Junho de 2014

Relatório Trimestral de Inteligência contra Ameaças da IBM X-Force, 2º Trim. de 2014

Descubra como vulnerabilidades em aplicativos, ameaças de spams e respostas a incidentes estão evoluindo — com base nos dados mais recentes e em análises contínuas

IBM

Índice

Visão geral executiva

A equipe de pesquisa e desenvolvimento do IBM® X-Force®, juntamente com colegas da divisão IBM Global Technology Services®, vem há algum tempo analisando as ondas de ameaças mais recentes e sente-se entusiasmada em compartilhar suas últimas descobertas. Iniciamos o ano de 2014 discutindo as muitas violações e incidentes de segurança que continuam desafiando as organizações. Neste segundo relatório trimestral de 2014, focamos nossa atenção no ressurgimento de métodos que obtiveram sucesso no passado e em questões praticamente recentes a serem consideradas no atual cenário de segurança.

Primeiramente, vamos analisar as antigas ameaças. Ao longo do tempo, inúmeras ameaças surgiram, substituindo ameaças anteriores. Vírus famosos disseminados por e-mail, como o ILOVEYOU, evoluíram para traiçoeiras instalações de malware embutidas em downloads que furtivamente coletam dados sigilosos de usuários. A invasão de sites com o único objetivo de violar direitos por motivos de vanglória transformou-se em uma distração para atividades mais mal-intencionadas contra servidores e bancos de dados. Além disso, worms, como Blaster e Storm, lançaram as bases para o que há de mais moderno em ataques distribuídos de negação de serviço (DDoS).

O que podemos aprender com esse histórico de ameaças na Internet, e o que mudou? Desde que se começou a escrever aplicativos de software, sempre houve aplicativos vulneráveis. Se o programador escreve um software e comente erros, os aplicativos se tornam vulneráveis. Neste relatório, analisaremos cuidadosamente os aplicativos vulneráveis de sites da Web e veremos como ainda representam um sério vetor de ameaças para invasores interessados em prejudicar organizações ou roubar dados sigilosos.

A varredura de aplicativos pode ajudar a proteger os componentes mais críticos direcionados ao usuário dos serviços e aplicativos da Web, analisando tanto o código do aplicativos personalizados, quanto componentes de terceiros. Ainda assim, os clientes devem estar atentos à segurança do próprio servidor da Web. Tecnologias vulneráveis que englobam o backbone de uma pilha de aplicativos da Web são capazes de deixar todo o ambiente em perigo.

Em abril de 2014, uma vulnerabilidade (CVE-2014-0160) no amplamente conhecido e usado software OpenSSL deixou um enorme percentual de sites sob risco de vazamento de dados e de informações privadas e críticas. A correção em si não foi difícil de aplicar, mas a redução dos possíveis danos causados por violações de credenciais do usuário, certificados SSL e outras informações sigilosas tornou o processo de limpeza um desafio. Quando vulnerabilidades críticas são divulgadas ou ocorrem incidentes, temos de aprender a "esperar o inesperado". Se a resposta ao incidente se basear em um planejamento para situações conhecidas, então a situação é de perda. O conteúdo da memória de acesso aleatório (RAM) é tão suscetível quanto os dados armazenados em disco.

Apresentaremos algumas recomendações direcionadas às organizações que queiram melhorar essa importante área da segurança.

Para obter mais informações sobre Heartbleed (a vulnerabilidade de pulsação no protocolo TLS do OpenSSL), consulte a última postagem no blog do IBM Security Intelligence.[1]

Na próxima seção do relatório, analisaremos como os spams (uma das mais antigas e duradouras ameaças à segurança) continuam mais vivos do que nunca. A maioria das organizações dispõe de controles adequados para combater o ataque de spams, porém os invasores ainda os utilizam com o intuito de obstruir servidores de e-mail e, às vezes, espalhar conteúdo malicioso a usuários ingênuos. A equipe de segurança de conteúdo do IBM X-Force continua monitorando a evolução do spam e como essa ameaça continua sendo um canal principal de infiltração de malware em redes corporativas. Em março de 2014, testemunhamos o retorno dos mais altos níveis de spam apurados durante os últimos dois anos e meio.

Analisamos também os dados de rastreamento de infecções causadas por robôs em spam e sua relação com o fim (hoje) do suporte ao Microsoft Windows XP.

Por fim, concluiremos o relatório com uma categoria ligeiramente nova de ameças à segurança. Com a ajuda da equipe de Serviços de Respostas a Emergências (ERS) da IBM Global Technology Services, compartilharemos as lições aprendidas quando a resposta a incidentes remotos se torna extremamente remota. Visto que as organizações em todo o mundo estão ampliando a sua penetração nos países em desenvolvimento e nas infraestruturas recém-criadas, o que acontece quando ocorre um incidente em uma área com comunicações e largura de banda limitadas? Como os especialistas poderão agir com rapidez transferindo seus dados críticos? Explicaremos como a resposta a incidentes em países remotos ou áreas carentes de infraestrutura requer um plano de ação exclusivo.

Aplicativos vulneráveis como um sério vetor de ameaças

De vulnerabilidades de injeção a violações de autenticação, descubra quais ameaças podem estar à espreita de seus aplicativos dinâmicos da Web.

Os invasores procuram alguma forma de explorar dados corporativos sigilosos e valiosos. Geralmente, o caminho mais rápido para invadir os sistemas internos de uma empresa são as vulnerabilidades, como SQLi (SQL injection) e autenticações violadas. Se não fizerem testes em seus sites e nos aplicativos que os acessam, as empresas correrão o risco de expor ativos valiosos.

No universo dos aplicativos móveis, por exemplo, os pesquisadores da IBM descobriram recentemente uma série de vulnerabilidades no Mozilla Firefox para Google Android que permitiram a aplicativos mal-intencionados provocar o vazamento de informações sigilosas sobre perfis de usuários[2] . Um invasor disfarçado pode explorar essas vulnerabilidades para extrair informações, como cookies e dados gravados em cache na forma de históricos do navegador e IDs do usuário.

Outra vulnerabilidade móvel descoberta pelos pesquisadores da IBM é a injeção de fragmentos na estrutura do Android, que afetou diversos aplicativos populares, como Google Now, Gmail, Dropbox e Evernote[3]. Os invasores que exploram essas vulnerabilidades conseguiram acessar informações sigilosas pertencentes ao aplicativo vulnerável violando a área de segurança do Android.

Aplicativos da Web são outro alvo atraente para invasores disfarçados, pois estes normalmente obtêm acesso a dados corporativos de alto valor armazenados internamente. A exploração de vulnerabilidades por injeção, como o SQLi, pode induzir à manipulação de bancos de dados de back-end protegidos. Além disso, quando dados em trânsito de e para um aplicativo da Web deixam de ser protegidos, o resultado pode ser vazamentos de dados de credenciais do usuário, dados de cartões de crédito e comunicações privadas.

Quais são as dez maiores ameaças a aplicativos da Web?

Em 2013, o Top 10 do Open Web Application Security Project (OWASP) identificou uma lista dos dez riscos mais críticos à segurança dos aplicativos da Web. Como mostra a Figura 1, os ataques por injeção, a violação de autenticações e do gerenciamento de sessões e o cross-site scripting lideram a lista.[4]

Nas próximas seções, analisaremos mais profundamente a pesquisa sobre ameaças a aplicativos da Web realizada pela equipe IBM responsável pelo gerenciamento de testes em aplicativos hospedados.

Dados de ameaças a aplicativos da Web

O serviço Hosted Application Security Management (HASM) da IBM é uma solução baseada na nuvem para testes de aplicativos dinâmicos da Web utilizando o IBM Security AppScan® em ambientes de pré-produção e produção. Os serviços HASM incluem um analista de segurança dedicado para configurar e gerenciar os testes.

Neste relatório, a equipe de HASM coletou dados de ameaças de mais de 900 varreduras de aplicativos dinâmicos da Web realizadas em 2013. Alguns pontos principais relacionados a esses dados são:

- O conjunto de dados consiste em aplicativos de uma ampla variedade de setores de mercado, incluindo governos, serviços financeiros, setor industrial, farmacêutico, varejista e de telecomunicações.
- A maioria das varreduras é realizada por organizações que utilizam o serviço HASM há mais de cinco anos. Essas organizações dispõem de práticas de segurança maduras e bem definidas, ou seja, os aplicativos verificados normalmente apresentam um número menor de vulnerabilidades que o verificado nas organizações com pouca experiência em aplicativos da Web.
- Apesar da execução de varreduras regulares nos aplicativos da Web dessas organizações, vulnerabilidades são detectadas constantemente, quase sempre introduzidas por alterações em códigos ou implantações de novos aplicativos. É por esse motivo que os aplicativos devem ser verificados novamente após a implantação de uma nova funcionalidade, bem como após atualizações e aplicações de correções no código.
- A maioria dos problemas encontrados está relacionada à falta de validação e limpeza adequadas de entradas de dados.

