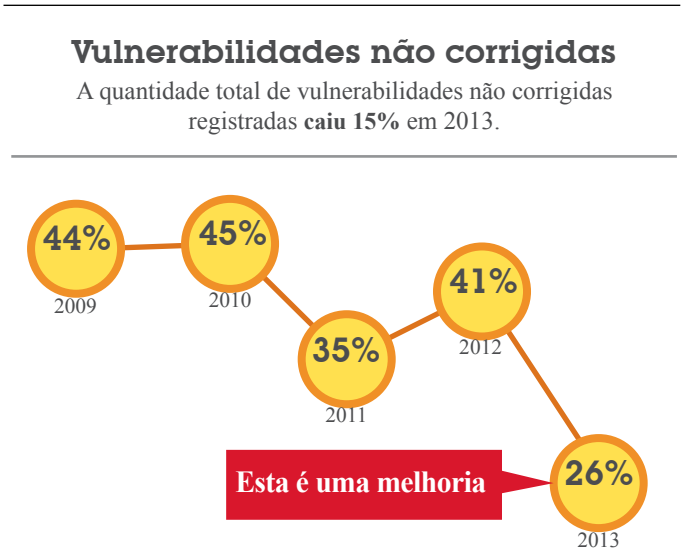


Figura 10. Índices de correções do fornecedor para vulnerabilidades divulgadas publicamente, de 2009 a 2013

Além disso, os índices de correções do fornecedor para vulnerabilidades divulgadas publicamente atingiram alguns dos pontos mais altos já vistos desde que o X-Force começou a monitorar esses dados. Em 2013, descobrimos que apenas 26% das vulnerabilidades divulgadas publicamente permaneciam sem correção — isso demonstra uma melhoria!

Ao observar as vulnerabilidades de aplicativos da web por técnica de ataque, percebemos quedas significativas tanto em XSS como de SQL injection.

As quedas nas vulnerabilidades demonstradas no final de 2013 em ambos XSS e SQL injection, mostradas na Figura 11, poderiam indicar que os desenvolvedores estão fazendo um trabalho melhor ao escrever aplicativos da web seguros, ou que possivelmente os alvos tradicionais, como sistemas de gerenciamento de conteúdo (CMSs) e plug-ins, estão amadurecendo, uma vez que vulnerabilidades mais antigas foram corrigidas. Conforme observado, a exploração da de XSS e SQL injection continua sendo observada em alto número, o que indica que ainda há sistemas legados ou outros aplicativos da web não corrigidos que permanecem vulneráveis. Isso já é esperado, considerando-se que há milhares de blogs e outros websites operados por indivíduos que podem não ter a habilidade necessária ou a consciência da necessidade de realizar a atualização da plataforma ou estrutura em questão para as versões mais recentes.

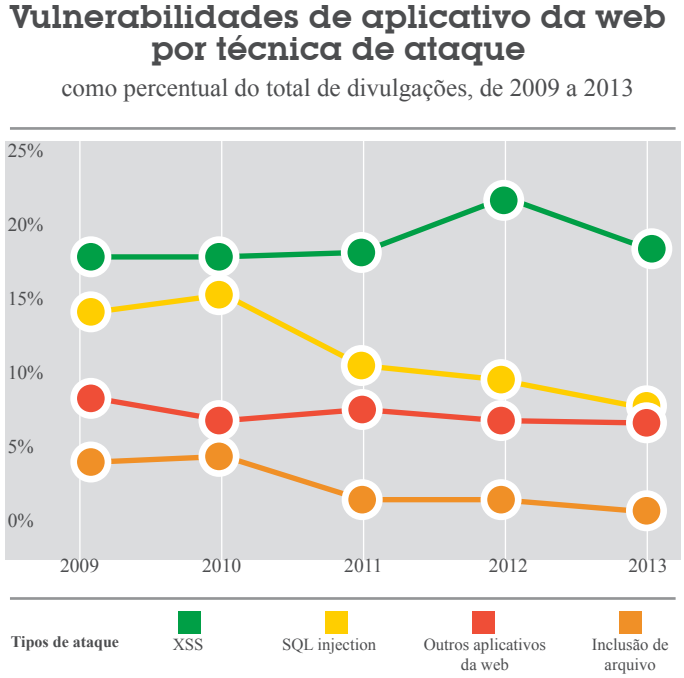


Figura 11. Vulnerabilidades de aplicativo da web por técnica de ataque, de 2009 a 2013

Consequências da exploração

O X-Force categoriza as vulnerabilidades de acordo com a consequência da exploração. A consequência é, essencialmente, o benefício que o invasor obtém ao explorar a vulnerabilidade. A Tabela 1 descreve cada consequência.

