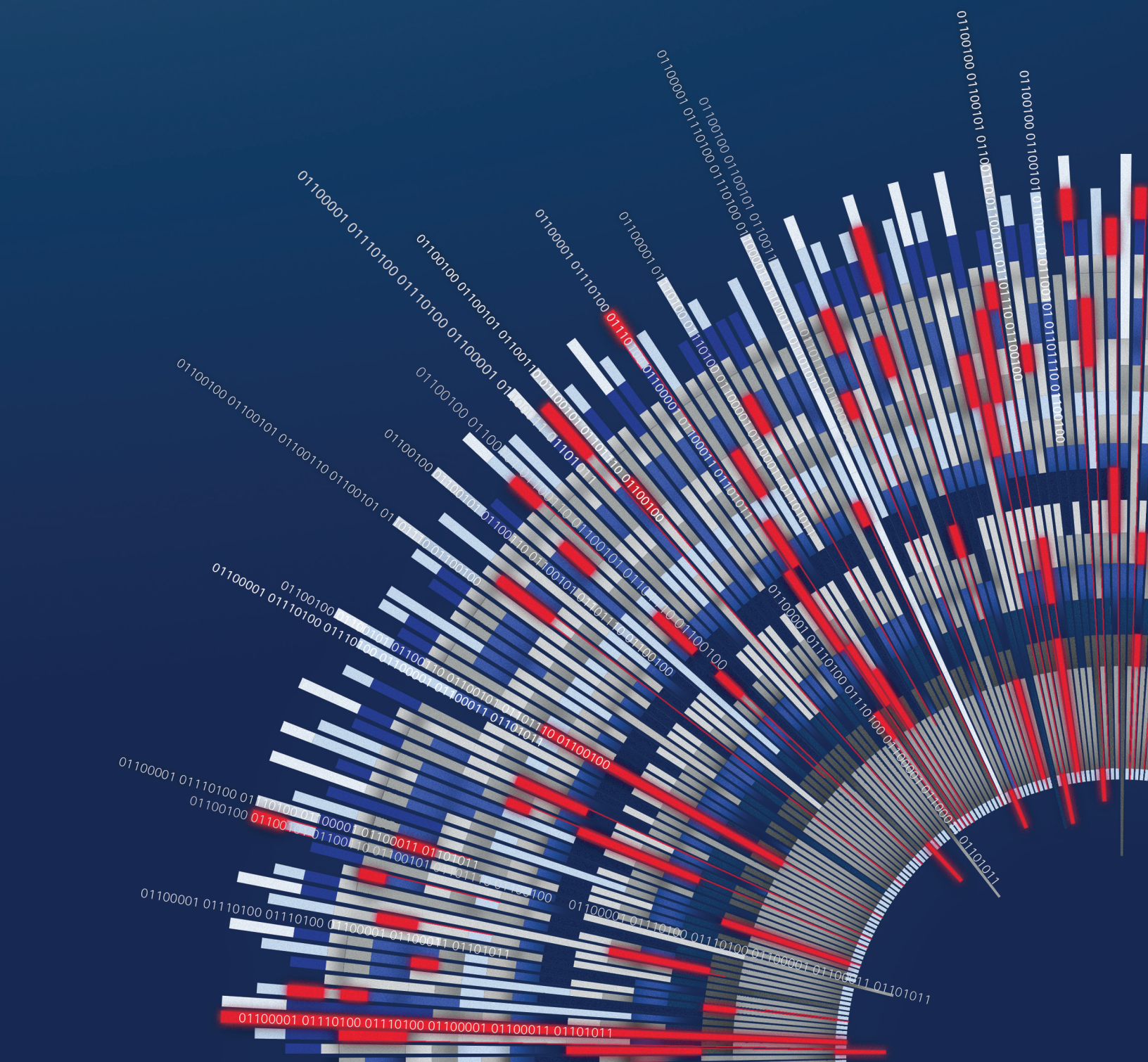
Cisco 2015

Relatório semestral sobre segurança



Resumo executivo

O setor de segurança está com dificuldades em acompanhar o ritmo de inovações imposto por criminosos cibernéticos, que desenvolvem e implantam malwares, burlam as defesas da rede e impedem a detecção, cada vez melhor e mais rapidamente.

Essa dinâmica cria um grande problema para as empresas que investem em serviços e produtos de segurança: para resolver falhas na segurança, geralmente elas acabam escolhendo soluções isoladas que só criam mais pontos fracos em suas defesas contra ameaças.

O Relatório semestral sobre segurança da Cisco de 2015 examina esses desafios cruzados e disponibiliza atualizações sobre as ameaças mais perigosas. Com base na pesquisa realizada pelos nossos especialistas, ele apresenta uma visão geral das principais ameaças observadas na primeira metade de 2015. Esse relatório também explora as prováveis tendências futuras e orienta empresas de pequeno, médio e grande porte que estão em busca de serviços e soluções de segurança.

O relatório está dividido em duas áreas principais:

Inteligência de ameaças

Esta seção apresenta uma visão geral da mais recente pesquisa sobre ameaças da Cisco. Discutiremos:

- Atualizações de kits de exploração, como o Angler
- O uso cada vez maior, por parte dos criminosos, de macros envolvendo o Office
- Novas táticas dos autores de malware para escapar da detecção
- Risco de detecções de malware para determinados mercados verticais
- Tempo para detecção de ameaças
- Atualizações sobre spams, alertas de ameaças, explorações de Java e malvertising (publicidade mal-intencionada)

Análise e observações

Nesta seção, vamos abordar a consolidação do setor de segurança e o conceito emergente de defesa integrada contra ameaças. Outros tópicos em foco são: a importância de desenvolver confiança e segurança nos produtos e a importância de mobilizar empresas de serviços de segurança em um mercado com escassez de especialistas nesse setor. Por fim, vamos debater como uma estrutura coesa de administração cibernética pode ser um passo para a sustentação da inovação empresarial e do crescimento econômico no cenário mundial.

Principais descobertas

Os criminosos continuam a inovar quando entram nas redes sem serem percebidos e escapam das medidas de segurança.

- As vulnerabilidades do Adobe Flash são cada vez mais exploradas. É comum que elas sejam integradas a kits de exploração amplamente difundidos, como Angler e Nuclear.
- Em termos de eficácia e sofisticação geral, o Angler segue na liderança do mercado de kits de exploração.
- Os operadores de crimeware, como ransomware, contratam e financiam equipes de desenvolvimento profissional para ajudá-los a assegurar que suas táticas permaneçam lucrativas.
- Os criminosos estão se voltando para a rede anônima Tor e I2P (Projeto Internet Invisível) para transmitir comunicados de comando e controle, escapando da detecção.
- Mais uma vez, os criminosos fazem uso das macros do Microsoft Office para distribuir malware. Essa é uma antiga tática que caiu em desuso, mas que tornou-se popular entre agentes maliciosos que buscam novas maneiras de anular proteções de segurança.
- Alguns autores de kits de exploração estão incluindo passagens do romance clássico *Razão e Sensibilidade*, de Jane Austen, nas páginas de destino da Web que hospedam seus kits de exploração. É muito provável que os antivírus e outras soluções de segurança categorizem essas páginas como legítimas após a "leitura" desse texto.
- Os autores de malware usam cada vez mais técnicas, como a detecção de sandbox, para ocultar sua presença nas redes.
- O volume de spams cresceu nos Estados Unidos, na China e na Federação Russa, mas se manteve relativamente estável em outras regiões nos primeiros cinco meses de 2015.
- O setor de segurança está mais alerta para a atenuação de vulnerabilidades em soluções de código aberto.
- Seguindo uma tendência abordada no Relatório anual sobre segurança da Cisco de 2015, as explorações envolvendo Java apresentaram queda na primeira metade de 2015.

Índice

Introdução

Introdução

As táticas desenvolvidas por autores de malware e criminosos cibernéticos vêm demonstrando uma sofisticação cada vez maior nos últimos anos. Relatórios recentes de segurança da Cisco apontaram essa inovação na economia paralela, como também o esforço dos profissionais de segurança para ficarem à frente dos criminosos.

A novidade é a capacidade cada vez maior dos agentes de ameaças de inovar rapidamente e aumentar seu poder de comprometer sistemas e escapar da detecção. Na primeira metade de 2015, talvez a principal característica dos invasores on-line seja a disposição para desenvolver novas ferramentas e estratégias – ou reciclar antigas – que permitam se esquivar das defesas de segurança. Por meio de táticas como ofuscação, eles não só conseguem passar pelas defesas de rede, mas também realizar as explorações muito antes de serem detectados – se é que serão.

Os fornecedores de segurança também estão respondendo com suas próprias inovações. Por exemplo, os pesquisadores estão tornando compatíveis a análise de novos formatos, como .cab e .chm, pois novos ataques são detectados usando esses formatos. Além disso, os fornecedores desenvolvem novos mecanismos de detecção e avaliam e aprimoram a heurística constantemente.

Os fornecedores de segurança sabem que precisam manter a agilidade. Se eles ou suas redes baixarem a guarda, ainda que por pouco tempo, os invasores assumirão o controle. O ritmo de inovação do setor, porém, não é tão rápido quanto deveria.

Muitos fornecedores oferecem soluções fragmentadas ou isoladas para problemas de segurança. E os compradores – ou seja, as empresas que compram ferramentas de segurança dos fornecedores – estão em busca de produtos paliativos, em vez de soluções estratégicas profundas. Como eles não integram tecnologias e processos em todo o espaço de segurança, o gerenciamento de ferramentas de segurança se torna complicado.

Com o tempo, a consolidação do setor de segurança e uma estreita integração das principais tecnologias podem fazer com que as empresas abandonem a abordagem produto por produto e implementem as defesas dos fornecedores (consulte a página 33). Enquanto isso, uma estratégia de defesa intensa e proativa, da qual a tecnologia é apenas um componente, pode ajudar empresas de pequeno, médio e grande porte e suas equipes de segurança a detectarem a ameaça de inovação criminosa descrita neste relatório.

Inteligência de ameaças

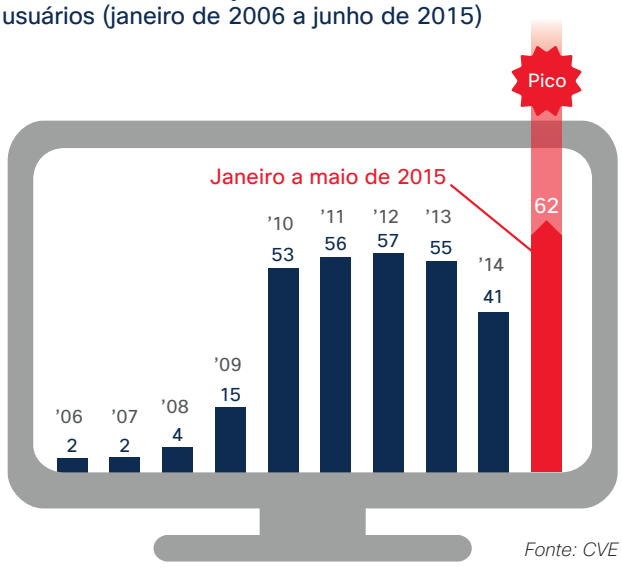
Inteligência de ameaças

A Cisco montou e analisou um conjunto global de dados de telemetria para este relatório. Nossas pesquisas e análises contínuas de ameaças descobertas, como o tráfego de malware, podem dar uma ideia sobre o possível comportamento criminoso e ajudar na detecção de ameaças.

A exploração de vulnerabilidades no Adobe Flash disparam na primeira metade de 2015

Nos primeiros cinco meses de 2015, o projeto CVE (Common Vulnerabilities and Exposures, Vulnerabilidades e exposições comuns) publicou 62 vulnerabilidades no Adobe Flash Player que resultaram na execução de códigos nas máquinas dos usuários. Como mostra a Figura 1, somente 41 desses tipos de vulnerabilidades foram identificados em 2014. O segundo pico mais significativo ocorreu em 2012, quando 57 dessas vulnerabilidades no Flash foram observadas. Se o padrão atual de atividade se mantiver no restante do ano, em 2015 poderão ser encontradas mais de 100 dessas explorações, o que seria um recorde.

Figura 1. Número de vulnerabilidades no Flash que resultaram na execução de código nas máquinas dos usuários (janeiro de 2006 a junho de 2015)



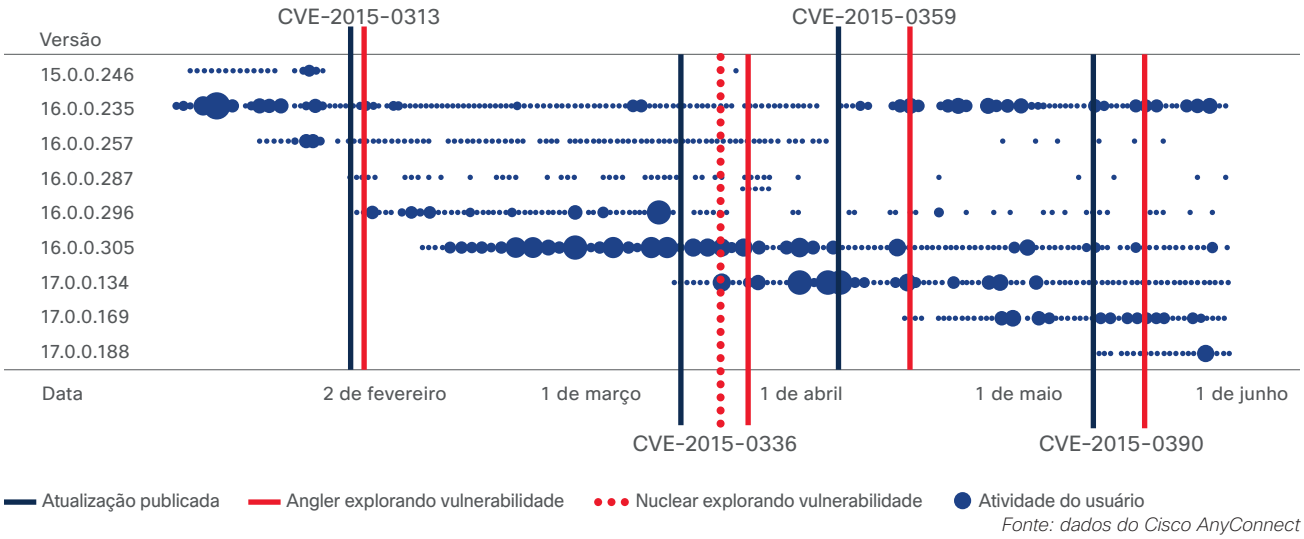
Fonte: CVE

Nós atribuímos o recente aumento na exploração de vulnerabilidades no Flash a dois fatores principais:

- **As explorações no Flash são integradas regularmente às últimas versões de kits de exploração amplamente difundidos, como o Angler (consulte a página 9).**
- **Embora a Adobe atualize o Flash Player com frequência, muitos usuários simplesmente não são rápidos o suficiente para aplicar as atualizações que os protegeriam de explorações cujo alvo é a vulnerabilidade que está sendo corrigida.**

Parece que muitos usuários têm dificuldade para administrar as atualizações do Adobe Flash, e talvez nem tenham conhecimento delas. A Figura 2 mostra que os autores do Angler têm tirado proveito dessa "lacuna de patches", ou seja, o tempo entre o lançamento pela Adobe de uma atualização e o momento no qual os usuários realmente atualizam. (A tecnologia da Cisco permite que os pesquisadores monitorem versões de software dos usuários a qualquer momento.)