2013: O ano da ameaça da autenticação violada

A figura 1 mostra que as ameaças XSS (cross-site scripting) e CSRF (cross-site request forgery) ainda são bastante predominantes em aplicativos da Web. Os ataques por injeção, embora menos frequentes neste conjunto de amostras de clientes, ainda são bem comuns e perigosos, pois diretamente dão acesso a dados internos sigilosos aos invasores difarçados. Contudo, visto que essas vulnerabilidades são bem conhecidas, iremos analisar mais detalhadamente outro problema predominante: autenticação violada.

A autenticação violada pode ser o resultado da falha em proteger as credenciais de ID do usuário e senha ou da falha em gerenciar adequadamente os IDs de sessão. Sem a devida proteção das informações de autenticação, o invasor pode apoderar-se de sessões do usuário e fazer-se passar por ele. Por exemplo, um invasor disfarçado é capaz de explorar essa vulnerabilidade para controlar sessões de Internet banking e transferir fundos como se fosse o legítimo usuário.

Os dados do HASM evidenciam que um dos problemas mais comuns de autenticação violada identificados nas varreduras autenticadas é do tipo "ID de sessão não atualizado durante o login". Esse teste em particular executa verificações para garantir que o valor do cookie de sessão tenha sido atualizado durante a sequência de login, isto é, após o usuário clicar no botão de envio na página de login. Se o ID de sessão (SID) não for atualizado no login, o aplicativo da Web poderá ficar vulnerável a ataques de fixação de sessão. Em ataques de fixação de sessão, se os invasores conseguirem acesso a um SID válido, eles poderão usar o ID para burlar o processo de login e acessar a conta da vítima. O ataque pode funcionar com SIDs gerados pelo usuário ou pelo servidor.

Com frequência, os aplicativos Microsoft ASP.NET encontram-se em situação de risco de ataques de fixação de sessão, pois, normalmente, o valor do cookie JSESSION é gerado na página de login antes de o usuário concluir o acesso, e, por padrão, ele não é atualizado durante o processo de login.

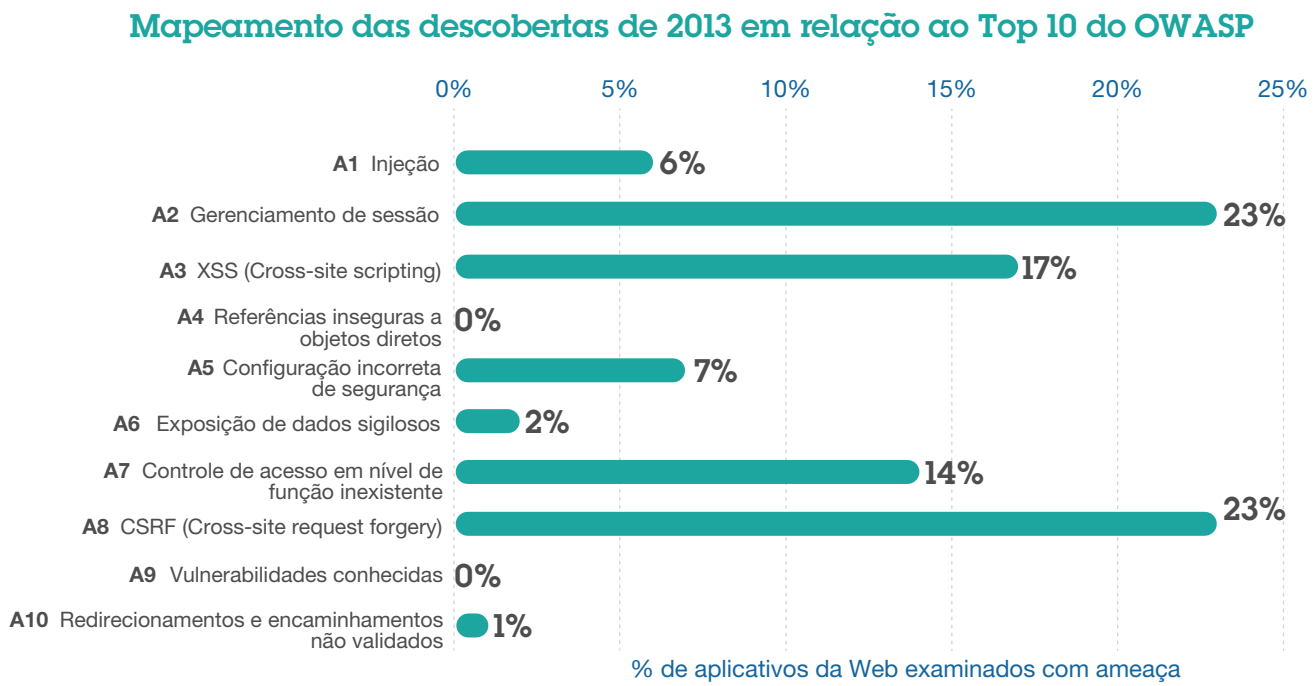


Figura 1. Constatação de vulnerabilidades comuns ocorridas em aplicativos da Web testados pelo serviço Hosted Application Security Management (HASM) da IBM em comparação ao Top 10 do OWASP de 2013.

Fixação de sessão e uso indevido de IDs são vulnerabilidades comuns. Descobrimos também que este problema em particular não é bem compreendido e normalmente requer algumas interações para que os desenvolvedores entendam o problema e a violação possa ser devidamente corrigida.

Com o intuito de ajudar a melhorar os testes de aplicativos para detecção e correção iniciais das vulnerabilidades de autenticação baseada em sessão, a IBM recomenda:

1. Atualizar o SID no login.
2. Impingir um tempo limite ao SDI para forçar o encerramento após o logout ou um período de inatividade.
3. Disponibilizar interfaces de programação de aplicativo (APIs) ou bibliotecas de funções de autenticação.

Tendências em testes de segurança de aplicativos

Da mesma forma como aumenta o cuidado com a segurança de aplicativos, também cresce a tendência de organizações investirem na varredura de aplicativos da Web.

As organizações desenvolvem uma linha de base dos riscos relacionados aos seus aplicativos da Web adicionando varreduras regulares desses aplicativos nos ambientes de pré-produção ou de produção.

Tradicionalmente, clientes HASM têm demonstrado um maior interesse em verificar seus aplicativos antes da implantação. Porém, no último ano, observamos um aumento distinto nas organizações que desejam executar varreduras contínuas em grande escala nos seus sites ativos.

Para facilitar essas iniciativas de varredura em grande escala dos aplicativos ativos, as organizações precisam montar um inventário de todos os aplicativos da Web que utilizam métodos automatizados de descoberta de aplicativos. As equipes de segurança de TI sentem cada vez mais dificuldade em rastrear ou localizar todos os aplicativos da Web sob seu controle. É comum às organizações subestimar o número dos seus aplicativos da Web em até 50%. E, se não sabem da existência de determinado aplicativo em execução, pode-se arriscar a dizer que não o examinam em busca de vulnerabilidades de segurança.

Contudo, os invasores estão à procura de vulnerabilidades. Por essa razão, a execução regular de varreduras e atualizações das informações sobre o inventário de aplicativos é fundamental.

Visto que a varredura de aplicativos da Web requer um conjunto específico de habilidades, investimentos significativos em software e talvez em infraestrutura adicional, muitas organizações estão utilizando modelos terceirizados. Pode ser dispendioso e moroso criar equipes internas com habilidades profundas em testes de segurança de aplicativos. Dessa forma, a terceirização do trabalho permite às organizações entrarem em pleno funcionamento rapidamente, com um ponto de preço baixo. Além do tempo mais rápido de inicialização, os fornecedores de testes possuem vasto conhecimento e experiência em segurança. Eles podem, igualmente, disponibilizar manutenção contínua para o software de varredura e a infraestrutura necessária.

Dicas para varredura segura da produção

Ao empregar varreduras terceirizadas, é importante compreender a natureza do exame que está sendo executado. Converse com a equipe de testes para entender como estão sendo configuradas as varreduras, o que está sendo testado, se algo não está sendo testado e que cobertura está sendo alcançada. Por fim, pergunte se há algum risco ou imprevisto. Este último ponto é particularmente importante, pois os aplicativos de teste em produção podem provocar indisponibilidade de serviço. Ao avaliar fornecedores, certifique-se de compreender sua abordagem para varredura da produção e a abrangência do teste.

