Relatório Semestral de Tendências e Riscos IBM X-Force 2013

Setembro de 2013

Colaboradores

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

Contribuidor	Cargo
Brad Sherrill	Manager, X-Force Data Intelligence
Carsten Hagemann	X-Force Software Engineer, Content Security
Chris Meenan	Product Manager QRadar Vulnerability Manager
Chris Poulin	Security Strategist - Critical Infrastructure
Cynthia Schneider	Technical Editor, IBM Security Systems
Dr. Jens Thamm	Database Management Content Security
Jason Kravitz	Techline Specialist for IBM Security Systems
Leslie Horacek	X-Force Threat Response Manager
Marc Noske	Database Administration, Content Security
Mark E. Wallis	Senior Information Developer, IBM Security Systems
Mark Yason	X-Force Advanced Research[ADMINIB-F2]
Michael Hamelin	X-Force Security Architect
Paul Sabanal	X-Force Advanced Research[ADMINIB-F2]
Perry Swenson	X-Force Marketing Manager
Ralf Iffert	Manager X-Force Content Security
Robert Freeman	Manager, X-Force Advanced Research
Scott Moore	X-Force Software Developer and X-Force Data Intelligence Team Lead
Yong-Chuan Koh	X-Force Advanced Research[ADMINIB-F2]

Sobre este relatório
Este relatório X-Force fornece percepções sobre alguns dos desafios mais significativos com que se deparam profissionais de segurança atualmente. Leia este relatório para uma análise profunda das últimas ameaças à segurança e tendências.

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

Colaboradores do Relatório IBM X-Force

Os colaboradores do relatório X-Force de tendências e risco representam um amplo espectro de competências de segurança, incluindo:

- A equipe de pesquisa e desenvolvimento IBM X-Force descobre, analisa, monitora e registra uma ampla gama de ameaças de segurança, vulnerabilidades e as últimas tendências e métodos utilizados por invasores. Outros grupos dentro da IBM utilizam esses dados valiosos para desenvolver técnicas de proteção para nossos clientes.
- A equipe IBM X-Force de segurança de conteúdo independentemente percorre e categoriza a web por meio de crawling, descobertas independentes e pelos feeds fornecidos pelo IBM Managed Security Services (MSS).
- O time IBM de desenvolvimento de software de segurança oferece um dos mais avançados e integrados portfólios de produtos corporativos de segurança. O portfólio oferece inteligência de segurança para ajudar as organizações a protegerem holisticamente seu pessoal, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de acesso e identidade, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de riscos, gerenciamento de terminal, segurança de rede, entre outros.

Conteúdos

Conteúdos

Visão geral executiva

Ao passo que olhamos para trás no primeiro semestre de 2013, fica claro que táticas bem sucedidas implementadas por invasores continuam a desafiar as corporações a manterem-se em dia com o básico em segurança.

A mídia social tornou-se um alvo principal para invasores e dispositivos móveis estão expandindo esse objetivo. Testemunhamos esforços contínuos para alcançar a segurança em empresas experientes e vimos como as técnicas relativamente novas se aproveitam de usuários confiáveis por comprometer websites que eles frequentam. Ataques DDoS (distributed-denial-of-service) estão sendo utilizados como distração; permitindo que os invasores violem outros sistemas na empresa enquanto o pessoal de TI é forçado a tomar decisões difíceis baseadas em risco, possivelmente sem visibilidade do escopo completo do que ocorre.

O IBM X-Force continua a ver ataques operacionalmente sofisticados como o principal ponto de entrada. Alguns desses foram ataques de oportunidade, onde aplicativos de web sem patch e não testados foram vulneráveis à exploração SQLi (SQL injection) básica ou XSS (cross-site scripting). Outros foram bem sucedidos porque violaram a confiança básica entre o usuário e sites ou personalidades de mídia social que se pensava serem seguros e legítimos.

Muitas das violações reportadas no ano passado foram resultados de fundamentos de segurança e políticas aplicados de modo inadequado e que poderiam ter sido mitigados colocando alguma higiene básica de segurança em prática. Invasores parecem estar capitalizando nesta “falta de fundamentos de segurança" ao utilizar um modelo de sofisticação operacional que lhes permite aumentar seu retorno na exploração. A ideia de que mesmo a limpeza básica de segurança não é mantida nas organizações nos leva a crer que por uma variedade de razões, as empresas estão lutando com um compromisso de aplicar fundamentos básicos de segurança.

Ataques do tipo watering hole, que continuaram, são um grande exemplo de como a sofisticação operacional tem sido utilizada para alcançar alvos não suscetíveis anteriormente. Este tipo de campanha envolve uma forma de ataque dirigido nos quais o invasor identifica um website que é visitado por um grupo seleto. Ao comprometer o site central e utilizá-lo para servir malware, os invasores são capazes de alcançar vítimas tecnicamente mais experientes que podem não ser enganadas por tentativas de phishing, mas que não suspeitam que os sites em que confiam poderiam ser maliciosos. Diversas empresas de alta tecnologia bem como agências do governo têm sido violadas nos últimos meses.

Sofisticação operacional adicional foi vista no ataque a corporações globais principais ao violar franquias ou sites de idioma local em países fora da matriz corporativa. Frequentemente esses sites satélites não estão protegidos com o mesmo padrão que a matriz. Ao ir atrás de um ponto fraco de entrada em grandes empresas, os invasores foram capazes de alcançar e denegrir marcas bem conhecidas. Isto pode danificar a reputação de uma marca e criar problemas legais se dados sensíveis do cliente “vazarem”. Esses tipos de vazamentos afetaram a indústria de alimentos, de eletrônicos de consumo, automotivas e em particular as indústrias de entretenimento.

Os invasores demonstraram sofisticação técnica melhorada na área de ataques DDoS (distributed-denial-of-service). Os métodos DDoS exatamente não são avançados, mas o método para aumentar as quantidades de largura de banda capaz é um modo novo e poderoso de deter o negócio ao interromper o serviço online. O segmento bancário foi particularmente atingido no primeiro semestre de 2013. Invasores em junho de 2013 começaram a focar sua atenção em provedores de DNS (Domain Name System). Ataques nos provedores DNS são outro exemplo de comprometimento de alvos estratégicos centrais. Esses ataques podem ser problemáticos de várias maneiras e nós os exploramos na seção de violações deste relatório.

Outra tendência em crescimento é a aquisição de perfis de mídia social que possuem um grande número de seguidores. Essa tendência continua a exercer um papel essencial no modo como invasores estão alcançando seus objetivos. A mídia social introduz desafios sociológicos que abrem a porta para a exploração de segurança e nós vemos que os mesmos abusos de confiança que foram eficazes três anos atrás ainda são relevantes hoje, ao que cabe perguntar, aprendemos alguma coisa sobre confiança e mídia social?

A mídia social explora mais o afeto do que indivíduos; elas podem ter um impacto negativo na reputação da marca corporativa e causar perdas financeiras. Vemos algumas maneiras diferentes de como a influência social pode ser usada para apanhar pessoas despercebidas e mesmo causar danos no mundo desconectado.

Dispositivos móveis ainda são alvos lucrativos para autores de malware. Embora as vulnerabilidades móveis continuem a crescer a grande velocidade, ainda as vemos como uma pequena porcentagem das vulnerabilidades em geral reportadas no ano. Um desenvolvimento significativo para as vulnerabilidades móveis é que menos de 30% de todas as divulgações móveis possuem explorações públicas ou código de protótipo disponível. A maioria dessas explorações é dirigida especificamente para aplicativos móveis e são primariamente divulgadas em repositórios públicos populares de exploração.

Dispositivos Android estão experimentando um rápido crescimento, e com esse mercado crescendo, existe um interesse renovado por autores de malware em capitalizar sobre esse aumento de possíveis vítimas. 2013 testemunhou o lançamento de um trojan de nome Obad que demonstrou novos recursos tecnicamente sofisticados que o destacaram. O X-Force acredita que este lançamento é significativo no sentido de que mostra como os autores de malware estão investindo mais esforço na criação de malware Android que são mais resilientes e perigosos.

No primeiro semestre de 2013, vulnerabilidades de segurança reportadas ao público estão caminhando para o mesmo nível do que foi divulgado em 2012. Novamente, no primeiro semestre do ano, mais da

metade de todas as vulnerabilidades de aplicativos de web que foram reportadas publicamente foram vulnerabilidades XSS (cross-site scripting). A equipe de bancos de dados do X-Force reporta que fornecedores de CMS (Content Management System) continuam a aumentar suas taxas de correções. Contudo, os fornecedores terceirizados que criam plug-ins para plataformas CMS não apresentaram melhorias. Com mais de 46% de vulnerabilidades deixadas sem correção, plug-ins de terceiros atraem muitas oportunidades para a ocorrência de ataques e de fato foram pontos de entrada conhecidos para várias violações no ano passado.

Com respeito à exploração de vulnerabilidades, nós assistimos nos primeiros seis meses do ano como diversas vulnerabilidades de "dia-zero" afetando softwares amplamente implementados já haviam sido exploradas "in-the-wild" (já difundidas). A maioria das explorações de "dia-zero" foram inicialmente encontradas em ataques dirigidos, e nós testemunhamos como muitos invasores querem investir nesses ataques quando explorações sofisticadas de "dia-zero" contornaram mecanismos modernos de segurança em software. Microsoft Internet Explorer e Oracle Java foram atingidos de forma particularmente dura.

Mais adiante em nosso relatório fornecemos uma atualização nas tendências de web, spam e phishing, as quais permaneceram comparativamente grandes nos últimos seis meses. O país da Bielorússia tornou-se o país de maior distribuição de spam na primeira parte do ano, empurrando os EUA para fora da posição mais alta.

Finalmente, em um esforço de continuar com o foco renovado em práticas seguras, nós discutimos os desafios que tantas empresas encaram quando se trata de gerenciamento de vulnerabilidades. Apesar de o gerenciamento de vulnerabilidades ser por muito tempo uma exigência principal da prática de segurança de toda organização, a razão primária para essa luta é o grande volume e taxas de novas vulnerabilidades que estão sendo introduzidas nos ambientes. Nós discutimos algumas maneiras de auxiliar os administradores de sistemas a executarem um trabalho melhor para ajudá-los com a segurança da corporação.

Vamos revisar como a primeira parte deste ano surgiu.

Destaques do meio do ano de 2013

Ataques dirigidos e violações de dados

- Baseado nos incidentes que cobrimos, o SQLi (SQL injection) permanece como o paradigma de violação mais comum e no primeiro semestre de 2013 incidentes de segurança já ultrapassaram o número total reportado em 2011 e estão em vias de ultrapassar 2012 até o final do ano. (página 12)
- A categoria de ataque "Watering Hole" foi utilizada por invasores para violar com sucesso diversas empresas de alta tecnologia e grupos governamentais por injetar exploradores de navegação em websites visitados frequentemente por funcionários direcionados. Essas explorações que podem levar à instalação de malware trojan são bem sucedidas porque elas quebram uma certa camada de confiança entre o alvo e o que eles acreditam ser um website legítimo e seguro. (página 15)
- A aquisição de contas notáveis de mídia social com um grande número de seguidores é outra tendência em crescimento neste ano. Se um usuário do Twitter com milhões de seguidores é capaz de enviar um link para um site infectado, isso aumenta grandemente as chances de que alguma porcentagem das pessoas irá clicar nele, despercebidas de que é malicioso. Além de infectar computadores de usuários finais, a quebra da confiança de perfis online pode também ser utilizada para causar danos offline. (página 16)
- Uma onda de violações de dados dirigida a filiais internacionais de grandes negócios, corporações e franquias tira proveito do fato de que websites satélites e de idioma local que representam sua marca nem sempre estão seguros pelos mesmos padrões da matriz. Esses tipos de incidente afetaram as indústrias de alimentos, automotiva, entretenimento e de eletrônicos de consumo e podem resultar em impacto na reputação bem como em implicações legais pela perda de dados sensíveis do consumidor. (página 17)
- Recapitulando alguns dos outros destaques de incidentes de segurança, ataques DDoS (distributed denial-of-service) em massa contra alvos proeminentes persistiram desde 2012 até o primeiro semestre de 2013. O segmento bancário foi atacado pesadamente, causando inatividade e interrupções de negócios para clientes de banco online. (página 17)
- Ataques de amplificação DNS (domain name system) estão transformando Provedores DNS legítimos em cúmplices contra a vontade à medida que ataques de banda larga alavancando resolvedores DNS abertos esgotam os recursos e afetam milhares de clientes. (página 18)

Sociais e móveis

Mídias sociais

- A mídia social explora mais o afeto do que indivíduos; elas podem ter um impacto negativo na reputação da marca de uma empresa e causar perdas financeiras. (página 19)
- Como os invasores aprenderam a monetizar as vulnerabilidades da mídia social, um mercado negro brotou para negociar contas comprometidas e fabricadas em sites de mídia social. (página 22)
- Os controles de tecnologias estão disponíveis, mas, em geral, ou não são ativados ou são burlados pela rede estendida de usuário. A única defesa efetiva é a educação e levantar suspeitas. (página 22)

Móveis – Malware de Android

- Com o crescimento do Android, mais atenção foi gerada por autores de malware esperando capitalizar em tal crescimento. Um exemplo é o malware Chuli, descoberto em março de 2013. Este malware foi considerado um ataque altamente dirigido e destinado somente a indivíduos específicos, mas a existência indica que usuários de Android estão cada vez mais se tornando alvos viáveis para esses tipos de ataques sofisticados com forte intenção relacionada a organizações específicas. (página 24)

- Obad, um trojan que foi espalhado na maior parte através de spam de SMS (short message service), ganhou atenção em junho de 2013 quando foi apelidado de "O mais sofisticado trojan de Android". Alguns recursos que fizeram com que se destacasse foram técnicas de antianálise, ofuscamento de código, administração de dispositivo e a habilidade de espalhar-se através de Bluetooth. Acreditamos que é significativo no sentido de que mostra como os autores de malware estão investindo mais esforço na criação de malware Android que são mais resilientes e perigosos. (página 25)
- Mesmo que novos aprimoramentos de segurança estejam sendo desenvolvidos para combater malware de Android, o X-Force ainda acredita que a fragmentação do SO (versões antigas que estão sendo utilizadas tanto quanto as mais novas) permanecerão como um problema. (página 27)

Vulnerabilidades e exploração

Estatísticas de vulnerabilidade

- No primeiro semestre de 2013, o X-Force reportou a adição de um pouco mais de 4100 novas vulnerabilidades de segurança reportadas publicamente no banco de dados. Se a tendência continuar, a contagem total anual projetada parece ser de aproximadamente o mesmo número de 8200 vulnerabilidades reportadas em 2012. (página 34)
- Novamente no primeiro semestre de 2013, mais da metade de todas as vulnerabilidades de aplicativos de web reportadas publicamente foram vulnerabilidades XSS (cross-site scripting). Contudo, a categoria de vulnerabilidades de aplicativos de web representou somente 31% do conjunto de vulnerabilidades. Este número caiu significativamente desde 2012 quando vimos níveis a 42%. (página 35)
- CMS (Content Management Systems) são alguns dos aplicativos de software mais populares utilizados na Internet. Ano após ano vemos fornecedores executando um trabalho melhor de manter seus produtos corrigidos, como vimos 78% de todas as vulnerabilidades de software CMS corrigidos no primeiro semestre de 2013 versus somente 71% corrigidos em 2012. (página 36)
- Criadores de plug-ins CMS terceirizados não foram tão bem em corrigir quanto os fornecedores principais com somente 54% de vulnerabilidades de plug-in corrigidas – deixando 46% daquelas vulnerabilidades sem correção e um alvo atraente para invasores. (página 36)
- **MÓVEIS:** Embora as vulnerabilidades que afetam aplicativos móveis e sistemas operacionais representem uma pequena porcentagem relativa das divulgações totais (projetada em mais de 4% em 2013), constatamos um crescimento significativo do número total de divulgações desde 2009, quando vulnerabilidades móveis representavam menos de 1% das divulgações totais. (página 37)
- **MÓVEIS:** Um desenvolvimento digno de nota relacionado a vulnerabilidades móveis em 2013 tinha a ver com o número de explorações públicas disponíveis. Em 2013, menos de 30% de todas as divulgações móveis possuem explorações públicas ou código de protótipo disponível. Em comparação, somente 9% das vulnerabilidades móveis divulgadas entre 2009 e 2012 possuíam explorações públicas. A maioria dessas explorações é dirigida especificamente para aplicativos móveis e são primariamente divulgadas em repositórios públicos populares de exploração. (página 37)
- O X-Force categoriza vulnerabilidades pela consequência da exploração. Essa consequência é basicamente o benefício que a exploração de vulnerabilidade fornece ao invasor. A consequência mais prevalecente da exploração de vulnerabilidade para o primeiro semestre de 2013 foi "obter acesso" com 28% de todas as vulnerabilidades reportadas. Cross-site scripting foi a segunda consequência mais prevalecente com 18% e tipicamente envolve ataques contra aplicativos de web. (página 38)

Exploração

- No primeiro semestre de 2013, o X-Force distribuiu 14 alertas e avisos sobre divulgações que mereciam detida atenção. Colocamos sete desses alertas e avisos, coincidentemente compostos inteiramente de IE (Internet Explorer) e Java, no quadrante superior direito da matriz – o que indica vulnerabilidades que possuem uma alta taxa de retorno para invasores que desenvolvem maneiras de explorá-los. Todas as sete vulnerabilidades podem ser usadas em exploração drive-by, alcançando tantas vítimas quanto possível. (página 41)
- Nos primeiros seis meses do ano, diversas vulnerabilidades de "dia-zero" afetando amplamente o software implementado, já haviam sido difundidas. A maioria das explorações de "dia-zero" foram inicialmente encontradas em ataques dirigidos, e nós testemunhamos como muitos invasores querem investir nesses ataques quando explorações sofisticadas de "dia-zero" contornaram mecanismos modernos de segurança em software. (página 28)
- Conforme destacado na seção de violações, ataques watering-hole utilizando explorações de "dia-zero" estão aumentando. Este tipo de campanha envolve uma forma de ataque dirigido no qual um invasor identifica os websites que um grupo-alvo geralmente visita ou provavelmente irá visitar e então compromete aqueles sites de modo que se tornem as plataformas de lançamento dos ataques. O IBM X-Force fornece algumas recomendações para administradores de website para auxiliá-los a reduzir o risco de comprometimento. (página 28)

Tendências da web, spam e phishing

- 23% de todos os links maliciosos hospedados na Internet estão localizados em sites pornográficos. Contudo, blogs que fornecem websites dinâmicos com a habilidade de adicionar conteúdo também permitem que malfeitores coloquem links maliciosos nos sites 16,5% das vezes. (página 45)
- O país com mais alta hospedagem de malware são os Estados Unidos, com mais de 42% de links maliciosos hospedados lá. Seguindo os EUA vemos a Alemanha hospedando aproximadamente 10% e então China, Rússia, Holanda, Reino Unido e França hospedando o restante de malware entre 5,9 e 3,4%. (página 46)
- Aproximadamente um terço de todos os servidores botnet C&C (command and control) estão hospedados dentro dos Estados Unidos. Em segundo lugar está a Rússia com aproximadamente 10%. (página 47)
- Dentro dos 100 maiores websites mais utilizados, implementações IPv6 continuam a aumentar e nos últimos seis meses eles já cresceram 10% se comparados aos números do final do ano de 2012. (página 48)

Spam e phishing

- A Bielorússia se tornou o país com maior distribuição de spam, ao enviar mais de 10% no segundo trimestre de 2013. No início deste ano, a primeira posição foi sustentada pelos Estados Unidos, que enviou 12% mas então caiu abaixo da Bielorússia com 8% no segundo trimestre. Completando os 5 países com maior origem de envio de spam estão a Espanha, Índia e Argentina. (página 49)
- As três maiores áreas que atraem os usuários para clicar em links ruins e anexos são: emails que se parecem como se estivessem chegando de empresas de pagamento pela Internet, redes sociais e scanners internos ou dispositivos de fax. Juntas essas três áreas de destaque respondem por mais de 55% de todos os incidentes de scam e phishing. (página 50)

Práticas de segurança

- Muitas equipes de segurança continuam a lutar com a administração da vulnerabilidade apesar de serem por muito tempo uma exigência principal das práticas de segurança de toda organização. A razão principal para esta luta é o grande número e taxas de novas vulnerabilidades sendo introduzidas em ambientes por software de sistema operacional e aplicativos de terceiros, e o processo relativamente manual e lento de mitigação e/ou correção dessas fraquezas. Redes típicas podem esperar ver em média algum ponto entre 10 e 30 vulnerabilidades por endereço IP em seu ambiente; algumas não terão nenhum e algumas terão centenas, com os números alterando diariamente. (página 52)

Para mais informações

Para saber mais sobre o software IBM X-Force, visite: http://www-03.ibm.com/security/xforce/

Ataques dirigidos e violações de dados

Incidentes em estado de segurança em 2013

Navegando através de mídia convencional, encontramos artigos sobre violação de dados e incidentes de segurança em base regular. Ao passo que a cobertura pela mídia expandiu grandemente em anos recentes, o número total de incidentes também está crescendo de forma mensurável. 2012 foi recorde quanto a incidentes de segurança e violações de dados, com um aumento de 40% no volume total em relação a 2011.[1] Na primeira metade de 2013, os incidentes de segurança já ultrapassaram o número total divulgado em 2011 e está a caminho de superar os de 2012.

