Estudo trimestral IBM X-Force Threat Intelligence, 1º trimestre de 2015

Explore as últimas tendências de segurança – de "vulnerabilidades de designers" a mutações de malware – com base nos dados de final de ano de 2014 e em pesquisas contínuas

IBM

Índice

Visão geral executiva

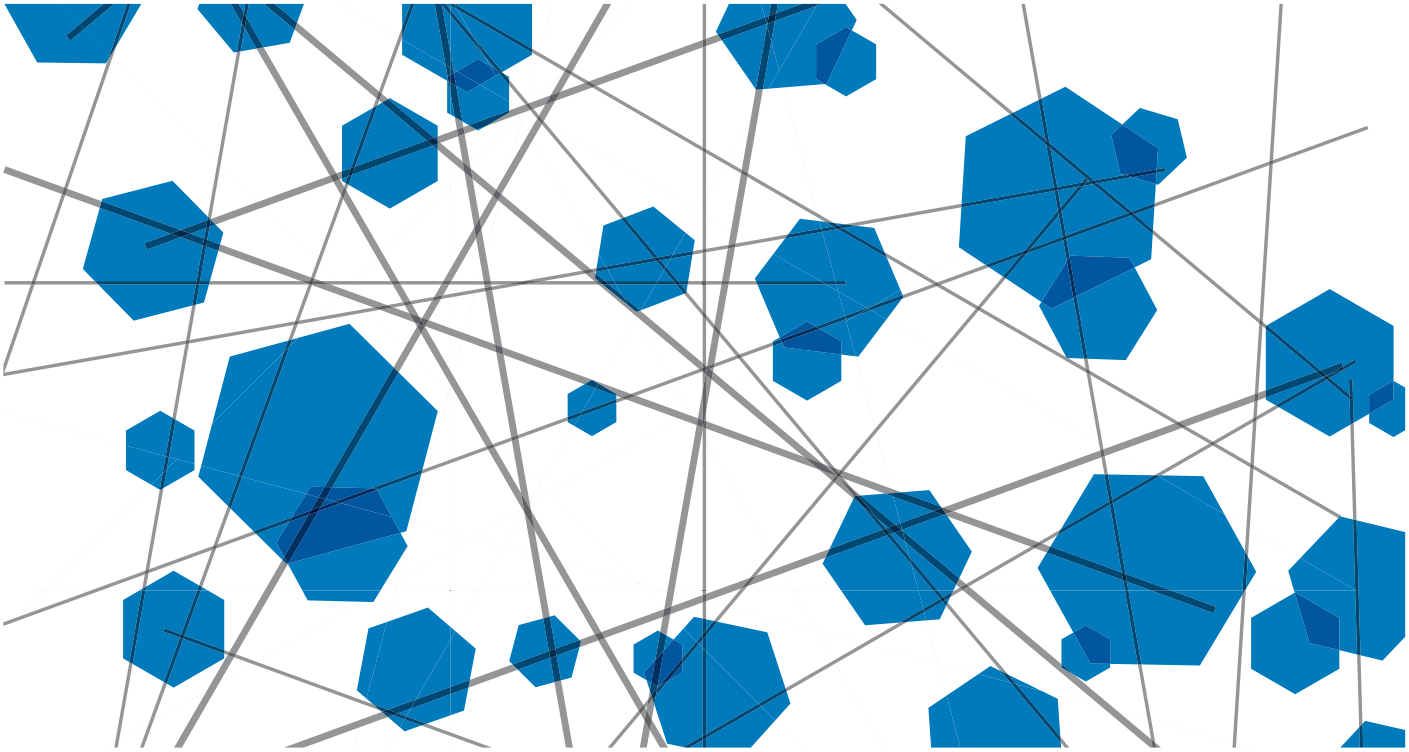
Quando analisamos o passado para revisar e compreender 2014, sabemos com certeza que ele será lembrado como um ano de mudanças significativas.

No início de janeiro de 2014, empresas de grande e pequeno porte juntaram-se para compreender e analisar melhor uma grande violação de varejo que as fez questionar se suas próprias medidas de segurança sobreviveriam ou não à próxima tempestade. Antes do início do segundo trimestre, tivemos nossa primeira experiência com a "vulnerabilidade de designers" – uma vulnerabilidade crítica que se comprovou não apenas letal em termos de ataques direcionados, mas que também apresentava logotipos, websites e nomes de identificação (ou identificadores) desenvolvidos de modo inteligente que identificariam essa divulgação para sempre.

As vulnerabilidades de designers apareceram nas estruturas de base de longa data usadas pela maioria dos websites, e continuaram aparecendo ao longo de 2014, acumulando nomes sempre fáceis de lembrar – Heartbleed, Shellshock, POODLE e, em 2015, Ghost e FREAK. Por si só, isso nos faz questionar o porquê de essa vulnerabilidade ter merecido campanhas de marketing, RP e design de logotipos, enquanto as outras milhares de vulnerabilidades descobertas ao longo do ano não tiveram direito a tudo isso.

As violações e incidentes de segurança foram anunciados tão rapidamente em 2014 que muitos tiveram que se esforçar para acompanhar essas informações. Até o final do ano, começamos a entender que essa tempestade digital de ataques não pararia e, em vez disso, ficaria ainda maior, tornar-se-ia mais abrangente e levantaria preocupações cada vez mais importantes acerca de privacidade pessoal, conforme foi evidenciado pela violação da Sony.

No entanto, as violações de dados e os incidentes de segurança não foram os únicos eventos de atenção de 2014. Nós também observamos uma nova utilização dos familiares e "antigos" malware que, rapidamente, tornaram-se a ferramenta preferida dos criminosos cibernéticos. O malware financeiro Citadel – que, historicamente, é um spawn de configurações do Zeus – adotou uma rota mais silenciosa, transformando-se lenta e furtivamente em novas variantes que, agora, visam aos vendedores e fornecedores do setor petroquímico, bem como ao software de gerenciamento de senhas.



Além das violações, dos incidentes de segurança e dos malware, as divulgações de dispositivos móveis também foram uma grande preocupação. Na verdade, os pesquisadores se aventuraram nas estruturas móveis para encontrar falhas e ajudar os desenvolvedores de software de aplicativos móveis a fazer um melhor trabalho de atualização de suas ferramentas e aplicativos. Até o momento, as divulgações críticas do Apache Cordova – que foram relatadas e corrigidas em julho – ainda estão afetando os aplicativos Android sujeitos a explorações que ainda precisam ser corrigidos ou atualizados. Muitos deles são aplicativos bancários, que são considerados integrantes de uma categoria de alto risco.

Surpreendentemente, até meados de 2014, a IBM® X-Force® estava preparada para declarar uma queda no número total de divulgações de vulnerabilidades relatadas. No entanto, tudo mudou em setembro, quando um pesquisador de Computer Emergency Readiness Team-Coordination Center (CERT Coordination Center) criou e anunciou uma ferramenta automatizada para testar a segurança dos aplicativos Android. Usando essa ferramenta, ele descobriu problemas de segurança em milhares desses aplicativos. Essas vulnerabilidades podem permitir que um invasor realize ataques “man-in-the-middle” (MitM) contra os aplicativos móveis afetados. O anúncio mudou não apenas a contagem de final de ano de 2014, como também o panorama de divulgações.

Terminamos o ano em um processo aterrorizante de análise contínua do estado da segurança da Internet e preparando-nos para uma possível mudança no modo como mediremos as vulnerabilidades nos próximos anos.

Resumo dos incidentes de segurança de 2014

De violações de dados a ransomware, aprenda sobre os temas gerais que surgiram em nossa análise de incidentes de segurança de final de ano.

Da exploração de vulnerabilidades críticas em bibliotecas amplamente utilizadas de código aberto da Internet e preocupações internacionais com a privacidade até um dilúvio de violações de dados altamente propagandeadas, poucas pessoas argumentariam que 2014 tinha tudo para tornar-se uma tempestade perfeita de incidentes de segurança. Analisando os dados mais detalhadamente, essa informação é exagerada ou é um prenúncio do que está por vir?

Devido a algumas estimativas que indicam a existência de mais de um bilhão de vazamentos de e-mails, números de cartão de crédito, senhas e outros tipos de informações de identificação pessoal (PII), é possível que as chances de sofrer impactos causados por um incidente de segurança no ano passado eram bastante altas. De Hollywood à loja local de consertos residenciais, o impacto dos incidentes de segurança sobre nossa vida diária tornou-se cada vez mais disseminado.

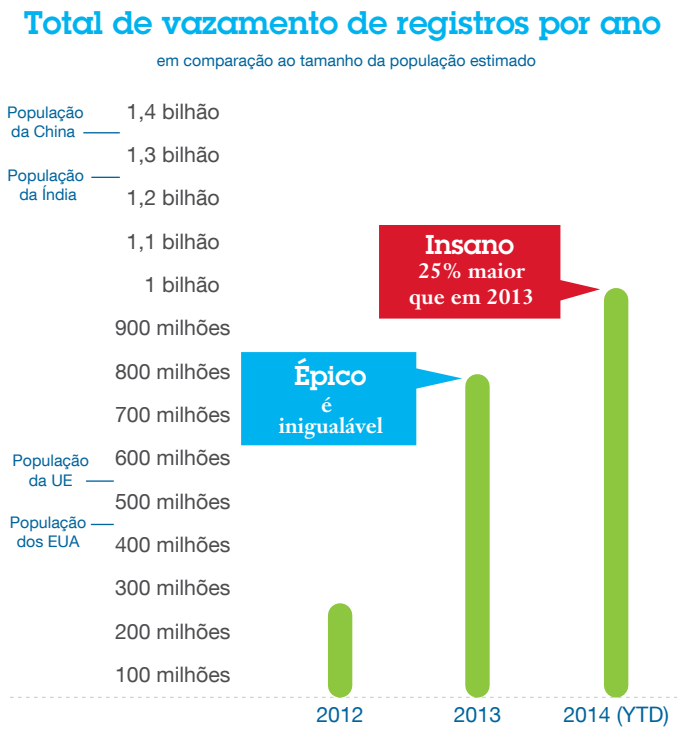


Figura 1. Total de vazamento de registros por ano, em comparação aos tamanhos populacionais estimados

A figura 1 oferece uma perspectiva sobre a aparência de um bilhão ou mais de registros em comparação aos tamanhos populacionais. Embora cada registro violado não necessariamente denote um usuário individual, esta é provavelmente uma porcentagem significativa da população conectada à Internet que experimentou qualquer forma de perda como resultado dos incidentes de segurança de 2014.