Verificações de produção

Se o fornecedor recomendar a execução de varreduras da produção, há alguns pontos a serem considerados. Os sites com conteúdo estático causam menos preocupação; porém, para os aplicativos que coletam dados e os salvam nos bancos de dados de back-end ou alimentam outros sistemas de back-end com esses dados, é importante compreender como o fornecedor irá testar essas áreas. Há duas abordagens principais à varredura da produção:

1. Teste de formulário completo — Nesta abordagem, todos os formulários do aplicativo são testados. Embora a abordagem proporcione boa cobertura a capture todos os principais problemas, há inúmeros riscos:

- Quando os dados são enviados ao banco de dados por meio de formulários, os testes podem gerar um grande volume de dados relacionados a serem inseridos nos sistemas e bancos de dados de back-end. Por exemplo, formulários com 10 preenchimentos podem ser enviados mais de 1.000 vezes.

- Alguns formulários são usados para enviar e-mails diretamente ou vincular outros sistemas de back-end geradores de e-mails. Novamente, se esses formulários forem testados, milhares de e-mails poderão ser gerados.
- Embora rara, existe a possibilidade de as varreduras provocarem falha total dos aplicativos ou sistema de back-end. Mesmo se não falharem, os dados de testes inseridos podem provocar falhas no processamento de back-end.
- A verificação de segurança de aplicativos da Web às vezes gera grandes volumes de tráfego http(s) e provoca problemas de largura de banda ou de desempenho com que afetam diretamente os usuários.

2. **Sem arquivos de formulário ou arquivos de formulário seletivos** — Nesta abordagem, não há nenhum preenchimento de formulário, ou apenas mínimo, o que pode ajudar a prevenir os possíveis problemas dos testes de formulário completo. Contudo, este tipo de teste é menos rigoroso e pode resultar em falhas de segurança. Formulários são normalmente as áreas do aplicativo onde se concentram diversos problemas críticos, a maioria provocada por validação de entrada inadequada. Ao deixarem de testar todos os formulários, as organizações correm o risco de ignorar esses problemas importantes.

A Figura 2 ilustra a ideia de que, quando a varredura da produção é executada de forma a reduzir os possíveis problemas dos testes de formulário completo, poucas vulnerabilidades são encontradas.

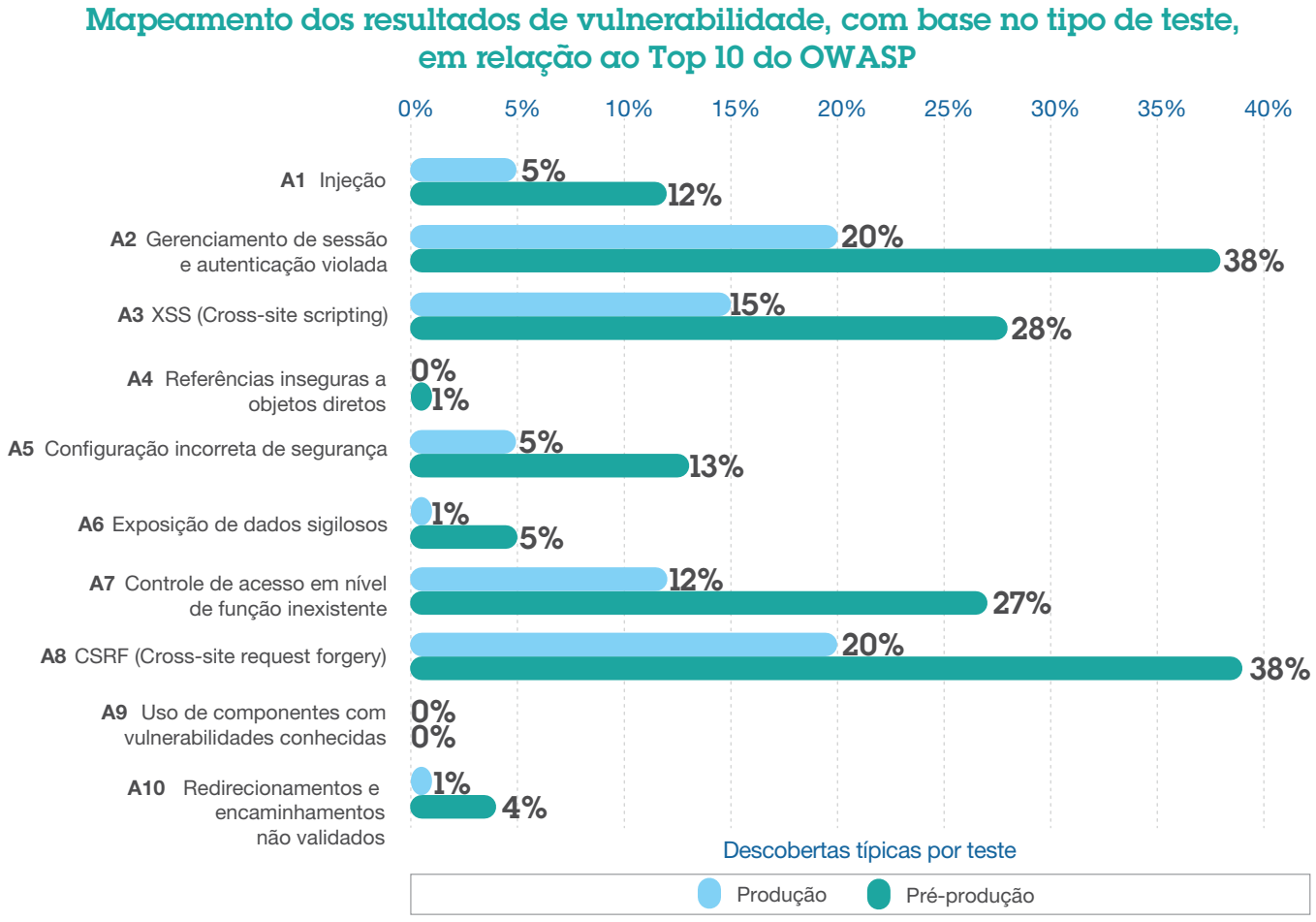


Figura 2. Resultados da varredura da produção e da pré-produção executada pelo serviço Hosted Application Security Management (HASM) da IBM em comparação ao Top 10 do OWASP de 2013.

Devido aos problemas com testes de formulário completo, é normalmente vantajoso executar varreduras em ambientes de preparação ou de controle de qualidade (QA) antes da implementação. A varredura da pré-produção pode ser complementada com verificações regulares discretas (isto é, sem preenchimento de formulário) nos aplicativos de produção. Essa abordagem possibilita a realização de testes completos de aplicativos sem o risco de corrupção de dados ou de interrupção dos sistemas de produção. Além disso, a abordagem promove também testes e monitoramento contínuos.

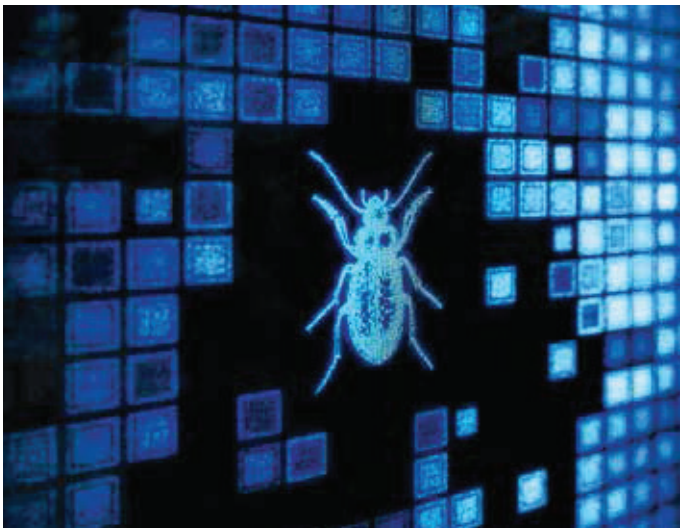
Cobertura

Outro item a ser considerado é a área de cobertura real do teste; por exemplo, o teste abrange apenas páginas da Web ou inclui áreas dinâmicas? Não suponha que as varreduras irão abranger a totalidade dos seus aplicativos. Há muitas formas de abordar a varredura de aplicativos, que, se executadas incorretamentes, poderão apresentar pontos cegos substanciais, deixando-os expostos.

Conforme mencionado anteriormente, é possível executar varreduras nos ambientes de produção e pré-produção. Dada a necessidade de proteger ambientes ativos, as varreduras da produção são frequentemente projetadas com cobertura limitada. Contudo, as varreduras da pré-produção devem ser executadas de uma forma mais invasiva, principalmente quando o assunto é preenchimento de formulários. Você pode ajudar a garantir uma cobertura adequada compreendendo a configuração da verificação em uso nas varreduras de pré-produção e produção.