Este ano iniciou com um número de ataques sofisticados de alto perfil em principais websites, mídias e empresas de tecnologia. No **IBM X-Force 2012 Trend and Risk Report**, discutimos a ideia da sofisticação operacional versus sofisticação técnica. Ao longo do primeiro semestre de 2013, observamos uma continuação dessa tendência em ambos os tipos de violação que ocorreram e as motivações por trás delas.

Sofisticação operacional versus sofisticação técnica

A atração da sofisticação operacional é que os invasores podem usar um caminho de menor resistência para ganhar um retorno máximo de explorações. Isto se traduz no uso de técnicas testadas e reais como o SQLi (SQL injection), XSS (cross site scripting) e spear phishing, bem como plataformas de exploração que alcançam um número maior de alvos de sistema cross-browser e cross-operating tais como o Adobe Flash e o plugin de navegador Java. O reconhecimento de alvos continua a se beneficiar grandemente de informações disponíveis ao público e localizadas dentro de perfis de mídia social ou outros documentos confidenciais que foram classificados involuntariamente em websites de presença pública e descobertos através de mecanismos comuns de busca. A Figura 1 mostra diversos exemplos de como invasores estão utilizando a sofisticação operacional para violar os alvos.

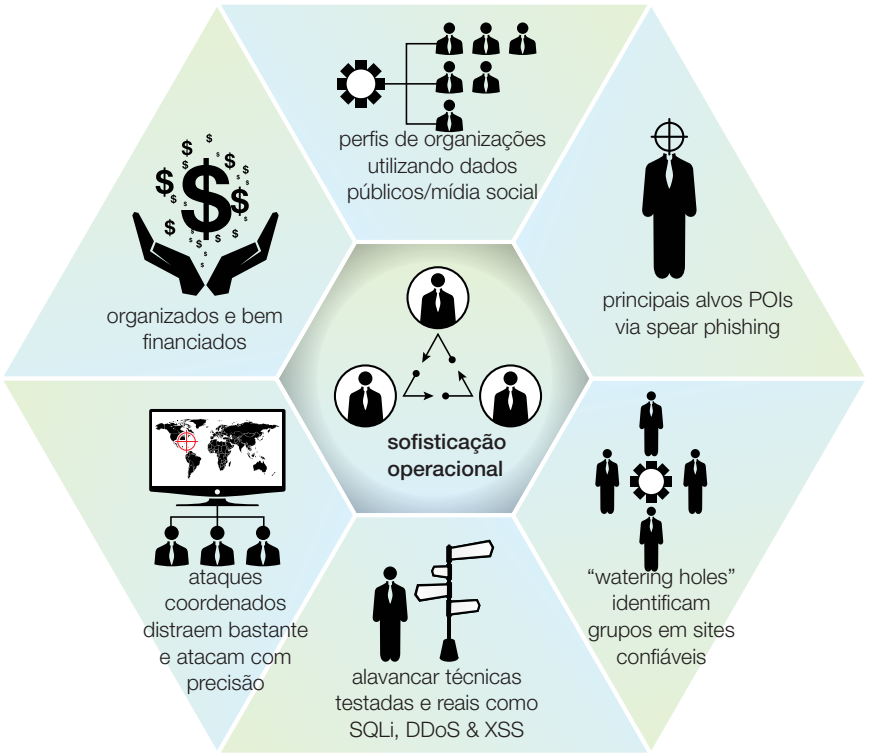


Figura 1: Métodos de sofisticação operacional de 2013.

1 http://datalossdb.org/statistics

Em contraste, a sofisticação técnica confia na utilização de ataques avançados tais como vulnerabilidades de "dia-zero" e em alguns casos, em técnicas de exploração personalizadas. Enquanto a sofisticação técnica existir, é atípica.

A Figura 2 ilustra uma amostra de violações de dados do primeiro semestre de 2013. Quando rastreamos violações divulgadas publicamente, nós determinamos o tipo de ataque por uma de duas maneiras principais. A primeira é através de uma nota da empresa, geralmente em uma carta oficial ou declaração aos clientes explicando a situação, e a segunda é através de um dump de dados, no qual o invasor divulga a vulnerabilidade utilizada para obter o acesso.

Um desenvolvimento positivo é que as empresas têm sido mais proativas em 2013[2] quanto a alertar seus clientes quando um incidente ocorreu. Em diversos casos, com grandes empresas online, todas as senhas de conta de clientes foram redefinidas automaticamente ou invalidadas. Essa honestidade em divulgar e a ação imediata é útil na mitigação do impacto das violações, em ambos os termos de danos técnicos e reputação da marca.

Com base nos incidentes que cobrimos, o SQLi (SQL Injection) permanece como o paradigma mais comum de violação. Não ficamos surpresos com isso, já que o SQLi é a maneira mais direta para obter acesso a registros nos bancos de dados. Em termos de retorno sobre a exploração, o SQLi é um ataque de oportunidade eficaz, em que scripts automáticos podem varrer uma ampla gama de alvos potenciais, que executam software de aplicativos comuns da web com as conhecidas vulnerabilidades SQLi. Diversos dos incidentes exibidos na Figura 2 foram resultado de fóruns de web não corrigidos ou vulneráveis ou outros produtos de terceiros amplamente utilizados.

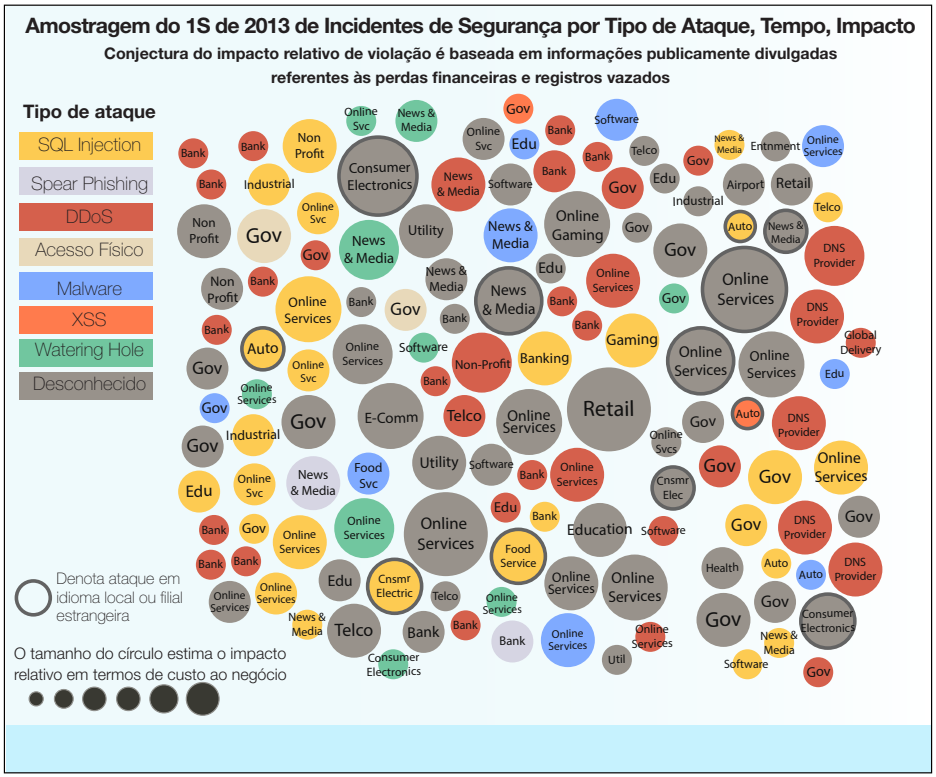


Figura 2: Amostragem do 1S de 2013 de Incidentes de Segurança por Tipo de Ataque, Tempo, Impacto.

2 http://www.wired.co.uk/news/archive/2013-03/04/evernote-hacked

Os incidentes que envolveram malware de tipo ataque foram às vezes o resultado de empresas descobrindo software malicioso em um ou mais servidores críticos. Estes por sua vez resultaram na divulgação[3] de uma possível violação, em alguns casos proativamente, mesmo se o impacto posterior não foi imediatamente discernível.

A distribuição de malware a usuários domésticos e corporativos ainda é altamente eficiente devido a vulnerabilidades em navegadores e plug-ins de navegação. Um desenvolvimento perturbador, reportado primeiramente em Abril, é a proliferação de um módulo fraudulento de servidor de web Apache apelidado Darkleech,[4] que até agora comprometeu mais de 40.000 sites, transformando-os em hospedeiros de malware capazes de infectar sistemas de usuários finais com kits de exploração tais como o Blackhole. Não há correlação definitiva entre todos os servidores de web infectados. Parece que em alguns, embora não em todos os casos, vulnerabilidades no Plesk cPanel foram utilizadas para obter a entrada.

O Darkleech, bem como outro backdoor similar (possivelmente o mesmo), chamado Linux/CdorkedA,[5] são uma nova classe de ameaça que utiliza a sofisticação técnica no modo como são implementados, e em como são capazes de operar furtivamente. Por exemplo, um recurso avançado é como o malware se comporta quando um usuário final visita um website infectado. Em vez de redirecionar cegamente o kit de exploração para cada visitante, como era o caso em cenários mais antigos conduzidos por download, o software utiliza o rastreio avançado de endereço IP para alvejar seletivamente os visitantes. Existe um recurso de whitelist e blacklist que fornece a habilidade de se esconder de pesquisadores de segurança e rastreadores, tornando a detecção mais difícil.

Enquanto o fornecimento de acesso remoto e snooping através de dados sensíveis são objetivos comuns, o malware também pode ser utilizado para objetivos mais destrutivos. Em março, no que parece ter sido um esforço coordenado para obter acesso contra diversas emissoras de televisão e bancos da Coreia do Sul[6], um programa malicioso chamado Jokra desabilitou sistemas de usuário final, causando dano permanente ao limpar o registro mestre de boot nos discos rígidos afetados.

Enquanto o malware remoto é prevalecente, o acesso físico ainda é um fator em diversas violações notadas. Isto poderia ser o resultado de membros do grupo furtando dados, ou a perda de ativos não criptografados como unidades de disco antigas, laptops ou dispositivos móveis. Esses tipos de incidentes nem sempre tem motivações maliciosas. Um erro ao imprimir informações de aposentadoria fez com que números de segurança social dos EUA[7] fossem visíveis na janela transparente do envelope, colocando dados sensíveis em risco. A perda de dados inadvertida por causa de falha humana não é incomum.

3 http://www.salemnews.com/local/x1533629707/SSU-data-breach-affects-25-000
4 http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/
5 http://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
6 http://www.infoworld.com/d/security/symantec-finds-linux-wiper-malware-used-in-s-korean-attacks-214965
7 http://blogs.newsobserver.com/business/26000-nc-retirees-warned-of-security-breach

Conforme ilustrado na Figura 3, nas violações rastreadas pelo IBM X-Force e nos termos do país onde o alvo do ataque estava localizado, os Estados Unidos é o país com as violações mais divulgadas e com uma margem considerável. Isto pode se basear no fato de que muitos websites são operados a partir dos Estados Unidos, ou possivelmente que seja mais comum que empresas e websites dos EUA estejam divulgando publicamente.

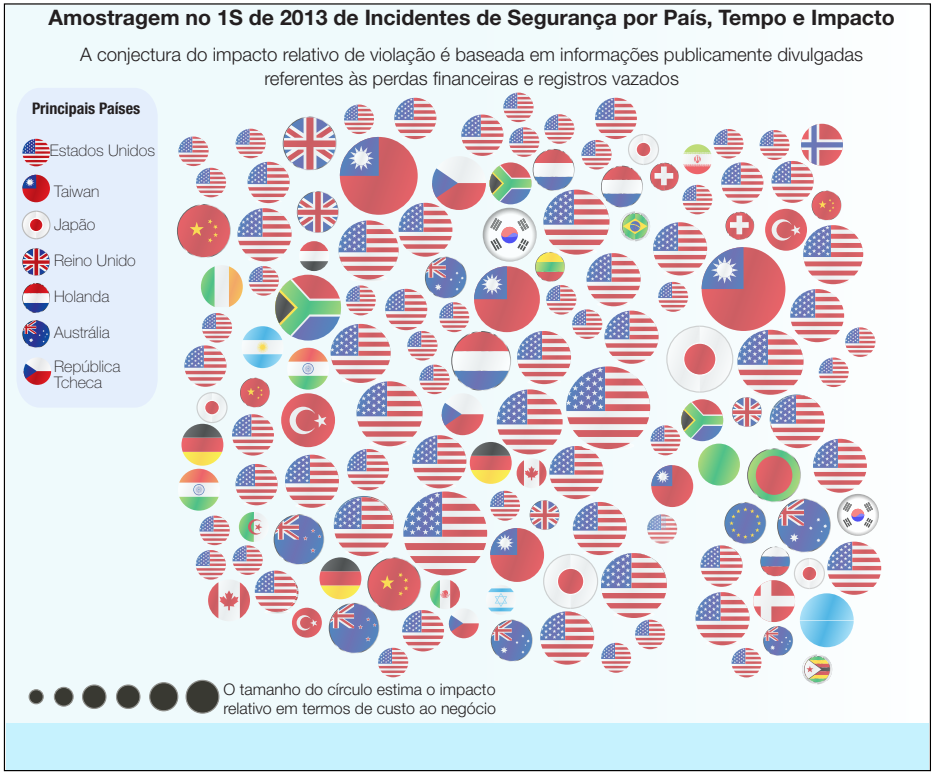


Figura 3: Amostragem no 1S de 2013 de Incidentes de Segurança por País, Tempo e Impacto.

Ataques watering hole continuam a crescer

Um tipo de ataque relativamente novo – que debutou recentemente em nossos gráficos – é o ataque "watering hole". Os invasores violaram, com êxito, várias empresas[8] de alta tecnologia, injetando explorações de navegador em websites visitados com frequência por funcionários visados. Essas explorações levaram à instalação de malware tipo trojan. Este mesmo tipo de ataque também foi utilizado neste ano para visar funcionários do governo.[9] Para uma explicação mais detalhada de ataques watering hole, veja o tópico intitulado "**Zero-Day Attacks in 2013 H1**."

Os ataques "watering hole" são bons exemplos de sofisticação operacional, pois atingem um grande número de alvos selecionados ao comprometer um único local centralizado. Em contrapartida, com o spear phishing, por exemplo, um invasor precisa se conectar individualmente a um grupo maior de pessoas e apenas uma pequena porcentagem poderá ser comprometida com êxito. Frequentemente esses ataques são bem sucedidos porque existe tráfego suficiente nas organizações visadas, e por natureza, elas rompem uma camada de confiança entre o alvo e o que o alvo acredita ser um website legítimo e seguro.

8 http://threatpost.com/why-watering-hole-attacks-work-032013/77647
9 http://news.softpedia.com/news/Cybercriminals-Behind-DOL-Watering-Hole-Attack-Target-USAID-Employees-353138.shtml

Esse padrão de comprometer alvos estratégicos centralizados, que por sua vez podem ser utilizados para alcançar uma base mais ampla de alvos, é repetido em uma variedade de vetores de diferentes ataques. O IBM X-Force destacou alguns desses tipos de ataques em relatórios anteriores. Por exemplo, atacar um fornecedor de segurança conhecido com o objetivo de integrar tokens de autenticação de dois fatores, comprometer certificados de assinatura de códigos de fornecedores de software e atacar fornecedores de certificados SSL com a intenção de interceptar tráfego criptografado.

Adicionalmente, tem havido uns poucos outros incidentes notáveis nos quais os invasores comprometeram alvos estratégicos centralizados. O conteúdo malicioso de malware foi injetado nas páginas de diversos websites de destaque com alto tráfego tais como o LA Times, National Journal, Toyota Japan e MSI Eletronics. Em junho, os criadores do navegador de web Opera[10] reportaram que foram alvejados em um ataque que resultou em comprometimento de pelo menos um de seus certificados de código. Isso significou que por um pequeno intervalo de tempo, pessoas que pensavam estar baixando uma versão legítima e assinada do navegador estavam na verdade baixando um malware.

Outra tendência em crescimento é a aquisição de contas notáveis de mídia social que possuem um grande número de seguidores. Se um usuário do Twitter com milhões de seguidores é capaz de enviar um link para um site infectado, isso aumenta grandemente as chances de que alguma porcentagem das pessoas irá clicar nele, despercebidas de que é malicioso. Além de infectar computadores de usuários finais, a quebra da confiança de perfis online pode também ser utilizada para causar danos offline. Em abril, quando uma conta comprometida da Associated Press[11] enviou informações falsas sobre explosões na Casa Branca, o mercado de ações sofreu impacto, resultando em uma queda temporária de 143 pontos. A habilidade de um único ataque influenciar as ações de milhões de pessoas em tempo real é alarmante. Discutiremos a psicologia de ataques à **Social Media** na próxima seção deste relatório.

10 http://www.scmagazine.com/maker-of-opera-browser-said-its-network-was-hacked-to-steal-code-signing-certificate/article/300580/
11 http://mashable.com/2013/04/23/ap-hacked-white-house/

Websites não franqueados – comprometidos distantes da origem

Ano passado o X-Force reportou violações de dados em filiais internacionais de grandes negócios e corporações, e em 2013 houve uma nova rodada de ataques dirigidos similares. As empresas frequentemente possuem websites de idiomas locais representando sua marca, mas esses sites nem sempre estão seguros com o mesmo padrão que os sites na matriz. Este foi o caso com várias marcas famosas que sofreram danos à reputação, assim como implicações legais pelo vazamento de grande quantidade de dados de clientes. Esses tipos de vazamento afetaram a indústria de alimentos, de eletrônicos de consumo, automotivas e em particular as de entretenimento. Diversos círculos no gráfico na Figura 2 possuem uma borda cinza escuro ao seu redor. São indicadores de empresas que experimentaram um incidente de segurança em uma filial estrangeira ou site de idioma local.

Em muitos casos, incluindo diversos dos vazamentos de dados de clientes na indústria alimentícia ano passado, o mesmo grupo reivindicou o crédito, indicando uma especialidade neste tipo de alvo.[12, 13, 14, 15, 16]

Muitas vezes, o ponto de entrada foi uma configuração de subsite para fins promocionais onde clientes se cadastraram para ganhar alguma coisa ao fornecer informações pessoais no processo. Esses tipos de páginas temporárias são um alvo lucrativo considerando que uma marca principal de alimentos ou entretenimento poderá alcançar muitos milhões de clientes em regiões locais. Quando esses subsites são rapidamente implementados sem controles apropriados de segurança, tais como formulários de web seguros e senhas criptografadas, o resultado do vazamento de dados pode ser danoso.