Figura 2. Solicitações feitas por versão do Flash, por data



Fonte: dados do Cisco AnyConnect

Por exemplo, o período de fevereiro de 2015 descrito na Figura 2 mostra que muitos usuários passaram rapidamente para a versão mais recente do Flash (16.0.0.305). Essa atualização, lançada em 2 de fevereiro de 2015, abordou as vulnerabilidades no CVE-2015-0313. No entanto, com a migração dos usuários para a nova versão do Flash, o Angler explorou ativamente a vulnerabilidade conhecida na versão anterior.

A Figura 2 também mostra que os autores do kit de exploração Angler conseguiram desenvolver rapidamente e lançar uma exploração funcional direcionada para a vulnerabilidade no CVE-2015-0313. Observamos uma inovação igualmente rápida com outras explorações no Flash durante a primeira metade de 2015. Por exemplo, outro kit de exploração sofisticado e constantemente ativo, o Nuclear, se apressou em atacar a vulnerabilidade no CVE-2015-0336. O Angler começou a explorar a mesma vulnerabilidade logo depois.

A lacuna de patches é uma razão pela qual os criminosos continuam conseguindo explorar os usuários do Java (consulte a Figura 3).

Ataques projetados para Flash e outras vulnerabilidades novas estão sendo integrados tão rapidamente em kits de exploração como o Angler e o Nuclear que fica cada vez mais difícil para as equipes de segurança acompanharem o ritmo. O tempo para detecção também é mais longo porque geralmente é necessária a análise retrospectiva para identificar essas ameaças.

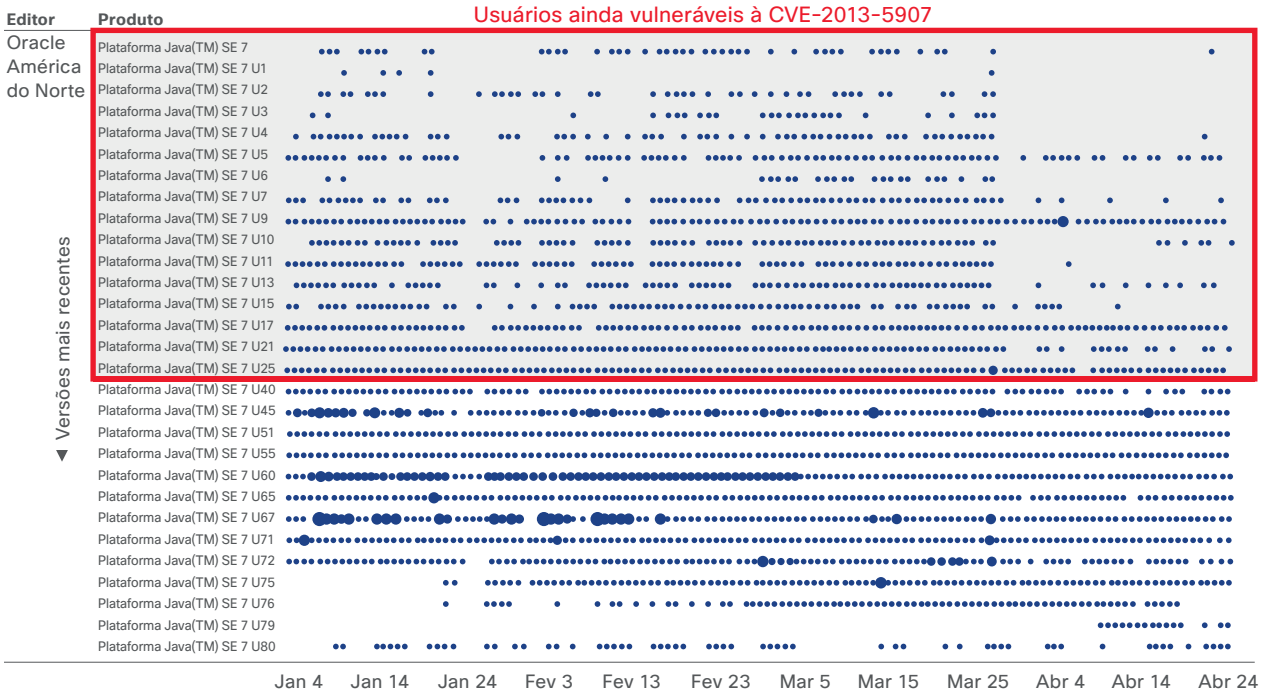
O risco de comprometimento para usuários individuais e empresas que dependem estritamente de um único mecanismo de detecção é significativo. Em ambientes sem recursos de análise retrospectiva, as ameaças disseminadas via ataques de dia zero ou por meios escusos podem permanecer não detectadas por longos períodos, ou até mesmo nunca serem identificadas.

No entanto, uma medida fundamental – a correção imediata e rotineira de falhas de software – pode ajudar a reduzir consideravelmente o risco de comprometimento por ameaças elaboradas para explorar vulnerabilidades conhecidas no Flash e no Java.

Compartilhe o relatório

Figura 3. Solicitações feitas por versão do Java, por data

Compartilhe o relatório



Fonte: dados do Cisco Cloud Web Security

O foco no Flash dá ao Angler uma vantagem significativa sobre os concorrentes

Compartilhe o relatório

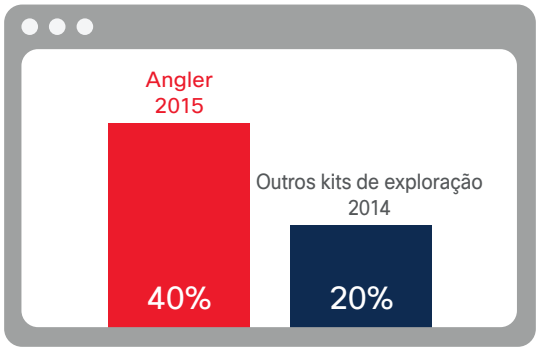
No início deste ano[1], a elegeu o kit de exploração Angler, devido a seu uso inovador das vulnerabilidades no Flash, no Java, no Microsoft Internet Explorer e no Silverlight. Até o momento, o Angler se destaca em termos de sofisticação e eficácia entre os kits de exploração atuais.

A concentração recente dos autores de kits de exploração das vulnerabilidades no Adobe Flash e seu trabalho rápido para tirar proveito delas são um exemplo do compromisso deles com a inovação.

A Cisco relata que, em média, 40% dos usuários que encontram uma página de destino do kit de exploração Angler estão comprometidos. (Consulte a Figura 4). Isso significa que o Angler é capaz de identificar uma vulnerabilidade conhecida do Flash (ou alguma outra) e explorá-la. Em seguida, ele faz download da carga para o computador do usuário.

Em comparação, no ano de 2014, outros kits amplamente utilizados que incluíam uma combinação de explorações tiveram uma taxa média de sucesso de apenas 20%, segundo a nossa pesquisa.

Figura 4. Taxa de visitantes explorados (dezembro de 2014 a maio de 2015)



Fonte: Cisco Security Research

1 Relatório anual sobre segurança da Cisco de 2015, janeiro de 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

Angler: executado nas sombras

O sucesso do Angler em comprometer usuários on-line pode ser atribuído em parte a suas páginas de destino da Web simples, porém bem construídas. Os pesquisadores da Cisco sugerem que os autores de kits de exploração talvez estejam usando a ciência de dados para criar páginas de destino geradas por computador que lembram páginas da Web normais e enganam os usuários facilmente. O malvertising (publicidade on-line mal-intencionada) é provavelmente o fator determinante de um fluxo estável de tráfego da Web para essas páginas. (Para obter mais informações sobre malvertising, consulte a página 29.)

O Angler também é muito bom em tentar escapar da detecção. A "duplicação de domínio" é uma técnica que os autores têm empregado recentemente. Os autores de kits de exploração comprometem a conta de uma pessoa registrada no nome de domínio e depois registram um subdomínio no domínio legítimo do usuário comprometido. A menos que os usuários examinem suas informações de conta, eles não saberão que esses subdomínios existem. Os subdomínios apontam para servidores mal-intencionados. É difícil bloqueá-los porque eles aparecem em grande volume, duram pouco e são aleatórios.

A técnica de duplicação de domínio não é nova, mas seu uso vem aumentando desde dezembro de 2014. De acordo com a nossa pesquisa, mais de 75% da atividade de subdomínio conhecida realizada por autores de kits de exploração desde essa época pode ser atribuída ao Angler. Mediante explorações de arquivo, o kit de exploração atende a uma variedade de cargas mal-intencionadas, como o cavalo de Troia Cryptowall, que é uma infecção ransomware.

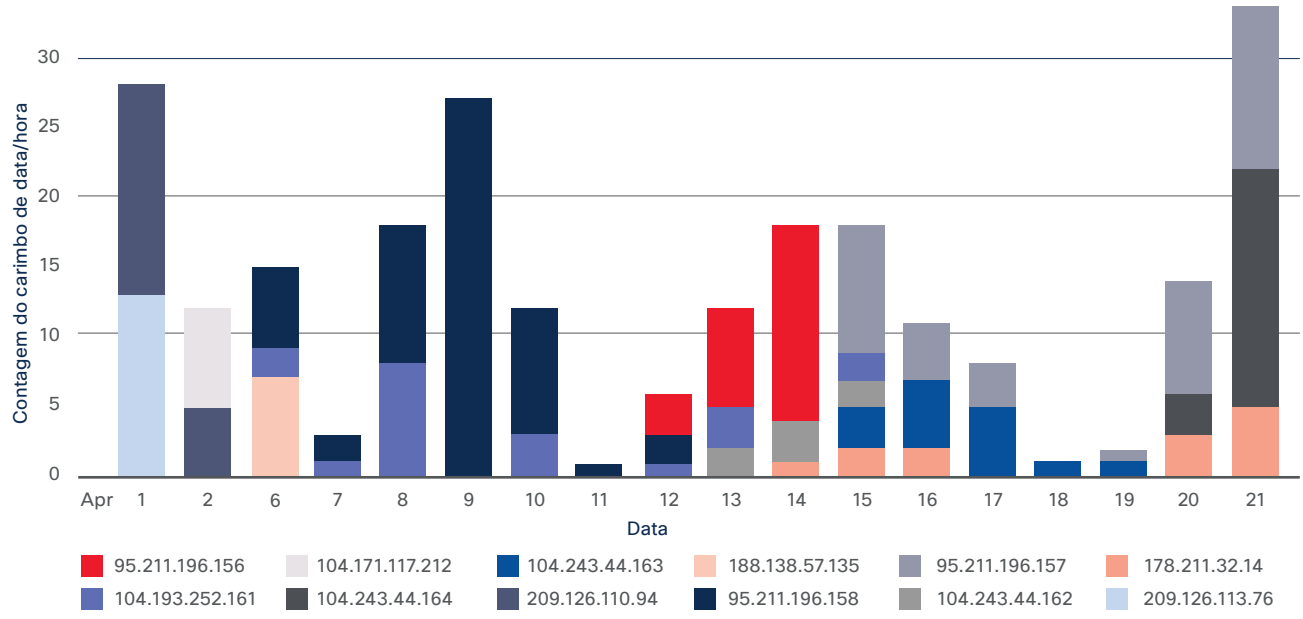
Além do sombreamento de domínio, o kit de exploração Angler usa vários endereços IP para dificultar a detecção. O exemplo na Figura 5 mostra a frequência com que o Angler pode alternar IPs em um determinado dia. O padrão parece aleatório.

A publicação **"Threat Spotlight: Angler Lurking in the Domain Shadows"** (Ameaça em destaque: Angler à espreita na sombra do domínio) publicada no blog do Cisco Talos Security Intelligence and Research Group (Talos) discute como o Angler cria subdomínios que podem oferecer conteúdo mal-intencionado e por que uma abordagem de defesa intensa à segurança é essencial para detectar esse tipo de ataque.

Consulte também a publicação **"Domain Shadowing Goes Nuclear: A Story in Failed Sophistication"** (A duplicação de domínio chega ao Nuclear: uma história sobre falha na inovação) no blog do Talos Group referente à campanha do kit de exploração Nuclear que inclui a duplicação de domínio. Quando concluído, esse trabalho em andamento provavelmente será uma plataforma de kit de exploração bem-sucedida.

Figura 5. Explorações bem-sucedidas no Flash (abril de 2015)

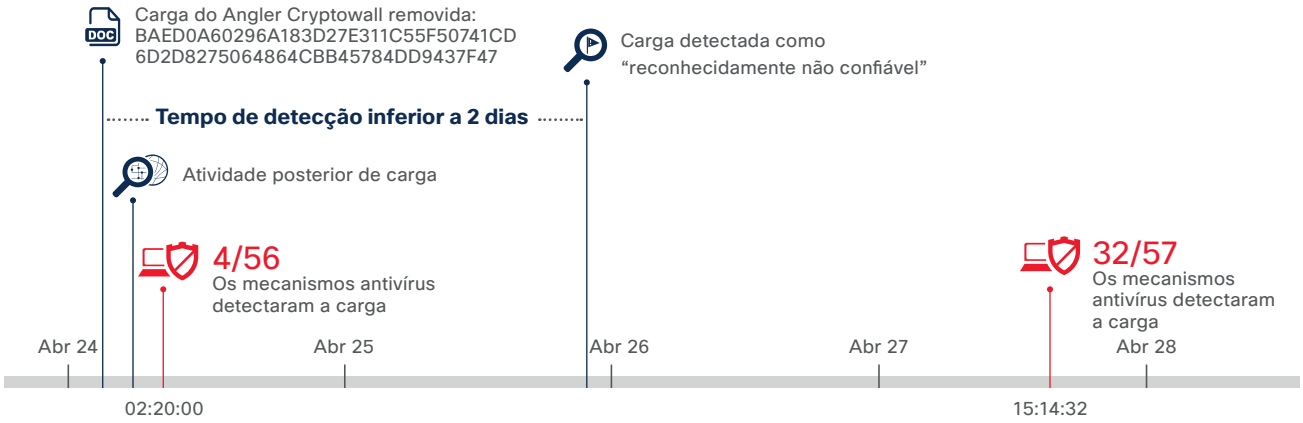
Compartilhe o relatório



*As cores representam faixas de IP.

Fonte: Cisco Security Research

Figura 6. Tempo de detecção para distribuição de carga do Angler em 24 de abril de 2015



Fonte: Cisco Security Research

Cargas criptografadas tornam lenta a detecção do Angler

O Angler normalmente fornece uma carga criptografada, que quase sempre é o ransomware representado pelo cavalo de Troia Cryptowall. Se não for bloqueado logo de início, essa carga só poderá ser identificada de forma retrospectiva e o tempo de detecção da ameaça poderá levar dias.

Quando uma carga é detectada, os autores de kits de exploração, fazendo jus à sua reputação de inovação, criam rapidamente uma técnica para distribuir ameaças como o Cryptowall e escapar das soluções antivírus.

A Figura 6 mostra o tempo para detecção da carga Cryptowall do Angler que foi removida pela primeira vez em 24 de abril de 2015: BAED0A60296A183D27E311C 55F50741CD6D-2D8275064864CBB45784DD9437F47.

No primeiro dia, apenas 4 de 56 mecanismos antivírus implantados pela VirusTotal identificaram a nova instância de malware. No entanto, até 27 de abril, 32 de 57 mecanismos antivírus já estavam detectando a ameaça.

- 24-04-2015 02:20:00 **4/56** (4 de 56 mecanismos antivírus implantados detectaram a carga)
- 27-04-2015 15:14:32 **32/57** (32 de 57 mecanismos antivírus implantados detectaram a carga)

A Cisco identificou a ameaça como "desconhecida" em 24 de abril e a analisou e condenou retrospectivamente (categorizando-a como "reconhecidamente não confiável") menos de dois dias depois.