Com base puramente no volume, o número total de registros violados em 2014 foi aproximadamente 25% maior que em 2013 (quando vazaram 800 milhões de registros). Em agosto de 2014, uma empresa de segurança anunciou que tinha descoberto um grande volume de credenciais vazadas.[1] No entanto, os detalhes desse anúncio ainda não foram totalmente confirmados; portanto, não incluímos esses registros adicionais em nossos cálculos.

Principais temas relacionados aos incidentes de segurança de 2014

Embora tenham ocorrido vários eventos notáveis ao longo do ano, boa parte das atividades dos incidentes de segurança pode ser vista com base em três temas abrangentes: privacidade em um mundo digital, falhas na base e falta de aspectos básicos de segurança.

Privacidade em um mundo digital

Desde 2013, as preocupações com o monitoramento das comunicações digitais por parte do governo e o problema de manter a privacidade na era da Internet intensificaram-se. Depositamos uma parte de nossa confiança no fato de que os fornecedores de comunicações e os serviços de armazenamento de dados possam adotar medidas adequadas de segurança para manter nossas informações pessoais com confidencialidade. No entanto, conforme os eventos de 2014 demonstraram repetidamente, mesmo quando os principais pontos de entrada são bem protegidos, os invasores buscarão meios alternativos de acesso.

Um dos principais exemplos foi a divulgação pública de fotos confidenciais armazenadas em um serviço em nuvem.[2] Basicamente, não foi a segurança do serviço em nuvem em si que falhou, mas as senhas fracas e perguntas de segurança fáceis de adivinhar dos usuários, combinadas a frouxas políticas de autenticação de força bruta, resultaram em roubo de dados. Embora a tecnologia simplifique o armazenamento de backups na nuvem, ela também inclui uma camada de isolamento para os usuários do dia a dia que não consideram onde seus dados residem e como eles podem estar em risco.

Um incidente semelhante ocorreu quando fotos particulares dos usuários de um aplicativo de mídia social foram vazadas por um serviço de terceiro. [3] Embora o aplicativo principal fosse usado para enviar imagens temporárias, que eram excluídas em questões de segundos após sua visualização, os serviços adicionais do terceiro usaram a interface de programação de aplicativos (API) para salvar o conteúdo para visualização posterior. Quando os invasores conseguiram comprometer o serviço do terceiro, eles tiveram acesso ao conteúdo que os usuários acreditavam ter sido excluído.

Em uma das violações de privacidade mais significativas do ano, as comunicações particulares por e-mail de um grande estúdio de Hollywood (Sony) foram liberadas como parte de um grande vazamento de dados.[4] Oferecendo uma visão dos bastidores do mundo das celebridades e produtores de filmes, muitos sites da mídia discutiram a propriedade intelectual exibida e as conversas particulares liberadas com a informalidade de qualquer outro tipo de fofoca diária.

O impacto dos incidentes de segurança não se limitou somente às interações online. Clientes de varejo, principalmente nos Estados Unidos, foram sujeitos a roubos repetidos de números de cartão de crédito em uma variedade de diferentes restaurantes, lojas e websites de e-commerce. De cadeias de fast-food a lojas de roupas, a conveniência de pagar com cartão de crédito – e as vulnerabilidades dos sistemas que processam esses pagamentos – colocam muitas pessoas em risco.

Falhas na base

Existem mais de um bilhão de websites exclusivos na Internet, e esse número aumenta todos os dias. Uma grande porcentagem desses sites depende dos mesmos sistemas operacionais, de bibliotecas de código aberto e de software de sistema de gerenciamento de conteúdo (CMS).

2014 provou ter sido um ano único, já que as divulgações de vulnerabilidades não afetaram apenas um, mas vários desses sistemas básicos, resultando em uma enorme quantidade de websites explorados.

Esse conceito de procurar as plataformas e serviços populares amplamente utilizados já existe desde os últimos anos, por exemplo, quando as vulnerabilidades do software de CMS resultaram na exploração de milhões de sites. Em 2014, várias das plataformas mais populares de CMS – como WordPress, Joomla! e Drupal – apresentaram grandes vulnerabilidades na plataforma principal e em seus plug-ins bastante utilizados. Também houve vulnerabilidades críticas em software de fórum da Web, como phpBB e vBulletin, que permitiram que os invasores assumissem o controle de servidores da Web.

Essas violações de dados são preocupantes, até mesmo para sites que não contêm dados confidenciais de usuários. A partir de praticamente qualquer website, os invasores podem utilizar violações para introduzir malware ou utilizá-las como bots sob o seu comando e controle para realizar ataques distribuídos de negação de serviço (DDoS) em grande escala. As empresas também enfrentam riscos com os servidores comprometidos que são usados para exportar dados confidenciais ou para atacar seus parceiros de negócios, clientes e cadeia de suprimento.

2014 também foi um ano único, em que as bibliotecas subjacentes que lidam com a funcionalidade criptográfica de praticamente todas as plataformas comuns da Web – incluindo Microsoft Windows, Mac OS X e Linux – foram consideradas vulneráveis a explorações remotas bastante triviais capazes de roubar dados críticos.

A primeira divulgação dessas vulnerabilidades criptográficas remotas ocorreu em abril, quando um erro de dois anos de idade na biblioteca OpenSSL foi divulgado publicamente como CVE-2014-0160 ou “Heartbleed”.[5] Descobriu-se que essa vulnerabilidade podia ser explorada remotamente, permitindo que os invasores obtivessem dados residentes na memória do servidor, incluindo registros de login de usuário, certificados de segurança particulares e outros dados confidenciais. Não apenas os servidores HTTPS da Web foram afetados, mas também todos os dispositivos ou aplicativos que usavam SSL para criptografia poderiam estar vulneráveis.

Embora a vulnerabilidade de OpenSSL tenha afetado principalmente os servidores da Web baseados em UNIX, os servidores da Microsoft também corriam o risco de serem executados remotamente a partir de uma biblioteca de criptografia. Em novembro, foi liberada uma correção para a CVE-2014-6321, que é uma vulnerabilidade do pacote de canais de segurança da Microsoft que afeta todas as versões de desktop e servidor do sistema operacional e que pode permitir que os invasores executem códigos remotos.

Além de exigir uma correção para as vulnerabilidades SSL do UNIX, o OS X também estava suscetível a um ataque "man-in-the-middle" (MitM) apelidado de "Goto Fail" (CVE-2015-1266), no qual os invasores podiam fazer espionagem do tráfego de rede ou interceptar o tráfego de rede criptografado por SSL a partir de pontos de acesso wireless públicos.[6]

O fato de todos esses três eventos terem ocorrido em um só ano é algo significativo, mas também houve várias outras vulnerabilidades de alto impacto ao longo do ano que afetaram um grande número de servidores da Web e terminais. Por exemplo, a família de erros Shellshock do shell bash UNIX (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186 e CVE-2014-7187) pode ser explorada para executar comandos shell remotamente em um servidor vulnerável.[7]

Outra família de vulnerabilidades que afeta os sistemas criptográficos foi chamada de Padding Oracle on Downgraded Legacy Encryption, ou POODLE (CVE-2014-3566 e CVE-2014-8730). Embora ela não seja tão prejudicial quanto a Heartbleed ou Shellshock, quando explorada, a POODLE pode permitir que os invasores realizem um ataque MitM para interceptar uma sessão segura silenciosamente.

Além de desencadear uma tendência identificar as vulnerabilidades de designers de alto perfil com um nome fácil de lembrar e um logotipo, esses tipos de vulnerabilidades afetaram uma grande porcentagem de websites e, em muitos casos, foram bastante fáceis de explorar com o uso de scripts e ferramentas automatizadas.

A falta de aspectos básicos de segurança

Durante muitos anos, a X-Force ofereceu recomendações sobre a importância de adotar aspectos básicos de segurança como um modo eficaz de proteger-se contra o impacto de uma violação de segurança e de minimizá-lo. Isso foi válido tanto em 2014 quanto nos anos anteriores.

Um dos melhores exemplos da importância dos aspectos básicos de segurança está relacionado à segurança das senhas, que continua sendo um fator principal das violações de dados. Seja porque os usuários têm senhas fracas ou previsíveis, ou porque reutilizam senhas na Internet e na empresa, a capacidade dos invasores de obter acesso como resultado de políticas de autenticação mal gerenciadas é preocupante.

Existem milhões de endereços de email e senhas simples conhecidos, que foram obtidos em anos de violações de dados anteriores e que podem ser usados para tentar obter acesso a outros sites. Esses dados ajudam os invasores a enumerar as senhas comuns, e fazem com que as pessoas que reutilizam senhas em vários sites corram o risco de terem suas contas controladas por meio de força bruta. Em um exemplo notável, mais de seis milhões de contas de um popular provedor de armazenamento em nuvem8 foram comprometidas. Embora o provedor de armazenamento em nuvem em si não tenha sofrido violação, os dados de login de outras violações, bem como malware, keyloggers e táticas de phishing, permitiram que os invasores acessassem essas contas.

O uso de senhas padrão também continua sendo um problema. Várias violações de varejo no ano passado foram realizadas por invasores que acessaram remotamente os servidores de ponto de venda (POS)[9] usando logins padrão ou conhecidos de software de compartilhamento de tela usado para fins legítimos de resolução de problemas de suporte técnico. Essas violações demonstram que as práticas básicas de segurança, como alterar as senhas padrão de contas, ainda não estão sendo implementadas devidamente.

Tipos e setores dos ataques

Todos os anos, a X-Force rastreia uma amostragem de incidentes de segurança por tipo e setor do ataque. Como nos anos anteriores, é interessante analisar esses dados para descobrir tendências. A figura 2 representa a iteração mais recente, mostrando um número de incidentes que foram divulgados publicamente em 2014.

