Relatório anual de segurança da Cisco de 2016

Resumo executivo

Os profissionais de segurança precisam repensar suas estratégias de defesa.

Criminosos e defensores desenvolvem tecnologias e táticas cada vez mais sofisticadas. Os criminosos criam infraestruturas sólidas de back-end, com as quais iniciam e apoiam suas campanhas. Criminosos on-line aprimoram suas técnicas para tirar dinheiro das vítimas e burlar a detecção, enquanto continuam roubando dados e propriedade intelectual.

O Relatório Anual de Segurança da Cisco de 2016, que apresenta dados de pesquisa, insights e perspectivas da Cisco Security Research, destaca os desafios que os defensores enfrentam para detectar e bloquear invasores que empregam um arsenal de ferramentas variadas e em constante evolução. O relatório também inclui a pesquisa de especialistas externos, como a Level 3 Threat Research Labs, para esclarecer melhor as atuais tendências de ameaças.

Analisamos atentamente os dados compilados pelos pesquisadores da Cisco para mostrar as mudanças ao longo do tempo, fornecer insights sobre o que esses dados significam e explicar como os profissionais de segurança devem responder às ameaças.

Neste relatório, apresentamos e discutimos:

INTELIGÊNCIA DE AMEAÇAS

Esta seção examina algumas das tendências mais fortes na segurança digital, conforme identificadas pelos nossos pesquisadores, bem como atualizações sobre vetores de ataque na Web, métodos de ataque na Web e vulnerabilidades. Isso também inclui uma análise detalhada de ameaças cada vez maiores, como ransomware. Para produzir sua análise de tendências observadas em 2015, a Cisco Security Research utilizou um conjunto global de dados de telemetria.

INSIGHTS DO SETOR

Esta seção examina as tendências de segurança que afetam as empresas, inclusive o uso crescente da criptografia e os potenciais riscos à segurança que ela representa. Examinamos os pontos fracos na proteção de redes de pequenas e médias empresas (SMBs). E apresentamos a pesquisa em empresas que confiam em software desatualizado, sem suporte ou no fim da vida útil para atender à sua infraestrutura de TI.

ESTUDO COMPARATIVO DOS RECURSOS DE SEGURANÇA

Esta seção aborda os resultados do segundo Estudo comparativo de recursos de segurança da Cisco, que enfatiza as percepções dos profissionais de segurança sobre o estado da segurança em suas empresas. Ao comparar os resultados da pesquisa de 2015 com os de 2014, a Cisco descobriu que os CSOs e os gerentes de operações de segurança (SecOps) têm menos certeza de que sua infraestrutura de segurança está atualizada ou que podem impedir ataques. No entanto, a pesquisa também indica um progresso das empresas que apostam em treinamento e outros processos de segurança para fortalecer suas redes. Os resultados do estudo são exclusivos do Relatório Anual de Segurança da Cisco de 2016.

UM OLHAR PARA O FUTURO

Esta seção apresenta uma perspectiva do panorama geopolítico que afeta a segurança. Discutimos as descobertas de dois estudos da Cisco: um que examina as preocupações dos executivos com a segurança digital, e outro que enfatiza as percepções dos tomadores de decisões de TI sobre o risco à segurança e confiabilidade. Também apresentamos uma atualização sobre nosso progresso para reduzir o tempo para detecção (TTD), e enfatizar a importância de migrar para uma arquitetura de defesa contra ameaças integrada como uma forma de combater ameaças.

Índice

Principais desenvolvimentos e descobertas

Principais desenvolvimentos e descobertas

Os criminosos cibernéticos aperfeiçoaram suas infraestruturas de back-end para realizar ataques com o objetivo de aumentar a eficiência e os lucros.

