Cisco
Relatório Anual de Segurança Digital de 2017

cisco

Índice

Resumo executivo

À medida que a superfície de ataque aumenta, os defensores devem se concentrar em sua meta mais importante: reduzir o espaço operacional dos criminosos.

Os criminosos têm mais ferramentas à sua disposição do que nunca. Eles também têm uma noção aguçada de quando usar cada uma delas para obter o máximo efeito. O crescimento explosivo dos endpoints móveis e do tráfego on-line trabalha a favor deles. Eles têm mais espaço onde podem operar e mais opções de público-alvo e abordagens.

Os defensores podem usar uma variedade de estratégias para enfrentar os desafios de um cenário de ameaças em expansão. Eles podem adquirir as melhores soluções, que trabalham separadamente para proporcionar informações e proteção. E podem competir por profissionais em um mercado de talentos escassos e orçamentos apertados.

Pode não ser possível impedir todos os ataques. Mas você pode minimizar o risco e o impacto das ameaças restringindo o espaço operacional dos criminosos e, assim, a capacidade que eles têm de comprometer ativos. Uma medida que pode ser adotada é a simplificação do seu conjunto de ferramentas de segurança em uma arquitetura de segurança interconectada e integrada.

Ferramentas de segurança integradas que trabalham juntas em uma arquitetura automatizada podem otimizar o processo de detecção e mitigar as ameaças. Com isso, você terá tempo para resolver problemas mais complexos e persistentes. Muitas empresas usam pelo menos meia dúzia de fornecedores diferentes (página 53). Em muitos casos, as equipes de segurança podem investigar apenas metade dos alertas de segurança que recebem em um determinado dia.

O Relatório Anual de Segurança Digital da Cisco de 2017 apresenta pesquisa, informações e perspectivas do Cisco Security Research. Destacamos a dinâmica do cabo de guerra persistente entre criminosos que tentam obter mais tempo para operar e defensores que trabalham para fechar as janelas de oportunidade que os invasores tentam explorar. Examinamos os dados compilados por pesquisadores de ameaças da Cisco e outros especialistas. Nossas pesquisas e informações pretendem ajudar as empresas a responder com eficiência às ameaças sofisticadas em constante evolução de hoje em dia.

Este relatório está dividido nas seguintes seções:

Comportamento do invasor

Nesta seção, examinamos como os invasores fazem o reconhecimento de redes vulneráveis e oferecem malware. Explicamos como ferramentas como e-mail, aplicações em nuvem de terceiros e adware são convertidas em armas. Descrevemos também os métodos que os criminosos digitais empregam durante a fase de instalação de um ataque. Esta seção apresenta também nossa pesquisa "hora de evoluir" (TTE), que demonstra como os criminosos renovam suas táticas e evitam a detecção. Também oferecemos uma atualização dos nossos esforços para reduzir a mediana de tempo médio de detecção (TTD). Além disso, apresentaremos a mais recente pesquisa da Cisco sobre o risco de malware em vários setores e regiões.

Comportamento do defensor

Nesta seção, oferecemos atualizações sobre vulnerabilidades. Um dos focos são os pontos fracos que surgem em bibliotecas de middleware que representam oportunidades para os criminosos usarem as mesmas ferramentas em várias aplicações, reduzindo o tempo e os custos necessários para comprometer usuários. Também compartilhamos a pesquisa da Cisco sobre tendências de correção de falhas. Observamos o benefício de apresentar aos usuários um ritmo regular de atualizações para incentivar a adoção das versões mais seguras de navegadores da Web e soluções de produtividade comuns.

Estudo referencial de recursos de segurança da Cisco de 2017

Esta seção aborda os resultados do nosso terceiro Estudo referencial de recursos de segurança, que enfatiza as percepções dos profissionais de segurança sobre o estado da segurança em suas empresas. Neste ano, os profissionais de segurança parecem confiar nas ferramentas que têm disponíveis, mas não sabem se elas podem ajudar a reduzir o espaço operacional dos criminosos. O estudo também mostra que as violações de segurança pública estão tendo um impacto mensurável nas oportunidades, na receita e nos clientes. Ao mesmo tempo, as violações estão impulsionando a tecnologia e melhorias de processos nas empresas.

Para obter uma análise mais aprofundada sobre o estado da segurança em empresas, vá para a página 49.

Setor

Nesta seção, explicaremos a importância de garantir a segurança da cadeia de valores. Examinamos os possíveis danos de os governos acumularem informações sobre vulnerabilidades e explorações de dia zero em produtos de fornecedores. Além disso, discutimos o uso da criptografia rápida como solução para proteger dados em ambientes de alta velocidade. Por fim, descrevemos os desafios da segurança corporativa à medida que o tráfego global da Internet e a possível superfície de ataque aumentam.

Conclusão

Na conclusão, sugerimos que os defensores adaptem suas práticas de segurança para que enfrentem melhor os desafios de segurança típicos ao longo da cadeia de ataque e reduzam o espaço operacional dos criminosos. Esta seção também oferece orientação específica sobre como estabelecer uma abordagem integrada e simplificada da segurança: uma abordagem que conecte a liderança executiva, a política, os protocolos e as ferramentas para prevenir, detectar e mitigar ameaças.

Principais constatações

- Os três principais kits de exploração, Angler, Nuclear, e Neutrino, desapareceram de forma abrupta do cenário em 2016 deixando espaço para que concorrentes pequenos e novos participantes se destaquem.
- De acordo com o Estudo referencial de recursos de segurança da Cisco de 2017, a maioria das empresas usa mais de cinco fornecedores de segurança e mais de cinco produtos de segurança em seu ambiente. Cerca de 55% dos profissionais de segurança usam pelo menos seis fornecedores; 45% usam entre um e cinco fornecedores; e 65% usam seis ou mais produtos.
- As principais restrições para adoção de produtos e soluções de segurança avançada, de acordo com o estudo referencial, são orçamento (citada por 35% dos entrevistados), compatibilidade de produto (28%), certificação (25%) e talentos (25%).
- O Estudo referencial de recursos de segurança da Cisco de 2017 revelou que, devido a várias restrições, as empresas podem investigar apenas 56% dos alertas de segurança que recebem em um determinado dia. Metade dos alertas investigados (28%) é considerado como legítimo; menos da metade (46%) dos alertas legítimos são corrigidos. Além disso, 44% dos gerentes de operações de segurança analisam mais de 5000 alertas de segurança por dia.
- Cerca de 27% das aplicações na nuvem de terceiros conectados introduzidos por funcionários em ambientes corporativos em 2016 impõem um alto risco à segurança. As conexões de autenticação aberta (OAuth) chegam à infraestrutura corporativa e podem se comunicar livremente com as plataformas corporativas na nuvem e SaaS (software como serviço) após a concessão do acesso pelos usuários.
- Uma investigação da Cisco que incluiu 130 empresas em mercados verticais revelou que 75% delas são afetadas por infecções de adware. Os criminosos potencialmente poderiam usar essas infecções para facilitar outros ataques de malware.
- Cada vez mais, os operadores por trás de campanhas de malvertising estão usando agentes (também conhecidos como "portas"). Os agentes permitem que eles se movam com maior velocidade, mantenham seu espaço operacional e escapem da detecção. Esses links intermediários possibilitam que os criminosos alternem rapidamente de um servidor mal-intencionado para outro sem alterar o redirecionamento inicial.
- O spam representa quase dois terços (65%) do volume total de e-mail, e nossa pesquisa sugere que o volume de spam global está crescendo devido a grandes e bem-sucedidos botnets de envio de spam. De acordo com pesquisadores de ameaças da Cisco, cerca de 8% a 10% do spam global observado em 2016 podem ser classificados como mal-intencionados. Além disso, a porcentagem de spam com anexos de e-mail mal-intencionados está aumentando, e os criminosos parecem estar experimentando uma variedade de tipos de arquivo para ajudar suas campanhas a prosperar.
- De acordo com o Estudo referencial de recursos de segurança, as empresas que ainda não sofreram uma violação de segurança podem acreditar que suas redes são seguras. Essa confiança é provavelmente indevida, considerando que 49% dos profissionais de segurança entrevistados disseram que suas empresas tiveram que lidar com as críticas resultantes de uma violação de segurança.

- O Estudo referencial de recursos de segurança da Cisco de 2017 também descobriu que cerca de um quarto das empresas que sofreram um ataque perdeu oportunidades comerciais. Quatro em 10 disseram que essas perdas foram substanciais. Uma em cinco empresas perdeu clientes devido a um ataque, e quase 30% perderam receita.
- Quando violações ocorrem, operações e finanças foram as funções com maior probabilidade de serem afetadas (36% e 30%, respectivamente), seguidas por reputação da marca e retenção do cliente (as duas em 26%), de acordo com os entrevistados no estudo referencial.
- As interrupções da rede causadas por violações de segurança muitas vezes podem ter impacto duradouro. De acordo com o estudo referencial, 45% das interrupções durou entre 1 e 8 horas; 15% durou entre 9 e 16 horas, e 11% duraram entre 17 e 24 horas. Quarenta e um por cento (consulte a página 55) dessas interrupções afetaram entre 11% e 30% dos sistemas.
- As vulnerabilidades no middleware (software que serve como uma ponte ou conector entre plataformas ou aplicações) estão se tornando mais visíveis, aumentando a preocupação de que o middleware esteja se tornando um vetor de ameaças muito utilizado. Muitas empresas dependem do middleware, por isso a ameaça poderia afetar todos os setores. Durante um projeto da Cisco®, nossos pesquisadores de ameaças descobriram que a maioria das novas vulnerabilidades examinada foi atribuída ao uso de middleware.
- O ritmo das atualizações de software pode afetar o comportamento do usuário quando se trata de instalar patches e atualizações. De acordo com nossos pesquisadores, cronogramas de atualização regulares e previsíveis fazem com que os usuários atualizem o software mais rapidamente, reduzindo o tempo em que os criminosos podem se valer de vulnerabilidades.
- O estudo referencial de recursos de segurança de 2017 descobriu que a maioria das empresas recorre a fornecedores de terceiros para no mínimo 20% de sua segurança, e aquelas que recorrem com maior intensidade a esses recursos têm probabilidade maior de expandir seu uso no futuro.

Introdução

Introdução

Os criminosos têm um portfólio vasto e variado de técnicas para ganhar acesso a recursos organizacionais a fim de obter tempo irrestrito para operar. As estratégias abrangem todos os conceitos básicos e incluem:

- Tirar proveito de lapsos na correção de falhas e na atualização
- Atrair os usuários para armadilhas socialmente projetadas
- Injetar malware em conteúdo on-line supostamente legítimo, como anúncios

Eles têm muitos outros recursos também, que vão desde a exploração de vulnerabilidades de middleware ao envio de spam mal-intencionado. E quando conseguem atingir seus objetivos, podem desativar de forma rápida e silenciosa suas operações.

Os criminosos trabalham sem parar para evoluir suas ameaças, mover-se com ainda mais velocidade e encontrar formas de ampliar seu espaço operacional. O crescimento explosivo do tráfego da Internet, motivado em grande parte pela maior velocidade móvel e pela proliferação de dispositivos on-line, trabalha a favor deles ajudando-os a expandir a superfície de ataque. À medida que isso acontece, os riscos ficam maiores para as empresas. O Estudo referencial de recursos de segurança da Cisco de 2017 descobriu que mais de um terço das empresas que sofreram um ataque perderam 20% ou mais da receita. Quarenta e nove por cento dos entrevistados disseram que sua empresa já havia enfrentado o escrutínio público devido a uma violação de segurança.

Quantas empresas podem sofrer prejuízos como esses em seus resultados e permanecer saudáveis? Os defensores devem se concentrar na redução do espaço operacional dos criminosos. Assim, os invasores acharão extremamente difícil obter acesso a recursos empresariais valiosos e realizar suas atividades sem serem detectados.

A automação é essencial para atingir esse objetivo. Ela ajuda você a compreender o que é atividade normal no ambiente de rede para que você possa concentrar poucos recursos na investigação e na resolução das ameaças reais. A simplificação das operações de segurança também ajuda você a se tornar mais eficiente na eliminação do espaço operacional irrestrito dos criminosos. Entretanto, o estudo referencial mostra que a maioria das empresas está usando mais de cinco soluções de mais de cinco fornecedores diferentes (página 53).

Uma rede tão complexa de tecnologia, e o número impressionante de alertas de segurança, é uma receita para menos (e não mais) proteção. É claro que acrescentar mais talentos de segurança pode ajudar. Com mais especialistas na equipe, segundo essa lógica, melhor seria a capacidade da empresa de gerenciar a tecnologia e oferecer melhores resultados. Entretanto, a escassez de talentos de segurança e os orçamentos limitados para segurança tornam ondas de contratações algo improvável. Em vez disso, a maioria das empresas deve se contentar com os talentos de que dispõem. Elas contam com talentos terceirizados para fortalecer as equipes de segurança ao mesmo tempo que economizam no orçamento.

Para enfrentar esses desafios, a verdadeira resposta, como explicaremos mais adiante neste relatório, é a operacionalização de pessoas, processos e da tecnologia de forma integrada. Operacionalizar a segurança é compreender verdadeiramente o que a empresa precisa proteger, bem como que medidas devem ser adotadas para proteger esses ativos fundamentais.

O relatório de segurança digital anual da Cisco 2017 apresenta nossos avanços mais recentes no setor de segurança projetados para ajudar as empresas e os usuários a defenderem-se contra ataques. Também analisamos as técnicas e estratégias que os criminosos usam para violar essas defesas. O relatório também destaca as principais descobertas do Estudo comparativo de recursos de segurança da Cisco de 2017, que examina o procedimento de segurança das grandes empresas e a percepção que elas têm de suas condições técnicas para se defenderem contra ataques.

A expansão da superfície de ataque

A expansão da superfície de ataque

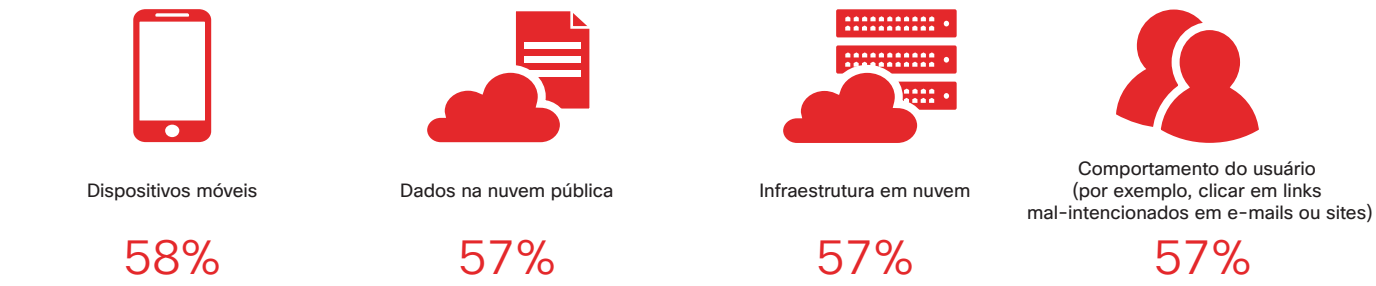
Dispositivos móveis. Nuvem pública. Infraestrutura na nuvem. Comportamento do usuário. Os profissionais de segurança que participaram do terceiro Estudo referencial de recursos de segurança anual da Cisco citaram todos esses elementos como principais razões de preocupação quando pensam no risco de a empresa se expor a um ataque cibernético (**Figura 1**). Isso é compreensível: a proliferação de dispositivos móveis gera mais endpoints para proteger. A nuvem está expandindo o perímetro da segurança. E os usuários são, e sempre serão, um elo fraco na cadeia de segurança.

À medida que as empresas adotam a digitalização, e a Internet de Todas as Coisas (IoE)[1] começa a tomar forma, os defensores terão ainda mais com o que se preocupar. A superfície de ataque só vai se expandir, oferecendo aos criminosos mais espaço para operarem.

Há mais de uma década, o Visual Networking Index (VNI) da Cisco® fornece previsões de tráfego IP global e analisa os fatores dinâmicos que facilitam o crescimento da rede. Considere estas estatísticas do relatório mais recente, *A era do zettabyte –Tendências e análises*:[2]

- O tráfego IP global anual ultrapassará o limite de 1 zettabyte (ZB) até o final de 2016 e chegará a 2,3 ZB por ano até 2020. (1 zettabyte são 1000 exabytes ou 1 bilhão de terabytes.) Isso representa a triplicação do tráfego IP global nos próximos 5 anos.
- O tráfego de dispositivos sem fio e móveis representará dois terços (66%) do tráfego IP total até 2020. Dispositivos com fio representarão apenas 34%.
- De 2015 a 2020, as velocidades médias da banda larga quase duplicarão.
- Até 2020, 82% de todo o tráfego global da Internet dos consumidores será tráfego de vídeo IP, aumentando dos 70% registrados em 2015.

Figura 1 Os maiores motivos de preocupação dos profissionais de segurança relacionados aos ataques digitais



Porcentagem de profissionais de segurança que consideram as categorias muito ou extremamente desafiadoras

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Baixe o gráfico de 2017 em: **www.cisco.com/go/acr2017graphics**

[1] "Internet of Everything FAQ", Cisco: http://ioeassessment.cisco.com/learn/ioe-faq.
[2] *The Zettabyte Era–Trends and Analysis*, Cisco VNI, 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

Além disso, o white paper Cisco *VNI™ Forecast and Methodology, 2015–2020*[3] prevê que o volume de tráfego global da Internet em 2020 será 95 vezes maior do que era em 2005.

É claro que os criminosos cibernéticos oportunistas prestam muita atenção a essas tendências também. Já estamos vendo operadores na economia paralela tomarem medidas para se tornarem mais ágeis nesse ambiente em constante mudança. Eles estão criando ataques altamente direcionados e variados destinados a prosperar na superfície de ataque em expansão. Enquanto isso, as equipes de segurança estão em um constante apagar de incêndios, sobrecarregadas por alertas. Eles estão precisando contar com uma série de produtos de segurança no ambiente de rede que apenas acrescentam mais complexidade e podem aumentar a suscetibilidade de uma empresa a ameaças.

As empresas devem:

- Integrar a tecnologia de segurança
- Simplificar as operações de segurança
- Utilizar mais a automação

Essa abordagem ajudará a reduzir despesas operacionais, aliviará a carga sobre a equipe de segurança e oferecerá melhores resultados de segurança. E de maneira mais importante, oferecerá aos defensores a capacidade de concentrar mais de seu tempo na eliminação do espaço irrestrito em que os criminosos operam no momento.

[3] *Cisco VNI Forecast and Methodology, 2015–2020*, Cisco VNI, 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

Comportamento do invasor

Comportamento do invasor

Reconhecimento | Armamento | Entrega | Instalação

Os invasores pesquisam, identificam e selecionam seu público-alvo

Métodos de ataque na Web: ameaças de "cauda curta" ajudam os criminosos a preparar o terreno para campanhas

O reconhecimento é, certamente, uma etapa básica para iniciar um ataque cibernético. Nesta fase, os criminosos buscam infraestrutura de Internet vulnerável ou pontos fracos da rede que os possibilitem obter acesso aos computadores dos usuários e, por fim, se infiltrar nas empresas.

Binários suspeitos do Windows e aplicações potencialmente indesejadas (PUAs) ficaram no topo da lista dos métodos de ataque à Web em 2016 com uma margem considerável (consulte a Figura 2). Os binários suspeitos do Windows oferecem ameaças como spyware e adware. Extensões de navegador mal-intencionadas são um exemplo de PUAs.

As tentativas de fraude no Facebook, incluindo ofertas e conteúdo de mídia falso junto com fraudes em pesquisas, ficaram em terceiro lugar em nossa lista. O destaque contínuo das tentativas de fraude no Facebook em nossas listas anual e semestral do malware mais comumente observado realça o papel fundamental da engenharia social em muitos ataques cibernéticos. O Facebook tem quase 1,8 bilhão de usuários ativos mensais no mundo todo.[4] É o território lógico dos criminosos digitais e outras pessoas que procuram enganar os usuários. Um desenvolvimento positivo é o anúncio recente da empresa de que ela está tomando medidas para eliminar as notícias falsas e os embustes. Os críticos sugerem que esse conteúdo possa ter influenciado os eleitores na eleição presidencial de 2016 dos EUA.[5]

[4] Facebook stats, setembro de 2016: http://newsroom.fb.com/company-info/.

[5] " Zuckerberg Vows to Weed Out Facebook 'Fake News'", de Jessica Guynn e Kevin McCoy, *USA Today*, 14 de novembro de 2016: http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/.

Figura 2 Malwares observados com mais frequência

Fonte: Cisco Security Research

O malware de redirecionamento de navegador completa os cinco tipos de malware mais comuns observados em 2016. Como discutido no *Relatório semestral de segurança digital da Cisco de 2016*[6], as infecções de navegador podem expor os usuários a anúncios mal-intencionados (malvertising), que os criminosos usam para preparar ransomware e outras campanhas de malware. Os pesquisadores de ameaças da Cisco alertam que adware mal-intencionado, inclusive injetores de anúncios, hijackers de configurações de navegador, utilitários e downloaders, é um problema cada vez maior. Na verdade, identificamos infecções por adware em 75% das empresas que investigamos recentemente como parte de nossa pesquisa sobre o problema. (Para obter mais informações sobre esse assunto, consulte "Investigação descobre que 75% das empresas são afetadas por infecções de adware", página 23.)

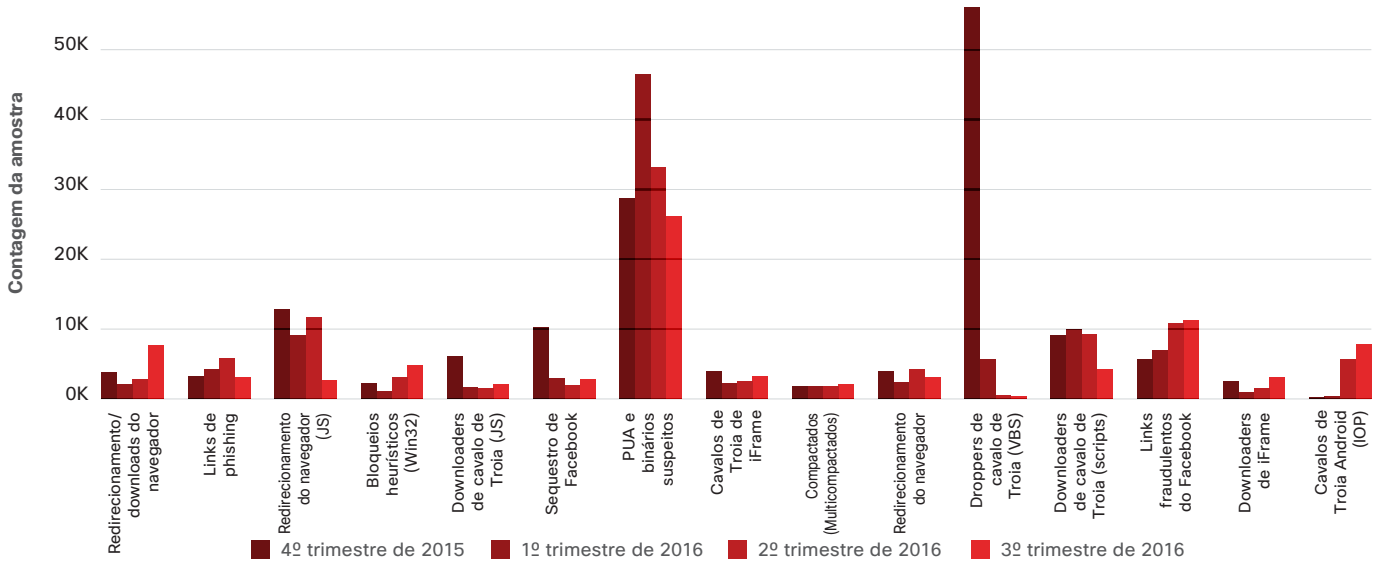
Outros tipos de malware listados na **Figura 3**, como malware que abusa de JavaScript no navegador e malware que abusa do iFrame no navegador, também são projetados para facilitar as infecções dos navegadores. Os cavalos de troia (droppers e downloaders) também aparecem entre os cinco tipos de malware observados com mais frequência, indicando que eles continuam sendo ferramentas populares para ganhar acesso inicial a computadores dos usuários e redes empresariais.

Outra tendência a ser observada: uso constantemente alto de malware que tem como público-alvo usuários da plataforma de operação Android. Os cavalos de troia do Android têm subido constantemente na lista de cauda curta ao longo dos últimos 2 anos. Eles ficaram classificados entre os 10 tipos de malware mais comuns vistos em 2016. O malware Loki, que aparece no final da cauda curta mostrada na **Figura 2** (consulte a página anterior), é particularmente problemático porque pode se replicar e infectar outros arquivos e programas.

A **Figura 3** ajuda a ilustrar as tendências de malware que os pesquisadores de ameaças da Cisco observaram desde o final de 2015. Ela mostra que os criminosos fizeram uma mudança definitiva na fase de reconhecimento dos ataques na Web. Mais ameaças agora buscam especificamente navegadores e plugins vulneráveis. Essa mudança corresponde ao uso cada vez maior do malvertising pelos criminosos, à medida que se torna mais difícil explorar um grande número de usuários através de vetores de ataque tradicionais da Web. (Consulte a próxima seção, "Vetores de ataques na Web: o Flash está em declínio, mas os usuários devem se manter vigilantes", página 15.)

A mensagem para usuários individuais, profissionais de segurança e empresas é clara: garantir que os navegadores sejam seguros, e desativar ou remover plugins de navegador desnecessários pode ser uma ótima medida para prevenir a infecção por malware. Essas infecções gerar ataques maiores, perturbadores e caros, como campanhas de ransomware. Essas etapas simples podem reduzir em grande medida sua exposição a ameaças comuns na Web e impedir que os criminosos encontrem o espaço operacional para realizar a próxima fase da cadeia do ataque: o armamento.

Figura 3 Malware observado com mais frequência, quarto trimestre de 2015 a terceiro trimestre de 2016



Fonte: Cisco Security Research

[6] *Relatório semestral de segurança digital da Cisco 2016*: http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Reconhecimento | **Armamento** | Entrega | Instalação

Os invasores aliam malware de acesso remoto com explorações em payloads de resultado.

Vetores de ataques na Web: o Flash está em declínio, mas os usuários devem se manter vigilantes

O Adobe Flash há muito tempo é um atraente vetor de ataques na Web para criminosos que desejam explorar e comprometer sistemas. Entretanto, como a quantidade de conteúdo do Adobe Flash na Web continua diminuindo, e a conscientização sobre as vulnerabilidades do Flash aumenta, está cada vez mais difícil os criminosos digitais explorarem usuários com a mesma frequência de antigamente.

A própria Adobe está abandonando o desenvolvimento completo e o suporte da plataforma de software e encorajou os desenvolvedores a adotarem novos padrões, como o HTML5.[7] Os fornecedores de navegadores da Web utilizados com frequência também estão adotando uma posição firme quanto ao Flash. Por exemplo, o Google anunciou que, em 2016, descontinuará o suporte completo do Adobe Flash em seu navegador Chrome.[8] O Firefox continuará a oferecer suporte para conteúdo em Flash herdado, mas está bloqueando "certo conteúdo em Flash que não é essencial para a experiência do usuário".[9]

O Flash pode estar em declínio, mas os desenvolvedores de kits de exploração estão o ajudando a resistir como vetor de ataques. Entretanto, há sinais de que isso pode estar mudando. Após três importantes kits de exploração, Angler, Nuclear e Neutrino, desaparecerem abruptamente do cenário de ameaças em 2016, nossos pesquisadores de ameaças observaram um declínio considerável no tráfego da Internet relacionado ao Flash. (Consulte "O desaparecimento dos principais kits de exploração apresenta oportunidades para concorrentes menores e novos participantes", página 20.) Os atores por trás do kit de exploração Angler visaram com intensidade às vulnerabilidades Flash para comprometer os usuários. O kit de exploração Nuclear tinha um foco similar no Flash. E o Neutrino dependia de arquivos flash para oferecer exploits.

Os usuários devem permanecer cautelosos e desinstalar o Flash a menos que precisem dele por motivos comerciais. Se precisam usá-lo, eles devem permanecer atualizados. Usar navegadores da Web com o recurso de correção de falhas automáticas pode ajudar. Conforme observado em "Métodos de ataque na Web: ameaças de 'cauda curta' ajudam os criminosos a preparar o terreno para campanhas" na página 13, o uso de navegadores seguros – e a desativação ou remoção de plugins de navegador desnecessários – reduzirá muito sua exposição a ameaças na Web.

Java, PDF e Silverlight

Tanto o tráfego da Internet de Java quanto o de PDF apresentaram grandes declínios em 2016. O tráfego do Silverlight já atingiu um nível que não vale mais a pena ser acompanhado regularmente pelos pesquisadores de ameaças.

Java, antes o principal vetor de ataques na Web, observou uma grande melhora de postura de segurança nos últimos anos. No início de 2016, a decisão da Oracle de eliminar o plugin de navegador do Java ajudou a torná-lo um vetor de ataques na Web menos atraente. Os ataques por PDF também são cada vez mais raros. Por isso, eles podem ser mais fáceis de detectar, motivo pelo qual muitos criminosos agora não usam essa estratégia com muita frequência.

Entretanto, como ocorre com o Flash, os criminosos digitais ainda usam Java, PDF e Silverlight para explorar usuários. Os usuários individuais, as empresas e os profissionais de segurança devem conhecer esses possíveis caminhos para comprometer sistemas. Para reduzir o risco de exposição a ameaças, eles devem:

- Baixar patches
- Usar tecnologia da Web atualizada
- Evitar conteúdo da Web que possa apresentar risco

[7] " Flash, HTML5 and Open Web Standards", Adobe News, novembro de 2015: https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html.
[8] " Flash and Chrome", de Anthony LaForge, The Keyword blog, Google, 9 de agosto de 2016: https://blog.google/products/chrome/flash-and-chrome/.
[9] " Reducing Adobe Flash Usage in Firefox", de Benjamin Smedberg, Future Release blog, Mozilla, 20 de julho de 2016: https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/.

Segurança de aplicações: gerenciamento do risco da conexão OAuth em meio a uma explosão de aplicações

Quando as empresas migram para a nuvem, o perímetro de segurança se estende para o território virtual. Entretanto, o perímetro de segurança dissipa-se rapidamente com cada aplicação em nuvem de terceiros que os funcionários introduzem no ambiente.

Os funcionários querem aumentar a produtividade e permanecer conectados enquanto estiverem no trabalho. Mas essas aplicações da TI paralela criam um risco para as empresas. Eles têm contato com a infraestrutura corporativa e podem se comunicar livremente com as plataformas corporativas em nuvem e SaaS (software como serviço) após a concessão do acesso pelos usuários por meio da autenticação aberta (OAuth). Essas aplicações podem ter escopos de acesso amplos (e, às vezes, excessivos). Elas devem ser cuidadosamente gerenciadas porque podem exibir, excluir, exteriorizar e armazenar dados corporativos, e até mesmo agir em nome dos usuários.

O provedor de segurança na nuvem CloudLock, agora parte da Cisco, tem acompanhado o crescimento de aplicações na nuvem de terceiros conectadas por um grupo de 900 empresas que representam uma série de setores. Como mostra a Figura 4, havia cerca de 129.000 aplicações exclusivas disponíveis no começo de 2016. No final de outubro, esse número cresceu para 222.000.

O número de aplicações aumentou aproximadamente 11 vezes desde 2014. (Veja a Figura 5.)

Classificação das aplicações mais arriscadas

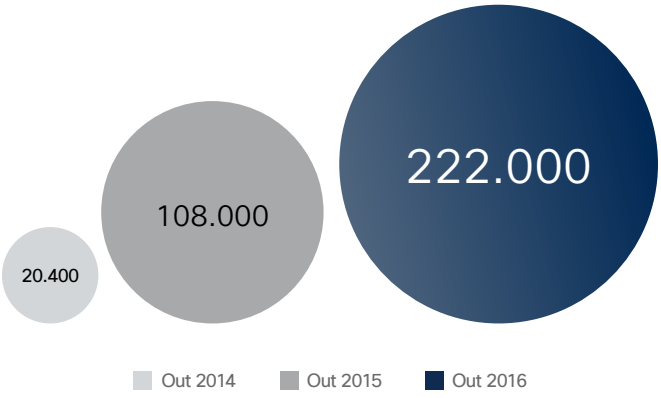
Para ajudar as equipes de segurança a compreender quais aplicações na nuvem de terceiros conectadas em seu ambiente apresentam o maior risco à segurança da rede, a CloudLock desenvolveu o Índice de risco de aplicações na nuvem (CARI). O processo envolve diversas avaliações:

- **Requisitos de acesso a dados:** as empresas respondem às seguintes perguntas, entre outras: quais permissões são necessárias para autorizar a aplicação? A concessão do acesso a dados significa que a aplicação tem acesso programático (de APIs) para plataformas corporativas de SaaS através de conexões OAuth? A aplicação pode (e por extensão, o fornecedor) agir em nome dos usuários e executar ações com os dados corporativos, como visualizar e excluir?
- **Classificação de confiança da comunidade:** avaliações obtidas por crowdsourcing e realizadas por empresas do mesmo setor são usadas para essa análise.
- **Inteligência de ameaças de aplicações:** essa comprovação de antecedentes abrangente, realizada por especialistas em segurança digital, tem como base vários atributos de segurança de uma aplicação, como certificações de segurança, histórico de violações e revisões de analistas.

Figura 4 Crescimento vertiginoso de aplicações na nuvem de terceiros conectadas, 2016

Fonte: Cisco CloudLock

Figura 5 Crescimento das aplicações na nuvem de terceiros, comparação ano a ano



Fonte: Cisco CloudLock

Baixe o gráfico de 2017 em: **www.cisco.com/go/acr2017graphics**

Pontuações de risco e exemplos

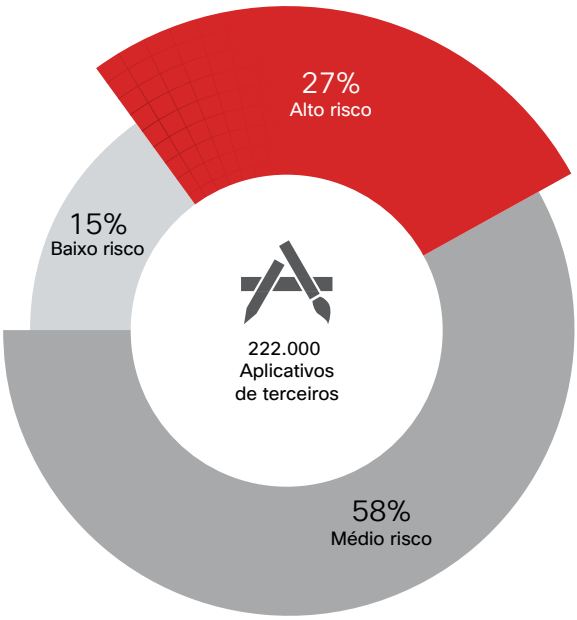
Após a classificação das aplicações na nuvem de terceiros usando o CARI, o CloudLock atribui uma pontuação de risco para cada aplicação numa escala de 1 (menor risco) a 5 (maior risco).

Uma aplicação com pontuação 1 na escala poderia ter, por exemplo, escopos de acesso mínimo (ela pode apenas ver e-mail), uma classificação de confiança 100% da comunidade e nenhum histórico de violações.

Uma aplicação com pontuação 5 na escala poderia ser uma com acesso de conta total (é possível ver todos os e-mails, documentos, histórico de navegação, calendário e outros), uma classificação de confiança de 8% (o que significa que apenas 8% dos administradores confiam nela) e nenhuma certificação de segurança.

A CloudLock usou o CARI para classificar as 222.000 aplicações que identificou nas mais de 900 empresas em sua amostra. Desse total de aplicações, 27% foram consideradas de alto risco, enquanto a maioria se encaixou na categoria de médio risco. (Consulte a **Figura 6**.) Metade dessas empresas tinha as conexões OAuth relacionadas a uma aplicação popular de jogo que foi lançada no verão de 2016.

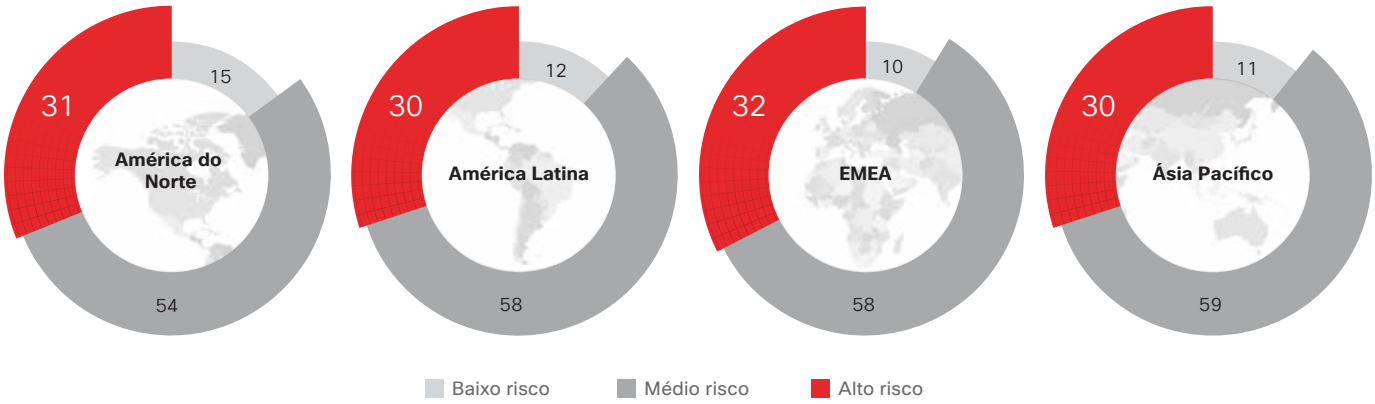
Figura 6 Aplicações de terceiros classificadas como de alto risco



Fonte: Cisco CloudLock

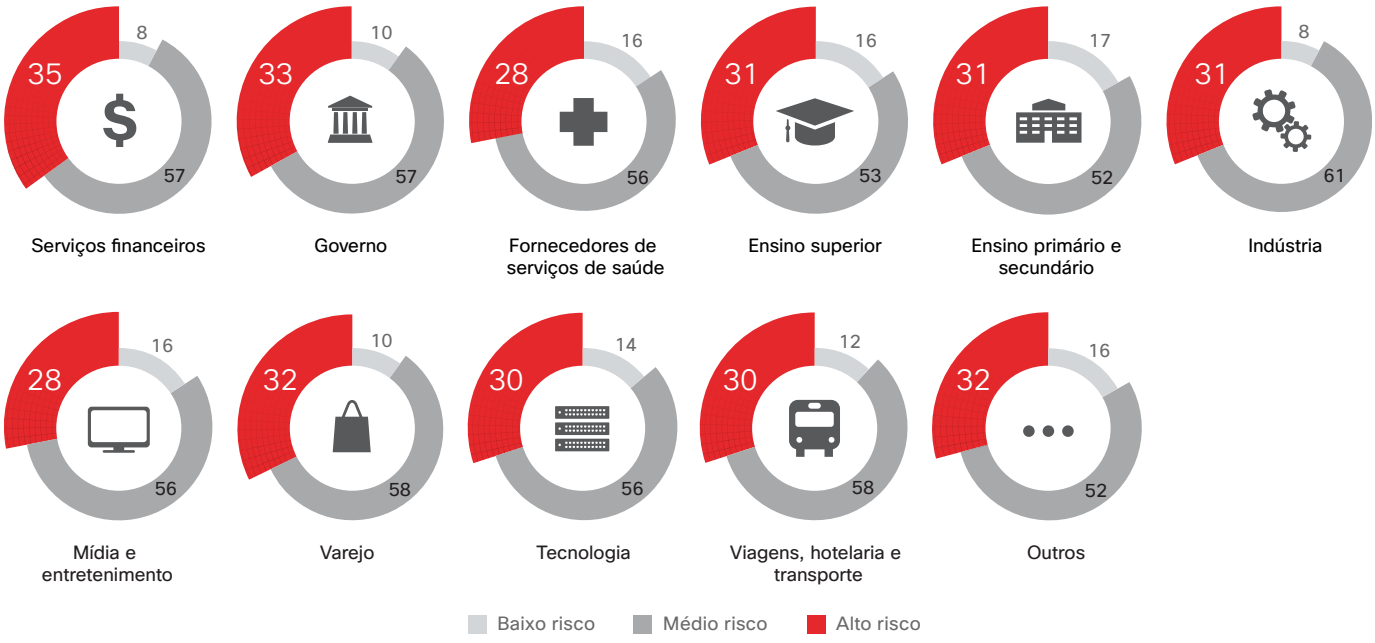
Com nossa análise, descobrimos que todas as empresas, seja qual for o tamanho, o setor ou a região, têm uma distribuição relativamente uniforme de aplicações de risco baixo, médio e alto (Figuras 7 e 8).