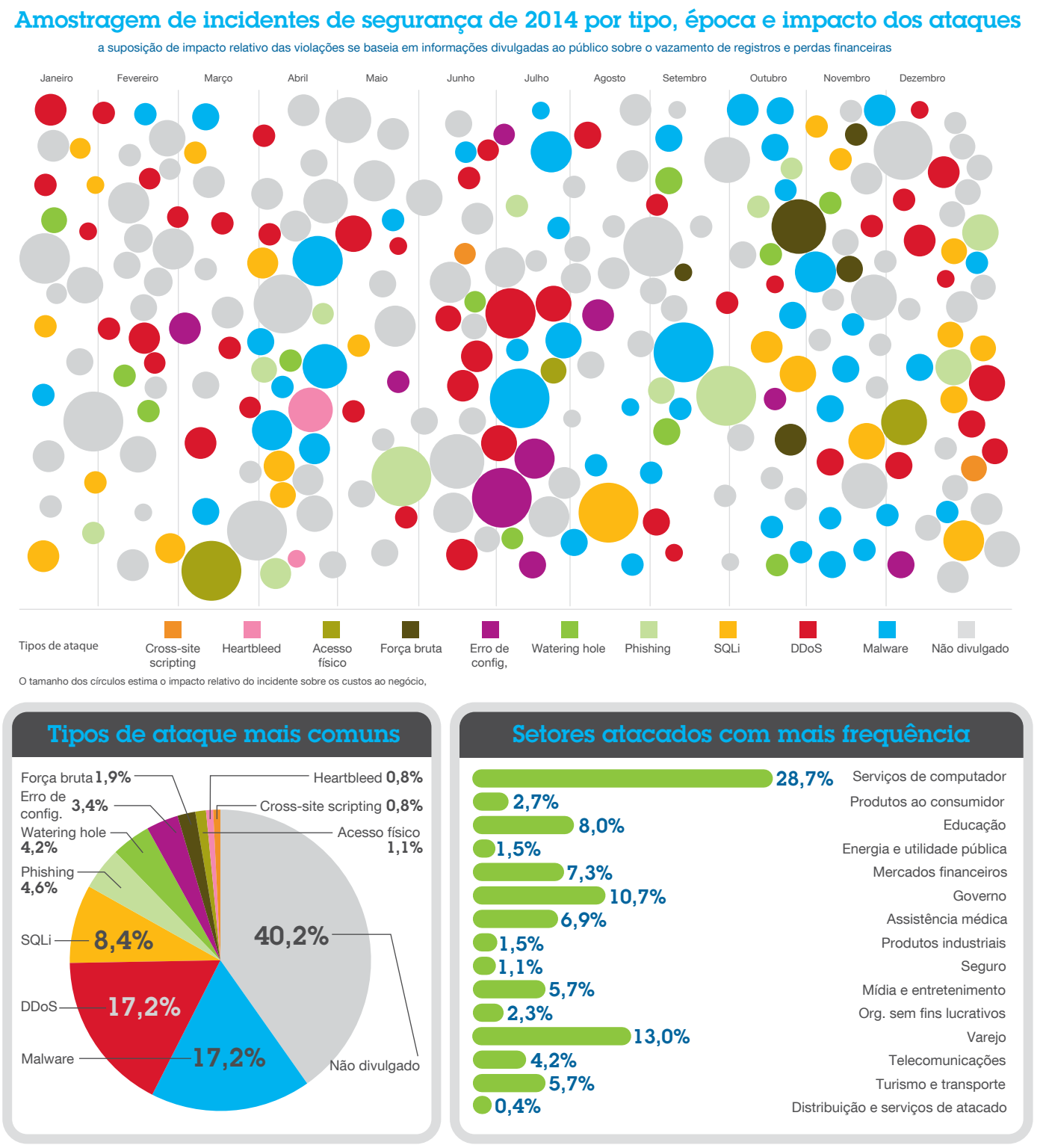


Figura 2. Amostragem de incidentes de segurança de 2014 por tipo, época e impacto dos ataques

Figura 3. Amostragem de incidentes de segurança de 2014 por país

De modo similar aos anos anteriores, o número de incidentes nos Estados Unidos é muito maior que em outros países. Isso provavelmente ocorre devido às leis de divulgação dos Estados Unidos, que são mais rígidas que as de outros países, resultante em incidentes mais divulgados publicamente. Além disso, nos Estados Unidos, há websites com perfil mais alto que em outros países. A República da Coreia passou por vários incidentes graves em 2014 que afetaram grandes porcentagens da população.

Como mencionado anteriormente, o setor de varejo, principalmente nos Estados Unidos, foi extremamente afetado. O sinal foi dado ao final de 2013, com uma grande violação das lojas Target, que afetou mais de 70 milhões de compradores[10] e continuou em 2014, com violações que afetaram algumas cadeias nacionais de restaurantes e lojas de varejo. Utilizando uma metodologia similar ao longo do ano, os invasores obtiveram acesso a essas empresas invasores um meio por meio de técnicas como spear phishing. Depois de obter acesso, eles conseguiam instalar um malware de remoção de RAM em sistemas de processamento de cartões, que podia registrar os dados de cartões criptografados à medida que eles eram transferidos em texto simples na memória do servidor. Assim, os dados roubados de cartão de crédito puderam ser exportados e vendidos no mercado negro.

Alguns negócios que auditaram seus próprios sistemas como resultado desse amplo padrão de ataques, descobriram malware que estavam sendo executados sem detecção por períodos que variavam de algumas a semanas a vários anos.

Os ataques de malware superam o SQLi

A divulgação quase semanal do malware de POS de varejo foi apenas um dos vários vetores de grandes ataques descobertos em 2014. Nos últimos anos, a X-Force relatou sobre a eficácia dos ataques de injeção de SQL (SQLi) como um meio de extrair dados dos servidores da Web e aplicativos. Historicamente, o SQLi era a principal causa dos incidentes de segurança. No entanto, em 2014, em relação aos incidentes rastreados pela X-Force, os ataques de malware e DDoS assumiram a liderança em termos de volume dos tipos de ataques de incidentes de segurança.

2004 também experimentou vulnerabilidades disseminadas de SQLi que resultaram em exploração e perda de dados em grande escala. O que é mais notável é que as vulnerabilidades das plataformas de CMS ofereceram aos invasores um meio de atingir muitos alvos usando uma quantidade mínimo de esforços. Por exemplo, acreditava-se que uma bolsa de valores da Polônia[11] tivesse sido violada por meio de uma vulnerabilidade conhecida de SQLi na plataforma de CMS Joomla!, ao passo que uma grande vulnerabilidade de SQLi na plataforma de CMS Drupal colocou centenas de milhares, se não milhões, de servidores em risco de exploração.[12] Ao final do ano, uma vulnerabilidade de SQLi em um website de seguro viagem australiano resultou no vazamento de mais de 750.000 de registros, o que representou uma das maiores violações da Austrália até o momento.[13]

As plataformas de CMS também foram afetadas por plug-ins inseguros. Os relatórios anteriores da X-Force abordaram o modo como, muitas vezes, os plug-ins de CMS são criados por pequenos grupos de desenvolvimento de terceiros que estão tentando resolver um problema de nicho e que, consequentemente, podem não empregar a proteção de segurança adequada. Esse foi o caso de uma vulnerabilidade de um popular plug-in deslizante do WordPress, que permitiu que os invasores injetassem JavaScript malicioso em mais de 100.000 websites.[14]

Os ataques DDoS também foram as manchetes dos últimos anos, à medida que o volume de tráfego direcionado a um só servidor e datacenter aumentou significativamente. Não é incomum ouvir falar sobre ataques DDoS que consomem mais de 100 Gbps de largura de banda, enquanto outros consomem até 400 ou 500 Gbps. Grandes ataques como esses podem controlar não apenas um só website, mas também outros sites do mesmo datacenter à medida que o tráfego transborda, saturando a largura de banda disponível.

Nos últimos anos, os ataques DDoS também foram usados como uma distração, como cobertura para a violação de um alvo. Em um caso infeliz nos Estados Unidos, vários danos financeiros e de propriedade intelectual causados por um paralisante ataque DDoS e por uma violação simultânea de dados resultaram no encerramento de um provedor de hospedagem de código fonte.[15] Outro provedor de email com base na Web da Irlanda teve que encerrar suas operações durante um período de tempo para minimizar uma tentativa de DDoS e violação de alto volume, deixando os clientes sem acesso a seu correio da Web.[16]

Nos últimos anos, o encerramento de um website com um ataque DDoS foi usado como uma forma de "hacktivismo" para protestar contra entidades governamentais. Esses tipos de ataques continuaram acontecendo durante 2014, embora o impacto do encerramento do website público de uma cidade ou de um partido político nem sempre seja claro de um ponto de vista operacional ou corporativo. Um tipo de impacto significativo pode assumir a forma de comunicações interrompidas, como foi o caso no Arizona, onde um protesto de DDoS encerrou um website de interação com o público[17] que os agentes da polícia usam remotamente em seus veículos para obter informações críticas durante suas rondas.

Aumentos de ransomware em 2014

Os ataques DDoS também foram usados como uma forma de "ransomware" ou extorsão durante o ano. Vários websites bem-estabelecidos[18] foram notificados que seriam direcionados por um ataque DDoS, a menos que pagassem um resgate que variava de algumas centenas a muitos milhares de dólares. A maioria desses negócios optou por não pagar o resgate e, embora tenha sofrido tempo de inatividade como resultado das ameaças de DDoS, conseguiu recuperar o serviço sem ter que ceder às demandas dos invasores.

O que é um resgate criptografado?

O ransomware mantém um sistema como refém criptografando dados e exigindo que os usuários paguem um "resgate" para obter as chaves necessárias para recuperar os dados. Geralmente, as instruções de pagamento são exibidas em uma mensagem enviada ao usuário; muitas vezes, os pagamentos têm um prazo, e a quantia pode aumentar se o pagamento for efetuado além da data especificada. Geralmente, o ransomware exige o pagamento usando uma "micro moeda", como Bitcoin, para reduzir o risco ao invasor. Os software de segurança podem detectar um ataque de resgate criptografado desde o início, já que a criptografia pode demorar certo tempo para ser concluída. A remoção imediata do malware pode ajudar a limitar os danos que ele pode causar, mas pode impedir a recuperação dos dados que já foram processados.

O que você pode fazer para se proteger? Etapas simples, como realizar backups regulares e manter software antivírus e correções atualizados para seu sistema operacional, são apenas algumas dicas. Para aprender mais maneiras de proteger-se, consulte o alerta US-CER sobre ransomware criptográfico.