- A Cisco, com a ajuda da Level 3 Threat Research Labs e a colaboração do provedor de hospedagem Limestone Networks, identificou e planejou a maior operação de kit de exploração Angler nos Estados Unidos, que tinha como alvo 90.000 vítimas por dia e a geração de dezenas de milhões de dólares por ano para os agentes da ameaça por trás da campanha.
- O SSHPsychos (Group 93), um dos maiores botnets de negação de serviços distribuídos (DDoS) já vistos pelos pesquisadores da Cisco, foi significativamente enfraquecido pelos esforços combinados da Cisco e da Level 3 Threat Research Labs. Como o estudo de caso Angler mencionado acima, esse sucesso aponta para a importância da colaboração do setor para combater os invasores.
- As extensões mal-intencionadas de navegador são um problema comum e podem ser uma grande fonte de vazamento de dados para as empresas. Nós estimamos que mais de 85% das empresas estudadas foram afetadas por extensões mal-intencionadas de navegador.
- Os botnets conhecidos, como Bedep, Gamarue e Miuref, representaram a maioria das atividades de comando e controle de botnet a afetar um grupo de empresas que analisamos em julho de 2015.
- A análise de malwares validados como “sabidamente prejudiciais” pela Cisco descobriu que a maioria desses malwares, 91,3%, usa o Serviço de nomes de domínio (DNS) para realizar campanhas. Através de uma investigação retrospectiva das consultas de DNS, a Cisco descobriu resolvedores de DNS “falsos” em uso nas redes de clientes. Os clientes não sabiam que os resolvedores eram usados pelos seus funcionários como parte de sua infraestrutura de DNS.
- As vulnerabilidades do Adobe Flash continuam populares com os criminosos cibernéticos. Entretanto, os fornecedores de software reduzem o risco de exposição dos usuários a malware através da tecnologia Flash.
- Ao observar as tendências em 2015, nossos pesquisadores sugerem que o tráfego com criptografia HTTPS atingiu um ponto crítico: em breve, essa será a forma dominante de tráfego da Internet. Embora a criptografia possa ajudar a proteger os consumidores, ela também pode minar a eficácia dos produtos de segurança, o que dificulta o rastreamento de ameaças por parte da comunidade de segurança. Além desse desafio, alguns malwares podem iniciar comunicações criptografadas em um conjunto diversificado de portas.
- Os criminosos usam sites comprometidos criados pela famosa plataforma de desenvolvimento para Web WordPress para suas atividades criminosas. Com ela, esses criminosos podem direcionar os recursos de servidor e escapar da detecção.

- A infraestrutura está cada vez mais ultrapassada e isso deixa as empresas vulneráveis ao comprometimento. Nós analisamos 115.000 dispositivos Cisco na Internet e descobrimos que 92% dos dispositivos em nossa amostragem executavam software com vulnerabilidades conhecidas. Além disso, 31% dos dispositivos Cisco no campo incluído em nossa análise estão no "fim da venda" e 8% estão no "fim da vida útil".
- Em 2015, os executivos de segurança mostraram confiar menos em suas ferramentas e processos de segurança do que em 2014, de acordo com o Estudo comparativo de recursos de segurança da Cisco de 2015. Por exemplo, em 2015, 59% das empresas afirmaram que sua infraestrutura de segurança estava "muito atualizada". Em 2014, 64% disseram o mesmo. No entanto, suas preocupações crescentes com segurança os motivam a aprimorar suas formas de defesa.
- O estudo comparativo mostra que empresas de pequeno e médio porte (SMBs) usam menos formas de defesa do que as grandes empresas. Por exemplo, 48% das SMBs afirmaram em 2015 que utilizavam segurança da Web, em comparação com 59% em 2014. E 29% disseram que usaram correções de falhas e ferramentas de configuração em 2015, em comparação com 39% em 2014. Esses pontos fracos podem colocar os clientes de pequenas e médias empresas em risco, pois os invasores encontram mais facilidade para entrar nessas redes.
- Desde maio de 2015, a Cisco reduziu o tempo médio para detecção (TTD) de ameaças conhecidas em nossas redes para aproximadamente 17 horas, ou seja, menos de um dia. Isso supera muito a estimativa atual de TTD do setor, que é de 100 a 200 dias.

De olho no prêmio: para os criminosos cibernéticos modernos, ganhar dinheiro é fundamental

De olho no prêmio: para os criminosos cibernéticos modernos, ganhar dinheiro é fundamental

No passado, muitos criminosos on-line espreitavam escondidos na Internet. Na tentativa de burlar a detecção, eles faziam apenas incursões rápidas nas redes empresariais para iniciar suas explorações. Hoje, alguns criminosos cibernéticos ousados invadem recursos on-line legítimos. Eles minam a capacidade do servidor, roubam dados e sequestram informações exigindo resgate das vítimas on-line.

Essas campanhas apresentam uma elevação preocupante na guerra entre defensores e invasores. Caso os criminosos encontrem mais locais on-line como base para operações, seu impacto poderá crescer exponencialmente.

Neste relatório, os pesquisadores de segurança da Cisco destacam as táticas que os autores de ameaças usam na criação de uma infraestrutura sólida para tornar suas campanhas mais fortes e eficazes. Os criminosos adotam métodos cada vez mais eficientes para aumentar seus lucros. Muitos deles prestam atenção especial ao aproveitamento de recursos de servidor.