Consulte "Definição de tempo de detecção", na página 30, para obter mais informações sobre como definimos e calculamos o tempo para detecção.

Autores de kits de exploração fazem manobras para mantê-los ocultos nas páginas de destino

Alguns autores de kits de exploração buscam a literatura do início do século XIX para ajudar a esconder suas ameaças do século XXI. Especificamente, alguns criminosos estão incluindo passagens do romance clássico *Razão e Sensibilidade*, de Jane Austen, nas páginas de destino da Web que hospedam seus kits de exploração.

A inclusão de trechos de textos clássicos em uma página de destino de um kit de exploração é uma técnica de ofuscação mais eficaz do que a abordagem tradicional, que usa textos aleatórios. O uso de passagens de obras mais contemporâneas, como revistas e blogs, é outra estratégia eficaz. É muito provável que os antivírus e outras soluções de segurança categorizem a página da Web como legítima após a "leitura" desse texto.

Para os usuários, encontrar referências inesperadas a personagens queridos de Jane Austen, como Elinor Dashwood e Sra. Jennings, em uma página da Web pode ser uma surpresa, mas não causa preocupação imediata. Mas essa falta de preocupação dá aos criminosos mais oportunidades para iniciarem suas explorações.

O uso de obras conhecidas em vez de textos aleatórios é apenas um exemplo do modo como os autores das ameaças desenvolvem seus esquemas para evitar a detecção.

Figura 7. Trecho do texto de *Razão e Sensibilidade* usado na página de destino do kit de exploração

```
https://rt1.mtd.cisco-services.com/Ticket/
Display.html?
id=137668&results=ad470ba70bfbd94464c2a0e9deff943b

Sense and sensibility - jane austin
    <small>
      Mr. Ferrars comfortable as a continual flow of
tears would permit her. In the society of both. Why
they should both attend through
    </small>
     She looked down as a difference of the three, by
their presence; and it will be so easily settled. it
    <i>
     the cruel situation in which she had by that
which only could convince her, a better match for
your mother--will you allow him to give rise to
conjectures, which might make it rare; for his
sisters by the hand, and speaking in an audible
voice, and walking the
    </i>
```

Fonte: Cisco Security Research

A evolução do ransomware: uma história de inovação – e diminuição das expectativas

Compartilhe o relatório

Na próspera economia de malware atual, com moedas criptografadas como o bitcoin e redes de anonimização como a Tor (consulte a página 15), ficou ainda mais fácil para os malfeitores entrarem no mercado de malware e começarem a gerar receita. Para aumentar ainda mais a lucratividade e continuar fugindo da detecção, os operadores de crimeware, como ransomware, contratam e financiam suas próprias equipes de desenvolvimento profissional para criar novas variações e táticas.

O ransomware criptografa os arquivos do usuário – visando tudo, de arquivos financeiros até fotos de família – e fornece as chaves para a descriptografia somente depois que os usuários pagam um "resgate". Todos são alvo do ransomware, de empresas grandes a escolas e usuários individuais.

O malware geralmente é distribuído por meio de alguns vetores, como e-mail e kits de exploração. O kit de exploração Angler (consulte a página 11), por exemplo, é conhecido por lançar a carga útil Cryptowall. O Cryptowall surgiu depois que a variação original, Cryptolocker, foi eliminada por lei em meados de 2014.

A Figura 8 descreve um exemplo de mensagem que os usuários podem receber ao encontrar o ransomware TeslaCrypt, que alega ser um derivado do Cryptolocker.

Figura 8. Exemplo de mensagem na tela do ransomware TeslaCrypt

Fonte: Cisco Security Research

O resgate exigido não é exorbitante. Normalmente, fica entre US$ 300 e US$ 500. Por que uma quantia tão modesta? Os criminosos que implantam ransomware fizeram uma pesquisa de mercado para determinar a faixa de preços ideal. A ideia é fixar um resgate que não seja alto demais para o usuário pagar ou, pior, que o motive a procurar as autoridades. Em vez disso, o resgate está mais para uma taxa de conveniência. E os usuários pagam.

De fato, a Cisco relata que praticamente todas as transações relacionadas a ransomware são realizadas pela rede anônima Tor (consulte a página 15). Usando canais como as redes Tor e I2P (Projeto de Internet Invisível), os criminosos mantêm o risco de detecção baixo e a lucratividade alta. I2P é uma camada de rede de computador que permite que as aplicações enviem mensagens entre si de modo seguro e sob pseudônimo. Muitas operações de ransomware também têm equipes de desenvolvimento que monitoram atualizações dos provedores de antivírus para que os autores saibam quando uma variação foi detectada e que está na hora de mudar de técnica.

Eles se valem do bitcoin como moeda criptografada para pagamentos, o que dificulta o rastreamento das transações por parte das autoridades. E para manter uma boa reputação no mercado (ou seja, serem conhecidos por cumprir suas promessas de liberar o acesso dos usuários a seus arquivos criptografados após o processamento do pagamento), muitos operadores de ransomware desenvolveram elaboradas operações de suporte ao cliente.

Nos últimos tempos, temos observado várias campanhas personalizadas que foram projetadas para comprometer grupos de usuários específicos, como jogadores on-line. Alguns autores de ransomware também criaram variações em idiomas incomuns, como o islandês, para assegurar que usuários nas áreas onde esses idiomas são predominantemente falados não ignorem a mensagem de ransomware.

Os usuários podem se proteger de ransomware fazendo backup de seus arquivos mais valiosos e mantendo-os isolados fisicamente da rede. Os usuários também devem perceber que seu sistema pode estar em risco mesmo depois que eles pagarem o resgate e descriptografarem seus arquivos. Quase todos os ransomwares são multivetoriais. O malware pode ter sido substituído por outro malware, o que significa que o vetor de infecção inicial ainda precisa ser resolvido para que o sistema possa ser considerado limpo.

Para obter mais informações sobre tendências de ransomware, consulte as publicações **"Cryptowall 3.0: Back to Basics"** (Cryptowall 3.0: de volta ao básico) e **"Threat Spotlight: TeslaCrypt–Decrypt It Yourself"** (Ameaça em destaque: TeslaCrypt – Descriptografe você mesmo) no blog do Talos Group.

Adoção da Tor por criminosos cibernéticos para ocultar a comunicação de rede

Os autores de malware naturalmente tentam fugir da detecção e manter a localização de seus servidores desconhecida. Para isso, muitos usam a rede anônima Tor para transmitir comunicados de comando e controle.

Nossos pesquisadores detectaram várias instâncias em que famílias de malware, especialmente variações de ransomware, geravam tráfego Tor. Embora a rede Tor seja usada com frequência nas empresas para fins legítimos (por exemplo, por profissionais de segurança), sua presença pode indicar a existência de tráfego de malware em uma rede. Algumas das qualidades que atraem usuários legítimos para a rede Tor também são atraentes para infratores.

Se os profissionais de segurança detectarem atividade de Tor em suas redes, deverão correlacionar essa descoberta a outros possíveis indicadores de atividade mal-intencionada (como downloads de arquivos executáveis desconhecidos ou conexões com os servidores de kits de exploração) para determinar se o tráfego Tor é legítimo.

Como mostra a Figura 9, os criminosos que implantam o ransomware Cryptowall 2.0 e diversas famílias de malware são usuários da rede Tor. (Consulte "A evolução do ransomware: uma história de inovação – e diminuição das expectativas", na página 13). Os dados são provenientes da monitoração pela Cisco das redes do cliente e mostram incidentes nos quais a rede Tor foi usada em famílias de malware entre outubro de 2014 e maio de 2015.

Figura 9. Famílias de malware que usam a Tor para comunicação

Fonte: Cisco Security Research

Macros do Microsoft Office ensaiam retorno como veículo de lançamento de explorações

O aumento no uso de macros do Microsoft Office para distribuir cavalos de Troia bancários mostra a convergência de duas tendências no mundo dos criminosos cibernéticos: ressuscitar ferramentas antigas ou vetores de ameaças para reutilização e mudar a ameaça com tanta rapidez e frequência que seja possível relançar ataques o tempo todo e escapar da detecção.

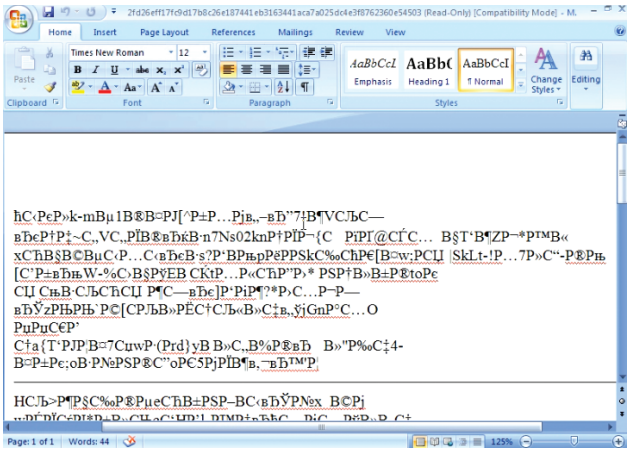
As ferramentas antigas usadas pelos criadores desses cavalos de Troia são as macros em produtos do Microsoft Office, como o Microsoft Word. Populares entre os criminosos anos atrás, essas macros caíram em desuso porque, com o tempo, eram desativadas por padrão. No entanto, usando técnicas de engenharia social, agentes mal-intencionados podem levar os usuários a ativar as macros, adicionando assim uma nova tática às suas caixas de ferramentas.

Estudamos duas campanhas recentes em que cavalos de Troia Dridex foram disseminados como anexos de e-mail (cada um deles enviado a destinatários específicos), a pretexto de entregar faturas ou outros documentos importantes. Desde meados de 2015, temos detectado novas campanhas relacionadas a Dridex diariamente.

Embora as linhas de assunto de e-mail na primeira campanha (Campanha 1) tentassem levar os destinatários a acreditar que os anexos eram documentos de negócios essenciais, alguns dos e-mails em si estavam em branco.

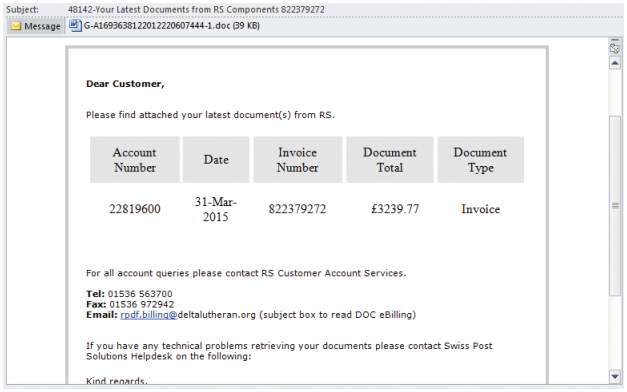
Dridex: Campanha 1

Quando os destinatários abriam os anexos, viam um documento do Word repleto de texto sem sentido.



Os e-mails na segunda campanha que analisamos (Campanha 2) incluíam uma mensagem que parecia ser legítima, fazendo referência a contas e números de fatura específicos e alegando que os documentos anexados eram faturas. Porém, quando os destinatários abriam o anexo do Word, também viam texto sem sentido, parecido com o que os usuários na Campanha 1 encontraram.

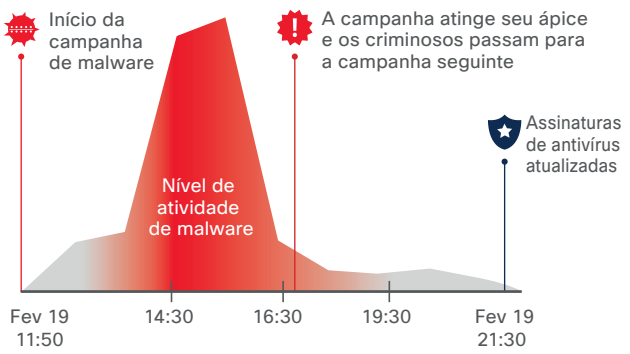
Dridex: Campanha 2



Em ambas as campanhas, assim que um destinatário de e-mail abria o documento do Word anexado, a atividade mal-intencionada ocorria. Em segundo plano, uma macro usava cmd.exe e PowerShell para baixar um executável mal-intencionado de um endereço IP codificado. Em algumas campanhas que observamos, foram incluídas instruções para dizer ao usuário como ativar as macros. Com as macros ativadas, o Dridex poderia tentar roubar logins e senhas das contas bancárias das vítimas.

Nossos pesquisadores notaram que as campanhas de spam transmissoras da carga útil do Dridex tendem a durar muito pouco, talvez apenas algumas horas, e também que elas eram modificadas com frequência, como uma tática de evasão. Embora as soluções de antivírus executem funções de segurança úteis, elas não são tão adequadas para detectar essas campanhas de spam de curta duração. Quando uma campanha é detectada, os invasores já mudaram o conteúdo dos e-mails, os agentes de usuário, os anexos e as referências. Em seguida, eles iniciam a campanha novamente, o que obriga os sistemas de antivírus a detectá-los outra vez. Conforme visto na Figura 10, que mostra uma campanha do malware DyrezaC, as atualizações de antivírus podem ocorrer depois que uma campanha tiver sido concluída.

Figura 10. O DyrezaC pode funcionar mais rápido do que os sistemas antivírus



Fonte: Cisco Security Research

Aparentemente, essa combinação de spam, macros do Microsoft Office e Dridex atraiu os criminosos cibernéticos durante a primeira metade de 2015. Nós examinamos 850 amostras exclusivas de e-mails e arquivos de anexo do Microsoft Office que eram portadores desse cavalo de Troia – um número relativamente grande de exemplos únicos para uma campanha de spam. Os autores dessas campanhas altamente mutáveis parecem ter um entendimento avançado sobre as medidas de evasão de segurança. Eles estão conscientes da dependência dos antivírus para revelar essas ameaças e se empenham para garantir que consigam evitar a detecção.

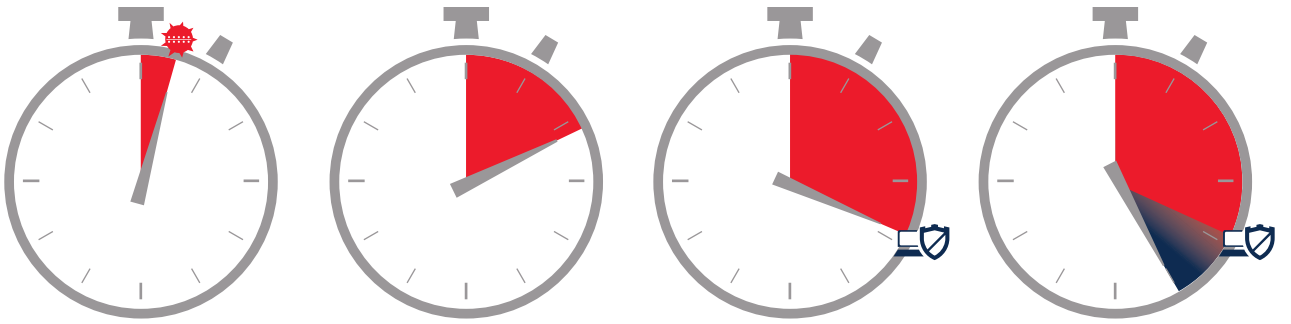
No exemplo da Figura 11, a imagem mostra que várias horas se passaram antes que os mecanismos de antivírus começassem a detectar a ameaça Dridex. Como a campanha durou cerca de cinco horas, as soluções de antivírus deram proteção apenas contra o final da campanha.