Direcionando indivíduos ou empresas, o ransomware pareceu estar em alta em 2014. Esses tipos de ataques se enquadraram em várias categorias. Um tipo, descrito anteriormente, envolve a extorsão de negócios para que eles paguem uma taxa e evitem um ataque DDoS ou o vazamento público de dados. Um segundo tipo de ataque assume a forma de um esquema de resgate criptografado, no qual os criminosos direcionam negócios e usuários residenciais. Os invasores de ransomware bloqueiam e criptografam os dados, impedindo que os usuários acessem seus próprios dados, computadores ou dispositivos móveis; em seguida, eles exigem um pagamento, geralmente em Bitcoin, em troca pela chave de desbloqueio. O sucesso das campanhas de resgates criptografados resultou em um aumento desses tipos de ataques, e as versões mais recentes dos kits de ferramentas de ransomware tornaram-se cada vez mais avançadas e difíceis de desativar.

A cidade de Detroit[19] foi direcionada por um esquema assim, no qual os invasores exigiram o equivalente a US$ 800.000 em Bitcoin para liberar um banco de dados da cidade que eles tinham criptografado. Felizmente, o banco de dados não era mais necessário e a tentativa de extorsão não foi bem-sucedida.

Muitas vezes, os incidentes de segurança que resultam em sistemas temporariamente offline – ou que resultam no roubo de dados pessoais e informações financeiras – deixam os sistemas subjacentes intactos. Por outro lado, alguns ataques são desenvolvidos para causar danos permanentes, seja excluindo discos rígidos e apagando o Registro de Inicialização Principal (tornando-o inutilizável) ou destruindo sistemas físicos, como os usados pelas empresas industriais e de manufatura.

Vários incidentes ao longo do último ano resultaram em danos desses tipos, e o mais notável deles foi o ataque à Sony,[20] no qual um malware wiper foi usado para desabilitar os sistemas de terminais. Na Alemanha,[21] um ataque de spear phishing resultou em grandes danos a um alto-forno de uma aciaria. Os servidores Microsoft Active Directory de uma empresa de cassinos também foram direcionados por malware wiper,[22] embora, nesse caso, ele tenha impedido a habilidade do invasor de obter acesso a sites internacionais e tenha limitado o ataque somente a propriedades dos EUA.

Em 2012, o termo "watering hole" foi introduzido para descrever ataques que direcionam grupos específicos de usuários, injetando códigos maliciosos nos websites onde esses usuários interagem. Vários novos ataques de watering hole ocorreram em 2014, como um ataque que direcionou os leitores de websites de notícias militares e sobre defesa.[23] Em outro caso, pesquisadores descobriram códigos maliciosos[24] em um website industrial que atendia empresas automotivas, aeroespaciais e de manufatura.

O malvertising é um tipo de ataque similar a um ataque de watering hole. Ele é um vetor de exploração que consiste em uma rede de núncios comprometida que fornece códigos maliciosos que foram injetados em anúncios exibidos em sites legítimos. Isso permite que os invasores atinjam um público muito maior, em vez de comprometer um só website. Além disso, ele serve como um modo de direcionar as empresas que podem ter uma segurança mais rígida em seus próprios servidores, mas que, sem saber, fornecem anúncios maliciosos que estão integrados em seu conteúdo.

Nos ataques de watering hole e malvertising, os invasores conseguem implementar kits de exploração em terminais vulneráveis, aproveitando várias vulnerabilidades baseadas em navegador e direcionando plug-ins, como Java e Adobe Flash.

Conclusão

Embora os tipos gerais de ataques permaneçam consistentes todos os anos, as aplicações criativas desses componentes básicos fundamentais podem variar significativamente. Uma análise das violações de 2014 mostra uma combinação de invasores que direcionaram alvos mais fáceis (por exemplo, executando scripts contra as vulnerabilidades conhecidas) ou que utilizaram explorações sofisticadas e personalizadas para atingir alvos mais difíceis com precisão cirúrgica.

Em resposta à alta capacidade, ao volume e à natureza dos ataques que aumentaram continuamente com o passar do tempo, a X-Force está lançando o website Interactive Security Incident (ISI) para ajudar os usuários a obter um entendimento detalhado sobre os eventos de segurança do ano atual e para oferecer uma perspectiva histórica de como os eventos de segurança evoluíram com o passar dos anos. Incentivamos todos a visitar esse site com frequência e, assim, permanecer atualizados sobre as violações e incidentes de segurança mais recentes à medida que eles forem confirmados pelas fontes públicas.

Para obter uma visão geral de três anos de incidentes de segurança, faça o download do pacote de gráficos do 1º trimestre de 2015 da X-Force (X-Force 1Q 2015 Graphics)

Para explorar o website Interactive Security Incident da X-Force agora, acesse:

***ibm.com**/security/xforce/xfisi/*

Citadel, o malware financeiro que continua se adaptando

Como você pode proteger-se contra os malware em constantes mutações? Aprenda sobre as variantes mais recentes do Citadel e como os alvos mudaram para além do setor financeiro.

Nos últimos oito anos, os malware financeiros passaram por muitas mudanças significativas. Elas incluem métodos evoluídos de roubo de dados (desde o uso de simples recursos de keylogging à implementação de crimeware totalmente automático que pode controlar dispositivos e capturar dados e credenciais), distribuição e entrega de malware a dispositivos direcionados, introdução de novas "atualizações de segurança" que permitem que os malware burlem a detecção, e muitas outras.

Uma dessas mudanças recentes dos malware é o tipo de alvos que eles direcionam. No passado, diversas variantes de malware financeiro direcionaram instituições não financeiras, incluindo sites de e-commerce, companhias aéreas, hotéis, organizações de assistência médica e empresas de jogos online. Agora, a lista se ampliou ainda mais. Uma variante do Citadel,[25] um popular malware financeiro, direciona vendedores e fornecedores petroquímicos, bem como software de gerenciamento de senhas — com o objetivo aparente de oferecer aos invasores o acesso à propriedade intelectual corporativa confidencial, e não aos dados financeiros.

Além disso, embora a maioria dos ataques use ferramentas de acesso remoto (RATs) e malware especialmente projetados, daqui a um tempo, poderemos ver o uso crescente de malware "à prova de batalhas", como o Citadel, obtendo acesso a diferentes tipos de organizações.

A evolução do Zeus do pioneirismo à utilização em massa

Quando os malware financeiros surgiram, havia apenas um malware que se destacava de todos os outros em termos de capacidade e usabilidade – Zeus. Rapidamente, ele se transformou na ferramenta preferida dos criminosos cibernéticos, já que permitia uma fácil configuração sem a necessidade de codificação, além de oferecer várias maneiras de extrair credenciais de suas vítimas. O Zeus v2 foi introduzido no final de 2009, mas, 18 meses depois, seu código fonte foi vazado em fórum clandestino. O vazamento permitiu que os criminosos cibernéticos desenvolvessem suas próprias variantes e, essencialmente, eliminou a necessidade de comprar o malware do grupo de venda.

Muitas discussões no fórum clandestino teorizaram o porquê de o código fonte ter sido vazado. Segundo um dos rumores, Slavik,[26] o alias do codificador do Zeus, teria discutido com as pessoas da equipe, e decidido iniciar seu próprio empreendimento privado e destruir o negócio da gangue. De qualquer forma, o efeito do vazamento do código fonte não demorou muito para materializar-se – e, logo depois, apareceram as novas variantes do Zeus. Essas variantes assumiram a forma de simples malware, como o Ice IX, até variantes bastante complexas, como o GameOver Zeus. Além disso, outras famílias de malware roubaram partes do código para implementar módulos específicos, como o Ramnit, que rouba o módulo de conexão de rede virtual (VNC). Uma dessas variantes foi o Citadel, que foi introduzido no mercado no final de 2011 e oferecia alguns recursos exclusivos.

Evolução do Citadel com o passar do tempo

O Citadel foi introduzido em um fórum clandestino da Rússia e oferecia aos criminosos cibernéticos uma nova ferramenta avançada que englobava as capacidades "clássicas" do Zeus, além de novos recursos. A publicação original no fórum indicava que o malware era "compatível com Zeus", o que significava que os arquivos de configuração e as injeções de HTML que foram usados com as versões mais antigas do Zeus funcionariam com o Citadel. A propaganda destacava que o Citadel permitia que o invasor executasse comandos shell a partir do dispositivo infectado (permitindo que um invasor, dentre outras coisas, mapeasse a rede onde o dispositivo foi infectado – obviamente, direcionando muito mais que apenas dados financeiros). A propaganda também indicava que o malware não funcionaria em dispositivos que utilizassem um layout de teclado cirílico, já que os autores não queriam direcionar sistemas russos ou ucranianos.

Além desses recursos, os compradores do Citadel podiam influenciar versões futuras, participando de pesquisas iniciadas pela equipe do Citadel. Essas pesquisas pediam que os usuários escolhessem os recursos que gostariam de ver nas futuras versões. Assim que um recurso recebesse um voto majoritário e uma quantia mínima de dinheiro, a equipe do Citadel se comprometia a desenvolvê-lo.[27]

As novas variantes do Citadel começaram direcionando instituições financeiras de todo o mundo com os recursos solicitados pelos usuários, que eram novos naquela época. Por exemplo, o módulo VNC permitia que os invasores controlassem os dispositivos infectados – superando os sistemas de reputação de ID e IP dos dispositivos. Outras variantes incluíam recursos de captura de vídeo, que permitiam que os invasores monitorassem os desktops dos usuários para aprender seu comportamento e padrões de cliques ao acessar aplicativos financeiros online.

Gráfico 1. Votos para recursos na "Citadel Store" (fonte: Brian Krebs)

Com o passar do tempo, o Citadel continuou evoluindo, liberando novas versões como v1.3.4.x e v1.3.5.x, e recursos como localização automática de conteúdo para fraude.[28] Uma variante interessante se expandiu com base na persistência do malware – ou, em termos mais precisos, constitui a habilidade de seu operador em controlar um dispositivo infectado. O VNC integrado do Citadel (o VNCfox) também se comprovou como uma ferramenta valiosa nas mãos dos criminosos cibernéticos.