A explosão de ransomware (consulte a **página 10**) é um bom exemplo. O ransomware fornece aos criminosos um método fácil para a retirada de mais dinheiro diretamente dos usuários. Quando os criminosos estabelecem campanhas que comprometem dezenas de milhares de usuários por dia com pouca ou nenhuma interrupção, a recompensa por seus esforços pode ser surpreendente. Além de desenvolver melhores formas de monetizar suas campanhas, os invasores usam recursos legítimos como base.

Atualmente, os criadores de algumas variações de ransomware e os desenvolvedores de outras formas de exploração deslocam o tráfego para sites de WordPress invadidos, como uma forma de burlar a detecção e usar o espaço do servidor (consulte a **página 33**). E os perpetradores do SSHPsychos, um dos maiores botnets já vistos pelos pesquisadores da Cisco, operavam em redes padrão com pouca interferência até que uma parceria entre a Cisco e a Level 3 Threat Research Labs para derrubar esse esquema convenceu os provedores de serviços a bloquear o tráfego do criador do botnet.

Inteligência de ameaças

Inteligência de ameaças

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

Artigos

A colaboração do setor ajuda a Cisco no planejamento de um kit de exploração de longo alcance e altamente lucrativo e uma campanha de ransomware

O kit de exploração Angler é um dos maiores e mais eficientes do mercado. Ele foi associado a várias campanhas de alto perfil de malvertising (propaganda mal-intencionada) e de ransomware. E isso tem sido um fator importante na explosão geral da atividade de ransomware que nossos pesquisadores de ameaças têm monitorado de perto há vários anos. Os criminosos usam ransomware para criptografar arquivos de usuários, fornecendo as chaves para descriptografia apenas depois que os usuários pagam um "resgate", geralmente no valor de US$ 300,00 a US$ 500,00.

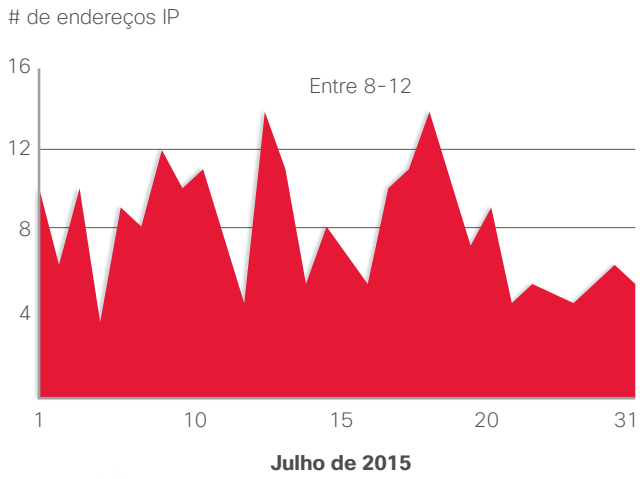
Conforme informado no Relatório Semestral de Segurança da Cisco de 2015, moedas criptografadas como bitcoin e redes de anonimização, como a Tor, facilitam a entrada dos criminosos no mercado de malware e começam a gerar receita rapidamente. O aumento da popularidade do ransomware pode estar associado a duas vantagens principais: é uma operação de baixa manutenção para os criminosos e oferece um caminho rápido para a monetização, porque os usuários pagam aos criminosos diretamente em moedas criptografadas.

Através da pesquisa do Angler e de tendências relacionadas de ransomware, a Cisco determinou que alguns operadores do kit de exploração usavam um percentual excessivo de servidores proxy no mundo para o Angler que estavam em servidores operados pela Limestone Networks. Esse uso de servidores é um exemplo básico de outra tendência que nossos pesquisadores têm observado na economia paralela: os criminosos combinam recursos legítimos e recursos mal-intencionados para realizar suas campanhas.

Nesse caso, a infraestrutura IP de suporte ao Angler não era grande. O número diário de sistemas ativos geralmente ficava entre 8 e 12. A maioria deles ficava ativa por apenas um dia. A figura 1 mostra o número de endereços IP exclusivos que a Cisco observou no mês de julho de 2015.

A Cisco descobriu que os operadores do Angler basicamente distribuem endereços IP de uma forma linear para ocultar a atividade de ameaça e evitar qualquer interrupção nos seus lucros.

