Relatório Semestral de Tendências e Riscos IBM X-Force 2013

Percepções de Segurança de CISO

Ao observar os métodos e as motivações dos incidentes de segurança da primeira metade de 2013, o IBM X-Force continua a constatar ataques operacionalmente sofisticados como o principal ponto de entrada.

– Pesquisa e Desenvolvimento IBM X-Force

Este documento examina alguns resultados do Relatório Semestral de Tendências e Riscos IBM X-Force 2013, os quais os CISOs (Chief Information Security Officers) e outros executivos de segurança podem utilizar para aprimorar as suas estratégias proativas de segurança.

Quantas vulnerabilidades a sua equipe de segurança encontrou ao executar as varreduras no último mês? Quantas eram de alto risco? Qual é a sua avaliação e abordagem? Resumimos os resultados da análise de ameaças apresentados pela equipe de Pesquisa e Desenvolvimento IBM X-Force.

Nos seis primeiros meses de 2013, o IBM X-Force:

- **Analisou 4.100 novas vulnerabilidades de segurança;**
- **Analisou 900 milhões de novas páginas e imagens da web;**
- **Criou 27 milhões de entradas novas ou atualizadas no banco de dados de filtragem da web IBM;**
- **Criou 180 milhões de assinaturas novas, atualizadas ou excluídas no banco de dados de filtragem de spam IBM.**

Alguns dos ataques operacionalmente sofisticados, no primeiro semestre de 2013, foram de oportunidades, em que aplicativos da web não testados e sem patch estavam vulneráveis à SQLi (SQL injection) ou à exploração XSS (cross-site scripting). Outros ataques ocorreram pela violação de confiança básica entre usuários finais e sites ou personalidades de mídia social que pareciam ser seguros e legítimos.

Com reportagens de violações de rede e perdas de dados marcando presença constante nos noticiários, não é nenhuma surpresa que 2013 está a caminho de ser outro ano recorde de ciberinvasões, mantendo a segurança como um tópico nas pautas das corporações e em repartições públicas. Os CISOs de hoje enfrentam adversários determinados e organizados, à medida que implementam novas iniciativas e esforçam-se para obter a melhor postura de segurança com base em riscos para as organizações.

Este documento examina alguns dos resultados apresentados no Relatório Semestral de Tendências e Riscos IBM X-Force 2013, os quais podem ser utilizados pelos CISOs para o aprimoramento das estratégias proativas de segurança. A discussão e orientação no relatório X-Force pode contribuir também para que se entendam as práticas de segurança que podem abordar esses riscos. As percepções apresentadas neste documento estão agrupadas dentro das seguintes áreas, em que o X-Force analisou as tendências em comportamentos de ataque:

- **Mídias Sociais:** Uma ferramenta para negócios, investigação e ataques
- **Malware de dispositivo móvel:** o crescimento excessivo de dispositivos Android atrai autores de malware.
- **Envenenamento watering hole:** comprometimento de um alvo estratégico central.
- **Distração e diversão:** invasores ampliam a negação de distribuição de serviços (DDoS) como uma brecha para violar outros sistemas.
- **Velhas técnicas, novos êxitos:** a complexidade de segurança permite a exploração de antigas falhas.

Percepções de "Mídias Sociais"

Uma tendência crescente é o roubo de perfis de mídias sociais que possuem um grande número de seguidores. As mídias sociais desempenham um papel central no modo como invasores estão atingindo seus alvos.

- **Solo fértil para captação de inteligência pré-ataque**
- **Mercado negro para contas de rede social**

As mídias sociais, devido a sua ampla difusão em ambientes pessoais e empresariais, se tornaram uma ferramenta corporativa valiosa para promover negócios e atrair novos talentos. Em vez de tentar bloquear o acesso às mídias sociais, as empresas devem pensar em como monitorar e reduzir os abusos dessas plataformas.

Na metade do ano de 2013, invasores continuam com foco voltado na exploração de relacionamentos de confiança por meio de redes sociais. De spam com aparência profissional a envio de links maliciosos que parecem ser de amigos, esses ataques são simples e eficientes para darem acesso às organizações que estão despreparadas. O relatório X-Force observa os diferentes modos como a influência social pode ser utilizada para detectar pessoas descuidadas que ainda causam danos no mundo off-line.

Em abril de 2013, uma "quebra repentina" da bolsa de valores dos EUA foi provocada quando a principal conta do Twitter de transmissão de notícias da Associated Press foi hackeada e os criminosos "tuítaram" "Notícias de última hora: Duas explosões na Casa Branca e Barack Obama está ferido."[1] O incidente sublinha a confiança que o público geral coloca na informação compartilhada em redes sociais.