No entanto, à medida que o malware Citadel foi ganhando popularidade, uma quantidade crescente de desenvolvedores de software antivírus e antimalware incluiu ferramentas de detecção e remoção para essa ameaça. Uma variante do Citadel tinha a solução para esse problema. Um invasor conseguiu usar a funcionalidade "AutoCMD" dessa variante do Citadel para executar comandos shell a partir de um dispositivo infectado. Após a infecção, essa variante criou um novo usuário no dispositivo infectado e o adicionou ao grupo nativo do Remote Desktop Protocol (RDP) do Microsoft Windows. Ao fazer isso, mesmo se o malware fosse removido do dispositivo infectado, o operador ainda tinha uma porta dos fundos para o dispositivo, usando o Windows RDP.

Além disso, os pesquisadores da IBM Security Trusteer® descobriram[29] que o Citadel também pode ser usado para direcionar novas entidades e software. Os alvos "clássicos" do Citadel eram de natureza financeira, como bancos, uniões de crédito ou e-commerce. No entanto, as novas variantes descobertas estão direcionando vendedores e fornecedores petroquímicos, além de software de gerenciamento de senhas. Considerando-se o histórico bem-sucedido do Citadel de infectar e roubar dados – além de suas habilidades de atravessar a rede de um dispositivo infectado, executar comandos e controlar dispositivos infectados e novos alvos –, parece que esse malware está deixando de promover fraudes para tornar-se uma ferramenta de crimes cibernéticos para ataques direcionados.

O que você pode fazer para proteger-se do Citadel?

À medida que o Citadel evolui e muda seus alvos e métodos de ataques, os usuários finais e empresas também devem mudar e adaptar-se. Para proteger-se melhor dessas ameaças, é necessário adotar uma combinação de proteção dos terminais e de detecção criminosa e de malware com base em nuvem para as instituições financeiras. As empresas também devem adotar proteção avançada contra malware.

A proteção de terminais pode ajudar os usuários a imunizar seus dispositivos contra infecção por malware e a remover as ameaças existentes. A detecção com base na nuvem pode ajudar a detectar malware em dispositivos não protegidos, e a detecção criminal pode identificar os ataques de controle de contas provenientes de um dispositivo criminoso, ou até mesmo os ataques que usam o dispositivo da vítima como proxy. As empresas devem proteger os dispositivos dos funcionários com proteção avançada contra malware, a fim de identificar as tentativas de infecção e os ataques direcionados que utilizam software popular, como produtos Java, Adobe, Microsoft, entre outros. Além disso, as grandes organizações devem usar sistemas avançados de proteção contra malware para identificar as tentativas de roubo de dados, que são a etapa final da maioria dos ataques direcionados.

Os desenvolvedores de aplicativos móveis para Android estão colocando seus usuários em risco?

As vulnerabilidades de aplicativos móveis estão crescendo mais que nunca. Saiba como o setor está reagindo e o que os desenvolvedores podem fazer para ser mais proativos.

O panorama do desenvolvimento móvel continua se fragmentando devido aos muitos dispositivos e plataformas disponíveis – cada um deles com sua própria linguagem de programação e sua estrutura de desenvolvimento. Dessa forma, os desenvolvedores estão enfrentando cada vez mais desafios para direcionar todas essas muitas plataformas.

Portanto, as estruturas que permitem o desenvolvimento de multiplataforma a partir de um só código de base estão em alta e são cada vez mais populares na comunidade de desenvolvimento de aplicativos.

O Apache Cordova (anteriormente conhecido como PhoneGap) é uma plataforma que permite que os desenvolvedores usem o HTML5 como uma só tecnologia de desenvolvimento de multiplataforma. De acordo com a AppBrain,[30] o Cordova é usado em aproximadamente 6% de todos os aplicativos Android. Além disso, ele é prevalecente em categorias que podem ser de alto interesse para invasores, como as categorias corporativa, médica e financeira, onde mais de 12% de todos os aplicativos de cada respectiva categoria se baseiam no Cordova.

Em julho de 2014, a IBM X-Force descobriu uma série de vulnerabilidades na versão do Cordova para Android, que foram divulgadas de modo particular para a Apache Foundation. As correções ou minimizações dessas vulnerabilidades foram fornecidas pela equipe de desenvolvimento do Cordova em agosto,[31] e uma consultoria de segurança técnica foi publicada junto com a divulgação pública das vulnerabilidades. Para destacar a gravidade das vulnerabilidades em relação à sua capacidade de exploração real, também demonstramos uma prova de conceito[32] que mostrava como um ataque completo e remoto pode ser interpretado e realizado e que acompanhava detalhes técnicos.

Quais são as divulgações de vulnerabilidades para a versão do Cordova para Android?

Scripting multiaplicativos do Apache Cordova (CVE-2014-3500)

Essa vulnerabilidade permite que um invasor execute código JavaScript no contexto do aplicativo Android, rompendo o mecanismo de proteção do ambiente de simulação da plataforma. O invasor pode explorar essa vulnerabilidade para roubar informações confidenciais, como o arquivo de cookies do aplicativo. Além disso, essa vulnerabilidade pode ser acionada por meio de um malware residente no dispositivo da vítima (contexto local) ou, em determinadas circunstâncias, também pode ser acionado remotamente (como por meio de um ataque de drive-by download).

Bypass da lista de desbloqueio do Cordova para URLs não relacionadas a HTTP (CVE-2014-3501) e vazamentos de dados a outros aplicativos por meio de URIs Android intencionais (CVE-2014-3502)

O Android oferece um mecanismo de lista de desbloqueio que, teoricamente, quando for configurado corretamente, deve impedir que um invasor faça solicitações a terminais arbitrários que estão sob o controle do invasor. Essas duas vulnerabilidades oferecem um mecanismo de bypass ao recurso de segurança da lista de desbloqueio que pode ser explorado por um invasor para exportar dados (por exemplo, os invasores podem combinar o mecanismo de bypass com uma exploração da vulnerabilidade de scripting multiaplicativos descrita anteriormente para exportar dados).

No momento da divulgação pública, começamos a rastrear os aplicativos Android de várias categorias que se baseiam no Cordova. Desses aplicativos, inicialmente descobriu-se que 91% estavam sujeitos a exploração.

Continuamos rastreando esses aplicativos durante um período de seis meses para ver com que rapidez os desenvolvedores conseguiriam aplicar a correção aos seus aplicativos. Os resultados desse rastreamento podem ser observados na figura 4.

Em outubro de 2014, começamos a rastrear 17 aplicativos financeiros adicionais para determinar a resposta dos desenvolvedores nessa categoria de alto risco.

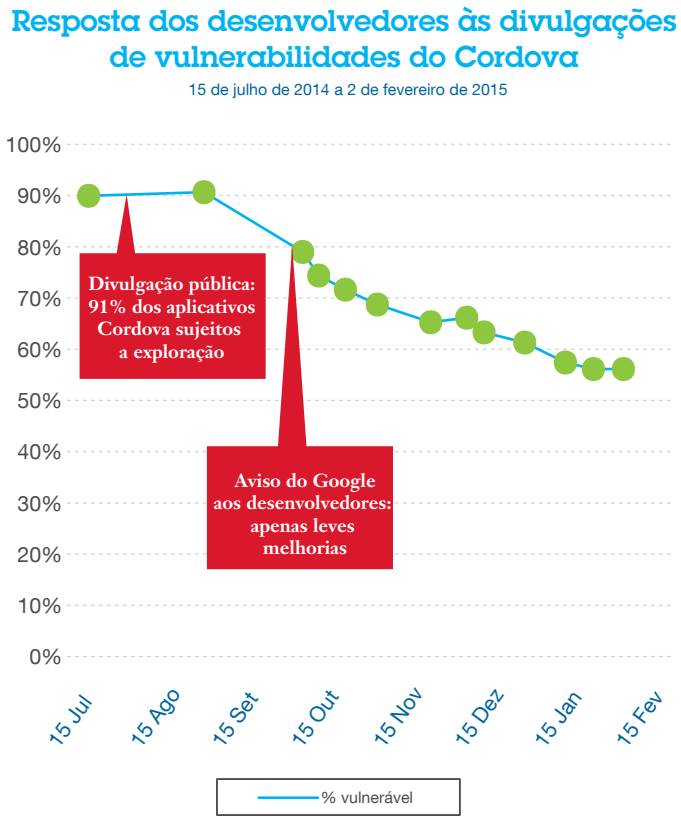


Figura 4. Resposta dos desenvolvedores às vulnerabilidades após as divulgações, 15 de julho de 2014 a 2 de fevereiro de 2015

O que é interessante é a aparente apatia dos desenvolvedores para fazer os esforços necessários para manter os usuários seguros. Embora essa reação possa ser esperada dos desenvolvedores de aplicativos da categoria geral de aplicativos (principalmente os aplicativos que não contêm informações atraentes para um invasor), essa aparente apatia é surpreendente dos desenvolvedores de aplicativos financeiros. Esses aplicativos podem ser considerados como alvos de alto valor para um invasor (por exemplo, porque alguns aplicativos financeiros permitem transferências de dinheiro online) e, considerando-se a baixa complexidade de um ataque como esse, poderíamos esperar uma resposta imediata por parte dos bancos, a fim de proteger seus clientes. No entanto, em janeiro de 2015, 10 dos 17 aplicativos financeiros que rastreamos (59%) ainda estavam vulneráveis – exatamente o mesmo número de aplicativos vulneráveis de quando começamos nossos rastreamentos em outubro!

No início de outubro de 2014, o Google enviou uma mensagem[33] aos desenvolvedores de aplicativos utilizando uma versão vulnerável do Cordova, pedindo que eles atualizassem para uma versão não vulnerável assim que possível ou correriam o risco de sanções contra seus aplicativos no Google Play.

Mensagem do Google aos desenvolvedores do Cordova

"Observem que os aplicativos com vulnerabilidades que exponham os usuários ao risco de comprometimento podem ser considerados 'produtos perigosos' e sujeitos a remoção do Google Play."

Após essa comunicação com os desenvolvedores do Google, observamos algumas melhorias nas atualizações de aplicativos de categoria geral; no entanto, aparentemente, os desenvolvedores de aplicativos financeiros continuam não respondendo a essas vulnerabilidades, já que as atualizações estão estagnadas.

Acreditamos que a tendência de não atualização identificada nesse caso é preocupante. É difícil encontrar justificativas para a não realização de ações imediatas para proteger os usuários finais – principalmente em casos de possíveis danos financeiros. Portanto, fica claro que os desenvolvedores de aplicativos precisam realizar mais esforços e assumir mais responsabilidades, já que são eles os responsáveis finais por manter os dados dos usuários seguros contra danos.