Figura 1. Número de endereços IP Angler por data, julho de 2015



Fonte: Cisco Security Research

COMPARTILHAR

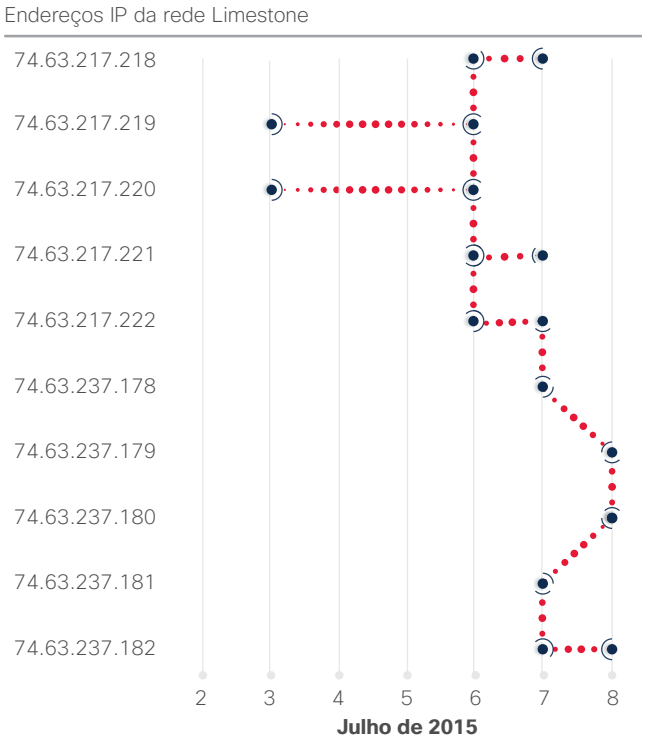
Como mostra a figura 2, o Angler começa com um endereço IP (aqui, 74.63.217.218). Conforme o sistema compromete os usuários e gera "ruído" detectável pelos defensores, os criminosos mudam para um endereço IP adjacente (74.63.217.219). Essa atividade continua através de blocos quase contíguos de espaço IP de um único provedor de hospedagem.

A Cisco examinou as informações de IP para identificar os números de sistemas autônomos (ASNs) e os provedores associados aos endereços IP. Determinamos que a maior parte do tráfego relacionado ao Angler vinha de servidores operados por dois provedores de hospedagem legítimos: Limestone Networks e Hetzner (figura 3). Eles foram responsáveis por quase 75% do volume geral do tráfego do mês de julho.

A Cisco acessou primeiro a Limestone Networks, que parecia hospedar a maior porção global do Angler. A Limestone aceitou a oportunidade de colaborar. A empresa teve que lidar com excessivos estornos de cartões de crédito a cada mês, porque os criminosos usavam nomes e cartões de crédito fraudulentos para comprar lotes aleatórios de seus servidores que valiam milhares de dólares.