Em geral, como em anos anteriores, uma grande porcentagem de todas as violações rastreadas pelo X-Force ocorreram devido a um lapso nos fundamentos básicos de segurança. Em um relatório anterior, o X-Force discutiu como assegurar senhas criptografadas de modo apropriado antes de armazená-las em um banco de dados. Ao passo que muitas das violações em 2013 reportaram que suas senhas foram armazenadas com segurança, é desconcertante que diversos alvos ainda estavam armazenando senhas em texto aberto. Essas não eram empresas pouco sofisticadas, mas sim universidades, grupos governamentais incluindo departamentos de polícia, bancos, provedores de hospedagem de web, e mesmo empresas que se autoproclamavam baseadas em segurança e privacidade.

O resultado desse lapso na segurança fundamental de web é que quando um banco de dados foi vazado com um endereço de email e senha de texto abertos, qualquer um que estiver reutilizando senhas em múltiplos sites estará correndo riscos. Também é válido notar que quando grandes lotes de dados de senhas do mundo real são descobertos, eles são adicionados a listas de senhas que podem então ser utilizadas para decifrar à força contas de usuários em relação a alvos futuros.

DDoS (distributed denial of service) dirigidos ao segmento bancário continua

Recapitulando outros destaques de incidentes de segurança, ataques DDoS (distributed denial-of-service) em grande escala contra alvos proeminentes persistiram desde 2012 até o primeiro semestre deste ano. O segmento bancário foi expressivamente atacado, causando tempo de inatividade e interrupções de negócios para clientes de serviços bancários on-line. Spamhaus,[17] uma organização sem fins lucrativos, dedicada a rastrear o abuso de spam, foi atingida pelo que alguns consideram ser o maior ataque de DDoS no mundo, com taxas elevadas de tráfego divulgadas de até 300 Gbps. Estes ataques DDoS de banda larga expandiram-se no ano passado e continuam a representar um desafio em termos de redução de ataques bem-sucedidos. Incidentes DDoS também continuam a fornecer uma excelente técnica de distração onde a verdadeira motivação é violar sistemas sob a cobertura do ataque DDoS.

12 http://www.cyberwarnews.info/2013/07/13/sony-italy-hacked-over-40k-personal-details-leaked/
13 http://www.cyberwarnews.info/2013/06/20/samsung-kazakhstan-social-hub-domain-hacked-62235-accounts-leaked/
14 http://www.cyberwarnews.info/2013/08/22/fast-food-giant-pizza-hut-spain-and-malta-hacked-data-leaked-site-redirected/
15 http://www.cyberwarnews.info/2013/03/31/official-mtv-taiwan-hacked-607286-account-credentials-leaked/
16 http://www.cyberwarnews.info/2013/03/28/official-mcdonalds-austria-taiwan-korea-hacked-over-200k-credentials-leaked/
17 http://www.informationweek.com/security/attacks/spamhaus-ddos-suspect-arrested/240153788

Ataques de amplificação DNS (Domain Name System)

Uma tendência emergente interessante em alvos DDoS tem evoluído desde junho onde muitos provedores DNS reportaram interrupções no serviço e inatividade.[18] Visar o provedor DNS é outro exemplo de padrão de ataque a um alvo estratégico centralizado para alcançar um grupo maior de vítimas em potencial. Existem diversas maneiras como isto pode ser problemático. A primeira e mais óbvia é que se o provedor DNS estiver indisponível,[19] devido a um DDoS bem sucedido, qualquer site que confie naquele DNS para seu domínio também será impactado. A segunda é que se invasores podem violar o provedor DNS pelo DNS Hijacking,[20] então eles podem redirecionar endereços de web para servidores alternativos que podem então ser utilizados para phishing ou para distribuir malwares. Provedores DNS também foram visados simplesmente para utilizar o DNS como uma etapa para atacar outros alvos. Ao abusar de resolvedores DNS abertos, invasores são capazes de realizar ataques de amplificação DNS contra outros alvos. Esses tipos de ataques são eficazes porque o invasor é capaz de enviar uma quantidade menor de tráfego, o que resulta em um pacote maior de resposta sendo enviado para a origem fraudulenta ou para o alvo do ataque DDoS. Os provedores DNS tornaram-se cúmplices contra a vontade neste processo ao responder ao que se parece com solicitações legítimas até que sua largura de banda seja excedida.

Conforme o escopo e a frequência de violações de dados continuam em uma trajetória ascendente, é mais importante do que nunca voltar aos fundamentos básicos de segurança. Ao longo deste relatório vemos muitas facetas da computação segura a partir das perspectivas administrativas da TI e da rede, e para usuários finais. Ao passo que a mitigação técnica é uma necessidade, educar os usuários dentro da empresa que segurança é uma cultura, não uma exceção, também pode reduzir esses incidentes.

Um dos tópicos mais interessantes que discutiremos é como a mídia social se expandiu como uma plataforma para exploração, e como funcionários e empresas podem ser mais alertas contra ameaças em potencial.

18 http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html
19 http://www.theregister.co.uk/2013/07/18/netsol_ddos/
20 http://www.zdnet.com/linkedin-just-one-of-thousands-of-sites-hit-by-dns-issue-cisco-7000017124/

Sociais e móveis

Mídia social – visando usuários e abusando da confiança

A psicologia do comportamento arriscado da mídia social

A mídia social é uma construção sociológica relativamente nova, e ainda assim foi incorporada em uma velocidade fenomenal como uma extensão de nossa presença no mundo real; um sentido adicional utilizado para comunicar nossos pensamentos, atividades, locais e mesmo sentimentos.

O risco desta rápida integração, que também é alimentado pela expansão de dispositivos móveis em nossas vidas, é que nós não entendemos plenamente como interpretar as sutilezas da interação online da mesma forma como nossos cérebros se adaptaram para analisar comunicação não verbal, como por exemplo, a linguagem corporal, micro expressões,[21] e como respondemos a elementos culturais e paralinguísticos. Apesar dessas nuances críticas nas comunicações garantimos a confiança para personalidades online que nunca encontramos – e que podem estar mortas[22] ou ser completamente fictícias. Os usuários ignoram seu melhor julgamento em favor de construir uma grande rede, com o status que a acompanha e a promessa de obter acesso a oportunidades que são obviamente boas demais para serem verdades.

Os invasores entendem essas fraquezas e estão começando a aprender como explorá-las de maneira eficiente. Ataques sociais, que são mais humanos e pessoais, podem ser criados para se referirem a tópicos relevantes de interesse e eventos atuais. Os invasores estão se inspirando em organizações de marketing em corporações profissionais e alavancando métricas tais como ROI (return on investment) e SEO (search engine optimization) para obter mais cliques através de taxas com máximo alcance, e enfim otimizar seu ganho de capital.

Esperamos ver o nível na manipulação psicológica tornar-se mais sofisticado à medida que os invasores criam redes de bancos de dados de identidades e refinam a arte de enganar as vítimas.

Impacto econômico e reputacional

A adoção difundida da mídia social, em ambos os círculos pessoal e de negócios, a torna muito mais interativa na corporação e necessária para atrair novos talentos bem como promover o negócio. Em vez de tentar bloquear o acesso à mídia social, os negócios devem pensar sobre como monitorar e mitigar abusos nessas plataformas.

Em abril de 2013, 60 caracteres custaram ao mercado de ações dos EUA US$200.000.000.000,00. Sim, são duzentos bilhões de dólares. A partir de um único tweet!

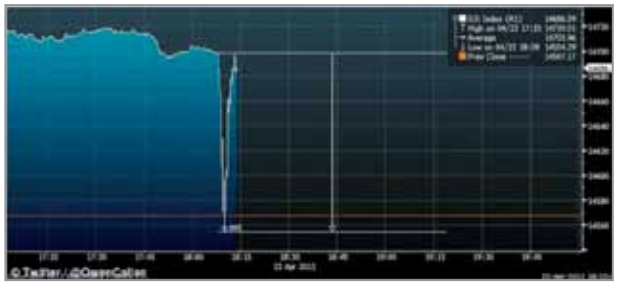
Isso torna falso o argumento de que redes sociais são meramente úteis aos adolescentes para transmitir fotos de si mesmos e para a sua tia compartilhar frases motivacionais sobre perda de peso.

21 http://www.paulekman.com/micro-expressions/
22 http://www.businessinsider.com/deceased-liking-stuff-on-facebook-2012-12

O "flash crash" foi instigado quando a conta principal de notícias da Associated Press[23] (AP) no Twitter foi hackeada e os perpetradores "tuítaram", "*Notícias de última hora: Duas explosões na Casa Branca e Barack Obama está ferido*." O incidente sublinha a confiança que o público em geral coloca na informação compartilhada em redes sociais.

A AP não foi a única grande organização que perdeu o controle de seu canal de mídia social. A conta de Twitter da Reuters[24] foi hackeada pelo SEA (Syrian Electronic Army) e utilizada para postar cartoons políticos em apoio ao presidente da Síria, Bashar al-Assad. O SEA também comprometeu a página de Facebook do New York Post[25] bem como as contas de Twitter de alguns de seus repórteres, seguido pelo site de notícias satíricas The Onion,[26] postando tweets denunciando Israel e os EUA.

Um dos hacktivistas originais, Anonymous, comprometeu a conta de Twitter do Burger King[27] e a usou para promover o concorrente, McDonald's. No dia seguinte, a conta de Twitter da Jeep foi hackeada e tweets foram enviados possuindo uma similaridade com aquelas do Burger King, reivindicando que a Jeep havia sido vendida para a Cadillac com uma foto de um carro de marca McDonald's como imagem de fundo.[28]



Crédito da imagem: http://www.dailymail.co.uk/news/article-2313652/AP-Twitter-hackers-break-news-White-House-explosions-injured-Obama.html

Estes comprometimentos possuem algumas coisas em comum:

- Foram motivados por hacktivismo, o impulso para fazer uma declaração política;
- Em vez de criar uma oportunidade financeira para os invasores, os incidentes causaram danos à reputação com potencial impacto econômico, embora temporários e insignificantes, para as organizações vítimas;
- Os ataques foram conduzidos contra humanos em vez de sites de mídia social, utilizando phishing para assumir as contas de usuários e de organizações.

A mídia social continua a servir como uma plataforma-chave de comunicação para a organização, fornecendo notícias, promoções, atualizações do negócio e outros tipos de anúncios e alertas. É mais importante do que nunca garantir a integridade e segurança dessas contas e perfis, e garantir que os usuários que confiam em contas associadas com a organização compreendam as robustas práticas de segurança. Qualquer organização é tão segura quanto o seu link mais fraco.

23 http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
24 http://www.theguardian.com/technology/2013/jul/30/reuters-twitter-hacked-syrian-electronic-army
25 http://www.thedailybeast.com/articles/2013/08/13/syrian-electronic-army-strikes-again-hits-socialflow-new-york- post.html
26 http://arstechnica.com/security/2013/05/no-joke-the-onion-tells-how-syrian-electronic-army-hacked-its-twitter/
27 http://www.telegraph.co.uk/technology/twitter/9878724/Burger-Kings-Twitter-account-hacked.html
28 http://www.huffingtonpost.com/2013/02/19/jeep-twitter-hack_n_2718653.html

Reunindo inteligência de pré-ataque

A mídia social é um terreno fértil para a reunião de inteligência de pré-ataque, conforme cobrimos no IBM X-Force Trend and Risk Reports anterior. O ataque em si tem sido tipicamente conduzido por meio de spear phishing via email e instigando o alvo a abrir um anexo infectado com malware.

Conforme discutido anteriormente na seção "*Ataques watering hole continuam a aumentar*", tudo o que o invasor precisa fazer é atrair uma vítima para um website – frequentemente um website legítimo que foi comprometido – para infectar o alvo intencionado. Um link simples dentro de um tweet ou uma postagem irá fazer isso, bem como a recente tentativa de exploração dirigida a um grupo de ativistas políticos chineses e seus afiliados.[29] É interessante notar que a mídia social pode ser utilizada tanto para reunir informações sobre os alvos, como por exemplo seus tópicos de interesse, novos sites que frequentam e idiomas, bem como para explorações mais diretas com mensagens diretas, por exemplo. Tais ataques podem se tornar mais eficientes ao incluir os comumente utilizados encurtadores de URL, que não dão qualquer indicação da URL de destino real e ainda fornecem outra forma de ofuscamento do link.

A mídia social fornece mais do que simples oportunidades de reconhecimento e exploração direta; pode ser utilizada para ativamente criar redes confiáveis. Por exemplo, a experiência Robin Sage[30] um consultor de segurança criou um personagem fictício, Robin Sage, que era propositadamente um analista de ameaças virtuais do Departamento de Defesa dos EUA. Robin possuía contas no LinkedIn, Twitter e Facebook, que eram utilizadas para criar uma rede de "alvos" profissionais. A maioria dos contatos trabalhava para organizações militares, governamentais ou afiliadas dos EUA. Apesar da falta de evidência sólida para corroborar a limpeza, credenciais ou mesmo a existência de Robin, os contatos compartilharam informações que revelaram seus endereços de email, contas bancárias e mesmo a localização de unidades militares secretas. Robin recebeu documentos para revisar e ofereceu vagas para palestras em conferências. Uma experiência parecida foi conduzida recentemente e apresentada na Defcon.[31]

29 https://www.cybersquared.com/apt_targetedattacks_within_socialmedia/
30 http://www.robinsageexperiment.com/
31 http://www.csoonline.com/article/737662/dating-guru-resurrects-robin-sage-by-social-engineering-ts-sci-holders-on-linkedin?source=rss_security_awareness

A ascensão do mercado negro de mídia social

O valor de ter acesso a contas de mídia social criou um mercado negro.[32] Criminosos estão vendendo contas, algumas das quais pertencem a pessoas reais cujas credenciais foram comprometidas, outras fabricadas e projetadas para ser críveis através de perfis realistas e uma malha de conexões.

Uma utilização é manipular o interesse ao redor de marcas ao falsificar "Likes"[33] o que é chamado de "likejacking", plantando avaliações controversas de produtos, ou ao ajudar um conteúdo a se tornar viral. Para obter o sentimento da escala do problema, considere que a página do próprio Facebook perdeu 125.000 "curtir" e Lady Gaga perdeu 65.000 fãs após o Facebook se comprometer em uma campanha para expulsar contas falsas.[34] As utilizações mais insidiosas do comércio de contas incluem ocultar a identidade de alguém para conduzir atividades criminosas, o equivalente online de um ID falso mas com amigos com recomendações, ou semear uma nova rede de conexões confiáveis, como na experiência Robin Sage.

E o tamanho conta. A reputação da identidade imaginária é reforçada pelo tamanho de sua rede social e a oportunidade para a exploração se expande na mesma proporção. Mais conexões são iguais a mais vítimas, vítimas para likejack, para infectar com malware e para extrair informações pessoais para maior exploração.

Levantar suspeitas para proteger usuários e ativos

Fomos ensinados na infância a sermos prestativos, e muitos usuários de mídia social carregam essa lição de ética em seu comportamento online. No mundo real existem controles sociais que impedem a conduta criminosa; a atividade online é frequentemente não monitorada ou existem tantos dados que as ameaças se escondem em meio ao ruído. Ultimamente, caixas de Pandora são entregues de muitas maneiras em mãos de usuários finais e eles tomam a decisão de espiar sob a tampa ou convocar a equipe da empresa de materiais virtuais perigosos.

Esquivar-se de tentativas de exploração da confiança que você, seus funcionários e sua família e amigos colocam em redes sociais exige uma combinação de modificação de comportamento e tecnologia. Não, não estamos defendendo a terapia de choque; e mesmo assim, as medidas evasivas podem ser excruciantes.

Discutimos os controles da tecnologia nos X-Force Trend and Risk Reports anteriores e aquelas recomendações ainda são relevantes. Adicionalmente, os usuários devem adotar uma mentalidade de culpado até que seja provado inocente quando se trata de mídia social.

- Somente aceite convites para se conectar com pessoas que você conhece. Se a solicitação surgir inesperadamente, confirme a intenção do solicitante através de outro canal, como por exemplo, email direto ou telefone.
- Não clique em links – quaisquer links, mesmo de amigos próximos – sem verificá-los ao passar o ponteiro do mouse sobre eles e examinar a barra de status. Em tablets, smartphones e qualquer dispositivo de toque, toque o link e mantenha-o pressionado para visualizar o destino. Para o paranoico verdadeiro, digite a URL manualmente em uma nova aba ou janela ou examine a origem da página.
- Se estiver preocupado com a aparência suspeita de URLs curtas, existem plug-ins de navegadores e serviços de web que podem reverter o link de modo que possa ver o destino atual da URL antes de clicar.
- Não poste nada confidencial; trate a mídia social como se estivesse gritando em um terminal de aeroporto onde todos podem ouvi-lo. Mesmo dados parciais não confidenciais podem ser combinados e completar uma história. O Departamento de Defesa dos EUA chama isto de OPSEC, ou segurança de operações.[35]

Lembre-se, mesmo se postar algo confidencial para seus melhores amigos, eles poderão repostar nas redes deles, e os controles de segurança e privacidade deles ainda podem ser por padrão, configurações frágeis.

32 http://blog.webroot.com/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/
33 http://www.ibtimes.co.uk/articles/499985/20130819/instagram-zeus-malware-virus-create-likes-followers.htm
34 http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-on-bogus-accounts-2013-2
35 http://en.wikipedia.org/wiki/Operations_security

Conclusão

Uma das lições de nossa incursão ainda em fase de protótipo na mídia social é que estamos interagindo com contas e não com pessoas. Contas podem ser comprometidas, elas podem ser fabricadas. A única analogia de universo cinético vem da ficção científica: Um humano comprometido é um ser gerado; um humano fabricado é um androide. Mesmo nos filmes, contudo, os mocinhos podem reconhecer o comportamento levemente estranho de parasitas alienígenas e ciborgues.

Ainda não atingimos a mesma capacidade de avaliar o virtuoso do vil, o sublime do suspeito, na mídia social. Assim como em toda interação entre humanos, o ponto essencial é a confiança. E pelo fato de que as redes sociais podem expandir exponencialmente mais amplamente e mais rápido do que a melhor rede política conectada na vida real, nós simplesmente não podemos rastrear quem é quem, menos ainda a quem deveríamos estender nossa confiança.

Como tal, o perigo da mídia social é algo de confiança transitiva: Nós tendemos a estender a confiança a amigos de amigos. Amigos falsos se infiltram em grupos sociais rapidamente uma vez que convençam o primeiro alvo a aceitar sua solicitação de conexão.

Como a expressão diz, “só porque sou paranoico, não quer dizer que não estão me observando”. Ao passo que raramente é bom incutir medo em nossas responsabilidades, uma dose saudável de ceticismo ligeiramente menor do que medo ou paranoia é apropriada à medida que os níveis para substanciar adequadamente a qualidade dos relacionamentos na mídia social.

Avanços recentes em malware de Android

Introdução

Nos últimos anos, houve um crescimento explosivo de dispositivos Android. De acordo com relatórios,[36] o Android atualmente possui 59% de todos os dispositivos móveis inteligentes. Foram embarcados 470 milhões de dispositivos Android somente em 2012 e se as previsões[37] são precisas, até 2017 haverá mais de 1 bilhão de dispositivos Android em uso. Infelizmente, o aumento em dispositivos Android também gerou mais atenção de autores de malware. De acordo com relatórios adicionais do mercado,[38] houve um aumento de mais de 600% no número de malwares de Android descobertos em comparação com o último ano, o que nos traz o total de malwares próximo de 276.000.