Recomendações

Os desenvolvedores devem ser proativos nas medidas adotadas para manter seus usuários seguros. Isso inclui estar ciente das atualizações de segurança que podem estar disponíveis para todo software de terceiros que puder ser utilizado. Muitos projetos de terceiros oferecem listas de distribuição ou blogs que podem ser usados para essa finalidade. Os desenvolvedores também devem ter processos implementados que permitem a rápida implementação e utilização de correções de segurança.

As grandes empresas devem considerar estabelecer equipes de resposta a incidentes de segurança dos produtos (PSIRTs), responsáveis por rastrear as vulnerabilidades dos produtos internos e por garantir que os desenvolvedores sejam notificados e realizem todas as ações necessárias.

O setor deve fornecer melhores mecanismos para garantir que os aplicativos sejam mantidos atualizados em relação ao software de terceiros. Muitas vezes, os desenvolvedores estão cientes das correções de segurança; no entanto, eles podem ter dificuldades para responder rapidamente a elas por vários fatores, como APIs em constantes mudanças, processos de construção de versão fixa e outros problemas que podem causar trabalhos significativos de desenvolvimento ou introduzir o risco de novos erros de software. Possivelmente, todos esses fatores diminuem o custo-benefício das atualizações. Portanto, as estruturas devem manter a compatibilidade com versões anteriores e, quando possível, fornecer atualizações aperfeiçoadas no processo de construção.

Além disso, o setor deve considerar a separação completa das estruturas em relação ao código do aplicativo, permitindo que as atualizações de software de terceiros sejam implementadas independentemente das atualizações dos desenvolvedores. Para que isso seja viável, esses projetos precisam oferecer APIs estáveis e compatíveis com versões anteriores, e garantir um alto nível de confiança no fato de que as atualizações automáticas não romperão o código do aplicativo.

Abalando as bases: divulgações de vulnerabilidades de 2014

Em nossa análise de vulnerabilidades de final de ano, aprenda como uma ferramenta de teste automatizada pode transformar o panorama de divulgações.

Desde 1997, a IBM X-Force está documentando divulgações públicas de vulnerabilidades de segurança. Nossos pesquisadores coletam consultorias de software de fornecedores, leem listas de distribuição relacionadas à segurança e analisam centenas de páginas da web com vulnerabilidades, onde dados, explorações e vulnerabilidade de recursos foram divulgados. Essa pesquisa está catalogada no banco de dados da X-Force que, hoje, contém mais de 88.000 vulnerabilidades exclusivas e serve como base para a plataforma IBM Security Network Protection.

Todas as vulnerabilidades catalogadas no banco de dados da X-Force são identificadas por um ID único da X-Force (XFID). Os novos XFIDs são atribuídos de acordo com as mesmas decisões de conteúdo que devem ser tomadas pelas CVE Numbering Authorities (CNAs) ao criar novos identificadores de CVE.[34] A X-Force monitora continuamente a lista oficial de CVE e inclui no em seu banco de dados todas as vulnerabilidades que são atribuídas a um identificador oficial de CVE. No entanto, uma vulnerabilidade não precisa ter um identificador de CVE para ser incluída no banco de dados da X-Force. No momento desta publicação, em toda sua história, a X-Force já documentou aproximadamente 20.000 vulnerabilidades que ainda não têm um identificador de CVE atribuído. Além disso, desenvolvimentos recentes podem aumentar esse catálogo drasticamente.

Exemplos de vulnerabilidades sem um identificador oficial de CVE

Muitas vezes, as vulnerabilidades são atribuídas a identificadores oficiais de CVE muitas semanas, meses ou anos depois de sua divulgação pública. Geralmente, isso ocorre quando as divulgações de vulnerabilidades são feitas por fornecedores ou pesquisadores de segurança que não são de nível corporativo e que não seguem as práticas padrão de divulgação. Isso também pode ocorrer quando um novo identificador de CVE não é solicitado formalmente pelo pesquisador.

A seguir, mostramos alguns exemplos de vulnerabilidades do banco de dados da X-Force que ainda não têm identificadores de CVE atribuídos. É possível que, futuramente, a MITRE emita um identificador de CVE a todas essas vulnerabilidades. O que é importante para a equipe do banco de dados da X-Force – e sobre fatores de proteção antecipada contra ameaças à plataforma IBM Security Network Protection – é que a vulnerabilidade seja registrada e, quando possível, receba uma proteção antecipada distintiva.

Spoofing de nomes de arquivos do WinRAR
- XFID da divulgação relatada em: **23 de março de 2014**
- Cobertura da IBM Security Network Protection fornecida em: **13 de maio de 2014**

Execução de código de remota CreateProcess do MicroSCADA Wserver
- XFID da divulgação relatada em: **5 de abril de 2013**
- Cobertura da IBM Security Network Protection fornecida em: **7 de julho de 2014**

Execução de código de remota do MicroSCADA Wserver
- XFID da divulgação relatada em: **5 de abril de 2013**
- Cobertura da IBM Security Network Protection fornecida em: **7 de julho de 2014**

Negação de serviço do NTP
- XFID da divulgação relatada em: **25 de agosto de 2014**
- Cobertura da IBM Security Network Protection fornecida em: **13 de outubro de 2014**

Divulgações de vulnerabilidades de 2014

2014 foi um ano recorde para a X-Force. Nós catalogamos mais de 9.200 novas vulnerabilidades de segurança que afetavam mais de 2.600 fornecedores exclusivos. Isso representa um aumento de 9,8% em relação a 2013 e é o maior total em um só ano nos 18 anos de história da X-Force. No estudo trimestral IBM X-Force Threat Intelligence - 3º trimestre de 2014, relatamos uma possível diminuição no número de divulgações de vulnerabilidades, o que poderia resultar na queda do total de vulnerabilidades anuais para um valor inferior a 8.000 pela primeira vez desde 2011. No entanto, a previsão mudou drasticamente em setembro – quando um pesquisador do CERT Coordination Center fez uma divulgação referencial sobre vulnerabilidades de Android.[35]

Conforme descrito na nota de vulnerabilidade do CERT Coordination Center, VU nº 582497, o pesquisador identificou uma classe de vulnerabilidades que afetavam milhares de aplicativos Android em relação à validação incorreta de certificados SSL. Essas vulnerabilidades podiam permitir que um invasor realizasse ataques "man-in-the-middle" (MitM) contra os aplicativos móveis afetados. Dependendo do tipo de aplicativo direcionado, o invasor poderia executar um código ou obter informações confidenciais (pessoais, financeiras ou outras informações) que poderiam ser usadas para alavancar outros ataques.

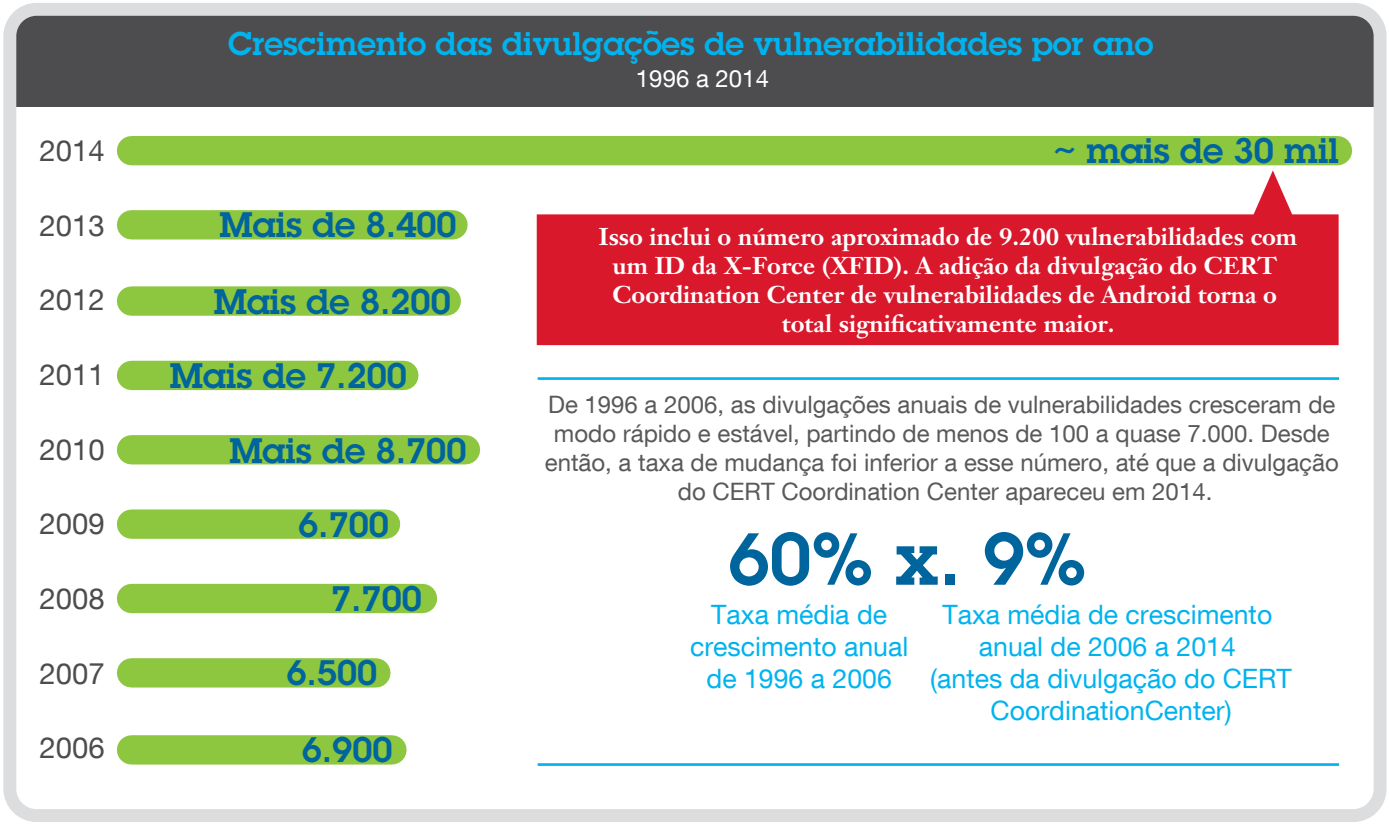


Figura 5. Crescimento das divulgações de vulnerabilidade por ano, 1996 a 2014

A X-Force continua analisando essa divulgação e os aplicativos vulneráveis, e esperamos criar XFIDs para eles à medida que a pesquisa progredir. Assim que essa análise for concluída, o total de vulnerabilidades de 2014 pode aumentar para mais de 30.000 vulnerabilidades relatadas para o ano. A questão é se esse total acabará sendo um aumento apenas de um ano ou se ele vai se tornar o novo normal à medida que mais vulnerabilidades forem descobertas e divulgadas por meio do uso de ferramentas automatizadas, como no caso da divulgação do CERT Coordination Center.