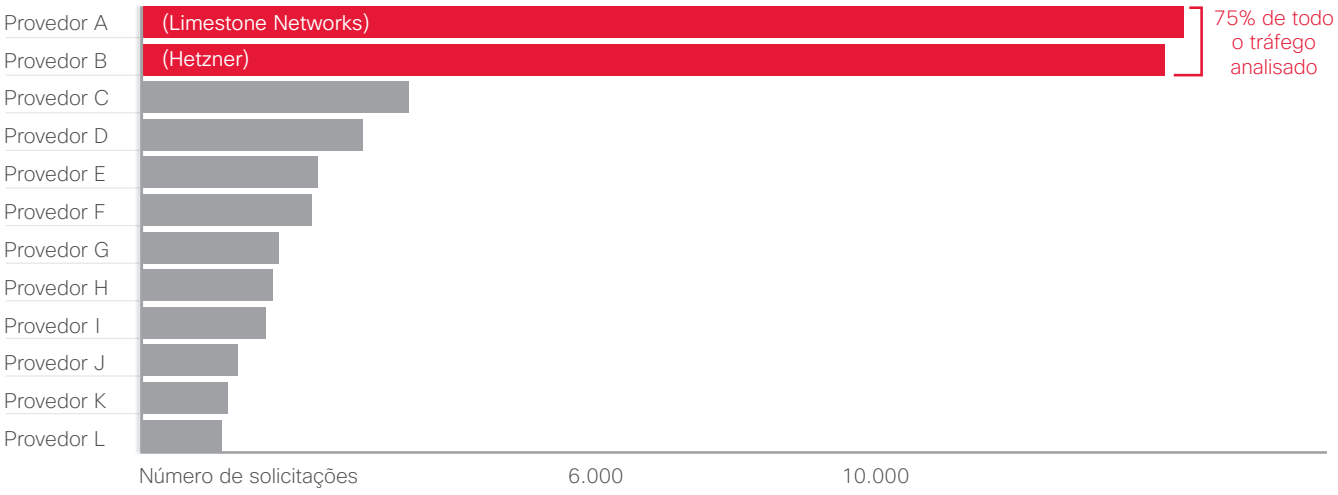
COMPARTILHAR

Figura 2. Baixa infraestrutura de IP que oferece suporte ao Angler



Fonte: Cisco Security Research

Figura 3. Solicitações HTTP do Angler por provedor, julho de 2015



Fonte: Cisco Security Research

A abordagem dos criminosos para a compra de servidores dificultava a associação da atividade fraudulenta a um único criminoso. Por exemplo, o autor de uma fraude podia comprar três ou quatro servidores em um dia, e depois usar outro nome e cartão de crédito para comprar três ou quatro servidores no dia seguinte. Dessa forma, eles podiam basicamente passar de um endereço IP para o próximo quando os servidores comprometidos fossem identificados e desconectados pelos defensores.

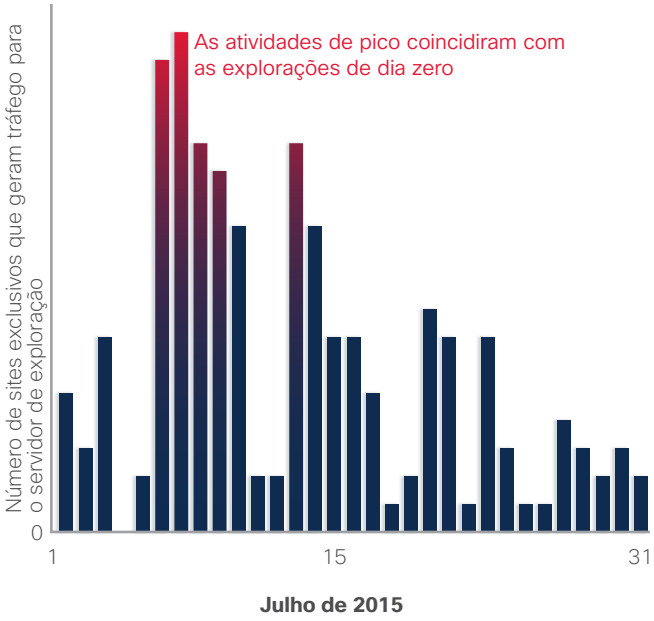
Para investigar essa atividade, a Cisco solicitou a ajuda da Level 3 Threat Research Labs, bem como da OpenDNS, uma empresa da Cisco. A Level 3 Threat Research Labs pôde fornecer um insight global mais amplo sobre a ameaça, permitindo à Cisco analisar mais profundamente o escopo da ameaça e seu alcance nos momentos de pico. Enquanto isso, a OpenDNS proporcionou uma visão exclusiva da atividade de domínio associada à ameaça. Com isso, a Cisco obteve uma compreensão maior do modo como técnicas como sombreamento de domínio eram incorporadas pelos criminosos.

Em seguida, os pesquisadores de ameaças da Cisco analisaram como, especificamente, os usuários encontravam o Angler e depois recebiam cargas mal-intencionadas. Os pesquisadores observaram que sites populares redirecionavam os usuários para o kit de exploração Angler através de malvertising. Os anúncios falsos eram colocados em centenas de sites de notícias importantes, sites de imóveis e de cultura popular. Esses tipos de sites geralmente são referenciados na comunidade de segurança como sites "sabidamente válidos".

Além disso, os pesquisadores de ameaças da Cisco encontraram inúmeros exemplos de pequenos sites aparentemente aleatórios executando o mesmo tipo de redirecionamento, inclusive o obituário de uma pessoa em um pequeno jornal rural nos Estados Unidos. Muito provavelmente, esta última estratégia foi criada visando pessoas idosas. Em geral, pessoas idosas apresentam maior probabilidade de usar navegadores da Web padrão, como o Microsoft Internet Explorer, e menor probabilidade de saber da necessidade de corrigir regularmente as vulnerabilidades do Adobe Flash.

Outro aspecto notável dessa operação do Angler foi o volume de referenciais exclusivos e a baixa frequência com a qual foram usados (figura 4). Descobrimos mais de 15.000 sites exclusivos para atrair pessoas para o kit de exploração Angler, 99,8% dos quais foram usados menos de 10 vezes. Assim, a maioria dos referenciais esteve ativa apenas por um breve período e foram removidos depois de direcionados a alguns usuários. Em nossa análise de julho de 2015, observamos que os picos de atividade coincidiram com as várias explorações de dia zero da Hacking Team (CVE-2015-5119, CVE-2015-5122).[1]

Figura 4. Referenciais exclusivos por dia, julho de 2015



Fonte: Cisco Security Research

A Cisco determinou que cerca de 60% das cargas do Angler fornecidas através dessa operação em particular entregavam algum tipo de variação de ransomware, sendo a maioria o Cryptowall 3.0. Outros tipos de cargas incluíram o Bedep, uma ferramenta de download de malware geralmente usada para instalar um malware de campanha de fraudes de cliques. (Consulte "Infecções de navegador: disseminadas – e uma grande fonte de vazamento de dados", na **página 16**.) Ambos os tipos de malware foram projetados para ajudar os criminosos a ganhar muito dinheiro dos usuários afetados muito rápido, e com pouco ou nenhum esforço.