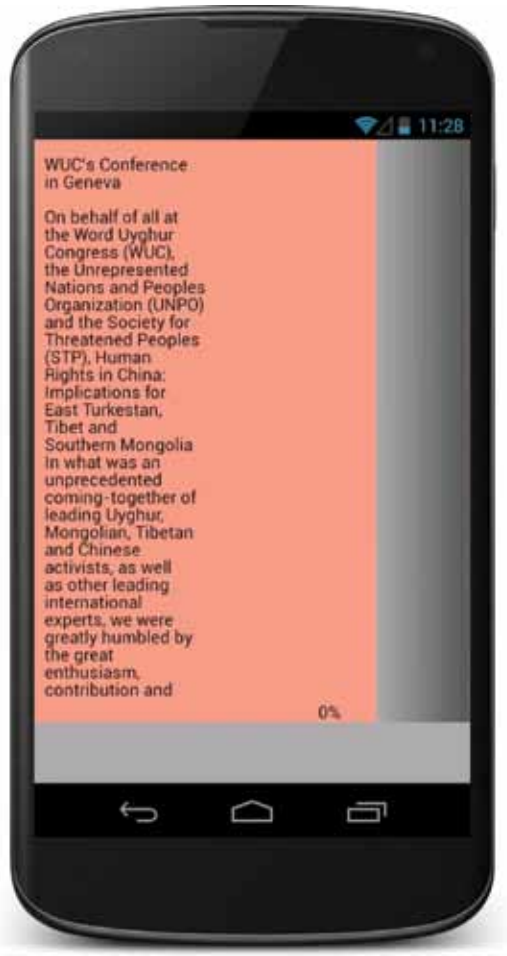
O primeiro semestre de 2013 também viu a descoberta de alguns malwares que indicam que o Android está progressivamente se tornando uma plataforma-alvo mais atraente para autores de malwares. Observemos dois desses.

Ataque dirigido

No "Mid-Year Trend and Risk Report" de 2012, discutimos ataques dirigidos e mencionamos que na plataforma Mac OS houve ataques contra ONGs tibetanas. Este ano, autores de malwares puseram seus olhos no Android bem como se voltaram para os mesmos tipos de vítimas.

O Chuli, descoberto em março de 2013, foi usado para alvejar contatos de um hacktivista tibetano que aparentemente foi hackeado e teve sua lista de endereços comprometida. Utilizando a conta hackeada, emails foram enviados para os contatos-alvo supostamente sendo sobre uma conferência dirigida pelo "World Uyghur Congress". O arquivo anexo é um arquivo APK de Android nomeado "WC's Conference.apk". Quando aberto, ele (Chuli) exibe uma mensagem sobre a conferência.

No plano de fundo, o Chuli configura vínculos ao serviço de SMS de Android, para que possa interceptar as mensagens recebidas de SMS e enviá-las a um servidor C&C (Command and Control). Também envia o histórico de SMS, histórico de chamadas, e



Exemplo de malware de Android – Chuli

36 http://www.canalys.com/newsroom/smart-mobile-device-shipments-exceed-300-million-q1-2013
37 http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017
38 http://thenextweb.com/insider/2013/06/26/juniper-mobile-malware-is-an-increasingly-profit-driven-business-as-92-of-all-known-threats-target-android/

geolocalização do usuário para o servidor C&C. O Chuli é um ataque altamente dirigido e destinado somente a indivíduos específicos, portanto o risco de infecção para o usuário comum é baixo. Contudo, a existência deste malware indica que usuários de Android estão cada vez mais se tornando alvos viáveis para esses tipos de ataques sofisticados. Realmente, neste caso, a sofisticação está relacionada à organização e intenção do ataque – a tecnologia bruta do Chuli não é particularmente original.

O malware de Android "mais sofisticado", Obad, um trojan que na maior parte foi espalhado através de spam SMS, ganhou atenção em Junho de 2013 quando foi apelidado de "o mais sofisticado trojan de Android"[39] Nós já vimos a funcionalidade principal do Obad em outro malware de Android antes, incluindo o furto de informações e envio Premium de SMS, mas aqui estão os recursos que o destacaram:

1. Técnicas de antianálise e ofuscamento de código
O Obad emprega duas explorações que tornam as análises estáticas e dinâmicas mais difíceis para o analista de malware e para os sistemas sandbox de análise de malware. Primeiro, modifica o executável Dalvik no APK de modo que causa um erro em algumas ferramentas de engenharia reversa, levando a uma saída errônea. Segundo, o AndroidManifest.xml fornecido no APK também é modificado de modo que fica incompleto, mas o código de checagem de manifestos do Android ignora e permite que o APK seja instalado. Infelizmente, a maioria das ferramentas dinâmicas de análise confia na informação ausente para executar e analisar o APK. Isso leva a um relatório de análise incompleto feito por essas ferramentas.

O Obad também usa ofuscamento de códigos e de cadeias para tornar a análise mais difícil. Todas as cadeias, incluindo nomes de classe e de método, são criptografadas e algumas são criptografadas múltiplas vezes. Para tornar a análise ainda mais dura, também emprega técnicas tais como chamar métodos API através de reflexão e adição de código de lixo.

2. Administração de dispositivo
Quando o Obad é instalado, pede ao usuário por privilégios de Administrador do Dispositivo, o que lhe dá certos privilégios tais como travar o dispositivo. Também impede o aplicativo de ser desinstalado de maneira normal. Para desinstalar um aplicativo de Administrador do Dispositivo, o usuário tem que desinstalá-lo através da lista do Administrador do Dispositivo no menu Settings. Contudo, o Obad explora um erro no Android que impede um aplicativo de ser listado na lista do Administrador do Dispositivo, portanto não há modo de desinstalá-lo.

3. Difusão por meio de Bluetooth
Outro recurso único do Obad é sua habilidade de dispersar a si mesmo e a outros malwares através do Bluetooth. Pode receber um comando do servidor C&C que lhe diz para buscar por dispositivos Bluetooth habilitados detectáveis na redondeza. Então tenta enviar um arquivo possivelmente malicioso a eles.

Não houve relatórios de infecção disseminada do Obad assim que surgiu, mas acreditamos ser significativo que ele demonstra como autores de malwares agora estão investindo maior esforço na criação de malwares de Android mais resilientes e perigosos.

Então, para recapitular, existem alguns atributos técnicos interessantes do trojan Obad que são recentes. Adicionalmente, o motivo por trás do Obad é diferente do Chuli e o X-Force espera uma maior variedade de ataques de malware na plataforma Android com o tempo. No momento, um aspecto problemático da segurança Android é quão desatualizada está a maior parte da base do usuário com relação a firmware de Android. Por exemplo, um usuário de Android desatualizado sem planos de atualização e/ou atualização de firmware disponível não tem chance real de estar imune às influências dos erros do Obad para impedir a desinstalação. Vamos continuar a olhar para o estado atual da segurança do Android desde Julho.

39 http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

Melhorias na segurança de Android

No momento em que este documento foi escrito, a versão Android mais amplamente utilizada é a 2.3 com 34%[40] de todos os dispositivos que executam o Android. Enquanto isso, a última versão do Android (em julho de 2013), a 4.2 é utilizada em menos de 6% de todos os dispositivos Android, apesar de ter estado disponível desde novembro de 2012. Essa versão oferece diversas melhorias de segurança que poderiam reduzir a probabilidade da infecção, ou no mínimo diminuir o impacto uma vez que seja infectado. Aqui estão algumas das melhorias de segurança que poderiam ajudar a frustrar o malware:

1. Verificação de aplicativo

O Android 4.2 inclui um verificador de aplicativo que checa se um aplicativo prestes a ser instalado é potencialmente perigoso ou não, independentemente se será instalado a partir do mercado do Google Play ou de outro lugar qualquer. Este recurso pode ser habilitado entrando em Settings > Segurança > Verificar aplicativos. Durante a instalação do aplicativo, informações sobre o aplicativo incluindo o nome do aplicativo, soma SHA1 do APK, e URLs associadas, entre outras, são enviadas ao Google. O Google então responde com o resultado da detecção. Aplicativos

Melhorias de segurança para o Android 4.2

são assinalados como potencialmente perigosos ou perigosos. Se um aplicativo é assinalado como potencialmente perigoso, o verificador de aplicativos exibe um aviso e dá ao usuário a escolha de continuar a instalação ou cancelá-la. Aplicativos assinalados como perigosos são bloqueados completamente e não serão instalados.

2. Exibição de permissões melhorado

A tela de permissões que é exibida durante a instalação do aplicativo foi melhorada para fornecer mais detalhes sobre as solicitações de permissão do aplicativo. Enquanto as versões anteriores simplesmente exibiam uma descrição curta das permissões a serem solicitadas, a nova tela de permissões também exibe avisos sobre os perigos de se permitir certas permissões.

3. Notificação premium de envio de SMS

Os scams (ou Toll Fraud) premium de SMS constituem o método mais prevalecente no qual autores de malware de Android ganham dinheiro. Para combater isto, o Android 4.2 adiciona um recurso no qual notifica o usuário sempre que um aplicativo tenta enviar uma mensagem SMS para um número de código curto. O usuário tem então a opção de permitir.

40 http://developer.android.com/about/dashboards/index.html

Estas melhorias de segurança, juntamente com as práticas seguras de computação do Android como, por exemplo, abster-se de instalar aplicativos de mercados de terceiros e permanecer informado sobre as permissões solicitadas pelos aplicativos que você instalar, devem percorrer um longo caminho na prevenção de infecções por malware em dispositivos Android.

Conclusão

Para o restante de 2013, o X-Force prevê que o número de aplicativos de malware de Android continue aumentando. Também prevemos que o grau de sofisticação para este malware competirá, eventualmente, com aqueles encontrados em malware de desktop. Poderia haver novos aprimoramentos para combater malware de Android em suas futuras versões, mas acreditamos que a fragmentação do SO (versões antigas que estão sendo utilizadas tanto quanto as mais novas) permanecerão como um problema. Infelizmente, e mais geralmente como norma, o novo firmware não está disponível. Contudo, recomendamos que usuários de Android confiram para ver se uma atualização de firmware está disponível e considerem a atualização.

Vulnerabilidades e explorações

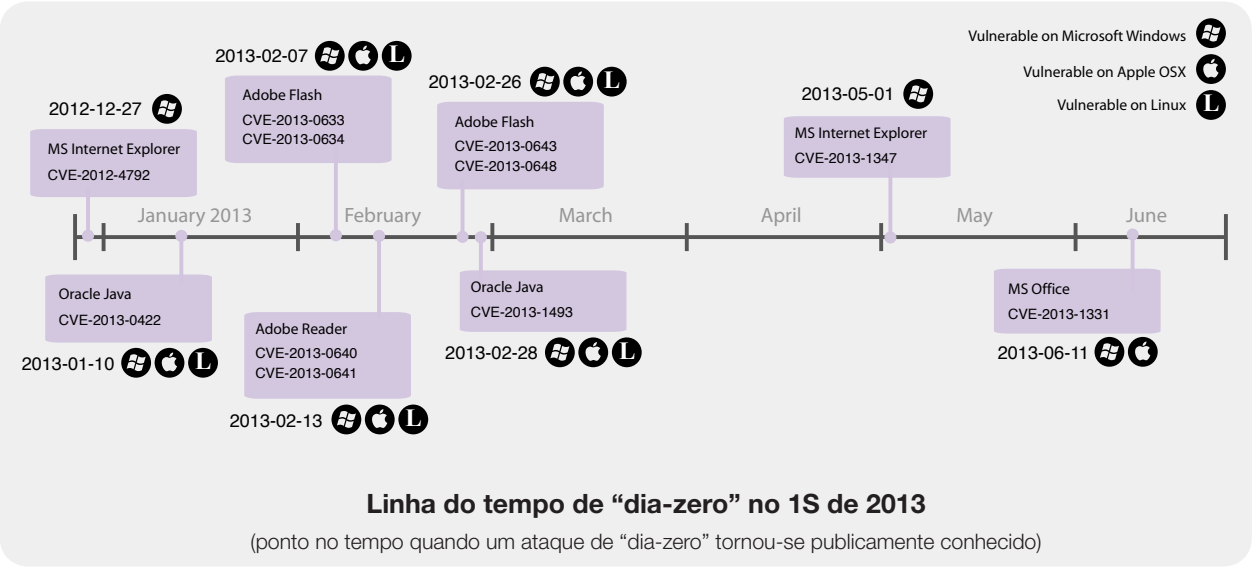
Ataques de "dia-zero" em 1S de 2013

O primeiro semestre de 2013 foi bastante intenso sobre a perspectiva de um ataque de "dia-zero". Nos primeiros seis meses do ano, diversas vulnerabilidades de "dia-zero" afetando amplamente o software implementado, já haviam sido difundidas. A maioria das explorações de "dia-zero" foram inicialmente encontradas em ataques dirigidos, e nós testemunhamos como muitos invasores querem investir nesses ataques quando explorações sofisticadas de "dia-zero" contornaram mecanismos modernos de segurança em software. Neste artigo, veremos esses ataques de "dia-zero" e daremos sugestões que podem reduzir o seu risco de se tornar uma vítima.

Internet Explorer e watering holes perigosos

O ano foi saudado com um ataque de "dia-zero" no Internet Explorer que explorou uma vulnerabilidade não corrigida do mesmo (CVE-2012-4792) circulando livremente durante a última semana de dezembro de 2012.[41] O ataque envolveu invasores implantando o código de exploração no website comprometido do Conselho de Relações Estrangeiras. Poucos meses depois, em maio de 2013, uma exploração para outra vulnerabilidade de "dia-zero" (CVE-2013-1347) no Internet Explorer emergiu.[42] Similar ao primeiro ataque, o código de exploração também foi encontrado em um website comprometido – desta vez o website do Departamento do Trabalho dos EUA foi usado pelos invasores para lançar a exploração de "dia-zero".

O que os dois ataques tinham em comum foi o uso de um website comprometido para lançar a exploração de "dia-zero". Acredita-se que ambos sejam parte de uma campanha de watering hole - uma forma de ataque dirigido no qual um invasor identifica os websites que um grupo-alvo geralmente visita ou provavelmente irá visitar e então compromete aqueles sites para que se tornem as plataformas de lançamento dos ataques.



Linha do tempo de "dia-zero" no 1S de 2013

(ponto no tempo quando um ataque de "dia-zero" tornou-se publicamente conhecido)

Figura 4: Vunerabilidades de "dia-zero"
(ponto no tempo quando um ataque de "dia-zero" tornou-se publicamente conhecido)

41 http://www.fireeye.com/blog/technical/malware-research/2012/12/council-foreign-relations-water-hole-attack-details.html
42 http://labs.alienvault.com/labs/index.php/2013/new-internet-explorer-zeroday-was-used-in-the-dol-watering-hole-campaign/

Como é possível proteger-se contra ataques

Para administradores de websites, tornar-se uma plataforma de lançamento para campanhas de watering hole danifica a reputação do seu website e podem resultar na perda da confiança do cliente. Se você é um administrador de website, abaixo estão algumas sugestões que podem ajudá-lo a reduzir o risco de seu website ser comprometido:

- Reforce seus servidores. Existe uma infinidade de orientações de reforço online para sistemas operacionais e softwares específicos; para orientações gerais, uma referência é o "Guide to General Server Security"[43] publicado pelo NIST (National Institute of Standards and Technology).
- Certifique-se de que o software e os aplicativos da web instalados no servidor estejam sempre atualizados. Se estiver desenvolvendo pessoalmente os aplicativos da web, o OWASP (Open Web Application Security Project)[44] fornece orientações para proteger aplicativos da web.
- Credenciais de login de servidores roubadas também são uma causa de comprometimento de websites. Uma das razões para credenciais de login roubadas é se a máquina cliente utilizada para conectar-se ao servidor fica comprometida. Portanto, certifique-se de que a máquina cliente que você utiliza para conectar-se ao servidor não está comprometida e que também esteja reforçada. Mais adiante neste artigo existem algumas sugestões que se aplicam ao reforço de máquinas clientes. Finalmente, utilizar senhas fortes e utilizar senhas diferentes para contas diferentes

O que é uma campanha watering hole?

Water holing foi inicialmente criado pela RSA em 2012.[45] Embora uma forma similar de ataques tenha sido observada no passado, a RSA o usou inicialmente em uma campanha apelidada de "VOHO"[46] Na campanha VOHO, diversos websites que atendiam a grupos específicos relacionados ao ativismo político, base industrial de defesa, e áreas geográficas específicas foram comprometidas ao carregar um código de exploração em outro website comprometido. No início de 2013, campanhas watering hole foram popularizadas adiante quando diversas empresas de perfil elevado tais como Apple[47] e Facebook[48] reportaram que alguns de seus funcionários foram atacados através de um website comprometido de um desenvolvedor.

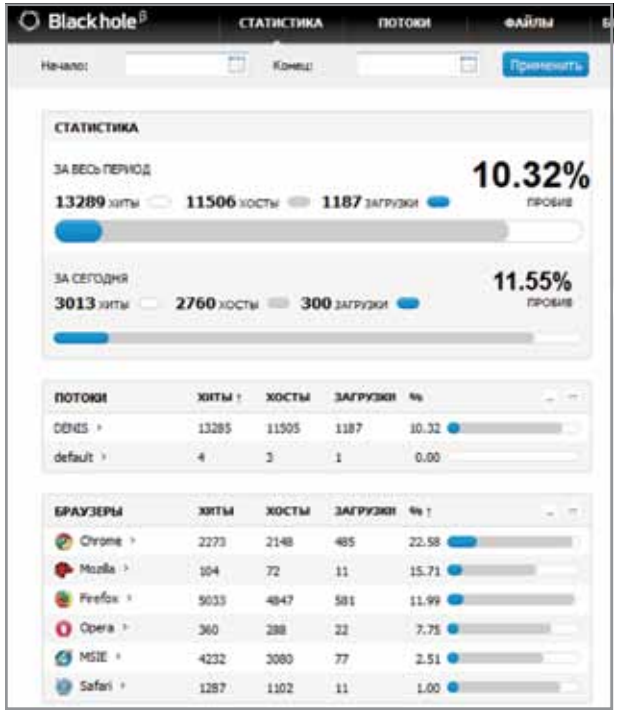
Campanhas watering hole são passivas se comparadas a campanhas spear-phishing na medida em que as vítimas em potencial não são diretamente atraídas por um invasor para executar uma ação em particular. Em vez disso, o invasor espera que as vítimas visitem o website comprometido e então lançam o ataque de lá. Esta propriedade particular dos ataques watering hole faz com que até mesmo usuários treinados se tornem alvos em potencial uma vez que esses tipos de usuários são menos propensos a se tornar presas de ataques spear-phishing, mas que muito provavelmente visitarão os sites comprometidos como parte de sua rotina normal.

43 http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
44 https://www.owasp.org/index.php/Main_Page
45 http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/
46 http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf
47 http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219
48 https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766

Java: Interesse contínuo por parte de autores de kits de exploração

Mesmo antes que a vulnerabilidade de "dia-zero" de dezembro do Internet Explorer foi corrigida, descobriu-se duas novas vulnerabilidades de "dia-zero" de Java (ambas rotuladas como CVE-2013-0422) já haviam sido difundidas. Durante a segunda semana de Janeiro, descobriu-se que kits de exploração tais como o Blackhole e o kit de exploração Cool estavam explorando vulnerabilidades de Java não corrigidas para escapar ao sandbox de Java a fim de instalar malware em máquinas de vítimas. Continuando a tendência que reportamos no **IBM X-Force 2012 Trend and Risk Report** anual, outros autores de kits de exploração demonstraram interesse nas vulnerabilidades de "dia-zero" de Java e logo seguiram adiante ao integrar a exploração de "dia-zero" em seus kits de exploração.[49]

Poucas semanas depois, uma terceira vulnerabilidade de "dia-zero" de Java (CVE-2013-1493) já estava difundida. Explorações iniciais para o "dia-zero" foram descobertas durante a última semana de fevereiro.[50] Não está claro como os ataques iniciais foram conduzidos, mas o que veio a seguir não foi uma surpresa: Diversos autores de kits de exploração começaram a integrar a exploração para o "dia-zero" em seus kits de exploração.[51]



Painel de controle do kit de exploração Blackhole

O primeiro semestre de 2013 não foi só de más notícias para a Java uma vez que a Oracle realizou duas importantes melhorias de segurança para a execução de Java no navegador. A primeira mudança foi feita no release 7u10 do Java que foi a adição de um recurso para desabilitar com facilidade o Java em um navegador. A segunda mudança importante foi realizada no release 7u11 do Java, que foi a mudança das configurações de segurança padrão utilizando o nível "Alto", o que significa que o usuário recebe o aviso antes da execução dos aplicativos de Java não assinado no navegador. Esta alteração tardia torna a utilização do Java menos atraente para os invasores uma vez que eles agora não precisariam utilizar táticas de engenharia para atrair usuários para seus aplicativos maliciosos de Java ou explorar uma vulnerabilidade secundária que permite ao invasor contornar o aviso de segurança do Java.