Figura 7 Distribuição de aplicações de baixo, médio e alto risco, por região



Fonte: Cisco CloudLock

Figura 8 Distribuição de aplicações de baixo, médio e alto risco, por setor



Fonte: Cisco CloudLock

Baixe o gráfico de 2017 em: **www.cisco.com/go/acr2017graphics**

Identificação do que é relevante

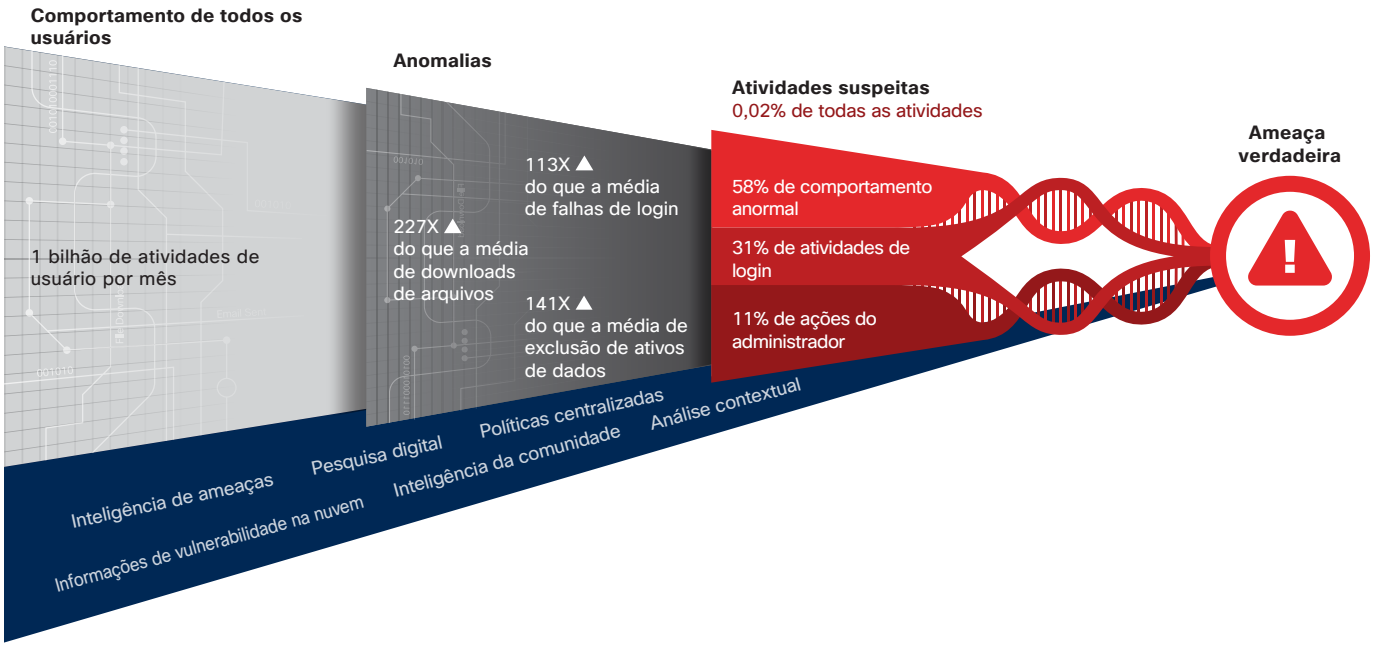
Para identificar o comportamento suspeito do usuário e da entidade em plataformas corporativas de SaaS (Software como serviço), inclusive aplicações na nuvem de terceiros, as equipes de segurança devem examinar meticulosamente os bilhões de atividades do usuário para definir padrões normais de comportamento do usuário no ambiente da empresa. Eles devem procurar anomalias que estejam fora desses padrões esperados. Depois, eles precisam correlacionar atividades suspeitas para determinar o que poderia ser uma ameaça real que exige investigação.

Um exemplo de atividade suspeita é um excesso de atividade de login de vários países em um período curto. Digamos que o comportamento normal do usuário em uma determinada empresa seja fazer login em uma aplicação específica de não mais que um ou dois países por semana. Se um usuário começar a fazer login nessa aplicação de 68 países no decorrer de uma semana, uma equipe de segurança investigará essa atividade para confirmar que é legítima.

De acordo com nossa análise, apenas 1 em 5000 atividades do usuário – 0,02% – que estão associadas à aplicações na nuvem de terceiros conectada é suspeita. O desafio das equipes de segurança, obviamente, é identificar essa única instância.

Apenas com automação as equipes de segurança podem eliminar o "ruído" dos alertas de segurança e concentrar seus recursos na investigação de ameaças reais. O processo em vários estágios de identificar atividades normais e possivelmente suspeitas do usuário que é descrito acima (e ilustrado na Figura 9) depende do uso da automação com algoritmos aplicados em cada estágio.

Figura 9 Identificação de padrões de comportamento de usuário com automação (processo)



Fonte: Cisco CloudLock

Reconhecimento | Armamento | **Entrega** | Instalação

Através do uso de e-mail mal-intencionado, anexos de e-mail, sites e outras ferramentas, os invasores transmitem suas armas digitais para o público-alvo.

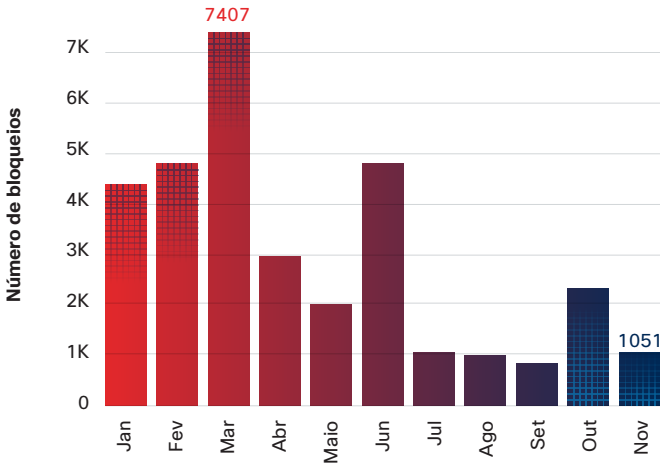
O desaparecimento dos principais kits de exploração apresenta oportunidades para concorrentes menores e novos participantes

Em 2016, aconteceram mudanças drásticas no ambiente dos kits de exploração. No início do ano, Angler, Nuclear, Neutrino e RIG eram líderes indiscutíveis entre os kits de exploração. Até novembro, RIK era o único nesse grupo que ainda estava ativo. Como mostra a **Figura 10**, a atividade de kits de exploração caiu bastante por volta de junho.

Nuclear foi o primeiro a desaparecer, encerrando subitamente a operação em maio. Por que os autores o abandonaram é um mistério. O kit de exploração Neutrino, que também saiu de cena em 2016, utilizava arquivos Flash para fornecer vulnerabilidades. (Consulte a **Figura 11** na próxima página para obter uma lista das principais vulnerabilidades nos kits de exploração conhecidos em 2016.)

O Flash continua sendo um atraente vetor de ataque na Web para os criminosos, mas provavelmente se tornará menos atraente ao longo do tempo. Menos sites e navegadores oferecem algum suporte ou suporte total ao Flash, e há no geral maior conscientização sobre as vulnerabilidades do Flash. (Para obter mais informações sobre esse assunto, consulte "Vetores de ataques na Web: o Flash está em declínio, mas os usuários devem se manter vigilantes", na página 15.)

Figura 10 Bloqueios de página inicial de kit de exploração, Janeiro–novembro de 2016



Fonte: Cisco Security Research

Baixe o gráfico de 2017 em: **www.cisco.com/go/acr2017graphics**

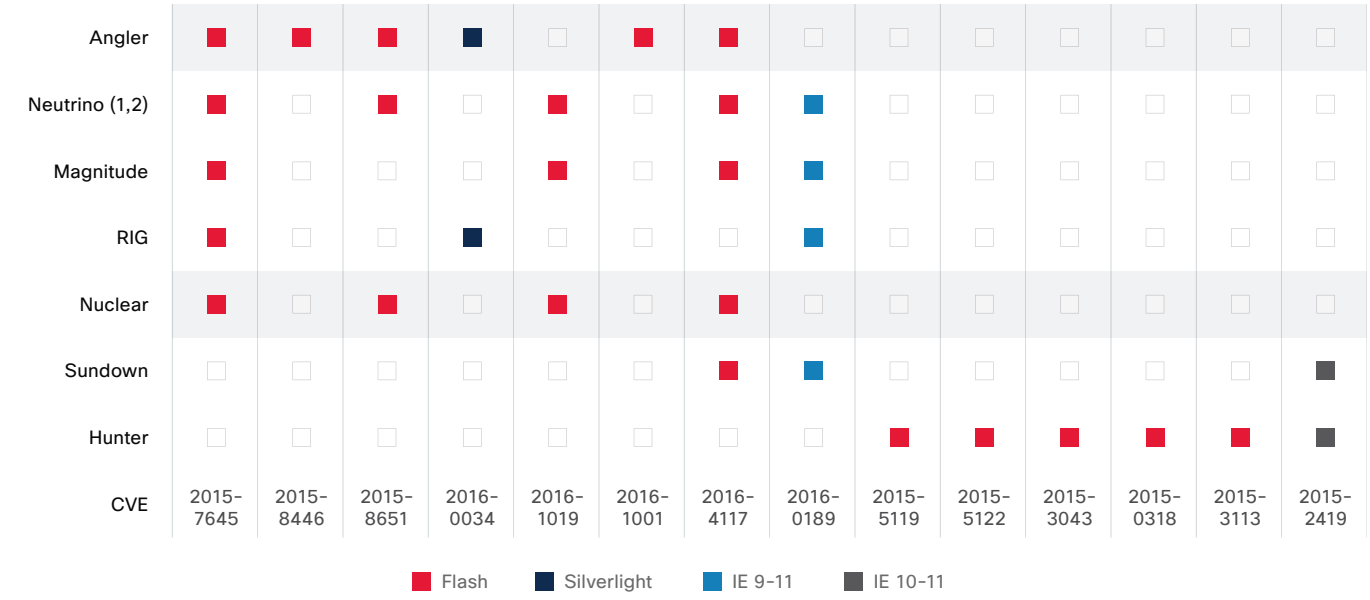
Um gigante se cala

O Angler (o mais avançado e maior entre os kits de exploração conhecidos) também visou a vulnerabilidades do Flash e foi vinculado a várias campanhas de malvertising e ransomware de destaque. Entretanto, ao contrário do desaparecimento do Nuclear e do Neutrino, a saída do Angler em 2016 não é um mistério.

Na primavera passada, cerca de 50 hackers, foram presos na Rússia, o grupo estava vinculado ao malware Lurk, um cavalo de troia bancário que visa especificamente a bancos russos.[10] Os pesquisadores de ameaças da Cisco identificaram conexões claras entre o Lurk e o Angler, incluindo o fato de que o Lurk estava sendo oferecido em grande parte por meio do Angler para as vítimas na Rússia. Em seguida às prisões, o Angler desapareceu do mercado de kits de exploração.[11]

Agora que três dos líderes entre os kits de exploração saíram de cena, competidores menores e novos participantes podem expandir sua participação de mercado. E estão se tornando mais sofisticados e ágeis. Os kits de exploração que apareciam posicionados para crescer no final de 2016 eram o Sundown, o Sweet Orange e o Magnitude. Esses kits, bem como o RIG, são conhecidos por visarem vulnerabilidades do Flash, Silverlight e Microsoft Internet Explorer. (Consulte a **Figura 11**.) Desinstalar o Flash e desativar ou remover plugins de navegador ajudará os usuários a reduzir o risco de que eles sejam comprometidos por essas ameaças.

Figura 11 Principais vulnerabilidades em kits de exploração



Fonte: Cisco Security Research

[10] " Russian Hacker Gang Arrested Over $25M Theft", BBC News, 2 de junho de 2016: http://www.bbc.com/news/technology-36434104.
[11] Para obter mais informações sobre esse assunto, consulte o post do blog Cisco Talos de julho de 2016, Connecting the Dots Reveals Crimeware Shake-Up.

Malvertising: criminosos usam agentes para aumentar a velocidade e a agilidade

Os usuários são direcionados para os kits de exploração de duas formas principais: sites comprometidos e malvertising. Os criminosos colocam um link para uma página inicial de kit de exploração em um anúncio mal-intencionado ou site comprometido, ou usam um link intermediário, conhecido como agente. (Esses links, posicionados entre os sites comprometidos e os servidores de kit de exploração, são também conhecidos como "portas".) O agente serve como um intermediário entre o redirecionamento inicial e o kit de exploração real que fornece o payload do malware aos usuários.

A última tática está se tornando mais popular à medida que os invasores descobrem que devem se mover mais rápido para manter seu espaço operacional e escapar da detecção. Os agentes possibilitam que os criminosos alternem rapidamente de um servidor mal-intencionado para outro sem alterar o redirecionamento inicial. Como eles não precisam modificar constantemente sites ou anúncios mal-intencionados para começar a cadeia de infecção, os operadores do kit de exploração podem realizar campanhas mais longas

ShadowGate: uma campanha econômica

À medida que fica mais difícil comprometer um grande número de usuários apenas através dos tradicionais vetores de ataque da Web (consulte a página 15), os criminosos contam cada vez mais com malvertising para expor os usuários a kits de exploração. Nossos pesquisadores de ameaças apelidaram de "ShadowGate" uma recente campanha global de malvertising. Essa campanha ilustra como anúncios mal-intencionados estão oferecendo aos criminosos mais flexibilidade e oportunidade de atingir usuários de todas as regiões em escala.

A ShadowGate envolvia sites que variavam desde cultura popular e varejo até pornografia e notícias. Ela pode ter afetado milhões de usuários nestas regiões: América do Norte, Europa, Ásia-Pacífico e Oriente Médio. O uso de muitos idiomas e o alcance global da campanha são impressionantes.

A ShadowGate, que usava sombreamento de domínio, foi detectada pela primeira vez no início de 2015. Ela permanecia inoperante e, de uma hora para outra, recomeçava aleatoriamente a funcionar, direcionando o tráfego para páginas iniciais de kits de exploração. A princípio, a ShadowGate era usada para direcionar usuários apenas para o kit de exploração Angler. Mas depois que o Angler desapareceu em meados de 2016, os usuários passaram a ser direcionados para o kit de exploração Neutrino, até ele também sumir alguns meses depois. (Para conhecer mais essa história, consulte "O desaparecimento dos principais kits de exploração representa uma oportunidade para estreantes e participantes de menor porte", na página 20.)

Mesmo que a ShadowGate detectasse um alto volume de tráfego da Web, apenas uma pequena fração das interações fazia com que um usuário fosse direcionado para um kit de exploração. Os anúncios mal-intencionados eram quase sempre impressões, ou seja, anúncios que renderizam na página e não requerem interação do usuário. Esse modelo de publicidade on-line permitiu que os agentes responsáveis pela ShadowGate tornassem a campanha mais econômica.

Nossa pesquisa sobre a ShadowGate gerou um esforço conjunto com uma empresa líder em hospedagem na Web. Trabalhamos juntos para reduzir a ameaça recuperando as contas de pessoas registradas que os criminosos usavam para hospedar a atividade. Em seguida, tornamos inativos todos os subdomínios aplicáveis.

Para obter mais detalhes sobre a campanha ShadowGate, consulte a publicação no blog do Talos Cisco de setembro de 2016, Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted.

Investigação descobre que 75% das empresas são afetadas por infecções de adware

O adware, quando usado para fins legítimos, é software que faz download ou exibe anúncios através de redirecionamentos, de pop-ups e injeções de anúncios e gera receita para seus criadores. Entretanto, os criminosos digitais também estão usando o adware como uma ferramenta para ajudar a aumentar o fluxo de receita. Eles usam o adware mal-intencionado não só para lucrar com a injeção de anúncios, mas também como primeira etapa para facilitar outras campanhas de malware, como o malware DNSChanger. O adware mal-intencionado é oferecido através de pacotes de software; os editores criam um instalador com uma aplicação legítima junto com dezenas de aplicações de adware mal-intencionadas.

Os agentes mal-intencionados usam adware para:

- Injetar anúncios, que podem resultar em mais infecções ou exposição a kits de exploração
- Alterar as configurações de navegador e o sistema operacional para enfraquecer a segurança
- Causar falha no antivírus ou em outros produtos de segurança
- Obter o controle total do host, de forma que possam instalar outros softwares mal-intencionados
- Rastrear os usuários por local, identidade, serviços usados e sites acessados com frequência
- Roubar informações como dados pessoais, credenciais e informações de infraestrutura (por exemplo, as páginas de vendas internas de uma empresa)

Para avaliar o escopo do problema do adware para as empresas, os pesquisadores de ameaças da Cisco examinaram 80 variedades diferentes de adware. Cerca de 130 empresas em mercados verticais foram incluídas em nossa investigação, que ocorreu de novembro de 2015 a novembro de 2016.

Classificamos o adware em quatro grupos, com base no comportamento principal de cada componente:

- **Injetores de anúncio:** esse adware geralmente reside no navegador e pode afetar todos os sistemas operacionais.
- **Hijackers de configurações do navegador:** esse componente de adware pode alterar as configurações do computador para tornar o navegador menos seguro.
- **Utilitários:** essa é uma categoria grande e cada vez maior de adware. Os utilitários são aplicativos da Web que oferecem um serviço útil para os usuários, como otimização do PC. Esses aplicativos podem injetar anúncios, mas seu objetivo principal é convencer os usuários a pagar pelo serviço. Entretanto, em muitos casos, os utilitários não passam de fraudes e não proporcionam nenhum benefício aos usuários.
- **Downloaders:** esse adware pode fornecer outro software, como uma barra de ferramentas.

Detectamos que 75% das empresas em nosso estudo foram afetadas por infecções de adware.

Figura 12 Porcentagem de empresas com infecções por adware

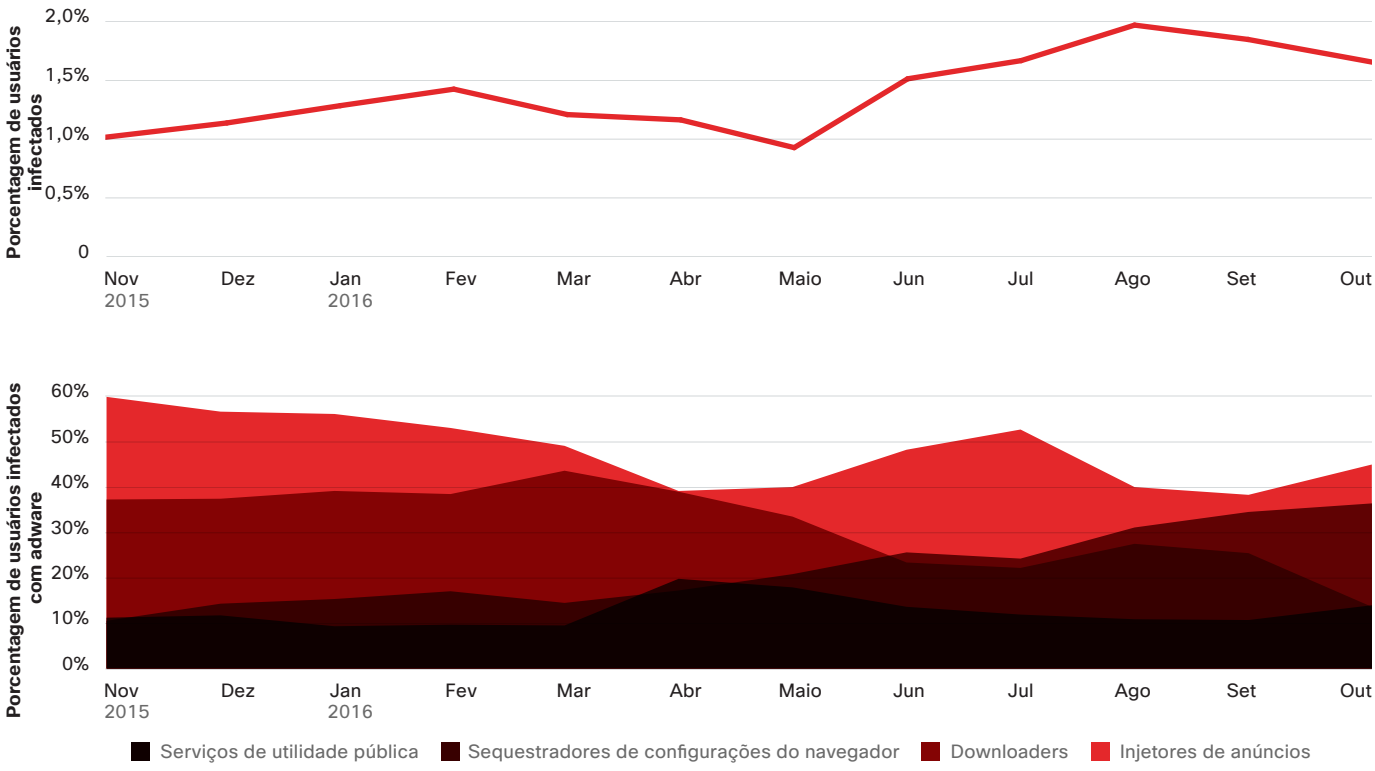
Fonte: Cisco Security Research

A Figura 13 mostra os tipos de incidentes que observamos nas empresas que participaram de nossa investigação. Os injetores de anúncio foram a principal fonte de infecções. Essa descoberta indica que a maioria dessas aplicações indesejadas é direcionada a navegadores da Web. Também percebemos um aumento de infecções no navegador durante os últimos anos, o que sugere que os criminosos estão sendo bem-sucedidos com essa estratégia de comprometer os usuários.

Todos os componentes do adware que identificamos durante nossa investigação podem por usuários e empresas em risco de serem vítimas de atividade mal-intencionada. As equipes de segurança devem reconhecer a ameaça que as infecções de adware representam e se certificar de que os usuários da empresa estejam totalmente conscientes dos riscos.

Para obter informações adicionais sobre este tópico, consulte o post do blog Cisco Security de fevereiro de 2016, DNSChanger Outbreak Linked to Adware Install Base.

Figura 13 Análise do total de incidentes por componente de adware



Fonte: Cisco Security Research

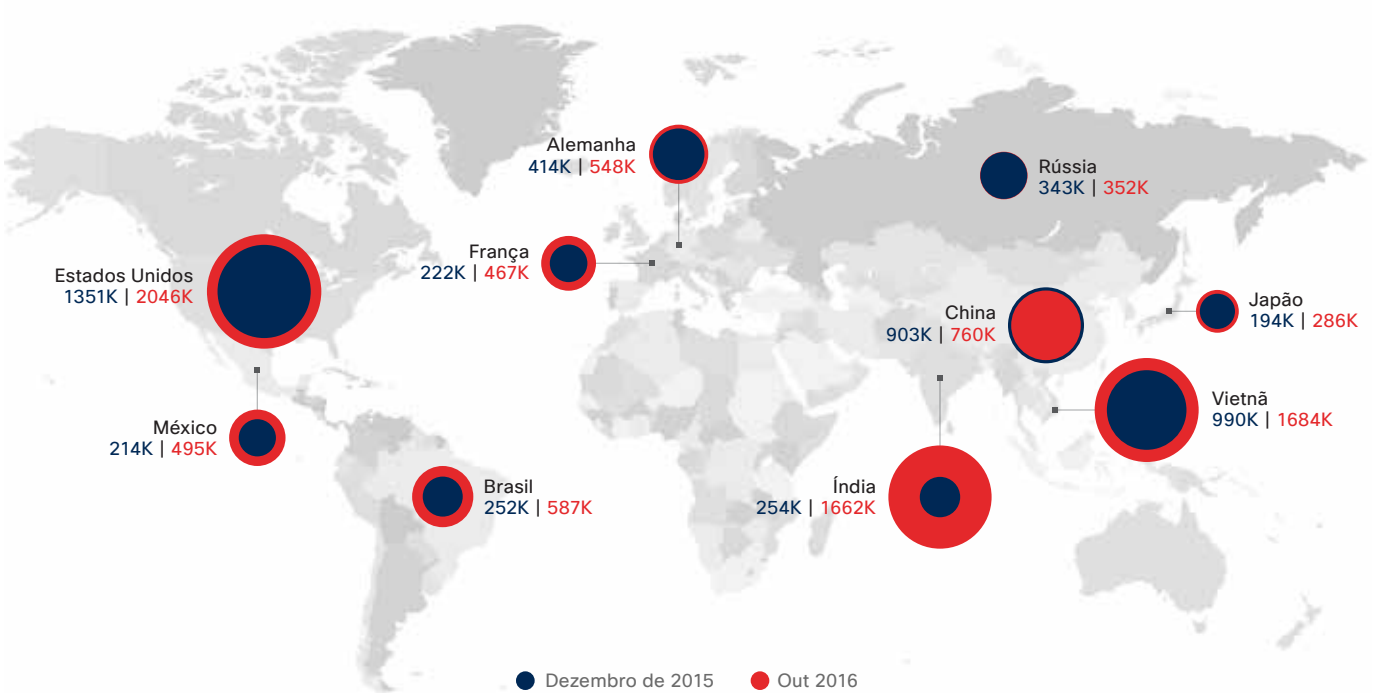
Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

O spam global está aumentando, assim como a porcentagem de anexos mal-intencionados

Os pesquisadores de ameaças da Cisco fizeram dois estudos em 2016 usando telemetria dos usuários para estimar qual porcentagem do volume total de e-mail é spam. Descobrimos que o spam representa quase dois terços (65%) do volume total de e-mail. Nossa pesquisa também sugere que o volume de spam global está aumentando, principalmente devido a grandes e bem-sucedidos botnets que enviam spam, como o Necurs. Além disso, descobrimos com nossa análise que cerca de 8% a 10% do spam global observado em 2016 poderia ser classificado como mal-intencionado.

De agosto a outubro de 2016, houve um aumento considerável no número de bloqueios de conexão IP (**Figura 14**).[12] Essa tendência pode ser atribuída a um aumento geral no volume de spam, bem como à adaptação pelos sistemas de reputação a informações sobre remetentes de spam.

Figura 14 Bloqueios de IP por país (dezembro de 2015 a novembro de 2016)



Fonte: Cisco Security Research

COMPARTILHAR

[12] Bloqueios de conexão IP são mensagens de spam bloqueadas imediatamente pela tecnologia de detecção de spam porque o remetente do spam tem uma baixa pontuação de reputação. Os exemplos incluem mensagens originadas de conhecidos botnets para envio de spam ou de redes comprometidas que são conhecidas por participar de ataques de spam.

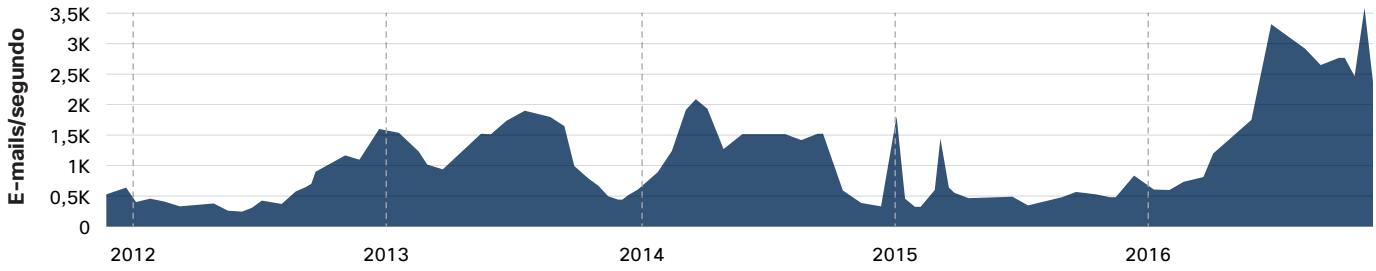
O gráfico de cinco anos da Composite Blocking List (CBL), a "lista de blackholes" em DNS de infecções de computador que enviam spam,[13] também mostra um aumento no volume total de spam durante 2016 (**Figura 15**).

Uma análise de 10 anos de dados da CBL (não mostrada) sugere que o volume de spam de 2016 está próximo aos níveis recordes vistos em 2010. Novas tecnologias anti-spam e o importante colapso dos botnets relacionados a spam ajudaram a manter os níveis de spam baixos nos últimos anos. Nossos pesquisadores de ameaças atribuem o aumento recente no volume de spam global ao botnet Necurs. O Necurs é um vetor importante para o ransomware Locky. Ele também distribui ameaças como o cavalo de troia bancário Dridex.

A **Figura 16** é um gráfico interno gerado pelo serviço SpamCop da Cisco que ilustra a mudança no volume de spam observada em 2016. Este gráfico mostra o tamanho geral da SpamCop Block List (SCBL) de novembro de 2015 a novembro de 2016. Cada linha da SCBL representa um endereço IP distinto.

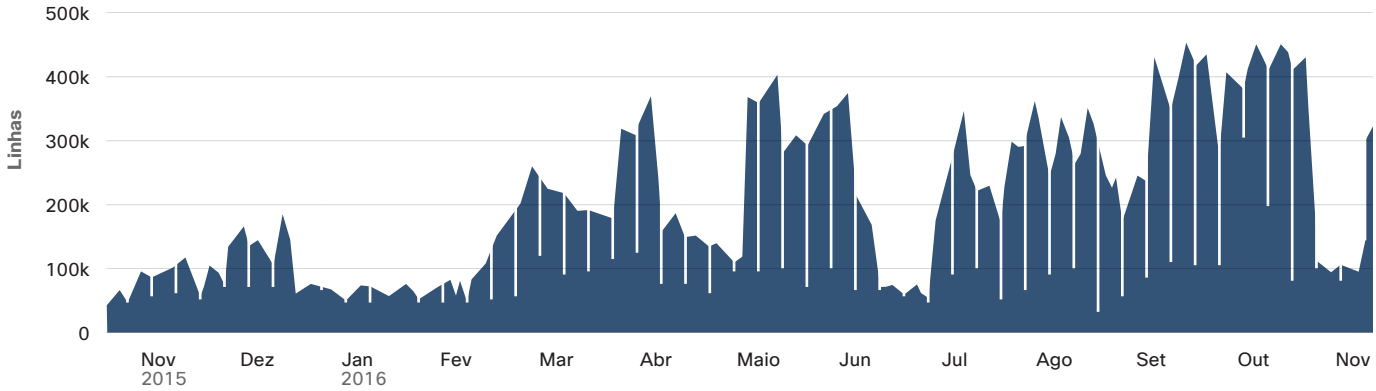
Entre novembro de 2015 e fevereiro de 2016, o tamanho da SCBL oscilou abaixo de 200.000 endereços IP. Em setembro e outubro, o tamanho de SCBL excedeu 400.000 endereços IP antes de reduzir em outubro, o que nossos pesquisadores de ameaças atribuem simplesmente a uma folga dos operadores do Necurs. Observe também o grande declínio em junho. No final de maio, houve prisões na Rússia relacionadas ao cavalo de troia bancário Lurk (**consulte a página 21**). Posteriormente, várias ameaças de destaque, incluindo o Necurs, ficaram inativas. Entretanto, 3 semanas depois, o Necurs estava de volta à ação, acrescentando 200.000 endereços IP à SCBL em menos de 2 horas.

Figura 15 Volume total de spam



Fonte: CBL

Figura 16 Tamanho total de SCBL



Fonte: SpamCop

[13] Para obter mais informações sobre CBL, acesse: http://www.abuseat.org/.

Muitos dos IPs host que enviam o spam do Necurs estão infectados há mais de 2 anos. Para ajudar a manter oculto o escopo completo do botnet, o Necurs envia spam somente de um subconjunto de hosts infectados. Um host infectado pode ser usado por 2 a 3 dias, e então não ser mais utilizado por 2 a 3 semanas. Esse comportamento complica o trabalho da equipe de segurança que responde aos ataques de spam. Ela pode acreditar que descobriu e limpou com êxito um host infectado, mas os agentes estão apenas esperando uma boa oportunidade para iniciar outro ataque.

Setenta e cinco por cento do spam total observado em outubro de 2016 continha anexos mal-intencionados. A maior parte do spam foi enviado pelo botnet Necurs (consulte a Figura 17). O Necurs envia os anexos .zip mal-intencionados que incluem arquivos executáveis integrados, como downloaders VBScript, JavaScript, .hta e .wsf. Ao calcular a porcentagem de spam total que contém anexos mal-intencionados, contamos tanto o arquivo "contêiner" (.zip) quanto os arquivos "filhos" dentro dele (como um arquivo JavaScript) como anexos individuais mal-intencionados.

Os invasores testam tipos de anexos para renovar as campanhas de spam mal-intencionadas

Nossos pesquisadores de ameaças examinaram como os criminosos usam tipos diferentes de anexos de arquivo para impedir que spam mal-intencionado seja detectado O que descobrimos foi que eles estão evoluindo continuamente com suas estratégias, testando uma ampla variedade de tipos de arquivos e mudando de tática rapidamente quando não obtêm êxito.

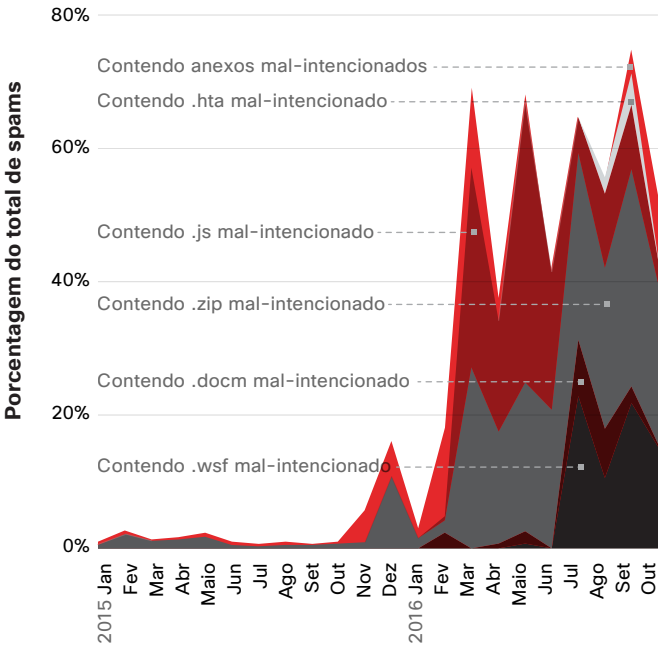
A Figura 17 mostra como os operadores de spam mal-intencionados usaram arquivos .docm, JavaScript, .wsf e .hta durante o período observado. Conforme observado anteriormente, muitos desses tipos de arquivos são associados ao spam enviado pelo botnet Necurs. (Para a pesquisa relacionada a outros tipos de arquivos examinados, consulte o Apêndice na página 78.)

As porcentagens específicas dos diferentes tipos de arquivos em um determinado mês são derivadas usando a porcentagem do spam total que continham anexos mal-intencionados observada naquele mês. Assim, por exemplo, em julho de 2016, os arquivos .docm representaram 8% da porcentagem total de anexos mal-intencionados observados.

Os padrões com os arquivos .wsf durante 2016 (consulte a Figura 17) oferecem um exemplo de como os criminosos evoluem as táticas mal-intencionadas de spam ao longo do tempo. Esse tipo de arquivo foi raramente usado como anexo mal-intencionado antes de fevereiro de 2016. Em seguida, o uso desse tipo de arquivo começa a crescer conforme o botnet Necurs se torna mais ativo. Até julho, os arquivos .wsf representavam 22% de todos os anexos de spam mal-intencionados. Isso ocorreu por volta do momento em que a atividade de spam global aumentou drasticamente (veja a seção anterior), um acréscimo que, em grande parte, foi gerado pelo botnet Necurs.

Durante agosto, setembro e outubro, percebemos flutuações nas porcentagens de arquivos .wsf. Isso indica que os criminosos interrompiam suas ações nos momentos em que o tipo de arquivo estava sendo detectado com mais frequência.

Figura 17 Porcentagem do total de spams contendo anexos mal-intencionados



Fonte: Cisco Security Research

Hailstorms e snowshoes

Dois tipos de ataques de spam mal-intencionados são especialmente problemáticos para os defensores: os ataques de hailstorm e os ataques de snowshoe. Ambos empregam os elementos de velocidade e de direcionamento, e ambos são altamente eficazes.

Os ataques de hailstorm visam a sistemas anti-spam. Os operadores por trás desses ataques lançam mão da janela de tempo muito pequena entre o momento em que iniciam sua campanha de spam e o momento em que os sistemas anti-spam a percebem e expulsam a cobertura dos scanners anti-spam. Normalmente, os criminosos têm somente segundos ou minutos para operar antes que suas campanhas sejam detectadas e bloqueadas.

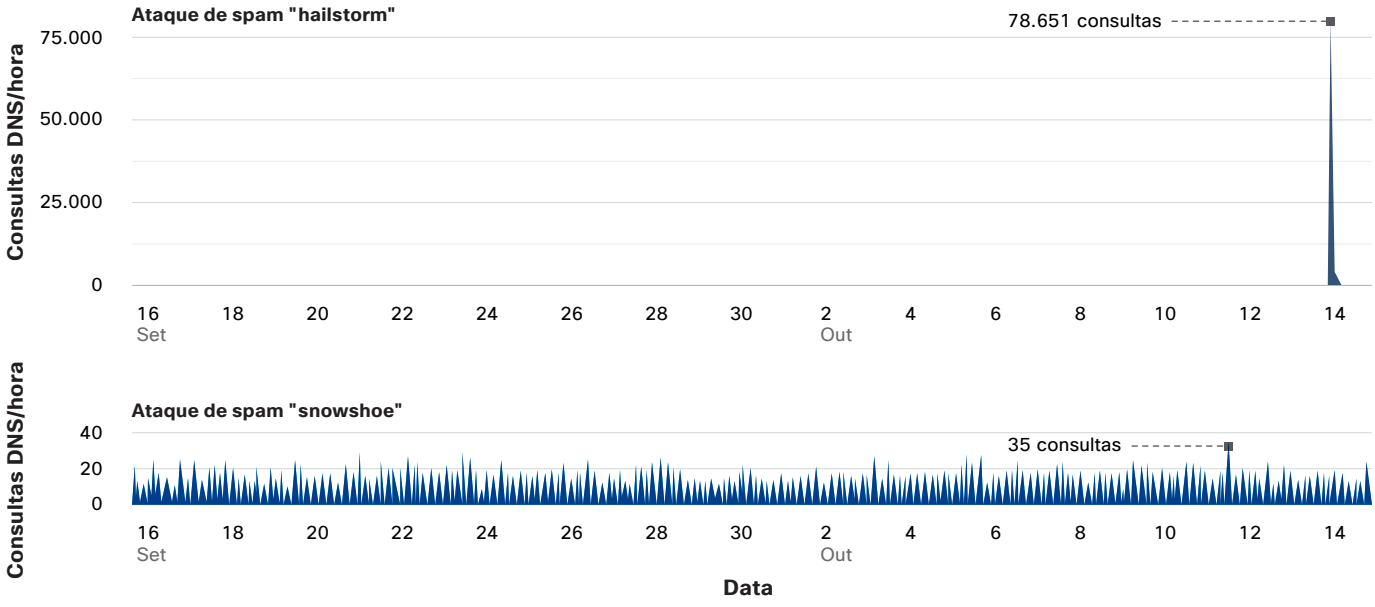
O pico na Figura 18 é um ataque de hailstorm. A atividade é mostrada na interface do Cisco Investigate. Imediatamente antes do ataque, nenhum equipamento estava resolvendo o endereço IP. Em seguida, subitamente, o número de computadores que estão resolvendo o domínio em DNS disparou para mais de 78.000 antes de reduzir a zero.

Contraste o ataque de hailstorm com a campanha de spam snowshoe, também mostrada na Figura 18, em que os invasores tentam passar despercebidos pelas soluções de detecção com base no volume. O número de pesquisas de DNS é constante, mas há apenas cerca de 25 consultas por hora. Esses ataques de baixo volume possibilitam que os criminosos distribuam silenciosamente o spam de uma grande faixa de endereços IP.

Muito embora esses ataques de spam operem de maneira diferente, eles têm aspectos em comum. Com qualquer uma das abordagens, os criminosos podem:

- Evitar uma reputação ruim ao enviar de IPs e domínios limpos
- Emular o marketing de e-mail com conteúdo profissional e gerenciamento de assinatura
- Usar sistemas de e-mail bem configurados em vez de scripts descuidados ou bots de spam
- Configurar corretamente os registros de DNS reverso de círculo completo e SPF (Sender Policy Framework)

Figura 18 Comparação de ataques de spam "snowshoe" e "hailstorm"



Fonte: Cisco Investigate

Os criminosos também podem prejudicar a detecção de conteúdo transformando o texto e alternando tipos de arquivo. (Para obter mais detalhes sobre como os criminosos digitais desenvolvem suas ameaças para escapar de defensores, consulte a seção "Hora de evoluir" na página 34.) Para obter mais informações sobre como eles testaram anexos de arquivo mal-intencionado para spam, consulte a seção anterior.

A Figura 19 mostra alertas de outbreak de ameaças importantes; esse é um resumo das mensagens de spam e phishing que observamos em 2016 que os criminosos atualizavam com frequência para contornar as verificações e as regras de segurança de e-mail. É importante saber que tipos de ameaças de e-mail são predominantes para que você possa evitar ser enganado por essas mensagens mal-intencionadas.