Quando a questão é o preenchimento de formulários de aplicativos dinâmicos da Web, o uso de um mecanismo de rastreamento automático em testes normalmente é insuficiente. Aplicativos altamente dinâmicos requerem dados específicos de formulários, e a interface do usuário (UI) é, na maioria das vezes, sofisticada para um mecanismo de rastreamento automático navegá-la com sucesso e testar todas as funcionalidades. Em outras palavras, para obter cobertura de testes total desses aplicativos, é necessário ampliar o mecanismo de rastreamento automático com o rastreamento manual sendo executado por um profissional perito em testes de segurança.

Por fim, do ponto de vista de cobertura de página, é importante compreender que filtragem está sendo aplicada à verificação. As definições nas configurações de verificação podem filtrar páginas



na similaridade de páginase em outras redundâncias de URL. Embora seja uma excelente ferramenta para ajudar a garantir a otimização das varreduras em execuções mais rápidas, a filtragem também pode limitar a cobertura. Normalmente, essas configurações podem ser ajustadas manualmente e talvez tenham de ser aplicadas de formas diferentes, dependendo do site da Web.

Recomendações finais

Aplicativos são um importante alvo dos invasores. Se os aplicativos não forem testados quanto à vulnerabilidades de segurança e corrigidos, os invasores poderão encontrar brechas de segurança e penetrá-las. Os pesquisadores da IBM recentemente descobriram vulnerabilidades na estrutura do Android e no navegador Firefox que colocaram em risco dados corporativos em dispositivos móveis. Da mesma forma, a equipe dos serviços HASM da IBM, usando o AppScan para testes, constatou que vulnerabilidades de injeção e autenticação violada estão ativas em vários aplicativos da Web nos ambientes de produção. A melhor forma de ajudar a prevenir essas ameaças e proteger dados acessíveis via dispositivos móveis e aplicativos da Web é testar os aplicativos para verificar se há vulnerabilidades de segurança e corrigir o que for identificado.

Spam e sua persistência ao longo do tempo

Quais são as ameaças mais recentes em spams? Saiba como os invasores estão reinventando formas de explorar a caixa de entrada de e-mails e fugir da detecção.

Desde suas origens no final da década de 1970, a guerra entre os criadores de spams e os sistemas de detecção de spams perdura. Avaliando os últimos aprimoramentos feitos na década passada, o Relatório de Riscos e Tendências da IBM X-Force 2011 apresenta uma análise abrangente da evolução do spam, incluindo ameaças de longo prazo, técnicas e flutuações nos volumes gerais.

Hoje, passados alguns anos, ainda constatamos as idas e vindas de algumas das mesmas ameaças. Spam em textos sem formatação e spam em anexos ZIP infectados ainda predominam, e os invasores descobrem novas formas de fugir da detecção. Outras técnicas, como envio de arquivos MP3 ou anexos em PDF, não são tão eficazes.

O spam baseado em imagem, lançado pela primeira vez em 2005, vai e volta de novas maneiras.

Seja promovendo cotas de ações de baixo preço em esquemas "pump-and-dump" (em que divulgam o aumento de uma determinada ação da bolsa, que na verdade tem um valor muito baixo, inflacionando falsamente o preço dessa ação) ou estabelecendo links para conteúdos mal-intencionados, os agressores continuam por aí, procurando novas formas de explorar caixas de entrada de e-mails a fim de obter eficácia máxima.

Uma visão diferente das origens do spam

O spam foi, e ainda é, um grave problema, pois continua sendo o principal canal de penetração de malware em redes corporativas. Em março de 2014, testemunhamos os mais altos níveis de spam apurados durante os últimos dois anos e meio. A Figura 3 mostra os principais países de onde se originaram spams nos últimos seis meses; muitos dos países listados no passado continuam liderando a lista atual de invasores (para obter mais informações sobre países originadores de spams, consulte o Relatório Semestral de Tendências e Riscos da IBM X-Force 2013).

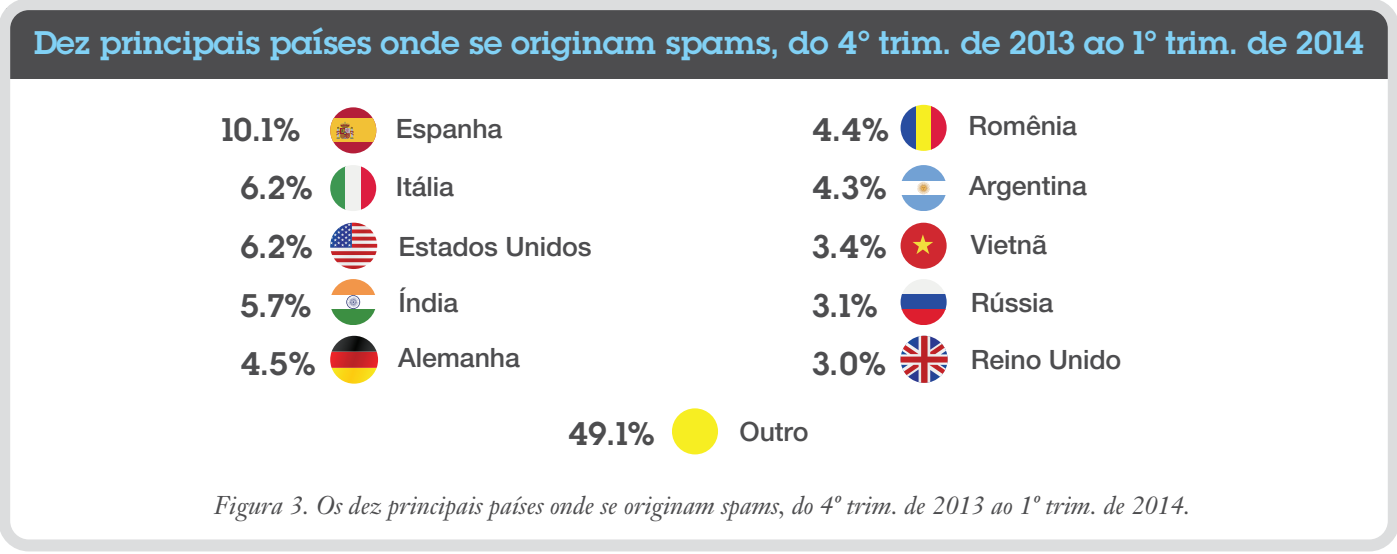


Figura 3. Os dez principais países onde se originam spams, do 4º trim. de 2013 ao 1º trim. de 2014.