49 http://malware.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html
50 http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/yaj0-yet-another-java-zero-day-2.html
51 http://malware.dontneedcoffee.com/2013/03/cve-2013-1493-jre17u15-jre16u41.html

Flash Player: Ataques através de documentos do Office

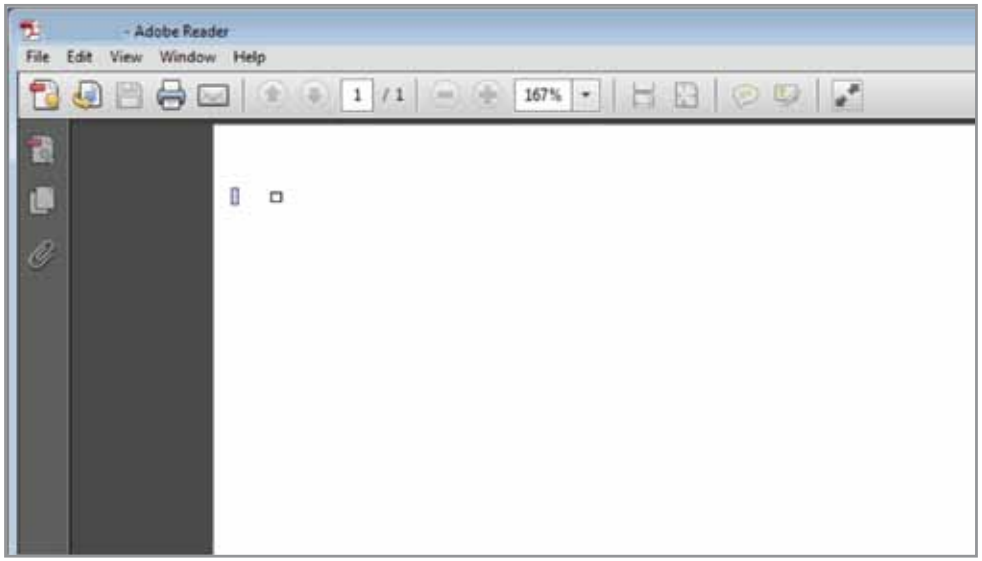
Fevereiro também foi um mês ocupado à medida que ataques de "dia-zero" foram descobertos ou relatados. Em adição à terceira vulnerabilidade de Java discutida anteriormente, descobriu-se que dois aplicativos adicionais amplamente implementados foram alvejados por explorações de "dia-zero". O primeiro destes é o Adobe Flash Player discutido aqui e o segundo é o Adobe Reader, discutido na próxima seção.

Enquanto os usuários estavam se recuperando do ataque de "dia-zero" de Java de janeiro, no início de fevereiro, descobriu-se duas vulnerabilidades de Flash Player (CVE-2013-0633 e CVE-2013-0634) já haviam sido difundidas. Do relatório do fornecedor,[52] uma característica em ambos os ataques para usuários de Windows foi que o ataque envolveu a entrega de explorações via arquivos em Flash embutidos em documentos do Word. E, em 26 de fevereiro, a Adobe publicou outro boletim de segurança declarando que foram detectadas duas vulnerabilidades adicionais de "dia-zero" (CVE-2012-0643 e CVE-2013-0648) já estavam sendo exploradas.

O Adobe assinalou que, [53]desde a introdução do sandbox do Reader em 2010, o método mais comum de entrega para ataques de "dia-zero" do Flash Player era feito pelos documentos do Office. Somado aos dois primeiros ataques de "dia-zero" de Flash abordados anteriormente, um exemplo notável disso é a violação RSA em 2011, na qual invasores integraram explorações de "dia-zero" de Flash em um documento do Excel.[54]

Adobe Reader: Explorações sofisticadas

Poucos dias após se descobrir que o primeiro grupo de vulnerabilidades de "dia-zero" de Flash Player estava sendo difundido, uma exploração sofisticada de "dia-zero" para Adobe Reader surgiu. Curiosamente, esta exploração de "dia-zero" em particular é a primeira exploração "in-the-wild" (já difundida entre utilizadores) capaz de escapar do sandbox do Reader (inicialmente introduzida em 2010).



A exploração de "dia-zero" do Reader – um arquivo PDF aparentemente em branco é mostrado enquanto um ataque sofisticado que explora duas vulnerabilidades de "dia-zero" é executado no plano de fundo.

52 http://www.adobe.com/support/security/bulletins/apsb13-04.html
53 http://blogs.adobe.com/asset/2013/02/raising-the-bar-for-attackers-targeting-flash-player-via-office-files.html
54 https://blogs.rsa.com/anatomy-of-an-attack/

O ataque explorou duas vulnerabilidades de "dia-zero" (CVE-2013-0640 e CVE-2013-0641), uma das quais permitiu que a exploração executasse um código arbitrário dentro do sandbox do Reader quando o usuário abrisse um arquivo PDF. A outra vulnerabilidade é utilizada pela primeira exploração para executar um código dentro do sandbox restritivo do Reader. Relata-se que explorações iniciais[54] foram utilizadas em ataques dirigidos onde as vítimas receberam um email com um arquivo PDF anexo contendo a exploração.

Explorações tais como a sofisticada exploração do Reader demonstram que os invasores desejam investir recursos significativos para se infiltrar em seus alvos. Desenvolver uma exploração que contorne diversos mecanismos modernos de segurança – como, por exemplo, o ASLR (Address Space Layout Randomization), DEP (Data Execution Prevention) e o sandbox do Reader neste caso – e que trabalhe em uma versão moderna de um sistema operacional, não é um feito fácil. O desenvolvimento desta exploração em particular exigiu muitas semanas ou meses de pesquisas e desenvolvimento dependendo das habilidades técnicas dos invasores envolvidos. À medida que os sandboxes crescem em popularidade, podemos esperar ver mais desses tipos de ataque no futuro.

Office: ataque extremamente dirigido

Em junho, a Microsoft relatou e corrigiu uma vulnerabilidade de "dia-zero" (CVE-2013-1331) no Microsoft Office. A Microsoft descreve [56]os ataques iniciais como extremamente direcionados. Isto é porque não se sabe muito sobre o ataque antes do informe da Microsoft ter sido publicado. A vulnerabilidade afetou a última versão do Office para Mac (Office 2011), mas afetou somente uma versão anterior do Office no Windows (Office 2003).

Reduzindo seu risco: reduzir, atualizar e educar

Vulnerabilidades de "dia-zero" continuarão a serem descobertas e exploradas se os invasores continuarem a vê-las como veículos para crimes e espionagem. Mesmo se as explorações iniciais de "dia-zero" forem encontradas em ataques dirigidos, as explorações eventualmente terminam em ferramentas automatizadas de ataque tais como os kits de exploração. Isso significa que eventualmente, todos os que estiverem utilizando o software afetado poderão se tornar alvos em potencial.

55 http://www.adobe.com/support/security/advisories/apsa13-02.html
56 http://blogs.technet.com/b/srd/archive/2013/06/11/ms13-051-get-out-of-my-office.aspx

Reduzir seu risco é um dos primeiros passos que você pode dar para evitar tornar-se uma vítima de ataques de "dia-zero". Seguem abaixo algumas sugestões que você pode seguir:

1. **Reduzir a superfície de ataque.**
   Um dos passos mais importantes na redução do risco de se tornar uma vítima de explorações de "dia-zero" – e explorações em geral – é reduzir os meios como você pode ser atacado. Tome tempo para revisar os plug-ins de seu navegador instalado e desinstale aqueles que já não tem utilizado há algum tempo. Se realmente precisa utilizar um plug-in de navegador específico, utilize o recurso "Click-to-play" se seu navegador tiver suporte para isso. O Click-to-play impede a exploração silenciosa ou "drive-by" de plug-ins ao solicitar uma interação adicional do usuário antes que um plug-in possa ser utilizado. Outro exemplo da redução de sua superfície de ataque é desabilitar os controles ActiveX no Office[57] que pode mitigar explorações de Flash entregues através de documentos de Office. Finalmente, se estiver utilizando Java para executar aplicativos de desktop (autônomos), mas não estiver utilizando o Java para executar aplicativos em seu navegador, é possível optar por desabilitar o Java em seu navegador.[58]
2. **Atualizar softwares instalados.**
   Versões recentes ou atualizadas de aplicativos introduzem novos recursos de segurança que o tornam mais custosos ou menos atraentes para um invasor utilizá-los como vetores para explorações. Exemplos de tais recursos de segurança incluem capacidades de sandbox e recursos que impedem o carregamento automático de conteúdo potencialmente inseguro. Esses incluem o Click-to-play em navegadores e as configurações de nível de segurança no Java, o que impede a execução automática de aplicativos Java não assinados no navegador.
3. **Obter instrução sobre ataques spear-phishing.**
   Em campanhas spear-phishing, o invasor envia emails personalizados a um grupo específico de vítimas, o email geralmente incentiva o destinatário a abrir um documento ou arquivo anexo, ou clicar em um link para um website que por sua vez poderá lançar uma exploração. Ao instruir-se em como reconhecer esses emails suspeitos, é possível evitar tornar-se presa dessas campanhas spear-phishing.

À medida que as explorações de "dia-zero" continuam a se tornar mais sofisticadas e os invasores desenvolvem maneiras diferentes de entregar esses ataques de "dia-zero", preparar-se para reduzir seu risco é uma das melhores ações que o X-Force acredita que você pode tomar.

57 http://office.microsoft.com/en-us/excel-help/enable-or-disable-activex-controls-in-office-documents-HA010031067.aspx
58 http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/client-security.html

Divulgações de vulnerabilidades no primeiro semestre de 2013

Desde 1997, o X-Force tem rastreado divulgações públicas de vulnerabilidades em produtos de software. O X-Force coleta anúncios de software de fornecedores, revisa listas de endereçamento relacionadas à segurança, e analisa centenas de páginas de web sobre vulnerabilidades onde dados de solução, explorações e vulnerabilidades são publicados.

No primeiro semestre de 2013, nós inserimos pouco mais de 4.100 novas vulnerabilidades de segurança reportadas publicamente. Se essa tendência continuar pelo restante do ano, o total projetado de vulnerabilidades deverá se aproximar de um total de 8.200 vulnerabilidades, virtualmente o mesmo número que vimos em 2012.

Desde 2006, nosso primeiro declínio em divulgações de vulnerabilidades em 2007, temos visto o número total de vulnerabilidades subir e descer a cada dois anos. Contudo, se os números se mantiverem, este poderia ser nosso primeiro ano em que esses totais não se alternam entre a sequência anual mais alta e a mais baixa vista durante os últimos sete anos.

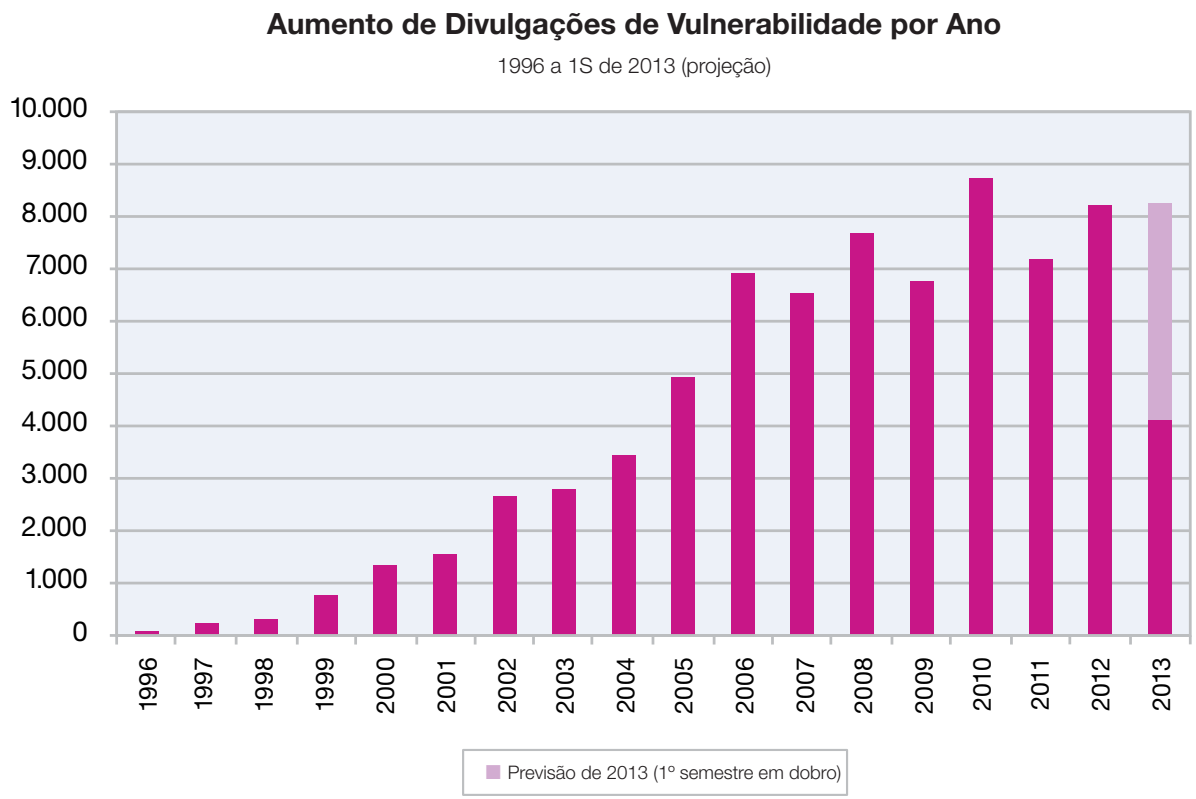


Figura 5: Crescimento de divulgações de vulnerabilidade por ano – 1996 a 1S de 2013 (projeção).

Vulnerabilidades de aplicativos da web

A maioria das vulnerabilidade que a equipe X-Force documenta são aquelas em programas de aplicativos da web, como por exemplo, o CMS (Content Management Systems). No primeiro semestre de 2013, 31% das vulnerabilidades que foram reportadas publicamente são as que categorizamos como aplicativos utilizados na Internet. Este número caiu significativamente desde 2012 aonde vimos níveis a 42%. Mais da metade de todas as vulnerabilidades de aplicativos da web são de cross-site scripting.

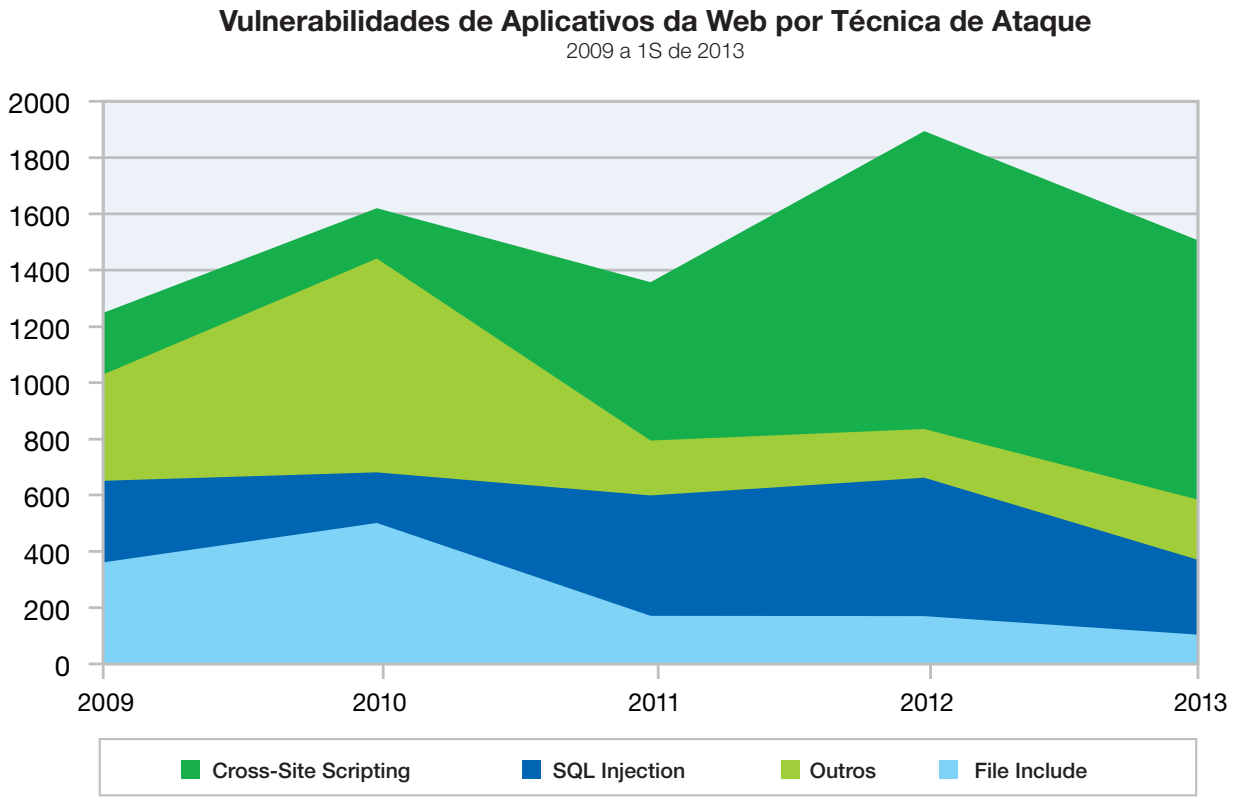


Figura 6: Vulnerabilidades de aplicativos da web por técnica de ataque – 2009 a 1S de 2013.

CMS (Content Management Systems) são alguns dos softwares mais populares utilizados na Internet. A maioria dos fornecedores adotou a segurança e realizou um bom trabalho na correção de seus softwares principais quando as vulnerabilidades de segurança são reportadas a eles. 78% de todas as vulnerabilidades reportadas no CMS foram corrigidas no primeiro semestre de 2013, enquanto que em 2012 vimos que somente 71% das vulnerabilidades foram corrigidas. Ano após ano vemos que esses fornecedores estão realizando um trabalho melhor em manter seus produtos atualizados com a mais recente cobertura de segurança. Contudo, criadores de plug-ins CMS terceirizados não foram tão bem ao fornecer uma correção para somente 54% das vulnerabilidades. Com mais de 46% de vulnerabilidades sem correção, os plug-ins de terceiros tornam-se oportunidades atraentes para que os ataques ocorram.

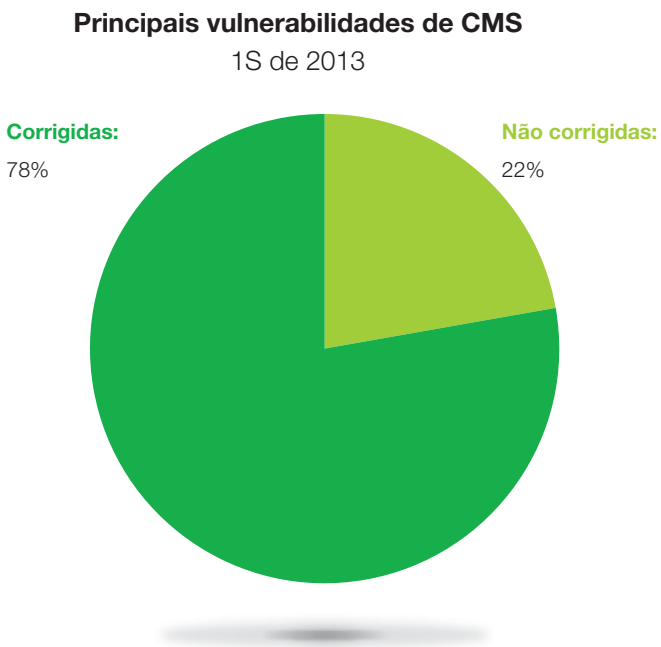


Figura 7: Vulnerabilidades publicadas em sistemas de gerenciamento de conteúdo principal – corrigidas versus não corrigidas no 1S de 2013.