Figura 19 Principais alertas de surto de ameaças

Versão	Identificador de publicação	URL e nome da publicação	Resumo da mensagem	Tipo de arquivo de anexo	Idioma	Data da última publicação
96	35656	RuleID4626	Fatura, pagamento	.zip	Alemão, inglês	25/04/16
87	34577	RuleID10277	Pedido de compra	.zip	Alemão, inglês	02/06/16
82	36916	RuleID4400KVR	Pedido de compra	.zip	Inglês	01/02/16
74	38971	RuleID15448	Pedido de compra, pagamento, recebimento	.zip, .gz	Inglês	08/08/16
72	41513	RuleID18688	Pedido, pagamento, seminário	.zip	Inglês	01/09/16
70	40056	RuleID6396	Pedido de compra, pagamento, recebimento	.rar	Inglês	07/06/16
66	34796	RuleID5118	Pedido de produto, pagamento	.zip	Alemão, inglês	29/09/16
64	39317	RuleID4626 (cont)	Fatura, pagamento, envio	.zip	Inglês, alemão, Espanhol	28/01/16
64	36917	RuleID4961KVR	Confirmação, pagamento/ transferência, pedido, envio	.zip	Inglês	08/07/16
63	37179	RuleID13288	Aviso de entrega, julgamento, fatura de bilhetes	.zip	Inglês, Espanhol	21/07/16
61	38095	RuleID858KVR	Envio, orçamento, pagamento	.zip	Inglês	01/08/16
58	39150	RuleID4961KVR	Solicitação de orçamento, pedido de produto	.zip	Inglês, alemão, Vários idiomas	25/01/16
47	41886	RuleID4961	Transferência, envio, fatura	.zip	Inglês, alemão, Espanhol	22/02/16

Fonte: Cisco Security Research

Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

Reconhecimento | Armamento | Entrega | **Instalação**

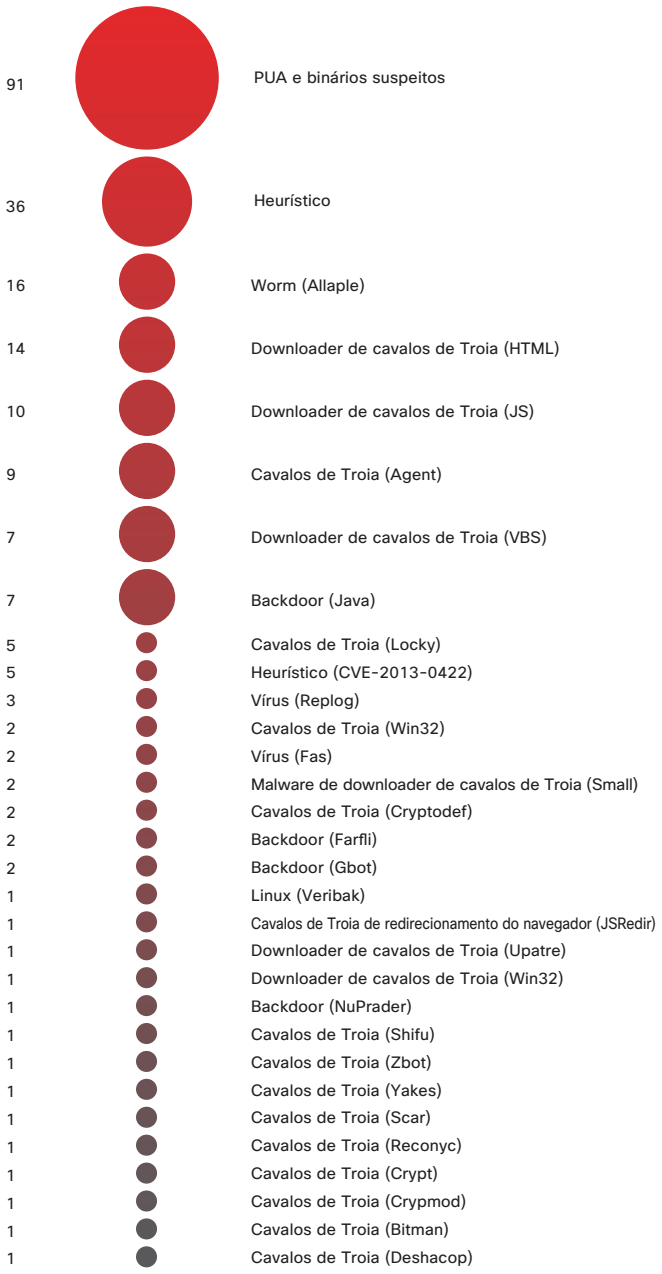
Depois de posicionada, a ameaça instala um backdoor em um sistema de destino, fornecendo acesso persistente aos criminosos.

Métodos de ataque na Web: uma amostra de "cauda longa" revela ameaças que os usuários não podem evitar

A chamada "cauda longa" do espectro dos métodos de ataque na Web (**Figura 20**) inclui um conjunto de tipos de malware de volume menor que são empregados em um estágio posterior na cadeia de ataque: a instalação. Nessa fase, a ameaça que foi entregue – um cavalo de troia bancário, um vírus, um downloader ou alguma outra exploração – instala uma porta dos fundos no sistema de destino, proporcionando aos criminosos o acesso persistente e a oportunidade para roubar dados, iniciar ataques de ransomware e se envolver em outro delito.

As ameaças listadas na **Figura 20** são amostras de assinaturas de malware descobertas que não pertencem aos 50 tipos de malware observados com mais frequência. A cauda longa dos métodos de ataque da Web é basicamente uma amostra das ameaças que estão silenciosamente operando em uma máquina ou sistema após um ataque bem-sucedido. Muitas dessas infecções foram geradas pela primeira vez ao encontrar adware mal-intencionado ou exposição a uma fraude de phishing bem arquitetada. Essas são situações que muitas vezes os usuários podem evitar com facilidade ou corrigir rapidamente.

Figura 20 Exemplo de malware de menor volume observado



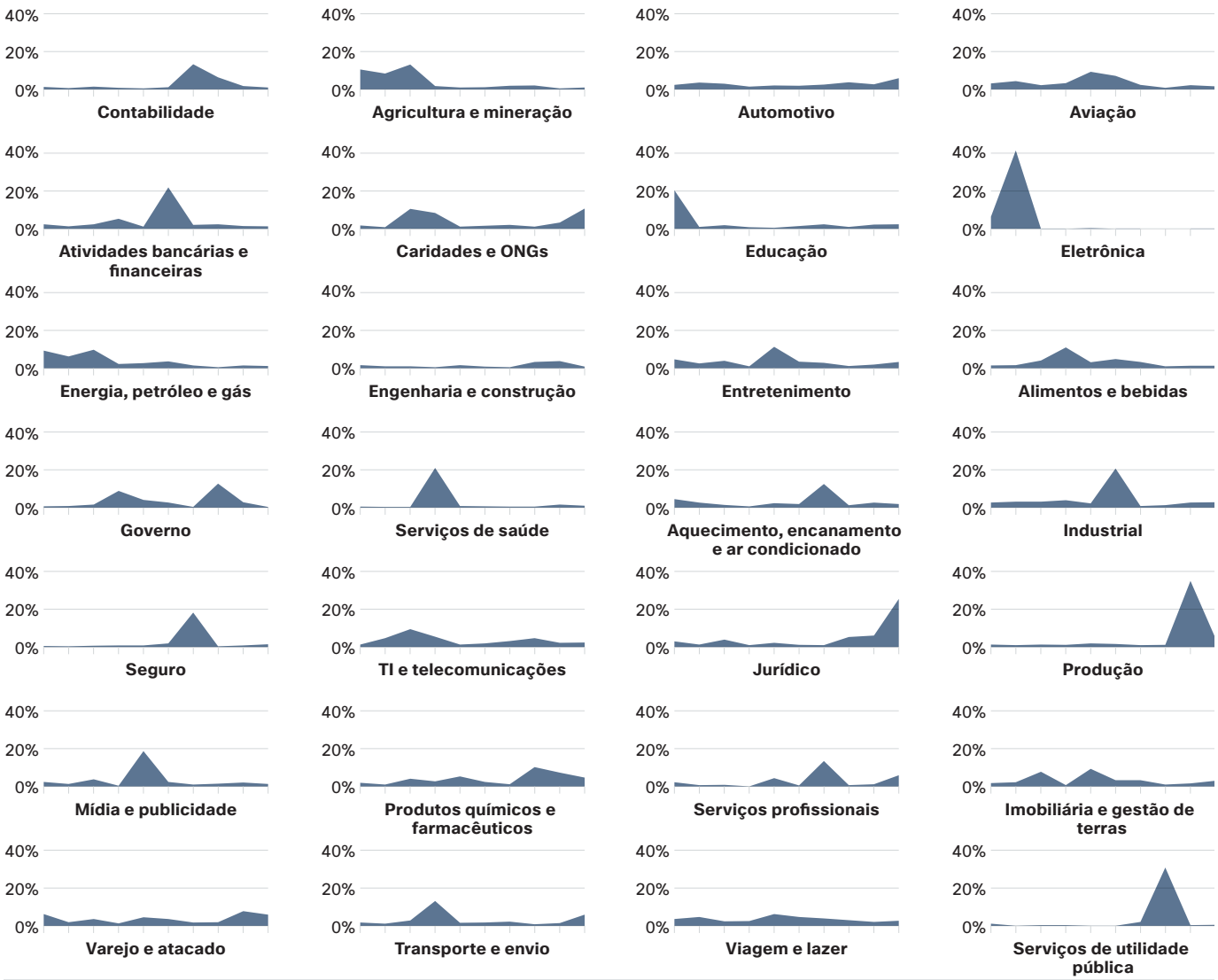
Fonte: Cisco Security Research

Risco de detecções de malware no mercado vertical: os invasores percebem o valor geral

No *Relatório semestral de segurança digital da Cisco de 2016*, uma mensagem fundamental sobre o risco de malware foi que "nenhum mercado vertical é seguro". A julgar pelo exame periódico de nossos pesquisadores do tráfego de ataque ("taxas de bloqueio") e tráfego "normal" ou esperado por setor, essa mensagem permaneceu válida na segunda metade do ano.

Ao analisar mercados verticais e suas taxas de bloqueio ao longo do tempo (Figura 21), percebemos que, em algum momento no decorrer de várias semanas, todos setores tinham ficado sujeitos ao tráfego de ataque em níveis variados. É claro que à medida que os ataques crescem ou fracassam, eles afetam diferentes partes do mercado vertical em épocas diferentes, mas nenhuma delas é poupada.

Figura 21 Porcentagem de taxas de bloqueio verticais mensais



Fonte: Cisco Security Research

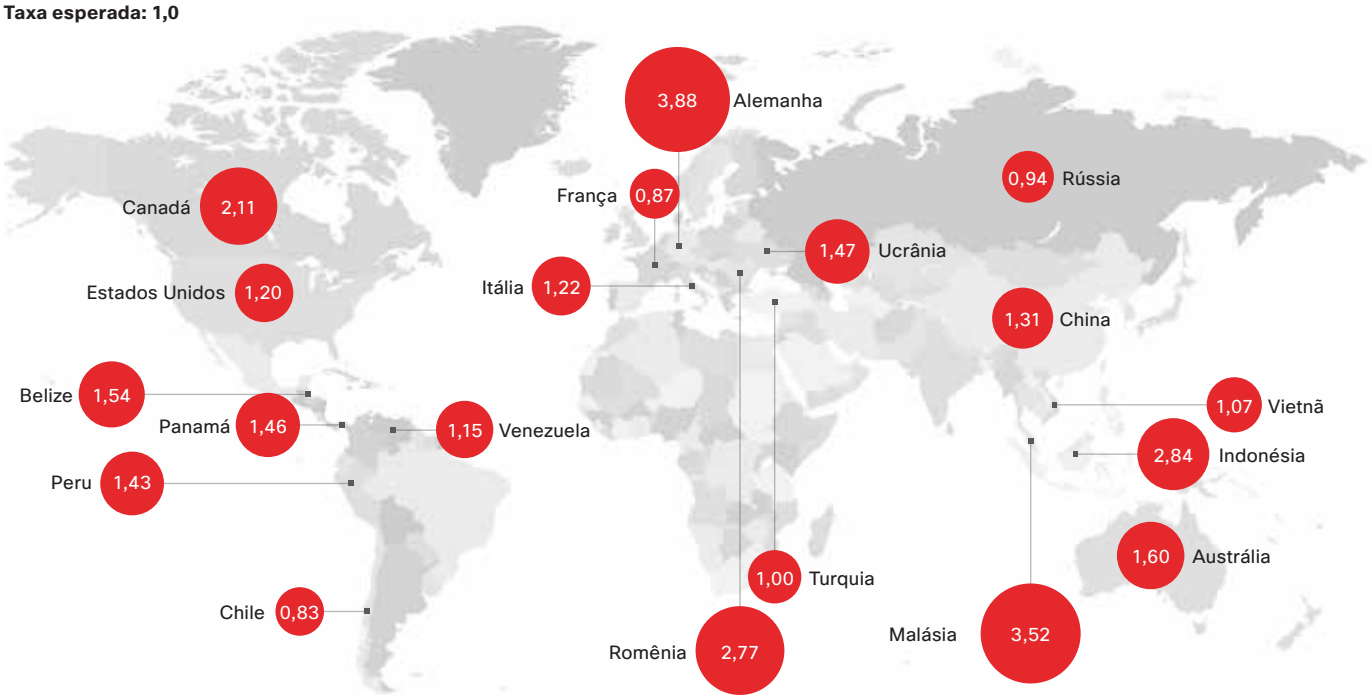
Resumo de atividades de bloqueio da Web por região

Os criminosos mudam frequentemente sua base de operações, pesquisando pontos fracos da infraestrutura de onde possam iniciar suas campanhas. Ao examinar a atividade de bloqueio e o volume geral de tráfego na Internet, os pesquisadores de ameaças da Cisco podem fazer sugestões sobre a origem do malware.

Como mostra a Figura 22, o tráfego dos Estados Unidos subiu ligeiramente das taxas de bloqueio observadas no *Relatório de segurança digital da Cisco 2016*. Os Estados Unidos abrigam uma parte muito maior de bloqueios, mas isso deve ser considerado em função de sua participação muito maior no tráfego on-line. Além disso, os Estados Unidos são um dos maiores públicos-alvo de ataques de malware no mundo.

O que precisa ser lembrado por profissionais de segurança: da mesma forma que a atividade de bloqueio da Web vertical, a atividade de bloqueio da Web regional mostra que o tráfego de malware é um problema global.

Figura 22 Bloqueios da Web por país



Fonte: Cisco Security Research

COMPARTILHAR

Tempo de detecção: uma métrica essencial para avaliar o progresso dos defensores

A Cisco está refinando continuamente nossa abordagem para medição do TTD para que possamos rastrear e relatar a estimativa mais precisa de nosso TTD médio. Os ajustes recentes à nossa abordagem aumentaram nossa visibilidade dos arquivos que foram classificados como "desconhecidos" quando foram vistos pela primeira vez e depois identificados como "conhecido e prejudicial" após contínua análise e observação global. Com uma visão mais holística dos dados, podemos identificar melhor quando uma ameaça surgiu e exatamente quanto tempo levou para que as equipes de segurança determinassem que ela era uma ameaça.

Esse novo insight nos ajudou a determinar que nosso TTD médio foi de 39 horas em novembro de 2015. (Consulte a Figura 23.) Até janeiro de 2016, reduzimos o TTD médio para 6,9 horas. Após coletar e analisar os dados de outubro de 2016, nossos pesquisadores de ameaças detectaram que os produtos Cisco obtiveram um TTD médio de 14 horas para o período de novembro de 2015 até outubro de 2016. (Observação: os números de TTD médio para 2016 representam a média do período observado.)

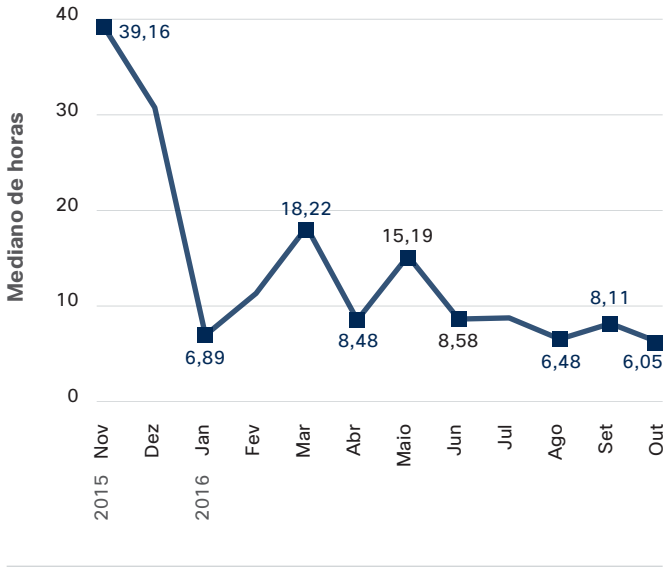
O TTD médio oscilou durante 2016, mas a tendência geral foi de baixa. Os aumentos no TTD médio indicam os horários em que os criminosos iniciaram uma onda de novas ameaças. As diminuições subsequentes refletem períodos em que os defensores obtiveram vantagem e puderam identificar as ameaças conhecidas rapidamente.

A Figura 23 também mostra que o TTD médio foi de cerca de 15 horas até o fim de abril de 2016, que é superior ao número de 13 horas relatado no *Relatório de segurança digital da Cisco 2016*.[14] Esse número de 15 horas tem como base os dados coletados de novembro de 2015 a abril de 2016. Não foi resultado do uso de nossa abordagem modificada para analisar informações retrospectivas mais detalhadas sobre os arquivos. Usando o novo número de TTD semestral, podemos relatar que o TTD foi reduzido para cerca de 9 horas para o período de maio a outubro de 2016.

A análise dos dados retrospectivos é importante não só para determinar uma medida mais precisa de nosso TTD médio, como também para estudar como as ameaças evoluem ao longo do tempo. Várias ameaças no cenário são particularmente evasivas e podem levar muito tempo para serem identificadas, muito embora sejam conhecidas pela comunidade de segurança.

Os criminosos evoluirão determinadas linhas de malware para evitar a detecção e aumentar seu tempo de operação. Essa tática impede o progresso dos defensores em ganhar e depois manter uma vantagem na detecção de muitos tipos de ameaças conhecidas. (Para obter mais informações sobre esse assunto, consulte "Hora da evolução: para algumas ameaças, a mudança é uma constante", página 34). No entanto, o fato de que os criminosos digitais estão evoluindo suas tarefas com frequência e rapidez indica que estão enfrentando pressão intensa e constante para encontrar formas de manter a operação e a lucratividade de suas ameaças.

Figura 23 Mediano de TTD por mês



Fonte: Cisco Security Research

A Cisco define "tempo para detecção" (TTD) como a janela de tempo entre um comprometimento 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. Usando nossa visibilidade global e um modelo contínuo de análise, podemos medir a partir do momento em que o código mal-intencionado é executado em um endpoint até o momento em que ele é determinado como uma ameaça, para todos os códigos mal-intencionados que não foram classificados no momento do encontro.

[14] *Relatório semestral de segurança digital da Cisco de 2016*: **http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html**.

Hora da evolução: para algumas ameaças, a mudança é uma constante

Os criminosos digitais usam várias técnicas de ofuscação para manter seu malware forte e lucrativo. Dois métodos comuns que empregam são a evolução de seus tipos de entrega de payload e a geração rápida de novos arquivos (derrubando os métodos de detecção exclusivos de hash). Nossos entrevistados examinaram como os criminosos usaram essas duas estratégias para ajudar seis linhas de malware bem conhecidas — Locky, Cerber, Nemucod, Adwind RAT, Kryptik e Dridex — a escapar da detecção e continuar comprometendo usuários e sistemas.

Através de nossa análise, buscamos medir o "tempo para evolução" (TTE): o tempo necessário para que os criminosos alterem a forma como o malware específico é disponibilizado e a duração de tempo entre cada mudança de tática. Analisamos dados de ataque da Web de diferentes fontes da Cisco, especificamente, dados de proxy da Web, produtos de malware avançados na nuvem e de endpoint e mecanismos antimalware compostos.

Nossos pesquisadores procuraram alterações nas extensões de arquivos que disponibilizavam o malware e o tipo de conteúdo do arquivo (ou MIME) conforme definido pelo sistema do usuário. Determinamos que cada linha de malware tem um padrão exclusivo de evolução. Para cada linha, examinamos os padrões nos métodos de entrega via Web e por e-mail. Também rastreamos a idade dos hashes exclusivos associados a cada família de malware para determinar com que velocidade os criminosos estão criando novos arquivos (e, assim, novos hashes).

Através de nossa pesquisa, descobrimos que:

- As linhas de ransomware parecem ter uma rotação similar de novos binários. Entretanto, o Locky usa mais combinações de MIME e extensão de arquivo para disponibilizar seu payload.
- Algumas linhas de malware empregam somente alguns métodos de entrega de arquivo. Outras usam 10 ou mais. Os criminosos tendem a usar binários eficazes durante períodos longos. Em outros casos, os arquivos surgem e são descartados rapidamente, indicando que os criadores do malware estão sob pressão para mudar de tática.
- As linhas de malware Adwind RAT e Kryptik têm um TTD médio mais alto. (Para saber mais sobre TTD, consulte a página 33.) Também observamos uma maior mistura de idades de arquivos para essas linhas. Isso sugere que os criminosos reutilizam binários eficazes que sabem que são difíceis de detectar.
- Analisando as idades dos arquivos para a linha de malware Dridex, a impressão é que a economia paralela pode estar abandonando o uso desse anteriormente conhecido cavalo de troia bancário. No final de 2016, o volume de detecção do Dridex foi reduzido, assim como o desenvolvimento de novos binários para fornecer esse malware. Essa tendência sugere que os criadores do malware não obtêm mais vantagens com a evolução dessa ameaça ou que eles descobriram uma nova forma de empacotar o malware que tornou mais difícil sua detecção.

TTE e TTD

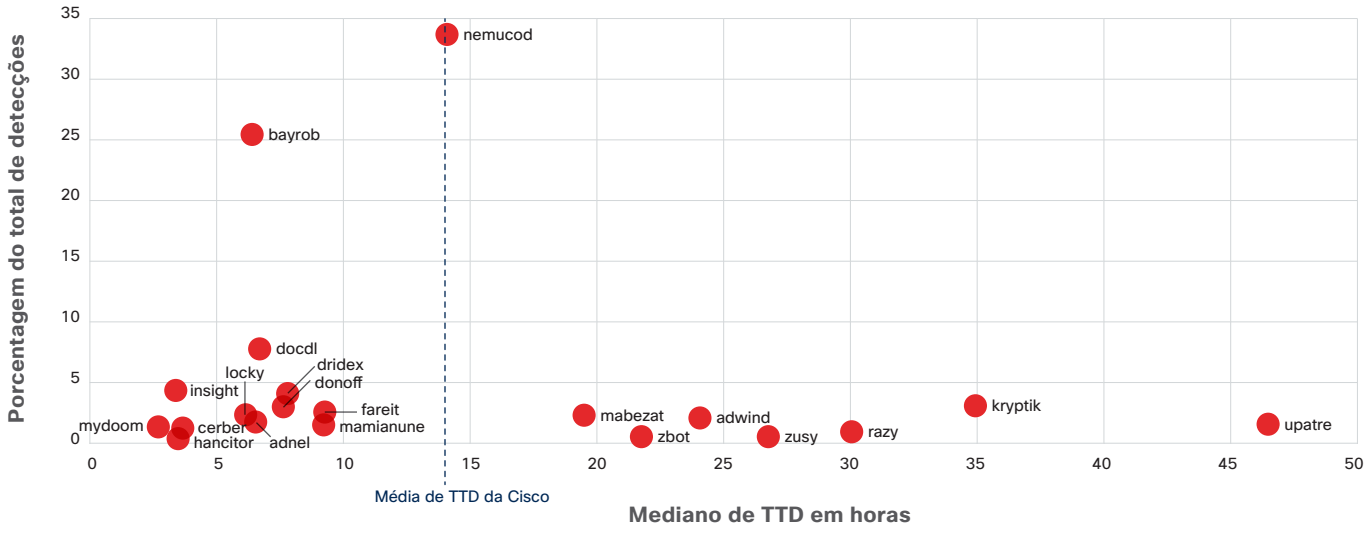
As seis linhas de malware que analisamos em nosso estudo de TTE estão listadas na **Figura 24**. O gráfico retrata o TTD médio para as 20 principais linhas (por número de detecção) que nossos pesquisadores observaram de novembro de 2015 a novembro de 2016. O TTD médio desse período foi de cerca de 14 horas. (Para obter detalhes sobre como calculamos o TTD, consulte a página 33.)

Muitas das linhas de malware que os produtos Cisco estão detectando no TTD médio são ameaças industrializadas que se espalham rapidamente e que, portanto, são mais predominantes. Dois exemplos são os tipos de ransomware Cerber e Locky.

As ameaças antigas e difundidas que os criminosos não se dão ao trabalho de evoluir muito, ou nada, são geralmente detectadas abaixo do TTD médio. Entre os exemplos estão linhas de malware como Bayrob (malware de botnet), Mydoom (um worm que afeta o Microsoft Windows) e Dridex (o cavalo de troia bancário).

Nas próximas seções, apresentaremos destaques da pesquisa sobre TTE e TTD para as linhas de malware Locky, Nemucod, Adwind Rat e Kryptik. Estão incluídas descobertas detalhadas do Cerber e do Dridex no Apêndice, na página 78.

Figura 24 Medianos de TTD das 20 principais linhas de malware (por contagem de detecção)



Fonte: Cisco Security Research

COMPARTILHAR

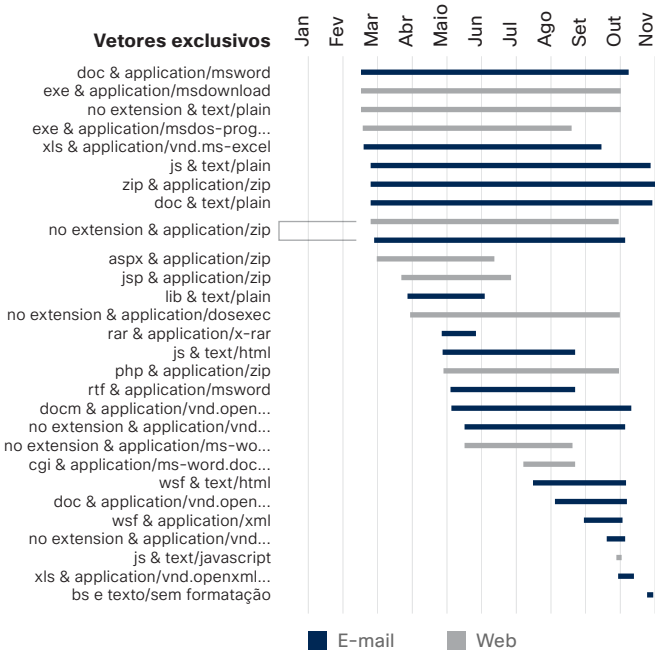
Análise de TTE: Locky

Com a nossa pesquisa de TTE, descobrimos que o Locky e o Cerber utilizam um número limitado de combinações de MIME e extensão de arquivo para distribuir malware pela Web ou por e-mail (Consulte a **Figura 25**). Observamos várias combinações que incluíam os tipos de conteúdo de arquivo relacionados ao Microsoft Word (msdownload, ms-word). Entretanto, as extensões de arquivo associadas (.exe e .cgi) não apontavam de volta para um arquivo Word. Também identificamos os tipos de conteúdo que apontavam para arquivos .zip mal-intencionados.

Tanto o Locky como o Cerber parecem usar binários novos com frequência, em uma tentativa de escapar da detecção em arquivos. O envelhecimento de arquivo para a família de malware Locky é mostrado na **Figura 26**. A parte superior do gráfico descreve o envelhecimento de arquivos que foram observados durante um determinado mês. A parte inferior do gráfico mostra alterações mensais no volume de hashes relacionados ao Locky, tanto arquivos novos como os já observados anteriormente.

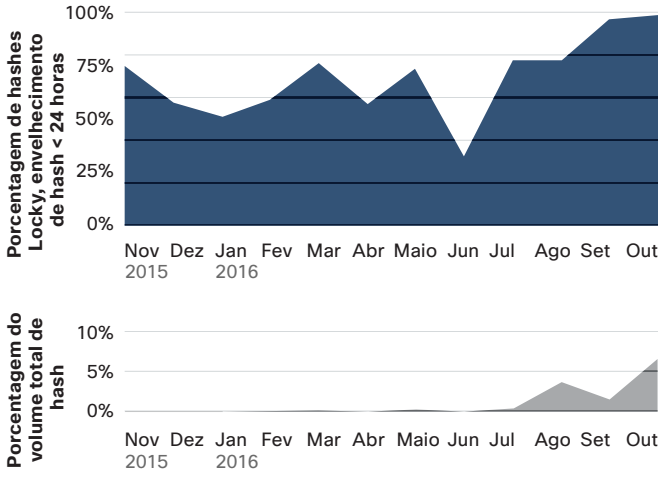
Na **Figura 26**, observe também o declínio no volume em junho e a distribuição do envelhecimento de arquivo. O botnet Necurs, conhecido por fornecer o Locky, foi retirado do ar em junho. Isso provavelmente anulou os esforços dos autores de malware para mantê-lo atualizado durante o mês. Entretanto, é claro que eles conseguiram se recuperar rapidamente. Em julho, o malware tinha retornado à sua combinação mais padrão de envelhecimento de arquivo, com a maioria (74%) tendo menos de um dia de vida quando detectado pela primeira vez.

Figura 25 Combinações de MIME e extensão de arquivo para a linha de ameaças e indicadores que geram e incluem o payload Locky (vetores Web e e-mail)



Fonte: Cisco Security Research

Figura 26 Envelhecimento de hash para a linha de malware Locky e percentual do volume total de hash observado por mês

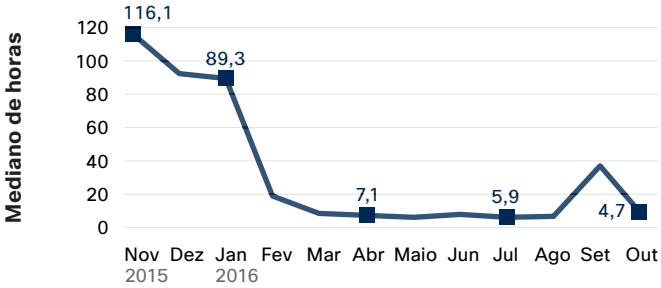


Fonte: Cisco Security Research

O ciclo rápido de binários para este ransomware não chega a ser uma surpresa. As instâncias do Locky e do Cerber geralmente são detectadas no mesmo dia em que são lançadas ou um a dois dias depois. Com isso, o desenvolvimento contínuo dessas ameaças passa a ser essencial para os criminosos se eles quiserem permanecer ativos e eficientes. A Figura 24, discutida anteriormente, mostra que os produtos da Cisco detectaram ransomware Locky e Cerber no mediano de TTD em 2016.

A **Figura 27** mostra o mediano de TTD para o ransomware Locky, que caiu drasticamente de aproximadamente 116 horas em novembro de 2015 para apenas 5 horas em outubro de 2016.

Figura 27 TTD da linha de malware Locky

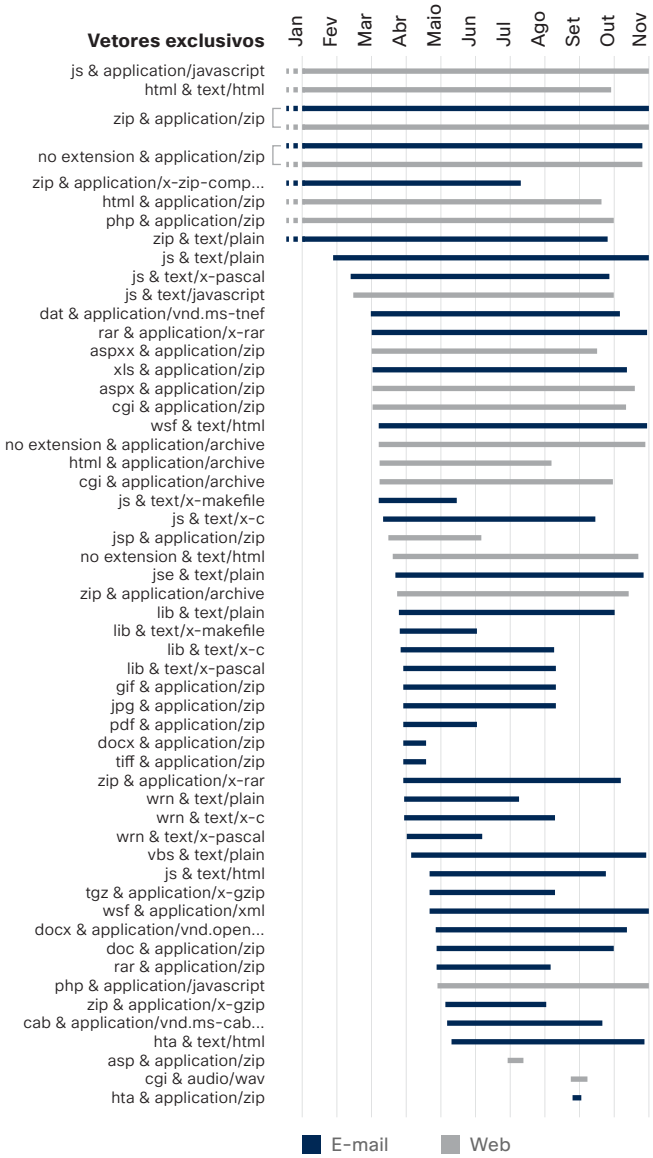


Fonte: Cisco Security Research

Análise de TTE: Nemucod

Em 2016, o Nemucod era o malware detectado com mais frequência entre as 20 principais famílias mostradas na Figura 24. Os criminosos usam esse malware de downloader para distribuir ransomware e outras ameaças, como cavalos de Troia backdoor que facilitam fraudes do clique. Algumas variações de Nemucod também servem como mecanismo para disponibilizar o payload do malware Nemucod.

Figura 28 Combinações de MIME e extensão de arquivo para Nemucod (vetores Web e e-mail)



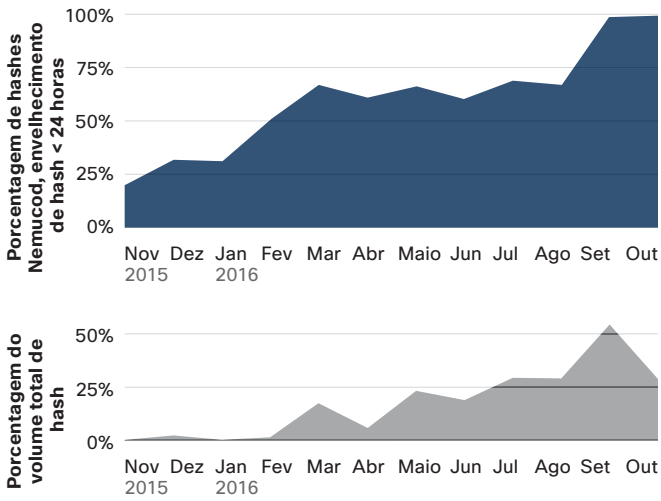
Fonte: Cisco Security Research

Um motivo para o malware Nemucod ter sido tão comum em 2016, segundo nossos pesquisadores de ameaças, é que seus autores evoluíram essa ameaça constantemente. A Cisco identificou mais de 15 combinações de MIME e extensão de arquivo associadas à família de Nemucod que foram usadas para distribuir malware pela Web. Muito mais combinações foram usadas para transmitir a ameaça para usuários por e-mail (Figura 28).

Várias combinações de MIME e extensão de arquivo (Web e e-mail) foram projetadas para direcionar os usuários para arquivos mortos ou arquivos .zip mal-intencionados. Os criminosos também reutilizaram muitas combinações durante os meses em que observamos.

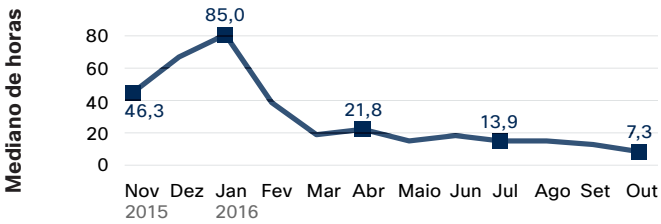
Como mostra a Figura 29, muitos hashes Nemucod têm menos de dois dias de vida quando são detectados. Em setembro e outubro de 2016, quase todos os binários relacionados à família de Nemucod que foram bloqueados tinham menos de um dia.

Figura 29 Envelhecimento de hash para a linha de malware Nemucod e percentual do volume total de hash observado por mês



Fonte: Cisco Security Research

Figura 30 TTD da linha de malware Nemucod



Fonte: Cisco Security Research

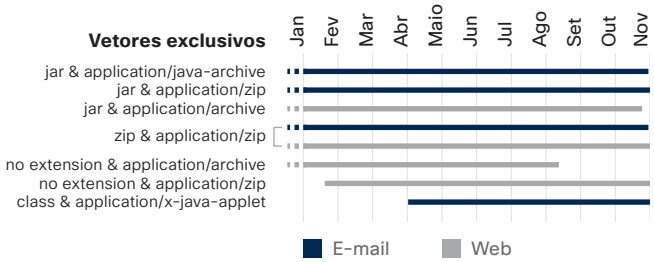
Análise de TTE: Adwind RAT

Os pesquisadores de ameaças da Cisco constataram que o malware Adwind RAT (cavalo de Troia para acesso remoto) é disponibilizado por meio de combinações de MIME e extensão de arquivo que incluem arquivos .zip ou .jar. Isso ocorre quando o malware é veiculado pelo vetor de ataque Web ou e-mail (Consulte a **Figura 31**).

O Adwind RAT usou uma ampla gama de envelhecimento de hash durante quase todo o período observado em 2016, exceto em setembro e outubro, quando a maioria dos arquivos analisados tinha um a dois dias de vida (**Figura 32**).

Também verificamos que o mediano de TTD para o Adwind RAT é consistentemente maior que o mediano de TTD para outras famílias de malware que analisamos (**Figura 33**). Os autores de malware aparentemente desenvolveram mecanismos de envio difíceis de detectar, que são a razão do sucesso do Adwind RAT. Com isso, eles não precisam fazer rodízio de hashes com tanta frequência ou tão rapidamente quanto os agentes por trás de outras famílias de malware. O cavalo de Troia Adwind também é conhecido por outros nomes, como JSocket e AlienSpy.

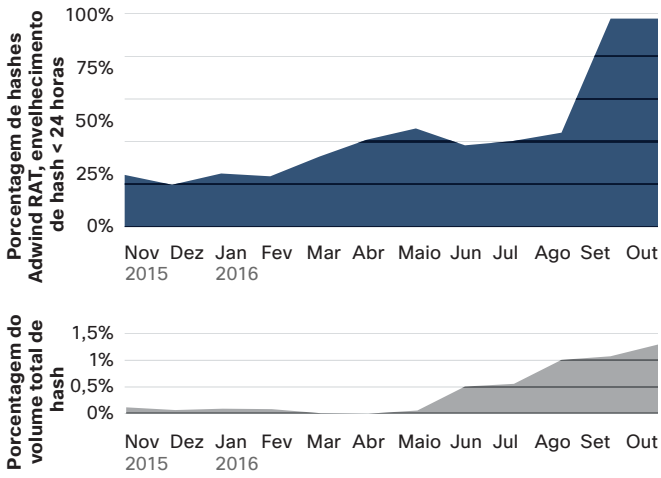
Figura 31 Combinações de MIME e extensão de arquivo para Adwind RAT (vetores Web e e-mail)



Fonte: Cisco Security Research

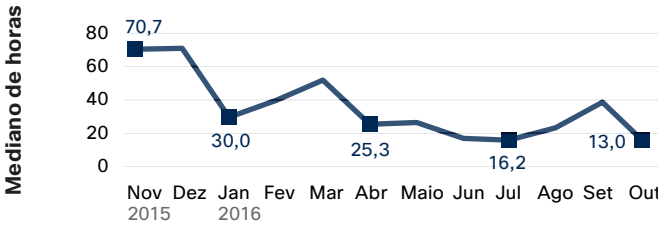
Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

Figura 32 Envelhecimento de hash para a linha de malware Adwind RAT e percentual do volume total de hash observado por mês



Fonte: Cisco Security Research

Figura 33 TTD da linha de malware Adwind RAT



Fonte: Cisco Security Research

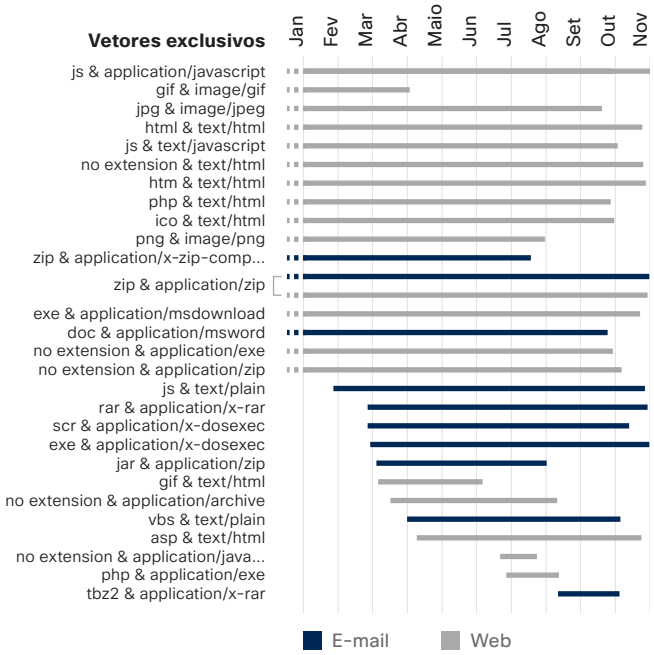
Análise de TTE: Kryptik

O Kryptik, assim como o malware Adwind RAT, teve um mediano de TTD consistentemente mais alto (aproximadamente 20 horas) do que as outras famílias de malware que a Cisco analisou para o estudo de TTE de novembro de 2015 a outubro de 2016 (Figura 36). Entretanto, até outubro, os produtos Cisco tinham reduzido a janela do mediano de TTD do malware Kryptik para menos de 9 horas (Figura 36).

A família de malware Kryptik também usou uma variedade maior de envelhecimento de hash do que as outras famílias de malware que analisamos, principalmente durante a primeira metade de 2016. A confiança dos autores de Kryptik em hashes mais antigos por tanto tempo indica que os defensores têm problema em detectar esse tipo de malware.

Durante o período que observamos, os autores de Kryptik utilizaram uma ampla variedade de métodos de distribuição de payload com o vetor de ataque da Web. Os autores usaram arquivos JavaScript e arquivos mortos, como arquivos .zip, em combinações de MIME e extensão de arquivo tanto para Web como para e-mail (Consulte a Figura 34). Algumas das combinações datam de 2011.