[1] "Adobe Patches Hacking Team's Flash Player Zero-Day" de Eduard Kovacs, *SecurityWeek*, 8 de julho de 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Receitas do Angler

147 servidores de redirecionamento por mês

90K destinos por servidor por dia

10% explorações servidas

40% comprometidos

62% ransomware entregue

2,9% de resgates pagos

X **$300** média de resgate = **$34M** renda anual bruta do ransomware por campanha

9515 usuários pagam resgates por mês

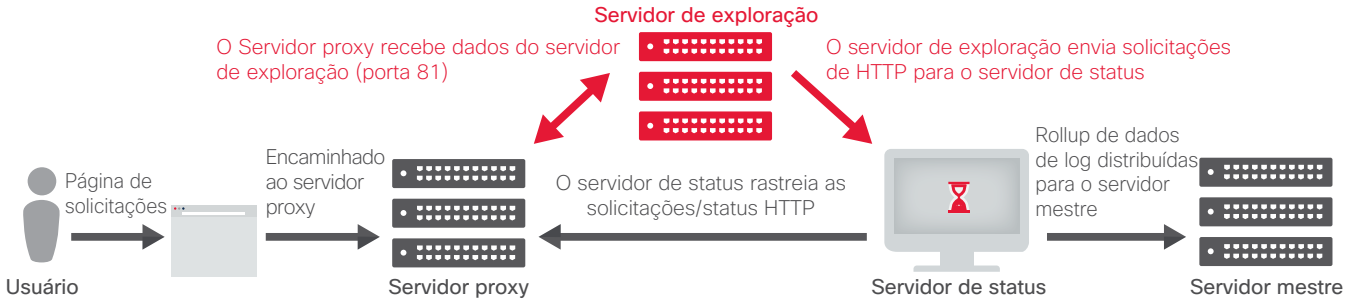
Fonte: Cisco Security Research

De acordo com a pesquisa da Cisco, o principal agente responsável por cerca de metade da atividade do kit de exploração do Angler nesta campanha em particular tinha o objetivo de atingir 90.000 vítimas por dia. Pela nossa estimativa, a campanha geraria para os criminosos mais de US$ 30 milhões por ano.

COMPARTILHAR

Tudo indicava que a rede da Hetzner tinha uma taxa de sucesso semelhante. Isso significa que o agente de ameaça por trás da operação que envolve os servidores da Limestone Networks e da Hetzner foi responsável por metade de toda a atividade global do Angler na época da análise da Cisco. Os pesquisadores da Cisco estimam que esta operação foi capaz de gerar uma renda bruta de US$ 60 milhões por ano.

Figura 5. Infraestrutura de back-end do Angler



Fonte: Cisco Security Research

A Cisco também descobriu que os servidores aos quais os usuários se conectavam não hospedavam realmente nenhuma das atividades mal-intencionadas do Angler. Eles serviam como condutores. Um usuário entraria na cadeia de redirecionamento e enviaria uma requisição GET para uma página inicial, que levaria ao servidor proxy. O servidor proxy encaminharia o tráfego a um servidor de exploração em outro país, em um provedor diferente. Durante nossa pesquisa, descobrimos que um único servidor de exploração estava associado a vários servidores proxy. (Veja a Figura 5).

A Cisco identificou um servidor de status que controlava tarefas como o monitoramento de integridade. Cada servidor proxy exclusivo que o servidor de status monitorou tinha um par de URLs individuais. Se o caminho fosse consultado, o servidor de status retornaria uma mensagem de código de status "204". Os criminosos podem identificar de modo exclusivo cada servidor proxy e verificar não só se ele estava funcionando, bem como se os defensores não tinham feito nenhuma alteração nele. Com o uso do outro URL, os invasores podem coletar os logs do servidor proxy e determinar o grau de eficiência de funcionamento da rede.

A colaboração do setor foi um componente essencial na capacidade da Cisco de investigar a atividade do kit de exploração do Angler. Definitivamente, isso colaborou na interrupção dos redirecionamentos para servidores proxy do Angler em um provedor de serviços dos EUA e na conscientização sobre uma operação de crime digital altamente sofisticada que afetava milhares de usuários todos os dias.