As redes sociais oferecem mais do que um simples solo fértil para captação de inteligência de pré-ataque – elas podem ser utilizadas para criar e explorar ativamente redes confiáveis. Criminosos já estão vendendo contas em sites de redes sociais, algumas pertencentes a pessoas reais cujas credenciais foram comprometidas, outras fabricadas e elaboradas para parecerem confiáveis por meio de perfis realistas e uma rede de conexões. Uma função mínima utilizada é preencher as páginas de "Curtir" ou falsificar resenhas. Os usos mais insidiosos incluem esconder-se sob a identidade de alguém para praticar atividades criminosas – o equivalente on-line de uma carteira de identidade falsa, mas com amigos de testemunha – ou disseminar uma nova rede de conexões confiáveis.

É de se esperar que as aplicações de manipulação psicológica se tornem mais sofisticadas à medida que os invasores criem complexas interligações de redes de identidades, de modo a refinar a arte de ludibriar as vítimas. Os controles da tecnologia estão em ordem, mas frequentemente estão ou desabilitados ou são driblados pela rede estendida do usuário. A única defesa efetiva é a educação e levantar suspeitas.

Percepções de "Malware de Dispositivo Móvel"

O crescimento excessivo de dispositivos Android está incitando invasores a explorar essa grande base de usuários com malware tecnicamente sofisticado.

- **Obad – o mais sofisticado Android Trojan**

Dispositivos móveis são um alvo lucrativo para autores de malware. Com uma remessa de 470 milhões de dispositivos Android só em 2012,[2] os invasores de alerta respondem com um crescimento correspondente em malware de Android. A maioria dessas explorações é dirigida especificamente para aplicativos móveis e são primariamente divulgadas em repositórios públicos populares de exploração.

O ano de 2013 testemunhou o lançamento de um Trojan chamado Obad, que é notável por apresentar alguns recursos novos e tecnicamente sofisticados. O X-Force acredita que esse lançamento é importante no sentido de que revela como os autores de malware estão agora redobrando os esforços agora para criar malware de Android cada vez mais perigoso e resiliente.

O Obad foi difundido principalmente por meio de spam SMS (short message service) e ganhou atenção em junho de 2013 quando foi denominado de "O mais sofisticado Android Trojan."[3] Já vimos antes a funcionalidade central do Obad – tal como roubo de informações e envio SMS premium – em outro malware de Android, mas os recursos que o fazem se destacar incluem: difusão por meio de Bluetooth, administração de dispositivo, técnicas de antianálise e ofuscação de código.

A versão mais recente do software Android, a 4.2, oferece várias melhorias de segurança – verificação de aplicativos, exibição aperfeiçoada de permissões e notificação de envio de SMS premium – que poderiam reduzir a probabilidade de infecção ou, pelo menos, minimizar o impacto depois de infectado. Porém, atualmente, menos de 6% de todos os dispositivos Android utilizam essa versão mais recente.[4] O X-Force recomenda aos usuários de Android verificar se uma atualização de firmware está disponível e considerar realizar um upgrade. Os CISOs deveriam também rever as políticas de segurança BYOD (Bring Your Own Device) e a avaliação de riscos de quais dispositivos e perfis possuem permissão de acesso.

Percepções de "Envenenamento Watering Hole"

Vários programas de explorações de "dia-zero" foram iniciados por meio de um website comprometido, o que nos faz acreditar ser parte de uma campanha watering hole.

O comprometimento de um alvo estratégico central – tal como um website de interesse especial que é muito frequentado por um grupo seleto de alvos potenciais – é um meio eficiente e otimizado para distribuir um programa de exploração. Tais alvos centrais, geralmente, não possuem uma segurança forte; e mesmo se a tivessem, o custo para descobrir como passar por eles vale a oportunidade de alterar e comprometer a base de usuários.

Esses ataques "watering hole" são um grande exemplo de como a sofisticação operacional está sendo utilizada para atingir alvos antes não suscetíveis. Ao comprometer o site central e utilizá-lo para servir ao malware, invasores são capazes de atingir, tecnicamente, mais vítimas experientes, que não poderiam ser enganadas em tentativas de phishing, mas não suspeitam que os sites em que confiam podem ser maliciosos.

