Semestral da Cisco 2014

Relatório de segurança

Resumo executivo

Qualquer ataque cibernético, de pequena ou grande proporção, tem início em um elo fraco na cadeia de segurança. Elos fracos podem assumir várias formas: softwares ultrapassados, códigos mal-escritos, um site abandonado, erros cometidos pelos desenvolvedores e até mesmo um usuário que confia cegamente em tudo e em todos. Nossos adversários buscam justamente esses elos fracos, com o objetivo de usá-los em suas operações.

Infelizmente, os agentes mal-intencionados não precisam se esforçar muito para encontrar os pontos fracos das empresas e dos usuários que são vítimas de ataques. Na Internet de Todas as Coisas, que tem como base a conectividade com a Internet das Coisas, o trabalho dos agentes maliciosos se torna ainda mais fácil, pois tudo o que estiver conectado a uma rede (de carros até sistemas de automação residencial) torna-se um possível alvo de ataque.

O impacto dos ataques cibernéticos é preocupante, tanto em termos de custos como em perdas de produtividade e reputação. De acordo com o Instituto Ponemon, o custo médio de uma violação de dados de uma empresa foi de US$ 5,4 milhões em 2014, maior do que a média de US$ 4,5 milhões em 2013. Além disso, o relatório de estimativa do custo ***de crimes cibernéticos e espionagem cibernética, realizado pelo Center for Strategic and International Studies***, estima que a economia dos EUA perde uma quantia de US$ 100 bilhões anualmente, e que cerca de 508.000 empregos norte-americanos são perdidos, devido à atividade online maliciosa.[1]

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Inteligência de ameaças

Ir para Inteligência de ameaças

O ***Relatório de segurança semestral da Cisco de 2014*** analisa informações sobre ameaças e tendências de segurança cibernética do primeiro semestre de 2014. A pesquisa da Cisco ajuda a enfatizar os diversos tipos de elos fracos que existem nos sistemas que utilizamos (incluindo a própria Internet), e o que pode ser feito para minimizar seu número e seus efeitos. Os principais resultados incluem:

Como parte do projeto contínuo "De dentro para fora" da Cisco, que examina consultas de Sistema do nomes de domínio (DNS), ou seja, pesquisa endereços IP associados a um nome de domínio que tenham origem dentro das próprias redes corporativas de clientes da Cisco, os pesquisadores que analisaram as redes de 16 empresas multinacionais concluíram que:

Cerca de 70% das redes dos clientes analisadas pelos pesquisadores da Cisco foram identificadas como emissoras de consultas de DNS para DNS dinâmico (DDNS).

Mais de 90% das redes desses clientes foram identificadas como emissoras de solicitações DNS para nomes de host associados à distribuição de malware.

Mais de 40% das redes desses clientes foram identificadas como emissoras de solicitações DNS para nomes de host associados a dispositivos que oferecem serviços como VPN IP Security (IPsec), VPN Secure Sockets Layer (SSL), Secure Shell (SSH) Protocol, Simple File Transfer Protocol (SFTP), FTP e FTP Secure (FTPS).

Dos 2.528 alertas de vulnerabilidade que foram publicados entre janeiro e junho de 2014, 28 foram identificados como sendo explorados ativamente. Estas são as prioridades ou vulnerabilidades urgentes que precisam ser corrigidas rapidamente.

Após sofrer uma queda em 2013, o volume global de spam começou a subir novamente desde outubro, mas nem todos os países estão observando esse aumento.

Tendências do setor

Ir para Tendências do setor

Durante o primeiro semestre de 2014, o setor farmacêutico e químico, que obteve lucros elevados, foi classificado novamente entre as três principais atividades de alto risco para a ocorrência de malware na Web.

O setor de mídia e publicidade observou um grande aumento no número de ataques, maior que a taxa comum de ocorrência de malware na Web anteriormente observada.

2014 foi um ano movimentado para os ataques de negação de serviço (DDoS) distribuídos pelo Network Time Protocol (NTP). Um dos ataques de amplificação de NTP mais significativos do primeiro semestre de 2014 foi direcionado ao cliente de um provedor global de DNS, o CloudFlare. No seu auge, o ataque de fevereiro atingiu quase 400 Gbps de tráfego de protocolo UDP.

De acordo com os pesquisadores de segurança da Cisco, o número de kits de exploração diminuiu 87% desde que o codificador Paunch, suposto criador do popular kit de exploração Blackhole, foi preso no ano passado.

A maioria dos kits de exploração usados no primeiro semestre de 2014 tentavam explorar territórios dominados pelo kit do Blackhole, mas ainda não havia um líder nessa batalha.

Em 2014, as explorações de ponto de venda (POS) se tornaram a escolha favorita dos criminosos por diversas razões:

A probabilidade cada vez maior de que os sistemas de ponto de venda (POS) estejam conectados à Internet, o que oferece aos criminosos um ponto de entrada para as redes empresariais.

A dificuldade de compreender que as informações de cartão de crédito devem ser consideradas dados importantes, o que significa que essas informações são menos protegidas.

A utilização cada vez maior de fornecedores terceirizados para todas as soluções de POS ou parte delas, disponibilizando ainda mais pontos de acesso para os criminosos.

Um olhar para o futuro

Ir para Um olhar para o futuro

Os riscos de segurança que a Internet das Coisas pode criar e por que as empresas devem abordá-los de forma proativa.

A importância de utilizar a análise preditiva e a aprendizagem automática para ajudar a identificar ameaças que são difíceis de serem detectadas na rede.

A tendência de as empresas considerarem a segurança cibernética um risco estratégico e um processo comercial.

A necessidade de soluções de segurança na plataforma, determinadas pela visibilidade e com enfoque nas ameaças, que englobem toda a sequência de ataque (antes, durante e depois) e ajudem a corrigir as falhas de segurança e a reduzir a complexidade causada por produtos discrepantes.

Conteúdo

Introdução 7

A Internet das Coisas: novas oportunidades, novos riscos 7

Inteligência de ameaças 9

Uma mudança de paradigma no comprometimento: olhando de dentro para fora 10

Tendências geopolíticas a serem observadas 14

Explorações na Web: explorações no Java continuam a dominar 15

Atualizações de vulnerabilidades: enfoque nas explorações mais comuns 17

Heartbleed: não é a única causa de preocupação 20

Relatório de risco vertical no setor: aumentos incomuns em alguns setores 21

Descobertas de malware por região 23

Cinco principais riscos verticais por região 25

Atualização de spam: o spam “Life Event” torna-se mais prevalente 26

Spammers tornam-se mais ágeis, Mudar as abordagens para aumentar o sucesso 26

Aumento de volume de spam global até duas vezes acima da faixa normal, mas alguns países observam um declínio acentuado 27

Tendências do setor 28

Conexões criptografadas seguras comprometidas 29

Ataques de ampliação: adversários sincronizados com NTP 31

Kits de exploração: o campo abre para a competição 33

Malvertising: um incômodo para a economia da Internet 35

Anúncios realmente nocivos: o papel da Malvertising em Ransomware 36

Vulnerabilidades do WordPress: quem está vigiando a loja? 37

Ataque de POS: vetor de ameaça popular para criminosos que procuram dados do cartão de pagamento 38

Monitoramento mais crítico dos dados do cartão de pagamento 39

Engenharia social: localização de links inseguros pessoalmente 40

Um olhar para o futuro 42

Segurança cibernética inteligente para o mundo real 43

Operacionalização da segurança: tornando a segurança um processo empresarial 45

Compreensão do risco cibernético em termos empresariais 47

Análise preditiva: um detetive que aumenta a segurança 49

Sobre a Cisco 50

Notas finais 51

Este documento contém material que pode ser pesquisado e distribuído

Clique para abrir o recurso no Adobe Acrobat

Compartilhe o conteúdo por e-mail e mídia social

Software recomendado:

Adobe Acrobat versão 7.0 e superior

A Internet das Coisas: novas oportunidades, novos riscos

A Internet das Coisas "é a rede de objetos físicos acessados pela Internet, conforme definido pelos analistas e visionários de tecnologia. Esses objetos têm tecnologia integrada para interagir com estados internos ou ambientes externos. Em outras palavras, quando os objetos podem detectar e se comunicar, ela altera como e onde as decisões são tomadas e quem as toma."[2]

A previsão é que a Internet das Coisas atinja aproximadamente 50 bilhões de coisas até 2020, de acordo com a Cisco.[3] Ela já está mudando o cenário da segurança, ampliando exponencialmente a superfície de ataque. A Internet das Coisas amplia a importância da proteção e da detecção contínua e difundida, à medida que pessoas, processos e dados ficam cada vez mais conectados.

Em um mundo de computação difundida e interconectividade extrema em rápida evolução, qualquer item conectado a uma rede representa uma superfície de ataque passível de exploração por adversários. O que os invasores *poderiam* fazer, na maior parte das vezes, ainda é hipotético, mas eles já fazem planos, testam ideias e obtêm algum sucesso.

Carros, dispositivos médicos e até mesmo babás eletrônicas foram alvos recentes da "pesquisa e desenvolvimento" da Internet das Coisas pelos hackers.[4–6]

A meta final da Internet das Coisas é aumentar a eficiência operacional, potencializar novos modelos empresariais e melhorar a qualidade de vida. Objetos rotineiros conectados e em rede nos trazem benefícios devido à capacidade de combinar dados simples para produzir inteligência utilizável. Mas isso também significa que há maior probabilidade de existir mais informações pessoais e dados empresariais na nuvem sendo recebidos e enviados. Com isso, surgem implicações importantes para a aplicação da segurança correta para proteger dados e determinar políticas para abordar a forma como os dados são usados.

A privacidade é uma preocupação importante na Internet das Coisas. Mesmo quando os usuários tomam cuidados para proteger as informações e evitar a ingenuidade excessiva ainda há risco, devido aos elos fracos na cadeia de segurança que estão além do controle (consulte Conexões criptografadas seguras que foram comprometidas, página 29). Os adversários poderão obter um cenário mais amplo sobre um usuário do que se estivessem vendo informações em um único dispositivo, sistema ou aplicativo quando começarem a correlacionar fontes diferentes, como um carro, smartphone ou sistema de automação residencial. Esses detalhes sobre usuários, desde os hábitos de compra até onde moram, permitirão que os agentes iniciem campanhas bem projetadas e altamente direcionadas com um nível de sofisticação nunca visto antes.

Para algumas pessoas, pode parecer impossível que algo tão simples como um dispositivo portátil de fitness ou um gravador de vídeo digital (DVR) represente um risco de segurança ou seja alvo de um hacker. Porém, por se assemelharem cada vez mais a plataformas de computador padrão, os carros e outros dispositivos de informática não tradicionais poderiam estar vulneráveis às mesmas ameaças[7] sofridas pelos dispositivos de informática tradicionais.

Os principais fornecedores estão cientes dos problemas de segurança nos dispositivos da Internet das Coisas e têm conhecimento e experiência para garantir a integração da segurança em seus produtos. As empresas em desenvolvimento, ao inovar, podem usar as lições aprendidas pelo setor de segurança cibernética nos últimos 20 anos para não cometer os mesmos erros. A maioria das melhores práticas aplicáveis aos computadores comuns também se aplica aos dispositivos da Internet das Coisas: por exemplo, a instalação do software mais recente. Porém, no mundo para o qual a Internet das Coisas está nos levando, a segurança será em grande parte gerenciada por sistemas, não por usuários, portanto o setor também deverá levar isso em consideração ao projetar a tecnologia de segurança para esse novo ambiente. Isso inclui garantir transparência aos usuários, para que eles tenham certeza que os dispositivos da Internet das Coisas estão automaticamente seguros ou para que reconheçam a necessidade de intervenção manual.

Sempre haverá algo novo sendo adicionado ao ecossistema da Internet. Ao mesmo tempo, a população de dispositivos abandonados e não gerenciados conectados à internet também aumentará. Assim como os inúmeros sites esquecidos ou abandonados por muito tempo na Internet hoje em dia (consulte Vulnerabilidades do WordPress: quem está vigiando a loja?, página 37), esses dispositivos, de utensílios de cozinha a câmeras de vigilância e impressoras pessoais, serão elos fracos na cadeia de segurança, oferecendo aos hackers corporativos acessos quase ilimitados, que podem ser desbloqueados e possivelmente levar ao data center.

Os recursos e as motivações dos criminosos cibernéticos são conhecidos, assim como o aumento do enfoque na Internet das Coisas é um progresso natural. Ao contrário da primeira investida da comunidade global em um mundo conectado à Internet, todos nós tiramos proveito dessa visão prospectiva: sabemos por experiência própria que o ambiente da Internet das Coisas oferece risco e que as empresas e usuários serão alvos de ataque. Hoje em dia, um maior risco é subestimar a destreza dos adversários e a rapidez com que a Internet das Coisas e a Internet de Todas as Coisas estão começando a tomar forma.

Inteligência de ameaças

Os especialistas em segurança da Cisco reuniram e analisaram as ideias de segurança do primeiro semestre de 2014 com base no maior conjunto de dados de telemetria disponível. Especialistas em segurança da Cisco realizam pesquisas e análises contínuas de ameaças descobertas, como o tráfego de malware, que podem dar uma ideia sobre o possível comportamento criminoso e ajudar na detecção de ameaças.

Uma mudança de paradigma no comprometimento: olhando de dentro para fora

A inteligência de ameaças apresentada no ***Relatório de segurança anual da Cisco de 2014*** incluiu uma descoberta importante de um projeto recente denominado "De dentro para fora", no qual os pesquisadores de segurança da Cisco analisaram as pesquisas de DNS originadas dentro das redes corporativas.[8]

Os pesquisadores de segurança da Cisco descobriram que o tráfego malicioso era visível em 100% das redes na amostragem.[9]

Com base na atividade que observaram, os pesquisadores da Cisco também determinaram que esse grupo específico de redes corporativas analisadas provavelmente havia sido invadido há algum tempo e que a infiltração principal não tinha sido detectada.