COMPARTILHAR

A Cisco trabalhou em parceria com a Limestone Networks para identificar novos servidores conforme eram colocados on-line e os monitorou atentamente para assegurar que fossem inativados. Depois de algum tempo, os criminosos se afastaram da Limestone Networks, e houve uma queda global na atividade do Angler.

Para obter mais informações sobre como a Cisco interrompeu um fluxo significativo de receita internacional gerado pelo kit de exploração do Angler, leia a postagem no blog Cisco Security "**Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone.**"

O esforço coordenado do setor ajuda a derrotar um dos maiores botnets DDoS da Internet

Com frequência, as tecnologias integradas de defesa contra ameaças podem impedir grandes ataques antes que eles afetem as redes empresariais. No entanto, em muitos casos, para impedir um ataque potencialmente grande, não só são necessárias defesas tecnológicas, como também coordenação entre os provedores de serviços, os fornecedores de segurança e os grupos do setor.

À medida que os criminosos ficam cada vez mais preocupados em monetizar suas atividades, o setor de tecnologia precisa melhorar o trabalho de parceria para impedir as campanhas dos criminosos. O SSHPsychos (também denominado Group 93), um dos maiores botnets de DDoS já observados pelos pesquisadores de segurança da Cisco, foi significativamente enfraquecido depois da colaboração entre a Cisco e a Level 3 Threat Research Labs.

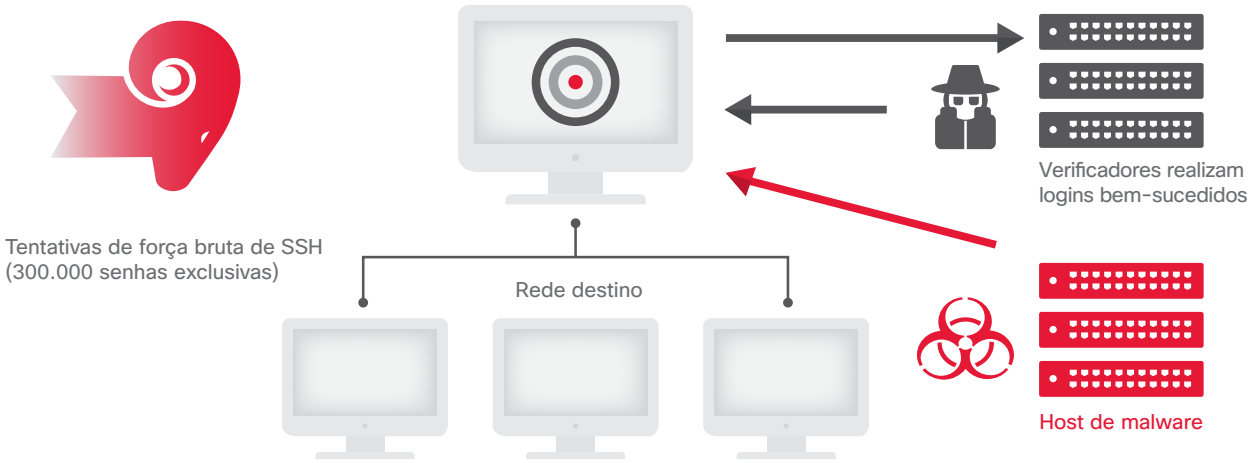
AMEAÇA INIGUALÁVEL

A rede de DDoS do SSHPsychos é uma ameaça inigualável por vários motivos. Como afeta dezenas de milhares de máquinas distribuídas na Internet, ela tem o poder de iniciar um ataque de negação de serviços distribuídos (DDoS) que não pode enviado para um dispositivo de cada vez. Nesse caso, o botnet era criado com o uso de ataques de força bruta que envolviam tráfego de shell seguro (SSH) (figura 6). O protocolo SSH é usado para permitir as comunicações seguras, e geralmente é empregado para a administração remota de sistemas. De acordo com a análise da Cisco e da Level 3, às vezes, o SSHPsychos era responsável por mais de 35% de todo o tráfego de SSH global da Internet (figura 7).

O SSHPsychos opera em dois países: China e Estados Unidos. São feitas tentativas de login de força bruta, com o uso de 300.000 senhas exclusivas, originadas de um provedor de hospedagem sediado na China. Quando os criminosos conseguiam adivinhar a senha correta para fazer login, os ataques de força bruta terminavam. Vinte e quatro horas depois, os criminosos se conectavam de um endereço IP nos EUA e instalavam um rootkit de DDoS na máquina afetada. Essa era claramente uma tática para reduzir a suspeita dos administradores de rede. Os alvos de botnet variavam, mas em muitos casos pareciam ser grandes provedores de serviços de Internet (ISPs).