Consequência	Definição
Obtenção de acesso	Obtenção de acesso local e remoto a um aplicativo ou sistema; além disso, inclui vulnerabilidades por meio das quais os invasores podem executar códigos ou comandos, uma vez que eles geralmente permitem que os invasores obtenham acesso ao serviço ou sistema operacional subjacente.
Cross-site scripting	Impacto variável, dependendo do aplicativo ou usuário visado, mas pode incluir consequências como divulgação de informações confidenciais, interceptação de sessão, spoofing, redirecionamento de site ou desfiguração do website.
Negação de serviço	Paralisação ou interrupção de um serviço ou sistema
Obtenção de informações	Obtenção de informações como nomes de arquivos e caminhos, código-fonte, senhas ou detalhes de configuração do servidor
Desvio da segurança	Contornar restrições de segurança como autenticação, firewall ou proxy, sistema de detecção de intrusão (IDS)/sistema de prevenção de intrusão (IPS) ou scanners de vírus
Obtenção de privilégios	Obtenção de privilégios elevados em um aplicativo ou sistema por meio de credenciais válidas
Manipulação de dados	Manipulação dos dados usados ou armazenados pelo host associado ao serviço ou aplicativo.
Desconhecido	Não é possível determinar a consequência, devido a informações insuficientes
Outros	Refere-se a tudo o que não é abordado pelas outras categorias
Manipulação de arquivos	Criação, exclusão, leitura, modificação ou sobrescrita de arquivos

Tabela 1. Definições das consequências da vulnerabilidade

A consequência de exploração de vulnerabilidade predominante no primeiro semestre de 2013 foi a *Obtenção de acesso*, com 26% de todas as vulnerabilidades relatadas. Na maior parte dos casos, a obtenção de acesso a um sistema ou aplicativo oferece aos invasores controle total sobre o sistema afetado, o que lhes permite roubar dados, manipular o sistema ou iniciar outros ataques a partir daquele sistema. *Cross-site scripting* foi a segunda consequência predominante, com 18%, e geralmente envolve ataques contra aplicativos da web.

A Figura 12 mostra um detalhamento completo de todas as consequências de vulnerabilidade relatadas durante 2013.

Consequências de exploração em 2013

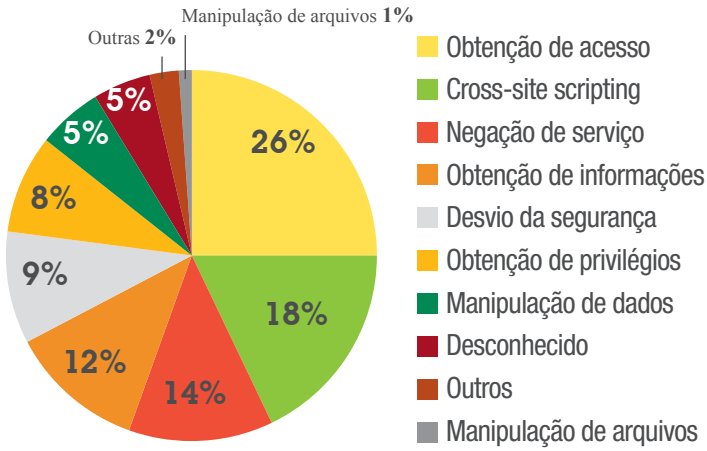


Figura 12. Consequências de exploração em 2013

Explorações

O X-Force classifica duas categorias de exploração: exploração e exploração verdadeira. Fragmentos simples com código de prova de conceito são contados como *explorações*, enquanto programas totalmente funcionais, capazes de ataques independentes, são categorizados como *explorações verdadeiras*.

As explorações verdadeiras disponíveis e divulgadas publicamente continuaram diminuindo ao longo dos últimos cinco anos, até chegar aos níveis mais baixos vistos desde 2006. Ao final de 2012, relatamos que o total de explorações verdadeiras ainda era baixo no geral e, ao final de 2013, essa tendência prosseguia.