A Cisco apresenta outras descobertas nesse relatório, provenientes do projeto contínuo De dentro para fora. As informações têm como base a análise de dados feita pelos pesquisadores de ameaças da Cisco realizada em redes de clientes selecionadas desde o início de 2014. Os pesquisadores analisaram detalhadamente 16 grandes empresas multinacionais que controlaram coletivamente mais de US$ 4 trilhões em ativos, com receitas de mais de US$ 300 bilhões em 2013. Essa análise originou três ideias de segurança interessantes ligando essas empresas ao tráfego malicioso.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Solicitações para DDNS

Descrição da ameaça

O DDNS é um sistema geralmente usado para fins legítimos, ou seja, usuários domésticos que precisam ser capazes de mapear um nome de domínio totalmente qualificado (FQDN) – por exemplo, homeserver.isp.com – para um número ou pool de endereços IP dinamicamente atribuído pelo provedor de serviço da Internet (ISP).

Infelizmente, o DDNS, como muitas tecnologias e recursos desenvolvidos para uso legítimo, tornou-se comum entre os adversários, pois permite que os botnets e outras infraestruturas de ataque sejam resilientes em relação a detecção e posterior destruição. Grandes volumes de solicitações incomuns para domínios usando provedores de serviço DDNS, como name-services.com, podem indicar um possível comprometimento em uma rede da empresa. Embora muitas, e às vezes todas, as consultas de uma empresa por provedores de DDNS sejam verdadeiras, essas solicitações devem ser vetadas para garantir sua real legitimidade.

Resultados

Quase 70% (66,67%) das consultas de amostra de rede do cliente observadas em 2014 como parte desse projeto "De dentro para fora" foram identificadas como emissão de consultas DNS para DDNS. (Observação: os pesquisadores de segurança da Cisco esperam ver esse aumento na porcentagem com o decorrer do tempo, devido ao crescimento do tamanho da amostra de redes de clientes analisadas. A Cisco começou recentemente a rastrear essa nova categoria como um possível indício de comprometimento [IOC]. Um IOC é um evento ou artefato observado em um sistema, muitas vezes sutil, que, quando correlacionado com outros IOCs para um sistema, aponta para um provável comprometimento). Conforme indicado anteriormente, isso não significa que esses clientes estejam comprometidos por malware usando provedores DDNS. Entretanto, a Cisco recomendou que eles observassem melhor essas solicitações de DDNS para garantir que estão sendo realizadas por razões legítimas dos negócios.

Solicitações de sites associados ao malware Dessa forma, a funcionalidade MiTB é incorporada

Descrição da ameaça

Palevo, SpyEye e Zeus são famílias de malware que incorporam a funcionalidade MiTB (man-in-the-browser). Pesquisas de DNS em hosts comprometidos por Palevo, Zeus e SpyEye são consideradas uma ameaça muito grande. Esses botnets são espalhados através de mensagens instantâneas, redes peer-to-peer (P2P) e unidades removíveis. Eles são utilizados para realizar ataques de negação de serviço distribuído (DDoS) e roubar informações inseridas nos campos criados em tempo real e adicionadas a um formulário.

Palevo, Zeus e SpyEye merecem destaque, pois representam uma classe específica de malware que identifica informações, inclusive financeiras, inseridas em formulários online em navegadores com o sistema operacional Windows.

Resultados

Mais de 90% (93,75%) das redes dos clientes analisadas em 2014 continham tráfego direcionado para sites que hospedam malware. As redes foram identificadas como emissoras de solicitações DNS para nomes de host, em que o endereço IP solucionado pelo nome de host é reportado como associado à distribuição do malware Palevo, Zeus ou SpyEye, ou infectado por eles.

Solicitações DNS para FQDNs, sites e hosts associados aos protocolos administrativos

Descrição da ameaça

Entidades maliciosas devem usar canais de comunicação seguros e criptografados ou protocolos de transferência de dados para cobrir seus rastreamentos ao roubar informações. Alguns exemplos são IP Security (IPsec) VPN, Secure Sockets Layer (SSL) VPN, Secure Shell (SSH) Protocol, Simple File Transfer Protocol (SFTP), FTP e FTP Secure (FTPS). As empresas devem monitorar e validar regularmente essas comunicações. Esses tipos de sites podem ser usados para extrair dados usando canais criptografados e evitar a detecção.

Resultados

Mais de 40% (43,75%) das redes de clientes analisadas em 2014 foram identificadas como emissoras de solicitações DNS para sites e domínios associados aos dispositivos que fornecem serviços como IPsec VPN, SSL VPN, SSH, SFTP, FTP e FTPS.

Os pesquisadores da Cisco utilizaram pesquisas de DNS provenientes de redes corporativas para criar um resumo das possíveis vulnerabilidades e comprometimentos de dados. Os especialistas em segurança da Cisco analisaram as informações com base em listas de bloqueios e observaram as tendências em comprometimentos cibernéticos, vulnerabilidades exclusivas com verticais específicas e fatores geopolíticos que podem afetar agentes e informações direcionadas. Os clientes da Cisco que fazem parte do projeto "De dentro para fora" recebem um *relatório de ameaças cibernéticas externas* preparado pela Cisco.

Tendências geopolíticas que devem ser observadas

De acordo com os especialistas em segurança cibernética da Cisco, os eventos geopolíticos na Europa Oriental e no Oriente Médio estão criando novas tendências no campo cibernético, expandindo um cenário de risco para negócios, governos, outras organizações e usuários individuais em todo o mundo:

A instabilidade política na Ucrânia deu início a uma série de ataques DDoS e destruições de sites, supostamente programados para complementar as ações terrestres. Os problemas na Crimeia e em Kiev levaram à descoberta de um malware de espionagem sofisticado em redes ucranianas (chamado Ouroboros ou Snake), que permaneceu desconhecido durante meses ou anos.

No Oriente Médio, a invasão de seções inteiras do norte e oeste do Iraque pelo Estado Islâmico do Iraque e o Levante (ISIL ou ISIS) está sendo acompanhada por uma campanha de mídia social por uma guerra psicológica e sabotagem.

Olhando para o futuro, antigas divisões étnicas e religiosas estão se aprofundando em uma parte do mundo que já assume a liderança no uso de táticas cibernéticas por agentes civis e do governo. No segundo semestre de 2014, as polêmicas eleições presidenciais na Turquia, as eleições intermediárias nos Estados Unidos e o aumento das operações militares ocidentais no Afeganistão podem criar novos efeitos cascata no cenário cibernético mundial.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Explorações da Web: as explorações de Java continuam dominando

A exploração da linguagem de programação Java continua líder entre os IOCs monitorados pela plataforma de detecção avançada de malware Cisco® FireAMP. Essas explorações aumentaram a liderança aparentemente impossível de ser alcançada no primeiro semestre de 2014.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

FIGURA 1

Parcela de comprometimento do aplicativo semestral de 2014

FONTE: Cisco® FireAMP[10]

As explorações de Java representaram 91% dos IOCs em novembro de 2013, de acordo com o ***Relatório de Segurança Anual da Cisco de 2014***. Essa porcentagem aumentou para 93% em maio de 2014. A ampla superfície de ataque do Java e o alto retorno de investimento o tornam a preferência de exploração dos adversários. (Para obter mais informações sobre o problema do Java e dicas sobre como atenuá-lo, consulte o ***Relatório de Segurança Anual da Cisco de 2014[11]).***

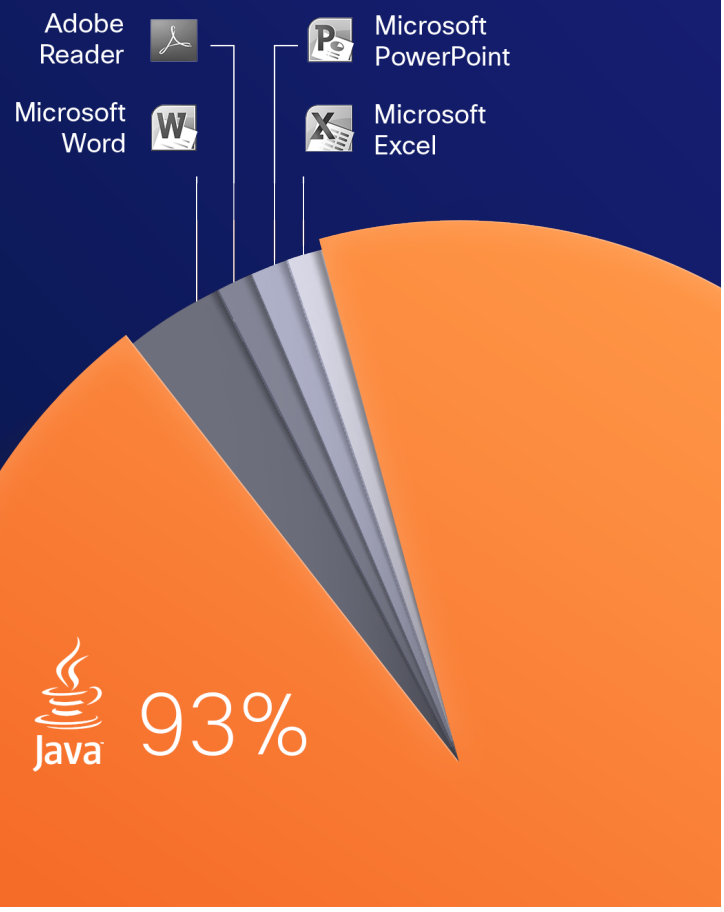


FIGURA 2

Descobertas de malware no Java (janeiro a maio de 2014)

FONTE: Cisco Cloud Web Security

Descobertas de malware no Java atingiram seu auge em março de 2014, com uma taxa aproximada de 10% de todo o malware da web encontrado.

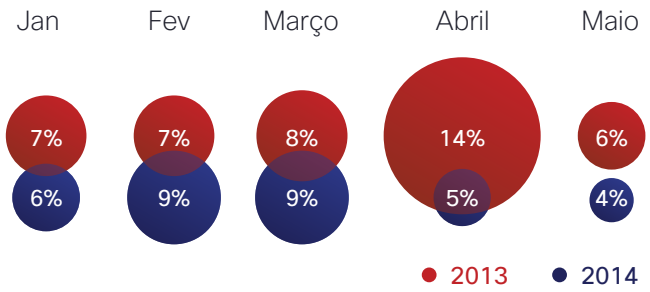


FIGURA 3

Descobertas de Java, PDF e Flash (janeiro a maio de 2014)

FONTE: Cisco Cloud Web Security

Java, Flash e Adobe PDF são vetores comuns para a atividade criminal.

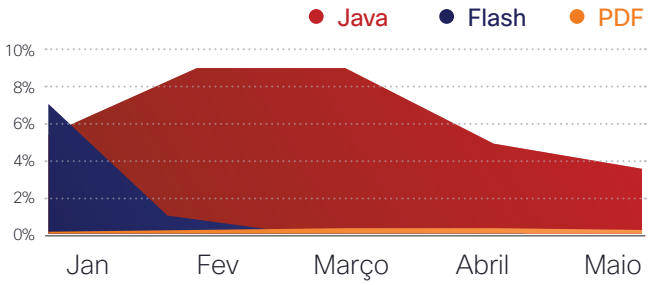
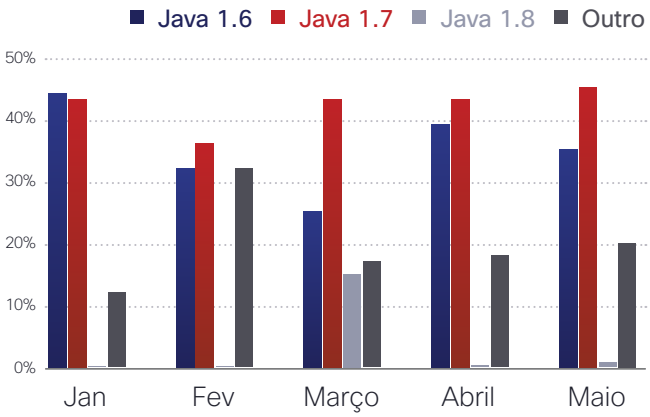


FIGURA 4

Descobertas de Java por versão (janeiro a maio de 2014)

FONTE: Cisco Cloud Web Security

Os adversários continuam obtendo sucesso na exploração de versões antigas do Java, principalmente as versões 6 e 7. Houve um aumento nas descobertas de malware na Web com o Java 8 em março, mês em que a nova versão foi lançada. Entretanto, as descobertas para o Java 8 diminuíram consideravelmente em abril e permaneceram muito baixas em maio. Com o aumento nos kits de exploração que dependem principalmente de vetores que não são do Java, como o Microsoft Silverlight, deveremos observar uma mudança a partir do Java 8 (que possui controles de segurança mais fortes) para outro software mais favorável a ataques.



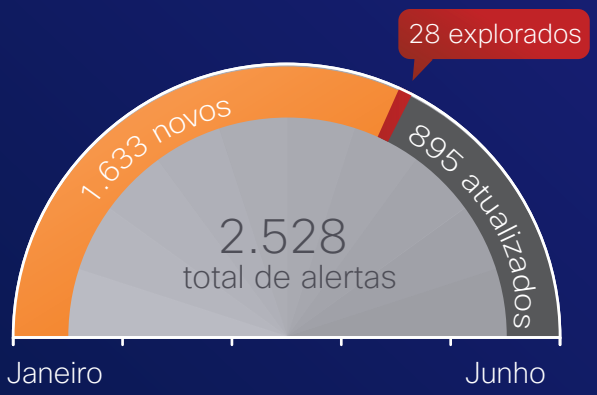
Atualização de vulnerabilidades: enfoque nas explorações mais comuns

FIGURA 5

Métricas de alerta (janeiro a junho de 2014)

FONTE: Cisco IntelliShield®

De 1º de janeiro a 30 de junho de 2014, a Cisco publicou milhares de alertas de diferentes fabricantes sobre as vulnerabilidades de segurança conhecidas. Embora esse número pareça intimidante, as vulnerabilidades extremamente graves representam cerca de 1% do total. De acordo com uma pesquisa da Cisco, dos 2.528 novos alertas de vulnerabilidade publicados durante esse período, somente 28 eram explorados ativamente após a publicação dos relatórios.