Figura 34 Combinações de MIME e extensão de arquivo para Kryptik (vetores Web e e-mail)

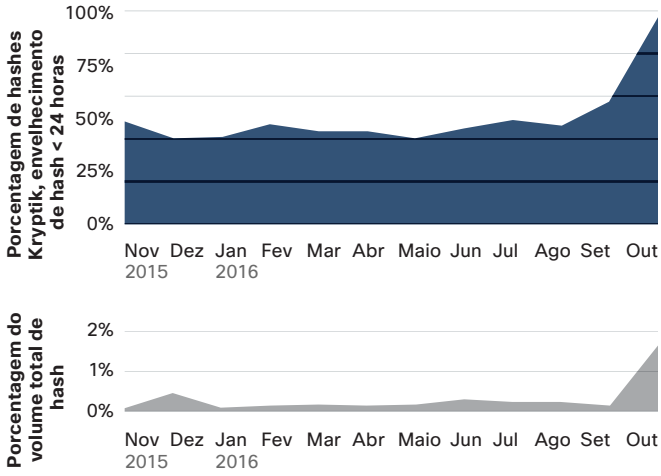


Fonte: Cisco Security Research

Em nossa análise das seis famílias de malware, descobrimos que os criminosos precisam mudar de tática com frequência para aproveitar a pequena janela de tempo em que as ameaças não encontram resistência. Esses ajustes indicam que os defensores estão detectando malware conhecido com maior rapidez, mesmo depois que uma ameaça tenha evoluído. Os invasores estão sob pressão para encontrar novas maneiras de evitar a detecção e manter suas campanhas lucrativas.

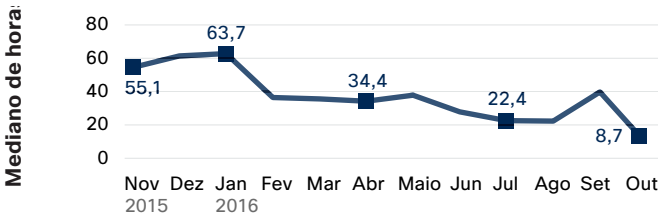
Neste cenário complexo e de rápida evolução, em que todas as famílias de malware se comportam de forma diferente, soluções pontuais e experiência em relação ao comportamento humano não são suficientes para identificar e responder rapidamente às ameaças. Uma arquitetura de segurança integrada que ofereça informações em tempo real sobre ameaças, juntamente com detecção e defesa automatizadas, é essencial para melhorar o TTD e garantir a correção rápida quando as infecções ocorrem.

Figura 35 Envelhecimento de hash para a linha de malware Kryptik e percentual do volume total de hash observado por mês



Fonte: Cisco Security Research

Figura 36 TTD da linha de malware Kryptik



Fonte: Cisco Security Research

Comportamento dos defensores

Comportamento dos defensores

Declínio das vulnerabilidades em 2016

Na segunda metade de 2016, as vulnerabilidades divulgadas por fornecedores caíram consideravelmente em relação a 2015, segundo nossa pesquisa (**Figura 37**). O National Vulnerability Database mostra um declínio semelhante. Os motivos para a queda em relatórios formais de vulnerabilidades divulgadas não são totalmente claros.

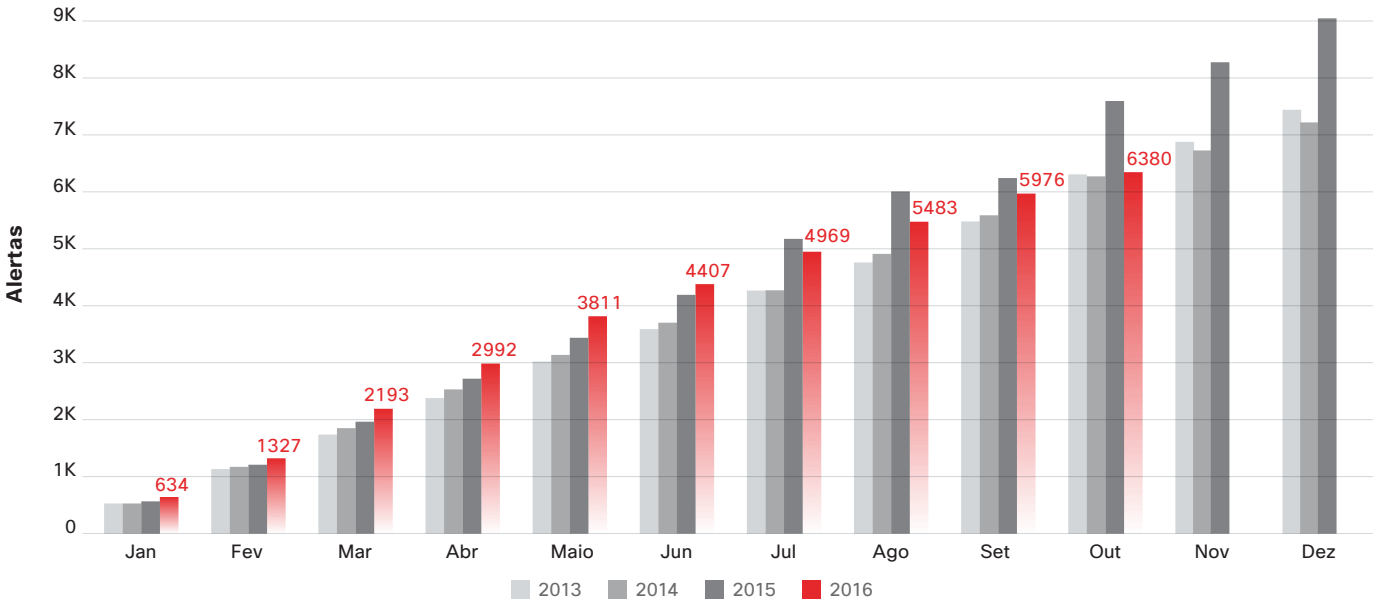
Observe que 2015 foi um ano excepcionalmente ativo em termos de vulnerabilidades, por isso os números de 2016 podem refletir um ritmo normal de avisos de vulnerabilidades. De janeiro a outubro de 2015, o total de alertas chegou a 7.602. Durante o mesmo período em 2016, o total de alertas foi de 6.380; nesse período em 2014, foram 6.272 alertas

O alto número de relatórios de vulnerabilidades em 2015 pode indicar que os fornecedores estavam mais atentos aos códigos e produtos existentes, implementavam com mais cuidado práticas de SDL (ciclo de vida de desenvolvimento seguro) e identificavam e corrigiam as vulnerabilidades. O declínio no volume de vulnerabilidades relatadas pode indicar que esses esforços estão compensando. Ou seja, os fornecedores agora estão se concentrando em identificar vulnerabilidades e corrigi-las antes que os produtos cheguem ao mercado.

Em 2016, a Apple foi o fornecedor que mostrou o maior declínio nas vulnerabilidades: a empresa relatou 705 vulnerabilidades em 2015 e 324 vulnerabilidades em 2016 (uma queda de 54%). Da mesma forma, a Cisco relatou 488 vulnerabilidades em 2015 e 310 em 2016 (uma queda de 36%).

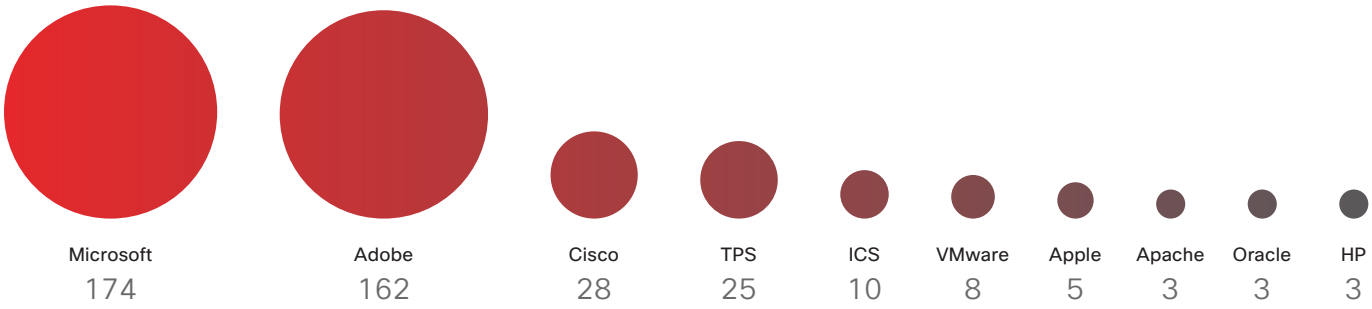
Uma preocupação entre os pesquisadores de segurança é que a "fadiga da vulnerabilidade" possa estar se alojando entre os profissionais de segurança. Nos últimos meses, não houve um comunicado importante de vulnerabilidade que repercutisse no setor, como foi o caso do Heartbleed em 2014. Na verdade, o entusiasmo em torno das "chamadas" vulnerabilidades (como o Heartbleed) e o aumento em 2015 provavelmente contribuíram para o nível de fadiga ou, pelo menos, para o menor interesse em relatar as vulnerabilidades.

Figura 37 Totais acumulados de alertas anuais



Fonte: Cisco Security Research

Figura 38 Relatórios formais de vulnerabilidade crítica por fabricante e tipo



Fonte: National Vulnerability Database (NVD)

A Cisco está adotando as classificações de gravidade/impacto (SIRs), em que os níveis de avaliação são "crítico", "alto", "médio" e "baixo". As classificações refletem uma priorização simplificada de pontuações do Common Vulnerability Scoring System (CVSS). Além disso, a Cisco adotou o CVSS v3.0, sucessor do CVSS v2.0. Devido a essa mudança, algumas vulnerabilidades podem ter pontuações mais altas e, consequentemente, os profissionais de segurança podem observar um pequeno aumento nas vulnerabilidades classificadas como "críticas" e "altas", em vez de "médias" e "baixas". Para obter mais informações sobre essa alteração na pontuação, leia a publicação do blog Cisco Security, The Evolution of Scoring Security Vulnerabilities: The Sequel.

No Estudo comparativo de recursos de segurança da Cisco de 2015 (página 49), os profissionais de segurança indicaram uma leve redução na aceitação da operacionalização da segurança. Essa redução pode estar relacionada à "fadiga" decorrente da necessidade de implementar continuamente atualizações e patches. Por exemplo, em 2016, 53% dos profissionais de segurança concordavam plenamente em revisar e aperfeiçoar as práticas de segurança de maneira regular, formal e estratégica. Em 2014 e 2015, 56% concordavam plenamente.

É óbvio que um declínio nas vulnerabilidades não deve resultar em excesso de confiança quanto ao cenário de ameaças. Ninguém deve achar que o cuidado com as ameaças pode ser interrompido, mesmo na ausência de grandes vulnerabilidades.

Como recomendamos em relatórios passados, os profissionais de segurança devem fazer um esforço concentrado para priorizar os patches. Se a falta de pessoal e outros recursos impedirem a instalação de todos os patches disponíveis dentro do prazo, avalie quais são os mais importantes para a segurança da rede e coloque-os no topo da lista de tarefas.

Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

Figura 39 Relatórios formais de vulnerabilidades selecionadas

Título da recomendação	Data emitida
Vulnerabilidade de execução de código de corrupção de memória do Adobe Acrobat e do Acrobat Reader	28 de julho de 2016
Vulnerabilidade de execução de código remoto de corrupção de memória do Adobe Acrobat e do Acrobat Reader	28 de julho de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	21 de julho de 2016
Vulnerabilidade de saturação de inteiros do Adobe Acrobat e do Acrobat Reader	terça-feira, 23 de maio de 2016
Vulnerabilidade de execução de código remoto de corrupção de memória do Adobe Acrobat e do Acrobat Reader	08 de fevereiro de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	28 de julho de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	18 de julho de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	23 de julho de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	terça-feira, 24 de maio de 2016
Vulnerabilidade de corrupção de memória do Adobe Acrobat e do Acrobat Reader	terça-feira, 23 de maio de 2016

Fonte: Cisco Security Research

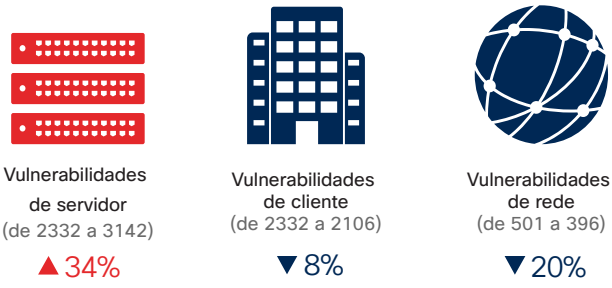
Os relatórios formais listados acima são vulnerabilidades de 2016 classificadas como críticas que foram relatadas por várias fontes por terem o código de exploração disponibilizado publicamente ou serem exploradas ativamente.

Vulnerabilidades do servidor e do cliente

Conforme discutido no *Relatório Semestral de Segurança Digital da Cisco de 2016*, os criminosos estão encontrando espaço e tempo para agir dentro das soluções de servidor. Ao realizar ataques no software de servidor, esses invasores podem controlar outros recursos de rede ou até se movimentarem lateralmente entre outras soluções essenciais.

Os pesquisadores da Cisco monitoraram as vulnerabilidades de clientes e servidores de acordo com os fornecedores (Figura 40).

Figura 40 Análise de vulnerabilidades de cliente-servidor, 2015-2016



Fonte: National Vulnerability Database

Middleware: Criminosos percebem software sem correções como ótima oportunidade

No *Relatório Semestral de Segurança Digital da Cisco de 2016*, nós compartilhamos dados sobre ataques realizados contra os sistemas de servidor. Em 2017, o middleware, responsável por conectar plataformas e aplicativos, será o principal alvo de criminosos que buscam espaços de operação nos quais o reconhecimento e a resposta a ameaças por parte dos defensores sejam lentos.

Enquanto procuravam vulnerabilidades em software de terceiros, os pesquisadores da Cisco descobriram uma média de 14 novas vulnerabilidades por mês em software. A maioria dessas vulnerabilidades (62) foram causadas pelo uso de middleware. Dessas 62 vulnerabilidades, 20 estavam no código que gerencia PDFs; 12, no código que gerencia imagens; 10, no código de soluções básicas de produtividade empresarial; 9, no código para compactação; e 11, em outras bibliotecas (Figura 41).

As vulnerabilidades de middleware representam uma ameaça singular à segurança, uma vez que suas bibliotecas não costumam ser atualizadas com a mesma frequência de um software voltado para clientes (ou seja, software com o qual os usuários interagem diariamente, como por exemplo as soluções de produtividade). As bibliotecas de middleware podem ser excluídas dos processos de auditoria de software, de modo que as vulnerabilidades permaneçam inalteradas.

Figura 41 Vulnerabilidades encontradas em bibliotecas de middleware

Fonte: Cisco Security Research

As empresas podem até apostar na segurança do middleware, dando maior atenção à atualização de soluções com maior visibilidade. Contudo, é possível que elas saiam no prejuízo, caso os criminosos tentem acessar as redes por meio de caminhos menos conhecidos. Desse modo, o middleware se transforma em um ponto cego da segurança para os defensores, sinalizando uma oportunidade para os criminosos.

O desafio de atualizar as bibliotecas de middleware está estreitamente relacionado ao problema do software de código aberto (questão discutida no *Relatório semestral sobre segurança da Cisco de 2015*), já que muitas soluções de middleware são projetadas por desenvolvedores de código aberto. (No entanto, o problema atual pode afetar os desenvolvedores de middleware proprietário e de código aberto.) Desse modo, as bibliotecas de middleware precisam contar com diversos desenvolvedores para mantê-las atualizadas. Na lista de tarefas de uma equipe de TI ou de segurança já sobrecarregada, é possível que as atualizações das bibliotecas de middleware não ganhem muita atenção; no entanto, elas devem receber maior prioridade.

Qual é o possível impacto de uma vulnerabilidade de middleware, se explorada por criminosos? Como existem conexões entre o middleware e outros sistemas essenciais, como os e-mails e as mensagens, um invasor pode se mover lateralmente até esses sistemas para enviar mensagens de pishing ou de spam. Além disso, os criminosos também podem se passar por usuários autorizados e se valer das relações de confiança entre usuários para obter acesso a áreas restritas.

Caso não queira ser vítima de um ataque lançado por meio da vulnerabilidade de middleware, você deve:

- Manter uma lista atualizada das bibliotecas e dependências mais conhecidas dos aplicativos que costuma utilizar
- Monitorar ativamente a segurança desses aplicativos e minimizar riscos sempre que possível
- Inserir um acordo de nível de serviço nos contratos firmados com fornecedores de software, cujo objetivo é o fornecimento de correções em tempo hábil
- Realizar auditorias e analisar as dependências do software e a utilização da biblioteca com frequência
- Pedir aos fornecedores de software detalhes sobre os processos de manutenção e teste dos produtos

Em resumo: os atrasos na correção de falhas aumentam o espaço operacional dos criminosos, dando a eles mais tempo para obter controle sobre os sistemas essenciais. Na próxima seção, discutiremos esse impacto e as tendências em relação à correção de falhas presentes em soluções básicas de produtividade, como os navegadores da Web.

Hora de corrigir falhas: Como reduzir o período de recuperação

Vários usuários não fazem o download nem instalam as correções em tempo hábil. E os criminosos podem usar essas vulnerabilidades sem correções para acessar as redes. Em nossa última pesquisa, descobrimos que a chave para encorajar os usuários a fazer o download e instalar as correções está na regularidade com que os fornecedores lançam atualizações de software.

O lançamento de uma versão de correção de segurança é um forte sinalizador de que há vulnerabilidades que podem ser exploradas. Ainda que alguns criminosos mais sofisticados já venham explorando essas vulnerabilidades há algum tempo, a notificação sobre a existência de uma correção informa a outros criminosos que as versões mais antigas do software podem ser exploradas.

Quando os fornecedores de software liberam novas versões regularmente, os usuários se acostumam a baixar e instalar essas atualizações. Por outro lado, quando um fornecedor não lança versões de atualização de maneira constante, os usuários não criam o hábito de instalá-las. Eles continuam a usar soluções desatualizadas, que podem conter vulnerabilidades prontas para serem exploradas.

Veja a seguir outros comportamentos que podem afetar o ciclo de atualizações:

- A inconveniência da experiência de lembrete
- A facilidade de cancelar as atualizações
- A frequência de uso do software

Existem algumas janelas de tempo durante as quais os usuários estão mais propensos a instalar uma atualização lançada pelo fornecedor. Nossos pesquisadores analisaram as instalações de software presentes nos endpoints utilizados por clientes. Constatou-se que o software pode ser dividido em três categorias:

- **Novas versões:** o endpoint executava a versão mais recente do software
- **Versões recentes:** o endpoint executava as três últimas versões do software, mas não a mais recente
- **Versões antigas:** o endpoint executava o software com uma versão anterior às três últimas versões

Veja o exemplo a seguir: se um fornecedor de software lançou a versão 28 no dia 1º de janeiro de 2017, a versão 28 é a mais nova; a versão 26 é a recente e a versão 23 é a antiga. (As figuras na próxima página contêm informações sobre os períodos semanais nos quais uma ou mais versões do software foram lançadas.)

Ao analisar os usuários do Adobe Flash (**Figura 42**), descobrimos que, na primeira semana de uma versão de atualização, quase 80% dos usuários instalaram a versão mais recente do software. Isso quer dizer que o tempo para que os usuários façam a atualização para a versão mais recente é de apenas uma semana. Esse período de "recuperação" de uma semana corresponde à janela de oportunidade durante a qual os hackers podem agir.

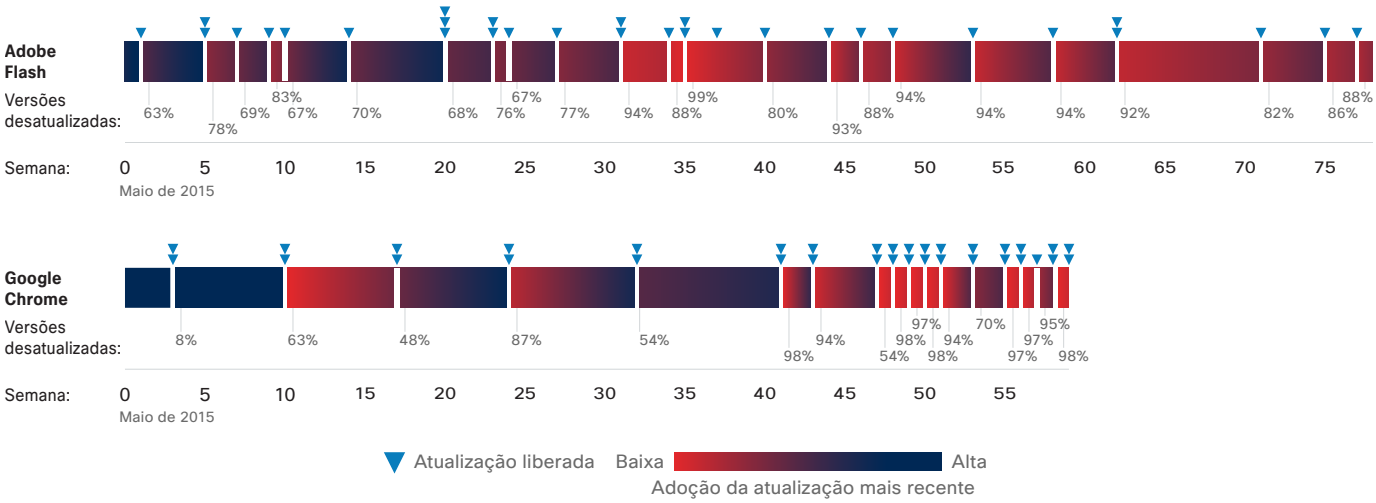
Se analisarmos o final do 4º trimestre de 2015 no gráfico do Adobe Flash, veremos que há uma forte queda no número de usuários que instalaram a versão mais recente da solução. No período examinado, a Adobe lançou cinco versões sucessivas do Flash, que incluíam uma combinação de novas funcionalidades, correções de bugs e atualizações de segurança. Uma enxurrada de atualizações como essa pode confundir os usuários. É possível que eles se questionem sobre a necessidade de baixar tantas atualizações. Além disso, os usuários também podem ficar incomodados com o número de notificações que recebem e podem achar que já baixaram a atualização em questão, ignorando as novas notificações. Qualquer que seja o motivo dessa falta de interesse, é sem dúvida algo ruim para os defensores.

Ao analisarmos as atualizações do navegador da Web Google Chrome, percebemos um outro padrão. Há um ritmo regular de atualizações, bem como uma forte política de cancelamento que torna difícil para os usuários ignorar as notificações de atualização. Como podemos ver na **Figura 42**, os endpoints que executam a versão mais recente permanecem relativamente estáveis ao longo de várias semanas.

Os dados do Chrome mostram que os usuários se recuperam com relativa rapidez. No caso de atualizações regulares, o período de recuperação é de cerca de uma semana. No entanto, em um período de nove semanas, entre o 2º e o 3º trimestre de 2016, houve sete atualizações. Por mais que os usuários tenham se recuperado, podemos ver que há uma certa fadiga: o percentual de usuários que optam por ficar com uma versão mais antiga começa a subir, ainda que a maioria deles esteja no período de recuperação.

O navegador Mozilla Firefox também oferece atualizações regularmente; no entanto, o período de recuperação pode durar até um mês. Isso quer dizer que os usuários do Firefox não baixam as atualizações com a mesma frequência que os usuários do Chrome. Um dos motivos para isso pode ser o fato de que alguns usuários não costumam usar o navegador com frequência e, portanto, não recebem os avisos de atualização (consulte a **Figura 43** na próxima página).

Figura 42 Tempo para correção de falhas no Adobe Flash e no Google Chrome



Fonte: Cisco Security Research

COMPARTILHAR

Descobrimos que o Firefox atualizou as versões a cada duas semanas e que a frequência dessas atualizações aumentou durante o período de observação. O aumento da frequência reflete-se no aumento do uso de versões antigas do Firefox. O tempo de recuperação é de aproximadamente 1,5 semanas; no entanto, os períodos se sobrepõem. Os usuários que tentam seguir as atualizações somam apenas 30% da base de usuários. Em algum momento, dois terços dos usuários estavam executando o navegador com uma versão anterior às quatro últimas versões. Desse modo, por mais que o Firefox consiga corrigir problemas com agilidade, os usuários não estão atualizando e reiniciando o navegador no mesmo ritmo.

Quanto ao software, o nível de uso também parece ser um indicador da vulnerabilidade. Quando não acessam o software com frequência, os usuários não ficam a par da necessidade de fazer o download das correções e atualizações. Isso faz com que o software fique vulnerável a ataques.

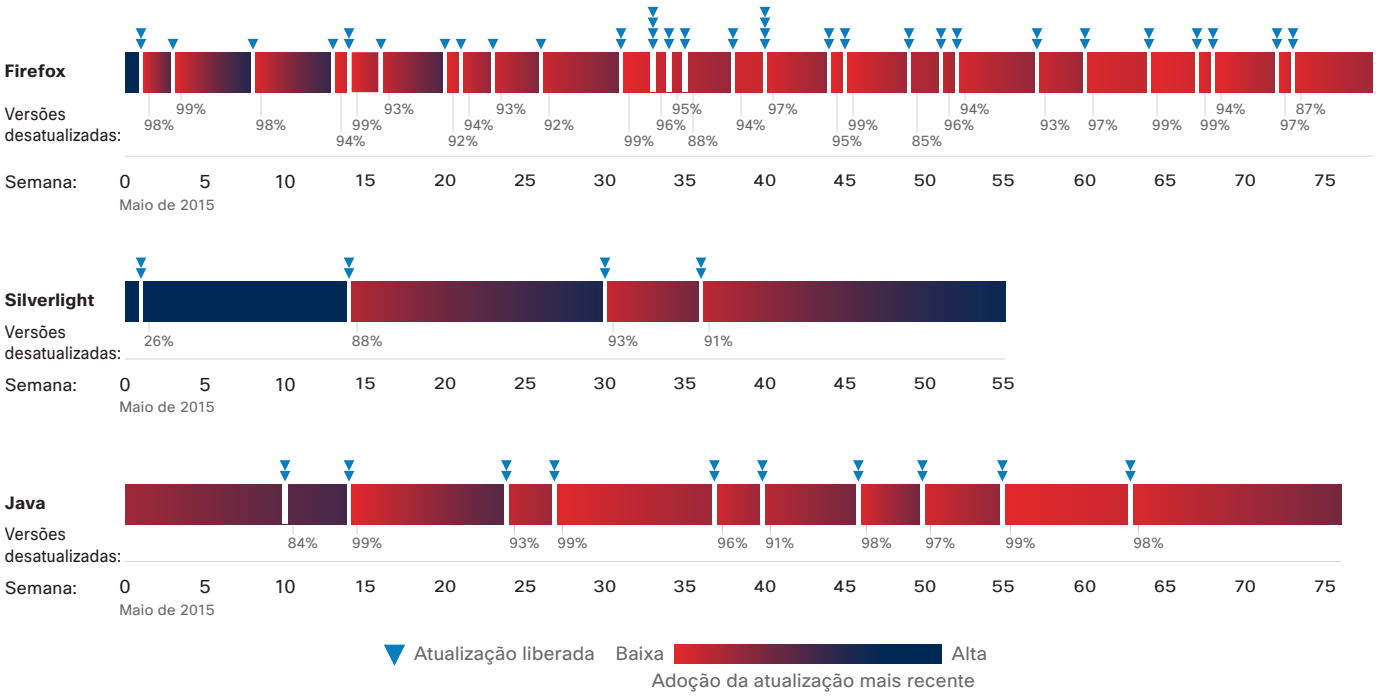
Esse fato fica bastante claro na pesquisa realizada com o Microsoft Silverlight, que mostra um período de recuperação de até dois meses para a instalação de atualizações após o lançamento de uma nova versão. Em determinado momento, o fornecedor lançou duas versões em um período de cinco semanas. Isso afetou os usuários por mais de três meses, como pode ser visto entre o 4º trimestre de 2015 e o 1º trimestre de 2016.

A Microsoft anunciou o fim da vida útil do Silverlight em 2012; no entanto, as correções de bugs e erros ainda estão sendo lançadas. No entanto, uma situação como essa cria o mesmo problema que temos com o Internet Explorer: um software ultrapassado e sem correções torna-se um convite para o ataque de criminosos.

O período de recuperação para usuários do Java mostra que a maioria está executando versões do software de três ou mais lançamentos atrás. E o tempo de recuperação é de 3 semanas. Contudo, o Java tem um padrão quase único, já que a maioria de seus usuários utiliza as versões mais recentes. O ciclo de atualização do Java é de 1 a 2 meses.

A lição que aprendemos sobre os ciclos de tempo até a correção é que os padrões de lançamento de novas versões são um fator essencial para garantir a postura de segurança do usuário, e isso pode colocar as redes em risco.

Figura 43 Tempo para correção de falhas no Firefox, no Silverlight e no Java



Fonte: Cisco Security Research

Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

Estudo comparativo de recursos de segurança da Cisco de 2017

Estudo comparativo de recursos de segurança da Cisco de 2017

Para avaliar a percepção dos profissionais de segurança sobre a situação da segurança em suas empresas, a Cisco perguntou a diretores executivos de segurança (CSOs) e a gerentes de operações de segurança (SecOps) em vários países e em empresas de vários portes sobre as percepções que eles têm dos seus próprios procedimentos e recursos de segurança. O Estudo comparativo de recursos de segurança da Cisco 2017 apresenta informações sobre o nível de maturidade das operações de segurança e das práticas de segurança em uso no momento, além de comparar esses resultados com os dos relatórios de 2015 e 2016. O estudo foi realizado em 13 países com mais de 2.900 participantes.

Os profissionais de segurança desejam tornar suas empresas mais seguras, mas de uma forma que responda ao complexo cenário de invasores e aos esforços dos criminosos para expandir seu espaço operacional. Muitas empresas dependem de diversas soluções de vários fornecedores. Essa tática aumenta a complexidade e a confusão na hora de proteger as redes, pois a Internet continua crescendo em termos de velocidade, dispositivos conectados e tráfego. As empresas precisam mirar na simplicidade e na integração se quiserem se proteger.

Percepções: quanto mais os profissionais de segurança confiam nas ferramentas, menos certeza eles têm de que as estão usando com eficiência

Em geral, os profissionais de segurança acreditam que têm soluções adequadas à disposição e que suas infraestruturas de segurança são modernas. Entretanto, segundo o nosso estudo, essa confiança vem com algum grau de incerteza. Esses profissionais nem sempre estão certos de que podem agrupar orçamentos e capacidade intelectual para aproveitar verdadeiramente a tecnologia que possuem.

As ameaças às empresas vêm de todas as direções. Ágeis e criativos, os criminosos são capazes de superar as defesas. Mesmo nesse ambiente preocupante, a maioria dos profissionais de segurança acredita que a sua infraestrutura de segurança está atualizada, embora aparentemente essa confiança tenha enfraquecido um pouco nos últimos anos. Em 2016, 58% dos entrevistados disseram que sua infraestrutura de segurança é muito moderna e é atualizada constantemente com as últimas tecnologias. Trinta e sete por cento disseram que substituem ou atualizam suas tecnologias de segurança regularmente, mas não estão equipados com as ferramentas mais recentes e eficientes (**Figura 44**).

Figura 44 Porcentagem de profissionais de segurança que consideram que sua infraestrutura de segurança está atualizada

Descrito como as melhores tecnologias disponíveis atualizadas

58%

Descrito como substituído/ atualizado regularmente, mas não equipado com as ferramentas mais recentes e eficientes

37%

2016 (n=2912)

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Além disso, mais de dois terços dos profissionais de segurança consideram suas ferramentas de segurança como muito ou extremamente eficientes. Por exemplo, 74% acreditam que suas ferramentas são muito ou extremamente eficientes em bloquear ameaças à segurança conhecidas, enquanto 71% acreditam que suas ferramentas são eficientes em detectar anomalias de rede e defender de forma proativa contra alterações em ameaças que se adaptam ao ambiente (Figura 45).

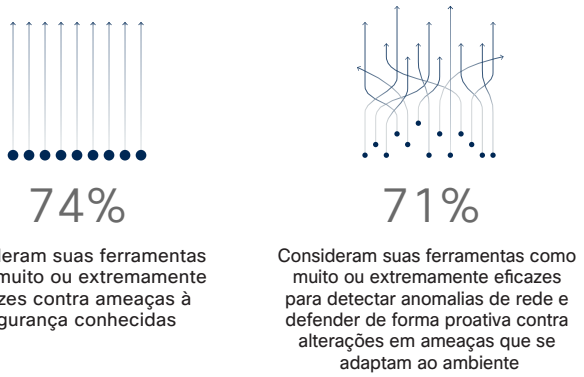
O problema é que a confiança nas ferramentas não necessariamente se traduz em uma segurança eficiente. Como o estudo indica, os departamentos de segurança estão lutando com ferramentas complicadas de vários fornecedores e a falta de talentos internos. Isso resume o problema a "intenção versus realidade". Os profissionais de segurança desejam ferramentas de segurança simples e eficientes, mas não têm a abordagem integrada de que precisam para fazer isso acontecer.

A segurança continua sendo uma prioridade para os níveis superiores de muitas empresas. E os profissionais de segurança acreditam que as equipes executivas mantêm a segurança no topo da lista de principais metas da empresa. O desafio, obviamente, é combinar o suporte executivo com talentos e tecnologias que podem afetar os resultados da segurança.

O número de profissionais de segurança que concordam plenamente que a liderança executiva considera a segurança uma prioridade era de 59% em 2016, pouco abaixo dos 61% de 2015 e dos 63% de 2014 (Figura 46). Em 2016, 55% dos profissionais de segurança concordavam que as funções e as responsabilidades de segurança estão claras dentro da equipe de executivos da empresa. Em 2015 e 2014, 58% concordavam.

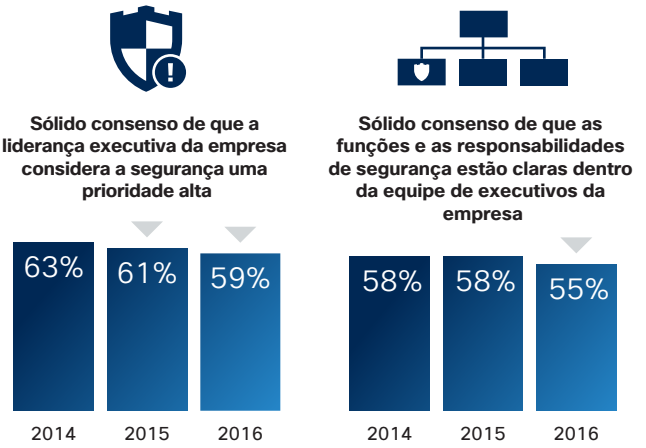
Em resumo, os profissionais de segurança confiam nas ferramentas disponíveis e parecem ser ouvidos pelos líderes na resolução de problemas de segurança. Mas essa confiança está desaparecendo aos poucos. Os profissionais de segurança estão cientes do sucesso dos invasores e do peso de gerenciar a superfície de ataque cada vez mais ampla.

Figura 45 Porcentagem de profissionais de segurança que consideram várias ferramentas de segurança como altamente eficientes



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 46 Porcentagem de profissionais de segurança que acreditam que a segurança é uma prioridade alta para os executivos, 2014-2016



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Restrições: tempo, talento e dinheiro afetam a capacidade de responder a ameaças

Se os profissionais de segurança estão relativamente confiantes de que têm as ferramentas necessárias para detectar ameaças e reduzir danos, eles também reconhecem que algumas restrições estruturais representam um obstáculo no caminho de seus objetivos. Orçamento apertado é um desafio constante. Mas outras restrições à segurança eficaz dizem respeito a como simplificar e automatizar a segurança.

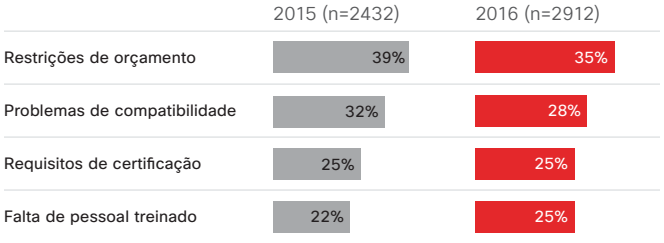
Em 2016, 35% dos profissionais de segurança afirmaram que o orçamento era o maior entrave para adotar tecnologias e processos de segurança avançados (uma leve redução em relação a 2015, quando 39% disseram que o orçamento era o principal obstáculo), como visto na **Figura 47**. Assim como em 2015, os problemas de compatibilidade com sistemas antigos eram o segundo obstáculo mais comum: 28% em 2016 contra 32% em 2015.

Dinheiro é apenas parte do problema. Por exemplo, os problemas de compatibilidade dizem respeito à ausência de integração entre sistemas desconectados. E preocupações relacionadas à falta de pessoal treinado realçam o problema de ter ferramentas, mas não talentos para compreender totalmente o que está acontecendo no ambiente de segurança.

O esforço para encontrar talentos é uma preocupação, considerando a capacidade de tomar decisões e a experiência que são necessárias para combater ataques direcionados e mudar a tática dos adversários. Uma equipe de segurança de TI bem aparelhada, com especialistas e as ferramentas certas, pode fazer a tecnologia e as políticas trabalharem em conjunto e obter melhores resultados de segurança.

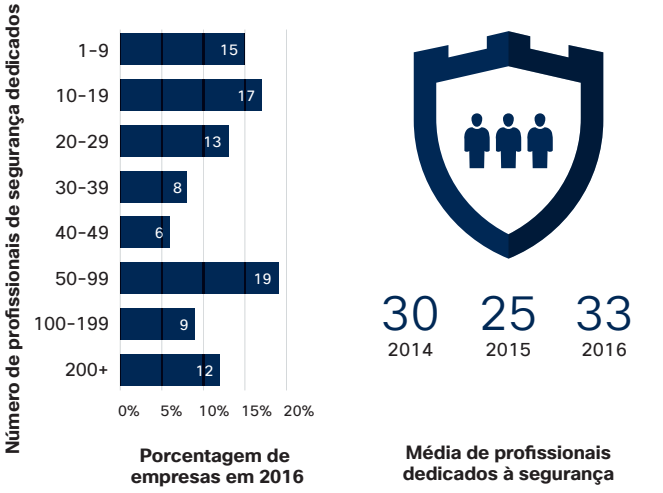
O número médio de profissionais de segurança nas empresas entrevistadas era 33, contra 25 em 2015. Em 2016, 19% das empresas tinham entre 50 e 99 profissionais de segurança exclusivos; 9% tinham de 100 a 199 profissionais de segurança; e 12 tinham 200 ou mais (**Figura 48**).

Figura 47 Os maiores obstáculos à segurança



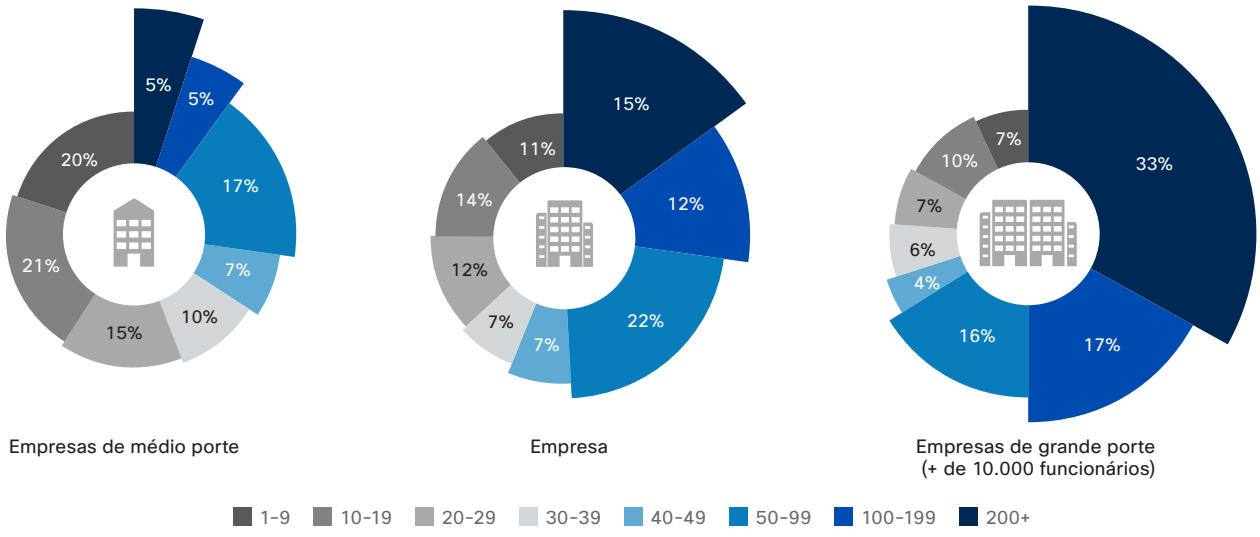
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 48 Número de profissionais de segurança empregados por empresas



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 49 Número de profissionais de segurança por porte de empresa



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

COMPARTILHAR

O número de profissionais de segurança varia de acordo com o porte da empresa. Como mostrado na **Figura 49**, 33% das grandes empresas com mais de 10.000 funcionários tinham pelo menos 200 funcionários de segurança.

Sejam quais forem as restrições, os profissionais de segurança precisam fazer perguntas difíceis sobre as barreiras que limitam a sua capacidade de enfrentar futuras ameaças.

Por exemplo, quando se trata de orçamento, quanto é o suficiente? Como os entrevistados da pesquisa explicaram, as equipes de segurança competem com muitas outras prioridades corporativas, mesmo dentro do próprio departamento de TI. Se não conseguirem garantir fundos para mais ferramentas, o orçamento com que terão de trabalhar ficará mais apertado. Por exemplo, a automação pode ser usada para compensar a limitação de mão de obra.

Perguntas semelhantes devem ser feitas sobre problemas de compatibilidade de hardware e software. À medida que os problemas de compatibilidade aumentam, quantas versões diferentes de software e hardware devem ser gerenciadas, considerando que a maioria pode não estar funcionando com eficiência? E como as equipes de segurança lidarão com os diversos requisitos de certificação necessários?

Terceirização e a nuvem ajudam a esticar o orçamento

Muitos profissionais de segurança que participaram do estudo comparativo achavam que não dispunham de meios financeiros suficientes para fazer aquisições de segurança. Eles esticaram o orçamento terceirizando algumas tarefas ou usando soluções de nuvem. Também contaram com automação.

Além dessas limitações, os profissionais de segurança também estão dando uma ênfase um pouco menor à operacionalização da segurança. Essa tendência pode levantar dúvidas sobre a possibilidade de os profissionais de segurança estarem criando uma infraestrutura de segurança de qualidade inferior. Os sinais de um foco de enfraquecimento na operacionalização podem indicar que as empresas não estão preparadas para se defender em um cenário de ataque mais amplo.