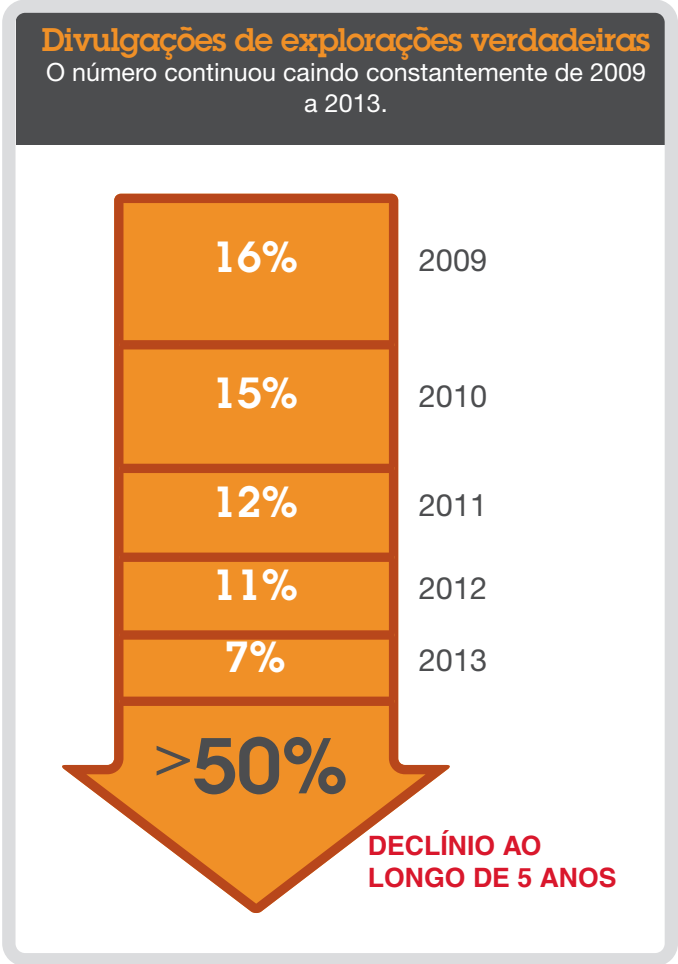


Figura 13. Divulgações de explorações verdadeiras, de 2009 a 2013

Sobre o X-Force

A equipe de pesquisa e desenvolvimento do X-Force estuda e monitora as mais recentes tendências de ameaças, incluindo vulnerabilidades, explorações e ataques ativos, vírus e outros malwares, spam, phishing e conteúdo da web malicioso. Além de fornecer orientação aos clientes e ao público geral sobre ameaças emergentes e críticas, o X-Force também fornece conteúdo de segurança para ajudar a proteger os clientes da IBM dessas ameaças.

Colaboração do IBM Security

O IBM Security representa diversas marcas que fornecem um amplo espectro de competências de segurança:

- A equipe de pesquisa e desenvolvimento do X-Force detecta, analisa, monitora e registra uma ampla gama de ameaças e vulnerabilidades de segurança de computadores, além das mais recentes tendências e métodos usados pelos invasores. Outros grupos dentro da IBM usam esses avançados dados para desenvolver técnicas de proteção para nossos clientes.
- A Trusteer oferece uma plataforma de prevenção holística contra crimes cibernéticos no terminal, que ajuda a proteger as organizações contra fraudes financeiras e violações de dados. Centenas de organizações e dezenas de milhões de usuários finais contam com a Trusteer para proteger seus aplicativos da web, computadores e dispositivos móveis de ameaças on-line (como malware avançado e ataques de phishing). Com uma equipe de pesquisa avançada e dedicada, a inteligência exclusiva e em tempo real da Trusteer permite que sua plataforma baseada na nuvem rapidamente se adapte às ameaças emergentes.
- A equipe de segurança de conteúdo do X-Force monitora e categoriza a web por meio de crawl, descobertas independentes e feeds fornecidos pelos IBM Managed Security Services.
- Os IBM Managed Security Services são responsáveis por monitorar explorações relacionadas a terminais, servidores (incluindo servidores da web) e infraestrutura de rede geral. Essa equipe rastreia explorações executadas pela web, bem como por outros vetores, como e-mails e mensagens instantâneas.
- Os IBM Professional Security Services oferecem serviços de avaliação, design e implementação de segurança para toda a empresa, a fim de ajudar a criar efetivas soluções de segurança da informação.
- O IBM QRadar® Security Intelligence Platform oferece uma solução integrada para Security Information and Event Management (SIEM), gerenciamento de log, gerenciamento de configuração, avaliação de vulnerabilidade e detecção de anomalias. O produto oferece um painel unificado e insight em tempo real sobre riscos de segurança e conformidade relacionados a pessoas, dados, aplicativos e infraestrutura.