Os adversários se concentram em vulnerabilidades comuns ou "elos fracos" fáceis de serem explorados através de suas "pesquisas e desenvolvimentos". Depois, as explorações bem-sucedidas são incorporadas aos kits de exploração vendidos clandestinamente. As linguagens de programação Java e Silverlight são exemplos de vulnerabilidades que podem ser encontradas em diversos kits de exploração conhecidos. (Consulte Explorações da web: as explorações de Java continuam dominando os na página 15 e kits de exploração: o campo está aberto para a competição na página 33.)

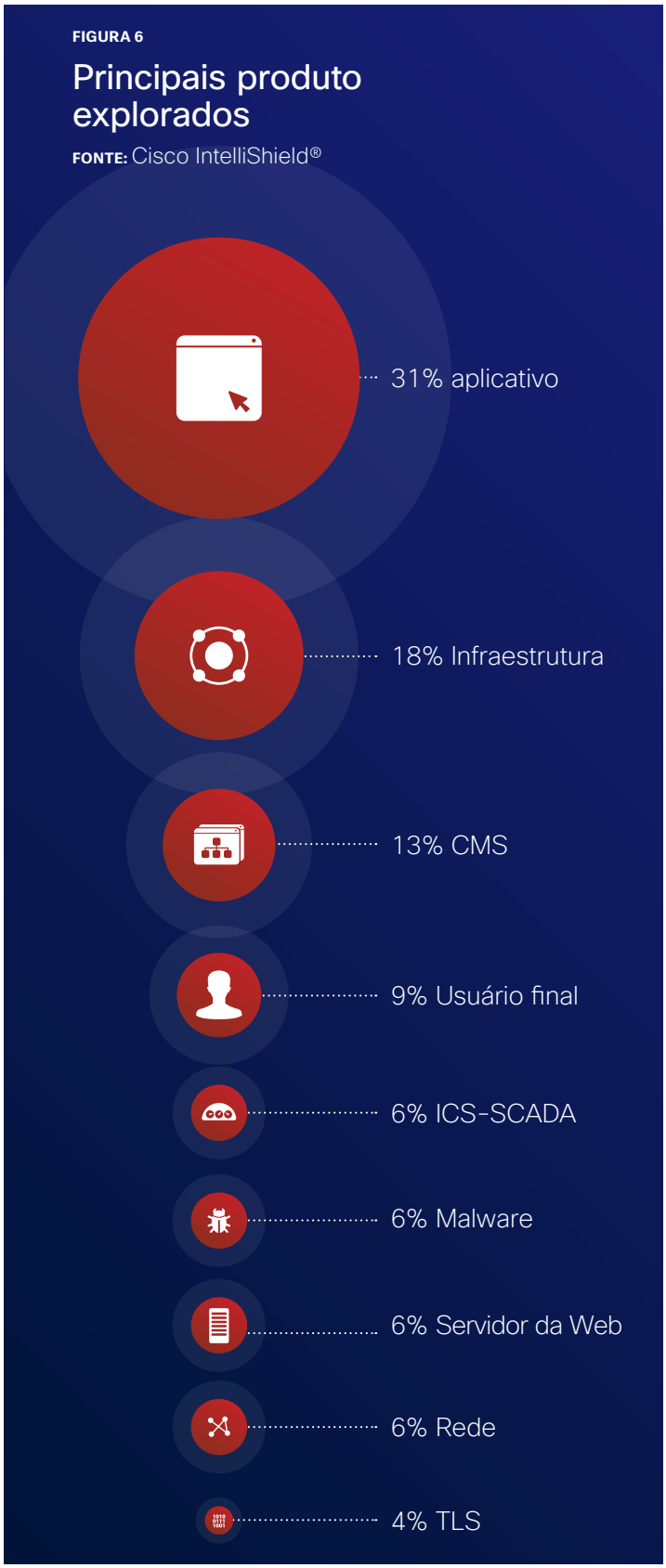
Todos os relatórios de vulnerabilidade são publicados e os profissionais de segurança e a mídia tendem a manter o foco em vulnerabilidades desconhecidas, pois há uma necessidade urgente de reagir a essas novidades de alta visibilidade. Entretanto, as empresas deveriam priorizar seus investimentos de tempo e dinheiro ao corrigir o pequeno número de vulnerabilidades que os criminosos estão explorando mais ativamente. Outras vulnerabilidades podem ser gerenciadas por processos mais rotineiros.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

FIGURA 6

Principais produto explorados

FONTE: Cisco IntelliShield®



Uma prática recomendada para as empresas é ter um "processo de correção urgente" que seria executado juntamente com os processos de correção padrão. Ao resolver rapidamente as principais vulnerabilidades direcionadas, as outras vulnerabilidades menos urgentes podem ser integradas no processo de correção e manutenção agendado regularmente. O resultado é um gerenciamento de risco mais preciso; melhor do que tentar instalar todos os patches ou não instalá-los até que cheguem os períodos de manutenção programados regularmente. É necessária uma forte inteligência de segurança para identificar vulnerabilidades urgentes e manter um processo de correção urgente de forma eficiente.

A figura 6 mostra os principais produtos explorados pelos invasores no primeiro trimestre de 2014. A figura 7 apresenta algumas das vulnerabilidades mais comuns de acordo com o Common Vulnerability Scoring System (CVSS).

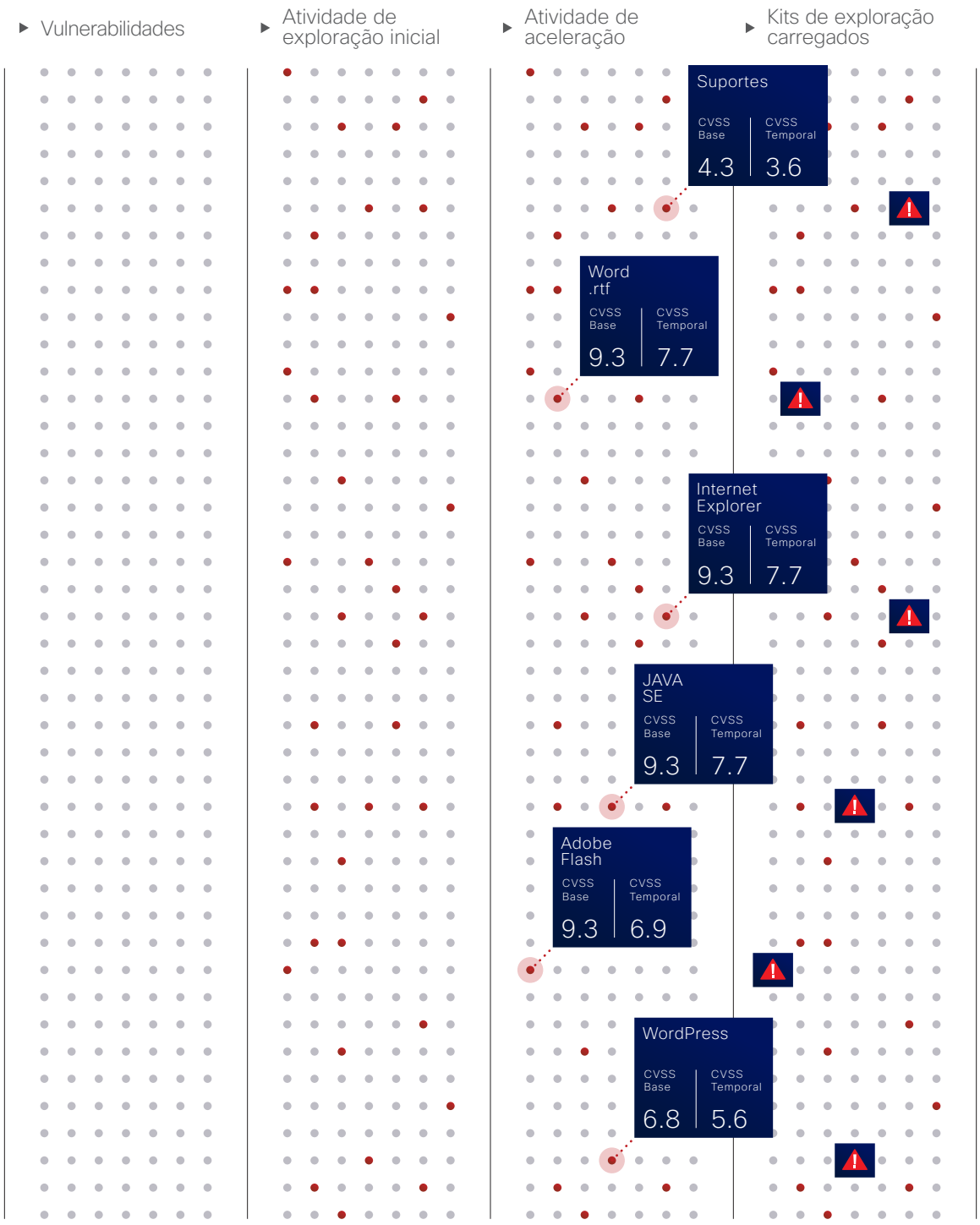
A pontuação "Urgência" no gráfico do CVSS é útil, pois indica que essas vulnerabilidades estão sendo exploradas ativamente, o que corresponde às pontuações "Temporais", indicando explorações ativas. Além disso, ao analisar a lista de produtos explorados, as empresas podem determinar quais estão sendo utilizados e quais precisam ser monitorados e corrigidos.

É importante entender que as vulnerabilidades na Figura 7 são as que indicam sinais iniciais de atividade de exploração durante o período observado. A maioria dessas vulnerabilidades ainda não foi integrada, o que significa que ainda não estão nos kits de exploração à venda.

FIGURA 7

Vulnerabilidades mais exploradas

FONTE: Cisco IntelliShield®



COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Heartbleed: não é a única causa de preocupações

Algumas empresas não foram expostas ao "Heartbleed bug"–uma vulnerabilidade de segurança na biblioteca de criptografia OpenSSL–, pois estavam usando uma versão antiga do OpenSSL que não incluía essa vulnerabilidade.[12] A vulnerabilidade envolve a implementação da extensão do heartbeat (RFC6520) Transport Layer Security (TLS) e pode permitir o vazamento de informações privadas ou senhas em comunicações criptografadas TLS.[13]

Entretanto, é importante que essas empresas saibam que de janeiro a abril de 2014 foram identificados 16 TLS e vulnerabilidades de validação de certificado *não* relacionadas ao Heartbleed.

Essas vulnerabilidades podem colocá-las em risco. Os especialistas em segurança da Cisco também recomendam que todos os usuários considerem a possibilidade de terem sido expostos a riscos devido ao Heartbleed e tomem ações apropriadas, como alterar as senhas ou fechar as contas da web.[14]

Desde que o Heartbleed foi descoberto, o projeto OpenSSL (OpenSSL.org) reportou várias outras falhas descobertas no software OpenSSL, e algumas delas "podem permitir que um invasor crie uma negação de condição de serviço ou, em determinadas situações, a execução de código remoto."[15] Algumas dessas falhas são erros há muito tempo esquecidos: por exemplo, a vulnerabilidade de injeção CCS, descoberta por um pesquisador de segurança no Japão, é uma falha de segurança que existe há 16 anos no software OpenSSL e que permite que um invasor intercepte e descriptografe dados na Internet.[16]

Relatório de riscos verticais do setor: aumentos incomuns para alguns setores

No primeiro semestre de 2014, o setor químico e farmacêutico, uma vertical com lucro elevado, mais uma vez foi classificado entre as três principais verticais de alto risco para descobertas de malware na web, ocupando o topo da lista em 2013.[17] O setor de aviação também aparece novamente entre os cinco primeiros, dessa vez assumindo o terceiro lugar da lista.[18] Isso não é surpresa devido ao valor da propriedade intelectual que acompanha o setor de aviação.

Enquanto isso, o setor de mídia e publicação, que está atualmente em primeiro lugar, está passando por um aumento consideravelmente superior em relação às taxas normais de descobertas de malwares na web, como observado pelos pesquisadores de segurança da Cisco, que compilaram esses dados desde 2008.