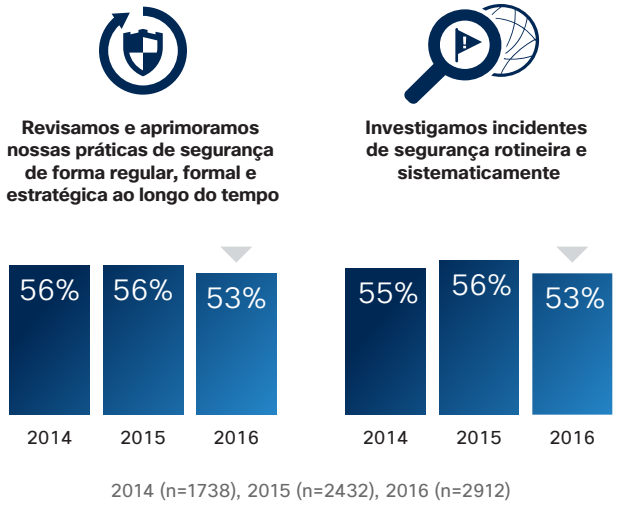
Por exemplo, em 2016, 53% dos entrevistados concordavam plenamente em revisar e aprimorar as práticas de segurança de maneira regular, formal e estratégica. Em 2014 e 2015, 56% concordavam plenamente. Da mesma forma, em 2016, 53% disseram que concordavam plenamente em investigar incidentes de segurança de forma rotineira e sistemática, em comparação com 55% em 2014 e 56% em 2015 (Figura 50).

Se os profissionais de segurança estão "patinando" em suas metas de colocar a segurança em uso, não é uma surpresa que eles não consigam implantar com eficiência as ferramentas que possuem, quanto mais adicionar novas ferramentas. Se, como os entrevistados do estudo nos disseram, eles não são capazes de usar a tecnologia disponível, precisam de ferramentas simplificadas que automatizem os processos de segurança. E essas ferramentas precisam oferecer uma visão holística do que está acontecendo no ambiente de rede.

A falta de integração na segurança pode permitir lacunas de tempo e espaço, que podem ser aproveitadas por agentes mal-intencionados para iniciar ataques. A tendência dos profissionais de segurança de fazer malabarismos com soluções e plataformas de vários fornecedores pode complicar a montagem de uma defesa integrada. Como ilustrado na Figura 51, a maioria das empresas usa mais de cinco fornecedores de segurança e mais de cinco produtos de segurança em seu ambiente. Cinquenta e cinco por cento dos profissionais de segurança usam pelo menos seis fornecedores; 45% usam de um a cinco fornecedores em qualquer lugar; e 65% utilizam seis ou mais produtos.

Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

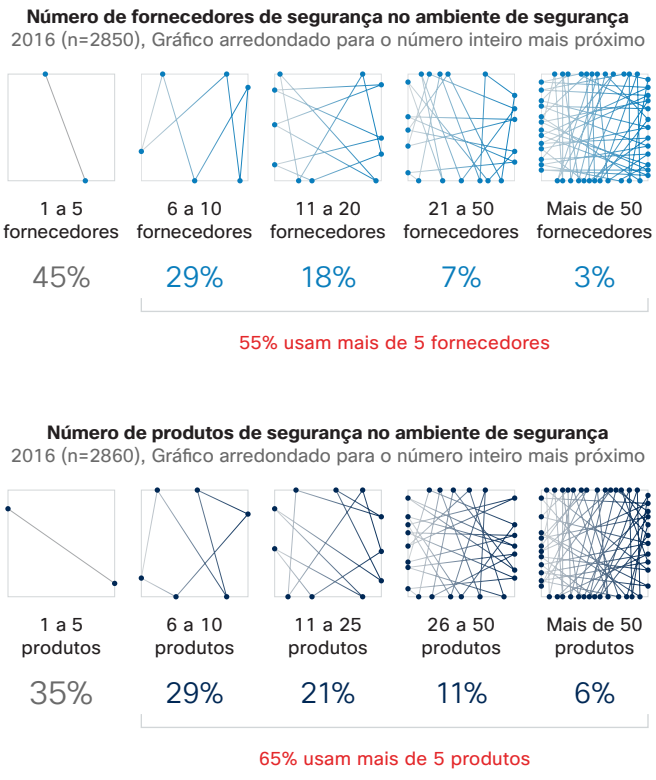
Figura 50 Porcentagem de entrevistados que concordam plenamente com as instruções de operacionalização da segurança



2014 (n=1738), 2015 (n=2432), 2016 (n=2912)

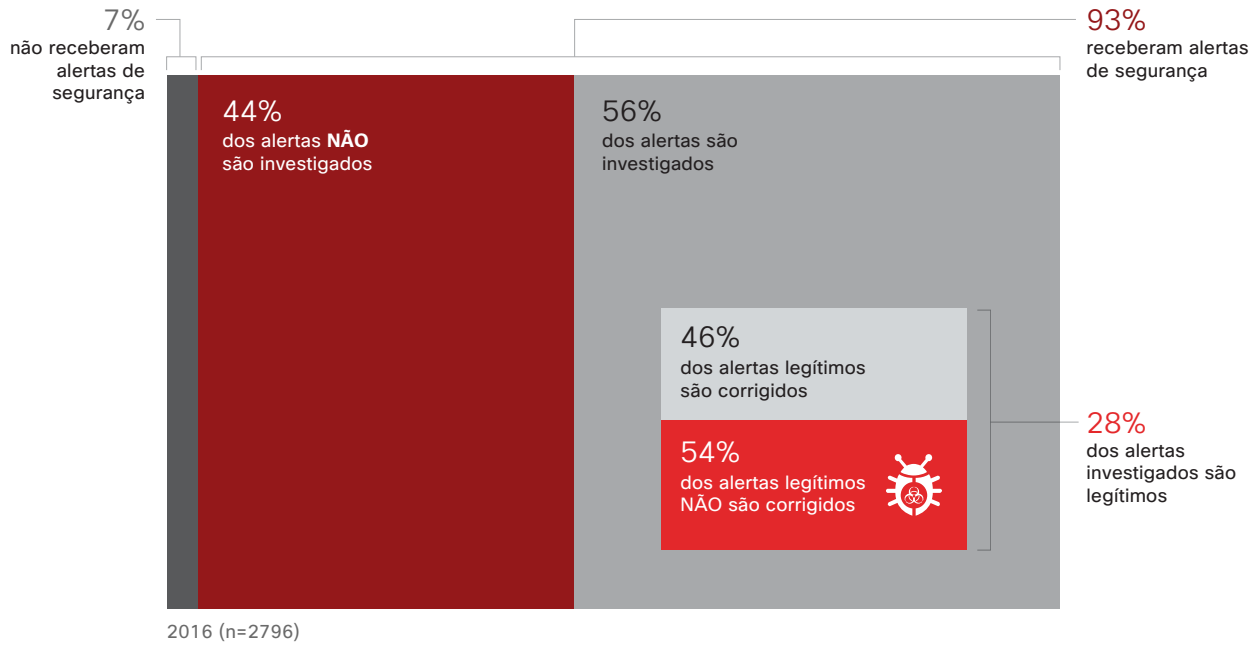
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 51 Número de fornecedores e produtos de segurança usados por empresas



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 52 Porcentagem de alertas de segurança que não são investigados ou corrigidos



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Se as metas de operacionalização estão patinando, as ferramentas não são usadas com o máximo de eficiência e a mão de obra não é competente, o resultado é uma segurança hesitante. Os profissionais de segurança são forçados a ignorar a investigação de alertas simplesmente porque não têm talentos, ferramentas ou soluções automatizadas disponíveis para determinar quais são importantes e porque eles estão ocorrendo.

Devido a vários fatores (como a ausência de um sistema de defesa integrado ou a falta de tempo dos funcionários), as empresas só podem investigar pouco mais da metade dos alertas de segurança que recebem em um determinado dia. Como mostrado na **Figura 52**, 56% dos alertas são investigados e 44% não são investigados; desses alertas que são investigados, 28% são considerados alertas legítimos. Quarenta e seis por cento dos alertas legítimos são corrigidos.

Para colocar o problema em termos mais concretos, se uma empresa registra 5.000 alertas por dia, isso significa que:

- 2.800 alertas (56%) são investigados, enquanto 2.200 (44%) não são
- Desses investigados, 784 alertas (28%) são legítimos, enquanto 2.016 (72%) não são
- Dos alertas legítimos, 360 (46%) são corrigidos, enquanto 424 (54%) não são

O fato de que quase metade dos alertas permanece sem investigação gera preocupação. O que está no grupo de alertas que não são corrigidos: ameaças de baixo nível que podem apenas difundir spam ou a possibilidade de um ataque de ransomware ou de dano à rede? Para investigar e entender uma fatia maior do cenário de ameaças, as empresas precisam confiar na automação e em soluções integradas corretamente. A automação pode ajudar a ampliar recursos preciosos e reduzir os encargos de detecção e investigação da equipe de segurança.

A incapacidade de ver tantos alertas desperta dúvidas sobre o impacto deles no sucesso de uma empresa. De que forma essas ameaças não investigadas podem afetar a produtividade, a satisfação do cliente e a confiança na empresa? Como os entrevistados disseram, até pequenas interrupções da rede ou violações de segurança podem ter efeitos a longo prazo no resultado. Mesmo se as perdas forem relativamente menores e os sistemas afetados forem fáceis de identificar e isolar, os líderes de segurança consideram as violações como significativas devido ao estresse imposto à empresa.

O estresse pode afetar as empresas de várias maneiras. As equipes de segurança acabam tendo que dedicar tempo ao gerenciamento de interrupções da rede que ocorreram após uma violação de segurança. Quase metade dessas interrupções duraram até 8 horas. Quarenta e cinco por cento das interrupções duraram de 1 a 8 horas (Figura 53); 15% duraram de 9 a 16 horas e 11% duraram de 17 a 24 horas. Quarenta e um por cento dessas interrupções afetaram entre 11% e 30% dos sistemas das empresas.

Impacto: Mais empresas sofrem perdas decorrentes de violações

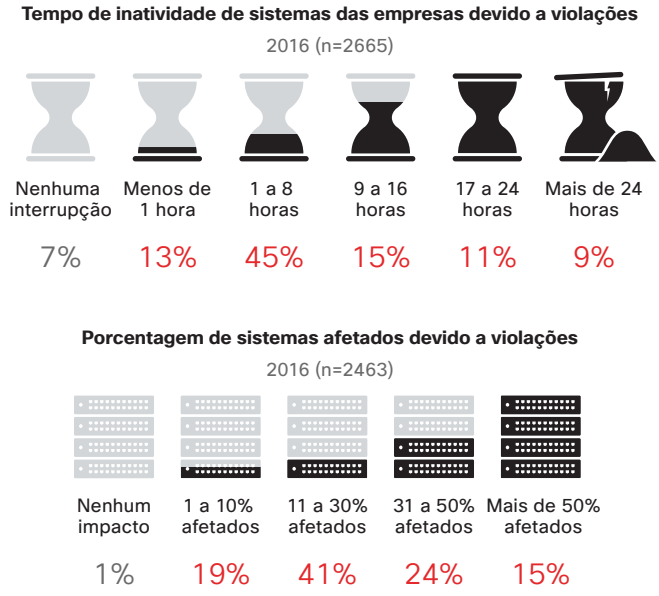
Os efeitos das violações não se limitam a interrupções. As violações também resultam em perda de dinheiro, tempo e reputação. As equipes de segurança que acham que conseguirão se livrar desse problema ignoram a realidade dos dados. Como nosso estudo mostra, quase metade das empresas teve que lidar com as críticas resultantes de uma violação de segurança. Devido à gama de habilidades e táticas dos invasores, a pergunta não é se uma violação de segurança acontecerá, mas sim quando.

Como mostra o estudo comparativo, os profissionais de segurança são sacudidos pela realidade quando as violações ocorrem. Geralmente, eles mudam as estratégias de segurança ou reforçam as defesas. As empresas que ainda não sofreram uma violação em suas redes por invasores podem estar aliviadas de terem escapado. No entanto, essa confiança não se justifica.

Quarenta e nove por cento dos profissionais de segurança entrevistados disseram que a empresa precisou lidar com o escrutínio público resultante de uma violação de segurança. Entre essas empresas, 49% divulgaram a violação voluntariamente, enquanto 31% disseram que a divulgação foi feita por terceiros (Figura 54). Em outras palavras, quase um terço das empresas entrevistadas foram forçadas a lidar com a divulgação involuntária de violações. É claro que os dias em que se podia lidar com violações sem muito alarde ficaram para trás. Há muitos reguladores, mídias e usuários de mídias sociais para expor as notícias.

COMPARTILHAR

Figura 53 Tamanho e alcance das interrupções causadas por violações de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 54 Porcentagem de empresas que passaram por uma violação pública

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 55 Funções que muito provavelmente devem ser afetadas por uma violação pública

Fonte: Cisco Security Research

O dano às empresas vai além do tempo necessário para lidar com uma violação ou uma interrupção. Há enormes repercussões que as empresas devem tentar evitar a todo custo.

Como ilustrado na Figura 55, 36% dos profissionais de segurança disseram que a função de operações provavelmente foi a mais afetada. Isso significa que os principais sistemas de produtividade, que afetam desde o transporte até os serviços de saúde e a produção, podem desacelerar ou até serem paralisados.

Depois de operações, finanças foi provavelmente a função a ser mais afetada (citada por 30% dos entrevistados), seguida por reputação da marca e retenção de clientes (ambos 26%).

Nenhuma empresa que planeje se expandir e atingir o sucesso deseja ter departamentos importantes afetados por violações de segurança. Os profissionais de segurança devem analisar os resultados da pesquisa sob a perspectiva de suas empresas e se perguntar: se a minha empresa sofrer esse tipo de perda decorrente de uma violação, o que acontecerá com ela no futuro?

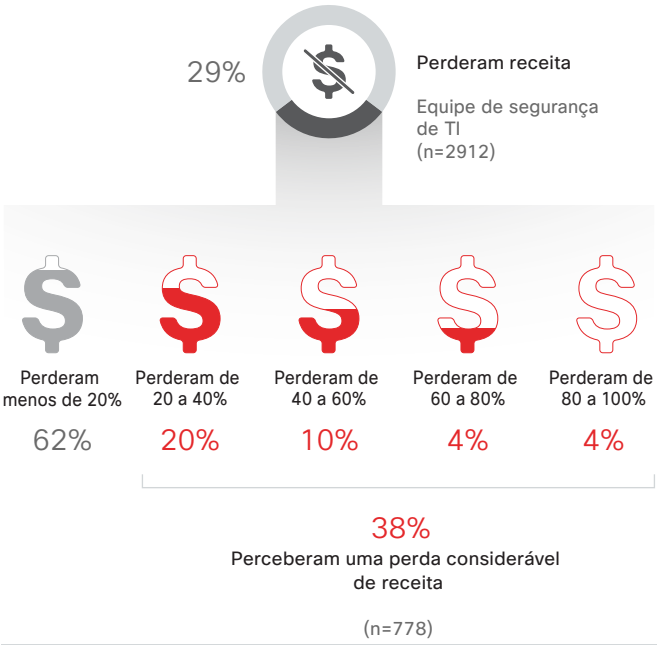
As perdas de oportunidades para as empresas que sofrem ataques on-line são alarmantes. Vinte e três por cento dos profissionais de segurança entrevistados afirmaram que, em 2016, suas empresas perderam oportunidades devido a ataques (**Figura 56**). Desse grupo, 58% disseram que o total de oportunidades perdidas foi inferior a 20%; 25% disseram as oportunidades perdidas ficaram entre 20% e 40%, e 9% afirmaram que o montante de oportunidades perdidas atingiu de 40% a 60%.

Muitas empresas podem quantificar as perdas de receita em decorrência de violações públicas. Como ilustrado na **Figura 57**, 29% dos profissionais de segurança disseram que suas empresas perderam receita como resultado dos ataques. Desse grupo, 38% disseram que a perda de receita foi igual ou superior a 20%.

Outro resultado dos ataques on-line é o menor número de clientes. Como ilustrado na **Figura 58**, 22% das empresas disseram que perderam clientes como resultado dos ataques. Desse grupo, 39% disseram que perderam 20% ou mais clientes.

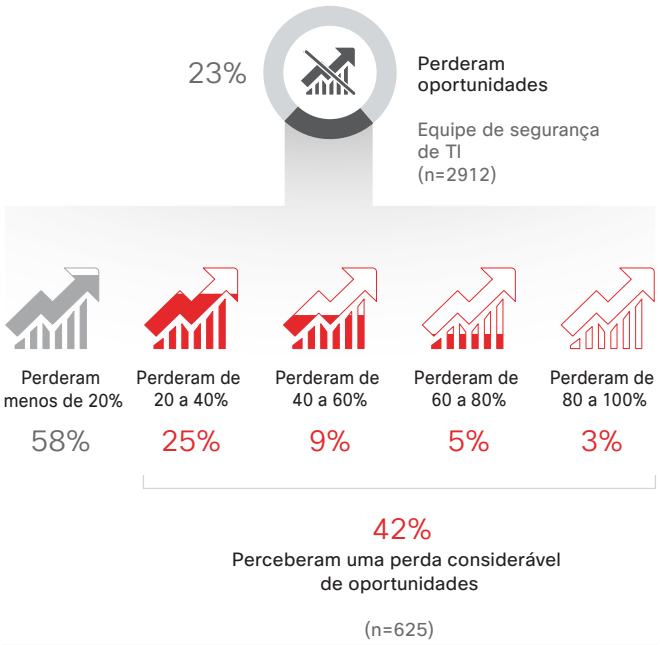
Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

Figura 57 Porcentagem de receitas da empresa perdidas como resultado de um ataque



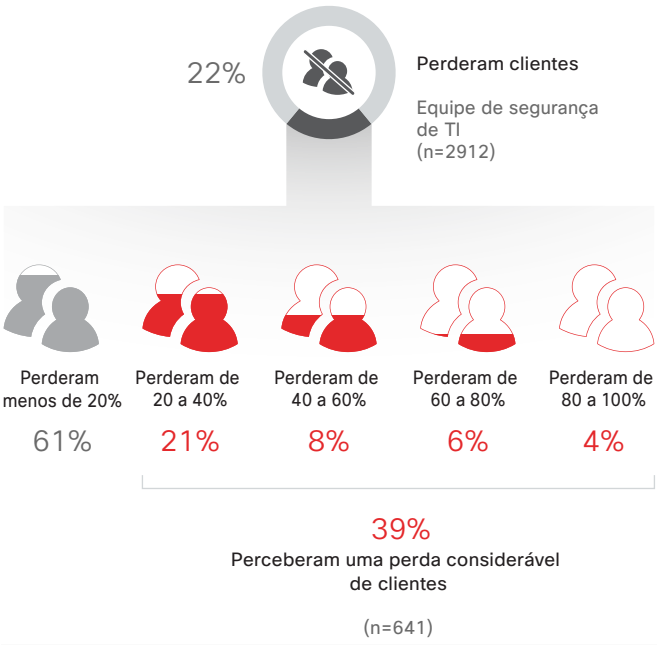
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 56 Porcentagem de oportunidades de negócios perdidas como resultado de um ataque



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 58 Porcentagem de clientes perdidos por empresas devido a ataques



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Resultados – A maior fiscalização terá uma importante função nas melhorias de segurança

Como mostram os resultados da pesquisa, o impacto das violações pode ser duradouro e generalizado. Se pressupomos que uma empresa será afetada por uma violação em algum momento, a pergunta é: o que acontece em seguida? Para onde a administração deve deslocar atenção e recursos a fim de diminuir a probabilidade de violações?

A oportunidade de aprendizado faz parte das consequências de uma violação. É uma experiência que não deve ser desperdiçada em termos de investimento em melhores abordagens.

Noventa por cento dos profissionais de segurança afirmaram que uma violação de segurança melhorou os procedimentos, as políticas e as tecnologias de defesa contra ameaças, como mostrado na **Figura 59**. Dessas empresas afetadas por violações, 38% disseram que responderam separando a equipe de segurança do departamento de TI; 38% afirmaram que aumentaram o treinamento de conscientização de segurança entre os funcionários; e 37% disseram que aumentaram o enfoque na análise e na redução de riscos.

Figura 59 Como as violações de segurança promovem melhorias

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

As empresas reconhecem que precisam exercer a criatividade para ir além das restrições de talentos, orçamentos e compatibilidade de tecnologias. Uma estratégia é adotar serviços terceirizados para reforçar o orçamento e utilizar talentos que podem não ser um recurso interno.

Em 2016, 51% dos profissionais de segurança terceirizaram a consultoria e 45% terceirizaram a resposta a incidentes (**Figura 60**). Cinquenta e dois por cento disseram que terceirizaram os serviços para economizar custos, enquanto 48% disseram ter feito isso para obter insights independentes.

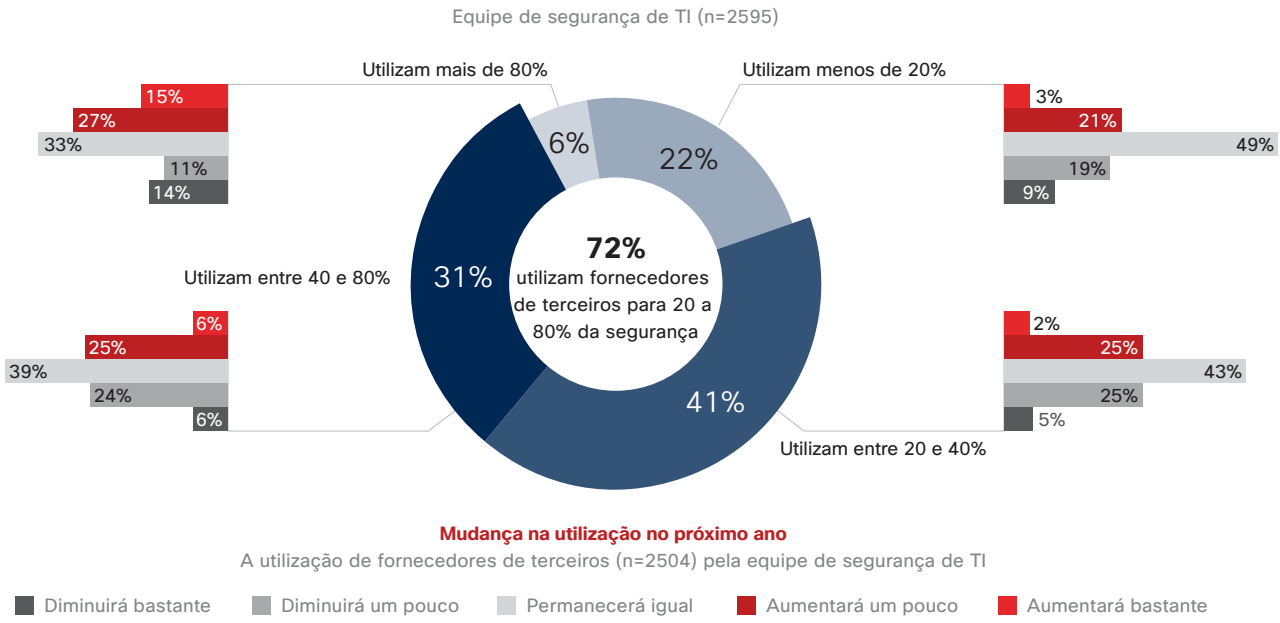
Assim como fazem com a terceirização, as empresas também contam com fornecedores externos para melhorar suas estratégias de defesa. O ecossistema de segurança oferece maneiras de compartilhar a responsabilidade pela segurança.

Setenta e dois profissionais de segurança disseram que contam com fornecedores externos para 20% a 80% de sua segurança, como ilustrado na **Figura 61**. Essas empresas que dependem muito de ajuda externa na segurança provavelmente aumentarão o uso de fornecedores terceirizados no futuro.

Figura 60 A confiança das empresas na terceirização

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 61 Porcentagem de confiança das empresas na terceirização



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

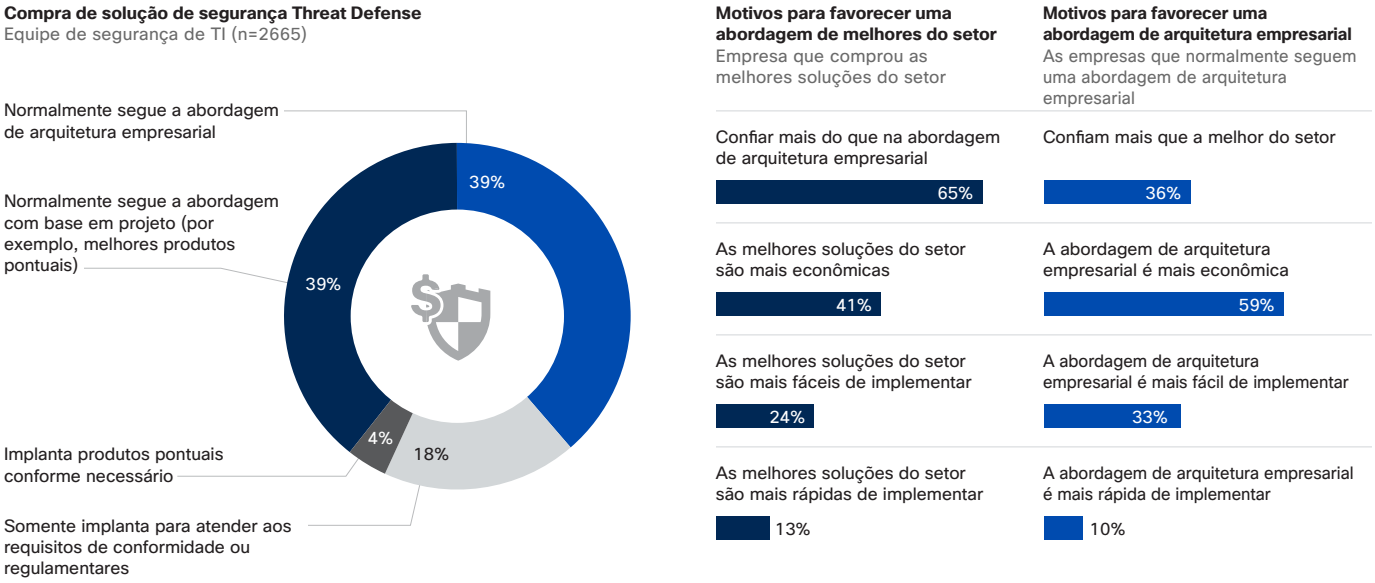
Figura 62 Fontes de maior controle

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

À medida que adotam etapas para reforçar a postura de segurança, as empresas podem esperar que seus esforços recebam mais atenção. Essa fiscalização virá de públicos influentes e, portanto, não poderá ser ignorada. O modo como as preocupações desses públicos serão encaradas pode ter um impacto considerável na capacidade de defesa de uma empresa.

Setenta e quatro por cento dos profissionais de segurança afirmaram que a fiscalização virá dos executivos; 73%, de clientes e consumidores; e 72%, dos funcionários, como ilustrado na Figura 62.

Figura 63 Como a confiança e a economia guiam as decisões de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Confiança versus custo: o que determina as aquisições de segurança?

Os profissionais de segurança querem as melhores soluções possíveis para proteger suas empresas, mas suas percepções diferem sobre como criar um ambiente seguro ideal. Eles compram as melhores soluções de diversos fornecedores porque acham que essas soluções resolverão vários problemas diferentes? Ou utilizam uma arquitetura integrada, pois acreditam que essa abordagem é mais econômica? Embora existam muitos determinantes para investimentos em segurança, um fator que pode beneficiar todas as empresas é a maior simplicidade.

Como ilustrado na Figura 63, os profissionais de segurança parecem divididos entre confiança e custo na hora de escolher entre as melhores soluções do setor ou soluções de arquitetura. Sessenta e cinco por cento disseram que preferem as melhores soluções do setor porque confiam mais nelas do que em uma abordagem de arquitetura empresarial. Por outro lado, 59% disseram que preferem uma abordagem de arquitetura porque acreditam que é mais econômica.

Este não é um dilema do tipo "uma coisa ou outra". As empresas precisam das melhores soluções de segurança integrada do setor. As duas abordagens oferecem benefícios e simplificam a segurança ao oferecer ferramentas de resposta automática (Figura 63).

Combinando as melhores soluções da categoria com uma abordagem integrada, as equipes de segurança podem adotar uma estratégia de segurança menos complexa e mais eficiente. A abordagem integrada ajuda os profissionais de segurança a entenderem o que está acontecendo em cada fase da defesa. Essa abordagem reduz o espaço operacional dos invasores. Ela é simples, permitindo que as equipes implantem soluções em escala. Ela é aberta, gerando as melhores soluções do setor conforme necessário. E é automatizada, para oferecer detecção mais rápida.

Resumo – O que o estudo comparativo revela

Há uma grande diferença entre amontoar ferramentas de segurança e saber usá-las para reduzir riscos e fechar o espaço operacional dos criminosos. Os entrevistados no estudo comparativo acreditam que têm ferramentas capazes de deter os invasores. Mas também reconhecem que restrições, como a falta de mão de obra e a compatibilidade inadequada entre produtos, podem diminuir a eficiência de boas ferramentas mais do que o esperado.

As preocupantes descobertas sobre o impacto das violações devem fornecer aos profissionais de segurança provas mais do que evidentes da necessidade de melhorar processos e protocolos. Diante de efeitos reais e imediatos como perda de receita e de clientes, as empresas não podem simplesmente querer distância de lacunas na proteção de segurança, pois a pergunta não é se acontecerá uma violação, mas sim quando.

Uma conclusão do estudo comparativo é que as restrições que limitam a segurança ágil e eficaz sempre estarão presentes: nunca haverá disponibilidade suficiente de orçamento e talentos na mesma medida que os profissionais de segurança acreditam que precisam. Se aceitarmos essas restrições, a ideia de simplificar a segurança e implantar soluções automatizadas passa a fazer sentido.

A simplificação da segurança também utiliza as melhores soluções da categoria e uma arquitetura integrada. As empresas precisam dos benefícios das duas abordagens.

Setor

Setor

Segurança da cadeia de valor – O sucesso em um mundo digital depende da redução do risco de terceiros

A segurança da cadeia de valor é um elemento essencial de sucesso em uma economia conectada. É fundamental garantir que a segurança adequada esteja no lugar certo e no momento oportuno ao longo de toda a cadeia de valor, ou seja, o ciclo de vida completo de hardware, software e serviços.

As oito fases da cadeia de valor são mostradas na Figura 64.

A tecnologia da informação e a tecnologia operacional estão convergindo neste mundo digitalizado. Não basta que as empresas se concentrem em somente proteger sua infraestrutura, suas ofertas e seus modelos de negócios internos. As empresas devem analisar a cadeia de valor de forma holística e ver se cada um dos terceiros envolvidos no modelo de negócios delas ou que façam menção às suas ofertas representam um risco à segurança.

A resposta mais simples é que a pesquisa do Sans Institute constatou que 80% das violações de dados são originadas de terceiros.[15] Para reduzir os riscos, as empresas devem promover uma cadeia de valor em que a segurança não esteja implícita e a segurança seja responsabilidade de todos. Como etapa fundamental para alcançar esse objetivo, as empresas devem:

- Identificar os principais participantes do ecossistema de terceiros e entender o que eles oferecem
- Desenvolver uma arquitetura de segurança flexível que possa ser compartilhada e implantada por terceiros nesse ecossistema
- Avaliar se esses terceiros estão operando dentro dos níveis de tolerância definidos pela arquitetura de segurança da empresa
- Ficar alerta quanto a novos riscos à segurança que o ecossistema pode apresentar com o aumento da digitalização

As empresas também devem considerar a segurança antes de apresentar um novo modelo de negócios ou uma oferta que exija envolvimento ou o que de outra forma afete o ecossistema de terceiros. Todo ganho de produtividade ou resultado em potencial deve ser avaliado levando em conta possíveis riscos, particularmente aqueles relativos a segurança de dados e privacidade.

Há uma maior percepção quanto à importância da cadeia de valor, tanto globalmente quanto em segmentos específicos do setor. Em recente lei norte-americana sobre aquisição de TI, determinou-se uma avaliação de um ano, realizada pelo Departamento de Defesa dos EUA, sobre padrões de tecnologia aberta em aquisições relacionadas a tecnologia da informação e segurança digital[16]. No setor altamente convergente da energia, a North-American Electric Reliability Corporation (NERC) está desenvolvendo de forma ativa novas exigências que abordam sua cadeia de valores digitais[17].

Figura 64 As etapas da cadeia de valor

Fonte: Cisco

COMPARTILHAR

[15] *Combatting Cyber Risks in the Supply Chain,* SANS Institute, 2015: https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.
[16] Lei pública 114-92 §
[17] O NERC solicitou que fosse empreendida esta iniciativa por parte da Comissão Federal de Regulamentação de Energia dos EUA (CFR 18, Parte 40) [Lista de sentenças nº RM15-14-002; Pedido nº 829].

As empresas, em conjunto com seus terceiros, devem responder a certas perguntas: "Como e por quem os dados serão gerados?" e "Os dados devem ser extraídos digitalmente?" Para se obter mais clareza, é preciso questionar "A quem pertence os recursos digitais que estamos coletando ou criando?" e "Com quem estamos dividindo essas informações?". Outra pergunta fundamental a ser respondida é "De quem é a responsabilidade e a obrigação quando ocorre uma violação?".

Essa abordagem centrada na cadeia de valor ajuda a assegurar que as considerações sobre segurança façam parte de cada estágio do ciclo de vida das soluções. A arquitetura certa, combinada à adesão aos padrões de segurança apropriados, ajudará a promover segurança difundida e confiança por toda a cadeia de valor.

Atualização geopolítica: Criptografia, confiança e um apelo à transparência

Em relatórios de segurança digital anteriores, os especialistas em geopolítica da Cisco examinaram a incerteza no cenário da administração da Internet, os direitos individuais em comparação aos direitos do Estado e as formas como governos e empresas privadas lidam com o dilema da proteção de dados. Um tema comum nessas discussões foi a criptografia. Acreditamos que a criptografia continuará a permear, e talvez dominar, o debate sobre segurança digital no futuro próximo.

A proliferação de leis nacionais e regionais sobre privacidade de dados gerou apreensão entre fornecedores e usuários ao tentarem se adequar à legislação. Nesse ambiente de incertezas, questões como soberania e localização de dados tornaram-se importantes, colaborando para impulsionar o crescimento da computação em nuvem e do armazenamento localizado de dados à medida que as empresas buscam soluções criativas para atender a regulamentações de privacidade complexas e em constante evolução[18].

Ao mesmo tempo, o aumento no número de violações de dados e ameaças avançadas persistentes, além da publicidade em torno de ataques patrocinados por países (inclusive aqueles feitos durante eventos de grande visibilidade, como as eleições presidenciais norte-americanas) fazem com que os usuários tenham menos confiança na real proteção de sua privacidade e dados confidenciais.

Os governos da era pós-Snowden vêm manifestando cada vez mais abertamente seu desejo de regular as comunicações digitais e de acessar dados quando julgarem necessário. Entretanto, os usuários têm se mostrado igualmente enfáticos em sua demanda por privacidade. Eventos como o recente conflito entre a Apple e o FBI acerca de um iPhone pertencente a um terrorista não colaboram para atenuar as preocupações dos usuários quanto à privacidade. Esses eventos serviram para ensinar uma geração de usuários digitais, especialmente nos Estados Unidos, sobre criptografia de ponta a ponta. Agora, muitos usuários exigem esse tipo de tecnologia dos provedores de tecnologia e desejam, também, ter acesso às chaves de criptografia.

Isso marca uma mudança fundamental no cenário de segurança digital como o conhecemos. As empresas precisarão planejar seus ambientes de modo que possam administrar e responder aos concorrentes.

Enquanto essa mudança está acontecendo, mais governos estão se dando o direito legal, em muitos casos de forma abrangente, de contornar ou violar medidas de proteção técnicas ou criptográficas. Com frequência, isso se dá sem que o fabricante, o provedor de comunicação ou o usuário tome conhecimento. Essas decisões vêm causando tensões não somente entre autoridades e empresas de tecnologia, mas também entre governos, que, em muitos casos, não desejam que os dados de seus cidadãos sejam acessados por autoridades de outros países. Muitos governos coletam informações sobre vulnerabilidades e exploits de dia zero descobertos em software de fornecedores. Nem sempre, contudo, eles compartilham essas informações com os fornecedores em tempo hábil ou são transparentes acerca das informações que possuem.

Reter essas informações valiosas impede que os fornecedores melhorem a segurança de seus produtos e ofereçam aos usuários uma proteção melhor contra ameaças. Embora os governos possam ter uma boa razão para manter algumas dessas informações para si, há também a necessidade de maior transparência e confiança no cenário global de segurança digital. Com isso em mente, as autoridades governamentais deveriam conduzir uma avaliação franca de suas políticas atuais acerca do armazenamento de exploits de dia zero. O primeiro passo seria assumir o posicionamento padrão de que dividir informações com os fornecedores só pode resultar em um ambiente digital muito mais seguro para todos.

[18] Para obter mais informações sobre este tópico, consulte " Data Localization Takes Off as Regulation Uncertainty Continues", de Stephen Dockery, 6 de junho de 2016, *The Wall Street Journal*: http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

Criptografia de alta velocidade: uma solução escalável para proteção de dados em trânsito

Conforme explicado na seção geopolítica da página 65, a criptografia completa continuará sendo assunto de muito debate e consternação entre os governos e o setor no futuro próximo. Independentemente da tensão resultante desse problema, está aumentando a demanda de usuários por criptografia de dados completa com chaves guardadas pelo cliente.

Os especialistas geopolíticos da Cisco antecipam que alguns fluxos e pools de dados provavelmente permanecerão criptografados com chaves gerenciadas pelo fornecedor pelo menos a curto prazo, principalmente em modelos de negócios orientados para anúncios. Em outros lugares, entretanto, devemos ver o uso da criptografia completa com chaves guardadas pelo cliente ganhar força, na ausência de documentação legal em contrário.

Enquanto isso, procure empresas que busquem mais controle sobre a proteção de dados em trânsito, principalmente durante a transferência em alta velocidade de um data center para outro. Essa costumava ser uma tarefa árdua para as empresas devido às limitações das tecnologias antigas e ao impacto no desempenho da rede. No entanto, novas abordagens estão simplificando esse processo.

Uma solução é a segurança da camada de aplicação, em que os aplicativos são modificados para criptografar dados. Dependendo do número de aplicativos que a empresa utiliza, a implantação desse tipo de segurança pode exigir alto consumo de recursos e ter implementação complexa e operação cara.

Outra abordagem que vem ganhando força são os recursos de criptografia integrados a uma rede ou a um serviço em nuvem para proteger dados em trânsito. É uma evolução do tradicional modelo de gateway VPN, uma solução que atende à natureza dinâmica das redes e às taxas de transmissão de alta velocidade do tráfego de data center. As empresas estão usando a eficiência dos custos operacionais proporcionada pelos novos recursos para proteger os dados recebidos de qualquer aplicativo nesse ambiente enquanto eles trafegam em alta velocidade para outro local.

No entanto, a criptografia na rede é apenas uma ferramenta para proteger dados. Para garantir que estão fazendo o suficiente para proteger os dados armazenados ou em trânsito, as empresas devem encarar o desafio de forma holística. Um bom ponto de partida é fazer aos fornecedores de tecnologia perguntas básicas, mas importantes, como:

- De que forma os dados são protegidos quando estão em trânsito?
- Como eles são protegidos quando estão armazenados?
- Quem tem acesso aos dados?
- Onde os dados são armazenados?
- Qual é a política de exclusão de dados e quando eles devem ser excluídos, se for o caso?

Além disso, essas perguntas são apenas o início de um diálogo mais amplo sobre a proteção de dados que deve evoluir para uma discussão de tópicos como disponibilidade e resiliência de dados.

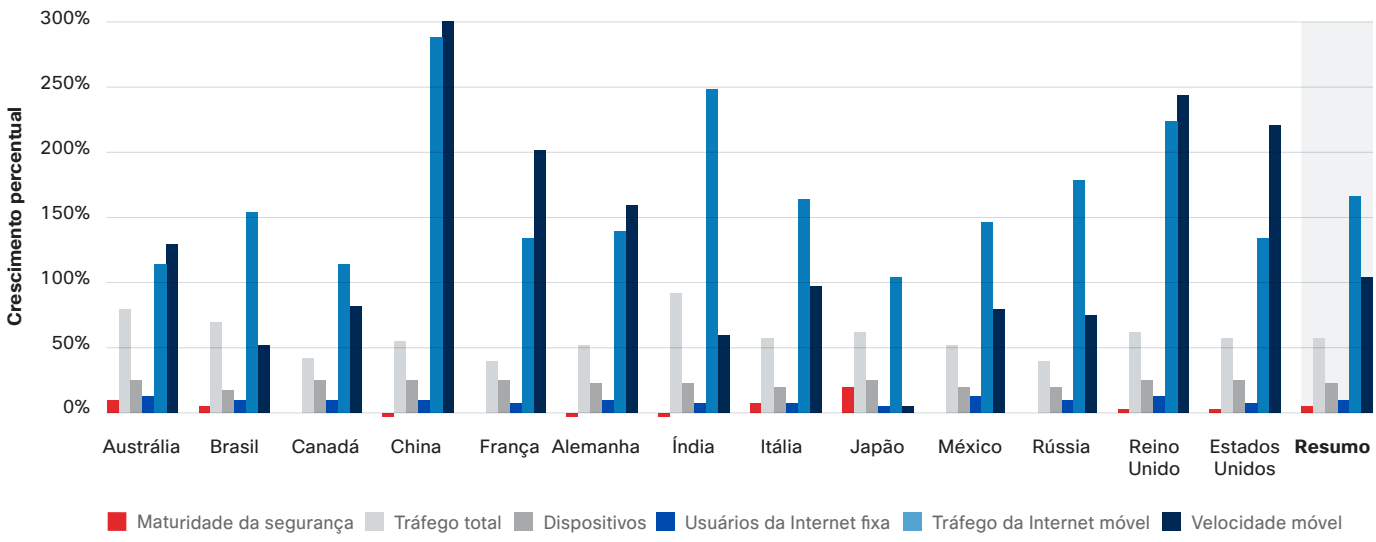
Adoção e desempenho da rede em comparação à maturidade da segurança: Velocidades on-line, tráfego e prevenção não estão crescendo no mesmo ritmo

Os defensores querem estar à frente dos invasores. Ficar para trás significa estar potencialmente em risco. A preocupação é de que os defensores não consigam melhorar sua postura de segurança na mesma velocidade em que os criminosos ganham espaço e tempo para agir. Dado o crescimento mundial do tráfego de Internet fixa e móvel, os defensores são obrigados a acompanhar o ritmo com o amadurecimento de sua infraestrutura de segurança.