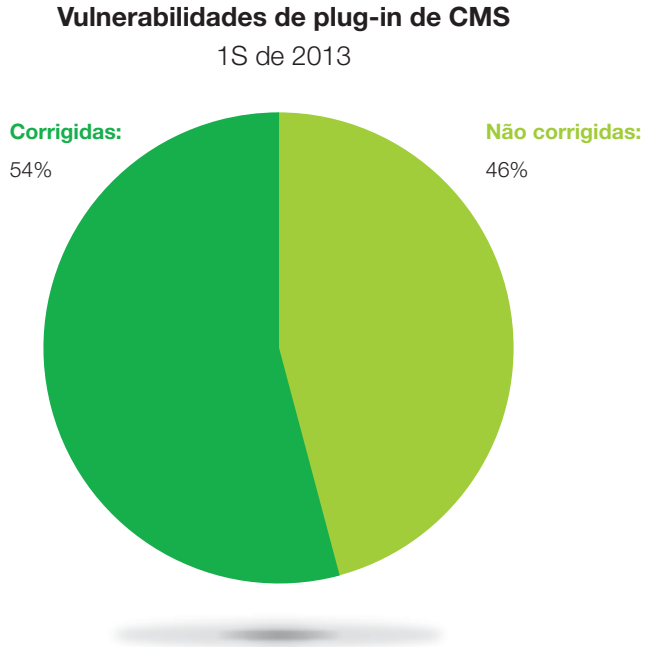


Figura 8: Vulnerabilidades publicadas em sistemas de gerenciamento de plug-ins – corrigidas versus não corrigidas no 1S de 2013.

Vulnerabilidades móveis

Apesar das vulnerabilidades que afetam aplicativos móveis e sistemas operacionais representarem uma porcentagem relativamente pequena do total das divulgações (projetado em pouco mais de 4% em 2013), temos visto o número total de divulgações aumentar significativamente desde 2009 quando as vulnerabilidades móveis representavam menos de 1% do total de divulgações. Após um salto substancial em 2009, o número decresceu levemente de 2010 a 2011 antes de outro salto substancial em 2012 (consulte a Figura 9).

Muitas das vulnerabilidades que afetam as plataformas móveis se originaram de componentes que são utilizados tanto em software móvel como em de desktop. As vulnerabilidades restantes são específicas de aplicativos móveis e representam uma grande porção do aumento em divulgações vistas em 2012 e 2013.

Um desenvolvimento digno de nota relacionado a vulnerabilidades móveis em 2013 tem a ver com o número de explorações públicas disponíveis. Em 2013, pouco menos de 30% de todas as divulgações móveis tinham explorações públicas ou código de prova de conceito disponíveis. Em comparação, apenas 9% das vulnerabilidades móveis divulgadas entre 2009 e 2012 possuíam explorações públicas. A maioria dessas explorações é dirigida especificamente para aplicativos móveis e são primariamente divulgadas em repositórios públicos populares de exploração.

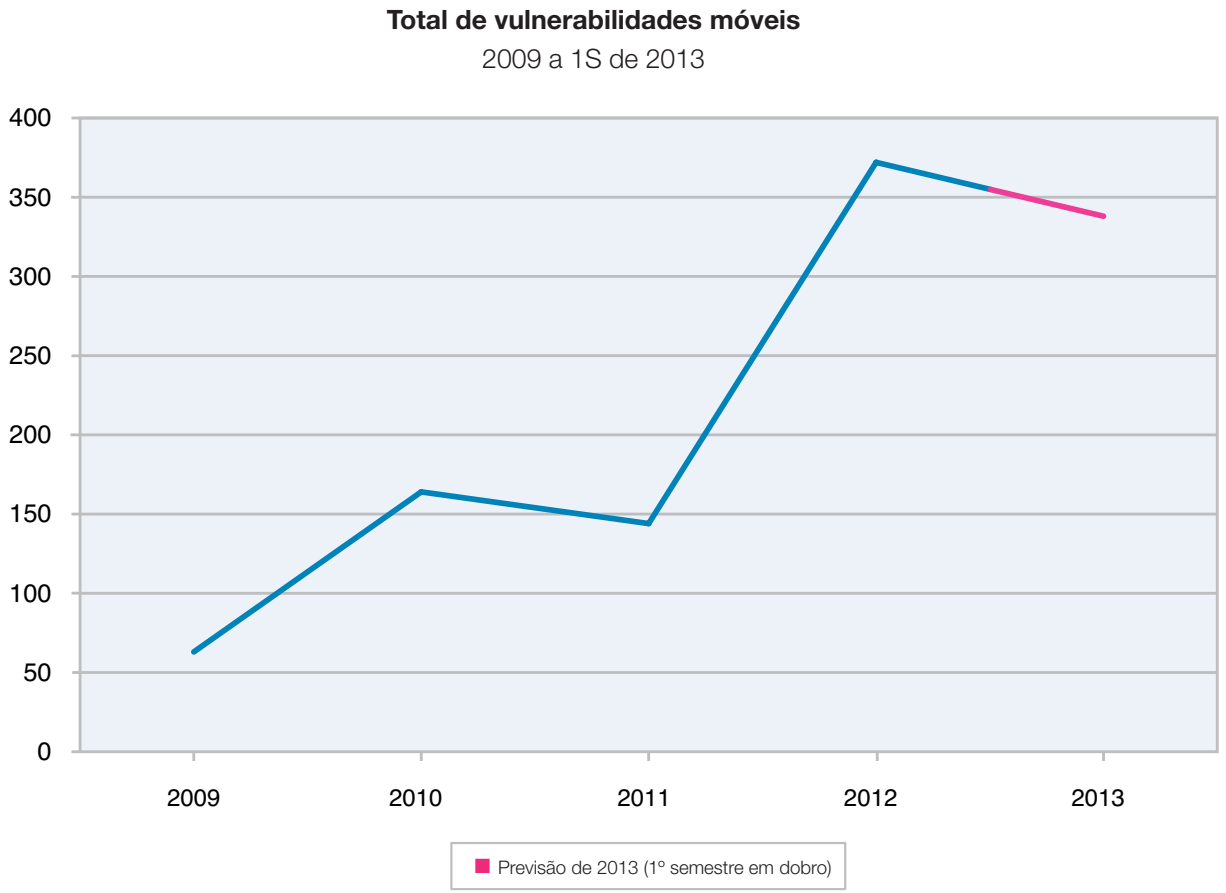


Figura 9: Total de vulnerabilidades móveis – 2009 a 1S de 2013 (projeção)

Consequências da exploração

O X-Force categoriza vulnerabilidades pela consequência da exploração. Essa consequência é basicamente o benefício que a exploração de vulnerabilidade fornece ao invasor. A Tabela 1 descreve cada consequência.

Consequência	Definição
Contornar Segurança	Driblar restrições de segurança, como autenticação, firewall, proxy, sistema IDS/IPS ou um scanner de vírus
Cross-Site Scripting	O impacto do cross-site scripting varia dependendo do aplicativo visado ou usuário-vítima, mas pode incluir consequências tais como: divulgação de informações confidenciais, interceptação de sessões, spoofing, redirecionamento de site, ou desfiguração de website
Manipulação de Dados	Manipular dados usados ou armazenados pelo host associado ao serviço ou aplicativo
Negação de Serviço	Perda ou interrupção de um serviço ou sistema
Manipulação de Arquivo	Criar, excluir, ler, modificar ou sobrescrever arquivos
Obter Acesso	Obtenção de acesso local e/ou remoto a um aplicativo ou sistema. Isso também inclui vulnerabilidades pelas quais um invasor pode executar código ou comandos, pois, em geral, isso permite que o invasor obtenha acesso ao serviço subjacente ou sistema operacional
Obter Privilégios	Um invasor que utiliza credenciais válidas pode obter privilégios elevados para um aplicativo ou sistema
Obter informações	Obter informações como nomes de arquivo e de caminho, código fonte, senhas ou detalhes de configuração de servidor
Outros	Refere-se a tudo ainda não abordado por outras categorias
Desconhecido	A consequência não pode ser determinada com base em informações insuficientes

Tabela 1: Definições para Consequências de Vulnerabilidade

A consequência mais prevalecente da exploração de vulnerabilidade para o primeiro semestre de 2013 foi "obter acesso" com 28% de todas as vulnerabilidades reportadas. Na maioria dos casos, obter acesso a um sistema proporciona ao invasor o controle total sobre o sistema afetado, o que lhes permite roubar dados, manipular o sistema ou iniciar outros ataques a partir de tal sistema. Cross-site scripting foi a segunda consequência mais prevalecente com 18% e tipicamente envolve ataques contra aplicativos de web. Para informações adicionais sobre vulnerabilidades de aplicativos de web em 2013, consulte a página 35.

Um detalhamento completo de todas as consequências de vulnerabilidades reportadas durante o primeiro semestre de 2013 é exibido na Figura 10.

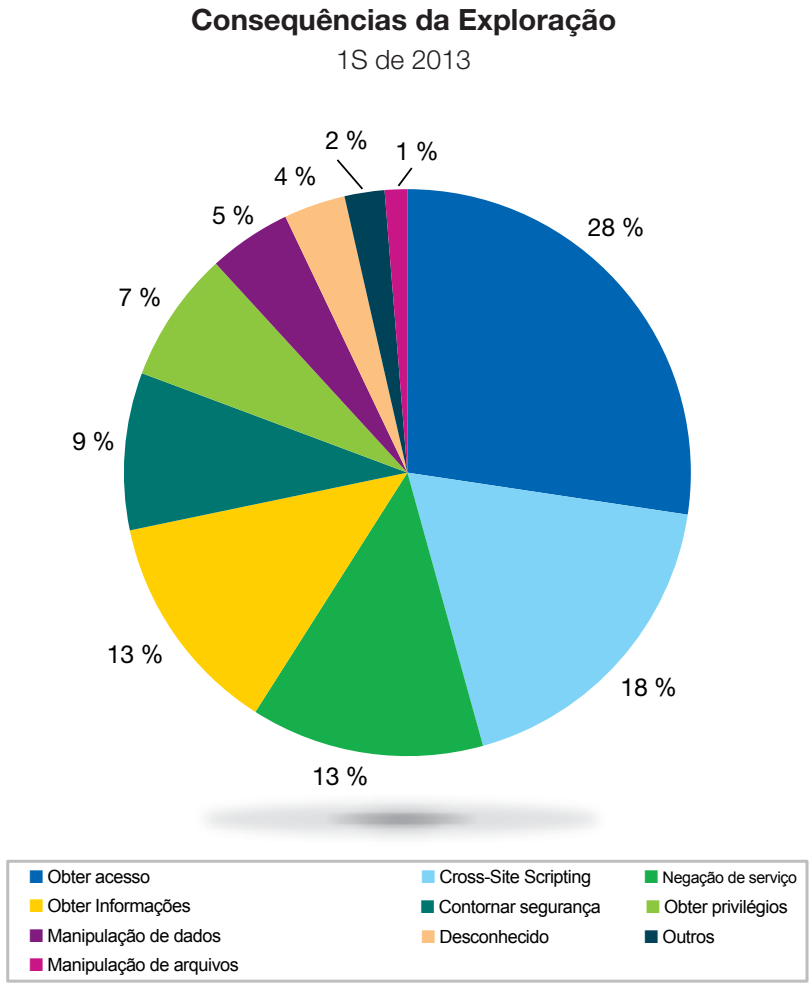


Figura 10: Consequências da exploração – 1S de 2013

Esforço da exploração versus retorno potencial

À medida que os ataques virtuais se intensificam, monitorar as numerosas divulgações de vulnerabilidades todo dia se torna assustador. Dentro do IBM X-Force, nós rastreamos vulnerabilidades emitidas publicamente através de um processo de triagem para identificar quais são aquelas que mais provavelmente serão utilizadas por um ataque e então determinamos quais exigem pesquisa mais detalhada. Ao realizar esta análise, reconhecemos que todas as vulnerabilidades caracterizam-se por dois fatores: a exploração de "recompensa potencial", que atrai o invasor e o "esforço de exploração para o sucesso", que impede o invasor de realizar desenvolvimentos posteriores. A matriz de probabilidades de exploração é desenvolvida por representação gráfica de "recompensa de exploração" e "esforço de exploração para o sucesso" ao longo dos eixos. Ao designar as vulnerabilidades a seu quadrante apropriado, torna-se claro quais são favorecidas por invasores.

A exploração "retorno em potencial" passa pelo eixo Y e indica o valor dos dados extraídos das máquinas comprometidas. Em termos quantitativos, as vulnerabilidades com ampla cobertura de produto em máquinas desktop, ou vulnerabilidades que afetam servidores corporativos contendo a conta de todos os funcionários são atraentes aos invasores. Em termos qualitativos, dados confidenciais possuem valor mais elevado e são mais sedutores. Os ganhos financeiros a partir dos dados e oportunidades de exploração são sinônimos desse eixo.

A exploração "esforço da exploração para sucesso" passa pelo eixo Y e indica os recursos exigidos para traduzir vulnerabilidades em explorações confiáveis. Esses recursos incluem a experiência, tempo e esforço que um invasor gasta para contornar os mecanismos de proteção, e/ou a manipulação do layout de memória para alcançar a execução do código. À medida que mais mecanismos de proteção são implementados em sistemas operacionais modernos, o conjunto de invasores habilidosos inevitavelmente diminui. Claramente, isso também significa que o valor dos dados comprometidos aumenta e implica na proporcionalidade direta entre a exploração "retorno em potencial" e o "esforço da exploração para sucesso".

Na matriz de probabilidades de exploração, emergem quatro categorias de classificação. No quadrante superior direito, vulnerabilidades com enorme retorno potencial e baixo custo de exploração se enquadram nessa categoria de "exploração em larga escala". Devido ao fato de produzirem os melhores retornos de investimento, espera-se que essas vulnerabilidades sejam amplamente difundidas. No quadrante superior esquerdo, vulnerabilidades com enorme retorno potencial e alto esforço de exploração se enquadram nessa categoria de "ataque sofisticado". Embora os invasores sejam igualmente motivados pelos ganhos, somente invasores sofisticados possuem as habilidades exigidas para conseguir a execução de códigos. Portanto, a exploração desses provavelmente será contida. No quadrante inferior esquerdo, vulnerabilidades com baixo retorno potencial, mas com alto esforço de exploração se enquadram nessa categoria de "não amplamente dirigido". Talvez essas vulnerabilidades estejam mais bem adaptadas a objetivos educacionais do que a ataques virtuais. No quadrante inferior direito, vulnerabilidades que também produzem baixo retorno potencial com baixo esforço de exploração se enquadram na categoria de "exploração ocasional". Mesmo que os retornos sejam baixos, elas são fáceis o suficiente para serem exploradas. Esperamos ver essas divulgadas somente quando os invasores possuírem objetivos muito específicos.

No primeiro semestre de 2013, o X-Force distribuiu 14 alertas e avisos sobre divulgações que merecem a devida atenção. Colocamos sete desses alertas e avisos, coincidentemente compostos inteiramente de IE (Internet Explorer) e Java, no quadrante superior direito – vulnerabilidades com alto retorno e baixo custo. Todas as sete vulnerabilidades podem ser usadas em exploração drive-by, alcançando tantas vítimas quanto possível. Os problemas de uso após a liberação do Internet Explorer podem ser explorados com capacidades de scripting do navegador. Esses se ajustam aos critérios para a "exploração em larga escala". O CVE-2013-1347 foi utilizado no ataque watering hole envolvendo o Departamento do Trabalho dos EUA (conforme discutido em seções anteriores). Embora tenha afetado somente o IE8, muitas outras máquinas ainda podem ter sido afetadas por duas razões – o IE8 é a versão mais atual permitida no Windows XP/2003 – e também é o navegador padrão em um Windows 7 recém-instalado.

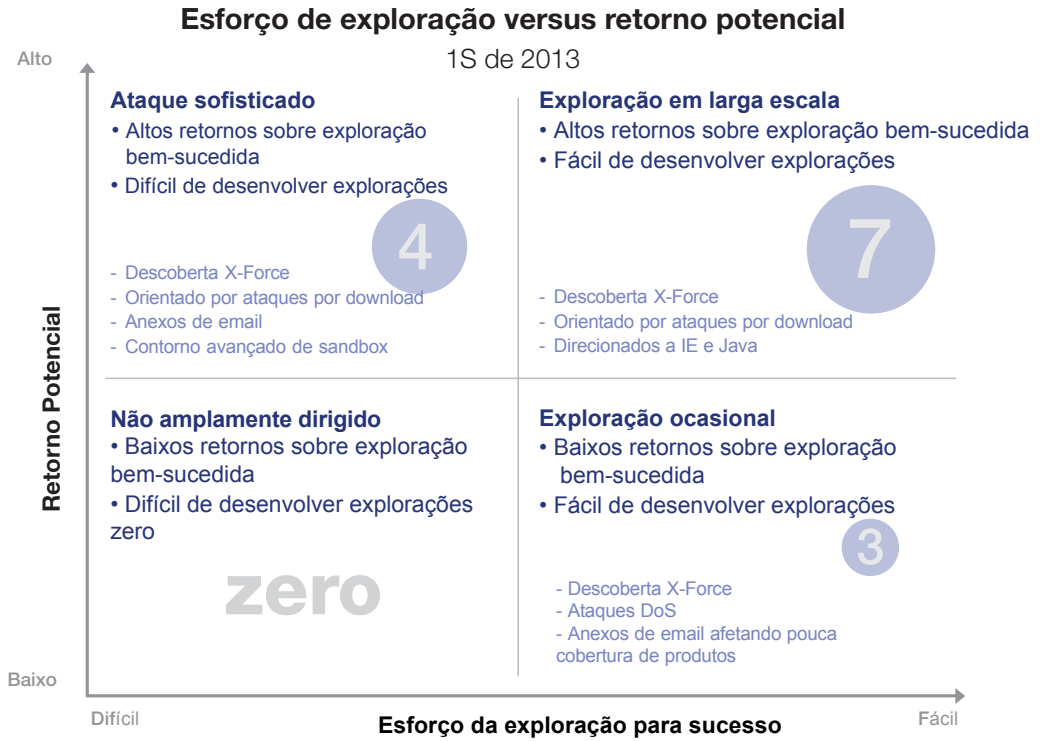


Figura 11: Esforço de Exploração versus Retorno Potencial – 1S de 2013

Colocamos quatro outros alertas e informes no quadrante superior esquerdo – vulnerabilidades com alto retorno e grande esforço de desenvolvimento. Essas vulnerabilidades envolvem problemas de estouro de fragmentação que exigem que os invasores manipulem a memória que segue o estouro com objetos úteis. Considerando a quantidade de experiência exigida, esperamos ver tais vulnerabilidades sendo utilizadas em ataques mais sofisticados. Dois dos alertas/informes são para vulnerabilidades de escape ao sandbox. Alcançar uma exploração completa de aplicativos em sandbox é normalmente um processo em dois estágios – uma vulnerabilidade para a execução de códigos no processo de sandbox antes de utilizar outra vulnerabilidade para escapar no processo de corretagem. Se qualquer dessas vulnerabilidades é vista em liberdade, isso implica que o invasor possui capacidade para outra. Subsequentemente, o X-Force não trata as vulnerabilidades de escape do sandbox de modo diferente. Os outros dois alertas e informes, CVE-2013-0633 e CVE-2013-0634, são vulnerabilidades envolvendo o Adobe Flash Player. Essas vulnerabilidades possuem vetores de ataque variáveis; eles podem ser utilizados na exploração drive-by de navegador ou por embutir os arquivos defeituosos em documentos de email.