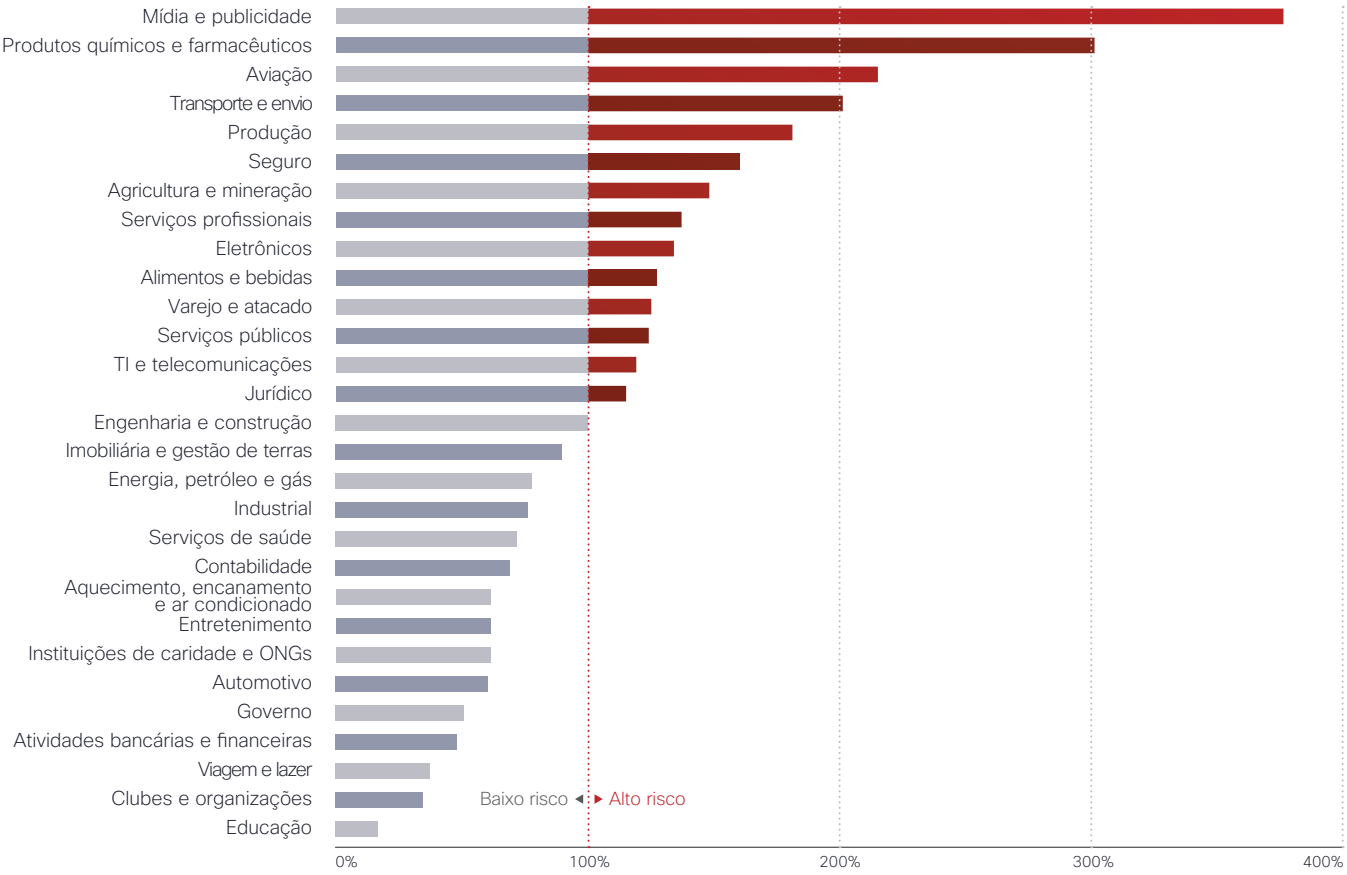
Os adversários que lançam explorações e outras fraudes em eventos de alta visibilidade, como os Jogos Olímpicos de Inverno de 2014 e o Oscar, e grandes acontecimentos recentes, como o mistério do voo 370 da Malaysia Airlines e o naufrágio na Coreia do Sul, são razões comuns para o aumento das descobertas no setor de mídia e publicação. Essas fraudes são criadas para tocar os pontos fracos das pessoas: os usuários são induzidos a clicar nos sites que hospedam os malwares, pois ficam curiosos ao ler as manchetes apelativas.

Sites de mídia e publicação, pequenos e grandes, podem atrair uma grande variedade de tráfego de empresas e clientes individuais em todo o mundo. Eles também dependem muito da propaganda para obter receita. Por esse motivo, é provável que o crescimento em malvertising seja parcialmente responsável pelo aumento das descobertas de malware na web no setor de mídia e publicação no primeiro semestre de 2014. (Consulte Malvertising: o problema da economia da Internet, página 35.)

FIGURA 8

Risco vertical de descobertas de malware na web, 1H14

FONTE: Cisco Cloud Web Security



Para determinar as taxas de descoberta de malware específicas do setor, os pesquisadores de segurança da Cisco comparam a média da taxa de descoberta de todas as empresas que se conectam através do proxy do Cisco Cloud Web Security com a média da taxa de descoberta de todas as empresas em um setor específico que se conectam através do proxy de serviço. Uma taxa de descoberta do setor acima de 100% reflete um risco maior que o normal para descobertas de malware na web, ao passo que uma taxa menor que 100% reflete um risco menor. Por exemplo, uma empresa com taxa de descoberta de 170% tem um risco 70% maior que a média. Da mesma maneira, uma empresa com taxa de descoberta de 70% tem um risco 30% menor que a média.

Descobertas de malware por região

Pela primeira vez, os pesquisadores de segurança da Cisco estão apresentando os dados de risco de uma descoberta de malware na web para verticais do setor de acordo com a região. As três regiões são definidas como AMER (América do Norte, América Central e América Latina), APJC (Ásia-Pacífico, China, Japão e Índia) e EMEAR (África, Europa e Oriente Médio).

Na região da AMER, conforme mostra a Figura 9, a aviação supera os outros setores na descoberta de malware na web com uma margem considerável.

O risco vertical em uma região específica é influenciado pelos seus produtos internos brutos. Normalmente, quanto maior o valor dos produtos e serviços, ou da propriedade intelectual, de uma vertical específica, maior o risco de descobertas de malware para aquele setor.

Uma vertical específica também pode ser sub-representada em uma região que normalmente não produz em um setor específico. Esse é o motivo para o risco "farm-to-table", geralmente enfrentado pelas empresas dos setores de transporte, agricultura, alimentos e bebidas. É por esse motivo que o setor de varejo de alimentos e bebidas observou o maior número de descobertas de malware na web na EMEAR. A seca, as enchentes e os problemas nessa região tiveram um efeito na disponibilidade de suprimentos básicos e na infraestrutura dos habitantes.

Descoberta x Comprometimento

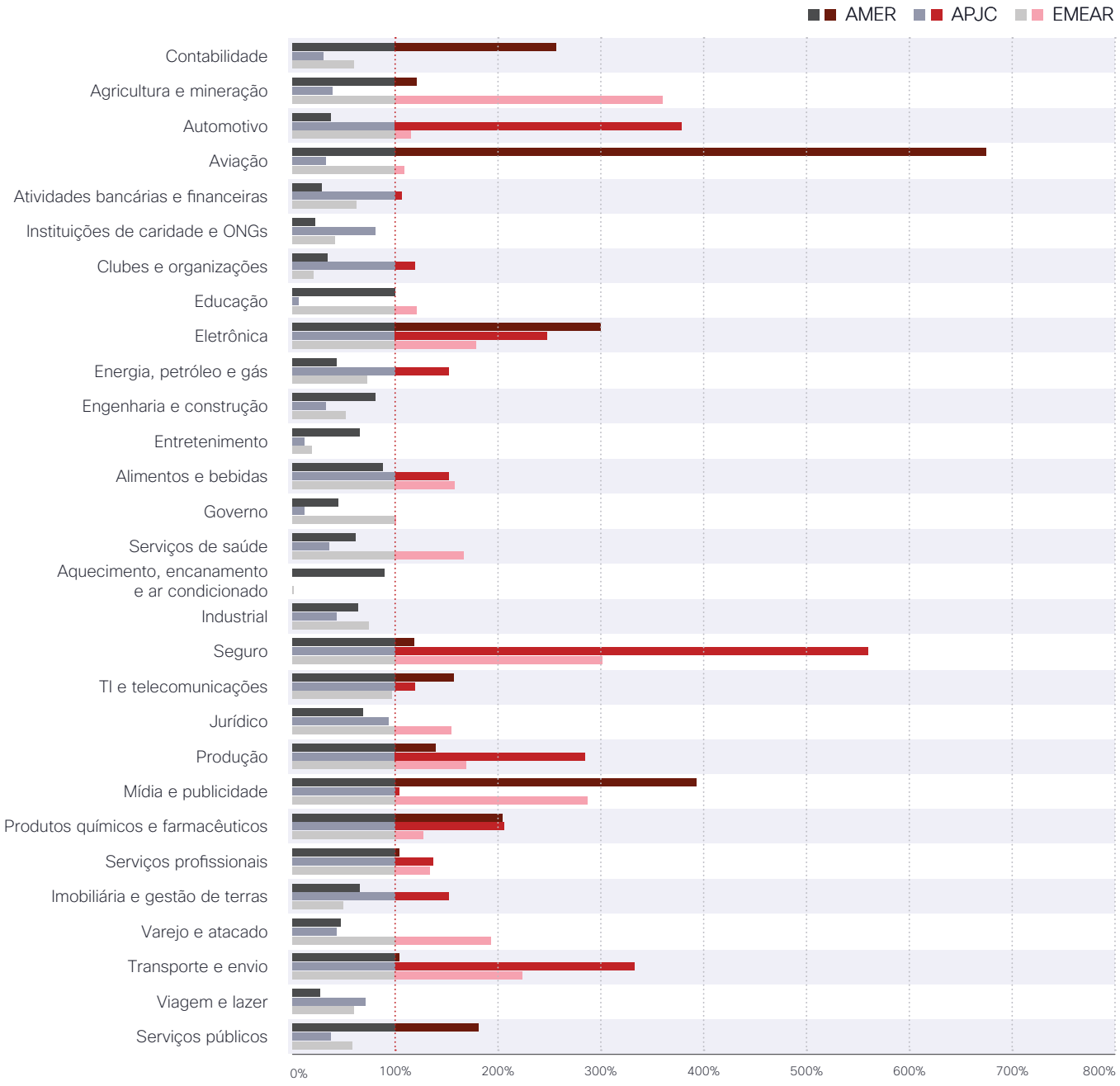
Uma "descoberta" é uma instância em que um malware é bloqueado. Diferente de um "comprometimento," um usuário não é infectado durante uma descoberta, pois não ocorre o download de um arquivo binário.

Na APJC, a maior vertical de risco era a de seguros, seguida pelas verticais farmacêutica, química e de eletrônicos. Os recentes eventos negativos na região da APJC, como terremotos, tsunami e o desastre nuclear no Japão em 2011, além do agravamento do mercado de seguros, são possíveis fatores para que o setor de seguros se torne um alvo para os adversários. Além disso, como o setor de seguros é um fornecedor de serviços para as principais corporações e outras entidades, agentes mal-intencionados podem estar planejando comprometer empresas de seguro como uma forma de obter informações confidenciais de clientes ou encontrar um caminho para suas redes e data centers.

FIGURA 9

Risco vertical de descobertas de malware na web por região

FONTE: Cisco Cloud Web Security



As cinco principais verticais de risco por região

A figura 10 apresenta detalhes das cinco principais verticais para cada região: AMER, APJC e EMEAR. iFrames e scripts mal-intencionados dominam todos os setores representados, embora agentes mal-intencionados nas três regiões pareçam estar dependendo muito de explorações para atingir setores específicos. Na APJC, golpes, phishing e fraudes do clique são usadas frequentemente para comprometer a confiança dos usuários nos setores de transporte e envio.

Parece que alguns adversários estão até mesmo tentando atingir as cinco principais verticais de risco em qualquer uma das três regiões com técnicas como ransomware e scareware ou vírus e worms. O índice de descoberta de malware na web móvel também é bem baixo para todas as regiões.

Os resultados desses gráficos têm como base principalmente o local onde os blocos de malware na web ocorreram (ou seja, as descobertas), de acordo com os dados do Cisco Cloud Web Security em relação aos tipos de ameaças na web.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

FIGURA 10

Risco vertical de malware na web

FONTE: Cisco Cloud Web Security

Atualização de spam: o spam “Life Event” se torna cada vez mais recorrente

Tradicionalmente, os criadores de spam dependiam de truques de engenharia social para convencer os destinatários a abrir suas mensagens e clicar nos links, geralmente levando a sites comprometidos ou a malware. As entregas de pacotes falsos ou taxas urgentes falsas são truques comuns, mas os profissionais de segurança agora veem uma nova tendência nos spams “life event” ou “misfortune”, que utilizam a emoção para obter resultados.

Por exemplo, o spam “life event” pode destacar o tratamento ou a recuperação de uma doença fatal, enquanto o spam “misfortune” pode mencionar despejos ou falências. Ambos podem exercer uma grande atração para que o destinatário clique na mensagem, muito mais do que uma mensagem sobre a entrega de uma encomenda.

Os spams “Life event” e “misfortune” atacam um elo fraco comum em proteções de segurança: o usuário, mesmo com treinamento em engenharia social, tende a responder detalhadamente sobre como amenizar infortúnios pessoais.

Assim como o combate de qualquer campanha de spam, a chave para atenuar o spam "life event" é o uso da tecnologia de bloqueio de spams, que pode ser atualizada dinamicamente.

Os spammers se tornam mais ágeis. Mude as abordagens para obter mais êxito

Os spammers são rápidos ao reagir a avanços de tecnologia que bloqueiam suas mensagens. Eles ajustam o texto, as imagens e os nomes de domínio para burlar os filtros de spam. E quando a eficácia da mensagem diminui, eles mudam tudo de novo.

Os pesquisadores de segurança da Cisco monitoram os tipos de spam e como as mensagens evoluem para informar aos clientes as novas táticas utilizadas pelos spammers para entrar nas redes ou roubar informações. Em alguns casos, as notas de cobertura para um tipo específico de spam – como uma notícia falsa sobre um pagamento eletrônico – podem ser atualizadas dezenas de vezes pelos pesquisadores da Cisco conforme os spammers mudam as táticas.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Volume global de spam quase duas vezes maior que a taxa normal, mas alguns países observaram uma forte queda

FIGURA 11

Volume global de spam (janeiro a março de 2014)

FONTE: Cisco Threat Intelligence Platform

Após uma queda geral em 2013, o volume global de spam vem aumentando desde outubro do ano passado. De acordo com uma pesquisa da Cisco, os volumes de spam aumentaram de tal maneira que o spam está agora no nível mais alto desde 2010. De junho de 2013 a janeiro de 2014, o spam estava em uma média de 50 a 100 bilhões de mensagens por mês. Entretanto, em março de 2014, os volumes atingiram uma marca superior a 200 bilhões de mensagens por mês, duas vezes maior do que as taxas normais.[19]

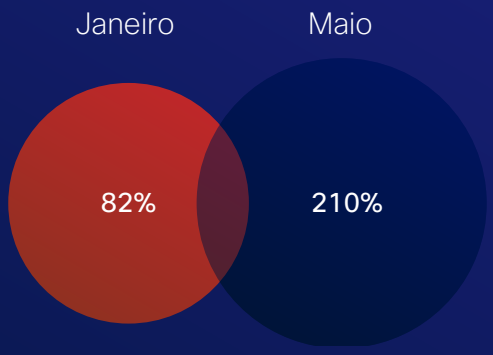
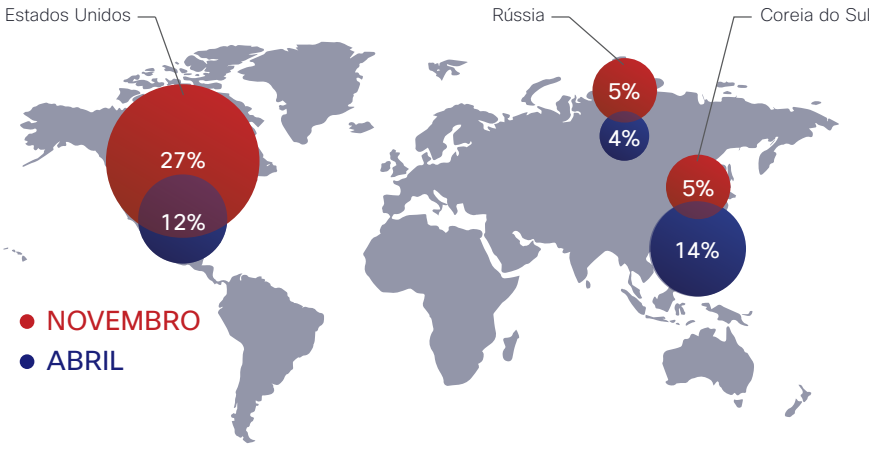


FIGURA 12

Tendências de volume por país (novembro de 2013 a abril de 2014)

FONTE: Cisco Threat Intelligence Platform

Embora o volume global de spam esteja alto, nem todos os países estão observando esse aumento. Na verdade, a Rússia e os Estados Unidos observaram grandes quedas no volume de spam desde novembro de 2013. Enquanto isso, a Coreia do Sul tem observado um pico considerável no volume de spam em relação aos outros 10 principais países monitorados pelos pesquisadores de segurança da Cisco.