Como os profissionais de segurança tendem a encarar as explorações de macro como coisa do passado, talvez não estejam preparados para defender suas redes contra essas ameaças. A melhor proteção contra elas é uma estratégia de defesa intensa em que várias soluções de segurança funcionem em conjunto com o antivírus. Os filtros para ataques de vírus, por exemplo, podem colocar mensagens suspeitas em quarentena por até 12 horas, permitindo que as ferramentas de antivírus acompanhem as novas ameaças.

Para obter mais informações sobre o cavalo de Troia Dridex e as macros do Microsoft Office, leia a publicação **"Threat Spotlight: Spam Served With a Side of Dridex"** (Ameaça em destaque: Spam servido com acompanhamento de Dridex) no blog do Talos Group.

Figura 11. Gráfico de detecção para Dridex (março a abril de 2015)

Compartilhe o relatório



A campanha do Dridex inicia com a exploração de uma macro conhecida

A atividade do Dridex atinge o ápice, mas permanece não detectada por várias horas

O Dridex é detectado pelos mecanismos antivírus

Os criminosos encerram a campanha rapidamente e passam para a campanha seguinte

Fonte: Cisco Security Research

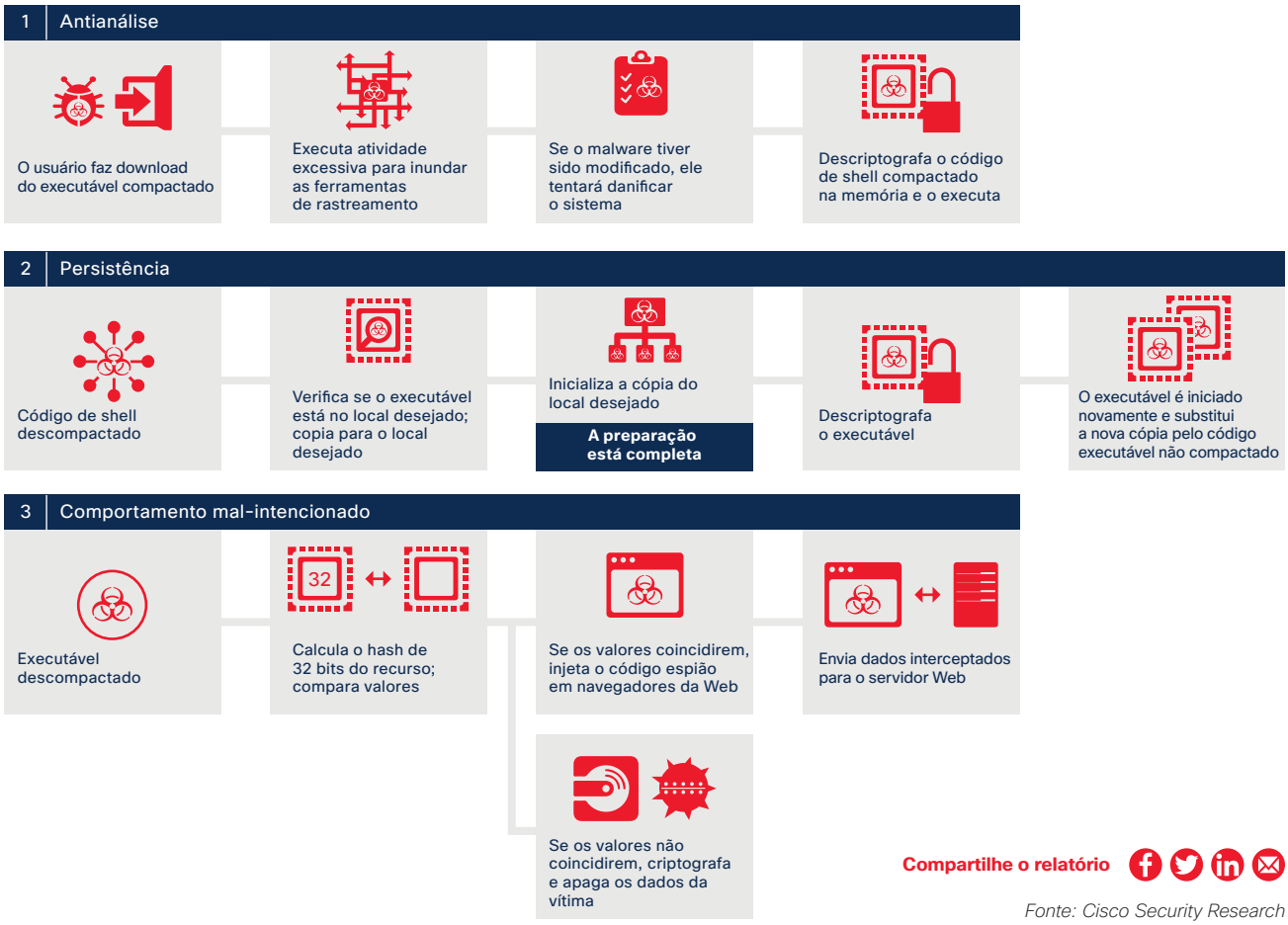
Rombertik: malware que não só pode roubar dados, como também destruí-los

Os autores de malware avançado o configuram para simplesmente parar de funcionar, a fim de que não seja bloqueado ou destruído quando for examinado por sistemas de segurança. Ao mesmo tempo, os pesquisadores de segurança estão constantemente à procura de novas ferramentas de análise estáticas, dinâmicas e automatizadas que tornem mais difícil para os invasores permanecerem não detectados.

Para atingir essa meta, a Cisco fez recentemente a engenharia reversa do Rombertik, um malware complexo que detecta qualquer tentativa de violar seu código binário, semelhante ao que ocorre na engenharia reversa. O Rombertik tenta destruir o registro mestre de inicialização (MBR) do computador host. Se isso não for possível, ele tentará destruir os arquivos no diretório inicial do usuário. Ao contrário do malware que tenta desviar a atenção de suas atividades, o Rombertik parece ter sido projetado para se destacar na multidão. A engenharia reversa é uma etapa essencial usada pela Cisco e outros pesquisadores de ameaças para entender como o malware opera (sua funcionalidade evasiva, por exemplo).

O objetivo do Rombertik é conectar-se ao navegador da Web de um usuário para extrair informações confidenciais do usuário e fornecê-las a um servidor controlado pelos invasores. Nesse aspecto, o Rombertik é semelhante ao malware conhecido como Dyre.[2] A diferença é que o Dyre existe para roubar logins bancários, enquanto o Rombertik coleta indiscriminadamente todos os tipos de dados do usuário.

Figura 12. Combinação exclusiva do Rombertik de comportamento antianálise e mal-intencionado



Compartilhe o relatório

Fonte: Cisco Security Research

O Rombertik marca presença nos sistemas dos usuários por meio de mensagens de spam e phishing que usam a engenharia reversa para induzir os destinatários a fazerem download dos anexos portadores do malware e descompactá-los. Quando um usuário descompacta o arquivo que parece ser um PDF, mas, na verdade, é um arquivo executável de proteção de tela que começa a comprometer o sistema. Como observado na Figura 12, se o Rombertik detectar que está sendo modificado, ele tentará destruir o MBR do sistema e reiniciar o computador, que ficará inoperante.

Ferramentas antianálise avançadas nos malwares de hoje

O Rombertik pode ser um precursor do que está por vir no mundo do malware, pois os autores de malware são rápidos em adotar as táticas bem-sucedidas de seus colegas. Conforme nossos pesquisadores descobriram, o Rombertik inteligentemente inclui vários recursos destinados a ofuscação e destruição. Por exemplo, o Rombertik inclui código excessivo ou "inútil" para obrigar os analistas de segurança a perder mais tempo investigando e analisando o malware. A ideia é sobrecarregá-los a ponto de não terem tempo de examinar todas as funções.

Para escapar da detecção e forçar um sandbox a atingir o tempo limite antes que a carga mal-intencionada tenha chance de ser executada, o Rombertik adota uma abordagem exclusiva. Normalmente, o malware fica "adormecido" quando está em um sandbox para que o tempo limite seja obrigatoriamente atingido. Porém, à medida que as ferramentas de análise de segurança foram se tornando mais eficientes na detecção do processo de "dormência", os autores de malware precisaram de uma nova estratégia.

No caso do Rombertik, o malware grava um byte de dados aleatórios na memória 960 milhões de vezes. Isso pode afetar tanto as ferramentas de rastreamento de aplicações quanto os sandboxes. É provável que os sandboxes não consigam determinar se a aplicação está travando intencionalmente, já que ele não está adormecido de verdade. Além disso, demora muito registrar todas as 960 milhões de instruções de gravação, complicando a análise para os dois tipos de ferramentas.

O Rombertik tem muitas dessas técnicas para ofuscação quando passa por engenharia reversa ou é analisado, mas sua técnica antimodificação final tem potencial para causar danos significativos. Se o malware detectar que está sendo modificado para análise, tentará substituir o MBR da máquina. Se ele não obtiver permissão para substituir o MBR, tentará destruir todos os arquivos no diretório inicial do usuário. Quando a máquina for reinicializada, ficará inoperante.

Se o Rombertik passar por todas as verificações antimodificação, ele finalmente começará sua tarefa principal: roubar os dados que os usuários digitam em seus navegadores e encaminhar essas informações ao seu servidor.

Rombertik: elevação das expectativas para os defensores de segurança

As características do Rombertik são suas técnicas aprimoradas para escapar da análise e sua capacidade de danificar o software do sistema operacional das máquinas nas quais é executado. Essa abordagem eleva as expectativas para os defensores de segurança que, sem dúvida, vão tentar enfrentar malwares como esse no futuro. Pode apostar que outros autores de malware vão não só se apropriar das táticas do Rombertik, como torná-las ainda mais destrutivas.

Boas práticas de segurança podem ajudar a proteger os usuários e treiná-los para que não cliquem em anexos de remetentes desconhecidos. No entanto, para encontrar a ameaça de malwares bem elaborados e perigosos como o Rombertik, também é preciso uma abordagem de defesa intensa que abranja toda a sequência da ameaça: antes, durante e depois de um ataque.

Consulte a publicação **"no blog do Talos Group"** (Ameaça em destaque: Rombertik – Escapando de todas as armadilhas) no blog do Talos Group para ver uma análise do malware Rombertik.

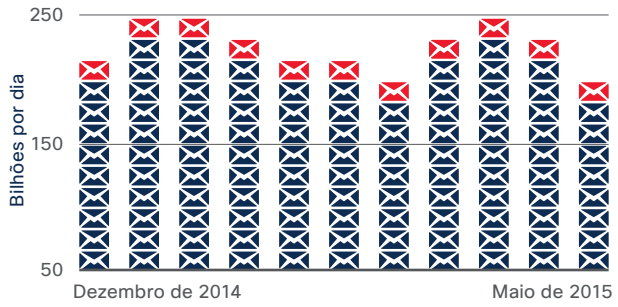
2 "Threat Spotlight: Dyre/Dyreza: An Analysis to Discover the DGA" (Ameaça em destaque: Dyre/Dyreza – Uma análise da descoberta do DGA), blog da Cisco Security, 30 de março de 2015, http://blogs.cisco.com/security/talos/threat-spotlight-dyre.

Volume de spams permanece estável

Conforme os criminosos desenvolvem métodos mais avançados para violar as defesas de rede, e-mails de spam e phishing continuam a desempenhar um papel importante nesses ataques. Ainda assim, o volume mundial de spams permaneceu relativamente estável, como observado na Figura 13.

A Figura 14 mostra uma análise por país indicando que, embora o volume de spams esteja em crescimento nos Estados Unidos, na China e na Federação Russa, ele permanece relativamente estável em outras regiões. Nós atribuímos essas mudanças a flutuações na atividade relativa das redes de spam subjacentes.

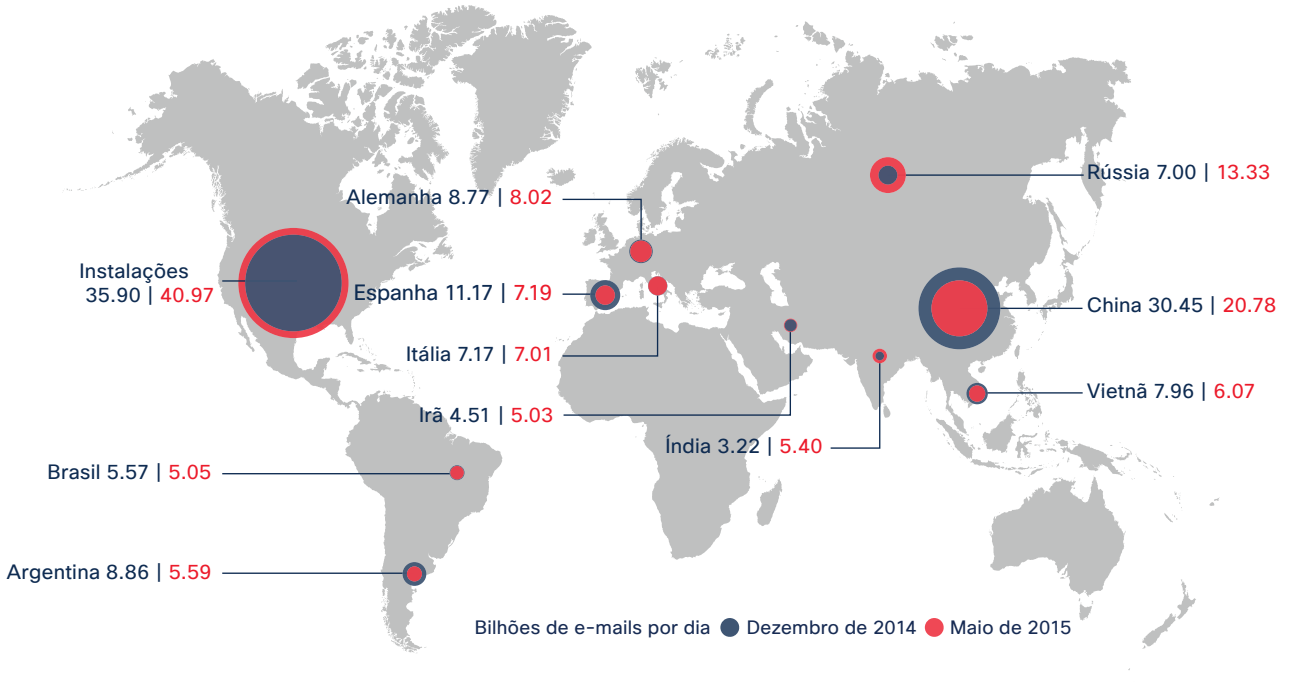
Figura 13. O volume de spams é estável



Fonte: Cisco Security Research

Figura 14. Volumes de spams por país

Compartilhe o relatório



Fonte: Cisco Security Research

Ameaças e vulnerabilidades: erros de codificação comuns criam entradas para explorações

Ao examinar as vulnerabilidades mais comuns da primeira metade de 2015, encontramos os mesmos tipos de erros que aparecem ano após ano. Por exemplo, conforme observado na Figura 15, mais uma vez os erros de buffer estão no topo da lista de categorias de ameaças CWE (Common Weakness Enumeration, Enumeração de pontos fracos comuns), segundo a definição do National Vulnerability Database (https://nvd.nist.gov/cwe.cfm).

As três CWEs mais frequentes na Figura 15 (erros de buffer, validação de entrada e erros de gerenciamento de recursos) estão sempre entre os cinco erros de codificação mais comuns explorados pelos criminosos. Se os fornecedores têm conhecimento dessa lista de CWEs, por que esses erros continuam ocorrendo com tanta regularidade?