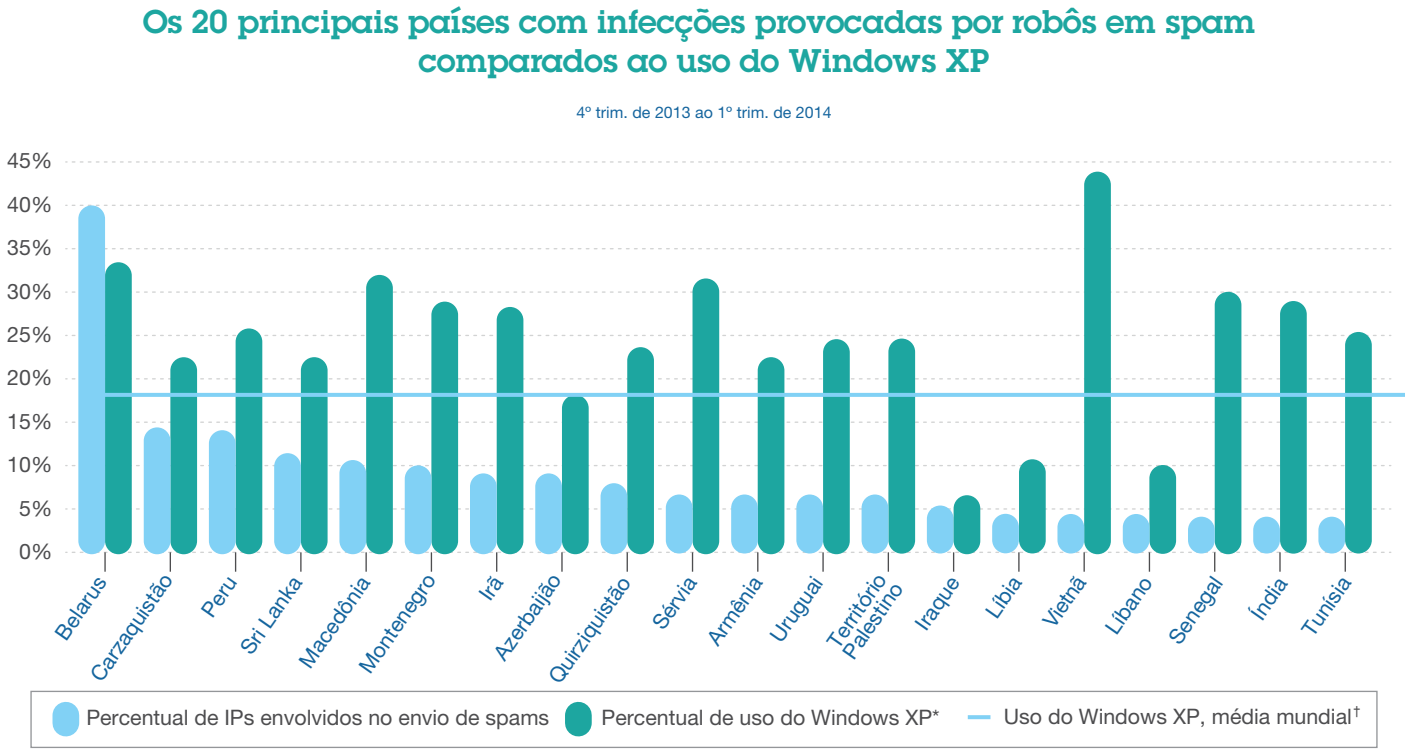


Figura 4. Os 20 principais países com infecções provocadas por robôs em spam comparados ao uso do Windows XP. 4º Trim. de 2013 ao 1º trim de 2014.

* Dados compilados de "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Oct to Dec 2013" e "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Jan to Mar 2014," StatCounter, último acesso em 14 de maio de 2014.

† "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014," StatCounter, último acesso em 17 de abril de 2014.

Infecções causadas por robôs em spam e o término do suporte ao Windows XP

Outra percepção interessante desses dados é obtida com o cálculo do percentual de computadores (ou endereços IP) envolvidos no envio de spams. Ao compararmos o número de IPs identificados em ataques de spam nos últimos seis meses com o número total de IPs por país, obtemos os resultados apresentados na Figura 4.

Embora cada um dos países listados na Figura 4 seja a origem de menos de 3% dos spams em nível mundial (com exceção de Índia e Vietnã), a proporção de infecções causadas por robôs em spam em computadores nesses países é assustadoramente alta. Um dos motivos pode ser o fato de muitos computadores não utilizarem as correções mais recentes ou mesmo os sistemas operacionais mais atuais. No momento, cerca de 18,4% dos computadores em todo o mundo ainda usam o Windows XP[5]. Porém, em 16 dos 20 países listados na Figura 4, o uso do Windows XP é significativamente maior que a média em todo o mundo.

Em alguns casos, o uso ultrapassa 30%, sendo ainda mais elevado no Vietnã, com 42,4%.

Em 8 de abril de 2014, a Microsoft anunciou o fim do suporte ao sistema operacional Windows XP[6]. A data de término do suporte foi amplamente divulgada por algum tempo e muitas organizações migraram grandes bases de usuários para versões mais atuais.

Contudo, há muitas organizações ainda enfrentando dificuldades (ou que, por opção, simplesmente não tomaram medidas) para abandonar o Windows XP. Além disso, certos setores, como o bancário, de software industrial e da saúde, estão enfrentando dificuldades com o anúncio do fim da vida útil do Windows XP. Por exemplo, 95% dos caixas eletrônicos nos EUA utilizam o Windows XP e poderiam se tornar alvos fáceis dos invasores[7]. Essas organizações provavelmente enfrentam agora desafios no mundo pós-suporte ao Windows XP.

De um ponto de vista diferente, o uso do Windows XP, em muitos casos, pode também estar correlacionado aos países de onde se originam os maiores volumes de spam. As estatísticas revelam que:

- Há uma evidência bastante difundida das infecções virais causadas por robôs em spam.
- O uso dos sistemas operacionais e aplicativos mais atuais, além da manutenção e aplicação das últimas atualizações e correções de segurança, continua sendo a forma mais eficaz de proteger destinatários e servidores vulneráveis contra o spam.

O retorno do spam em imagens

O spam em imagens esteve no apogeu em 2006 e 2007. De outubro de 2006 a março de 2007, mais de 40% de todo spam continha um anexo de imagens. Contudo, em meados de 2007, as ameças de spam em imagens pararam quase que completamente. Houve apenas duas breves reaparições:

- No terceiro trimestre de 2008, o percentual de spams contendo anexos de imagens atingiu a marca de 13,5% no início de outubro (medição feita mensalmente).
- Ao final de abril de 2009, os spams baseados em imagem respondiam por 13% de todos os spams (novamente, quando medidos mensalmente).

Desde abril de 2009, o percentual de spams em imagens não ultrapassa 10%. De tempos em tempos, observamos ameaças de spams em imagens, mas a uma proporção bem inferior a 10% (quando medidos semanalmente).

Contudo, em dezembro de 2013, os spams em imagens fizeram uma reaparição. Como mostra a iFgura 5, em 5 de dezembro os remetentes de spam surpreenderam, espalhando um grande volume de spams em imagens. Esse novo ataque de spams baseados em imagens perdurou até 16 de dezembro, com novas ocorrências sendo registradas praticamente todos os dias. Após um breve intervalo, os remetentes de spam iniciaram um forte ataque com spams em imagens em 23 de dezembro. O ataque durou um mês, com outro breve intervalo entre 8 e 13 de janeiro, parando em 22 de janeiro de 2014.

A Figura 5 também mostra que um mês depois, no dia 24 de fevereiro, teve início outra ameaça com spams em imagens. Porém, essa ameaça durou apenas três dias. Nesses dias, o volume foi apenas metade do volume constatado em dezembro e janeiro.

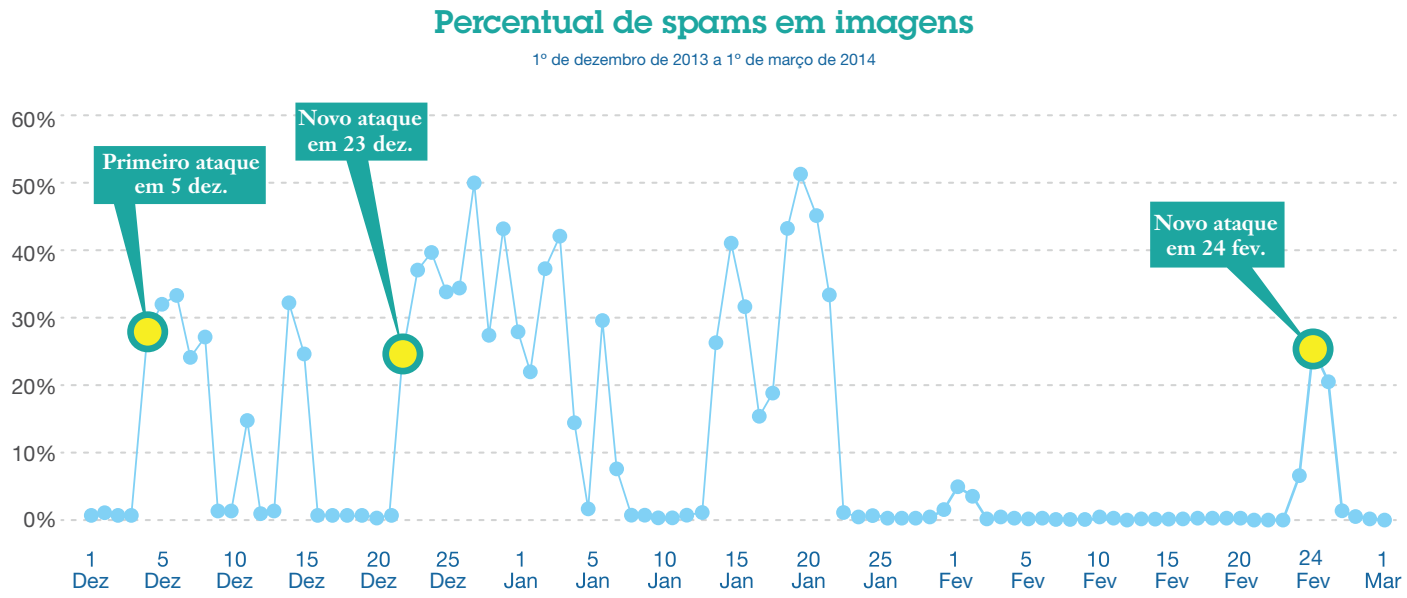


Figura 5. Percentual de spams em imagens, 1º de dezembro de 2013 a 1º de março de 2014.