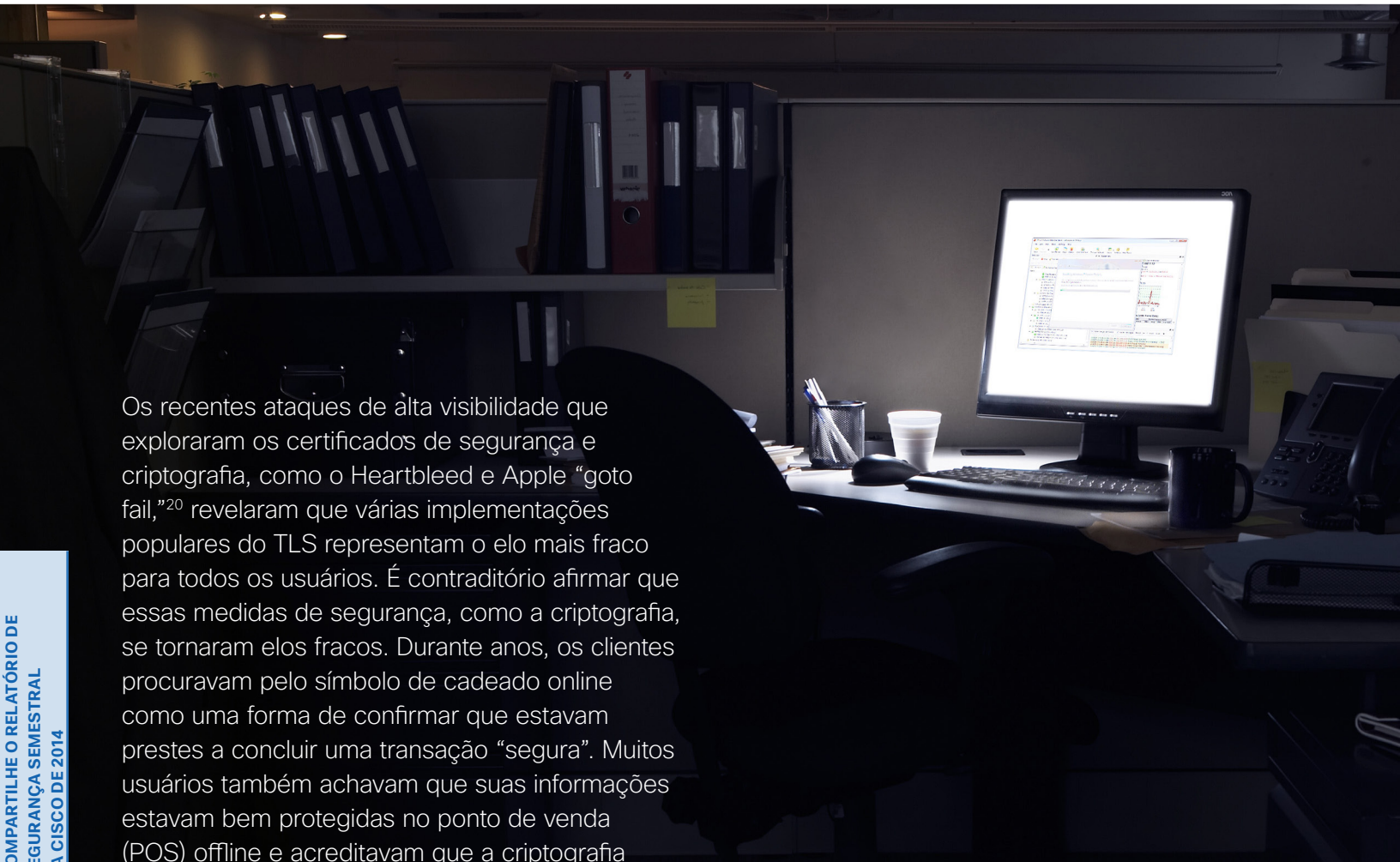


Argentina	2% | 7%	Alemanha	2% | 6%
China	11% | 5%	Irã	1% | 4%
Japão	2% | 7%	Espanha	3% | 7%
Reino Unido	2% | 4%		

Tendências do setor

Os especialistas em segurança da Cisco oferecem insight e análise sobre as ameaças e tendências de segurança observadas durante o primeiro semestre de 2014, bem como as projeções do que pode ser esperado nos próximos meses.

Segurança comprometida Conexões criptografadas



Os recentes ataques de alta visibilidade que exploraram os certificados de segurança e criptografia, como o Heartbleed e Apple "goto fail,"[20] revelaram que várias implementações populares do TLS representam o elo mais fraco para todos os usuários. É contraditório afirmar que essas medidas de segurança, como a criptografia, se tornaram elos fracos. Durante anos, os clientes procuravam pelo símbolo de cadeado online como uma forma de confirmar que estavam prestes a concluir uma transação "segura". Muitos usuários também achavam que suas informações estavam bem protegidas no ponto de venda (POS) offline e acreditavam que a criptografia estava sendo aplicada de ponta a ponta – isso se chegassem a pensar sobre esse aspecto.

Entretanto, o que os últimos seis meses mostraram é que não importa o quão atentos ou cuidadosos sejam os usuários, ou quantas soluções de segurança estejam sendo usadas; os elos fracos vão além dos seus controles e ainda podem representar um grande risco.

Enfrentar o problema de conexões criptografadas com segurança comprometida é sem dúvida uma obrigação para qualquer empresa que receba pagamentos. Isso requer uma análise mais detalhada dos processos do setor que ajudam a levar a criptografia e outros problemas de segurança ao mercado.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

O Heartbleed e eventos similares destacam que várias empresas que usam conexões criptografadas seguras e tecnologia relacionada partem do princípio que:

- Os protocolos criptografados com base em códigos abertos conhecidos e padrão oferecem segurança robusta.
- Todos os códigos fonte incorporados em serviços e produtos de segurança, inclusive o código que era fornecido por terceiros, foram completamente analisados pelos especialistas em segurança.

Nenhuma suposição está correta, mas ambas participam da implementação bem-sucedida de ataques como o Heartbleed, que aproveitam as vulnerabilidades e outras falhas de segurança e exploram a confiança dos usuários.

Melhorar os processos do setor não será fácil. No estado atual, de acordo com os especialistas da Cisco, o OpenSSL é complexo. É difícil implementá-lo corretamente e testá-lo contra as vulnerabilidades. O processo atual de análise de código-fonte aberto e código proprietário requer uma abordagem mais robusta, mas quem deveria desenvolver e manter essa abordagem? Essa questão permanece em aberto. Enquanto isso, a comunidade de segurança está debatendo se o sistema de autoridade de certificado violado pode ser corrigido.

No mundo da segurança, a simplicidade é primordial. Diminuir a quantidade de códigos que precisam ser confiáveis é uma etapa importante ao fazer as implementações de segurança. Os especialistas em segurança da Cisco acham que para melhorar as bibliotecas de segurança SSL/TLS de código aberto será necessário, no mínimo:

- Reduzir a complexidade dos protocolos e suas implementações
- Validar a implementação correta do código, sem vulnerabilidades e falhas ocultas
- Verificar se aqueles que testam e validam o código são qualificados

Um resultado positivo dos eventos recentes, como o Heartbleed: muitas pessoas na comunidade do desenvolvedor estão procurando proativamente seus códigos para encontrar e corrigir falhas. A Linux Foundation anunciou recentemente a formação da Core Infrastructure Initiative, que "permite que empresas de tecnologia identifiquem de forma colaborativa e financiem projetos de código-fonte aberto que precisam de assistência. Além disso, permite que os desenvolvedores continuem seus trabalhos de acordo com normas da comunidade que tornaram o código-fonte aberto um sucesso."[21] O OpenSSL foi um dos primeiros projetos que recebeu recursos financeiros da Core Infrastructure Initiative. A Cisco é uma das financiadoras na iniciativa.

Ataques de ampliação: adversários sincronizados com NTP

Os especialistas em segurança da Cisco alertaram, no *Relatório de Segurança Anual da Cisco de 2014*, que os ataques de DDoS, por exemplo, lançados através da ampliação DNS, permaneceriam como uma das principais preocupações de segurança nas empresas em 2014.[22] Mas, mesmo antes disso, os pesquisadores da Cisco afirmaram que o NTP, criado para sincronizar os relógios dos computadores em uma rede, era um elo fraco e pronto para se tornar um vetor para os ataques de DDoS ampliados. Eles embasaram suas projeções ao observar que as ferramentas de ataque criadas para utilizar o número cada vez maior de servidores NTP vulneráveis estavam começando a ser distribuídas na comunidade de hackers.[23]

FIGURA 13

Ataque de DDoS CloudFlare NTP, 2014

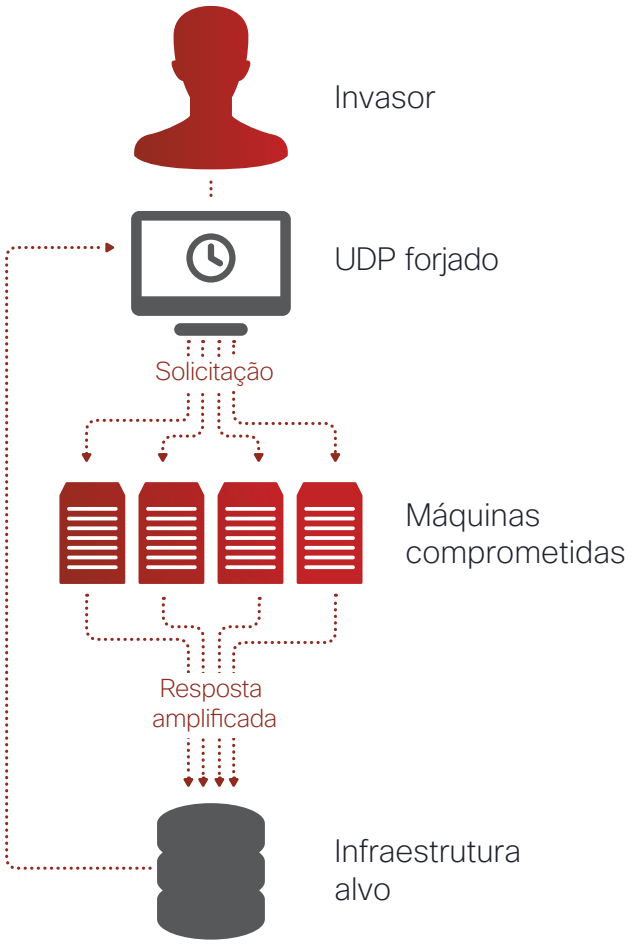
FONTE: Cisco Threat Intelligence Platform

Um dos ataques de amplificação de NTP mais significativos do primeiro semestre de 2014 foi direcionado ao cliente de um provedor global de DNS, o CloudFlare (consulte a figura 13). Em seu pico, o ataque de fevereiro atingiu quase 400 Gbps de tráfego UDP, superando o ataque de DDoS Spamhaus, de março de 2013, com 300 Gbps, que envolveu 30.000 resolvedores de DNS aberto.[24]

É fácil entender por que alguns agentes estão testando o NTP como uma ferramenta para seus ataques de DDoS: OpenNTPProject.org, um projeto de varredura NTP criado para aumentar a conscientização em relação ao problema do NTP, identificou mais de 1 milhão de servidores NTP vulneráveis.[25] Em conjunto, a largura de banda desses servidores é bem maior do que qualquer outro ataque de DDoS visto até hoje.

FIGURA 14

Execução de um ataque NTP



COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Para executar um ataque de ampliação de NTP, o adversário envia pequenas solicitações para máquinas NTP vulneráveis, forjando o endereço do pacote UDP, para que as solicitações pareçam estar vindo do destino que o invasor está tentando assumir offline. O UDP é stateless. A habilidade de forjar o endereço UDP é um componente necessário para os ataques de ampliação DNS e NTP. Os servidores NTP envolvidos no ataque retornam uma resposta muito grande para pequenas solicitações, enviando todas as informações de volta ao destino cujas máquinas estão inundadas e offline. (Há iniciativas do setor para evitar o UDP spoofing, que precisam continuar.)

É necessário atualizar servidores NTP públicos para a versão mais recente do NTP para evitar um possível ataque de ampliação NTP. Atualmente, essa versão é a 4.2.7. Essa atualização elimina o suporte para comando MON_GETLIST ou “monlist”, que é um comando remoto que retorna os endereços das últimas 600 máquinas com as quais um servidor NTP interagiu. Se não for possível atualizar, usar a opção *noquery* na configuração NTP também evitará as consultas de monlist.