Os três alertas e informes restantes são colocados dentro do quadrante inferior direito – que são vulnerabilidades com baixo retorno e baixo esforço de desenvolvimento. O CVE-2013-1331 é um estouro de pilha clássico que afeta o Microsoft Office 2003 e Office para Mac 2011. Acreditamos que a oportunidade para exploração é limitada por razões diferentes; o Microsoft Office 2003 já é um produto com dez anos de vida enquanto que o Office para Mac 2011, embora atual, é menos amplamente implementado do que a versão Windows. O CVE-2013-0176 e o CVE-2013-1305 são vulnerabilidades DoS (denial of service) que afetam sistemas de servidores. Embora menos atraentes que a execução de códigos, ataques DoS ainda servem ao propósito, conforme evidenciado por ataques DoS de alto perfil recentes. Com essas vulnerabilidades, os invasores são capazes de DoS os sistemas com um único pacote em vez de ter que cultivar uma botnet. Portanto, parece apropriado ao X-Force emitir alertas e informes a respeito deles.

Qual é a diferença entre um Alerta de Proteção e um Informe?

Basicamente, é a diferença entre se o problema de segurança foi descoberto pelo IBM X-Force, ou se o mesmo está fornecendo informações adicionais sobre um problema de segurança existente descoberto por alguém. Ambos fornecem informações de proteção para a ameaça classificada.

Alertas de proteção do IBM X-Force são lançados quando o X-Force descobre informações adicionais significativas sobre um problema de segurança existente.

Informes de proteção do IBM X-Force contêm informações de pesquisas internas originais do X-Force. Cada informe inclui uma descrição detalhada da vulnerabilidade de segurança, seu impacto, versões afetadas, e recomendações para o gerenciamento e/ou correção do problema.

Exploração em larga escala	CVE-2013-1347	Alerta	Microsoft Internet Explorer Use After Free Vulnerability
	CVE-2013-1486	Alerta	Oracle Java Runtime Environment JMX code execution
	CVE-2013-0027	Informe	Microsoft Internet Explorer CPasteCommand code execution
	CVE-2013-0029	Informe	Microsoft Internet Explorer CHTML code execution
	CVE-2012-3342	Informe	Oracle Java Runtime Environment Remote Code Execution
	CVE-2013-0422	Alerta	Oracle Java Runtime Environment MBean code execution
	CVE-2012-4792	Alerta	Microsoft Internet Explorer Could Allow Remote Code Execution
Ataque sofisticado	CVE-2013-0504	Informe	Adobe Flash Player for Firefox Sandbox Bypass
	CVE-2013-0640	Alerta	Adobe Reader and Acrobat XFA Remote Code Execution
	CVE-2013-0641	Alerta	Adobe Reader and Acrobat XFA Remote Code Execution
	CVE-2013-0633	Alerta	Adobe Flash Player buffer overflow
Exploração ocasional	CVE-2013-1331	Alerta	Microsoft Office vulnerability could allow Remote Code Execution
	CVE-2013-1305	Alerta	Microsoft Vulnerability in HTTP.sys Could Allow Denial of Service
	CVE-2013-0176	Informe	libsshpublickey_from_privatekey() function denial of service

Tabela 2: Alertas e informes X-Force no 1S de 2013

Tendências de ameaças da web

O centro de processamento de dados IBM X-Force Content revisa constantemente novos dados de conteúdo da web e analisa 150 milhões de novas páginas da web e imagens por mês.

O centro de processamento de dados IBM X-Force Content tem rastreado e classificado páginas da web continuamente por 14 anos e até o momento, analisou e classificou 20 bilhões de páginas e imagens. O resultado principal desta classificação é o banco de dados IBM de filtro da web que consiste de 81 milhões de entradas através de 69 categorias únicas de classificação. O banco de dados captura hoje cerca de 150.000 entradas novas ou atualizadas todos os dias na medida em que acompanha a natureza dinâmica da Internet.

Este tópico fornece uma revisão dos itens a seguir:

- Metodologia de análise
- Porcentagem de conteúdo indesejado da Internet
- Categorias de websites que contém links maliciosos
- Distribuição geográfica de malware e servidores C&C
- Implementação IPv6 para websites

Metodologia de análise

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

Porcentagem de conteúdo indesejado da Internet

Em nossos esforços de classificar qual porcentagem de websites fornece conteúdo indesejado, nós nos concentramos no primeiro milhão de websites mais populares e mais utilizados conforme classificados pelo Alexa.[59]

Ao passo que cerca de 93% da web contém conteúdo normal, cada 20º website exibe pornografia e 2,1% fornece outros conteúdos obscenos, como proxies de web, jogos de azar, malware, phishing, entre outros.

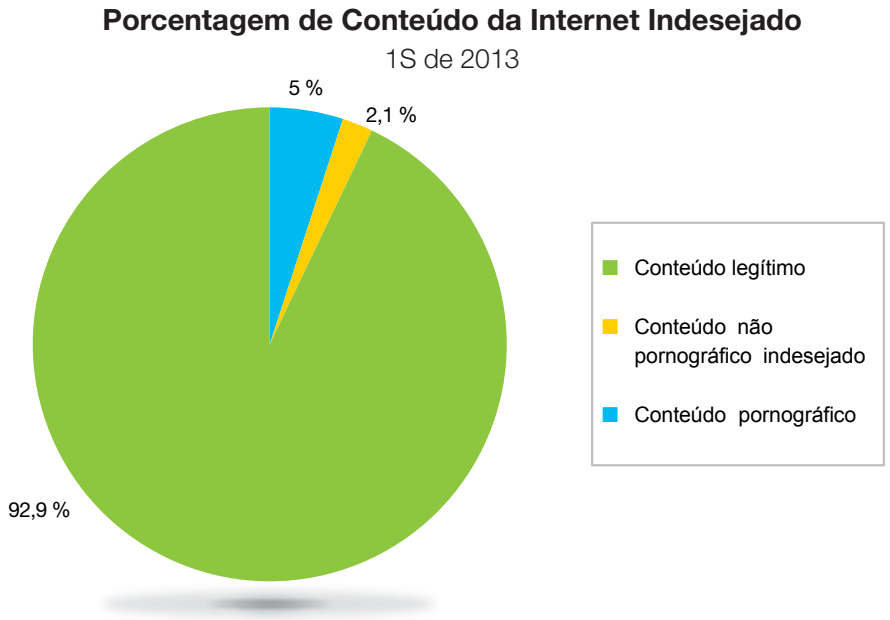


Figura 12: Porcentagem de conteúdo de Internet indesejado – 1S de 2013.

59 De acordo com a classificação de sites pelo Alexa: http://www.alexa.com/

Categorias de websites que contém links maliciosos

Ao passo que o malware se espalha por toda a Internet alguém poderia perguntar se existem áreas mais ou menos perigosas. Ao olhar para as categorias de conteúdo de websites nós realmente detectamos diferenças nos riscos.

- A única área de conteúdo mais arriscada da Internet está contida dentro de sites hospedeiros de pornografia. Esses sites foram responsáveis por cerca de 23% de todos os links maliciosos encontrados.
- Websites dinâmicos como blogs, onde os usuários podem contribuir com conteúdo através de artigos, comentários e mensagens são a segunda área mais perigosa da Internet. Os criminosos estão utilizando essas plataformas para colocar o malware e 16,5% de todos os links nocivos são encontrados nesses sites.
- Mesmo alguns sites em categorias razoavelmente seguras de websites "tradicionais", como por exemplo, páginas de portais e pessoais hospedam 8% e 5,7% respectivamente.
- Outra categoria importante são os sites de jogos de azar que hospedam 7,9% de todos os links maliciosos.
- 39% dos links maliciosos estão amplamente espalhados em outras categorias de conteúdo – nós listamos estes como "outros". É possível concluir com segurança que os links maliciosos e malwares estão ocultos em todos os lugares na Internet.

Principais categorias de website contendo pelo menos um link malicioso
Junho de 2013

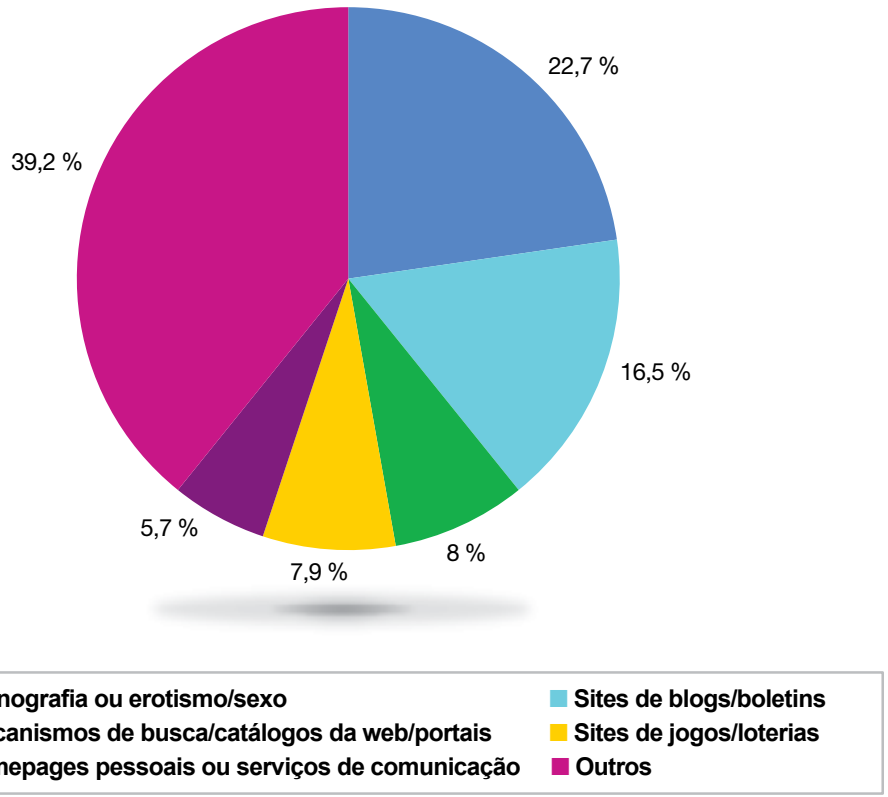


Figura 13: Principais categorias de website contendo pelo menos um link malicioso – Junho de 2013.

Distribuição geográfica de malwares e servidores C&C botnet

Este tópico discute os países onde links maliciosos estão hospedados e a distribuição geográfica do comando botnet e servidores de controle (C&C).

- Os Estados Unidos dominam o cenário ao hospedar mais de 42% de todos os links maliciosos.
- A geografia com a segunda maior concentração de links maliciosos é a Alemanha, com aproximadamente 10%.
- Os cinco países seguintes, nas posições 3 a 7, estão todos hospedando quantidades muito parecidas de links maliciosos: China, Rússia, Holanda, Reino Unido e França hospedam entre 5,9 a 3,4% de malware.

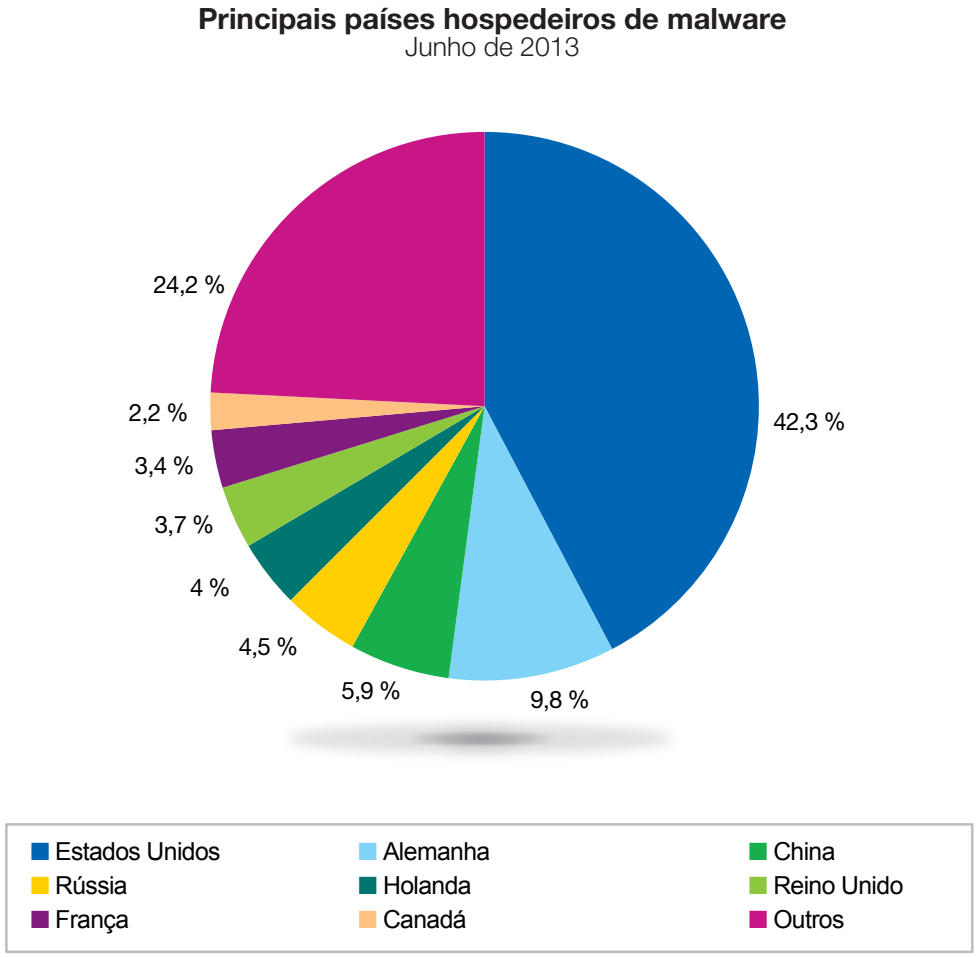


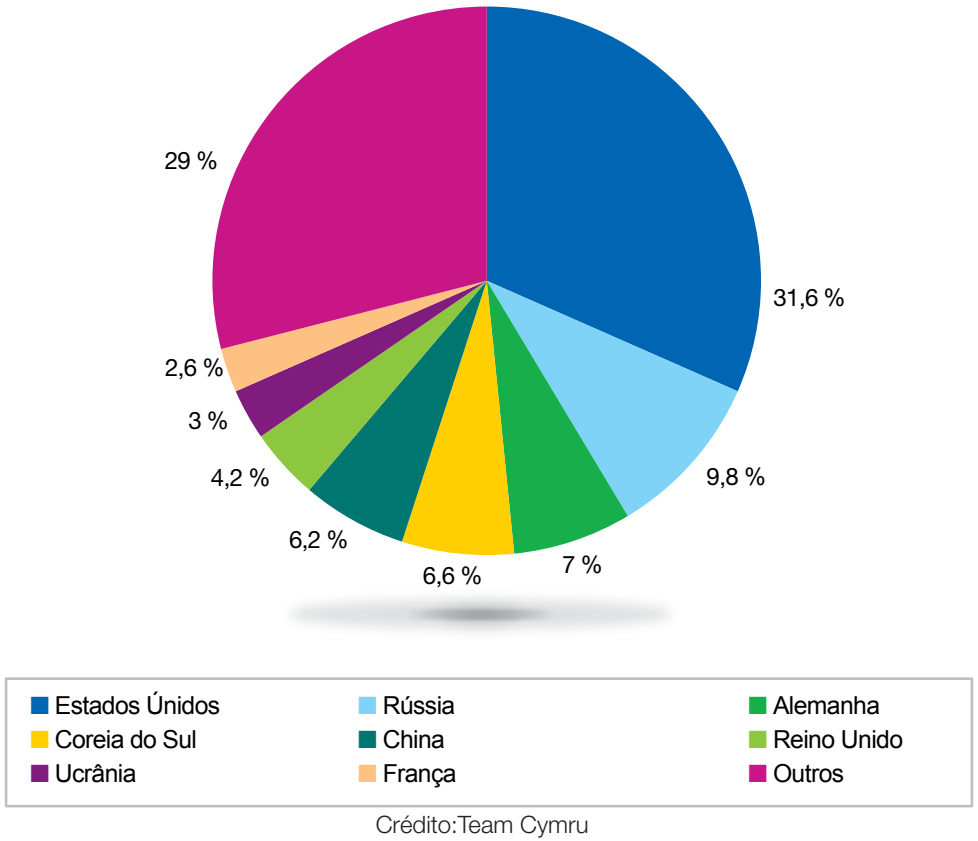
Figura 14: Principais países hospedeiros de malware – Junho de 2013.

Ao examinar a distribuição geográfica do comando botnet e servidores de controle (C&C) a fotografia é parecida.

- O país com maior número de servidores C&C com aproximadamente um terço de todos os servidores C&C são os Estados Unidos.
- O país com o segundo maior número de servidores C&C é a Rússia com aproximadamente 10%.
- Alemanha, Coreia do Sul, China e Reino Unido estão próximos, hospedando entre 7 a 4,2% dos servidores C&C.

Comando de botnet e servidor de controle
Servidores botnet C&C (command and control) são computadores que enviam comandos e recebem feedback de computadores que são parte da botnet (parasitas botnet). Botnets são utilizadas para tipos diferentes de ataque, como por exemplo, ataques DDoS (distributed-denial-of-service) e envio de emails de spam. Para iniciar tal ataque, o servidor C&C envia comandos especiais a seus parasitas para executar o ataque a um alvo específico (que falha por não ser capaz de lidar com tantos parasitas botnet) ou para enviar uma nova campanha de spam.[60]

Principais países hospedeiros de servidores botnet C&C
Junho de 2013



Crédito:Team Cymru

Figura 15: Principais países hospedeiros de servidores botnet C&C – Junho de 2013 – Crédito: Team Cymru.

60 Para mais detalhes consulte http://en.wikipedia.org/wiki/Botnet

Implementação IPv6 para websites

Para medir a implementação de IPv6 para websites, temos realizado solicitações DNS (que verificam por um registro AAAA no DNS) para milhões de hosts a cada semana. Ao passo que o IPv4 está ficando sem espaço, nós esperamos que mais e mais sites da Internet estejam migrando para o IPv6. Já focamos nossa análise nos 100.000 websites mais populares e mais utilizados[61] para ver como muitos deles já avançaram rumo ao mundo do IPv6.

- Nos 100 websites mais utilizados, 32% já são IPv6 – 10% a mais do que há seis meses.
- Cerca de 14% dos 1.000 sites principais já são IPv6 – 4% a mais do que há seis meses.
- Olhando para os 10.000 sites principais, quase 6% estão fornecendo IPv6 – 1,2% acima.

Em comparação com o status de seis meses atrás, os sites de Internet mais acessados já investiram na disponibilidade do IPv6.

Ao revisar a porcentagem de malware hospedado em endereços IPv6 nós encontramos somente 2,8% e para IPs de servidores botnet C&C somente 2% deles estão hospedados em IPs IPv6. Por enquanto, os malfeitores ainda parecem estar concentrados no mundo do IPv4 que oferece mais conectividade de todas as redes utilizando uma pequena porcentagem do espaço do IPv6 (até o momento) para recursos desprezíveis.