Recurso	Ataque de dezembro de 2013 a janeiro de 2014	Ataque em fevereiro de 2014
Produtos anunciados	**Produtos médicos**	**Ações**
Recursos de imagem usados em ambos os ataques	Observamos algumas diferenças na forma como os invasores utilizam os spams em imagens atualmente em relação à época em que a técnica ganhou popularidade, no período de 2006 a 2007. Originalmente, os invasores pareciam ser mais cuidadosos em evitar a detecção de filtros de spam, modificando ligeiramente as mensagens. Visto que muitos filtros de spam utilizavam um hash de arquivo para determinar se certo anexo estava associado a atividades de spam, os invasores da época fizeram com que uma imagem básica aparentasse ser um arquivo diferente usando variações sutis, como mudança de cores ou de alguns pixels. Porém, em ataques recentes, as imagens não sofrem alterações frequentes. Os remetentes de spam usam a imagem idêntica repetidas vezes.	
Recursos de imagem	As imagens mostravam produtos médicos.	O texto da captura de tela apresentada anunciava uma ação em particular. Nessa ameaça, apenas duas imagens diferentes foram utilizadas.
Recursos de URL	Ao clicar nas imagens contidas no email, os destinatários eram direcionados a websites que, na maioria das vezes, apresentavam URLs como [...]doctor[...].ru (médico) ou [...]medic[...].ru (paramédico). Essas URLs não foram alteradas com muita frequência.	Não foram utilizadas URLs. Os spammers forneciam o símbolo da ação na expectativa de que os destinatários procurassem tal símbolo para adquirir as ações correspondentes.
Texto aleatório utilizado em ambos os ataques	Abaixo da imagem contida no email, os invasores inseriram textos aleatórios, os quais, em muitos dos casos, eram copiados de artigos da Wikipédia. Normalmente, os textos eram utilizados para ofuscar os filtros de spam, tais como os filtros bayesianos.	
Texto aleatório	Era difícil ler o que estava escrito, uma vez que as letras estavam um tanto quanto apagadas e em fundo branco. O texto se encontrava logo abaixo da imagem.	Texto incluído no email sem nenhuma ofuscação. No entanto, havia muitas linhas vazias inseridas abaixo da imagem de modo que era preciso rolar para baixo para visualizar o texto aleatório.

Tabela 1. Detalhes técnicos encontrados durante os ataques de spam em imagens no período de dezembro de 2013 a janeiro de 2014 em comparação com fevereiro de 2014.

A Tabela 1 resume alguns dos detalhes técnicos encontrados durante esses ataques recentes.

Ao comparar os ataques, concluímos que:

- Em termos técnicos, essas ameaças recentes de spam não utilizaram nenhuma técnica nova. Na verdade, o uso de variações de imagens e o período de manutenção das URLs de spam estão "fora de moda". Não sabemos ao certo porque os spammers utilizam essas técnicas mais antigas, mas, talvez por terem ficado afastados cinco anos, presumem que os filtros não estejam preparados para grandes ataques de spam baseados em imagens.
- Existem muitas semelhanças entre esses dois ataques, o que sugere que ambos possam ter sido iniciados pelo mesmo conjunto de ferramentas de spam.
- O spam em imagens continua a ser um problema relevante e interessante, uma vez que os spammers conseguem transmitir a mensagem desejada exclusivamente dentro da imagem, na qual os módulos de análise de conteúdo normalmente são incapazes de extrair informações baseadas no conteúdo textual. Isso pode causar impactos nos recursos de detecção dos filtros de spam que funcionam com detecção de conteúdo textual. Os spammers podem até solicitar que os usuários insiram uma URL a partir de uma imagem (como já visto antes), fazendo com que tal URL infecte o computador do usuário por meio de um drive-by-download. Nesse contexto, essas novas ameaças de spams de imagens podem ser consideradas algum tipo de teste para futuros ataques de spam relacionados a imagens.

Será interessante observar se 2014 será ou não o ano do retorno dos spams baseados em imagens.

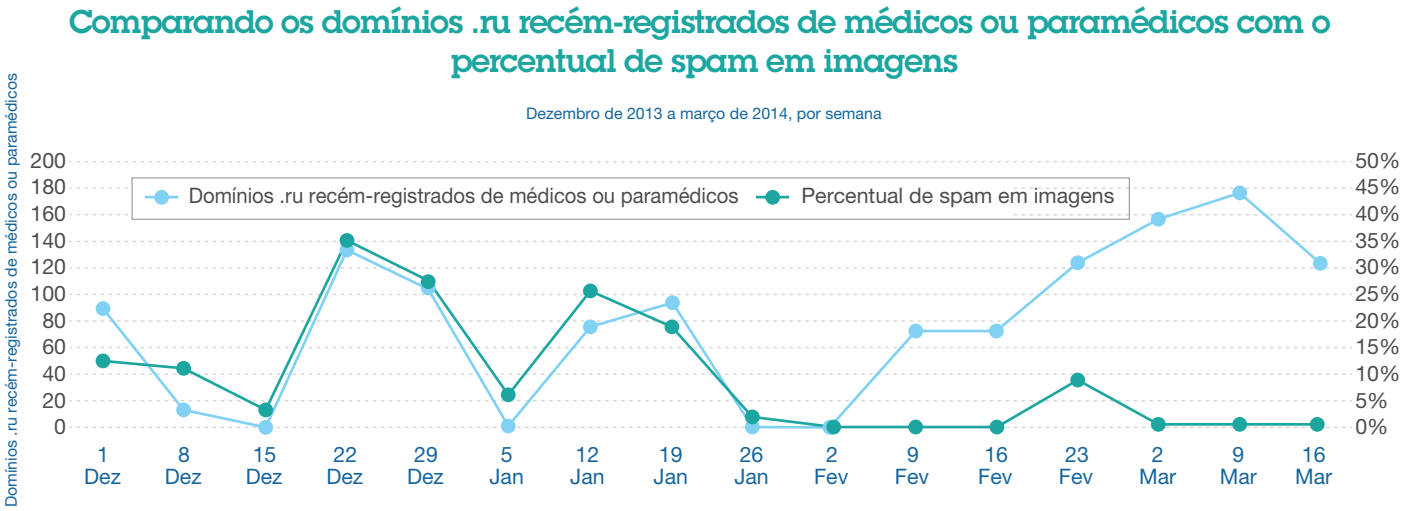


Figura 6. Comparando domínios .ru recém-registrados de médicos ou paramédicos com o percentual de spam em imagens por semana, de dezembro de 2013 a março de 2014.

Como mostra a Figura 6, os invasores estão utilizando os domínios .ru de médicos e paramédicos nesses ataques, o que desperta a curiosidade para saber se os spammers ainda utilizam o mecanismo para registrar os domínios [...]médico[...].ru ou [...]paramédico[...].ru. A resposta é sim.

Do início de dezembro de 2013 ao final de janeiro de 2014, o número de domínios [...]médico[...].ru ou [...]paramédico[...].ru recém-registrados correspondia ao percentual de spam baseado em imagens. No entanto, desde o início de fevereiro de 2014, os spammers têm utilizado esses domínios para outros tipos de spam que não são baseados em imagens.

Curiosamente, os spammers que utilizam o spam baseado em imagens ainda utilizam esses domínios por períodos relativamente longos, às vezes por várias horas ou até por um dia ou mais. Não houve alteração nesse tempo de vida nos últimos quatro meses observados. Esse período é considerado longo para URLs utilizadas em spam. Por outro lado, a maioria dos spammers utilizam os domínios apenas por algumas horas ou até mesmo por alguns minutos, uma vez que muitos filtros de spam verificam as URLs contidas em emails e as bloqueiam caso tenham sido detectadas como spam anteriormente. Como os spammers são os proprietários desses domínios, eles podem medir com facilidade o tempo que os usuários levam para clicar nas URLs. Com isso, mesmo se um domínio estiver ativo por um ou mais dias, parecem ainda existir filtros de spam que não os detectam ou usuários que permanecem sem utilizar o filtro de spam.

Os cinco itens principais a serem considerados para que a resposta remota a incidentes não se torne tão remota

Violações de segurança podem ocorrer em praticamente qualquer lugar. Descubra como preparar sua equipe de TI para a resposta remota a incidentes.

No passado, todo e qualquer serviço de resposta a incidentes implicava viajar até as instalações do cliente. Os responsáveis pela resposta a incidentes explodiam em felicidade ao receberem uma chamada de um cliente com instalações localizadas em uma ilha tropical.