Na figura 6, comparamos a quantidade de divulgações de aplicativos Android associadas à VU nº 582497 com as outras divulgações anunciadas pelos fornecedores, incluindo os 10 principais fornecedores de software de nível corporativo. A divulgação do CERT Coordination Center representa quase 15% do total do ano, o que amplia a contagem final para um novo pico histórico. Somente para fins informativos, essas porcentagens incluem apenas os aproximadamente 1.400 problemas SSL de Android que têm IDs de CVE, e não contêm os mais de 20.000 possíveis problemas que ainda estão sendo rastreados na nota de vulnerabilidade do CERT Coordination Center que foi discutida anteriormente.

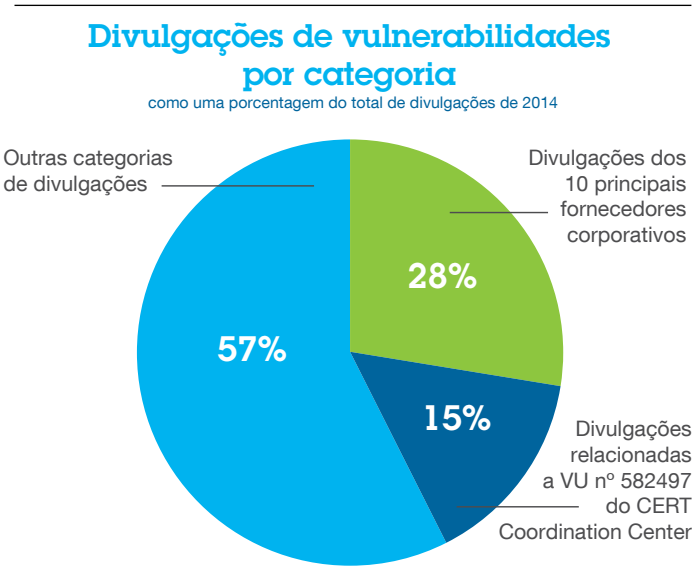


Figura 6. Divulgações de vulnerabilidades por categoria, como uma porcentagem do total de divulgações de 2014

O impacto de uma ferramenta de teste automatizada

O artigo de Will Dormann, intitulado "Announcing CERT/CC Tapioca for MITM Analysis" (Anunciando a ferramenta Tapioca do CERT Coordination Center para análise de MITM)[36] , descreve os métodos usados por um pesquisador do CERT Coordination Center para testar a segurança dos aplicativos Android. Durante o processo, ele criou uma ferramenta para ajudar a automatizar esses testes. O CERT Coordination Center disponibiliza a ferramenta Tapioca gratuitamente em seu website como um dispositivo de máquina virtual pré-configurado para realizar testes e análises de MitM. As ferramentas contidas no pacote Tapioca permitem que os desenvolvedores e pesquisadores inspecionem os aplicativos Android em busca de vulnerabilidades a ataques MitM e analisem os resultados sem contribuições dos operadores.

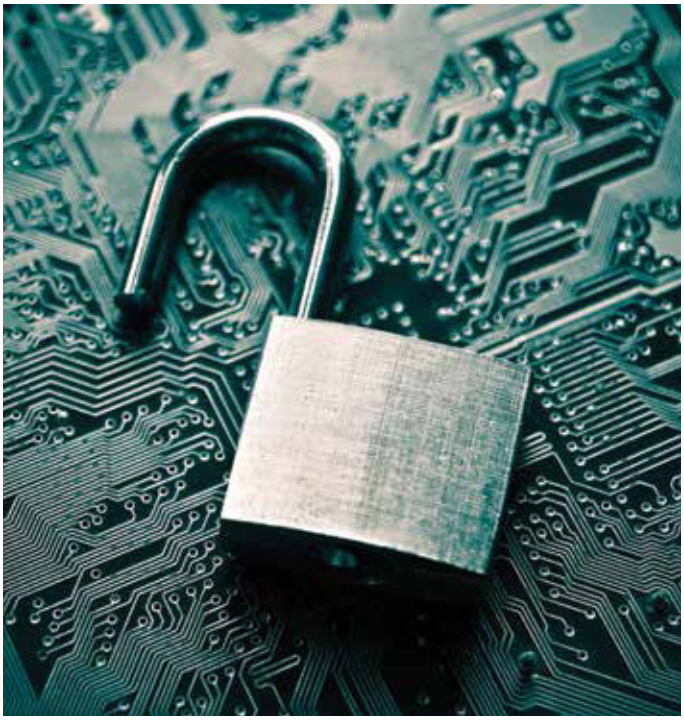
A pesquisa do CERT Coordination Center começou com a varredura sistemática e o teste dinâmico dos aplicativos da Google Play Store, a fim de determinar quais aplicativos falharam em validar devidamente os certificados SSL. Essa iniciativa (até o momento) produziu, literalmente, milhares de divulgações de aplicativos individuais que são vulneráveis a ataques MitM. Em outras palavras, esses relatórios apresentam a mesma vulnerabilidade fundamental que afeta uma grande variedade de aplicativos individuais. Eles não apresentam milhares de métodos exclusivos de atacar os diferentes aplicativos, mas sim uma só maneira de atacar milhares de aplicativos. Os muitos desenvolvedores precisam atualizar seus aplicativos, mas todos precisam fazer as mesmas mudanças lógicas, em vez de ter que descobrir individualmente como fazer tudo do zero. Além disso, o modo de rastreamento desses tipos de problemas será uma questão de debate pelo conselho editorial de CVE e, provavelmente, as discussões continuarão acontecendo à medida que as novas escolhas forem determinadas.

Conclusão

Basicamente, o CERT Coordination Center criou uma ferramenta que pode ajudar o setor a começar a sistematizar e automatizar os testes de segurança que são feitos manualmente há muito tempo, quando são feitos. Até o momento, os testes concentraram-se em problemas de SSL/ TLS que podem tornar uma conexão supostamente segura em uma conexão sem segurança. A ferramenta oferece recursos adicionais. Porém, uma questão continua sem resposta: os outros reagirão ao desafio e seguirão o caminho do CERT Coordination Center?

Se eles o fizerem, provavelmente, verão um enorme aumento no volume de vulnerabilidades divulgadas à medida que esses esforços produzirem resultados. Alguns relatórios estarão relacionados a problemas com aplicativos específicos; já outros refletirão práticas disseminadas de desenvolvimento insuficiente (como a não validação de cadeias de certificados SSL). Outros relatórios, por sua vez, identificarão erros nas estruturas e nos serviços de sistemas usados por muitos aplicativos. No entanto, com os milhares de aplicativos disponíveis nas diversas "lojas", o problema de cada sistema ou estrutura pode resultar em milhares de divulgações individuais conforme as práticas atuais.

Como usuários e como um setor, podemos esperar que os outros reajam ao desafio. Podemos esperar que a publicidade resultante dessas divulgações faça com que, no mínimo, os fornecedores mais respeitados e com melhor financiamento implementem testes mais completos de seus aplicativos antes da liberação. Isso pode acabar sendo a melhor coisa para o setor, caso resulte em uma segurança geral significativamente melhor por meio da identificação de problemas, da propaganda das correções necessárias e da aplicação de pressão sobre os desenvolvedores de aplicativos, para que eles fiquem mais atentos.



Sobre a X-Force

As ameaças avançadas estão em todos os lugares. Ajude a minimizar seus riscos com insights dos especialistas da IBM.

A equipe de pesquisa e desenvolvimento da IBM X-Force estuda e monitora as tendências mais recentes de ameaças, incluindo vulnerabilidades, explorações, ataques ativos, vírus e outros conteúdos de malware, spam, phishing e conteúdo da web malicioso. Além de aconselhar os clientes e o público em geral sobre as ameaças críticas e emergentes, a IBM X-Force também oferece conteúdo de segurança a fim de ajudar a proteger os clientes IBM dessas ameaças.

Colaboração da Segurança IBM

A Segurança IBM representa várias marcas que oferecem um grande espectro de competências de segurança:

- A equipe de pesquisa e desenvolvimento da IBM X-Force descobre, analisa, monitora e registra uma ampla variedade de ameaças de segurança a computadores, vulnerabilidades, e as tendências e os métodos mais recentes utilizados por invasores. Outros grupos da IBM utilizam esses dados variados para desenvolver técnicas de proteção aos nossos clientes.
- A família de produtos IBM Security Trusteer oferece uma plataforma holística de prevenção contra crimes cibernéticos em terminais, 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 esses produtos da Segurança IBM para proteger seus aplicativos da web, computadores e dispositivos móveis das ameaças online (como ataques avançados de malware e phishing).
- A equipe de segurança de conteúdo da IBM X-Force investiga e categoriza a web por meio de crawling, descobertas independentes e pelos feeds fornecidos pelo IBM Managed Security Services.
- O IBM Managed Security Services é responsável pelo monitoramento de explorações relacionadas aos terminais, aos servidores (incluindo servidores da web) e à infraestrutura geral da rede. Essa equipe rastreia as explorações realizadas pela web, além de outros vetores, como email e mensagens instantâneas.
- O IBM Professional Security Services oferece serviços corporativos de avaliação, design e implementação de segurança para ajudar a desenvolver soluções efetivas de segurança da informação.
- IBM QRadar® Security Intelligence Platform oferece uma solução integrada de inteligência de segurança e gerenciamento de eventos (SIEM), gerenciamento de registros, gerenciamento de configuração, avaliação de vulnerabilidades e detecção de anomalias. Ela oferece um painel unificado e insights em tempo real sobre os riscos de segurança e conformidade para as pessoas, os dados, os aplicativos e a infraestrutura.
- O IBM Security QRadar Incident Forensics foi projetado para oferecer às equipes de segurança corporativa visibilidade sobre as atividades da rede e clareza sobre as ações dos usuários. Ele pode indexar metadados e conteúdo de carga útil em arquivos de captura de pacotes (PCAP) para reconstruir sessões completamente, criar impressões digitais, destacar conteúdo suspeito e promover explorações de dados orientadas por busca auxiliadas por visualizações. O QRadar Incident Forensics integra-se facilmente à QRadar Security Intelligence Platform, e pode ser acessado usando a interface de gerenciamento com um só console do QRadar.
- O IBM Security AppScan® permite que as organizações avaliem a segurança dos aplicativos móveis e da web, reforcem o gerenciamento de programas de segurança dos aplicativos e garantam a conformidade regulamentar identificando vulnerabilidades e gerando relatórios com recomendações inteligentes sobre correções para facilitar a remediação de problemas. O serviço IBM Hosted Application Security Management é uma solução baseada na nuvem para testes dinâmicos de aplicativos da web que usam o AppScan nos ambientes de produção e pré-produção.