Contribuidores

A produção do X-Force Threat Intelligence Quarterly ocorre com a dedicada colaboração de toda a IBM. Gostaríamos de agradecer pela atenção e contribuição dos seguintes indivíduos para a publicação deste relatório.

Contribuidor	Cargo
Avner Gideoni	Vice-presidente de segurança da Trusteer
Brad Sherrill	Gerente do banco de dados do IBM X-Force Threat Intelligence
Chris Poulin	Estrategista de pesquisa do IBM X-Force
Dana Tamir	Diretora de marketing de produtos de segurança corporativa da Trusteer
Jason Kravitz	Especialista de Techline do IBM Security Systems
Leslie Horacek	Gerente de resposta a ameaças do IBM X-Force
Pamela Cobb	Gerente mundial do segmento de mercado de inteligência de segurança
Perry Swenson	Marketing do produto IBM X-Force
Robert Freeman	Gerente de pesquisa avançada do IBM X-Force
Scott Moore	Desenvolvedor de software e líder de equipe do banco de dados do IBM X-Force Threat Intelligence

Para obter mais informações

Para saber mais sobre o IBM X-Force, visite: **ibm.com**/security/xforce/

[1] A Trusteer, Ltd. foi adquirida pela IBM em setembro de 2013.

[2] David Gilbert, "35,000 Websites Hacked Using Vulnerability in vBulletin Forum Software", *International Business Times*, 15 de outubro de 2013. http://www.ibtimes.co.uk/35000-websites-hacked-vbulletin-vulnerability-cms-software-514034

[2] Arnold Kim, "MacRumors Forums: Security Leak", *MacRumors*, 12 de novembro de 2013. http://www.macrumors.com/2013/11/12/macrumors-forums-security-leak/

[3] John Koetsier, "LinkedIn DNS hijacked, traffic rerouted for an hour, and users' cookies read in plain text", *VentureBeat*, 19 de junho de 2013. http://venturebeat.com/2013/06/19/linkedin-dns-hijacked-traffic- rerouted-for-an-hour-and-users-cookies-read-in-plain-text/

[4] Christina Warren, "Buffer Users' Facebook and Twitter Feeds Spammed After Hacking", *Mashable*, 26 de outubro de 2013. http://mashable. com/2013/10/26/buffer-hacked/

[5] Elad Shapira, "The Android BitCoin vulnerability explained", *AVG Technologies*, 20 de agosto de 2013. http://blogs.avg.com/mobile/android-bitcoin-vulnerability-explained/

[6] Larry Seltzer, "PHP project site hacked, served malware", *ZDNet*, 28 de abril de 2013. http://www.zdnet.com/php-project-site-hacked-served-malware-7000022513/

[7] Emmanuel Tacheau, "Watering-Hole Attacks Target Energy Sector", *Cisco Systems*, 18 de setembro de 2013. http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/

[8] Jeremy Kirk, "Yahoo's malware-pushing ads linked to larger malware scheme", *PCWorld*, 10 de janeiro de 2014. http://www.pcworld.com/article/2086700/yahoo-malvertising-attack-linked-to-larger-malware-scheme.html

[9] George Tubin, "Malvertising Campaigns Get a Boost from Unpatched Java Zero-Day Exploits", *Trusteer Blogs*, 30 de janeiro de 2013. http://www. trusteer.com/blog/malvertising-campaigns-get-a-boost-from-unpatched-java-zero-day-exploits

[10] IBM Center for Applied Insights, "A new standard for security leaders: Insights from the 2013 IBM Chief Information Security Officer Assessment", *IBM Corp.*, outubro de 2013. http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03087usen/CIW03087USEN.PDF

[11] Aaron Smith, "Smartphone Ownership 2013", *Pew Internet & American Life Project*, 5 de junho de 2013. http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx

[12] Chris Poulin, "A Fresh Look at Healthcare Data Breach Numbers", *IBM Security Intelligence Blog*, 25 de novembro de 2013. http://security-intelligence. com/healthcare-data-breach-numbers/#

[13] "State of Security in the App Economy: Mobile Apps Under Attack", *Arxan Technologies, Inc.*, 2013. https://www.arxan.com/assets/1/7/State_of_Security_in_the_App_Economy_Report_Vol._2.pdf

Recicle

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América

Fevereiro de 2014

WGL-03045-USEN-00