No início de 2013, as campanhas "watering hole" foram popularizadas quando várias empresas de alto nível, tais como a Apple[5] e o Facebook[6] relataram que alguns de seus funcionários foram atacados por meio de um website de desenvolvedor comprometido. Outras empresas de alta tecnologia e alguns funcionários do governo foram também violados com êxito com esta técnica.

O Relatório Semestral de Tendências e Riscos IBM X-Force 2013 fornece orientações de como os administradores de website podem contribuir para reduzir o risco de um website ser comprometido por um ataque de "watering hole", incluindo: Reforço dos servidores, garantia de circulação de aplicativos de software e web e reforço das máquinas de clientes utilizadas para efetuar logon nos servidores.

Percepções de "Distração e Diversão"

Locais remotos e sites com idioma local podem ser o lado mais frágil para a organização.

- **Taxas de tráfego de DDoS superiores a 300 Gbps**[7]

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. Invasores têm demonstrado sofisticação técnica incrementada na área de DDoS. Isso inclui novas técnicas de evasão de redução de DDoS e o uso de métodos de largura de banda com capacidade de aumento, como um novo e poderoso modo de estagnar negócios ao interromper serviços on-line.

O surgimento de uma tendência interessante em alvos de DDoS se desenvolve desde junho, em que muitos provedores DNS (Domain Name System) relataram interrupções de serviços e tempo de inatividade. Resolvedores de DNS aberto, que servem a um propósito legítimo, podem também permitir a invasores a ampliação de ataques de DDoS, de modo a criar um surto enorme de tráfego direcionado a um único alvo. Diversos provedores DNS de destaque foram atingidos off-line[8], enquanto serviam de cúmplices em ataques de DDoS de grande escala. Ataques em provedores de DNS são outro exemplo de alvos estratégicos centrais comprometidos para atingir um grande grupo de vítimas potenciais.

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. Esses sites satélites não são sempre seguros com os mesmos padrões da matriz. Ao ir atrás de um ponto fraco de entrada em grandes empresas, os invasores foram capazes de alcançar e denegrir marcas bem conhecidas. Isso pode resultar em um golpe reputacional, bem como em implicações legais, devido ao vazamento de dados confidenciais de clientes. Esses tipos de vazamento afetaram a indústria de alimentos, de eletrônicos de consumo, automotivas e em particular as de entretenimento.

Como o escopo e a frequência de violações de dados continuam em uma trajetória ascendente, retornar aos fundamentos básicos de segurança é essencial. Por todo o Relatório Semestral de Tendências e Riscos IBM X-Force 2013, observamos muitas faces de computação segura, tanto da perspectiva de administração de rede, quanto de TI, assim como para usuários finais. Enquanto a redução técnica é uma necessidade, condicionar usuários em toda a corporação para ver a segurança como uma cultura – não uma exceção – pode ser o caminho para a redução desses incidentes.

Percepções de "Velhas Técnicas, Novos Êxitos"

Vulnerabilidades conhecidas deixadas sem correção em aplicativos e softwares criam oportunidades para a ocorrência de ataques, tanto que foram verificadas, no último ano, pontos de entrada em várias violações.

Consequências da exploração:

- **Obtenção de Acesso – 28%**
- **XSS – 18%**

As vulnerabilidades de aplicativos da web, tal como o CMS (Content Management Systems), continuam a totalizar a maioria daquelas que a equipe X-Force relata. No primeiro semestre de 2013, 31% das vulnerabilidades relatadas publicamente foram classificadas pela equipe X-Force como aplicativos utilizados na web, e mais da metade de todas as vulnerabilidades de aplicativos da web eram XSS (Cross site script).

A consequência mais comum de exploração de vulnerabilidades foi a "Obtenção de Acesso", que registrou 28% de todas as vulnerabilidades relatadas. Na maioria dos casos, obter acesso a um sistema ou a um aplicativo proporciona aos invasores o controle total sobre o sistema afetado – o que permitiria roubar dados, manipular o sistema ou iniciar outros ataques a partir de tal sistema. Com 18%, o XSS foi a segunda consequência mais comum e envolvia, tipicamente, ataques contra aplicativos da web.

No primeiro semestre de 2013, o X-Force emitiu 14 alertas e avisos em divulgações que mereceram muita atenção. Sete desses alertas/avisos, constituídos completamente de Internet Explorer e Java, eram vulnerabilidades com impacto de alto potencial e com baixo custo de desenvolvimento para invasores. Essas vulnerabilidades podem ser todas utilizadas em ataques de exploração feitos às pressas para atingir muitas vítimas potenciais em diferentes sistemas operacionais e navegadores.