Todos os anos, a previsão da Cisco VNI examina o tráfego de IP global, inclusive tráfego móvel e de Wi-Fi. As previsões apresentam projeções de 5 anos para tráfego de IP, o número de usuários de Internet e o número de conexões de dispositivos pessoais e máquina a máquina (M2M) que serão comportados por redes IP. (Acesse esta página para obter mais detalhes sobre as previsões da VNI.) Por exemplo, a previsão estima que até 2020 os smartphones vão gerar 30% do tráfego total de IP.

A Cisco comparou a previsão da VNI com dados sobre a maturidade das defesas, retirados do Security Capabilities Benchmark Study anual da Cisco (consulte a página 49). Ao examinar as taxas de crescimento de maturidade nos relatórios de 2015, 2016 e 2017, como exposto na **Figura 65**, a maturação da segurança está abaixo do esperado em comparação com o crescimento do tráfego da Internet. Alguns países, como China e Alemanha, mostram uma leve queda de maturidade durante esse período. As velocidades da banda larga, em especial, estão melhorando e crescendo a um ritmo bem mais acelerado do que outras variáveis de rede mostradas na **Figura 65**. Velocidades maiores e mais dispositivos conectados propiciam um maior crescimento do tráfego, mas as empresas estão enfrentando dificuldades para reforçar suas medidas e infraestruturas de segurança em um ritmo semelhante.

Figura 65 Maturidade de segurança e taxas de crescimento



Fonte: Cisco Security Research, Cisco VNI e Estudo comparativo de recursos de segurança da Cisco de 2017

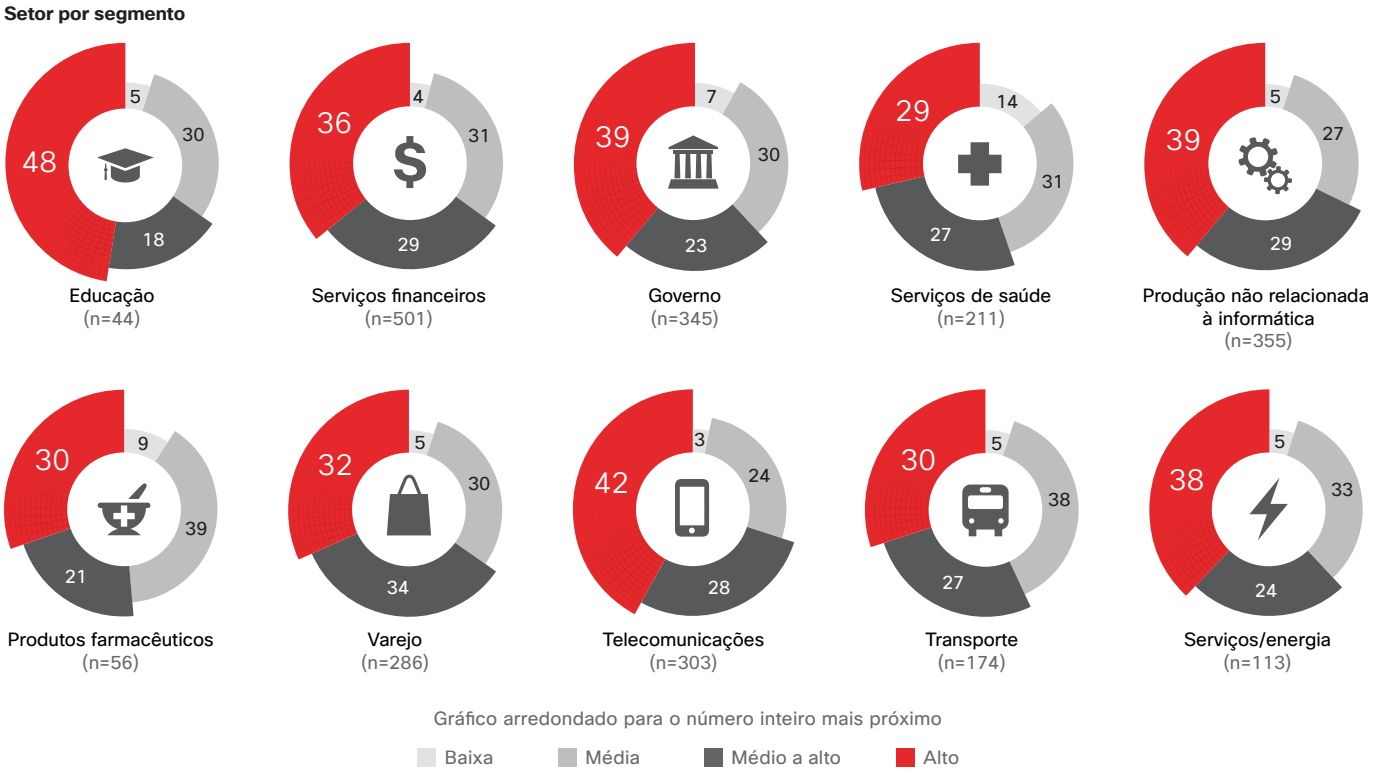
COMPARTILHAR

Certos setores também apresentam um atraso em termos de maturidade da segurança em comparação com outros setores, como mostra a **Figura 66**. Os mercados de produtos farmacêutico, serviços de saúde e transporte, em especial, apresentam mais atrasos do que outros.

É importante observar que o grande crescimento das velocidades móveis é resultado da ampla adoção de redes 4G e LTE por operadoras de telecomunicações. Quando implantações em larga escala de redes 5G estiverem disponíveis ao fim desta década, espera-se que as velocidades móveis sejam comparáveis às velocidades da rede fixa. Segundo o relatório mais recente sobre dados móveis da VNI, a previsão é de que o tráfego mundial de dados móveis deve ganhar uma porção maior do tráfego total de IP quando o 5G for amplamente adotado. O tráfego global de dados móveis correspondeu a 5% do tráfego total de IP em 2015, de acordo com a previsão da VNI. A projeção é de que chegue a 16% até 2020.

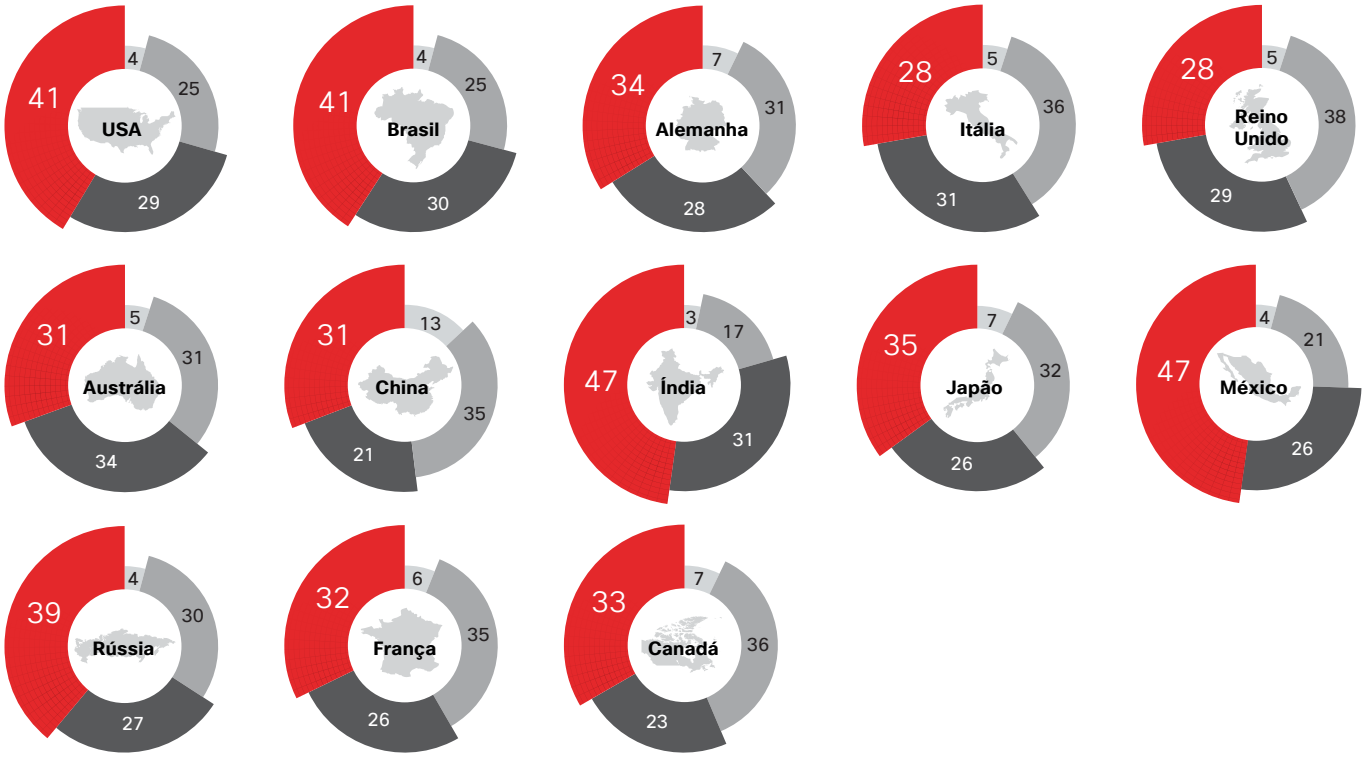
É evidente que as empresas de segurança devem intensificar, e rápido, seus esforços em prol da maturidade, se desejarem acompanhar o crescimento do tráfego da Internet, que traz consigo o crescimento da superfície de possíveis ataques. Além disso, as empresas devem responder ao aumento do uso de endpoints móveis e sem fio em redes corporativas. Precisam também comportar um uso mais amplo de dispositivos pessoais que possibilitem o acesso a dados corporativos por parte dos funcionários.

Figura 66 Maturidade de segurança em mercados verticais



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 67 Maturidade de segurança por país



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Velocidades mais rápidas não são o único fator que vêm impulsionando o crescimento do tráfego da Internet. A Internet das Coisas (IoT) está aumentando o número de dispositivos conectados à Internet, o que contribui para o aumento do tráfego e abre o caminho para invasores.

Para obter mais informações sobre as previsões da Cisco VNI, acesse o site da site da Cisco ou leia a publicação no blog da Cisco sobre a previsão anual da VNI para os anos de 2015 a 2020.

Conclusão

Conclusão

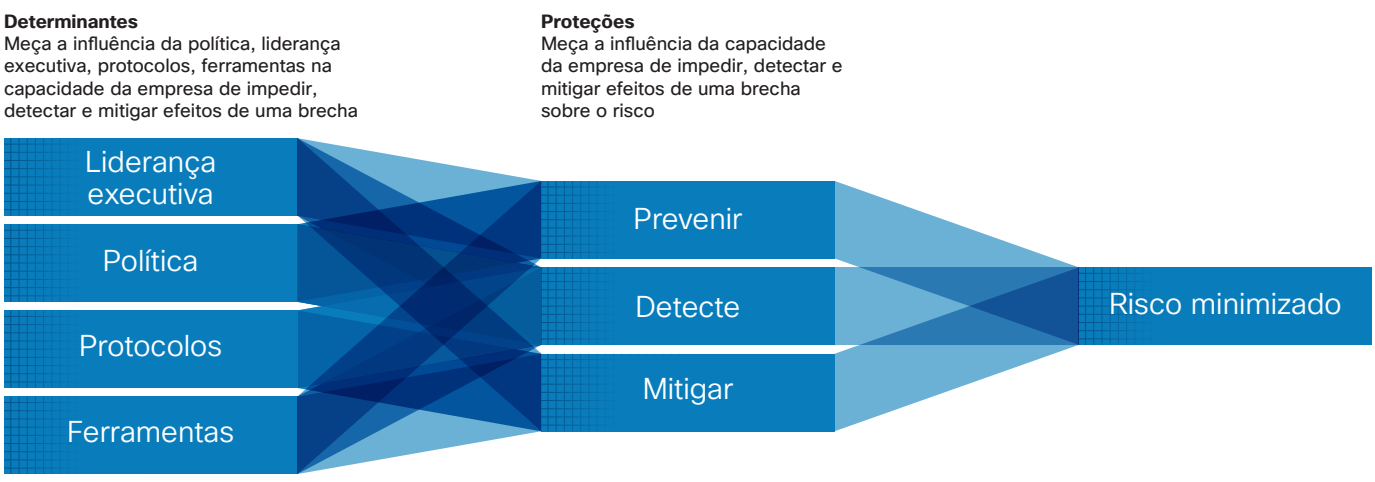
Uma superfície de ataque em rápida expansão requer uma abordagem interconectada e integrada da segurança

Ao analisar dados do Security Capabilities Benchmark Study da Cisco (consulte a página 49), podemos identificar padrões e decisões que ajudam as empresas a minimizarem os riscos. Podemos, então, detectar onde devem ser feitos investimentos em segurança de forma a gerar uma diferença considerável em relação à exposição a riscos. Mensuramos os riscos ao analisar a dimensão das violações, bem como o percentual das interrupções no sistema (consulte a Figura 53 na página 55, acerca da dimensão das violações e os sistemas afetados).

Para compreender como as empresas criam proteções eficientes contra riscos, é preciso identificar os determinantes que afetam a capacidade de prevenir, detectar e minimizar riscos (consulte a Figura 68). Os determinantes devem compreender os seguintes elementos:

- **Liderança executiva:** os líderes devem priorizar a segurança. Isso é fundamental para a redução e a prevenção de ataques. A equipe executiva deve ter métricas claras e estabelecidas para avaliar a eficiência de um programa de segurança.
- **Política:** está estreitamente ligada à redução de invasões. Controlar os direitos de acesso a redes, sistemas, aplicativos, funções e dados influencia a capacidade de reduzir danos resultantes de violações de segurança. Além disso, políticas que garantem a constante revisão das práticas de segurança ajudam a prevenir ataques.
- **Protocolos:** os protocolos corretos podem ajudar a evitar e detectar violações, além de ter forte relação com a redução de invasões. Avaliações regulares das atividades de conexão em redes, para garantir que as medidas de segurança estejam funcionando, em especial, são cruciais tanto para a prevenção quanto para a redução das ameaças. Também é útil revisar e aperfeiçoar as práticas de segurança de modo regular, formal e estratégico ao longo do tempo.
- **Ferramentas:** a aplicação criteriosa e adequada de ferramentas está fortemente ligada à redução de riscos. Com o acesso às ferramentas certas, os usuários podem analisar e fornecer feedback fundamental para a detecção, prevenção e redução de ameaças.

Figura 68 Determinantes e proteções para minimizar riscos



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Baixe os gráficos de 2017 em: **www.cisco.com/go/acr2017graphics**

As disposições de segurança usadas pelas empresas (prevenção, detecção e redução) podem ser vistas como medidas de influência quanto à capacidade de minimizar riscos por parte de uma empresa (consulte a Figura 68).

Essas proteções devem incluir os seguintes elementos:

- **Prevenção:** para minimizar o impacto das violações de segurança, os funcionários devem relatar falhas e problemas de segurança. Também é fundamental que procedimentos e processos de segurança estejam claros e bem assimilados.
- **Detecção:** os melhores métodos de detecção para reduzir o impacto das violações são aqueles que permitem às empresas identificar pontos fracos na segurança antes que se tornem incidentes graves. Para isso, é essencial ter um bom sistema para classificar informações relativas a incidentes.
- **Redução:** processos e procedimentos bem documentados de monitoramento e resposta a incidentes são fundamentais para reduzir com eficiência as violações. As empresas também precisam ter protocolos sólidos para gerenciar respostas a crises.

Todos esses determinantes e medidas de proteção são interconectados e interdependentes. Os profissionais de segurança não podem se limitar a alguns determinantes ou medidas de proteção e acreditar que estes são suficientes para resolver o problema da segurança. É necessário garantir toda a segurança possível, aplicando cada determinante e medida de segurança. As equipes de segurança devem identificar seus pontos fracos, como níveis insatisfatórios de suporte de líderes ou falta de ferramentas para reduzir violações, além de calcular onde devem ser feitos os investimentos de segurança.

O objetivo principal: reduzir o espaço operacional dos invasores

Reduzir (de preferência, eliminar) o espaço operacional irrestrito dos criminosos e identificar a presença de ataques devem ser a prioridade máxima dos defensores. A realidade é que não se pode deter todos os ataques ou proteger tudo que pode e deve ser protegido. Contudo, se as iniciativas se concentrarem em eliminar o espaço operacional necessário para que os ataques dos criminosos digitais sejam eficientes e lucrativos, você pode evitar que os invasores acessem sistemas e dados essenciais sem que sejam detectados.

Este relatório organizou em categorias as diferentes abordagens utilizadas por invasores para comprometer e atacar usuários e sistemas. Utilizamos como base para criar as categorias (reconhecimento, agressão, fornecimento e instalação) o ponto da cadeia de ataque em que os ataques são normalmente lançados. Esse exercício pretende ilustrar quando, como e onde os criminosos lançam mão das vulnerabilidades e de outros pontos fracos para acessar um dispositivo ou sistema, iniciar suas campanhas e obter os resultados que desejam.

Sugerimos que os defensores adotem abordagens de segurança que possibilitem permanecer à frente dos processos básicos dos criminosos. Por exemplo, para impedir o sucesso dos invasores durante a fase de reconhecimento, as equipes de segurança devem:

- Coletar informações sobre as ameaças e vulnerabilidades mais recentes
- Garantir o controle do acesso às redes
- Limitar a exposição da empresa em uma superfície de ataque em expansão
- Gerenciar as configurações
- Desenvolver práticas e procedimentos de resposta coerentes que tomem este documento por base

Quando ameaças agressivas são disseminadas, os defensores devem aplicar todas as ferramentas em seu arsenal para evitar que elas se espalhem e se intensifiquem. É aí que uma arquitetura de segurança integrada passa a ser crucial. Ela oferece informações em tempo real sobre ameaças, bem como detecção e defesa automatizadas, que são essenciais para melhorar os mecanismos de detecção.

Na fase de instalação, as equipes de segurança devem manter-se informadas sobre a condição do ambiente enquanto respondem e investigam o comprometimento. Se esse ambiente for simples, aberto e automatizado, e se os defensores seguiram as demais etapas descritas acima, eles podem, então, concentrar seus recursos na resposta a perguntas importantes para a empresa como:

- O que os invasores acessaram?
- Como conseguiram invadir com sucesso?
- Para onde foram?
- Ainda estão agindo em nossa rede?

As respostas para essas perguntas permitem que as equipes de segurança tomem as medidas apropriadas para evitar futuros ataques e possam informar a diretoria e o conselho sobre possíveis exposições e divulgações necessárias. A empresa pode, então, dar início ao processo que visa garantir a viabilização de controles e reduções de risco abrangentes para solucionar quaisquer lacunas de segurança identificadas durante o comprometimento, ou seja, os pontos fracos que asseguram aos invasores o espaço operacional de que precisam para serem bem-sucedidos.

Sobre a Cisco

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

Os pesquisadores de ameaças do ecossistema da CSI (Collective Security Intelligence, Inteligência de segurança coletiva) da Cisco reúnem, em uma mesma área, a melhor inteligência de ameaças do setor, usando a telemetria obtida da ampla variedade de dispositivos e sensores, de feeds públicos e privados e da comunidade de código aberto. 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, endpoints, dispositivos móveis, sistemas virtuais, Web, e-mail e na nuvem, a fim de identificar as principais causas e o escopo dos ataques. A inteligência resultante é convertida em proteções em tempo real para nossas ofertas de produtos e serviços, que são disponibilizadas de imediato para clientes da Cisco no mundo inteiro.

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

Colaboradores do Relatório Anual de Segurança Digital da Cisco de 2017.

CloudLock

A CloudLock, uma empresa da Cisco, é líder no fornecimento de soluções de agentes de segurança de acesso à nuvem (CASB) que ajudam empresas a usarem a nuvem com segurança. A CloudLock oferece visibilidade e controle para ambientes de software como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS), englobando usuários, dados e aplicativos. A CloudLock oferece informações práticas sobre segurança digital por meio de seu laboratório CyberLab, liderado por cientistas de dados, e de dados analíticos de segurança provenientes de colaboração coletiva. Para obter mais informações, acesse https://www.cloudlock.com.

Security and Trust Organization

A Security and Trust Organization da Cisco destaca o compromisso da empresa em abordar duas das questões mais críticas que preocupam tanto as diretorias quanto os líderes mundiais. As principais missões da empresa são proteger os clientes públicos e privados da Cisco, permitir e assegurar as iniciativas do Cisco Secure Development Lifecycle e Trustworthy Systems no portfólio de produtos e serviços da Cisco e proteger a empresa Cisco contra ameaças cada vez mais sofisticadas. A Cisco adota uma abordagem holística para segurança e confiança abrangentes, que inclui pessoas, políticas, processos e tecnologia. A Security and Trust Organization fomenta a excelência operacional com enfoque em InfoSec, engenharia de credibilidade, proteção de dados e privacidade, segurança na nuvem, transparência e validação e pesquisa de segurança avançada e governo. Para obter mais informações, acesse http://trust.cisco.com.

Global Government Affairs

A Cisco interage com governos em muitos níveis para ajudar a modelar a política e os regulamentos públicos que oferecem suporte ao setor de tecnologia e ajuda esses governos a atingirem suas metas. A equipe Global Government Affairs desenvolve e influencia políticas públicas e regulamentos pró-tecnologia. Ao trabalhar de modo colaborativo com as partes interessadas do setor e os parceiros da associação, a equipe cria relacionamentos com os líderes governamentais para influenciar políticas que afetam os negócios da Cisco e a adoção geral de ICT, colaborando para tomar decisões políticas globais, nacionais e locais. A equipe Government Affairs é composta por ex-representantes eleitos, parlamentares, agências regulatórias, funcionários seniores do governo dos EUA e profissionais de assuntos governamentais. Eles ajudam a Cisco a promover e proteger o uso da tecnologia em todo o mundo.

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 anormalidades. 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.

Equipe do IntelliShield

A equipe do IntelliShield realiza 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 oferece suporte a vários produtos e serviços da Cisco.

Talos Security Intelligence and Research Group

Talos é a empresa que cuida da inteligência de ameaças da Cisco, um grupo de elite composto por especialistas em segurança e dedicado a fornecer mais proteção para clientes, produtos e serviços da Cisco. O Talos é formado pelos melhores pesquisadores de ameaças, com o apoio de sofisticados sistemas de criação de inteligência de ameaças para produtos Cisco que detectam, analisam e protegem contra ameaças novas e conhecidas. 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.

Security Research and Operations (SR&O)

A Security Research & Operations (SR&O) é responsável pelo gerenciamento de ameaças e vulnerabilidade de todos os produtos e serviços da Cisco, inclusive a equipe Product Security Incident Response Team (PSIRT), que é líder do setor. A SR&O ajuda os clientes a entender o panorama de ameaças dinâmicas em eventos como o Cisco Live and Black Hat, bem como através da colaboração com seus colegas da Cisco e do setor. Além disso, a SR&O oferece novos serviços, como Cisco's Custom Threat Intelligence (CTI), que pode identificar os indicadores de comprometimento que não foram detectados ou mitigados pelas infraestruturas de segurança atuais.

Índice do Cisco Visual Networking (VNI)

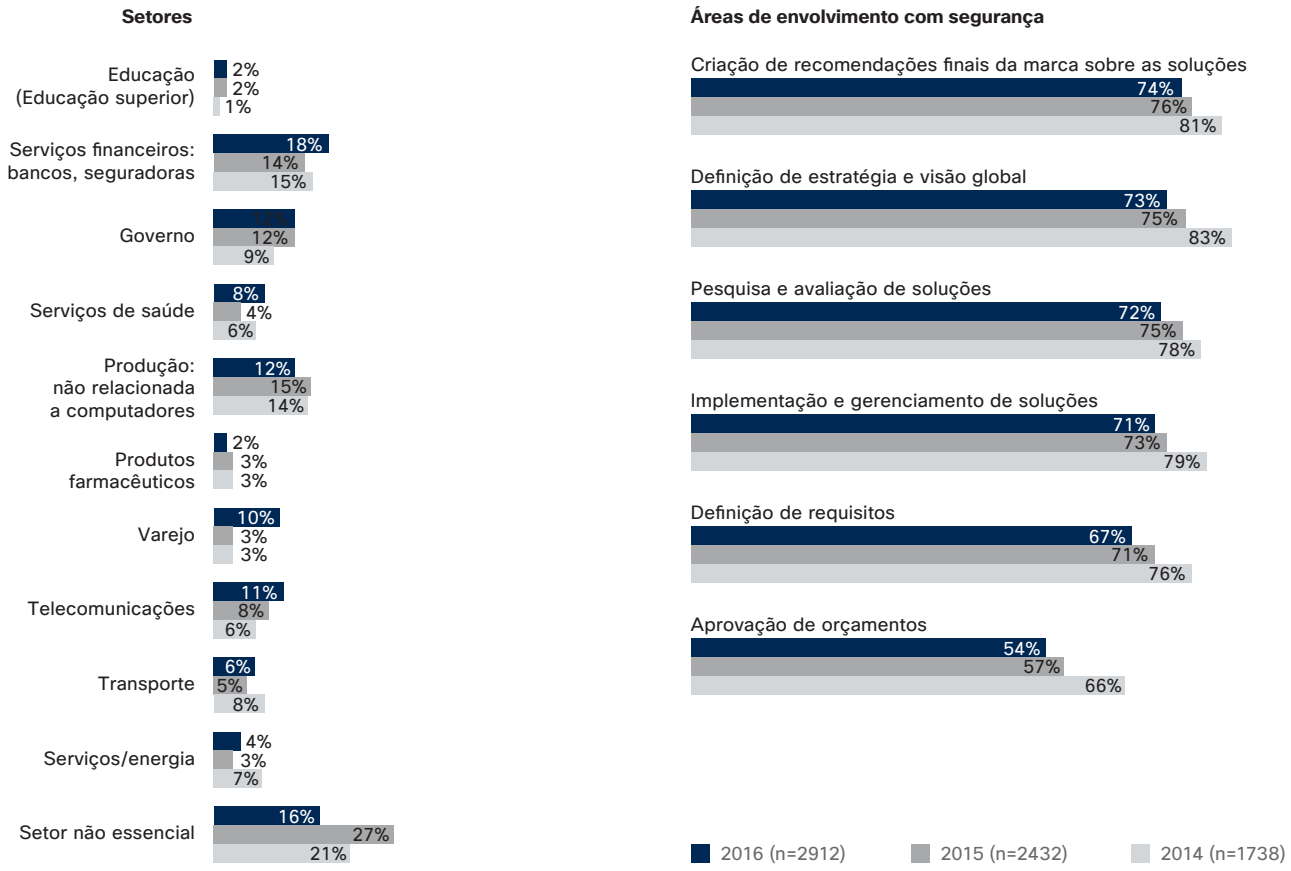
A previsão do tráfego IP global da Cisco VNI para 2015 a 2020 tem como base previsões de analistas independentes e dados de uso de rede reais. Com base nessa premissa são estabelecidas as próprias estimativas da Cisco para a adoção de serviços e tráfego IP global. Uma descrição da metodologia detalhada é incluída no relatório completo. Ao longo dos seus 11 anos de história, a pesquisa da Cisco VNI tornou-se uma medida de grande reputação do crescimento da Internet. Governos nacionais, reguladores da rede, pesquisadores acadêmicos, empresas de telecomunicações, especialistas em tecnologia e a imprensa e os analistas do setor e de negócios dependem do estudo anual para ajudá-los no planejamento do futuro digital.

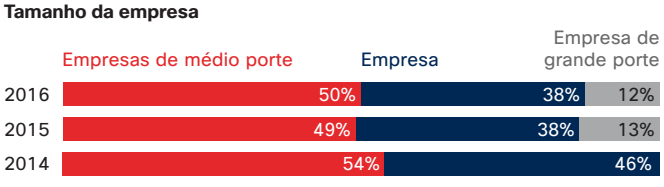
Apêndice

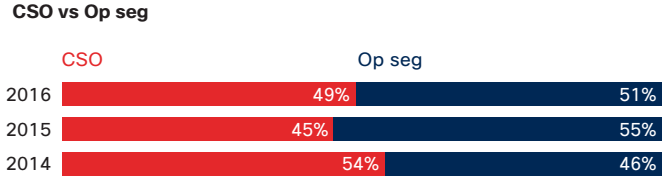
Apêndice

Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 69 Estudo comparativo de recursos de segurança







Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

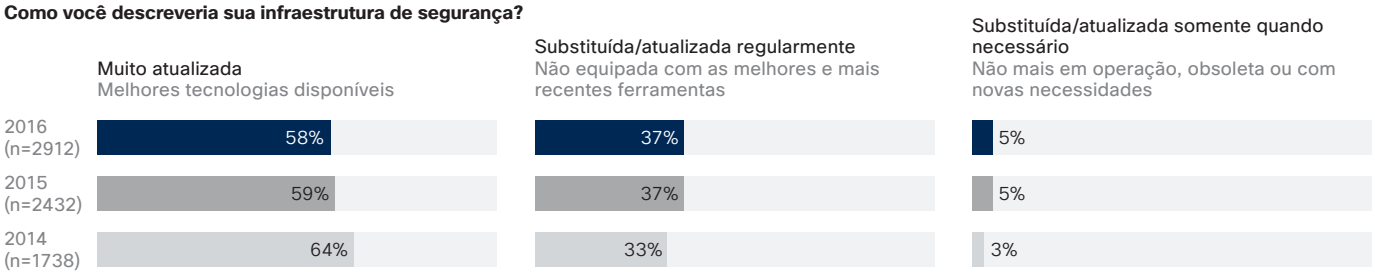
Figura 70 Número de profissionais de segurança dedicados

	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
(200 ou mais)	15%	10%	12%
Número médio de profissionais exclusivos para segurança	**30**	**25**	**33**

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

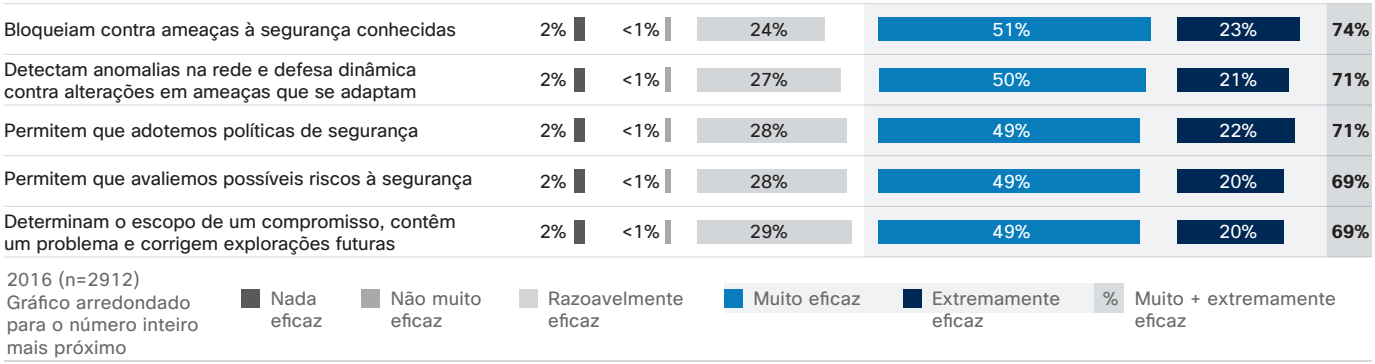
reais

Figura 71 A maioria dos profissionais de segurança considera que a infraestrutura de segurança está atualizada



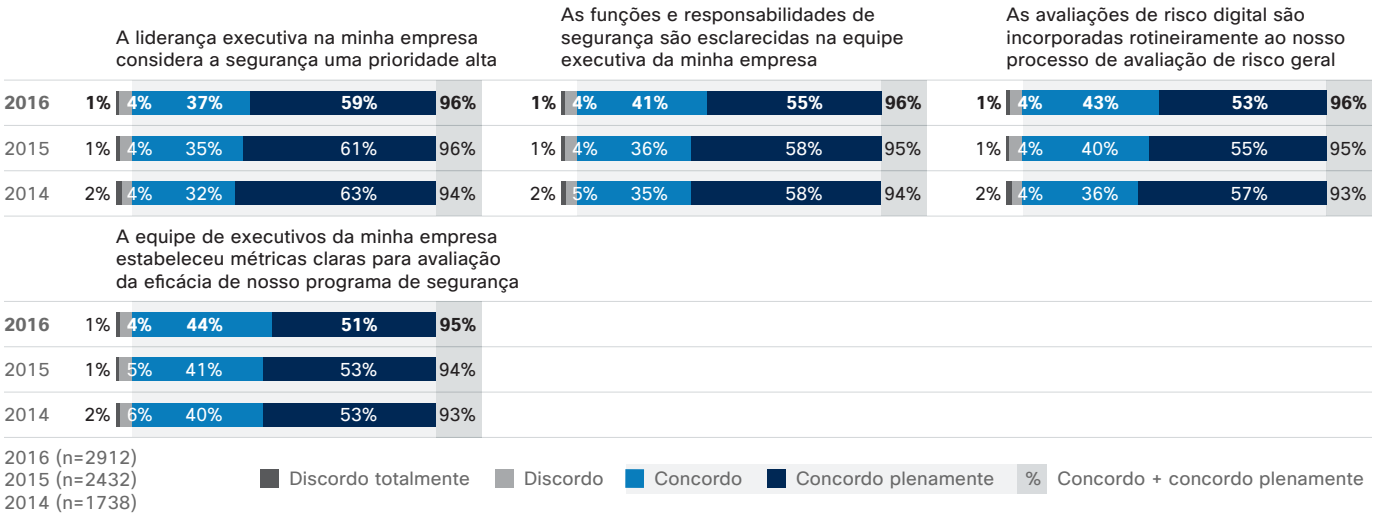
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 72 Porcentagem de profissionais de segurança que consideram várias ferramentas de segurança como altamente eficientes



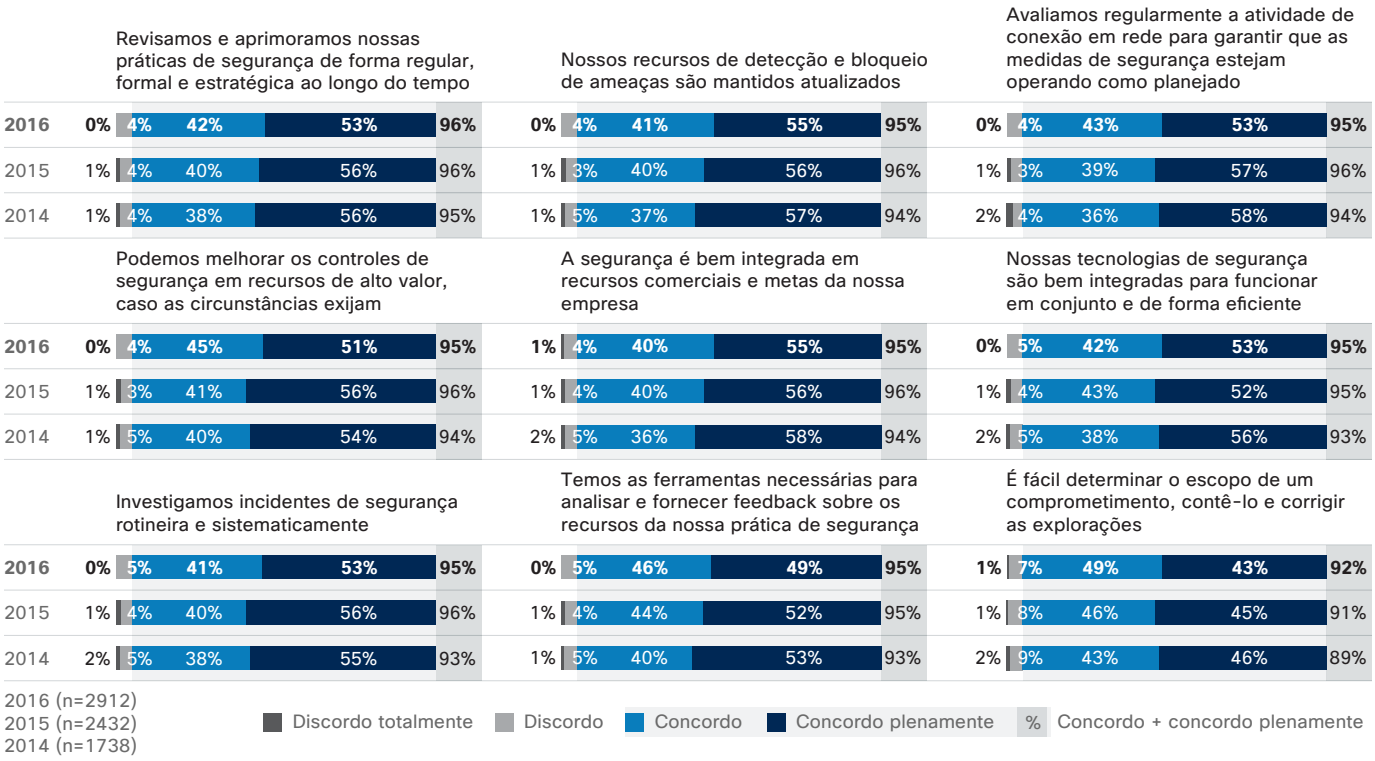
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 73 Porcentagem de profissionais de segurança que acreditam que a segurança é uma prioridade alta para os executivos



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 74 Porcentagem de entrevistados que concordam plenamente com as instruções de operacionalização da segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

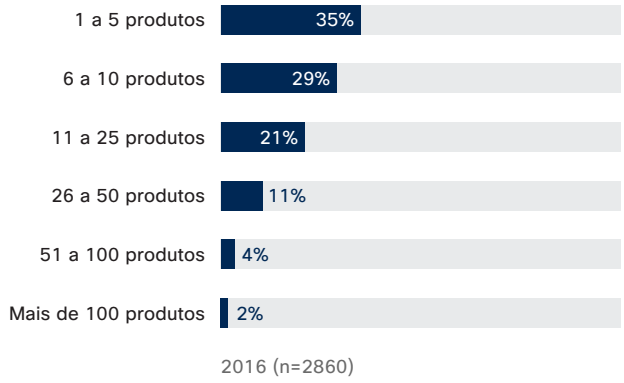
Restrições

Figura 75 Os maiores obstáculos à segurança

	2015 (n=2432)	2016 (n=2912)
Restrições de orçamento	39%	35%
Problemas de compatibilidade	32%	28%
Requisitos de certificação	25%	25%
Falta de pessoal treinado	22%	25%
Outras prioridades	24%	24%
Carga de trabalho atual muito pesada	24%	23%
Falta de conhecimento	23%	22%
Relutância em comprar até obter comprovação	22%	22%
Cultura/atitude da empresa	23%	22%
A empresa não é um alvo de grande valor para os ataques.	N/D	18%
A segurança não é uma prioridade de nível executivo	N/D	17%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 76 Número de fornecedores e produtos de segurança usados por empresas



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 77 Número de fornecedores de segurança usados por porte da empresa

Quantos fornecedores de segurança diferentes (por exemplo, marcas, fabricantes) fazem parte do seu ambiente de segurança?	Empresas de médio porte 250 a 1.000 funcionários	Empresa 1.000 a 10.000 funcionários	Grande empresa Mais de 10.000 funcionários
1-5	46,9%	43,4%	39,9%
6-10	28,4%	30,9%	21,3%
11-20	17,6%	15,8%	23,1%
21-50	5,6%	7,1%	8,7%
Mais de 50	1,4%	2,8%	6,9%
Total de empresas	**1435**	**1082**	**333**

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 78 Número de produtos de segurança usados por porte da empresa

Quantos produtos de segurança diferentes fazem parte do seu ambiente de segurança?	Empresas de médio porte 250 a 1.000 funcionários	Empresa 1.000 a 10.000 funcionários	Grande empresa Mais de 10.000 funcionários
1-5	37,9%	32,7%	25,1%
6-10	29,0%	30,1%	22,5%
11-25	19,8%	20,4%	23,7%
26-50	9,6%	10,5%	15,6%
51-100	3,0%	4,3%	7,8%
Mais de 100	0,8%	1,9%	5,4%
Total de empresas	**1442**	**1084**	**334**

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 79 Redução ano a ano do orçamento de segurança apresentado no orçamento de TI

O orçamento de segurança faz parte do orçamento de TI? (Membros do departamento de TI)	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
Tudo dentro da TI	61%	58%	55%
Parcialmente dentro da TI	33%	33%	36%
Completamente separado	6%	9%	9%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

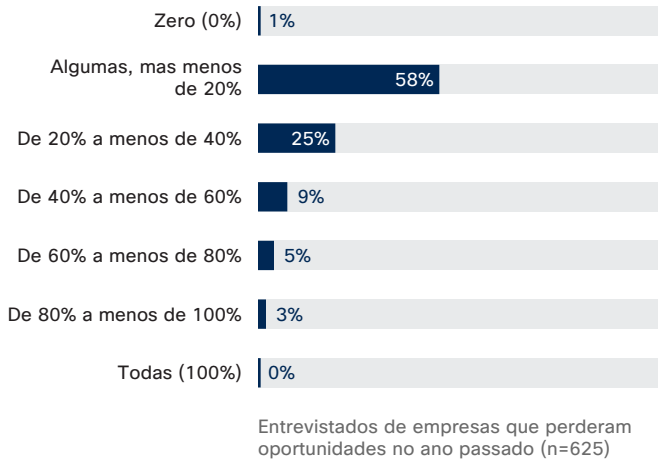
Figura 80 Redução ano a ano do gasto com segurança como uma proporção do orçamento de TI