Colaboradores

A produção do estudo trimestral IBM X-Force Threat Intelligence é uma colaboração dedicada de toda a IBM. Gostaríamos de agradecer às pessoas a seguir por sua atenção e contribuição na publicação deste relatório.

Colaborador	Cargo
Brad Sherrill	Engineering Manager, IBM X-Force Exchange e IBM X-Force Database
Chris Poulin	Research Strategist, IBM X-Force
David Kaplan	Application Security Research Strategist, IBM X-Force Advanced Research
Doug Franklin	Research Technologist, IBM X-Force Advanced Research
Etay Maor	Senior Fraud Prevention Strategist, IBM Security
Jason Kravitz	Techline Specialist, IBM Security
Leslie Horacek	Manager, IBM X-Force Threat Response
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force e Threat Portfolio
Roee Hay	Application Security Group Lead, IBM X-Force Advanced Research
Scott Moore	Software Developer, IBM X-Force

Para obter mais informações

Para saber mais sobre a X-Force, acesse:
ibm.com/security/xforce/

[1] "Russia gang hacks 1.2 billion usernames and passwords," *BBC News Technology*, 6 de agosto de 2014. http://www.bbc.com/news/technology-28654613

[2] Natalie Kerris e Trudy Muller, "Apple Media Advisory: Update to Celebrity Photo Investigation," *Apple Press Info*, acessado em 16 de fevereiro de 2015. http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html

[3] "Third-Party Applications and the Snapchat API," *Snapchat*, 14 de outubro de 2014. http://blog.snapchat.com/post/99998266095/third-party-applications-and-the-snapchat-api/

[4] Dana Tamir, "Who Hacked Sony? New Report Raises More Questions About Scandalous Breach," *IBM Security Intelligence Blog*, 5 de fevereiro de 2015. http://securityintelligence.com/who-hacked-sony-new-report-raises-more-questions-about-scandalous-breach

[5] Chris Poulin, "What to Do to Protect against Heartbleed OpenSSL Vulnerability," *IBM Security Intelligence Blog*, 10 de abril de 2014. http://securityintelligence.com/heartbleed-openssl-vulnerability-what-to-do-protect

[6] Paul Ducklin, "Anatomy of a 'goto fail' - Apple's SSL bug explained, plus an unofficial patch for OS X," *Naked Security*, 24 de fevereiro de 2014. https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/

[7] Michelle Alvarez, "Revelations in data protection in the aftermath of shellshock," *Security Intelligence*, 28 de outubro de 2014. http://securityintelligence.com/revelations-in-data-protection-in-the-aftermath-of-shellshock/#.VNjLpGNTcog

[8] Rose Troup Buchanan, "Dropbox passwords leak: Hundreds of accounts hacked after third-party security breach," *The Independent*, 14 de outubro de 2014. http://www.independent.co.uk/life-style/gadgets-and-tech/nearly-seven-million-dropbox-passwords-hacked-pictures-and-videos-leaked-in-latest- thirdparty-security-breach-9792690.html

[9] Lisa Vaas, "Carwash POS systems hacked, credit card data drained," *Naked Security*, 25 de junho de 2014. https://nakedsecurity.sophos.com/2014/06/25/carwash-pos-systems-hacked-credit-card-data-drained

[10] Chris Poulin, "What Retailers Need to Learn from the Target Breach to Protect against Similar Attacks," *IBM Security Intelligence Blog*, 31 de janeiro de 2014. http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers

[11] "Exchange hacked - stolen passwords and documents," *Niebezpiecznik*, 23 de outubro de 2014. http://niebezpiecznik.pl/post/gielda-papierow-wartosciowych-zhackowana/

[12] Mark Stockley, "Millions of Drupal websites at risk from failure to patch," *Naked Security*, 30 de outubro de 2014. https://nakedsecurity.sophos.com/2014/10/30/millions-of-drupal-websites-at-risk-from-failure-to-patch/

[13] Claire Reilly, "Aussie Travel Cover hack exposes details of 770,000 customers," *CNET*, 20 de janeiro de 2015. http://www.cnet.com/au/news/aussie-travel-cover-hack-exposes-customer-details/

[14] Kate Knibbs, "Report: Mysterious Russian Malware Is Infecting 100,000+ Wordpress Sites," *Gizmodo*, 15 de dezembro de 2014. http://gizmodo.com/mysterious-russian-malware-is-infecting-over-100-000-wo-1671419522

[15] Stephanie Mlot, "DDoS Attack Puts Code Spaces Out of Business," *PCMag*, 19 de junho de 2014. http://www.pcmag.com/article2/0,2817,2459765,00.asp

[16] Adrian Weckler, "Eircom forced to shut email services after hacking breach," *Independent.ie*, 5 de janeiro de 2015. http://www.independent.ie/business/technology/eircom-forced-to-shut-email-services-after-hacking-breach-30234537.html

[17] Ionut Ilascu, "City of Phoenix Computers Under DDoS Attack," *Softpedia*, 28 de outubro de 2014. http://news.softpedia.com/news/City-of-Phoenix-Computers-Under-DDoS-Attack-463286.shtml

[18] Lily Hay Newman, "Evernote and Feedly Are Recovering After Sustained Hacker Attacks," *Future Tense*, 11 de junho de 2014. http://www.slate.com/blogs/future_tense/2014/06/11/evernote_and_feedly_were_down_because_of_a_ddos_attack.html

[19] Ms. Smith, "Ransomware: City of Detroit didn't pay, TN sheriff's office did pay to decrypt," *Network World*, 19 de novembro de 2014. http://www.networkworld.com/article/2850052/microsoft-subnet/ransomware-city-of-detroit-didnt-pay-tn-sheriffs-office-did-pay-to-decrypt.html

[20] Rick M. Robinson, "Wiper Malware Poses Destructive Threat," *Security Intelligence*, 21 de janeiro de 2015. http://securityintelligence.com/wiper-malware-poses-destructive-threat/#.VNDlQmPVuhM

[21] Pamela Cobb, "German Steel Mill Meltdown: Rising Stakes in the Internet of Things," *IBM Security Intelligence Blog*, 14 de janeiro de 2015. http://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things

[22] Benjamin Elgin e Michael A. Riley, "Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony," *Bloomberg Business*, 11 de dezembro de 2014. http://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony

[23] Eset Research, "Sednit espionage group now using custom exploit kit," *welivesecurity*, 8 de outubro de 2014. http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/

[24] Jaime Blasco, "Scanbox: A Reconnaissance Framework Used with Watering Hole Attacks," *AlienVault*, 28 de agosto de 2014. https://www.alienvault.com/open-threat-exchange/blog/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

[25] Dana Tamir, "Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical Organizations," *IBM Security Intelligence Blog*, 15 de setembro de 2014. http://securityintelligence.com/massively-distributed-citadel-malware-targets-middle-eastern-petrochemical-organizations

[26] Brian Krebs, "ZeuS Source Code for Sale. Got $100,000?" *Krebs on Security*, fevereiro de 2011. http://krebsonsecurity.com/2011/02/zeus-source-code-for-sale-got-100000/

[27] Brian Krebs, "'Citadel' Trojan Touts Trouble-Ticket System," *Krebs on Security*, 23 de janeiro de 2012. http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/

[28] Etay Maor, "Going Global: New Citadel Trojan Automatically Localizes Fraud Content," *IBM Security Intelligence Blog*, 30 de junho de 2014. http://securityintelligence.com/new-citadel-trojan-automatically- localizes-fraud-content-global

[29] Dana Tamir, "Cybercriminals Use Citadel to Compromise Password Management and Authentication Solutions," *IBM Security Intelligence Blog*, 19 de novembro de 2014. http://securityintelligence.com/cyber-criminals-use-citadel-compromise-password-management-authentication-solutions

[30] "PhoneGap / Apache Cordova," *AppBrain: Stats*, acessado em 16 de fevereiro de 2015. http://www.appbrain.com/stats/libraries/details/phonegap/phonegap- apache-cordova

[31] Marcel Kinard, "Apache Cordova Android 3.5.1," *Cordova*, 4 de agosto de 2014. http://cordova.apache.org/announcements/2014/08/04/android-351.html

[32] Roee Hay, "Apache Cordova Vulnerability Discovered: 10% of Android Banking Apps Potentially Vulnerable," *IBM Security Intelligence Blog*, 5 de agosto de 2014. http://securityintelligence.com/apache-cordova-phonegap-vulnerability-android-banking-apps

[33] "Cordova vulnerability," *Google Groups*, outubro de 2014. https://groups.google.com/forum/#!topic/android-security-discuss/FC3bMzY83dc

[34] "CVE Content Decisions Overview," *CVE*, 27 de outubro de 2011. https://cve.mitre.org/cve/editorial_policies/cd_overview.html

[35] Will Dormann, "Vulnerability Note VU#582497: Multiple Android applications fail to properly validate SSL certificates," *CERT*, 8 de dezembro de 2014. https://www.kb.cert.org/vuls/id/582497

[36] Will Dormann, "Announcing CERT Tapioca for MITM Analysis," *CERT*, 21 de agosto de 2014. http://www.cert.org/blogs/certcc/post.cfm?EntryID=203

Recicle

Segurança IBM
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América, março de 2015

WGL03073-USEN-00