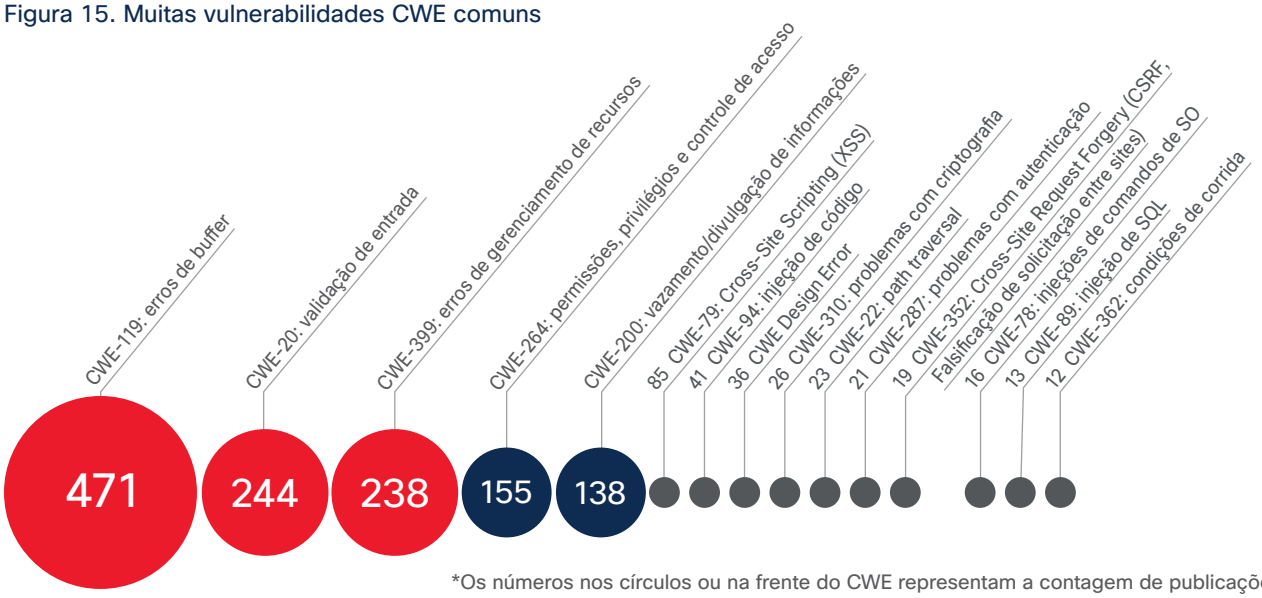
O problema é que se dá pouca atenção ao ciclo de vida de desenvolvimento seguro. As proteções de segurança e os testes de vulnerabilidade deveriam estar integrados ao desenvolvimento de um produto. Em vez disso, os fornecedores esperam o produto chegar ao mercado para só então resolver suas vulnerabilidades.

Os fornecedores precisam dar mais ênfase à segurança durante o ciclo de vida de desenvolvimento. Caso contrário, continuarão perdendo tempo e dinheiro em esforços posteriores para detectar, corrigir e relatar vulnerabilidades. Além disso, os fornecedores de segurança devem garantir aos clientes que estão fazendo todo o possível para lançar soluções confiáveis e seguras: nesse caso, tornando o teste de vulnerabilidade um componente crucial do desenvolvimento do produto.

Vulnerabilidades de terceiros

Desde o lançamento em abril de 2014 do Heartbleed com a falha de segurança na utilização do Transport Layer Security (TLS), as vulnerabilidades de software de terceiros se tornaram um agravante para empresas que desejam repelir os invasores. O Heartbleed marcou o início de exames mais detalhados de vulnerabilidades de software de terceiros (TPS), principalmente com o aumento na popularidade das soluções de código aberto.

Figura 15. Muitas vulnerabilidades CWE comuns



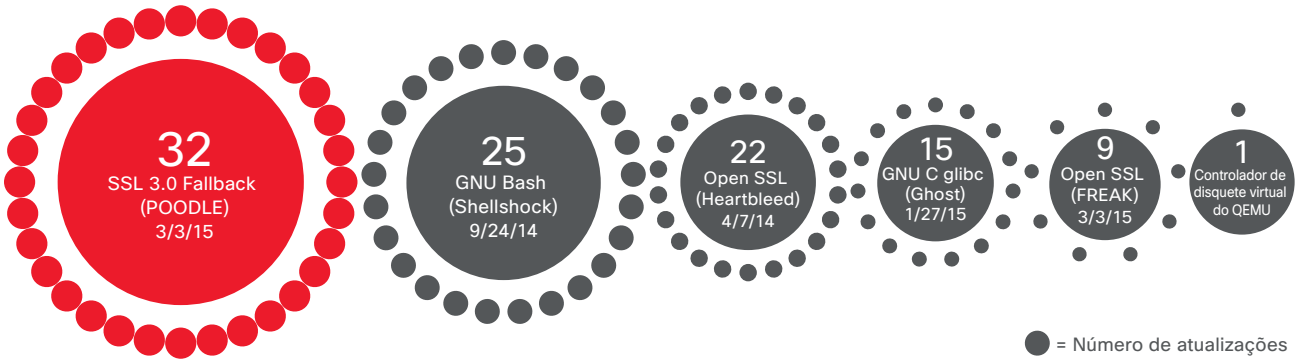
*Os números nos círculos ou na frente do CWE representam a contagem de publicações

Fonte: Cisco Security Research

Compartilhe o relatório

Figura 16. Vulnerabilidades de código aberto

Compartilhe o relatório



Fonte: Cisco Security Research

A Figura 16 mostra seis das vulnerabilidades de código aberto mais comuns que rastreamos na primeira metade de 2015. (Para ver respostas detalhadas dos fornecedores, clique nas vulnerabilidades acima e navegue até o histórico de alertas.)

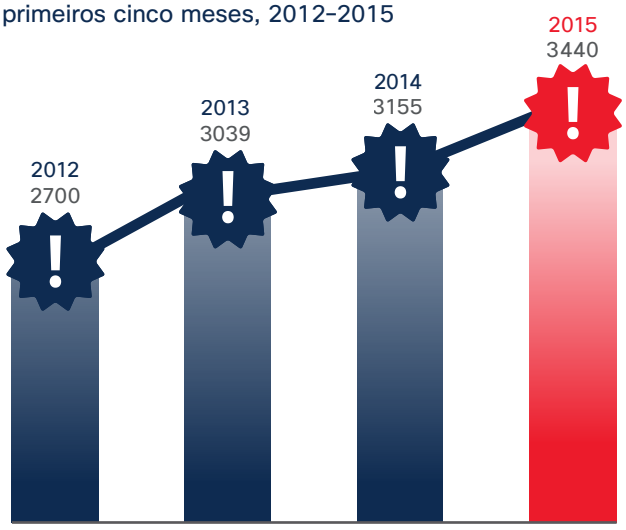
As vulnerabilidades de código aberto representam um desafio inerente, pois o encerramento de uma vulnerabilidade requer a coordenação de muitos fornecedores. A comunidade de desenvolvedores que mantêm soluções de código aberto pode fornecer prontamente uma correção ou um patch, mas depois as correções precisam ser integradas em todas as versões do produto.

O bom é que, quanto maior a conscientização sobre as vulnerabilidades do código aberto, mais rápida é a resposta da comunidade de segurança a elas. Por exemplo, quando surgiu a vulnerabilidade VENOM (Virtualized Environment Neglected Operations Manipulation), que afetava o código aberto de sistemas de virtualização, os fornecedores lançaram patches mesmo antes da divulgação dessa vulnerabilidade.

Os recentes investimentos em OpenSSL feitos por várias empresas líderes da área de tecnologia, inclusive a Cisco, ajudam a melhorar a infraestrutura do OpenSSL. Os investimentos são feitos em forma de doações para a Linux Foundation. Esses investimentos ajudam os pesquisadores de segurança a realizar análises de código que visam identificar correções e patches para soluções de código aberto.[3]

Com o software de código aberto em vigor em muitas empresas, os profissionais de segurança precisam obter uma compreensão mais aprofundada de onde e como esse código aberto é usado nas empresas e se os pacotes ou bibliotecas de código aberto estão atualizados. Isso significa que, no futuro, o gerenciamento da cadeia de fornecimento de software passará a ser ainda mais essencial.

Figura 17. Total anual acumulado de alertas, primeiros cinco meses, 2012–2015



Fonte: Cisco Security Research

Compartilhe o relatório

3 "Cisco, Linux Foundation e OpenSSL", blog da Cisco Security, 25 de abril de 2014: http://blogs.cisco.com/security/cisco-linux-foundation-and-openssl.

O total anual acumulado de alertas IntelliShield nos primeiros cinco meses de 2015 apresenta uma ligeira tendência de elevação, em comparação com o mesmo período de 2014 (Tabela 1). Como a Cisco observou anteriormente, o aumento contínuo no total de alertas é um resultado provável do foco dos fornecedores em testes de segurança e na descoberta e correção de suas próprias vulnerabilidades.

Tabela 1. Níveis de atividade de alertas

	Atualizado	Novo	Total
Janeiro	211	359	570
Fevereiro	255	379	634
Março	285	471	756
Abril	321	450	771
Mai	237	472	709
	1309	**2131**	**3440**
Janeiro a maio de 2014		**Total de alertas: 3155**	

Fonte: Cisco Security Research

A Tabela 1 mostra a atividade dos alertas relatados e dos alertas atualizados. Observamos um aumento de 9% no total de alertas em maio de 2015, em relação ao número informado para maio de 2014. Os fornecedores de segurança e os pesquisadores têm observado um número crescente de novos alertas, enquanto o número de alertas atualizados caiu. Deduz-se, portanto, que as empresas precisam aumentar o foco no gerenciamento de patches.

A Tabela 2 apresenta algumas das vulnerabilidades mais exploradas de acordo com o Common Vulnerability Scoring System (CVSS). O National Vulnerability Database (NVD) do National Institute of Standards and Technology (NIST) dos EUA oferece uma estrutura para comunicar as características e os impactos das vulnerabilidades de TI e dar suporte ao CVSS.

A pontuação de urgência na tabela de CVSS indica que essas vulnerabilidades estão sendo exploradas ativamente. Ao verificar a lista de produtos explorados, as empresas podem determinar quais desses produtos estão em uso e, portanto, precisam ser monitorados e corrigidos.

Tabela 2. Vulnerabilidades mais exploradas

ID de alerta	Título	Urgência	Credibilidade	Severidade	CVSS Base	CVSS Temp.
35845	Manipulação do valor de string variável de ambiente GNU Bash	●●●●○	●●●●●	●●●●○	10,0	9,0
35816	Vulnerabilidade de injeção de comando de variável de ambiente GNU Bash	●●●●○	●●●●●	●●●●○	10,0	8,6
37181	Vulnerabilidade de estouro de buffer das chamadas à função GNU glibc gethost	●●○○○	●●●●●	●●●●○	10,0	7,8
37318	Vulnerabilidade de execução de código remoto do Adobe Flash Play	●●○○○	●●●●●	●●●●○	9,3	7,7
37848	Bypass de sandbox do mecanismo de criação de scripts Elasticsearch Groovy	●●○○○	●●●●●	●●●●○	9,3	7,7
37123	Uso do Adobe Flash Player após execução de código arbitrário livre	●●○○○	●●●●●	●●●●○	9,3	7,7
36849	Vulnerabilidade de estouro de buffer do daemon do protocolo NTP	●●○○○	●●●●●	●●●○○	7,5	5,5
37181	Vulnerabilidade de estouro de buffer das chamadas à função GNU glibc gethost	●●○○○	●●●●●	●●●●○	10,0	7,8
37326	Vulnerabilidade de divulgação de informações de bypass da mesma origem do Microsoft Internet Explorer	●●●○○	●●●●●	●●●○○	5,8	4,8
36956	Vulnerabilidade de downgrade criptográfico de chave temporária RSA do OpenSSL (FREAK)	●●○○○	●●●●●	●●○○○	5,0	4,1

Fonte: Cisco Security Research

Redução das explorações com o uso de Java

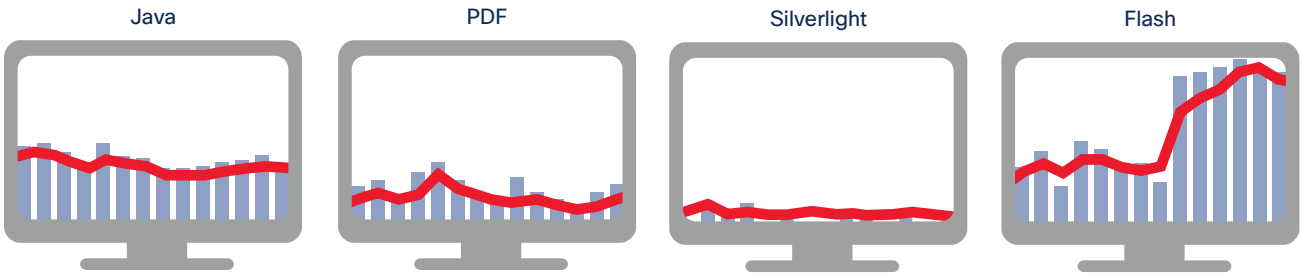
Seguindo uma tendência que monitoramos e abordamos no Relatório de anual sobre segurança da Cisco de 2015[4], as explorações envolvendo Java apresentaram queda na primeira metade de 2015. O Java costumava ser o vetor de ataque preferido de criminosos on-line, mas os aprimoramentos de segurança e os esforços de correção obrigaram os invasores a desistirem dele. Nenhuma exploração de dia zero para o Java foi divulgada desde 2013.

A Oracle realizou várias ações para melhorar a segurança do Java como, por exemplo, encerrar miniaplicativos não assinados. O Java 8, a versão mais recente, possui controles mais eficientes do que os das versões anteriores. Ele é mais difícil de explorar porque requer a interação com usuários humanos, como caixas de diálogo que pedem ao usuário para ativar o Java.

Em abril de 2015, a Oracle anunciou que encerraria o suporte ao Java 7.[5] Infelizmente, quando os fornecedores deixam de oferecer suporte para uma determinada versão de um produto, as empresas não adotam a nova versão de imediato. Esse tempo de retardo abre uma janela de oportunidades para os criminosos explorarem as vulnerabilidades na versão agora sem suporte. Ao longo do ano, poderemos ver um aumento no número de explorações do Java, conforme as empresas migram do Java 7 para o Java 8.

Figura 18. Muitos vetores de malware comuns

Compartilhe o relatório



Fonte: Cisco Security Research

A Figura 18 mostra o volume de registros de explorações do Java, do Flash e de PDF na primeira metade de 2015. Em geral, embora variem mês a mês, as explorações de PDF não são tão comuns quanto as explorações do Flash. Como o Flash é a ferramenta preferida dos desenvolvedores de kits de exploração, sua presença no gráfico de volume de registros acima pode estar diretamente associada a surtos de atividade criminosa envolvendo kits de exploração como o Angler (consulte a página 10). Além disso, o volume de explorações do Silverlight é muito pequeno em comparação com o número de explorações baseadas em Flash, PDF e Java.

4 Relatório anual sobre segurança da Cisco de 2015, janeiro de 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

5 "Oracle to End Publicly Available Security Fixes for Java 7 This Month" (Oracle encerrará este mês correções de segurança para Java 7 disponíveis publicamente), por Paul Krill, *InfoWorld*, 15 de abril de 2015: http://www.infoworld.com/article/2909685/application-development/oracle-cutting-publicly-available-security-fixes-for-java-7-this-month.