Gasto do orçamento de TI em segurança como função	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
0%	7%	9%	10%
1-5%	4%	3%	4%
6-10%	12%	11%	16%
11-15%	23%	23%	27%
16-25%	29%	31%	26%
26%-50%	21%	19%	15%
51% ou mais	5%	4%	2%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

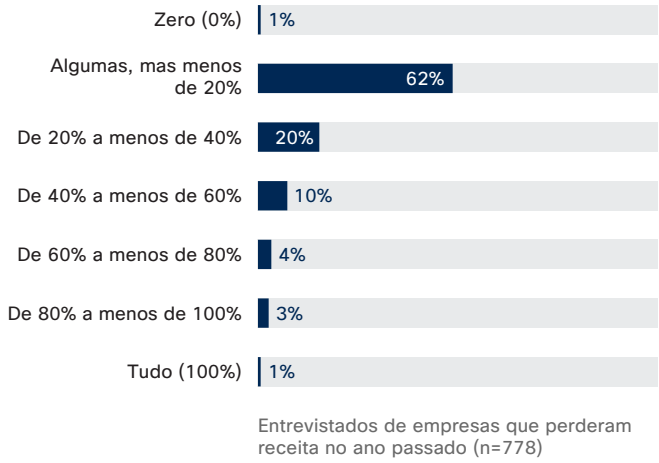
Impactos

Figura 81 Porcentagem de oportunidades perdidas pela empresa como resultado de ataques



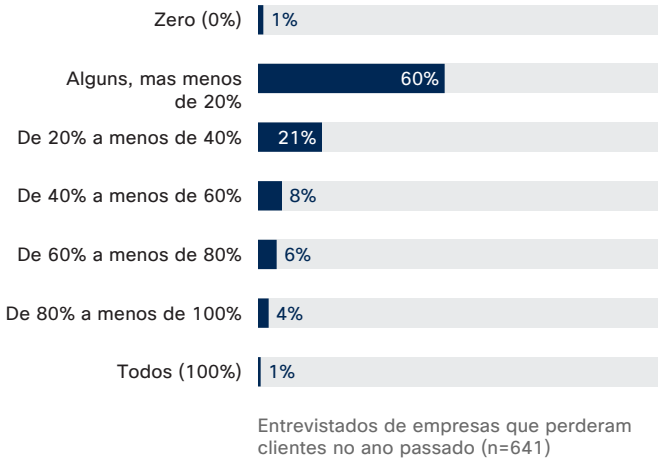
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 82 Porcentagem de receita perdida pela empresa como resultado de ataques



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 83 Porcentagem de clientes perdidos pela empresa como resultado de ataques



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Resultados

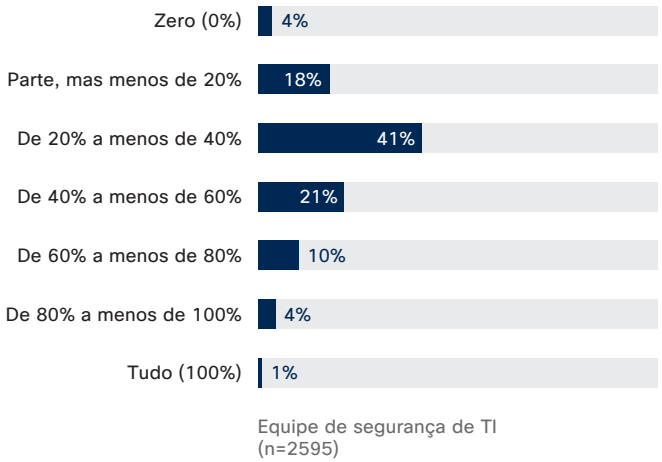
Figura 84 Porcentagem de empresas que confiam na terceirização

Quais serviços de segurança são terceirizados?	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Conselho e consultoria	51%	52%	51%
Auditoria	41%	47%	46%
Resposta a incidentes	35%	42%	45%
Monitoramento	42%	44%	45%
Inteligência de ameaças	N/D	39%	41%
Remediação	34%	36%	35%
Nenhum/Todos internos	21%	12%	10%

Por que esses serviços são terceirizados?	2015 (n=2129)	2016 (n=2631)
Mais economia	53%	52%
Desejo de um insight independente	49%	48%
Resposta mais oportuna a incidentes	46%	46%
Falta de experiência interna	31%	33%
Falta de recursos internos	31%	33%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 85 Porcentagem de empresas que confiam sua segurança a fornecedores terceirizados



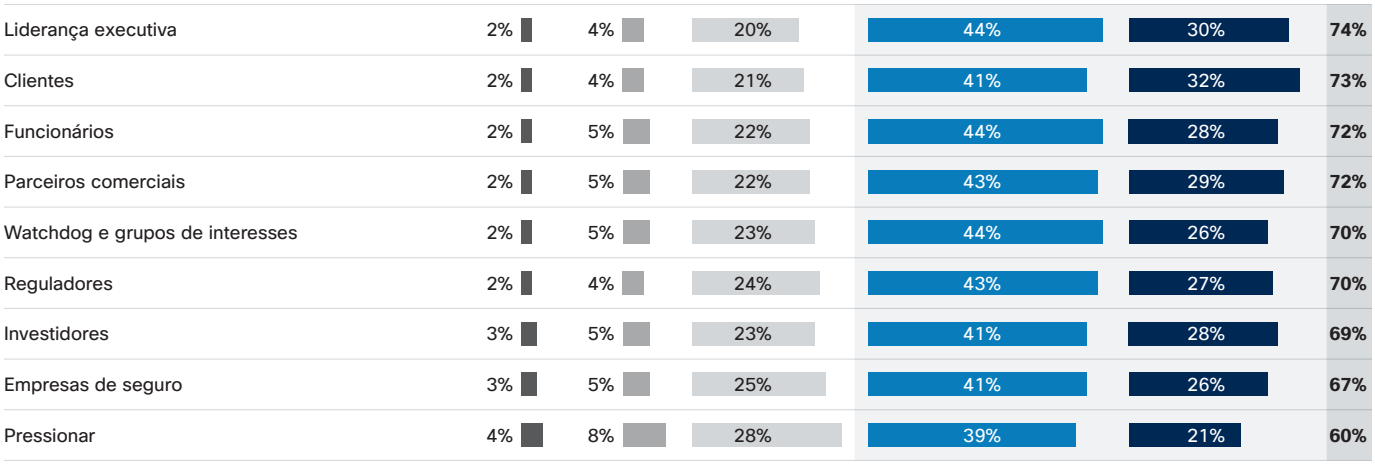
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 86 Porcentagem de serviços de segurança terceirizados por porte da empresa

Quais serviços de segurança são terceirizados?	Mercado intermediário (n=1459)	Empresa (n=1102)	Grandes empresas (n=351)
Conselho e consultoria	50%	52%	51%
Auditoria	44%	47%	50%
Monitoramento	46%	43%	44%
Inteligência de ameaças	41%	41%	40%
Resposta a incidentes	48%	44%	39%
Remediação	35%	34%	37%
Nenhum/Todos internos	8%	11%	11%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 87 Fontes de maior controle



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

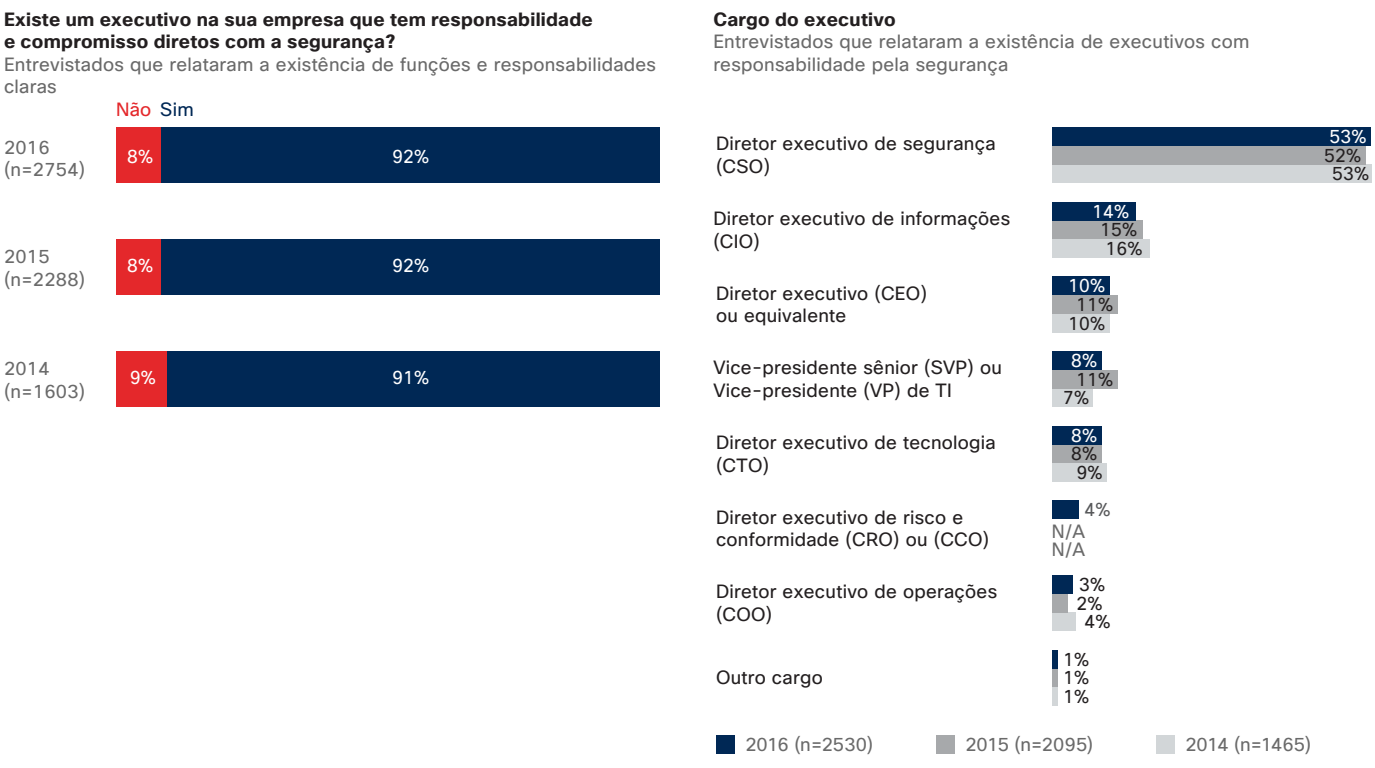
Figura 88 Aumento da nuvem privada fora das instalações e hospedagem no local gerenciada por terceiros

Onde as redes estão hospedadas?	2014 (n=1727)	2015 (n=2417)	2016 (n=2887)
Local como parte de uma nuvem privada	50%	51%	50%
No local	54%	48%	46%
Local, mas gerenciada por terceiros	23%	24%	27%
Nuvem privada fora do local	18%	20%	25%
Nuvem pública fora do local	8%	10%	9%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

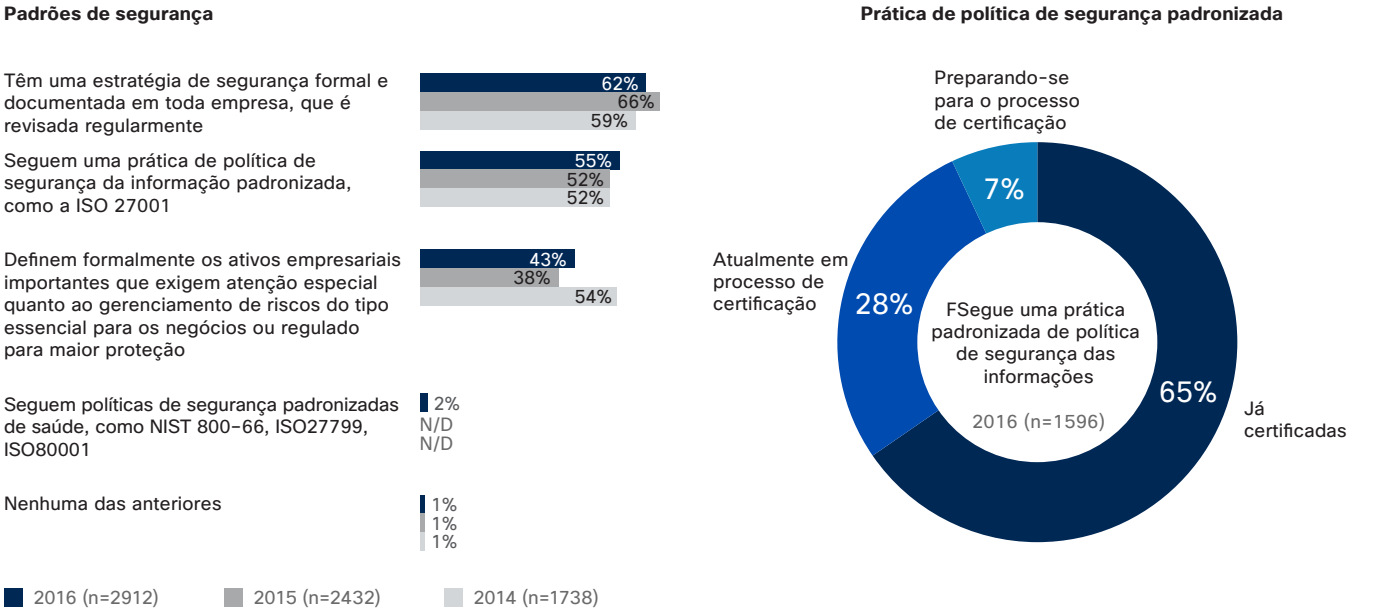
Operações, políticas, procedimentos e recursos

Figura 89 Proporção de empresas com um executivo de segurança



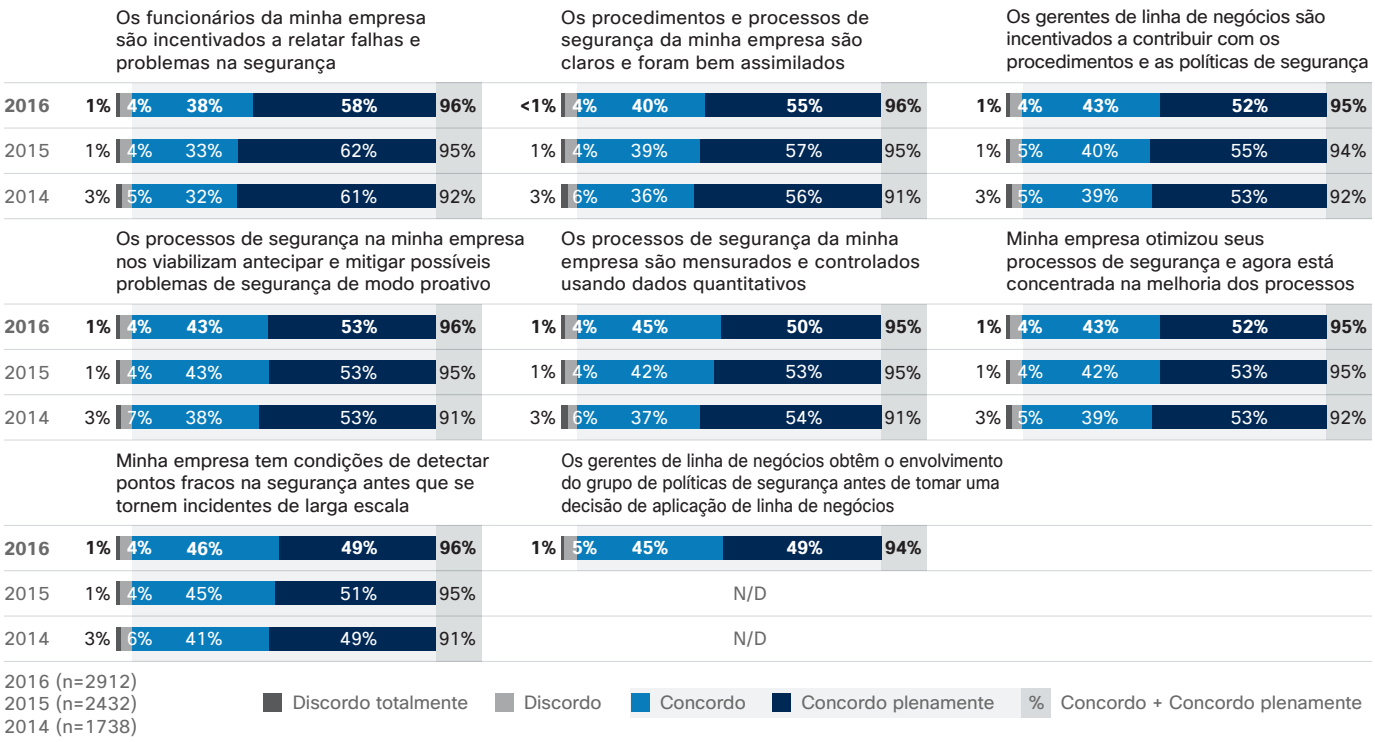
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 90 Porcentagem de empresas que têm uma estratégia de segurança formal global da empresa e seguem práticas de política de segurança padronizada



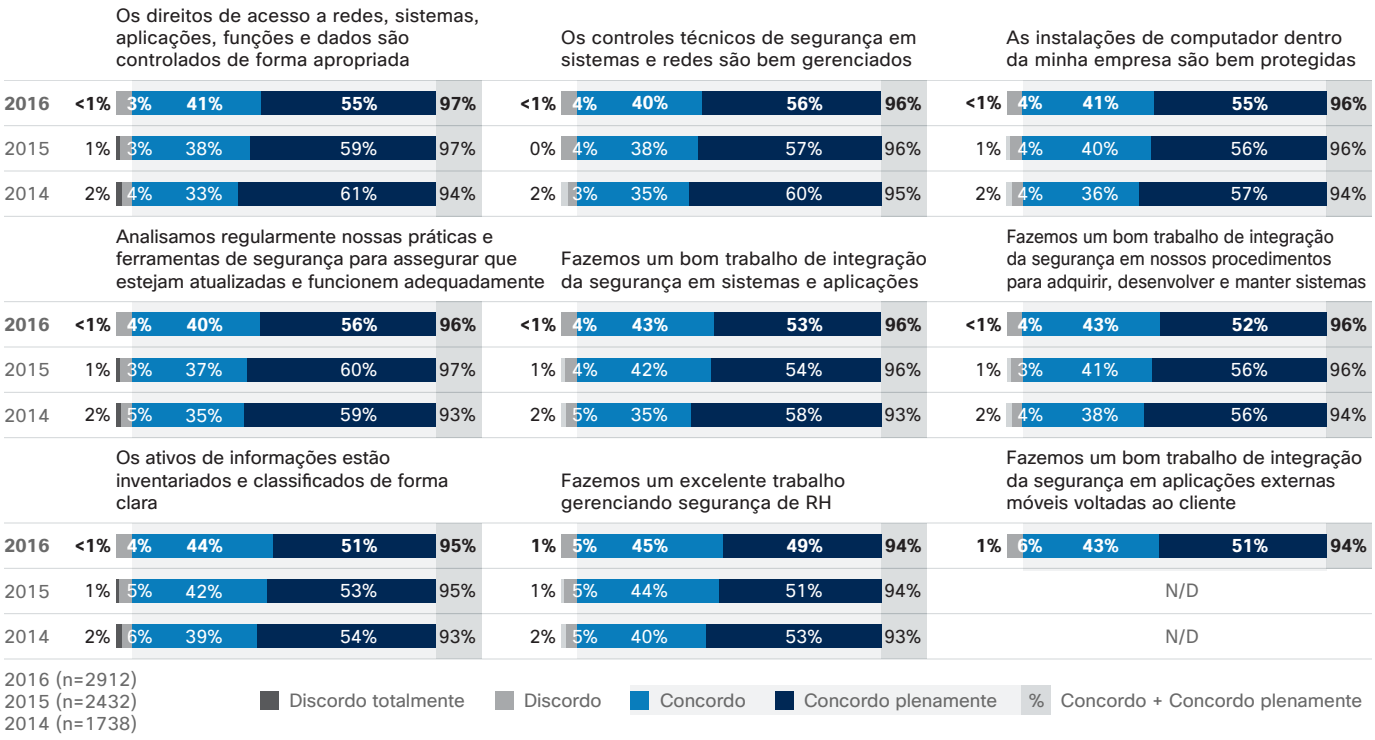
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 91 Porcentagem de entrevistados que concordam plenamente com as instruções do processo da segurança



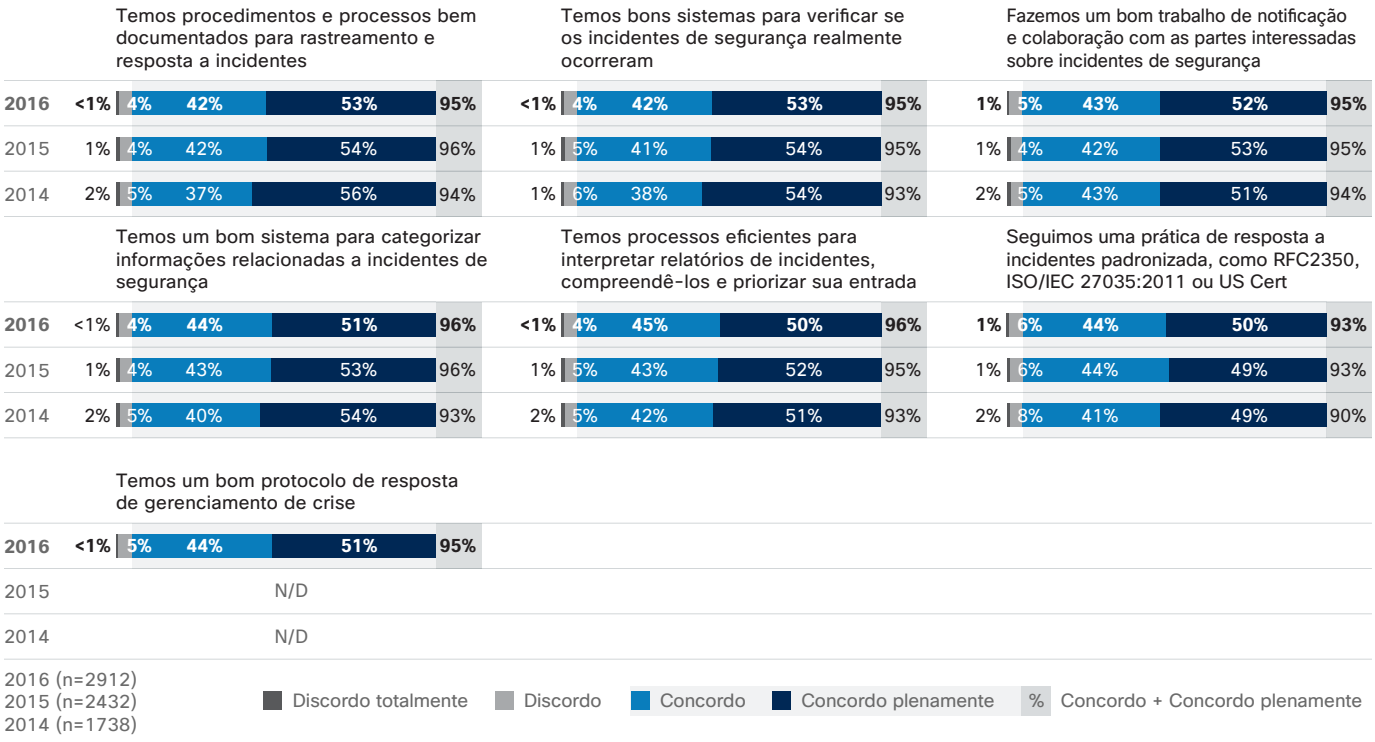
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 92 Porcentagem de entrevistados que concordam plenamente com as instruções do processo da segurança



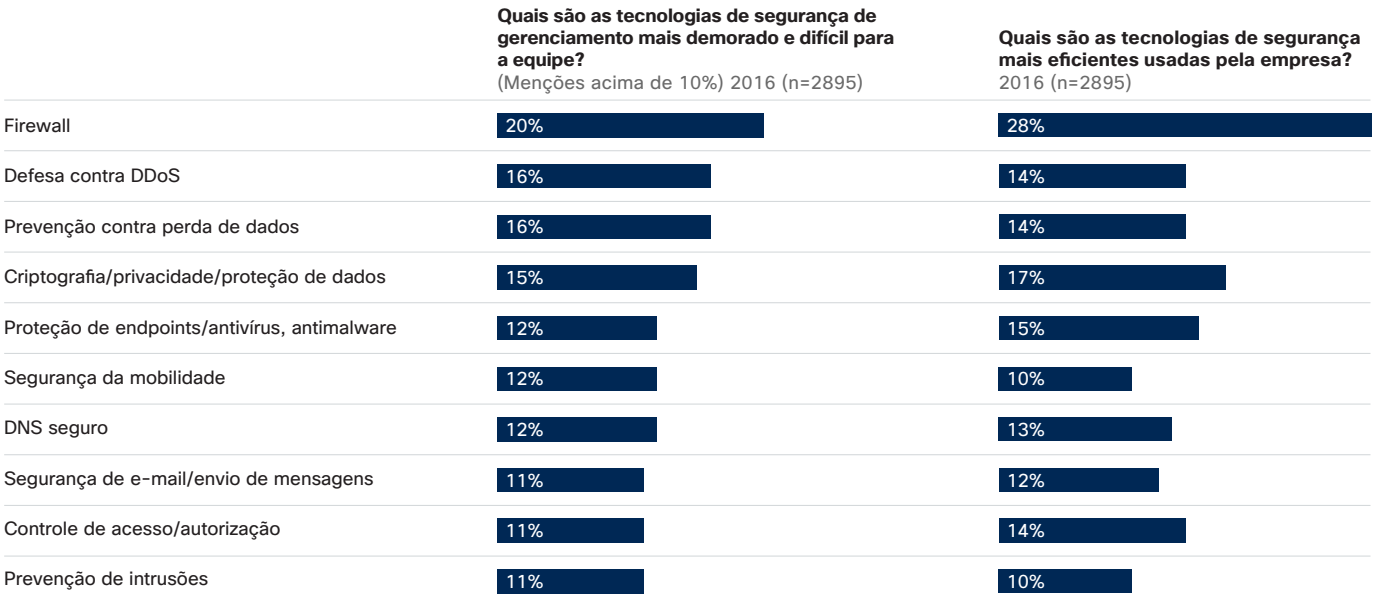
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 93 Porcentagem de entrevistados que concordam plenamente com as instruções de controles de segurança



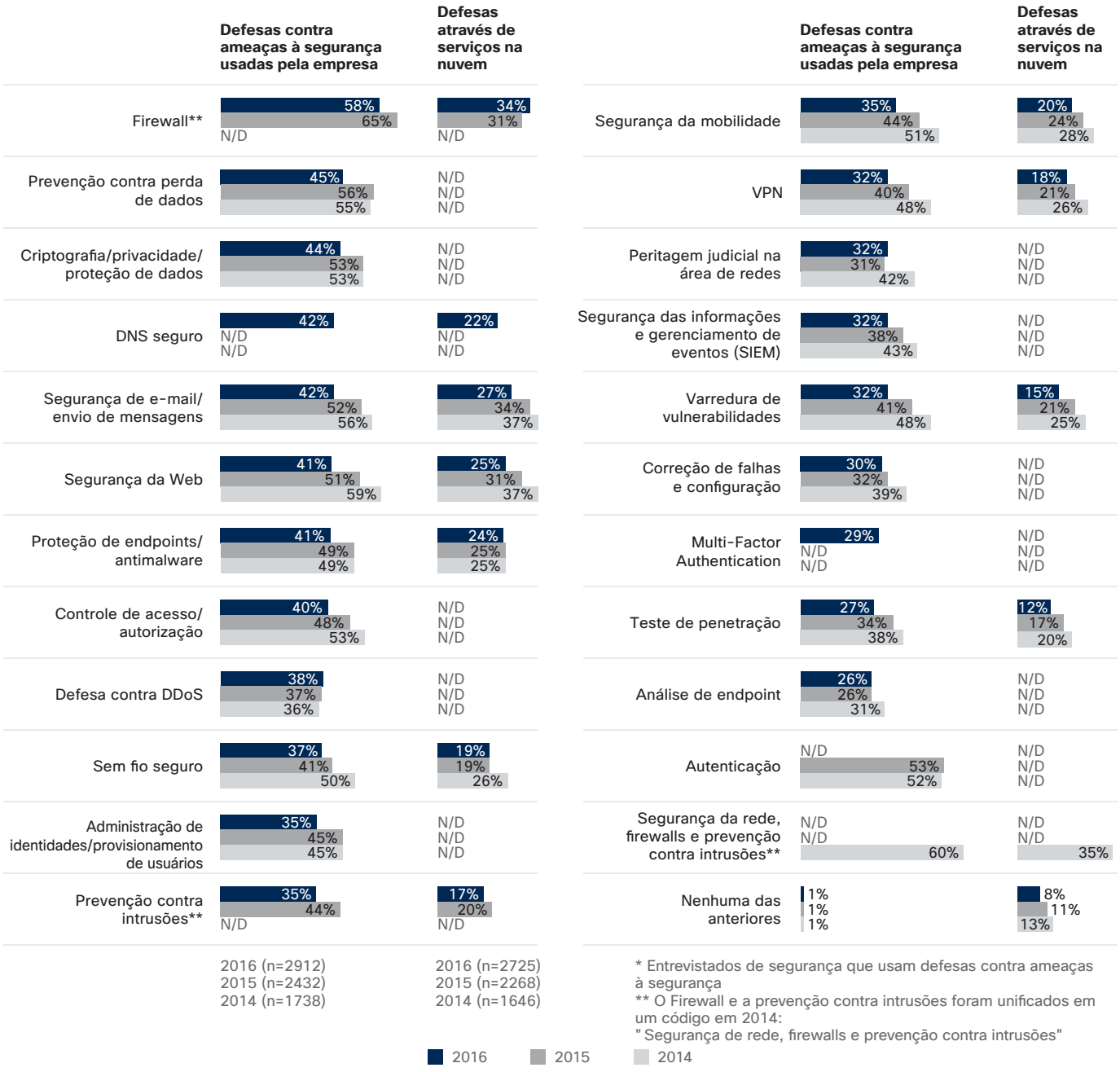
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 94 Gerenciamento e eficiência das tecnologias de segurança



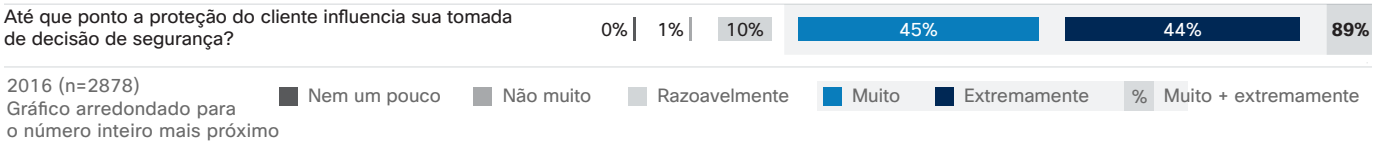
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 95 Uso ano a ano da defesa contra ameaças à segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

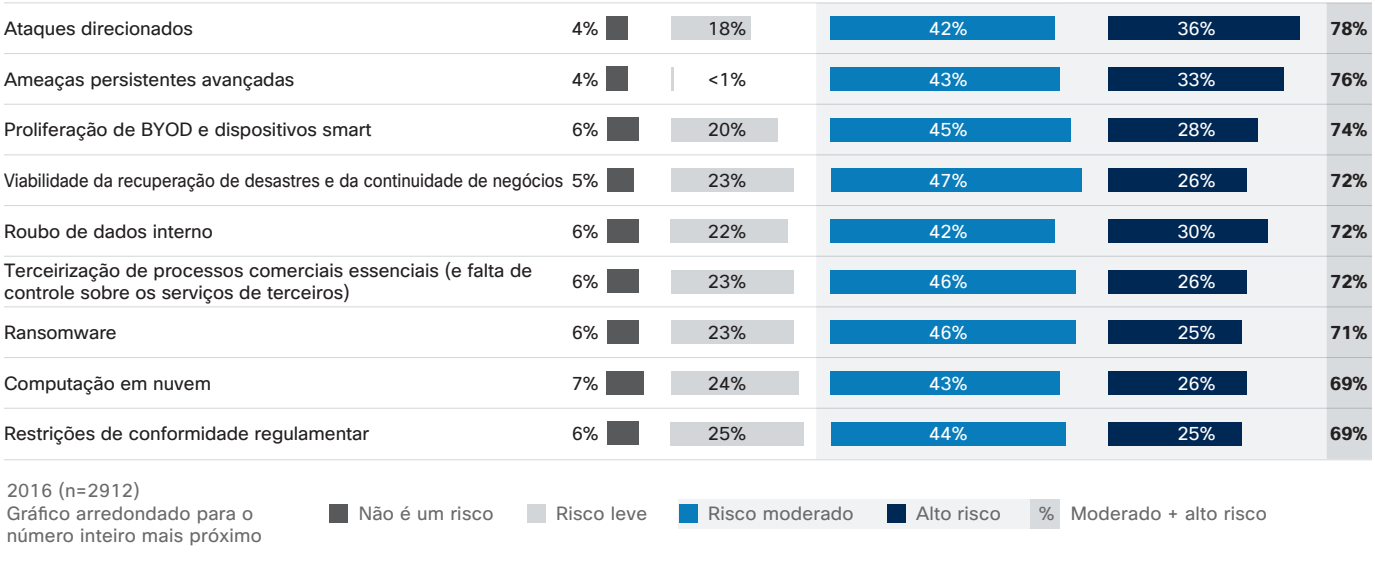
Figura 96 Grau em que a proteção do cliente afeta a tomada de decisões de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

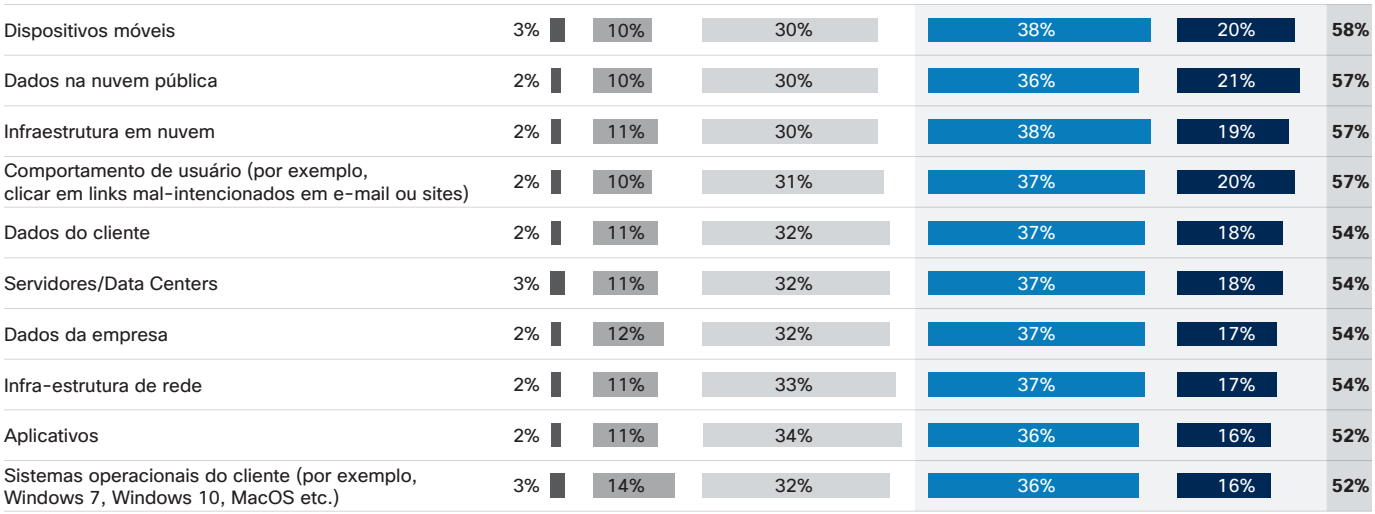
Riscos e vulnerabilidades

Figura 97 As principais razões de preocupação da equipe de segurança de TI em relação a ataques digitais



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 98 As principais razões de preocupação dos profissionais de segurança em relação a ataques digitais



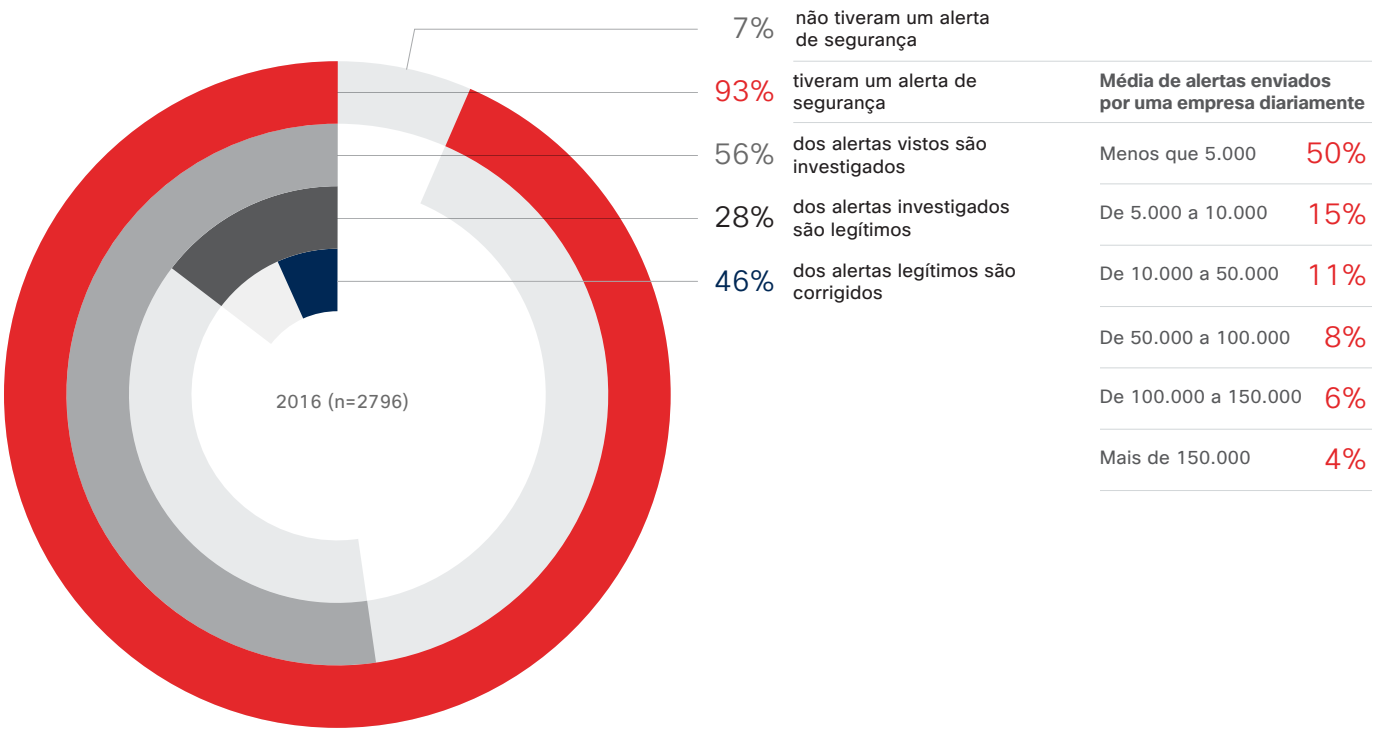
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 99 Distribuição de iniciativas das equipes de segurança

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

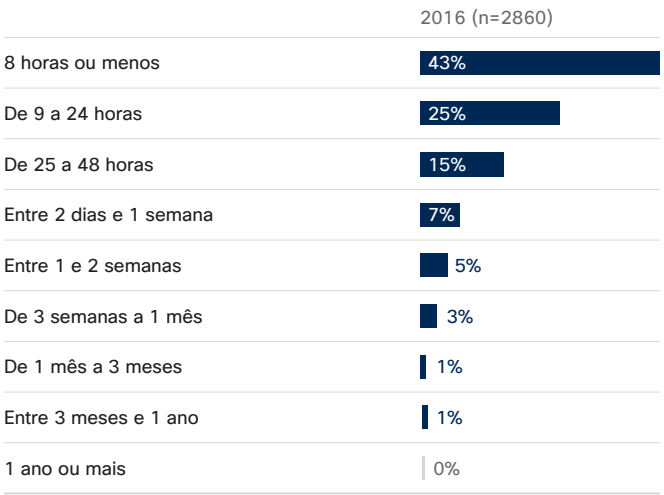
Resposta a incidentes

Figura 100 Porcentagem de alertas de segurança que são investigados ou corrigidos



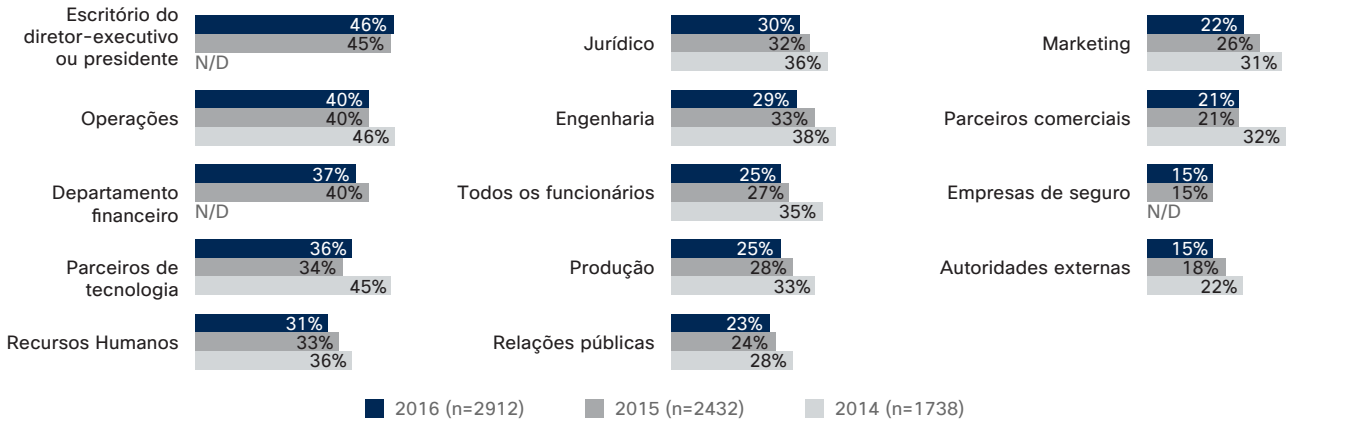
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 101 Tempo médio para detectar violações de segurança



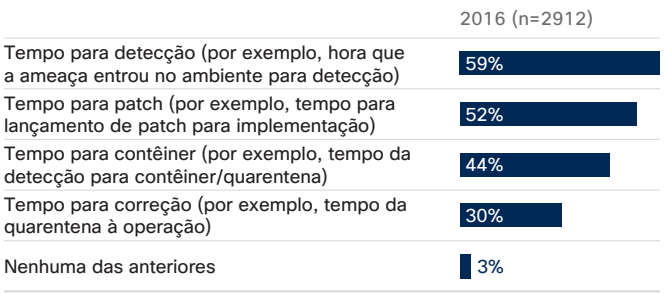
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 102 Grupos notificados em caso de incidente



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 103 KPIs usados por empresas para avaliar o desempenho da segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 104 Uso ano a ano do processo para analisar sistemas comprometidos

Processos para analisar sistemas comprometidos	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Log de firewall	61%	57%	56%
Análise de log do sistema	59%	53%	50%
Análise de fluxo de rede	53%	49%	49%
Análise de regressão de arquivo ou malware	55%	48%	47%
Análise do registro	50%	47%	43%
Análise de captura do pacote completo	47%	38%	40%
Detecção de IOC	38%	35%	38%
Análise de disco	40%	36%	36%
Análise de log/evento correlacionado	42%	37%	35%
Análise de memória	41%	34%	34%
Equipes de resposta/análise de incidentes externos	37%	33%	34%
Nenhuma das anteriores	2%	1%	1%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 105 Uso ano a ano do processo para eliminar a causa de incidentes de segurança

Processos para eliminar a causa de incidentes de segurança	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Quarentena ou remoção de aplicativos mal-intencionados	58%	55%	52%
Análise da causa principal	55%	55%	51%
Interrupção de comunicação de softwares mal-intencionados	53%	53%	48%
Monitoramento adicional	52%	48%	48%
Atualizações de políticas	51%	47%	45%
Interrupção de comunicação de aplicações comprometidas	48%	47%	43%
Desenvolvimento de correções em longo prazo	47%	40%	41%
Repaginação do sistema para o estado anterior	45%	41%	39%
Nenhuma das anteriores	2%	1%	1%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 106 Uso ano a ano do processo para restaurar sistemas afetados

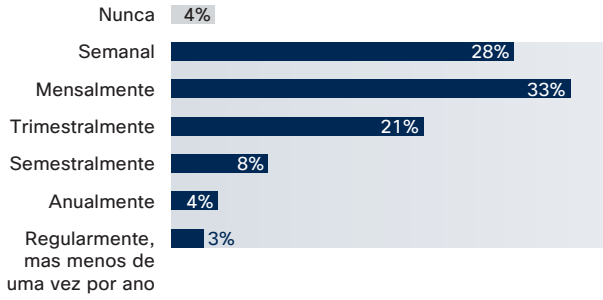
Processos para restaurar sistemas afetados	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Implementação de controles e detecções novos ou adicionais com base em pontos fracos identificados após um incidente	60%	56%	56%
Restauração usando um backup anterior ao incidente	57%	59%	55%
Correção de falhas e atualização de aplicações consideradas vulneráveis	60%	55%	53%
Restauração diferencial (remoção das alterações causadas por um incidente)	56%	51%	50%
Restauração da Gold Image	35%	35%	34%
Nenhuma das anteriores	2%	1%	1%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 107 Simulações de ataque: frequência e grau de aprimoramento da defesa de segurança

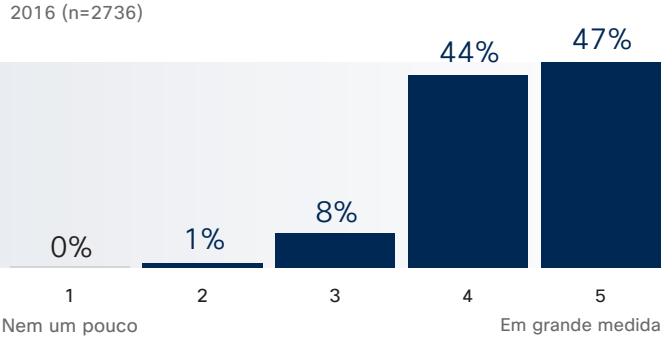
Com que frequência sua empresa executa simulações de ataques?