Ainda que os ataques de ampliação de NTP façam parte de um novo tipo de ataque de DDoS, espera-se que a ampliação de DNS continue a ser uma técnica de referência para vários de nossos adversários. Segundo o Projeto Open Resolver, em outubro de 2013 cerca de 28 milhões de resolvedores apresentavam ameaças significativas.[26]

Kits de exploração: o surgimento da concorrência

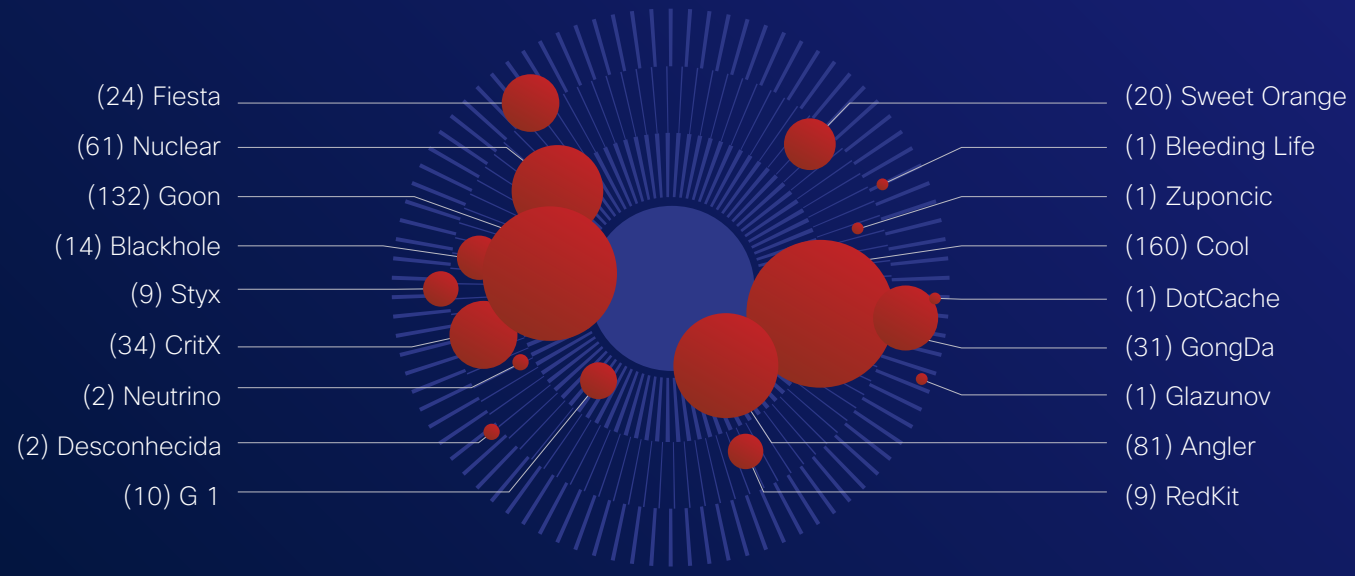
Quando o "chefe do malware e suposto criador e distribuidor do kit de exploração Blackhole, conhecido como Paunch" foi preso na Rússia, em outubro de 2013,[27] não demorou muito até que os criadores de outros kits de exploração começassem a ocupar o território antes dominado por ele.

O Blackhole era sem dúvida o kit de exploração mais utilizado e bem conservado. Quando Paunch e o Blackhole tiveram suas atividades interrompidas pelo governo, nossos adversários voltaram suas atenções para os novos kits de exploração. Segundo os pesquisadores de segurança da Cisco, tivemos muitos candidatos competindo pelo lugar de destaque durante o primeiro semestre de 2014. Contudo, um líder ainda estava por vir.

FIGURA 15

Kits de exploração observados desde janeiro de 2014

FONTE: Cisco Threat Intelligence Platform



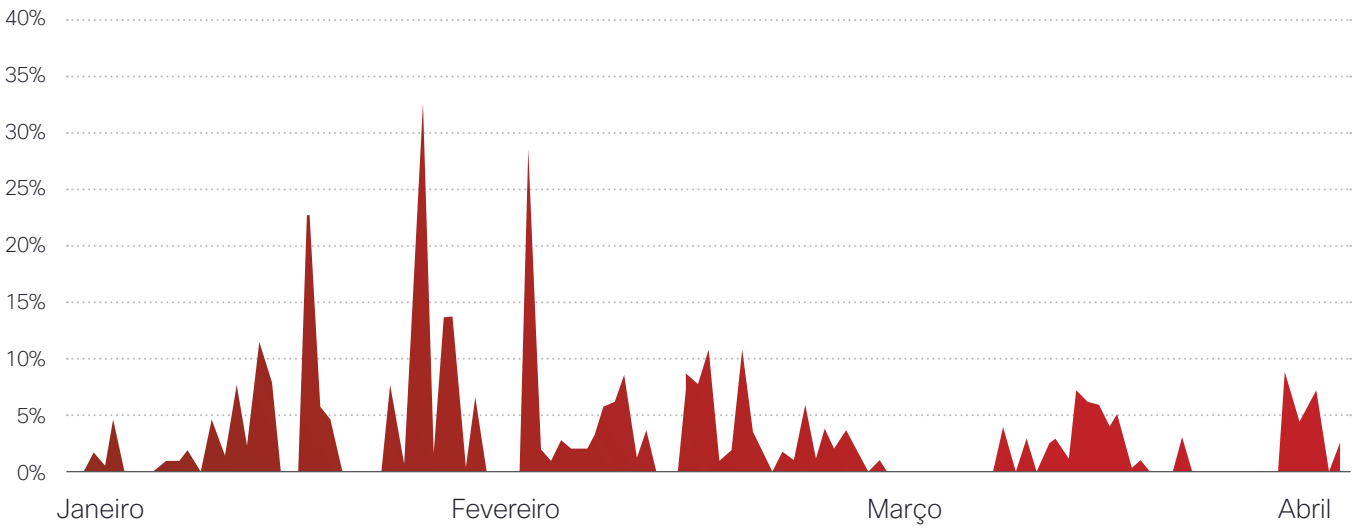
(número de ataques) Nome do kit de exploração

Apesar da competição acirrada, o número de kits de exploração diminuiu 87% desde a prisão de Paunch no ano passado, segundo os pesquisadores de segurança da Cisco (consulte a Figura 16).

FIGURA 16

Diminuição do número de kits de exploração (janeiro a abril de 2014)

FONTE: Cisco Threat Intelligence Platform



Os invasores também estão usando os kits de exploração para campanhas mais direcionadas e sofisticadas, visando comprometer usuários já definidos com o objetivo de descobrir vulnerabilidades em aplicativos, programas e sistemas que funcionam como caminho direto para a infraestrutura. Por exemplo, os kits de exploração "LightsOut" ou "Hello" têm como alvo específico o setor de energia.

Malvertising (publicidade maliciosa): um problema para a economia da Internet

O gasto com publicidade virtual ultrapassou todas as outras formas de mídia.[28] Tendo em vista o começo tímido da publicidade virtual (um simples anúncio em banner em Hotwired, no ano de 1994), é um crescimento impressionante para apenas duas décadas. Apesar de incomodar os usuários, a publicidade virtual é importante pois permite que as pessoas consumam livremente tudo que é disponibilizado na Web. Se esse modelo for alterado ou as pessoas perderem a confiança em toda a publicidade virtual, as repercussões para a Internet seriam catastróficas.

"Malvertising", a publicidade online que espalha malware, ameaça justamente esse modelo de publicidade e a confiança dos usuários. Ele afeta todos os usuários e interrompe a economia da Internet. Segundo os especialistas de segurança da Cisco, o malvertising ressalta o nível de sofisticação da economia de crimes cibernéticos modernos em termos da divisão do trabalho, cooperação e especialização em toda a cadeia de ataque.

O malvertising está se tornando cada vez mais predominante, e nossos adversários são capazes de lançar campanhas altamente direcionadas. Um criador de malvertising que deseja direcionar o ataque a uma população específica e durante um período determinado (por exemplo, os torcedores de futebol alemães que estão assistindo a uma partida da Copa do Mundo) pode utilizar um ad exchange legítimo para realizar esse ataque. Assim como os anunciantes legítimos, eles entram em contato com empresas que agem como guardiãs dos ad exchanges. Esses criadores de malvertising pagam à vista pelo anúncio (valores em torno de US$ 2.000 ou mais pelo tempo de publicação) e instruem as empresas a venderem os ad exchanges para que atuem como anúncios o mais rápido possível, fazendo com o que o conteúdo do anúncio não seja devidamente inspecionado.

As vítimas de malvertising são afetadas pelo malware enquanto navegam pela Internet, e por isso não sabem identificar o local e o momento em que foram infectadas. Rastrear a origem do ataque é quase impossível, uma vez que o anúncio que continha o malware já desapareceu.

Anúncios realmente nocivos: o papel do malvertising no Ransomware

Conforme relatado no ***Relatório de Segurança Anual da Cisco de 2014***, o malvertising desempenhou papel decisivo na distribuição do ransomware CryptoLocker. O ransomware é tão sinistro quanto parece: trata-se de um tipo de malware que criptografa os arquivos nos computadores das vítimas, e só reverte a ação quando o regaste é pago.[29]

O CryptoLocker foi neutralizado recentemente: O Departamento de Justiça dos EUA anunciou em junho que estava trabalhando juntamente com as autoridades policiais de outros países e com empresas de tecnologia para interromper um gigantesco botnet com dois anos de atividade conhecido como "Gameover Zeus", um dos maiores distribuidores do CryptoLocker.[30] Mas não demorou muito até que uma nova marca de ransomware, a "CryptoWall", ocupasse o seu lugar.

Durante o primeiro semestre de 2014, os pesquisadores da Cisco dissecaram as campanhas de ataque que utilizam a web, especialmente aquelas onde o malvertising redireciona o usuário para sites que hospedam kits de exploração - sejam eles alugados ou comprados pelo adversário - que então forçam um "instalador" nos sistemas dos usuários e infectam os pontos vulneráveis do sistema. Como parte da pesquisa, os especialistas de segurança da Cisco analisaram altos níveis de tráfego compatíveis com um novo kit de exploração, conhecido como "RIG". Esse kit foi observado pela primeira vez em fóruns criminosos, em abril de 2014.[31] O RIG utiliza o malvertising para realizar um ataque drive-by em usuários que estão visitando sites legítimos e bastante conhecidos. O kit de ferramentas do ataque está sendo usado por adversários para a distribuição do ransomware CryptoWall.

Desde junho, a Cisco já havia bloqueado solicitações de vários sites WordPress comprometidos que foram redirecionados para malvertising.

(Consulte Vulnerabilidades no WordPress: quem está vigiando o forte?, na página 37.)

As páginas de destino dos sites hospedam explorações para Java, Flash e o protocolo multimídia do Microsoft Silverlight. Segundo os pesquisadores da Cisco, a utilização desse último plug-in para ajudar a lançar explorações parece estar ganhando espaço na comunidade de crimes cibernéticos. Em 2013, o Fiesta foi o primeiro kit de exploração a integrar uma exploração para o Silverlight. O RIG e um outro kit de exploração, o Angler, logo seguiram a tendência e mantiveram a natureza competitiva do mercado de kits de exploração. (Consulte Kits de exploração: o surgimento da concorrência, página 33.)

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Vulnerabilidades no WordPress: quem está vigiando o forte?

Empresas de todos os portes usam o WordPress, um software da web que é basicamente uma coletânea de scripts e complementos que possibilitam ao usuário fazer o que quiser com seus sites: criar um blog, hospedar fóruns, administrar e-commerce e muito mais.

O WordPress foi projetado para ser funcional, não seguro.

A maioria dos usuários do WordPress não possui o conhecimento ou as habilidades para utilizá-lo de forma segura. E não é raro um usuário configurar um site com o sistema de gerenciamento de conteúdo (CMS) do WordPress ou outros sistemas similares e depois abandoná-lo.

Existem vários sites como esses na Web, que são elos fracos em uma cadeia de segurança. Os invasores que conseguem violar esses sites esquecidos podem carregar binários mal-intencionados e usá-los como sites de exploração. Os usuários se deparam com esses sites quando estão navegando em outros sites ativos e legítimos (mas que também foram comprometidos); um iFrame extrai o conteúdo do site abandonado e o coloca nos sites legítimos que o usuário está acessando.

O WordPress não é o único CMS com esse problema, mas se destaca de sites como o Joomla e o e107 por ser mais conhecido. Sites abandonados apresentam um alto risco para a segurança da Internet e, como não há ninguém vigiando o forte, é mais difícil limpar esses sites ou tirá-los do ar. Mesmo que os proprietários dos sites queiram fazer algo, a maioria apenas corrige o ponto de entrada e não verifica se os sites já foram comprometidos. Eles não encontram a porta dos fundos e tiram-na de seus sites.

A maioria dos provedores de hospedagem oferece serviços de instalação do WordPress de baixo custo e gerenciados para sites comerciais como parte do pacote de hospedagem. Os provedores garantem a aplicação de todos os patches e a execução correta de todas as configurações de segurança. Quanto mais pessoas utilizarem esse tipo de serviço, menor será o número de sites que apresentam vulnerabilidades no WordPress.

Ataques de POS: vetor de ameaças conhecido para criminosos que buscam dados de cartões de crédito

Diversos cruzamentos de tendências tornaram os sistemas de ponto de venda (POS) um local atraente para os criminosos que estão atrás de grandes quantidades de dados de cartões de crédito. Violações de segurança recentes em varejistas conhecidos apontam para o fato de que esses tipos de ataques podem ser bem-sucedidos e rápidos. Examinar os recursos de detecção antes de um ataque aos dados de cartões de crédito é uma ação sensata, assim como a redução de janelas de remediação durante e após um ataque.

Os ataques envolvem o roubo de dados armazenados nas tarjas magnéticas dos cartões de crédito. Uma vez roubados, esses dados podem ser usados para criar cartões falsos, que serão então usados em compras na loja. O malware em POS permite a extração de dados da memória, causando a evasão dos dados criptografados dos discos ou da rede. As tendências que estão tornando essa exploração possível em uma escala maior incluem:

Conexão com a Internet do POS

A probabilidade cada vez maior de que os sistemas de ponto de venda (POS) estejam conectados à Internet, o que oferece aos criminosos um ponto de entrada para as redes empresariais.