Autores de malware adotam táticas de detecção e evasão

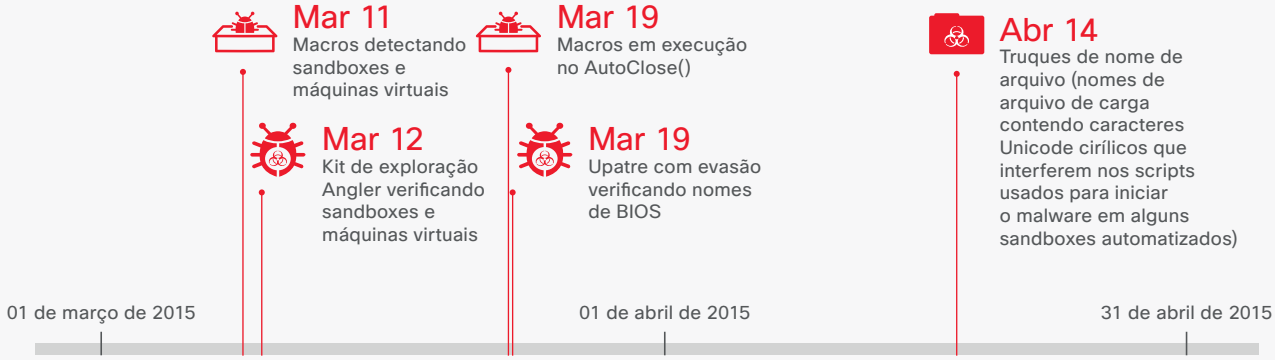
Os criminosos on-line se tornaram especialistas em ocultar suas atividades dos pesquisadores de segurança e das soluções de tecnologia. Por exemplo, eles criam malware que tenta escapar de controles tradicionais como os sandboxes usados pelos pesquisadores para iniciar malware e registrar sua atividade.

Nos casos que examinamos, esse malware não seria ativado se detectasse atividade de sandbox. Essa tática foi observada em uma variação do kit de exploração Angler, em algumas variações do malware Upatre e em documentos mal-intencionados do Microsoft Office.

Para combater malwares que usam essas táticas de evasão, as empresas precisam adotar uma abordagem de defesa intensa que inclua a capacidade de verificar e identificar malware retrospectivamente, mesmo depois de ele passar pelas linhas iniciais de defesa.

Detecção de sandbox recente

A detecção de sandbox não é uma tática nova dos autores de malware, mas está se tornando cada vez mais comum, segundo nossos pesquisadores, que encontraram os seguintes incidentes entre março e abril de 2015:



Risco vertical de detecções de malware: nenhum setor está imune a ataques

A fim de apresentar resultados mais precisos, a Cisco aperfeiçoou e simplificou sua metodologia para rastrear mercados com alto risco de ataques de malware na Web. Não comparamos mais a taxa média de ataques de todas as empresas que usam o Cisco® Cloud Web Security com a taxa média de ataques de todas as empresas de um determinado setor que estejam usando o serviço. Agora, comparamos os volumes relativos de tráfego de ataque ("taxas de bloqueio") com os do tráfego "normal" ou esperado.

A Figura 19 mostra 25 dos principais setores e sua atividade de bloqueio relevante como uma proporção do tráfego de rede normal. Uma proporção de 1,0 significa que o número de bloqueios é proporcional ao volume de tráfego observado. Qualquer coisa acima de 1,0 representa taxas de bloqueio maiores que o esperado, e qualquer coisa abaixo de 1,0 representa taxas de bloqueio menores que o esperado.

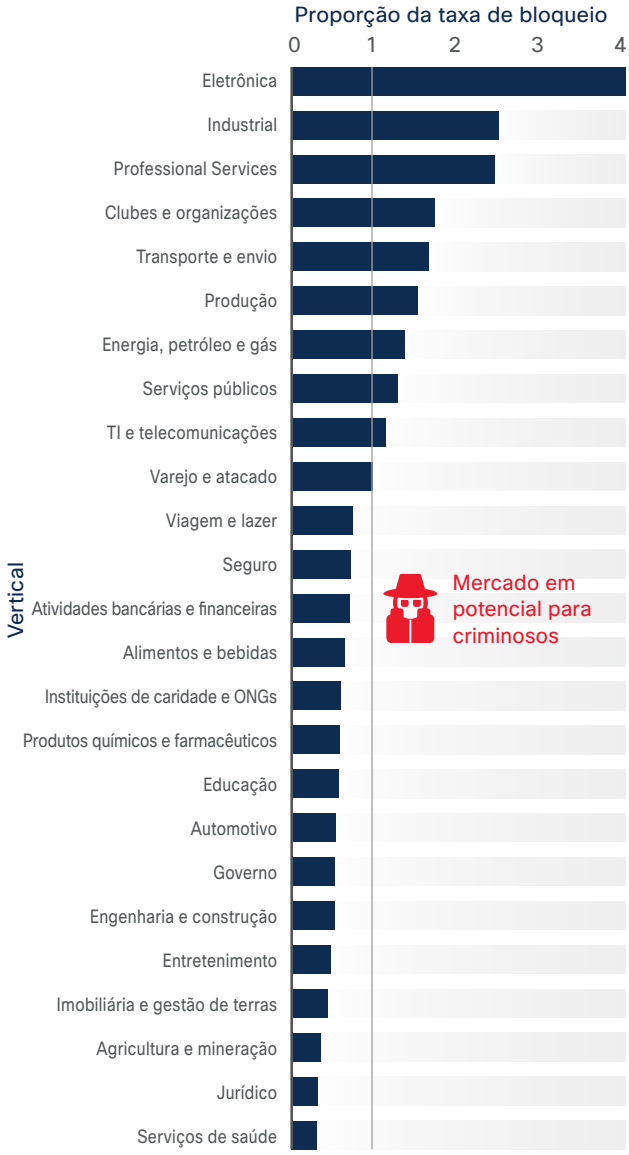
Por exemplo, as taxas de bloqueio do setor de varejo e atacado são proporcionais ao volume de tráfego observado para esse setor.

Ao examinar as taxas de bloqueio dos clientes da Cisco, determinamos que o setor de eletrônicos tem a maioria dos ataques bloqueados entre os 25 setores rastreados. A Cisco atribui essa alta proporção a um surto do spyware Android.

Como observado na Figura 19, a maioria dos setores fica no nível "normal" (a linha 1,0) da taxa de ataques para tráfego de rede normal. No entanto, apontar os setores que estão acima da linha 1,0 como muito mais vulneráveis a ataques pode induzir a erros, principalmente porque essa análise engloba apenas a primeira metade de 2015.

Além disso, em termos de ser ou não visado, nenhum setor deve se considerar "mais seguro" do que outros. Cada empresa em cada setor deve assumir que é vulnerável, que vão ocorrer ataques e que deve implementar as devidas estratégias de defesa intensa.

Figura 19. Taxas de bloqueio de mercados verticais em comparação com o volume de tráfego observado



Fonte: Cisco Security Research

Compartilhe o relatório

Atividade de bloqueio: visão geral geográfica

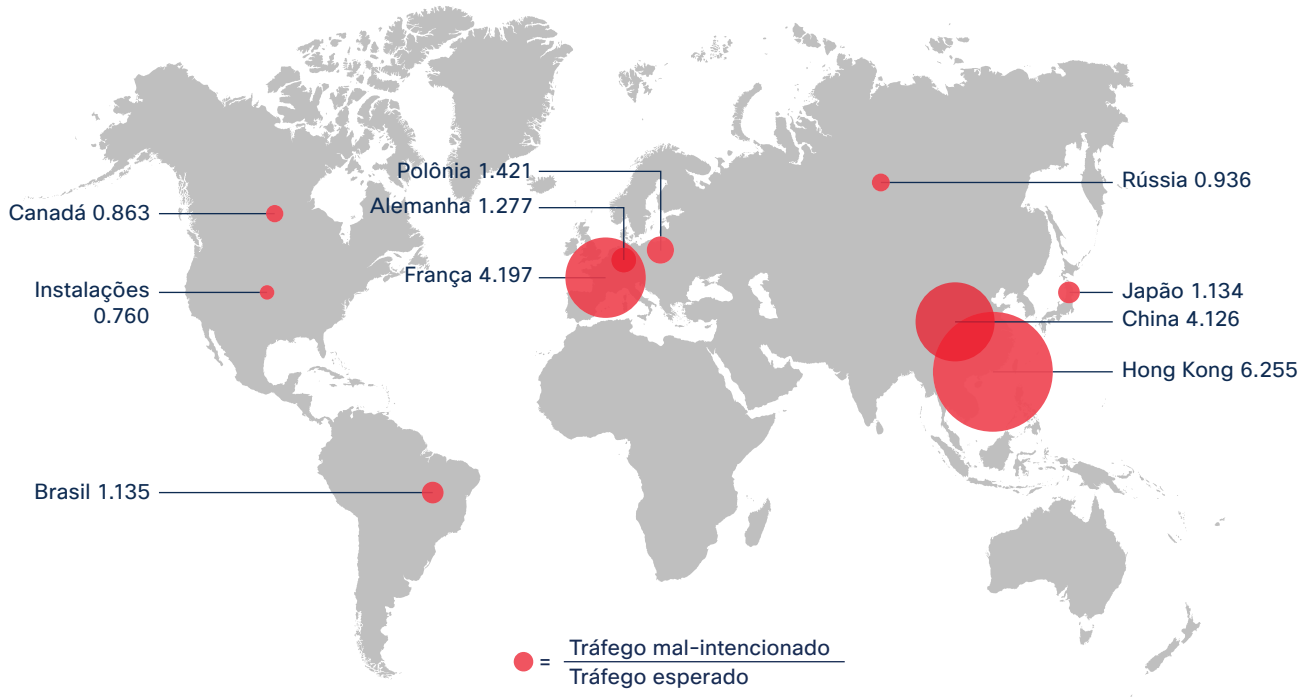
Os pesquisadores da Cisco também examinaram os países e as regiões onde se originam as atividades de bloqueio de malware, como visto na Figura 20. Os países foram selecionados para estudo com base no seu volume de tráfego na Internet. Uma taxa de bloqueio de 1,0 indica que o número de bloqueios observados é proporcional ao tamanho da rede.

O malware ocupa posição de destaque em dispositivos vulneráveis. Países e regiões com atividade de bloqueio que consideramos mais alta que o normal provavelmente têm muitos hosts e servidores da Web com vulnerabilidades não corrigidas em suas redes. Uma presença em redes grandes e comercialmente viáveis nas quais trafegam um grande volume de Internet é outro fator para a alta atividade de bloqueio.

A Figura 20 mostra onde os servidores estão hospedados. Este gráfico não atribui padrões de atividade mal-intencionada na Web aos países ou regiões descritos. Hong Kong, que ocupa a posição nº 1 na lista, é um exemplo de região em que foi observado um alto percentual de servidores Web vulneráveis. Um pequeno número de redes hospedadas na França participou de um surto no meio do período do relatório, o que elevou seu perfil para níveis além do esperado.

Figura 20. Bloqueios da Web por país ou região

Compartilhe o relatório



Fonte: Cisco Security Research

Tipos de ataques baseados na Web

As Figuras 21 e 22 mostram os diversos tipos de técnicas que os criminosos usam para acessar redes empresariais. A Figura 21 ilustra os métodos mais utilizados, como tentativas de fraude no Facebook e redirecionamentos mal-intencionados.

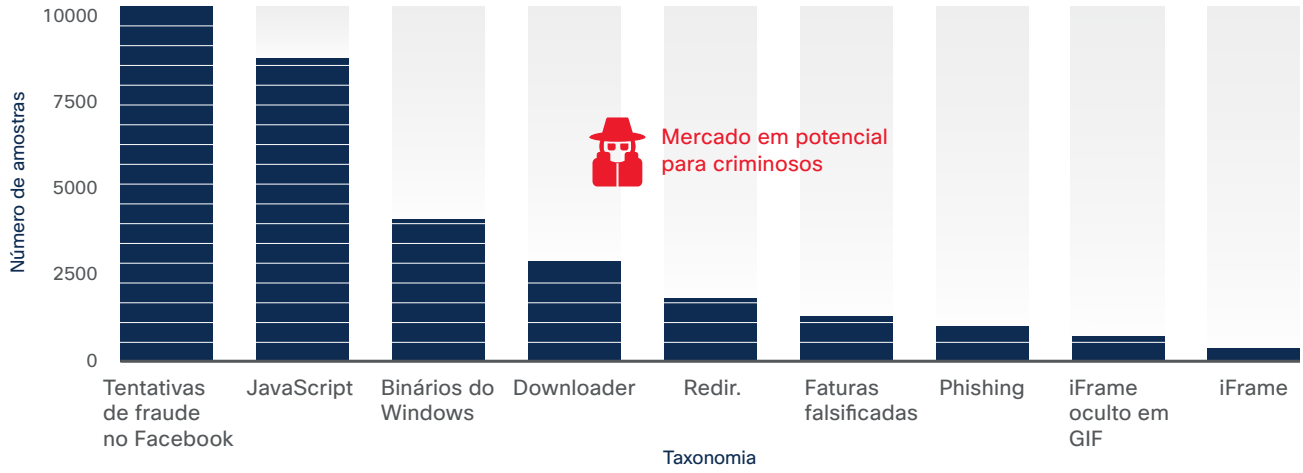
A Figura 22 mostra métodos de ataque de volume menor observados na amostra cega que examinamos. Observe que "volume menor" não significa "menos eficácia".

Métodos de ataque de volume menor e o malware associado a eles podem representar ameaças emergentes ou campanhas altamente direcionadas.

Portanto, durante o monitoramento de malware na Web, não basta simplesmente se concentrar nos tipos de ameaças mais comuns. Todo o espectro de ataques deve ser considerado.