A reutilização de senha é ainda excessiva, permitindo que os invasores tomem o comando de contas em vários sites. Apesar dos compromissos bem conhecidos dos serviços da web, incluindo alguns sites de rede social, os usuários, em geral, ainda utilizam a mesma senha em muitas de suas contas. Além disso, muitos confiam no mecanismo de recuperação de senha de email – uma vez que a conta da vítima estiver comprometida, não há solução.

Então, por que essas técnicas de ataque mais antigas ainda são por diversas vezes bem-sucedidas? A complexidade da segurança pode abrir antigas falhas que podem ser exploradas. Algumas dessas falhas poderiam ser evitadas pela manutenção consistente e de alto nível da correção, tanto em terminais, como em servidores. Outra medida preventiva é manter os sistemas operacionais e softwares nas versões mais atuais. E até mesmo a melhor execução prática de políticas de segurança, tais como reforçar a utilização de senhas fortes, por meio de senhas diferentes para contas diferentes e possibilitar a autenticação forte (duplo fator de autenticação) pode ajudar.

Resumo

Uma abordagem de segurança preventiva requer pesquisa líder de segmento de mercado, olho clínico para tendências e técnicas de ataque e a habilidade para processar e agir de acordo com essa inteligência de ameaças. Já que a equipe de desenvolvimento e pesquisa X-Force coleta, correlaciona e analisa informações de ameaças a partir de milhares de clientes ao redor do mundo, é possível identificar novas ameaças com antecedência. As organizações podem alavancar esses dados para ajudar a prevenir incidentes de segurança e/ou minimizar o impacto dos ataques de segurança.

Agora, mais do que nunca, os CISOs (Chief Information Security Officers) precisam manter um conhecimento maior do cenário de ataques e de vulnerabilidades, dentro de um contexto global de segurança, para, efetivamente, combater o rápido crescimento destes ataques. Como as organizações implementam novas iniciativas e esforçam-se para obter a melhor postura de segurança com base em riscos, uma abordagem integrada e holística para a segurança de TI deveria ser a estratégia central. Isso permite aos gerentes de segurança compreender os padrões de comportamento normal, identificar anormalidades emergentes e resolver rapidamente ameaças, antes que ocorra um prejuízo real.

Faça o download completo do Relatório Semestral de Tendências e Riscos IBM X-Force 2013 para obter informações que podem ajudá-lo a incrementar a sua estratégia de segurança proativa e a compreender as práticas de segurança, de modo a contribuir com a resolução dessas ameaças emergentes.

Sobre o IBM X-Force

O IBM X-Force Research and Development é uma das equipes de pesquisa e desenvolvimento de segurança comercial mais conhecidas do mundo. Esses profissionais de segurança monitoram e analisam os dados de uma variedade de fontes, incluindo o banco de dados de mais de 73.000 vulnerabilidades de segurança computacional, um crawler(motores de busca na internet) da web global e coletores internacionais de spam. Os Centros de Operações de Segurança (SOC) global da IBM fornecem monitoramento em tempo real de 15 bilhões de eventos, diariamente, para aproximadamente 4.000 clientes em mais de 130 países.

Para mais informações

Para mais informações sobre o IBM Security, visite: **ibm.com**/security e participe do debate no CISO Corner em securityintelligence.com/ciso/

Este documento pretende servir como um sumário executivo do "IBM X-Force 2013 Mid-Year Trend and Risk Report" completo publicado pela IBM. O relatório completo pode ser acessado no endereço: http://ibm.co/xforce2013

[1] http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

[2] http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017

[3] http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

[4] http://developer.android.com/about/dashboards/index.html

[5] http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219

[6] https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766

[7] http://www.informationweek.com/security/attacks/spamhaus-ddos-suspect-arrested/240153788

[8] http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html

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

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

Esse documento está vigente desde sua data inicial de publicação e pode ser alterado pela IBM a qualquer momento.

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.

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.

Declaração de Práticas Adequadas de Segurança: O sistema de segurança de TI envolve a proteção de sistemas e informações por meio de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar na alteração, destruição ou desapropriação de informações, ou pode resultar em danos ou uso impróprio de seus sistemas, inclusive para atacar terceiros. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto único ou medida de segurança pode ser totalmente eficaz na prevenção de acesso incorreto. Os sistemas e produtos 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 os sistemas e produtos sejam imunes à conduta ilegal ou maliciosa de qualquer parte.

Por favor, recicle

WGE03021-BRPT-00