Falta de compreensão

A falta de compreensão por parte de muitas empresas, que não consideram informações de cartões de crédito como dados importantes, o que faz com que essas informações sejam menos protegidas

Fornecedores terceirizados

A utilização cada vez maior de fornecedores terceirizados para todas as soluções de POS ou parte delas, disponibilizando ainda mais pontos de acesso para os criminosos.

Dados armazenados em cartões de crédito são produtos altamente valiosos no mercado criminoso e oferecem um alto retorno de investimento. Criminosos acreditam que é mais fácil roubar dados dos sistemas de POS do que roubá-los diretamente dos vendedores de e-commerce; os bancos estão mais capacitados para detectar e impedir esse tipo de roubo.

Além disso, como os Estados Unidos são uma das poucas principais economias cujos cartões de crédito ainda possuem tarjas magnéticas em vez do sistema mais seguro de "chip e PIN", é mais fácil lucrar com os dados armazenados neles. (Porém, sem a criptografia de ponta a ponta dos dados do cartão, os números e datas de validade ainda podem ser roubados e utilizados em transações online, mesmo com sistemas de chip e PIN.)

Monitoramento básico dos dados de cartões de crédito

Para prevenir o roubo de dados de cartões de crédito e outras informações confidenciais em um POS, as empresas devem investir mais em barreiras tecnológicas que evitam a entrada de criminosos. Elas também precisam compreender que dados de cartões de crédito devem receber mais atenção dos profissionais de segurança.

Algumas empresas optaram por adicionar dispositivos de criptografia de hardware aos POS; isso pode ajudar a evitar que dados de cartões de crédito sejam interceptados enquanto navegam pela rede. Caso esse gasto seja considerado muito alto, as empresas devem ao menos marcar esses dados como "críticos" e monitorá-los para detectar acessos não autorizados e movimentações irregulares. As empresas devem supor que os invasores já são capazes de entrar em uma rede, visto que há diversas maneiras de comprometê-la.

Os indícios de comprometimento (IOCs) mais óbvios que podem esclarecer o possível roubo de dados de cartões de crédito são a importação de um conjunto de ferramentas, um novo processo de execução em um terminal de POS e a extração de arquivos de dados com tamanhos e frequências uniformes. Os sistemas que podem analisar esses comportamentos em toda a extensa rede devem ser considerados.

Também é interessante realizar a detecção de alteração de processo e aplicativo em todos os sistemas de processamento de pagamentos com cartões. Qualquer alteração em um endpoint deve ser considerada motivo para uma análise imediata. Além disso, ainda que a maioria dos protocolos costume usar a compactação para ganhar velocidade e eficácia, as ferramentas de compactação devem ser parte das "listas brancas do aplicativo".

Por último, as redes devem ser segmentadas para que as empresas não facilitem o acesso dos criminosos às coleções de dados valiosos: os sistemas de POS devem ficar localizados em um segmento de rede separado da rede corporativa para limitar o acesso e dinamizar os ataques nos sistemas POS.

Com a popularização e proliferação dos dispositivos móveis na rede corporativa, a segmentação deve incluir recursos robustos de identidade que sejam capazes de detectar quem é o usuário, o tipo de dispositivo e o método que estão sendo usados para acessar a rede. Por exemplo, o acesso à rede LAN sem fio do campus de uma empresa por meio de um laptop de propriedade da empresa pode ser permitido, e o acesso remoto à VPN por meio de um tablet pode ser negado devido à confidencialidade dos dados de POS.

A Cisco espera que os invasores que estão atrás de dados de cartões de crédito continuem a concentrar seus esforços nos sistemas de POS. Contudo, a detecção cuidadosa e os sistemas de alerta, além da implementação da criptografia de hardware, podem evitar que esses esquemas sejam colocados em práticas.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

Engenharia social: como encontrar os elos fracos pessoalmente

Uma empresa pode pagar centenas de milhares de dólares (ou até mais) por softwares de segurança modernos e achar que está protegida contra ataques direcionados que começam na rede. Porém, se a ameaça for uma pessoa real entrando pela porta da frente de um escritório ou de uma torre de servidores, qual a vantagem de ter um software de borda de rede?

Criminosos inteligentes conseguem maiores lucros ao aparecer no local com o objetivo de entrar em uma rede fisicamente, em vez de criar e-mails de phishing com links que levam a sites comprometidos. (Sem contar que o spam e outras campanhas de engenharia social online já estão ultrapassados; consulte a página 26 para obter mais detalhes.) O simples fato de conseguir entrar em uma conexão Ethernet ou desconectar o telefone IP e usar o mesmo cabo para acessar as informações de rede pode ter consequências graves. A engenharia social é o ato de hackear pessoas. Portanto, as pessoas – seus funcionários – tornam-se o elo mais fraco da sua postura de segurança digital e física.

Os criminosos usam táticas similares de engenharia social em uma visita presencial, semelhantes às usadas em e-mails e sites comprometedores. A intenção é conquistar a confiança (apesar de enganosa) de alguém que pode acessar as instalações da empresa.

Ao pesquisar um funcionário-alvo no LinkedIn – por exemplo, descobrindo todas as informações, desde suas funções no trabalho até onde cursou a faculdade e os times favoritos – o criminoso pode se apresentar como um conhecido ou alguém que inspire confiança.

Devido à popularidade das redes sociais, especialmente entre os profissionais, há diversas informações e fotos facilmente disponíveis para qualquer pessoa que precise literalmente entrar pela porta.

Armado com um histórico obtido em pesquisas online, um criminoso pode fingir ser um jornalista e solicitar uma entrevista, ou alegar ser um possível parceiro ou cliente e solicitar uma visita presencial. O criminoso também pode usar um crachá falso para parecer uma autoridade.

Os criminosos também descobriram que não é necessário aplicar esses golpes na porta da frente da empresa-alvo. Em vez disso, eles se voltarão para o elo mais fraco, ou seja, um parceiro empresarial mais vulnerável ou um fornecedor que tenha acesso ao alvo real, que é a rede. Essa é uma técnica especialmente eficaz para ser usada quando a segurança de um alvo é alta, mas quando o mesmo não acontece com a segurança de um parceiro empresarial confiável. Os hackers sempre tentarão encontrar a melhor rota de entrada.

Garantir que as portas de acesso à rede apliquem a autenticação e a autorização antes de conceder acesso à rede é uma forma de abordar as violações de segurança com base em engenharia social que envolvem a obtenção de acesso à rede física. Além disso, as empresas podem criar “domínios de segurança dinâmicos” por usuário, por dispositivo, por usuário e dispositivo ou com qualquer outra configuração necessária. Esses domínios de segurança dinâmicos podem usar tecnologias como 802,1x, lista de controle de acesso à porta (ACLs), VPN e avaliação de postura do host.

Solução

Seja qual for o método de acesso usado pelo invasor (com fio, sem fio ou VPN), os profissionais de TI podem criar dinamicamente um domínio de segurança ou “bolha” feita somente para eles. Se o criminoso conectar um laptop a uma porta no próprio local, a rede vai barrar a pessoa, vai autenticá-la, gerar um perfil, avaliar sua postura, observar seu comportamento e, em seguida, oferecer àquele usuário direitos de autorização muito específicos e dinâmicos que restringem o acesso à rede com base em uma política contextual.

Um olhar para o futuro

Os especialistas em segurança da Cisco oferecem conselhos sobre como as empresas podem melhorar a segurança ao visualizá-la como um processo empresarial, aumentar o diálogo entre os líderes de tecnologia e comerciais da empresa e usar novas soluções de tecnologia que oferecem mais visibilidade às ameaças cada vez mais difíceis de serem detectadas.

Segurança cibernética inteligente para o mundo real

Reforçar os elos fracos em toda a cadeia de segurança depende da habilidade de cada empresa e setor compreender o risco cibernético e tornar a segurança cibernética um fator essencial à empresa, partindo da diretoria. Também é fundamental alinhar a estratégia empresarial, as operações de segurança e os controles que permitem a resiliência cibernética, além da capacidade de criar maior visibilidade da rede no meio de toda a "turbulência" ao empregar soluções novas e inteligentes, como a análise preditiva.

Para oferecer cobertura antes, durante e após uma sequência de ataque, as empresas devem abordar uma ampla variedade de vetores de ataque, com soluções de segurança que operam em qualquer local em que a ameaça possa se manifestar. Isso inclui a rede e dispositivos móveis, virtualmente e na nuvem ou no data center.

Redução de falhas de segurança—sejam elas vulnerabilidades conhecidas e ativamente exploradas em Java, Flash ou Adobe PDF; sites abandonados criados no WordPress; falhas de segurança ignoradas há muito tempo no software OpenSSL; acesso físico desprotegido a redes ou servidores NTP vulneráveis—e a dificuldade gerada por produtos distintos e soluções desarticuladas na tentativa de oferecer mais segurança a todos os usuários. Para garantir a resiliência da rede de dar respaldo à empresa, também é fundamental avaliar o status do ciclo de vida dos dispositivos de rede descobertos, as possíveis vulnerabilidades de segurança e a versão do sistema operacional.[32]

A estratégia da Cisco para ajudar as empresas a lidar com esses desafios de segurança novos e conhecidos tem como base três mandamentos estratégicos:

Determinada pela visibilidade

Quanto mais observarmos, mais poderemos correlacionar as informações e aplicar a inteligência para compreender o contexto, tomar decisões melhores e agir de forma manual ou automática.

Com enfoque nas ameaças

Precisamos nos concentrar na detecção, compreensão e interrupção das ameaças por meio de análise contínua e inteligência de segurança em tempo real oferecida pela nuvem e compartilhada em toda as soluções de segurança para aumentar a eficiência.

Na plataforma

Atualmente, a segurança é mais do que um problema de rede. Ela exige um sistema integrado de plataformas ágeis e abertas que englobam os dispositivos de rede e a nuvem.

A segurança cibernética inteligente do mundo real ajudará a proteger a Internet das Coisas, além de formar a base da Internet de Todas as Coisas, onde a segurança, assim como a computação, serão eficientes e onipresentes, além de ilimitadas para os usuários finais.

Operacionalizar a segurança: tornar a segurança um processo empresarial

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

As avaliações de segurança frequentemente revelam que a causa de um problema de segurança é uma falha operacional ou técnica da empresa. A falta de maturidade e/ou de recursos operacionais gera controles de segurança fracos ou inexistentes.

À medida que a segurança cibernética se torna um risco estratégico para as empresas, há um enfoque cada vez maior na obtenção da "maturidade nas operações de segurança", onde a empresa tem uma perspectiva holística dos riscos e está melhorando constantemente as práticas da segurança cibernética.

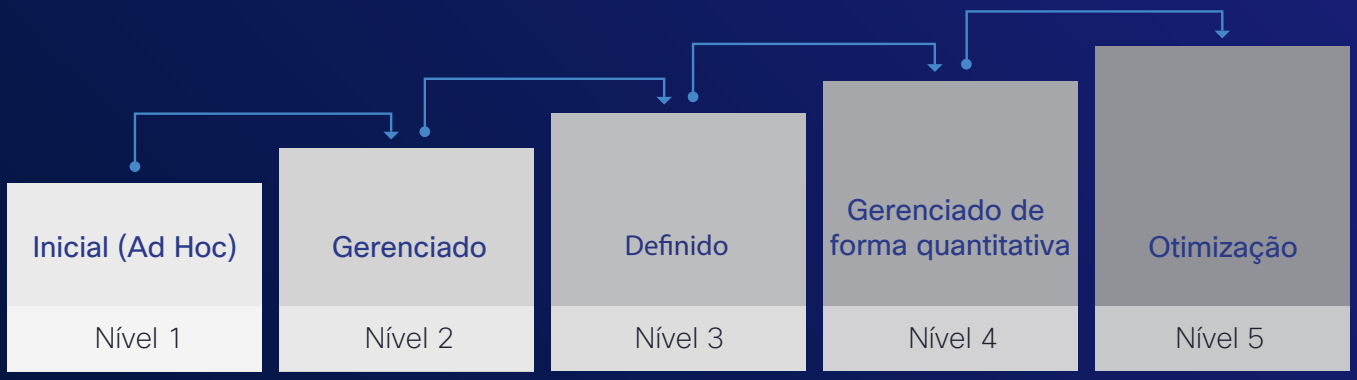
Com a ajuda dos provedores de serviço nesse espaço, muitas empresas trabalham para tornar a segurança um processo, ou conjunto de processos, empresarial altamente padronizado e mensurável, que é analisado regularmente para garantir que os objetivos estratégicos estão sendo atingidos. A decisão de encarar a segurança como um processo empresarial frequentemente surge de iniciativas de negócios mais amplas, projetadas para melhorar a governança, o risco e a conformidade (GRC) em toda a empresa. Muitas empresas descobrem, frequentemente tarde demais, que quando se trata de segurança de TI, a conformidade não é suficiente.

As empresas que operacionalizam a segurança compreendem melhor os seguintes aspectos:

1. O que eles precisam proteger
2. Qual é a eficiência das medidas de segurança atuais
3. O que é necessário realizar em relação à segurança cibernética

FIGURA 17

Modelo CMMI



A operacionalização da segurança gera melhor visibilidade do que está acontecendo com a segurança de TI em toda a empresa: quais funcionários são responsáveis por ela, se são as pessoas certas para lidar com essa responsabilidade e, caso sejam, se trabalham de modo eficiente. As empresas que operacionalizam a segurança também podem determinar se os recursos de TI estão sendo implantados e usados de modo eficaz.

Um componente essencial da operacionalização da segurança é o diálogo produtivo entre os líderes de segurança, como diretores de informação (CIOs) e diretores de segurança da informação (CISOs) e líderes empresariais. Esses dois grupos de liderança precisam trabalhar em estreita colaboração para transformar a segurança cibernética em um processo empresarial formal e definir os níveis aceitáveis de risco, além de estabelecer as metas estratégicas relacionadas à segurança da empresa. Para ajudar a direcionar esse diálogo, os CISOs precisam apresentar as informações sobre segurança cibernética de forma clara aos líderes empresariais; métricas, por exemplo, podem ajudar a mostrar a importância das etapas que a empresa deve adotar para evitar um risco específico de segurança cibernética.