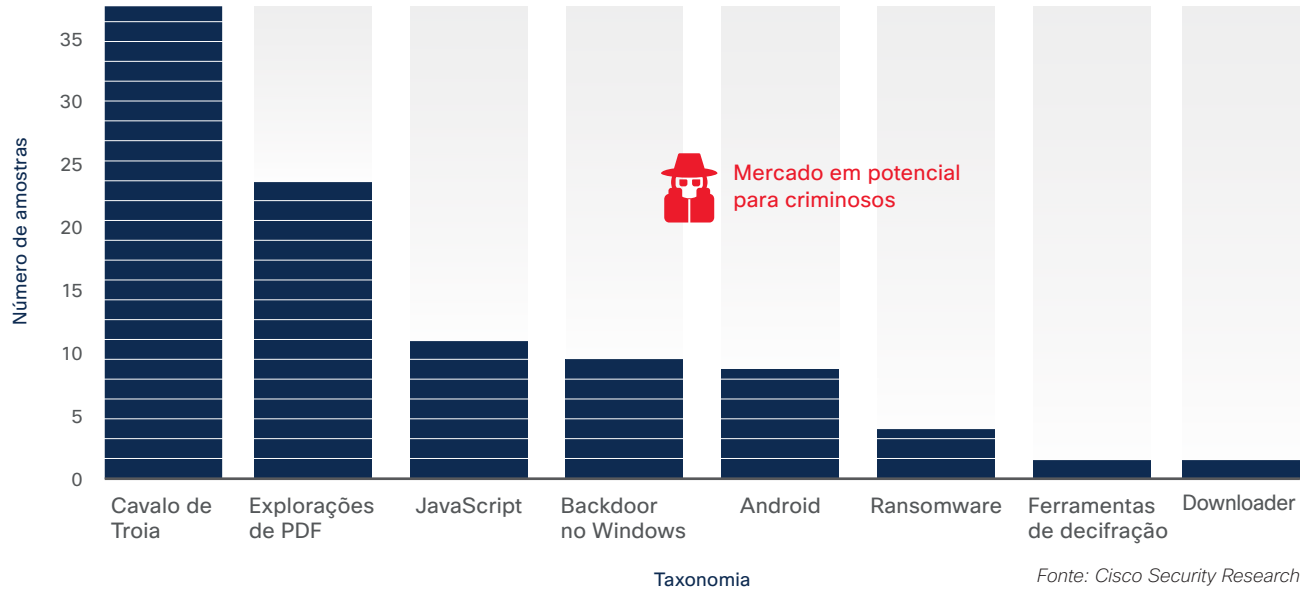
Figura 21. Métodos observados com mais frequência

Compartilhe o relatório



Fonte: Cisco Security Research

Figura 22. Exemplo de métodos de volume menor observados



Fonte: Cisco Security Research

Atualização sobre malvertising: ameaça da Web amplamente difundida muda para escapar da detecção e aumentar sua eficiência

Conforme indicado no Relatório anual sobre segurança da Cisco de 2015,[6] realizamos uma análise aprofundada em 2014 de uma ameaça baseada na Web do tipo botnet altamente sofisticada, que usa malvertising (publicidade on-line mal-intencionada) de complementos do navegador da Web como meio de distribuir aplicações e malware indesejados. Essa família de malware tem uma assinatura clara: Adware MultiPlug. As extensões do navegador são fornecidas junto com outras aplicações aparentemente úteis, ainda que indesejadas, como ferramentas de PDF e players de vídeo.

Os usuários são afetados quando instalam essas aplicações indesejadas e o pacote de software que as acompanha. Em muitos casos, trata-se de complementos do navegador, nos quais eles confiam cegamente ou que consideram benignos. As informações de usuário – especificamente a página da Web interna ou externa que o usuário está visitando (e não as credenciais dele) – são extraídas por essas extensões do navegador quando instaladas.

A distribuição do malware segue um esquema de monetização PPI (pagamento por instalação), no qual o publicador é pago por cada instalação do software oferecido em conjunto com a aplicação original. Isso leva à maior prevalência do malware projetado deliberadamente para reduzir o impacto no host afetado e otimizado para monetização a longo prazo em uma grande população afetada.

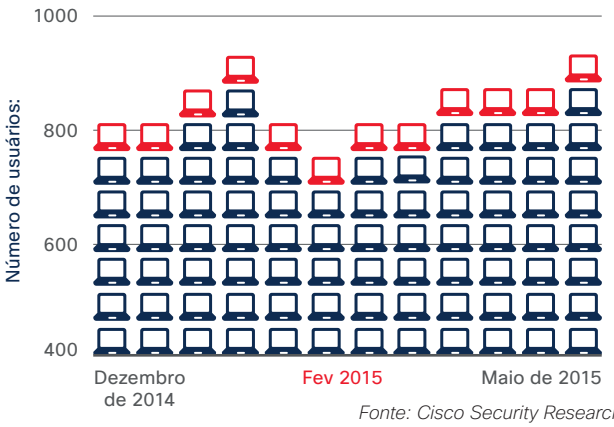
Disfarçado no tráfego comum da Web

A Cisco vem monitorando esta ameaça há mais de um ano. Observamos que a ameaça muda constantemente para continuar sem ser detectada. Três meses é o tempo médio durante o qual a ameaça usa um nome de domínio, e os nomes dos complementos são alterados com frequência. Conforme informado no Relatório anual sobre segurança da Cisco de 2015, até agora descobrimos mais de 4.000 nomes de complementos diferentes e mais de 500 domínios associados a essa ameaça.

Em janeiro de 2015, os pesquisadores começaram a perceber que a ameaça era mutável. Ela abandonava seu esquema de codificação de URL para escapar da detecção e se esconder no tráfego comum da Web. Aparentemente, essa mudança de tática aumenta a eficácia da ameaça em comprometer os usuários.

Nós rastreamos o tráfego associado a esse novo padrão até agosto de 2014, mas isso só se tornou perceptível devido ao volume de tráfego no período compreendido entre dezembro de 2014 e janeiro de 2015. Como mostra a Figura 23, o número de usuários afetados associados a essa ameaça vem apresentando uma tendência de aumento geral desde fevereiro.

Figura 23. Número de usuários afetados por mês (dezembro de 2014 a maio de 2015)



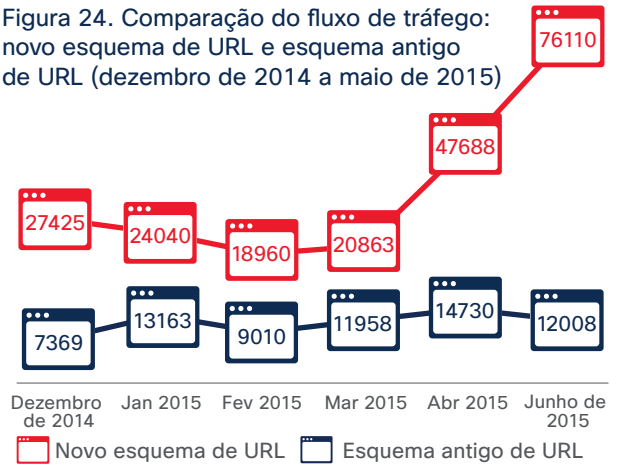
Fonte: Cisco Security Research

Para obter mais detalhes sobre essa pesquisa, consulte a publicação **"Bad Browser Plug-Ins Gone Wild: Malvertising, Data Exfiltration, and Malware, Oh My!"** (Plug-ins de navegador inválidos: Malvertising, extração de dados e malware) no blog do Talos Group.

6 Relatório anual sobre segurança da Cisco de 2015, janeiro de 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

A Figura 24 ilustra como o número de fluxos de tráfego relacionados ao novo esquema de URL tem ultrapassado em muito os do antigo esquema, principalmente desde março de 2015.

Figura 24. Comparação do fluxo de tráfego: novo esquema de URL e esquema antigo de URL (dezembro de 2014 a maio de 2015)



Fonte: Cisco Security Research

Definição de tempo de detecção

Definimos "tempo de detecção" (ou "TTD") como a janela de tempo entre a primeira observação de um arquivo e a detecção de uma ameaça. Para determinar essa janela de tempo, usamos a telemetria de segurança opcional obtida dos produtos de segurança da Cisco implantados em todo o mundo.

A categoria "retrospectivas" na Figura 25 mostra o número de arquivos que a Cisco categorizou inicialmente como "desconhecidos" e que depois foram considerados "reconhecidamente não confiáveis".

O número de retrospectivas tem aumentado desde dezembro de 2014. Essa tendência também é outro indicador de que os autores de malware inovam rapidamente para se manterem um passo à frente dos fornecedores de segurança. Ao mesmo tempo, porém, o TTD médio para detecção de ameaças pela Cisco tem caído.

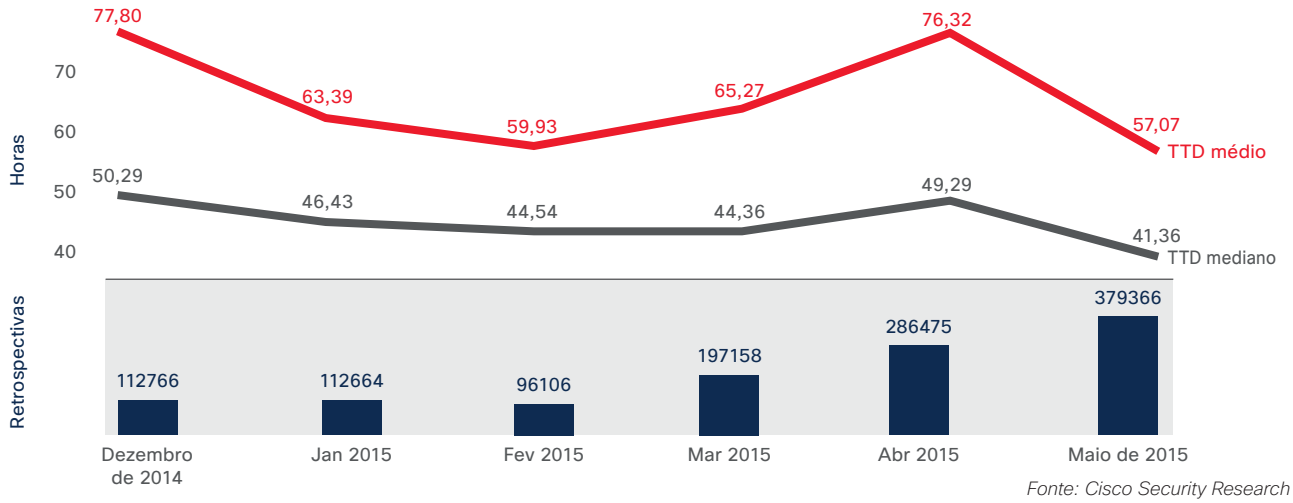
Em dezembro de 2014, o TTD médio (ou seja, o tempo necessário para uma análise revelar se um arquivo desconhecido é uma ameaça) foi de dois dias (50 horas). O padrão do setor atual para o tempo de detecção é de 100 a 200 dias – um nível inaceitável, dada a rapidez com que os autores de malware de hoje são capazes de inovar.

Nós atribuímos a recente tendência de elevação nas retrospectivas a um aumento na atividade evasiva (consulte "Autores de malware adotam táticas de detecção e evasão", na página 25) e às distribuições bem-sucedidas de carga de novas explorações no Flash pelos kits de exploração Angler e Nuclear (consulte a página 9).

De janeiro a março, o TTD médio foi aproximadamente o mesmo: entre 44 e 46 horas, com ligeira tendência de queda. Em abril, ele subiu um pouco, para 49 horas.

No entanto, no final de maio, o TTD da Cisco diminuiu para cerca de 41 horas. Essa melhoria deve-se, em parte, à capacidade da Cisco de identificar rapidamente malwares comuns, como o Cryptowall, que, embora evasivo, não é uma novidade.

Figura 25. Retrospectivas, TTD médio e mediano (dezembro de 2014 a maio de 2015)



Fonte: Cisco Security Research

Análise e observações

Plano de ação da segurança cibernética: rapidez na inovação por parte dos fornecedores de segurança

Os especialistas em segurança da Cisco sugerem que a mudança é iminente para o setor de segurança. É necessária uma onda de consolidação e integração para desenvolver soluções de segurança inovadoras, adaptáveis e confiáveis que consigam reduzir o tempo de detecção e prevenir ataques. Além disso, nossos especialistas geopolíticos disponibilizam informações úteis sobre a importância da administração cibernética para o apoio à inovação e ao crescimento econômico da empresa no cenário mundial.

Em um mundo no qual o comprometimento de usuários e sistemas é tanto garantido quanto assumido, a detecção de ameaças evasivas é um foco óbvio e necessário para empresas e equipes de segurança. É cada vez maior a atividade de ameaças, inclusive a atividade de estados-nações. Com isso, muitas empresas pensam ainda mais seriamente em desenvolver planos de continuidade de negócios que possam ajudá-las a recuperar serviços essenciais após um ataque cibernético contra a empresa ou a infraestrutura que a apoia.

No entanto, vimos também uma demanda perceptível tanto de empresas como de indivíduos para o setor de segurança desenvolver recursos capazes de rechaçar, e não só detectar, ataques cibernéticos com mais eficiência. No mínimo, eles buscam soluções com mais rapidez de detecção e resolução.

A complexidade de segurança está a caminho de atender a essas demandas, por enquanto.

Em um lado do setor de segurança estão concorrentes grandes e bem estabelecidos que criam conjuntos de segurança baseados em um ou mais produtos de destaque. No entanto, esses conjuntos também podem conter outras soluções que não são tão eficazes quanto as soluções líderes ou que não funcionam com elas.

Enquanto isso, alguns fornecedores de nicho estão desenvolvendo produtos para ajudar a preencher as lacunas de segurança. Muitas empresas são rápidas em investir nas últimas inovações que preenchem uma lacuna conhecida, em vez de dar um passo atrás para analisar a segurança de maneira global.

O resultado é uma "colcha de retalhos" de produtos que dificulta o gerenciamento por parte das equipes de segurança. As soluções podem ter recursos sobrepostos, podem não atender aos padrões do setor e provavelmente não são interoperáveis. E as tecnologias de nicho que não podem ser implantadas em escala para atender às necessidades de usuários normais geralmente duram pouco, independentemente da sua eficácia.

Além disso, muitas tecnologias de segurança exigem que as empresas reestruturem sua arquitetura de segurança apenas para se adaptarem aos riscos mais recentes. Essas tecnologias não são capazes de evoluir com o cenário de ameaças em constante mudança, não importa de que lado do espectro do setor de segurança elas venham. Não é um modelo sustentável.

Consolidação do setor e defesa integrada contra ameaças

Nossos especialistas em segurança sugerem que a necessidade de soluções adaptáveis levará a uma mudança significativa no setor de segurança nos próximos cinco anos. Veremos a consolidação do setor e um movimento rumo a uma arquitetura de defesa integrada contra ameaças que proporciona visibilidade, controle, inteligência e contexto em muitas soluções.

Essa estrutura de detecção e resposta permitirá uma resposta mais rápida a ameaças tanto conhecidas como emergentes. A essência dessa arquitetura é uma plataforma de visibilidade que disponibiliza reconhecimento contextual completo. Ela deve ser continuamente atualizada para avaliar ameaças, correlacionar inteligência local e global e otimizar defesas. A inteligência local disponibiliza infraestrutura referente ao contexto, enquanto a inteligência global correlaciona todos os eventos detectados e os indicadores de comprometimento para proteção compartilhada imediata e análise.

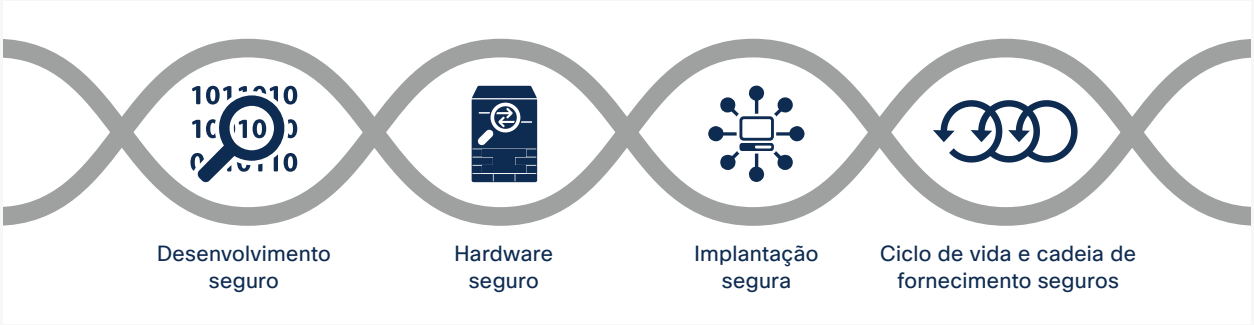
A intenção da plataforma de visibilidade é criar uma base com a qual todos os fornecedores possam operar e contribuir. Esse sistema reunirá o enorme volume de informações de segurança disponibilizadas pela comunidade de segurança e atuará sobre ele. A visibilidade proporcionada por ele daria às equipes de segurança mais controle, permitindo oferecer uma proteção melhor em mais vetores de ameaça e contornar mais ataques.