Nos últimos tempos, esse paradigma mudou. Com os regulamentos mais rígidos referentes a dados pessoais e a importância colocada nas violações de segurança, muitas organizações precisam de respostas com maior rapidez eficiência do que nunca. Em alguns Estados, as organizações devem notificar as agências reguladoras poucos dias após não só da confirmação da violação, como também de sua suspeita. Em vista disso, os responsáveis pela resposta a incidentes, tais como os membros da equipe de Serviços de Resposta a Emergências (ERS) do IBM Global Technology Services, desenvolveram metodologias e utilizam ferramentas de triagem para ajudar a acelerar a resposta a incidentes. Essas ferramentas e metodologias são utilizadas para que seja possível obter artefatos relevantes com rapidez, tais como a memória RAM e os logs de eventos dos sistemas comprometidos, para enviá-los a analistas remotos que possam iniciar rapidamente a análise.

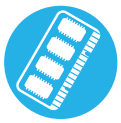
No entanto, o que acontece quando o sistema de informação que se suspeita fazer parte de uma violação está localizado em uma região do mundo sem infraestrutura para apoiar os esforços de resposta a incidentes? Por exemplo, imagine se a largura de banda da Internet não for suficiente o bastante para permitir a transferência de artefatos essenciais aos analistas de resposta a incidentes (uma técnica comum para possibilitar uma avaliação rápida)? O sistema de informação pode estar localizado também em um país subdesenvolvido distante, o que faz de uma viagem algo impraticável, e, além disso, pode haver escassez de profissionais de TI qualificados.

É exatamente essa a situação que a equipe de ERS da IBM enfrenta com cada vez mais frequência. Com um maior número de empresas expandindo suas operações para mercados menos tradicionais, os serviços de resposta a incidentes em locais extremamente remotos ocorrem com mais frequência. Responder a incidentes em países remotos ou em áreas com infraestrutura deficiente exige um plano de atuação exclusivo.

Esta seção do relatório analisa os cinco itens principais a serem considerados ao enfrentar situações de resposta a incidentes nas quais os sistemas de informação afetados estão extremamente remotos. Algumas das considerações são técnicas, enquanto outras são de natureza gerencial. No entanto, todas são igualmente valiosas.

Itens a serem considerados na resposta remota a incidentes

1. Largura de banda
A transferência de dados pode ser limitada em função de conexões lentas e não confiáveis.



2. RAM
Pode não haver unidades externas disponíveis para armazenar os arquivos de dump da memória RAM.

3. Serviço de correio expresso
Podem existir dificuldades para enviar os sistemas afetados e os dados forenses.

4. Horário comercial
As diferenças de fuso horário podem afetar os planejamentos dos serviços.

5. Conjuntos de habilidades
Os administradores de sistema talvez não possuam treinamento para resposta a incidentes.

Figura 7. Os cinco itens principais a serem considerados na resposta remota a incidentes segundo a equipe de Serviços de Resposta a Emergências (ERS) do IBM Global Technology Services.

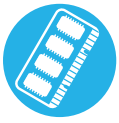
1. Largura de banda é primordial

Como nem todos os incidentes de segurança ocorrem em sistemas de informação localizados em áreas com alta largura de banda, como em um datacenter ou em um país industrializado, os responsáveis pela resposta a incidentes podem ter de trabalhar com conexões de rede lentas e não confiáveis. Essa situação pode prejudicar os esforços de resposta a incidentes. Normalmente, quando a equipe de ERS é envolvida em um incidente de segurança, os analistas de ERS começam a trabalhar assim que ocorre a transferência de alguns arquivos selecionados (tais como logs, amostras de malwares, memória RAM e outros artefatos). Embora transferir vários gigabytes de arquivos possa levar muito tempo, trata-se de uma atividade perfeitamente viável, além de permitir que a ERS inicie a análise de forma mais rápida do que enviar analistas de avião para uma localidade remota ou enviar os discos rígidos pelo correio.

Quando a largura de banda passa a ser um problema, os responsáveis pela resposta a incidentes são forçados a eliminar vários artefatos maiores e possivelmente valiosos dos sistemas de informação para ficar com artefatos menores.
A eliminação de um conjunto de artefatos de um sistema de informação pode aumentar o tempo para a obtenção de resultados, reduzir a certeza quanto a tais resultados e aumentar o custo geral da resposta.
As restrições quanto à largura de banda também limitam a capacidade de utilização de um jumpbox ou host bastião, um método de realização de análise testado e comprovado, para possibilitar a conexão a sistemas extremamente remotos.

O que é um servidor bastião?

Um host bastião[9] é um computador para fins especiais que fica totalmente exposto a ataques. O computador é colocado no lado público da zona desmilitarizada (DMZ) sem a proteção de um firewall ou de um roteador de filtragem. Em função dessa exposição, os hosts bastiões normalmente são configurados para cumprir uma função específica (por exemplo, atuar como um servidor proxy) e todos os serviços, protocolos, programas e portas de rede desnecessários são desativados ou removidos.
Os hosts bastiões recebem também reforço extra para ajudar a controlar o acesso de intrusos e limitar os possíveis métodos de ataque.



2. A RAM pode estar inacessível

Sem nenhuma dúvida, um dos artefatos mais valiosos para uma resposta a um incidente é a memória RAM de um sistema comprometido. A RAM de um sistema PC moderno é considerada o melhor local para encontrar dados abrangentes e comprobatórios, além de quase não existir mais nada que corresponda ou supere seu valor nesse sentido. A RAM pode conter uma vasta quantidade de informações, incluindo detalhes sobre portas abertas, conexões de rede, processos em execução e assim por diante.

Porque acessar a RAM pode ser impossível? De acordo com a experiência da equipe de ERS da IBM, serviços extremamente remotos apresentam dois desafios principais. Durante vários serviços extremamente remotos, a ERS enfrentou uma infinidade de problemas para coletar a memória RAM. Em primeiro lugar, o tamanho dos arquivos da RAM, principalmente em servidores de alta capacidade de processamento, pode ser muito grande, muitas vezes superior a 8 GB mesmo após a compactação. Problemas de largura de banda de Internet e de confiabilidade normalmente fazem com que as transferências de arquivos grandes sejam inaceitavelmente lentas ou falhem. Em segundo lugar, ao coletar a RAM, é necessário fazer o dump de arquivos em uma unidade externa, como um dispositivo USB. A ERS trabalhou em vários incidentes em que não havia dispositivos USB disponíveis para armazenar um arquivo de dump de memória RAM. Se um dispositivo USB não estiver prontamente disponível, é quase certo que será difícil encontrar uma loja de eletrônicos na vizinhança, por exemplo, se o sistema comprometido estiver em uma plataforma de petróleo na costa da Nigéria ou na zona rural de Uganda.

Embora talvez seja impossível acessar o arquivo de dump inteiro da RAM, pode ser possível acessar (ou pedir que um administrador do sistema acesse) os dados mantidos na memória RAM. Usuários logados, arquivos abertos, tarefas agendadas e outras informações talvez ainda possam ser coletadas, apesar de ser necessário utilizar técnicas rudimentares e menos eficientes.
Não importa se a memória RAM está completamente inacessível ou o responsável pela resposta a incidentes utiliza técnicas menos eficientes, a organização deve estar preparada para os desafios na coleta de dados voláteis.

Trabalhar dentro das limitações mínimas de largura de banda e a impossibilidade de acesso ao dump da RAM não impossibilita a resposta a incidentes. No entanto, as equipes de resposta a incidentes não acostumadas a trabalhar com tais limites devem estar preparadas. O desenvolvimento de metodologias e treinamentos para saber o que fazer frente a esses obstáculos deve ser obrigatório em organizações com sistemas de informação em locais com largura de banda deficiente ou em situações em que não é possível realizar o dump da memória RAM. Caso contrário, esses desafios podem se tornar obstáculos intransponíveis.

3. Talvez não exista serviço de correio expresso

Os clientes nacionais da equipe de ERS da IBM frequentemente optam por enviar os sistemas afetados ou os dados coletados por correio expresso aos analistas de resposta a incidentes de ERS. O envio de imagens forenses, RAM coletadas, arquivos de log ou até mesmo sistemas inteiros pode demorar 12 horas, no mínimo, se realizado por um serviço expresso de transporte. Além disso, ao considerar a transferência de dados entre países, seja de maneira física ou pela rede, é importante conhecer os regulamentos que podem impedir tal transferência. É evidente que, caso seja urgente fornecer resultados o mais rápido possível, o correio expresso pode ser uma boa opção.

No entanto, e se os seus sistemas de informação e dados estiverem em uma localidade que não possua serviço de correio expresso? Considerando ainda o exemplo da plataforma de petróleo, pode não ser logisticamente viável enviar um sistema ou selecionar arquivos de uma localidade como essa. Como alternativa, mesmo que o sistema de informação esteja em um país no qual os serviços da UPS ou Fedex existam, não é raro que os itens de possível alto valor enviados, como computadores, fiquem retidos na alfândega por dias. Quando for necessário obter respostas e o tempo for curto, atrasos como esse podem interferir nos esforços para a obtenção de respostas ágeis e eficazes.