A operacionalização da segurança também deve seguir um “modelo de maturidade”. O Capability Maturity Model Integration (CMMI) da Carnegie Mellon é um exemplo. Esse modelo bastante usado começou como um projeto no Instituto de Engenharia de Software da universidade nos anos 80. Conforme apresentado na Figura 17, o ponto de início do modelo de maturidade é a fase “ad hoc”, que é essencialmente um modo de “combate a incêndios”. Quando alcançar a última fase, a empresa estará usando processos padronizados e reproduzíveis que podem ser medidos.

Compreensão do risco cibernético em termos empresariais

Muitas empresas estão apostando o futuro dos seus modelos corporativos na conectividade universal que o mundo da Internet das Coisas promete. Mas, para estar preparado e prosperar nesse ambiente de rápida expansão, a liderança executiva deve compreender, em termos empresariais, os riscos cibernéticos associados à dependência cada vez maior da rede.

Há muito tempo a postura de muitas empresas tem sido não discutir os problemas de segurança cibernética em público, mas isso está mudando. Vários líderes empresariais estão começando a compreender que os riscos de segurança cibernética são desafios comuns para todas as empresas, especialmente à medida em que se tornam cada vez mais digitalizadas e os recursos de informações se transformam em ativos estratégicos.

Esses executivos também começam a compreender que, no ambiente da Internet das Coisas, deve haver um diálogo transparente dentro da empresa, entre as empresas (incluindo concorrentes) e entre os setores públicos e privados para abordar as ameaças e as melhores práticas para atenuá-las. O aumento da pressão dos diretores, que procuram compreender os efeitos comerciais dos riscos da segurança cibernética, tem ajudado a desenvolver esse ponto de vista a partir dos cargos de chefia.

Ações recentes dos EUA: A Securities and Exchange Commission (SEC) ajudou a tornar a segurança cibernética um tópico de destaque para os conselhos de diretores. A SEC emitiu requisitos de relatório de segurança cibernética para empresas públicas em 2011,[33] exigindo que essas empresas informem às partes interessadas as “instâncias significativas de furto ou ataque cibernético, ou mesmo quando estão sob risco material devido a esses eventos.”[34] A SEC também realizou uma mesa redonda no início desse ano “para discutir a segurança cibernética e os problemas e desafios que afetam participantes do mercado e empresas públicas, e como eles estão lidando com essas preocupações.”[35]

No cenário global, o World Economic Forum (WEF), uma instituição internacional comprometida com a melhoria da situação mundial por meio de parceria público-privada, apresentou o seu conceito de “resiliência cibernética” em 2011, como forma de ajudar a levar a segurança cibernética e outros problemas relacionados à Internet ao nível de diretoria. O WEF promove a resiliência cibernética como um ecossistema interdependente, em que cada empresa é tão forte quanto o mais fraco dos seus elos. Isso é descrito em um dos quatro princípios orientadores da iniciativa "Parceria para resiliência cibernética" do WEF[36]:

Todos somos tão fortes quanto o mais fraco dos elos da cadeia dos quais dependemos; cada um de nós contribui para a segurança do nosso mundo hiperconectado. Um espaço online aberto, seguro e resiliente é um bem público; todos os agentes compartilham a responsabilidade de criação e suporte desse recurso.

COMPARTILHE O RELATÓRIO DE SEGURANÇA SEMESTRAL DA CISCO DE 2014

A iniciativa de resiliência cibernética do WEF foi projetada para ajudar os diretores executivos e outros líderes com cargo de chefia, incluindo CIOs e CISOs, a conduzir discussões sobre segurança cibernética em suas empresas e falar sobre riscos e oportunidades cibernéticas. Por exemplo: "qual é o custo para a empresa se decidirmos não investir em uma tecnologia geradora de valor, devido às preocupações sobre o risco cibernético?"

FIGURA 18

Modelo de maturidade para a resiliência empresarial

Para atingir a resiliência cibernética as empresas devem adotar uma abordagem baseada em risco para a segurança cibernética, de acordo com o WEF, sendo válida para qualquer empresa que procure melhorá-la. A instituição oferece esse modelo de maturidade, que mostra um caminho para a resiliência cibernética.

Por meio dessa iniciativa, o WEF enfatiza que a segurança cibernética não é algo que possa ser obtido por um departamento em uma empresa, especialmente o de TI. Isso ocorre porque os recursos cibernéticos não são apenas técnicos, mas também institucionais. Além disso, o WEF ressalta que promover a conscientização da segurança cibernética na empresa é responsabilidade dos diretores, que também são responsáveis por ajudar a empresa a atingir a resiliência cibernética.

Análise preditiva: um detetive que oferece mais segurança

É um ciclo vicioso: o setor de segurança cria uma resposta específica à ameaça cibernética, e os invasores descobrem novas maneiras de evitar a detecção. Os adversários trabalham de modo proativo para compreender quais tipos de soluções de segurança estão sendo implantadas e mudar para padrões de comportamento com menor nível de detecção de conteúdo e menor visibilidade, para que as suas ameaças possam estar bem ocultas. Hoje em dia, as ameaças não são tão facilmente detectadas pelas soluções e pelos profissionais de segurança. Existe um tráfego mais codificado e criptografado, e maior randomização por parte dos agentes mal-intencionados, que buscam tornar os comportamentos de comando e controle indistinguíveis do tráfego real.

A falta de visibilidade que as empresas têm das redes "turbulentas" de hoje em dia significa que as ameaças onipresentes têm vários esconderijos. Para superar a turbulência e compreender se há algo de anormal em uma rede, primeiro é necessário saber o que é o "normal". A análise preditiva é um recurso de detecção em desenvolvimento, que oferece exatamente esse tipo de visão prática e também ajuda as empresas a aumentar a resiliência de suas soluções de segurança. É uma ferramenta projetada para detectar comportamentos incomuns em uma rede (ou seja, os sintomas de uma infecção) por meio da análise comportamental e da detecção de anomalias.

Com a análise preditiva, as empresas podem avaliar o comportamento de entidades (servidores de host e usuários) em suas redes. Um modelo, derivado de vários modelos menores e de uma representação concisa de comportamentos passados, é criado e usado para prever como as entidades devem se comportar no futuro. Em condições ideais, os dados são correlacionados na nuvem para aumentar a velocidade, a agilidade e a intensidade da detecção de ameaças. Os dados serão sinalizados para investigação caso haja discrepância expressiva ou prolongada em seu comportamento.

A análise preditiva ajuda a tornar as técnicas de segurança já utilizadas mais exatas, bem como mais capazes de detectar comportamentos desconhecidos ou incomuns na rede. Ela requer algoritmos de tomada de decisão avançados, que analisam diversos parâmetros e captam dados do tráfego em tempo real; os recursos de aprendizagem automática permitem que o sistema aprenda e se adapte com base no que é visualizado.

Os sistemas de aprendizagem automática funcionam como detetives. Eles procuram locais suscetíveis a ataques e evidências de um incidente que já ocorreu, está prestes a ocorrer ou já está ocorrendo. Ainda que não tratem da aplicação de segurança ou política, os sistemas de aprendizagem capacitam outros sistemas para encontrar ameaças inesperadas e realizar a aplicação. Para proporcionar vantagens e ajudar as empresas a aumentar a eficácia da segurança, a análise preditiva deve ser implementada junto com soluções de segurança dependente de conteúdo, soluções de gerenciamento de perímetro e soluções de gerenciamento de política.

Sobre a Cisco

A Cisco oferece segurança cibernética inteligente para o mundo real. Essa visão tem como base uma abordagem que enfoca ameaças à segurança e que diminui a complexidade e oferece mais visibilidade, controle contínuo e proteção contra ameaças avançadas em toda a sequência de ataque. Com esse modelo de segurança centrado em ameaças, as empresas podem agir com rapidez antes, durante e depois de um ataque.

Os pesquisadores de ameaças do ecossistema de Inteligência de segurança coletiva da Cisco usam o conhecimento de comandos e os sofisticados sistemas de big data para apoiar a descoberta, a análise e a proteção de ameaças conhecidas e em desenvolvimento. Os renomados especialistas em segurança da Cisco contam com infraestrutura e sistemas sofisticados que oferecem visibilidade única da agregação e da análise da incomparável telemetria de bilhões de solicitações e e-mails da Web, milhões de amostras de malware, conjuntos de dados de fonte aberta e milhares de invasões de rede da Cisco.

O resultado disso é a "big intelligence": uma rede de informações que oferece eficácia superior de segurança e protege de maneira imediata e profunda as redes ampliadas em todo o mundo.

Para obter mais informações sobre a abordagem de segurança com enfoque em ameaças da Cisco, visite www.cisco.com/go/security.

Notas finais

1 *Estimating the Cost of Cyber Crime and Cyber Espionage*, Center for Strategic and International Studies (CSIS), julho de 2013: https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.

2 "Internet of Things", Cisco.com: http://www.cisco.com/web/solutions/trends/iot/overview.html.

3 "Internet of Things" infographic, Cisco Internet Business Solutions Group: http://share.cisco.com/internet-of-things.html.

4 "Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel," por Andy Greenberg, *Forbes*, 12 de Agosto de 2013: http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

5 "Hackers Reportedly Targeted Three Large Medical Device Makers", iHealthBeat.com, 11 de fevereiro de 2014: www.iheace-lthbeat.org/articles/2014/2/11/hackers-reportedly-targeted-three-large-medical-devimakers.

6 "How secure is your baby monitor? What can happen when the 'Internet of Things' gets hacked", por Matt Hartley, *Financial Post,* 03 de maio de 2014: http://business.financialpost.com/2014/05/03/how-secure-is-your-baby-monitor-what-can-happen-when-the-internet-of-things-gets-hacked/?__lsa=bc1b-f93e.

7 "The Internet of Everything, Including Malware", por Craig Williams, blog da Cisco Security, 4 de dezembro de 2014: http://blogs.cisco.com/security/the-internet-of-everything-including-malware/.

8 O foco deste relatório é destacar o número de FQDNs, domínios, sites, entre outros que podem ser mal-intencionados e que são provenientes do cliente.

9 *Relatório de Segurança Anual da Cisco de 2014:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

10 Clientes interessados em participar do compartilhamento direto de inteligência do programa AEGIS da Equipe de pesquisa de vulnerabilidades devem enviar um e-mail para threatintel@cisco.com.

11 Ibid.

12 Para obter mais informações sobre o Heartbleed, acesse www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

13 "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations", por Pano Kampanakis, blog da Cisco Security, 9 de abril de 2014: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations.

14 Para obter mais informações sobre a redução de riscos da vulnerabilidade Heartbleed do OpenSSL, consulte "Cisco Event Response: Vulnerabilidade Heartbleed do OpenSSL CVE-2014-0160", 22 de abril de 2014, Cisco.com: www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

15 "New OpenSSL Defects – Another Heartbleed? Tor Stripped?" por James Lyne, *Forbes*, 5 de junho de 2013: www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed.

16 "Severe OpenSSL Security Bug Uncovered by Japanese Researcher Months After Heartbleed", por Luke Villapaz, *International Business Times*, 5 de junho de 2014: www.ibtimes.com/severe-openssl-security-bug-uncovered-japanese-researcher-months-after-heartbleed-1594989.

17 *Relatório de Segurança Anual da Cisco de 2014:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

18 Ibid.

19 "Spam Hits Three Year High-Water Mark", blog da Cisco Security, 2 de maio de 2014: http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

20 "Major Apple security flaw: Patch issued, users open to MITM attacks", por Violet Blue, blog "Zero Day", *ZDNet*, 22 de fevereiro de 2014: http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/.

21 "Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects", comunicado de imprensa, Linux Foundation, 24 de abril de 2014. Para obter mais informações sobre a Iniciativa, acesse http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel

22 *Relatório de Segurança Anual da Cisco de 2014:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

23 "When Network Clocks Attack", por Jaeson Schultz, blog da Cisco Security blog, 10 de janeiro de 2014: http://blogs.cisco.com/security/when-network-clocks-attack/.

24 "Chronology of a DDoS: A Spamhaus", por Seth Hanford, blog da Cisco Security, 28 de março de 2013: http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/.

25 Para descobrir se seu servidor NTP é vulnerável, acesse openntpproject.org. Para obter mais informações sobre as melhores práticas de DNS, consulte "Melhores práticas de DNS, proteções de rede e identificação de ataques": http://www.cisco.com/web/about/security/intelligence/.

26 Projeto Open Resolver: www.openresolverproject.org.

27 "Meet Paunch: The Accused Author of the Blackhole Exploit Kit", por Brian Krebs, blog KrebsOnSecurity, 6 de dezembro de 2013: http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.

28 "Global Internet Ad Spend Sees Double-Digit Growth, Outpaces Other Media," *Nielsen,* 10 de Julho de 2012: http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+(Nielsen+Wire).

29 *Relatório de Segurança Anual da Cisco de 2014:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

30 "Malicious Advertisements on Major Websites Lead to Ransomware", por Jeremy Kirk, IDG News Service, 6 de junho de 2014: http://www.pcworld.com/article/2360820/malicious-advertisements-on-major-websites-lead-to-ransomware.html.

31 "RIG Exploit Kit Strikes Oil", por Andrew Tsonchev, blog da Cisco Security, 5 de junho de 2014: http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/.

32 Network Barometer Report: A gauge of global networks' readiness to support business, *Dimension Data,* 2013: http://www.dimensiondata.com/Global/Documents/Network%20Barometer%20Report%202013.pdf.

33 "CF Disclosure Guidance: Tópico nº. 2: Cybersecurity", Division of Corporation Finance, SEC, 13 de outubro de 2011: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

34 "Cybersecurity: SEC outlines requirement that companies report data breaches", por Ellen Nakashima e David S. Hilzenrath, *The Washington Post,* 14 de outubro de 2011: http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQArGjskL_story.html.

35 "Mesa redonda sobre segurança cibernética", SEC: http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

36 Para obter mais informações sobre a iniciativa de resiliência cibernética criada pela Parceria WEF, acesse http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience.

CISCO