Essa é a direção que o setor de segurança deve seguir para ajudar todos os usuários finais a se defenderem das sofisticadas táticas dos autores de ameaças de hoje. No entanto, o desenvolvimento de uma defesa integrada contra ameaças, conforme descrito aqui, exigirá melhor cooperação, diálogo e ação coordenada entre todos os fornecedores de segurança igualmente, tanto inovadores de nicho como concorrentes antigos no mercado.

O setor caminha a passos largos para compartilhar informações de forma mais proativa e apropriada, especialmente por meio de alianças. Mas a troca automatizada e em tempo real de informações sobre ameaças é indispensável para estimular a inovação necessária na defesa de segurança e obter resposta sistêmica na pilha de segurança implantada. Quanto mais rápido o setor puder distribuir conhecimento e inteligência pela rede de uma forma coesa e aceitável, menor será a probabilidade de os criminosos desfrutarem de sucesso e anonimato contínuos.

Produtos de confiança

Compartilhe o relatório



Com a maior consolidação e integração no setor de segurança prevista para os próximos cinco anos, as empresas que adquirirem produtos e serviços de segurança deverão garantir que essas soluções sejam eficazes, sustentáveis e confiáveis.

Elas devem reservar um tempo para entender o que os fornecedores de segurança e outros fornecedores de TI estão fazendo para incorporar a segurança a seus produtos. As empresas também devem verificar se esses produtos continuam confiáveis em cada ponto da cadeia de fornecimento que disponibiliza esses produtos para ela. Além disso, devem pedir aos fornecedores para demonstrar que seus produtos são de confiança e substanciar suas declarações contratualmente.

A importância do conhecimento especializado

Os fornecedores de segurança têm uma função importante a desempenhar para ajudar os usuários finais a entenderem a importância de investir em soluções confiáveis e manter a tecnologia de segurança atualizada. As empresas que dependem de uma infraestrutura desatualizada acabam colocando em risco dados, sistemas e usuários – ou seja, a empresa inteira.

A defasagem cada vez maior de profissionais especializados em segurança implica que muitas empresas têm recursos qualificados limitados para monitorar os desenvolvimentos tanto em ambientes de risco quanto no cenário de fornecedores. A falta de experiência em segurança por parte dos funcionários é um fator primordial para a abordagem fragmentada ("colcha de retalhos") que muitas empresas adotam ao criar suas defesas de segurança (consulte a página 32).

O recrutamento de terceiros com experiência oferece às empresas a flexibilidade necessária para dinamizar o sempre diferente panorama de ameaças. Os fornecedores de serviços de segurança estão bem posicionados para analisar a segurança de maneira global e ajudar as empresas a investirem e aproveitarem ao máximo seus investimentos em segurança.

Além de incrementar equipes de segurança enxutas, os especialistas terceirizados podem oferecer avaliações que testam a capacidade dos procedimentos de segurança de uma empresa. E podem ajudar a identificar estratégias eficazes para lidar com vulnerabilidades e outros riscos. Eles também podem ajudar as empresas a implantarem automação e gerenciarem soluções que forneçam a análise e a correlação de ameaças em tempo real necessárias para combater ameaças difíceis de detectar e que surgem rapidamente.

Algumas empresas procuram orientação junto aos fornecedores de serviços de segurança quando adotam modelos de negócios móveis, sociais, em nuvem e outros modelos de negócios emergentes. Outras buscam ajuda na privacidade de dados de navegação e em requisitos de soberania de dados nos mercados em que operam. Há também aquelas que contatam especialistas terceirizados para ajudá-las a encontrar modelos gerenciados e hospedados que atendam às suas necessidades, como as empresas de pequeno e médio porte que desejam tirar proveito de operações e tecnologias de segurança adotadas por grandes corporações.

Uma estrutura global de administração cibernética para apoiar a inovação futura

Empresas do mundo todo confiam cada vez mais na Internet para desenvolver modelos de negócios que as tornam mais competitivas e beneficiam seus clientes. Mas elas enfrentam criminosos que vêm implantando táticas capazes de minar seu sucesso. Se não forem vigiados, os riscos cibernéticos terão consequências graves na inovação e no crescimento econômico de todas as empresas.

Segundo os especialistas geopolíticos da Cisco, uma estrutura de administração cibernética coesa e com vários participantes representa um passo positivo para a sustentação da inovação empresarial e do crescimento econômico da empresa no no cenário mundial, apoiando os investimentos das empresas na economia digital. No entanto, a estrutura de administração atual não protege as empresas contra ataques cibernéticos. Esses ataques incluem não só os que levam a violações de dados e roubo de propriedade intelectual, como também aqueles capazes de interromper cadeias de fornecimento globais, danificar a infraestrutura crítica, ou até pior.

Muitas empresas não buscam soluções para ataques cibernéticos porque não recebem apoio das autoridades de outros países. No entanto, mais governos estão se abrindo ao conceito de atribuição pública de ataques e à imposição de sanções.

A falta de uma administração cibernética global eficaz também pode impedir a colaboração necessária no setor de segurança para criar tecnologias adaptáveis capazes de detectar e prevenir novas ameaças. Recentemente, foram propostas alterações no Wassenaar Arrangement[7], um acordo multinacional voluntário cuja finalidade é controlar a exportação de certas tecnologias de "uso duplo", inclusive software invasivo, como ferramentas de vigilância digital. Tais propostas ameaçam restringir esse controle e impedir que os pesquisadores de segurança compartilhem informações com seus colegas sem pesados encargos regulatórios. Esse desenvolvimento pode ter um impacto significativo sobre os recursos de pesquisa de segurança e exacerbar ainda mais a falta de profissionais especializados no setor.

Maior harmonização na criação de regras: um caminho futuro?

A questão dos limites – especialmente em relação ao modo como os governos coletam dados sobre cidadãos e empresas e compartilham, ou não, essas informações entre as jurisdições – é um obstáculo significativo ao tipo de cooperação necessário para conseguir uma administração cibernética coesa. À medida que a Internet das Coisas toma forma e o mundo se torna mais interconectado, a indústria, os governos e a sociedade precisam trabalhar juntos de maneira mais eficaz para enfrentar desafios cada vez maiores de segurança e privacidade.

No momento, a cooperação e a confiança entre as entidades no plano global estão limitadas, na melhor das hipóteses, a alguns concorrentes e não existe entre outros. Até mesmo entidades com alianças sólidas têm filosofias diferentes sobre a administração cibernética e estão naturalmente focadas em aprovar leis que beneficiem seus interesses soberanos e seus cidadãos. Assim como as discussões sobre mudanças climáticas, somente alguns escolhidos vão se sentar à mesa para dialogar, e é difícil obter um consenso até mesmo para pequenas medidas.

A nível regional, pelo menos, há alguns esforços para olhar além das fronteiras nacionais. Por exemplo, na União Europeia, há um movimento para melhorar a coordenação do compartilhamento de informações por meio da diretiva NIS (Network and Information Security) proposta. Essa diretiva "visa assegurar um alto nível comum de segurança cibernética na União Europeia" ao "melhorar a cooperação entre estados-membro e entre os setores público e privado", além de outras medidas.[8]

A União Europeia e os Estados Unidos também parecem estar perto de assinar um acordo abrangente que definirá os padrões de proteção de dados para os dados compartilhados entre as autoridades. Esse acordo não responderá a questões mais amplas relacionadas ao tipo de dados que podem ser acessados e de que maneira. Mas ele pode, de alguma forma, melhorar a atmosfera tensa entre os dois poderes, que ameaçavam colocar as empresas no meio de um conflito de jurisdição. As equipes jurídica, técnica e de segurança de empresas que operam na União Europeia e nos Estados Unidos precisarão trabalhar em conjunto nos requisitos de acesso caso esse acordo abrangente seja assinado.

7 "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items" (Implementação dos contratos de plenário do Acordo de Wassenaar 2013: itens de invasão e vigilância), *Registro federal*: https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

8 "Network and Information Security (NIS) Directive" (Diretiva NIS [Network and Information Security]), Comissão Europeia: http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

Porém, há outra legislação em análise na Europa que pode acabar criando mais limites, especialmente para empresas. As instituições da União Europeia pretendem finalizar o novo Regulamento Geral de Proteção aos Dados (GDPR, General Data Protection Regulation) até o final do ano, para substituir a diretiva de proteção a dados atual.

Esse regulamento contém uma definição ampla de dados pessoais e regras prescritivas sobre como esses dados devem ser gerenciados, sob pena de serem aplicadas multas pesadas. Ele terá um impacto considerável no modo como as empresas que fazem negócios com a União Europeia coletam, armazenam e usam dados de clientes e na forma como elas relatam violações de dados. Criado para gerar mais responsabilidade e transparência, o GDPR obrigará mais empresas a adotarem melhores práticas e examinarem sua abordagem à privacidade de dados e à administração.

As equipes técnicas, por exemplo, terão que levar em conta considerações de design a respeito de limitações ou dificuldades associadas à movimentação de dados entre fronteiras. Elas precisarão conhecer os diferentes graus de confidencialidade de dados caracterizados como "pessoais" ou não por região. As equipes de segurança também deverão ter consciência dos desenvolvimentos que afetam a transferência de dados, a definição de dados pessoais, os requisitos para emissão de relatórios de violação de dados e a base legal para o processamento de segurança de informações e da rede.

Uma maior harmonização na criação de regras pode servir como caminho para a criação de uma estrutura de administração cibernética que eleva a defesa das negociações entre os governos no tocante a regulamentos de proteção aos dados e, ao mesmo tempo, impede que o setor seja pego desprevenido. Até isso acontecer, os profissionais de segurança precisam desempenhar um papel ativo para assegurar que os tomadores de decisão em suas empresas entendam o impacto que os regulamentos emitidos por diferentes países pode ter nas operações. Entre os desafios estão sistemas incompatíveis, requisitos de dados conflitantes ou trabalhosos, violações da lei de privacidade e requisitos para manuseio e transferência de dados.

Conclusão

Conclusão

As ameaças discutidas neste relatório representam apenas uma pequena amostra dos desafios de segurança cibernética enfrentados por empresas, equipes de segurança e usuários. Até agora, 2015 parece ser um ano de velocidade sem precedentes em termos de inovação, resiliência e capacidade de evasão por parte dos ataques cibernéticos. Os criminosos pretendem derrubar todas as barreiras para atingir o sucesso. Eles dinamizam ou alteram suas táticas com a mesma rapidez com que o setor de segurança consegue desenvolver tecnologias para bloquear e detectar ameaças.

A disputa por inovações entre criminosos e fornecedores de segurança está cada vez mais acirrada, e as empresas correm o risco de ficar mais vulneráveis a ataques se não fizerem nada. Elas precisam mostrar proatividade na identificação e resolução de riscos de segurança cibernética que possam afetar os negócios, como também no alinhamento de pessoas, tecnologias e processos certos para enfrentar esses desafios.

"A segurança precisa fazer parte do pensamento holístico das empresas sobre seus negócios", diz David Goeckeler, vice-presidente sênior e gerente geral do grupo de segurança empresarial da Cisco. "Há muito em risco: marca, reputação, propriedade intelectual e dados de clientes. Tudo isso está em risco. As empresas precisam adotar uma abordagem sistêmica para minimizar esses riscos com procedimentos de segurança apropriada."

"Produtos confiáveis são um componente essencial de procedimentos eficientes de segurança", afirma John N. Stewart, diretor de segurança e confiança da Cisco. "As empresas não querem mais aceitar que o comprometimento é inevitável", diz ele. "Elas procuram o setor de segurança para obter produtos confiáveis, resilientes e capazes de rechaçar até as ameaças mais avançadas."

Sobre a Cisco

Sobre a Cisco

A Cisco oferece segurança cibernética inteligente para o mundo real, disponibilizando um dos portfólios de soluções mais amplos para proteção avançada contra ameaças em todo o abrangente conjunto de vetores de ataque. A estratégia de segurança operacionalizada com foco em ameaças da Cisco reduz a complexidade e a fragmentação, proporcionando maior visibilidade, controle uniforme e proteção avançada contra ameaças antes, durante e após um ataque.

Os pesquisadores de ameaças do ecossistema Cisco Collective Security Intelligence (CSI) reúnem, em uma mesma área, a inteligência de ameaças líder do setor, usando a telemetria obtida através da ampla variedade de dispositivos e sensores, de feeds públicos e privados e da comunidade de código aberto da Cisco. Isso equivale à entrada diária de bilhões de solicitações da Web e milhões de e-mails, amostras de malware e invasões de rede.

Nossa infraestrutura e nossos sistemas sofisticados consomem essa telemetria, ajudando pesquisadores e sistemas de aprendizado em máquina a monitorar ameaças em redes, data centers, terminais, dispositivos móveis, sistemas virtuais, Web, e-mail e na nuvem, a fim de identificar as principais causas e o escopo de ataques. A inteligência resultante é convertida em proteções em tempo real para nossas ofertas de produtos e serviços, que são fornecidos de imediato para clientes da Cisco no mundo inteiro.

Para saber mais sobre a estratégia de segurança com foco em ameaças da Cisco, acesse www.cisco.com/go/security.

Colaboradores do Relatório semestral sobre segurança da Cisco de 2015

Collective Security Intelligence

O Cisco Collective Security Intelligence (CSI) é compartilhado entre várias soluções de segurança e oferece eficácia e proteções de segurança que são líderes do setor. Além dos pesquisadores de ameaças, o CSI é pautado pela infraestrutura de inteligência, telemetria de serviços e produtos, feeds públicos e privados e a comunidade de código aberto.

Talos Security Intelligence and Research Group

O Talos Security Intelligence and Research Group é formado pelos melhores pesquisadores de ameaças, com o apoio de sofisticados sistemas para criar inteligência de ameaças para produtos da Cisco que detectam, analisam e protegem contra ameaças conhecidas e emergentes. O Talos mantém os conjuntos de regras oficiais de Snort.org, ClamAV, SenderBase.org e SpamCop e é a principal equipe a contribuir com informações de ameaças para o ecossistema Cisco CSI.

Equipe do IntelliShield

A equipe do IntelliShield executa pesquisas sobre ameaças e vulnerabilidades, análise, integração e correlação de dados e informações do Cisco Security Research & Operations e de fontes externas para produzir o IntelliShield Security Intelligence Service, que sustenta vários produtos e serviços da Cisco.

Equipe do Active Threat Analytics

A equipe do Cisco Active Threat Analytics (ATA) ajuda as empresas a se defenderem de ameaças persistentes avançadas, invasões conhecidas e ataques de dia zero aproveitando tecnologias avançadas de Big Data. Esse serviço totalmente gerenciado é oferecido por nossos especialistas em segurança e nossa rede global de centros de operações de segurança. Ele disponibiliza vigilância contínua e análise sob demanda 24 horas por dia, sete dias por semana.

Cognitive Threat Analytics

O Cognitive Threat Analytics da Cisco é um serviço em nuvem que detecta violações, malwares executados em redes protegidas e outras ameaças à segurança usando análise estatística de dados do tráfego de rede. Ele lida com defasagens nas defesas do perímetro identificando os sintomas de uma infecção por malware ou violação de dados usando a análise comportamental e a detecção de anormalidade. O Cognitive Threat Analytics conta com a modelagem estatística avançada e a aprendizagem automática para identificar novas ameaças de modo independente, aprender com o que é observado e fazer adaptações ao longo do tempo.

Sede – América
Cisco Systems, Inc.
San Jose. CA

Sede – Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede – Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site www.cisco.com/go/offices.