2016 (n=2868)



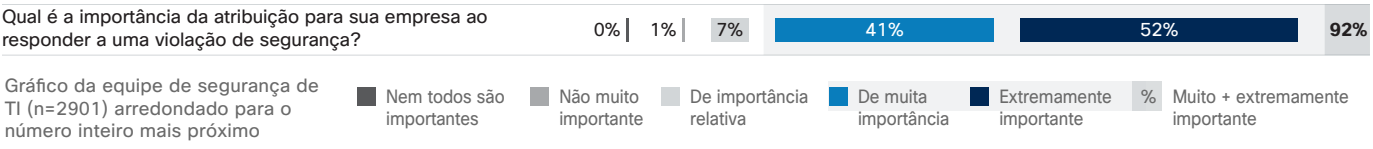
Até que ponto os resultados das simulações de ataque geram melhorias em políticas de defesa de segurança, procedimentos ou tecnologias de segurança?

2016 (n=2736)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

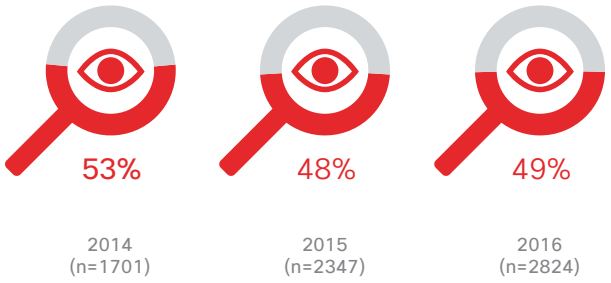
Figura 108 Importância de atribuir a origem de uma violação de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

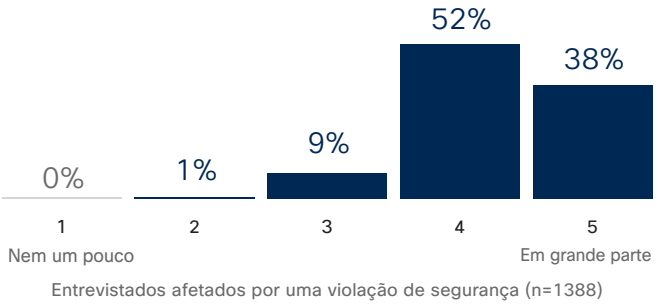
Violações e seus impactos

Figura 109 Porcentagem de empresas que passaram por uma violação pública



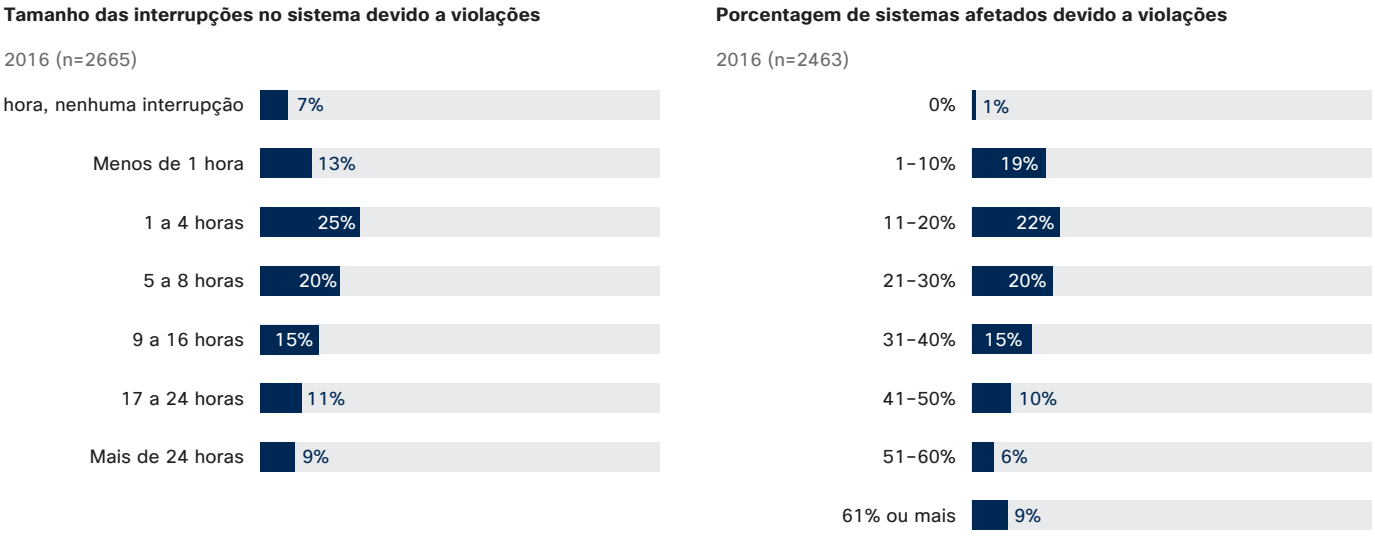
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 110 Quantas melhorias a violação gerou nas suas tecnologias, políticas ou procedimentos de defesa contra ameaças de segurança?



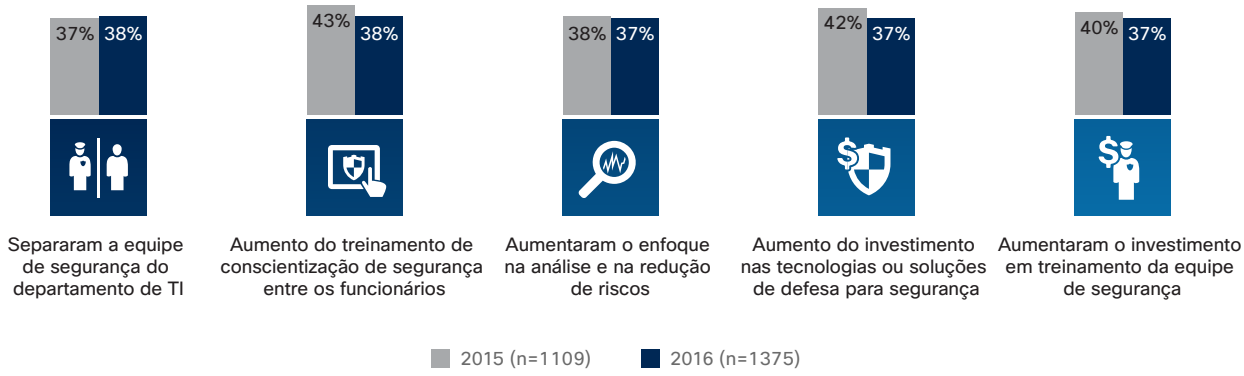
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 111 Tamanho e alcance das interrupções causadas por violações de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 112 Melhorias para proteger a sua empresa contra violações de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

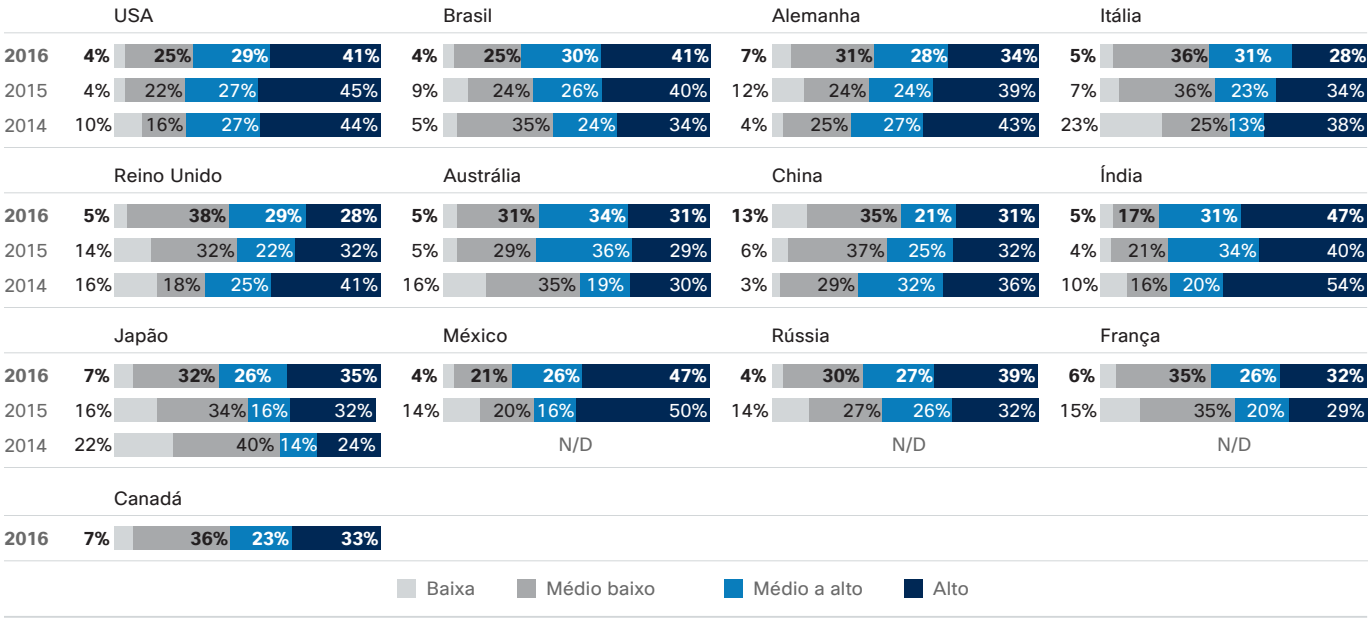
Escolha de fornecedor e expectativas

Figura 113 Importância da privacidade e da proteção dos dados para os fornecedores

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

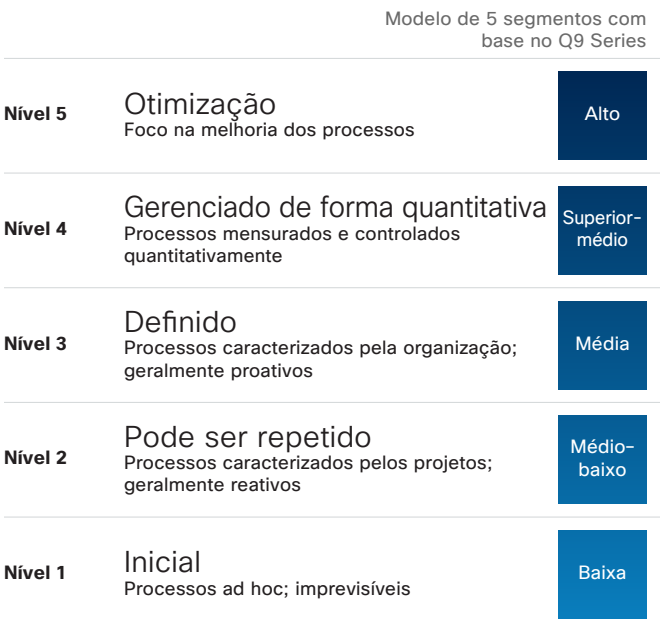
Modelo de maturidade do recurso de segurança

Figura 114 Maturidade de segurança por país



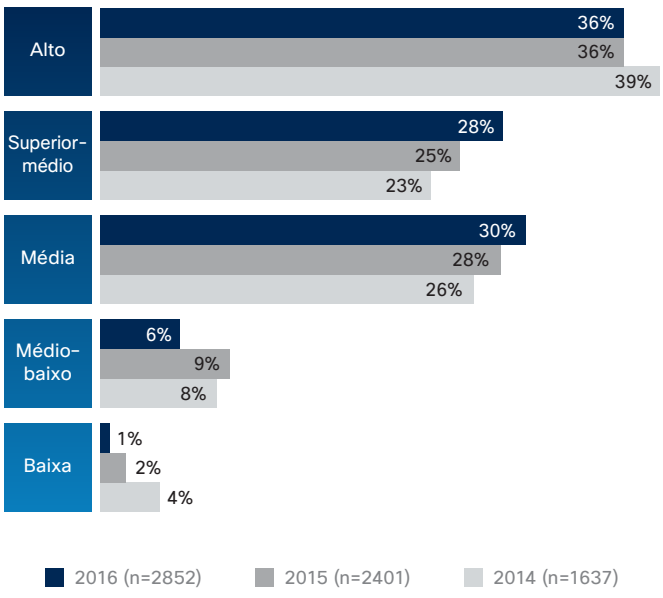
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 115 O modelo de maturidade classifica as empresas com base no processo de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 116 Dimensionamento de segmentos do modelo de maturidade

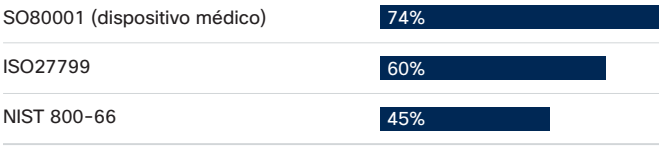


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Específico do setor

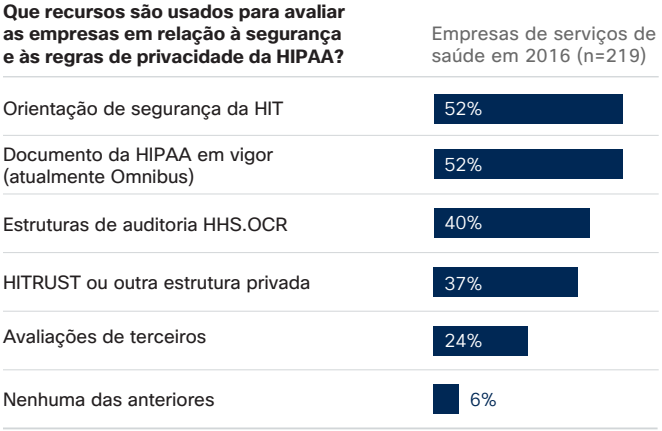
Figura 117 Porcentagem de empresas de serviços de saúde que implementaram políticas de segurança padronizadas

Políticas de segurança padronizadas
As empresas de serviços de saúde seguem uma prática de política de segurança de informações específica para o setor, 2016 (n=65)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

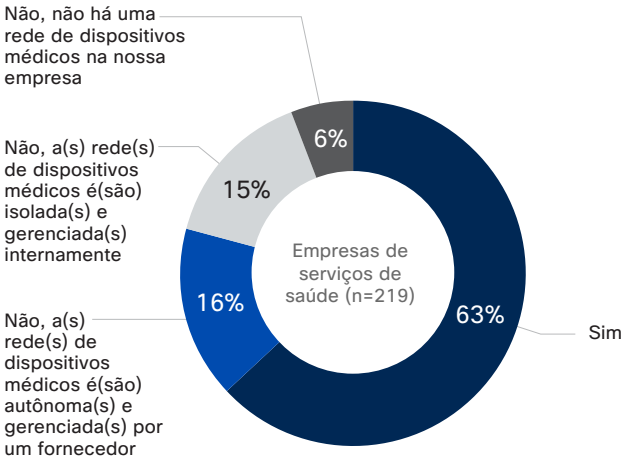
Figura 118 Recursos que empresas da área de saúde utilizam para avaliar a si próprias em relação às regras de privacidade da HIPAA



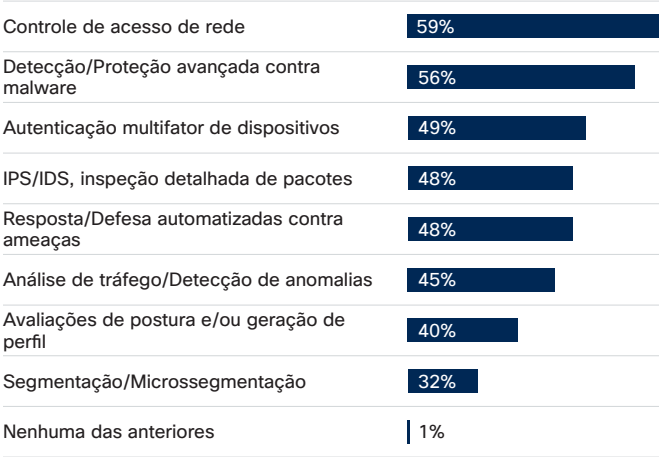
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 119 As medidas de segurança mais comuns entre as empresas de serviços de saúde com redes de dispositivos médicos

A sua empresa tem uma rede de dispositivos médicos que converge com a rede de um hospital central?



Quais destas medidas de segurança (se houver) foram implementadas pela sua empresa para proteger a rede de dispositivos médicos?
Empresas com uma rede de dispositivos médicos (n=207)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 120 Exemplo de perfil para telecomunicações

Em que subsetor de telecomunicação a sua empresa está envolvida?
Empresas de telecomunicações (n=307)

Equipamento de comunicação	47%
Provedor de serviços (tradicional)	33%
Operador a cabo/satélite	11%
Mídia/transmissão	7%
Provedor acima das expectativas (Netflix, Hulu, etc.)	2%

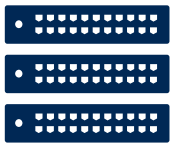
Quais destes serviços a sua empresa oferece para os clientes?
Empresas de telecomunicações (n=308)

Serviços de segurança gerenciados fornecidos para usuários finais	71%
Redes centrais de produção, como IP (Including Television), Mobile, etc.	60%
Ambiente corporativo	59%
Data centers	57%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 121 Fatores estratégicos de segurança para telecomunicações

Prioridade relativa para protocolos e estratégias de segurança
Empresas de telecomunicações (n=308)



Percentual médio de disponibilidade

34%

Disponibilidade: garantia de acesso confiável aos dados

Percentual médio de confidencialidade

36%

Confidencialidade: garantia de que os dados sejam acessados somente por quem tem esse direito

Percentual médio de integridade

31%

Integridade: garantia da precisão e da exatidão dos dados

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 122 Prioridades de segurança para telecomunicações

Classificação em termos de prioridade para a segurança na empresa
Empresas de telecomunicações (n=308)

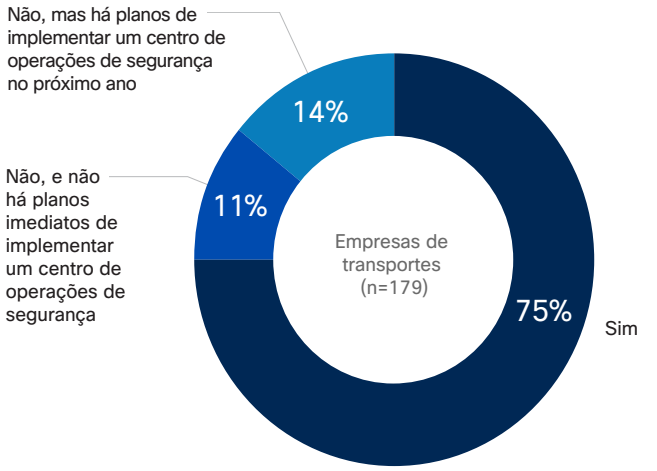
Proteção dos data centers	34%	21%	24%	22%
Na rede central de produção que disponibiliza serviços móveis e/ou de IP	26%	21%	29%	24%
Prestação de serviços de segurança gerenciados	21%	30%	19%	30%
A rede corporativa e os dados internos	20%	28%	29%	24%

Classificado em 1º | Classificado em 2º | Classificado em 3º | Classificado em 4º

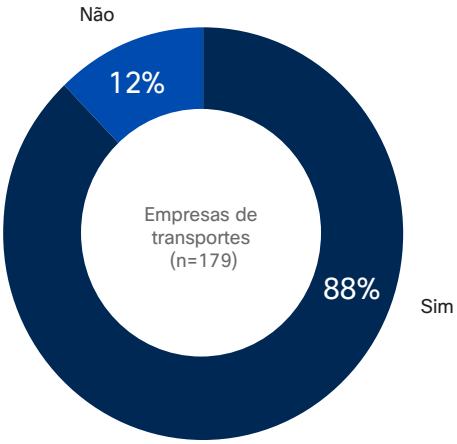
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 123 Exemplo de perfil para transportes

A sua empresa utiliza um SOC (centro de operações de segurança)?



A sua empresa participa de entidades de padrões de segurança ou organizações do setor?



Em qual subsetor de transportes a sua empresa está envolvida?
Empresas de transportes (n=180)

Frete e logística	54%
Transporte coletivo	11%
Trilho	9%
Estradas	9%
Aviação	7%
Transporte marítimo	5%
Vehicles	5%

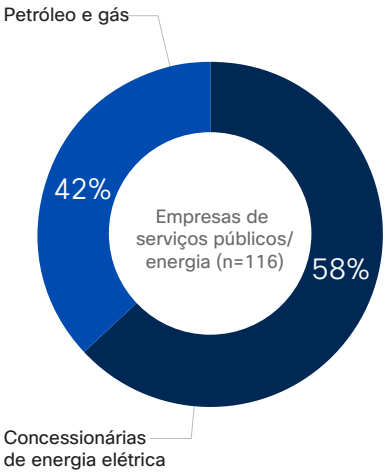
Em quais das seguintes áreas de segurança você tem responsabilidades?
Empresas de transportes (n=180)

Segurança de tecnologia operacional	84%
Segurança de infraestrutura essencial	71%
Segurança de veículos	43%

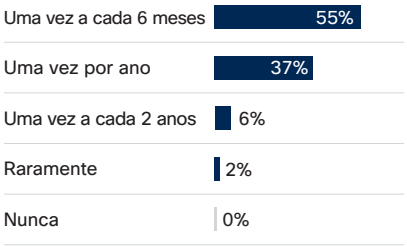
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 124 Exemplo de perfil para serviços públicos/energia

Em qual subsetor de serviços públicos/ energia a sua empresa está envolvida?

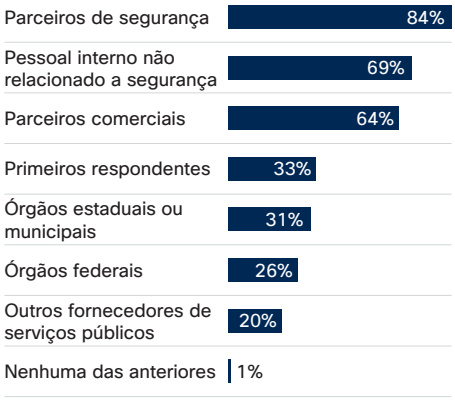


Com que frequência a sua empresa organiza um treinamento ou um exercício para testar o plano de resposta a um incidente de segurança digital?



Empresas de serviços públicos/energia (n=116)

Quando esses treinamentos ou exercícios são realizados, quem está envolvido?

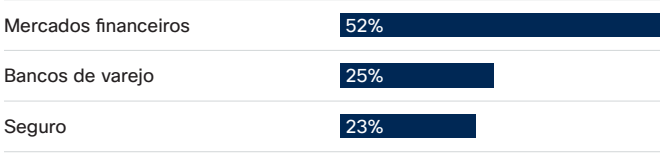


Empresas de serviços públicos/energia (n=116)

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

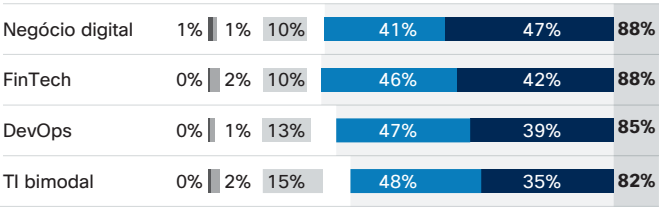
Figura 125 Exemplo de perfil para serviços financeiros

Em qual subsetor de serviços financeiros a sua empresa está envolvida?



Empresas de serviços financeiros (n=509)
Gráfico arredondado para o número inteiro mais próximo

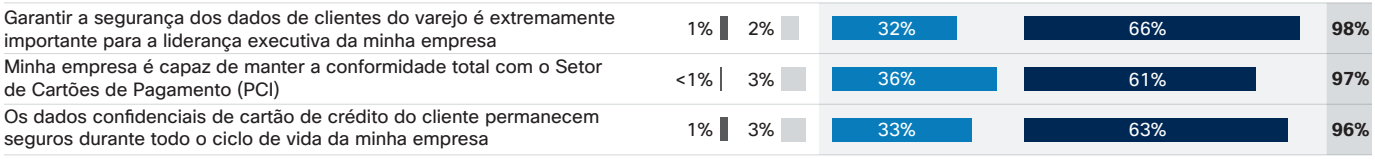
Quanto você acha que a segurança está sendo influenciada pelas seguintes tendências?



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

Figura 126 Segurança de dados no varejo

Até que ponto você concorda ou discorda destas declarações?



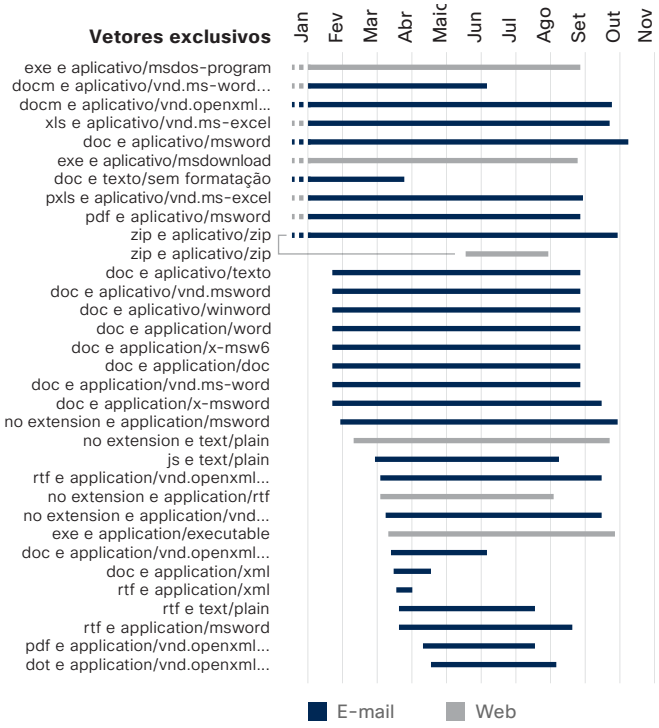
Empresas do varejo (n=290), Gráfico arredondado para o número inteiro mais próximo

Discordo totalmente | Discordo parcialmente | Concordo parcialmente | Concordo plenamente | % Concordo parcialmente + plenamente

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2017

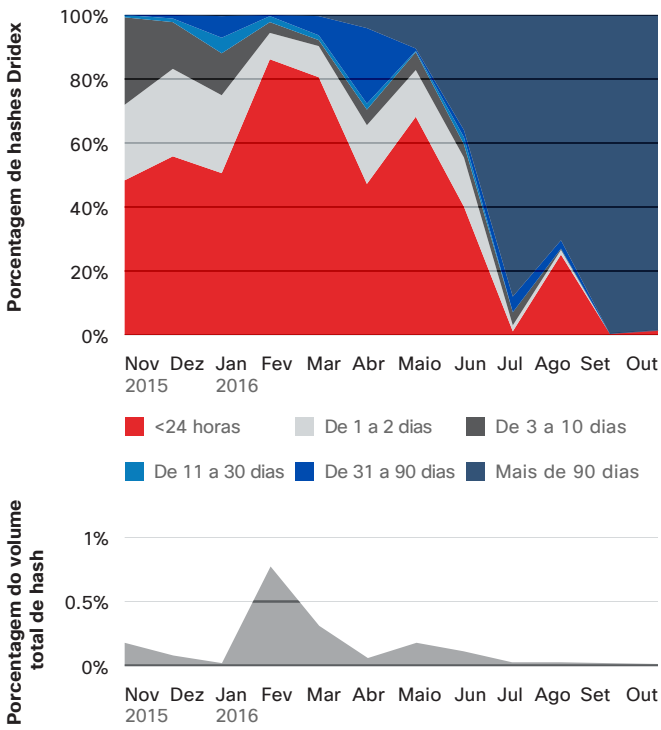
Linhas de malware

Figura 127 Combinações de MIME e extensão de arquivo para Dridex (vetores Web e e-mail)



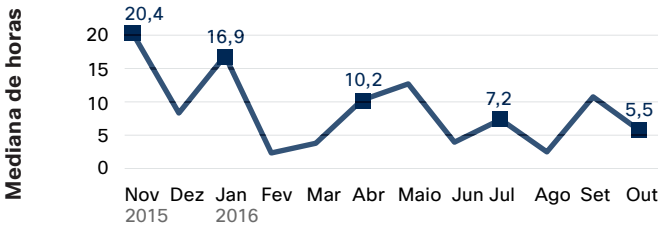
Fonte: Cisco Security Research

Figura 128 Envelhecimento de hash para a linha de malware Dridex e percentual do volume total de hash observado por mês



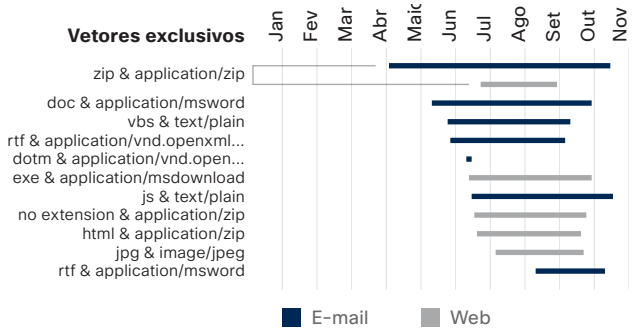
Fonte: Cisco Security Research

Figura 129 TTD da linha de malware Dridex



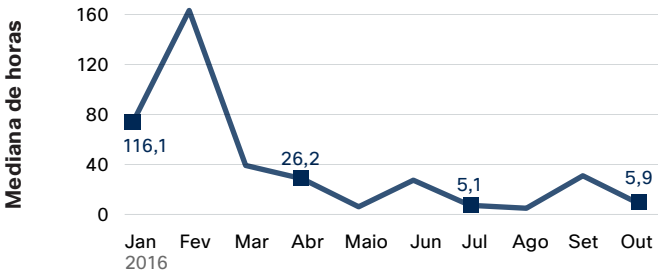
Fonte: Cisco Security Research

Figura 130 Combinações de MIME e extensão de arquivo para a linha de ameaças e indicadores que geram e incluem o payload Cerber (vetores Web e e-mail)



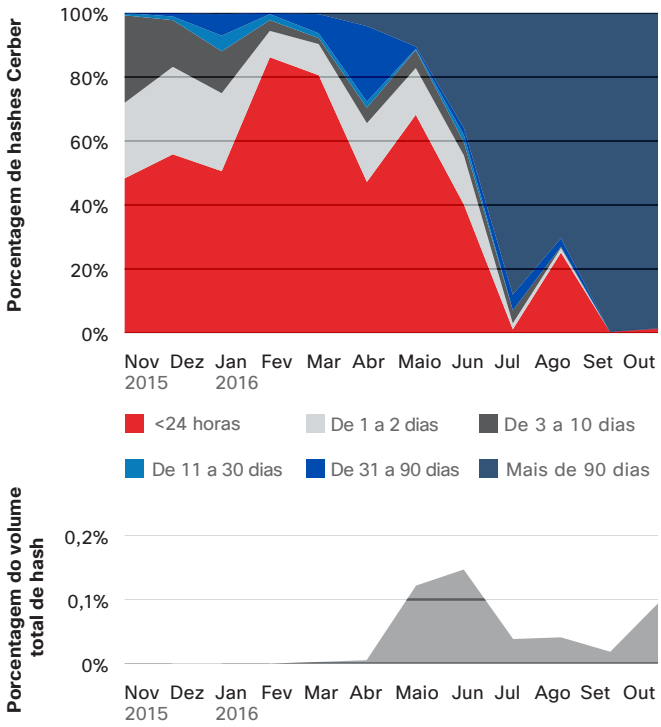
Fonte: Cisco Security Research

Figura 131 TTD da linha de malware Cerber



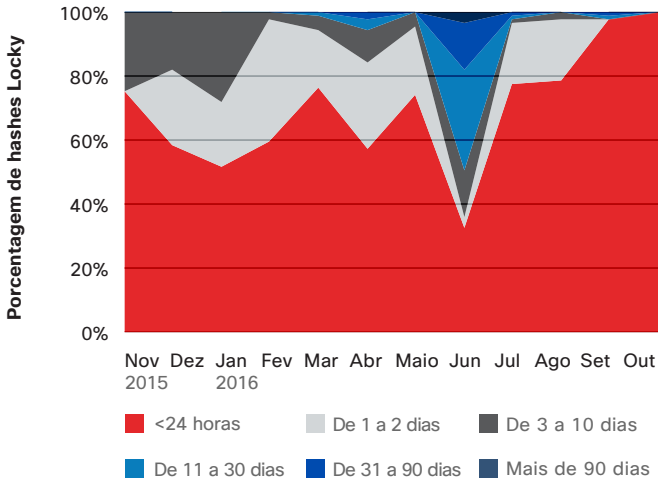
Fonte: Cisco Security Research

Figura 132 Envelhecimento de hash para a linha de malware Cerber e percentual do volume total de hash observado por mês



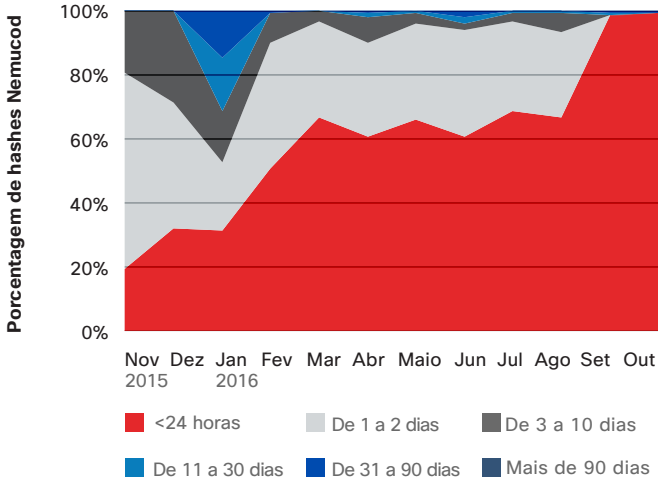
Fonte: Cisco Security Research

Figura 133 Envelhecimento de hash para a linha de malware Locky por mês



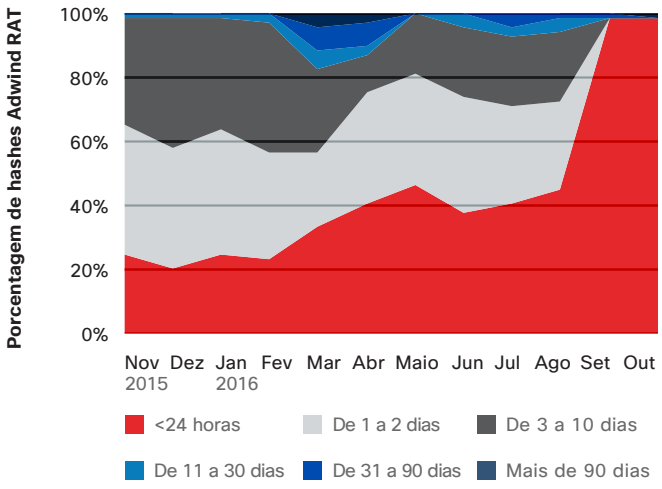
Fonte: Cisco Security Research

Figura 134 Envelhecimento de hash para a linha de malware Nemucod por mês



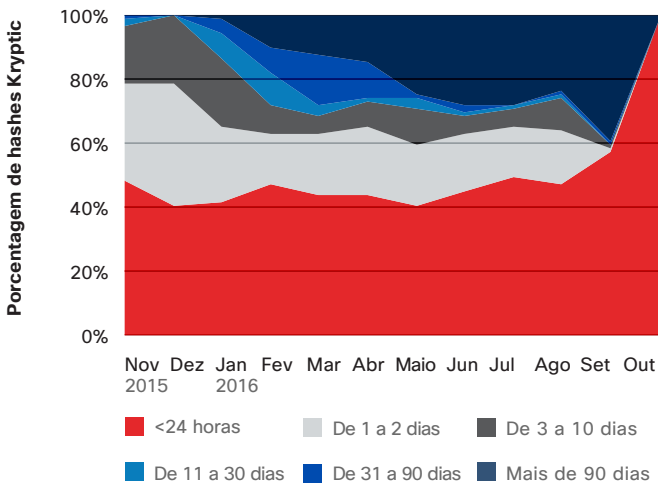
Fonte: Cisco Security Research

Figura 135 Envelhecimento de hash para a linha de malware Adwind RAT por mês



Fonte: Cisco Security Research

Figura 136 Envelhecimento de hash para a linha de malware Kryptik por mês



Fonte: Cisco Security Research

Download dos gráficos

O download de todos os gráficos deste relatório pode ser feito em:
www.cisco.com/go/acr2017graphics

Atualizações e correções

Para ver atualizações e correções das informações deste relatório, acesse:
www.cisco.com/go/acr2017errata

Sede nas Américas
Cisco Systems, Inc.
San Jose, CA

Sede na Ásia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapura

Sede na Europa
Cisco Systems International BV Amsterdam,
Holanda

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

Publicação: janeiro de 2017