4. O horário comercial pode afetar os planejamentos

Normalmente durante os serviços de resposta a incidentes, a ERS realiza solicitações aos pontos de contato (tais como os administradores de sistema) durante o horário comercial à medida que análise avança. É um processo fluido em que as solicitações são normalmente atendidas com urgência por causa da gravidade dos comprometimentos à segurança.

Isso pode não ocorrer ao analisar possíveis comprometimentos à segurança de organizações localizadas em áreas extremamente remotas. As diferenças de fuso horário podem fazer com que o horário comercial de seus pontos de contato esteja várias horas antes ou depois do horário comercial local, com pouco tempo em comum. Essa restrição pode exigir que a equipe de resposta a incidentes ajuste o planejamento de serviços ou realize solicitações agregadas. Seus analistas precisarão considerar cuidadosamente quais itens são necessários para avançar com a análise, uma vez que uma solicitação de acompanhamento talvez só possa ser atendida após 24 horas.

5. Escassez de conjuntos de habilidades

Os responsáveis pela resposta a incidentes na ERS geralmente têm sorte de trabalhar com administradores de sistemas altamente qualificados ao responder a um comprometimento à segurança. Em alguns casos, essa pode ser a diferença entre um incidente que dura alguns dias e um incidente que leva semanas a ser resolvido.

Na maioria dos serviços, a ERS trabalha em áreas extremamente remotas; no entanto, administradores de sistemas qualificados ou até mesmo pontos de contato com conjuntos de habilidades técnicas básicas são escassos. Ao trabalhar em ambientes extremamente remotos, os especialistas de resposta a incidentes devem estar cientes dessa limitação e ajudar a garantir que todas as instruções, perguntas e outras comunicações sejam extremamente específicas, sem margem à interpretação e sem dependência de um alto grau de habilidade.

Uma forma de ajudar a minimizar os problemas enfrentados pelas diferenças de fuso horário e escassez de conjuntos de habilidades técnicas é garantir que a organização tenha especialistas no assunto (SMEs) em diversas áreas geográficas.

Os SMEs não precisam ser gurus de resposta a incidentes. Em vez disso, ter um administrador de sistema com treinamento mínimo que possua um conjunto básico de habilidades de resposta a incidentes pode ajudar a garantir pelo menos um pouco de disponibilidade do suporte do SME no local do incidente. Ter um SME local com conhecimentos básicos das metodologias de socorrista a incidentes, de preservação de dados e de análise pode ser a diferença entre um incidente que se estende por semanas e outro que é resolvido em poucos dias.

Para resumir, a resposta a incidentes em áreas extremamente remotas é possível, no entanto, os responsáveis por realizá-la devem estar preparados para ajustar seus procedimentos operacionais, desenvolver táticas diferentes e trabalhar com um conjunto limitado de dados.

Entender as limitações e fazer ajustes no início do serviço podem ajudar a garantir uma resposta bem-sucedida, apesar dos obstáculos indesejáveis.

Sobre a X-Force

As ameaças avançadas estão em toda parte. Ajude a minimizar os riscos com insights de especialistas da IBM.

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

Colaboração da IBM Security

A IBM Security representa várias marcas que oferecem um grande espectro de competência de segurança:

- A equipe de pesquisa e desenvolvimento IBM X-Force descobre, analisa, monitora e registra uma ampla variedade de ameaças e vulnerabilidades à segurança de computadores, além das tendências e dos métodos mais recentes utilizados por invasores. Outros grupos da IBM utilizam esses dados ricos para desenvolver técnicas de proteção aos nossos clientes.
- A Trusteer[8], uma empresa IBM, oferece uma plataforma holística de prevenção de crimes em endpoints que ajuda a proteger as organizações contra fraudes financeiras e violações de dados. Centenas de organizações e milhões de usuários finais dependem da Trusteer para proteger seus aplicativos da web, computadores e dispositivos móveis de ameaças online (tais como malwares avançados e ataques de phishing). Com uma equipe de pesquisa avançada e dedicada, a inteligência exclusiva e em tempo real da Trusteer possibilita que a sua plataforma baseada em nuvem se adapte rapidamente às novas ameaças.
- A equipe de segurança de conteúdo da IBM X-Force busca e categoriza a web por meio de rastreamento, descobertas independentes e feeds fornecidos pelos Serviços Gerenciados de Segurança da IBM.
- Os Serviços Gerenciados de Segurança da IBM atuam em 10 centros de operações de segurança que fornecem serviços gerenciados de segurança, ferramentas e conhecimento para clientes ao redor do mundo, 24 horas, 7 dias por semana. Eles são responsáveis por monitorar explorações relacionadas a endpoints, servidores (incluindo servidores da Web), aplicativos e infraestrutura de rede em geral. Seus especialistas em segurança rastreiam explorações, ataques e incidentes para milhares de clientes.
- Os Serviços Profissionais de Segurança da IBM oferecem serviços corporativos de avaliação, design e implementação de segurança para ajudar a criar uma estratégia eficaz de inteligência em segurança, bem como desenvolver soluções eficazes de segurança de informações.
- A Plataforma de Inteligência em Segurança IBM QRadar® oferece uma solução integrada de gerenciamento de inteligência e eventos de segurança (SIEM), gerenciamento de logs, gerenciamento de configuração, avaliação de vulnerabilidades e detecção de anormalidades. Ela fornece um painel unificado e insights em tempo real sobre os riscos de segurança e conformidade de pessoas, dados, aplicativos e infraestrutura.
- O IBM Security AppScan permite que as organizações avaliem a segurança de aplicativos da Web e móveis, fortaleçam o gerenciamento de programas de segurança de aplicativos e obtenham conformidade regulatória pela identificação de vulnerabilidades e geração de relatórios com recomendações inteligentes para facilitar as correções. O serviço de IBM Hosted Application Security Management (HASM) é uma solução baseada em nuvem para testar aplicativos da web com o uso do AppScan em ambientes de pré-produção e produção.

Colaboradores

O Relatório Trimestral de Inteligência contra Ameaças da IBM X-Force é resultado de uma colaboração dedicada que envolve todos da IBM. Gostaríamos de agradecer às seguintes pessoas pela atenção e contribuição para a publicação deste relatório.

Colaborador	Cargo
Andrew Cranke	Senior Application Security Consultant, IBM Hosted Application Security Management
Anik Campeau	Application Security Consultant, IBM Hosted Application Security Management
Diana Kelley	Application Security Strategist, IBM Security AppScan
Dr. Jens Thamm	Database Manager, IBM X-Force Content Security
John Adams	Senior Incident Response Analyst, IBM Global Technology Services - Emergency Response Services
Leslie Horacek	Manager, IBM X-Force Threat Response
Marc Noske	Database Administrator, IBM X-Force Content Security
Mark Wallis	Senior Information Developer, IBM Security Systems
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force and Security Intelligence
Ralf Iffert	Manager, IBM X-Force Content Security
Rob Lelewski	Engagement Lead, IBM Global Technology Services - Emergency Response Services
Robert Freeman	Manager, IBM X-Force Advanced Research
Thomas Millar	Senior Incident Response Analyst, IBM Global Technology Services - Emergency Response Services

Para mais informações

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

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

[2] Roee Hay, "New Vulnerabilities in Firefrox for Android: Overtaking Firefox Profiles," *IBM Security Intelligence Blog*, 26 de março de 2014. http://securityintelligence.com/vulnerabilities-firefox-android-overtaking-firefox-profiles/

[3] Roee Hay, "A New Vulnerability in the Android Framework: Fragment Injection," *IBM Security Intelligence Blog*, 10 de dezembro de 2013. http://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/

[4] "OWASP Top 10 for 2013," *OWASP*, 12 de junho de 2013.. https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

[5] "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014," *StatCounter*, acessado em 17 de abril de 2014. http://gs.statcounter.com/#os-ww-monthly-201310-201403-bar

[6] Enterprise Customers: Support for Windows XP has ended," *Microsoft*, abril de 2014. https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

[7] Jose Pagliery, "95% of bank ATMs face end of security support," *CNNMoney*, 4 de março de 2014. http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/?iid=EL

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

[9] Kurt Dillard, "Intrusion Detection FAQ: What is a bastion host?" *The SANS Institute*, acessado em 13 de maio de 2014. http://www.sans.org/security-resources/idfaq/bastion.php

Recicle

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América,
junho de 2014

WGL03050-BRPT-00