Sites prontos para IPv6 entre os sites principais mais utilizados
Dezembro de 2012 versus junho de 2013

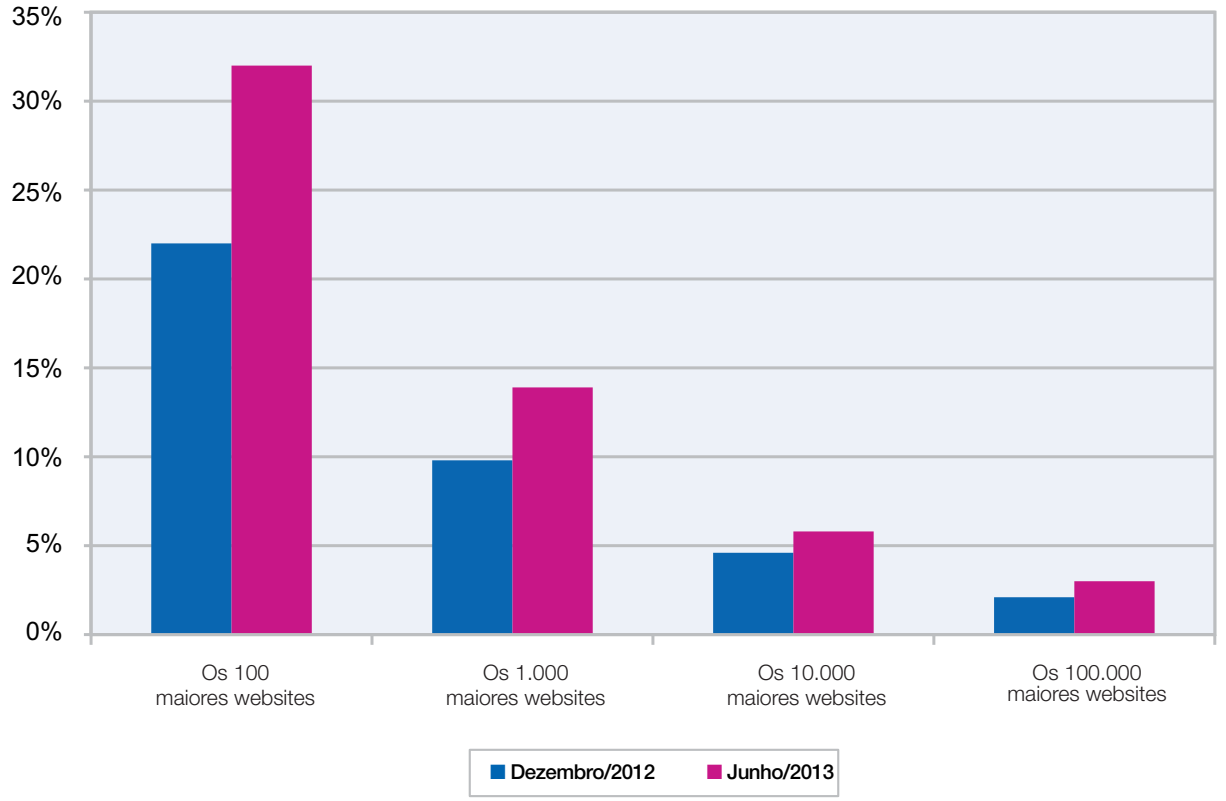


Figura 16: Sites prontos para IPv6 entre os sites principais mais utilizados – Dezembro de 2012 versus junho de 2013.

61 De acordo com a classificação de sites pelo Alexa: http://www.alexa.com/

Spam e phishing

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

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

Este tópico abrange os seguintes tópicos:

- Spam – tendências[62] do país de origem
- Alvos de scam/phishing por segmento de mercado

62 As estatísticas neste relatório para spam, phishing e URLs usam as informações do IP-to-Country provindos diretamente dos cinco Registros de Internet (ARIN, AfriNIC, APNIC, RipeNCC, LacNIC). A distribuição geográfica foi determinada por solicitação de endereços IP dos hosts (no caso de distribuição de conteúdo) ou do servidor de envio de email (no caso de spam e phishing) nestas informações de IP para país.

Spam – tendências do país de origem

Ao olhar para os países que enviaram a maioria dos spams nos últimos dois anos e meio, algumas tendências interessantes de longa data tornam-se visíveis.

- A Bielorússia é a nova estrela com spam, enviando 10% no segundo trimestre de 2013.
- No primeiro trimestre de 2013, e pela primeira vez em dois anos, os EUA continuaram na liderança por enviar 12%, mas então declinaram até cerca de 8% no segundo trimestre.
- No primeiro semestre de 2013, a Espanha ficou entre os três maiores pela primeira vez em anos.
- Enquanto a Índia dominou o cenário no final de 2012, e enviou mais de um quinto de todo o spam no terceiro trimestre de 2012, foi ultrapassada nos últimos seis meses pela Bielorússia, EUA e Espanha.
- Argentina e Itália alcançaram a quinta e a sexta posições pela primeira vez em anos.
- A Arábia Saudita não repetiu seu desempenho no terceiro trimestre de 2012 ao enviar spam e permanece inchada com cerca de 1%.

Origens de spam por trimestre

1T de 2011 até 2T de 2013

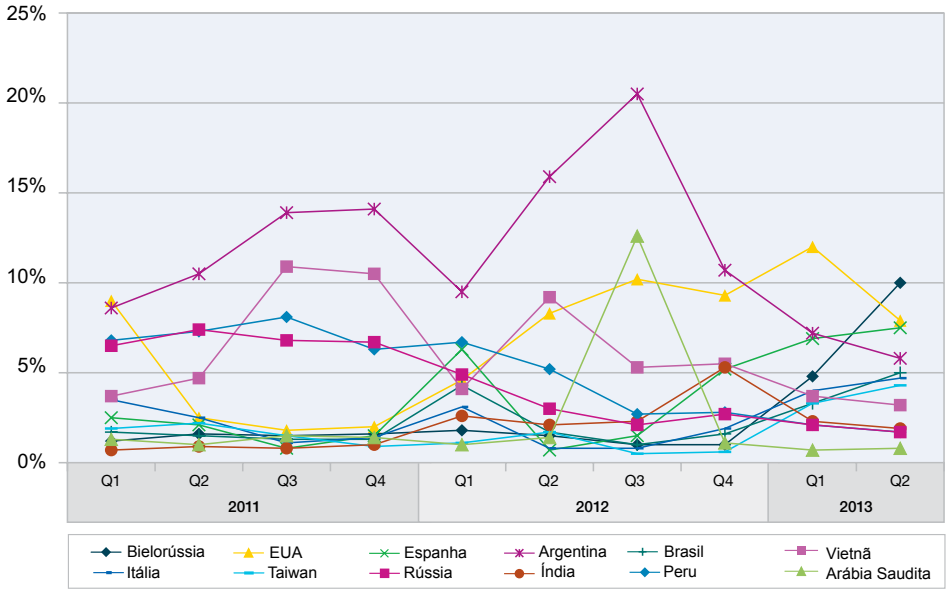


Figura 17: Origens de Spam por Trimestre – T1 2009 até T2 2011

Alvos de scam e phishing por área

Nesta seção revisaremos incidentes de scam e phishing relacionados a áreas específicas. As estatísticas são calculadas de acordo com as condições a seguir:

- As estatísticas são exclusivamente baseadas em campanhas de scam e phishing implementadas por email.
- As estatísticas incluem todos os emails que utilizam o nome de marcas bem conhecidas para fazer com que o usuários cliquem em um link ou anexo fornecido, mesmo se esse anexo ou link não estiver relacionado a phishing. Com isso, alguns dos emails incluídos são somente emails "estilo phishing".
- As estatísticas não incluem quaisquer tentativas de phishing não relacionadas a email; como por exemplo, acionamentos que registram malware de phishing que foi fornecido através de downloads drive-by.

Informações adicionais sobre a metodologia das estatísticas de scam e phishing fornecidas podem ser encontradas na seção correspondente do IBM X-Force 2011 Trend and Risk Report.

- As três maiores campanhas observadas que atraem o usuário para clicar em links ruins e anexos em emails são empresas de pagamento pela Internet, redes sociais e scanners internos ou dispositivos de fax. Juntas essas três áreas de destaque respondem por mais de 55% de todos os incidentes de scam e phishing.
- Nas posições quatro e cinco, existem emails "fingindo" ser de serviços de encomendas e de instituições financeiras. Essas duas áreas de destaque respondem por mais de 12,9% e 10,1% desses tipos de scams.

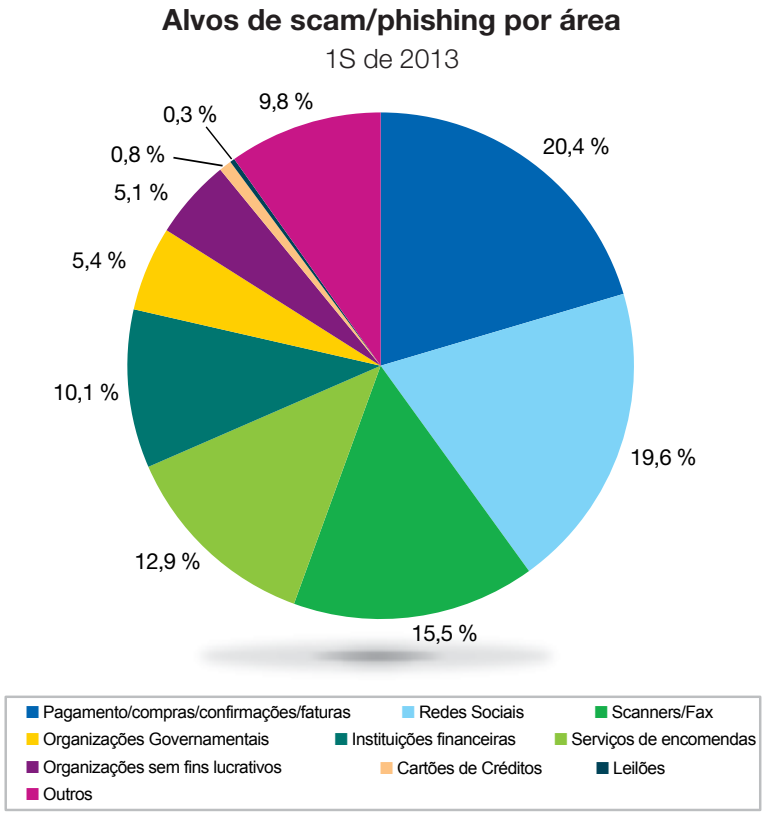


Figura 18: Alvos de scam/phishing por área – 1S de 2013.

- Ainda existe uma quantidade considerável de scams de email que se pensa virem de organizações do governo, como por exemplo, do FBI (Federal Bureau of Investigations dos EUA), ou de autoridades tributárias, ou organizações não governamentais; por exemplo, o BBB (Better Business Bureau).

Em comparação com o ano passado, não há grandes alterações relativas a esses tipos de spam, nem em marcas alvejadas nem tecnicamente dentro dos emails. Obviamente, do ponto de vista dos scammers, esta é uma abordagem bem estabelecida para fazer com que usuários – talvez novos – cliquem em links ou anexos. As técnicas a seguir funcionam bem para scammers:

- O espanto inicial de um usuário quando recebe um email que aparentemente veio das autoridades tributárias e o ameaça com um alto pagamento adicional de impostos.
- Funcionários que aguardam um fax, um scanner, uma confirmação de pedido, ou uma mensagem da rede social à qual se juntaram.

Práticas de segurança

O desafio de endereçar vulnerabilidades – reduzindo a superfície de ataque

Muitas equipes de segurança continuam a lutar com a administração da vulnerabilidade apesar de serem por muito tempo uma exigência principal das práticas de segurança de uma organização. O gerenciamento da vulnerabilidade auxilia as organizações a compreender plenamente a extensão de suas exposições bem como o estado geral de segurança de suas redes. A razão principal para este desafio é o grande número e taxas de surgimento de novas vulnerabilidades sendo introduzidas em seus ambientes por software de sistema operacional e aplicativos de terceiros. Isso é agravado pelo processo relativamente manual e lento de mitigar e corrigir essas fraquezas. Redes típicas deverão esperar ver, em média, algo entre 10 a 30 vulnerabilidades por endereço IP em seu ambiente. Algumas não terão e outras terão centenas, com os números mudando diariamente.

Esses números simplesmente comprometem muitas empresas de modo que elas se concentram na correção e proteção de servidores críticos ao negócio e naqueles com maior chance de serem atacados. Esses servidores incluem aqueles que controlam ou mantêm processos críticos para o negócio e dados, são acessíveis a partir da Internet ou de redes não confiáveis, ou aqueles que potencialmente abrigam ameaças desconhecidas. Ainda assim no ambiente de hoje onde o perímetro é muito mais poroso, isso não é adequado porque não protege contra ameaças internas, cavalos de Tróia, ou outras ameaças trazidas de fora devido ao comportamento de usuários em suas redes.

Para reduzir a probabilidade de ser explorado, o foco precisa se voltar para a redução de uma superfície potencial de ataque.[63] A superfície de ataque é representada por aquelas vulnerabilidades que são mais acessíveis a potenciais invasores. A acessibilidade da vulnerabilidade a atacar é definida primeiramente pelo contexto da rede na qual ela reside. Para tornar o gerenciamento da vulnerabilidade mais eficiente, técnicas que incorporam o contexto da rede no processo precisam ser aplicadas. Algumas técnicas eficientes estão listadas abaixo.

Entendendo o que é ativo e o que não é

A maioria das vulnerabilidades é detectada por rastreadores utilizando um processo chamado de rastreio autenticado. Isso envolve conectar-se a um usuário final, rastrear os softwares instalados, recuperar a versão específica e o nível de correção e então examinar as vulnerabilidades conhecidas daquela versão. O ponto chave nesse processo é que o rastreador de vulnerabilidade não sabe se aquele aplicativo vulnerável está ativo ou não naquele host. Claramente, aplicativos ativos oferecem potencial muito maior para um possível invasor do que os que estão inativos. Exemplos de software inativo que um rastreador de vulnerabilidade irá detectar incluem:

1. Internet Explorer instalado em servidores onde nunca é utilizado
2. Aplicativo da web e software de servidor instalados onde não estão ativos
3. Bancos de dados de aplicativos integrados não acessíveis remotamente

No clima atual de software autoinstalado e rápido download de softwares de testes por usuários finais, os administradores de rede podem esperar que até 60% dos aplicativos vulneráveis em suas redes estão inativos. Isto apresenta uma poderosa ferramenta para auxiliar a manter o foco nas vulnerabilidades e hosts que poderiam ser reparados primeiro.

Consciência de ameaça e conhecimento utilizado

Pode parecer óbvio, mas as vulnerabilidades não são um problema até que alguém ou alguma coisa tente explorá-las. Em muitas redes, a maioria dos pontos finais não se comunica com hosts maliciosos ou que poderiam ser potencialmente maliciosos. Ainda assim, existe um subgrupo de pontos finais que o fazem. Por exemplo, tome dois pontos finais que possuem o Internet Explorer instalado, ambos vulneráveis. Um navega na Internet dia sim dia não; o outro às vezes acessa o site da intranet local. Está claro que o primeiro, por causa de sua comunicação regular com uma potencial ameaça, possui uma superfície de ataque muito maior que o último. Claro que existem ameaças mais específicas na Internet e também pode haver ameaças, ou potenciais ameaças, dentro de uma corporação. Exemplos de potenciais ameaças incluem recursos que se comunicam com:

1. IPs maliciosos conhecidos e websites na Internet
2. Redes de parceiros não confiáveis e redes sem fio
3. Recursos que foram potencialmente comprometidos ou que se comportam de modo anormal
4. Recursos que foram usados por uma conta de usuário potencialmente comprometida
5. Recursos que possuem uma vulnerabilidade específica ou outra configuração fraca de segurança

Aplicar a inteligência em ameaça deste ambiente dinâmico no processo de gerenciamento de vulnerabilidade é uma ferramenta eficiente que as empresas podem utilizar para garantir que as vulnerabilidades com maior probabilidade de ser exploradas sejam mitigadas ou reparadas primeiro.

63 Controlling The Big 7 http://www.darkreading.com/vulnerability/controlling-the-big-7/240157835

Mitigações e reparos

Muitas empresas investem significativamente em defesas de perímetro como, por exemplo, firewalls, dispositivos IPS (intrusion prevention system), e sistemas de gerenciamento de pontos finais para aplicar automaticamente as últimas correções aprovadas em centenas e milhares de pontos finais. Esses investimentos em perímetro podem ser alavancados significativamente ao integrá-los mais de perto com o processo de gerenciamento de vulnerabilidades por compreender quais as vulnerabilidades que foram atualmente mitigadas da exploração por firewall e regras IPS, e quais ainda são um risco aberto. Essa é uma técnica eficiente para refinar o foco para um subgrupo de vulnerabilidades que provavelmente serão exploradas.

Além disso, possuir um sistema de gerenciamento de vulnerabilidades que seja capaz de fornecer um relatório claro sobre quais vulnerabilidades específicas possuem programação de correção por um sistema de "end-point" e quais não possuem, ajuda a garantir que esforços de reparos sejam direcionados mais eficientemente.

Na prática, habilitar o gerenciamento de vulnerabilidades com dados contextuais adicionais exigirá que seja integrado sem interrupções a um sistema de inteligência de segurança tanto com visão em tempo real como histórica da atividade da rede, incluindo com que o ambiente atual de ameaça se parece e qual o status dos controles atuais de segurança.

Para mais informações

Para saber mais sobre o software IBM X-Force, visite: **http://www-03.ibm.com/security/xforce/**

Inativos: Dados de fluxo de rede podem ajudar a identificar se aplicativos estão ativos

Bloqueado: Regras de firewall e IPS podem identificar quais vulnerabilidades estão expostas

Corrigidas: Integração com gerenciamento de correções irão revelar quais vulnerabilidades serão corrigidas

Exploradas: Integração com plataformas de ameaças podem alertar quando vulnerabilidades específicas são atacadas

Crítico: Base de conhecimento de vulnerabilidades, fluxo de reparos e políticas informam sobre vulnerabilidades críticas do negócio

Em risco: Dados de utilização e ameaças podem ser usados para identificar quais vulnerabilidades estão em risco

Técnicas para reduzir a superfície de ataque representada por vulnerabilidades

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

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

Informações neste documento relativas a produtos não IBM foram obtidas dos fornecedores destes produtos, de seus anúncios publicados ou outras fontes públicas disponíveis. Perguntas sobre os recursos de produtos não IBM devem ser dirigidas aos fornecedores destes produtos.

Este documento está vigente desde sua data inicial de publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países nos quais a IBM opera. Os exemplos de desempenho de dados e clientes citados são apenas para efeito ilustrativo. Os resultados reais de desempenho podem variar de acordo com configurações específicas e condições de operações. É de responsabilidade do usuário avaliar e verificar o funcionamento de qualquer produto ou programa com produtos e programas da IBM.

AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM QUALQUER GARANTIA, EXPLÍCITAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO-VIOLAÇÃO. Os produtos IBM são garantidos de acordo com os termos e condições dos acordos sob os quais foram fornecidos. O cliente é responsável por garantir a conformidade com as leis e regulamentos aplicáveis a ele. A IBM não fornece orientação ou representação legal ou garantia de que seus serviços ou produtos irão assegurar que o cliente esteja em conformidade com quaisquer leis ou regulamentos. Quaisquer instruções sobre a direção ou intenção futura da IBM estão sujeitas à alteração ou à retirada sem aviso prévio e somente representam as metas e objetivos.

O uso de dados, estudos e/ou materiais citados terceirizados não representa um endoso da IBM para a publicação da organização, nem necessariamente representa o ponto de vista da IBM.

O sistema de segurança de TI envolve a proteção de sistemas e informações através de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar na alteração, destruição, desapropriação ou uso indevido de informações, ou pode resultar em danos ou uso impróprio de seus sistemas, inclusive para utilização no ataque de terceiros. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto único, serviço ou medida de segurança pode ser totalmente eficaz na prevenção de acesso ou utilização incorreta. Os sistemas, produtos e serviços IBM foram projetados para fazer parte de uma abrangente abordagem de segurança, que necessariamente envolverá procedimentos operacionais adicionais e pode exigir que outros sistemas, produtos ou serviços se tornem mais efetivos. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES, OU TORNARÃO SUA EMPRESA IMUNE À CONDUTA ILEGAL OU MALICIOSA DE QUALQUER PARTE.

Por favor, recicle

WGL03036-BRPT-01