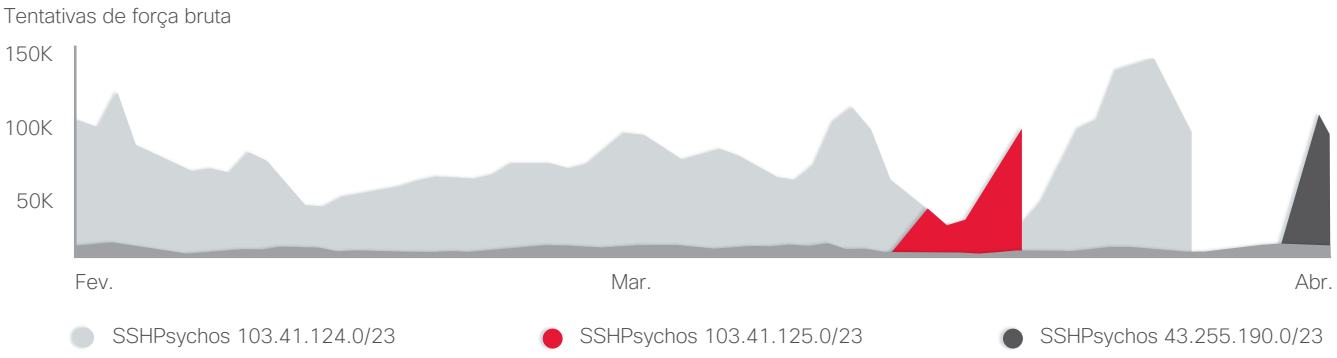
COMPARTILHAR

Figura 6. SSHPsychos usa ataques de força bruta



Fonte: Cisco Security Research

Figura 7. Em seu pico, o SSHPsychos foi responsável por 35% do tráfego global da Internet



Fonte: Cisco Security Research

COLABORAÇÃO COM OS ESPECIALISTAS EM SEGURANÇA

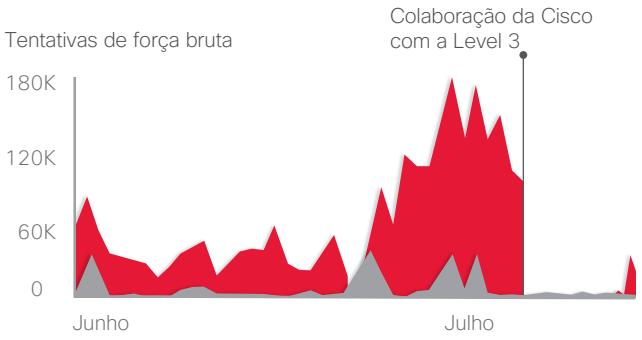
Devido à escala da rede de DDoS, nossos pesquisadores acreditavam que os danos fossem de difícil contenção. Era essencial trabalhar lado a lado com uma empresa que pudesse remover o grupo de força bruta da Internet com eficiência. Entretanto, os provedores de backbone hesitam em filtrar o conteúdo de seus clientes.

A Cisco convidou a Level 3 Threat Research Labs. A Level 3 analisou o tráfego no bloco de rede, ou intervalo de endereços IP, em que se achava que o SSHPsychos residia (103.41.124.0/23). Isso confirmou que nenhum tráfego legítimo era originado desse endereço ou destinado a ele. Ele encaminhava o tráfego de rede dentro de suas próprias redes. Em seguida, contatava os provedores de serviços dos domínios relevantes para pedir que removessem o tráfego de rede.

Os resultados desse esforço eram observados imediatamente (figura 8). A rede original não mostrava quase nenhuma atividade. No entanto, uma nova rede no bloco de rede 43.255.190.0/23 mostrava grandes volumes de tráfego de ataque de força bruta de SSH. Ela tinha o mesmo comportamento associado ao SSHPsychos. Depois desse súbito ressurgimento de tráfego semelhante ao SSHPsychos, a Cisco e a Level 3 decidiram adotar ações contra 103.41.124.0/23, bem como o novo bloco de rede 43.255.190.0/23.

Tornar inativos os blocos de rede usados pelo SSHPsychos não desativava permanentemente a rede de DDoS. Entretanto, isso certamente desacelerava a capacidade de seus autores de executar suas operações, e impedia que o SSHPsychos se espalhasse para novas máquinas, pelo menos temporariamente.

Figura 8. O tráfego do SSHPsychos cai radicalmente após intervenção



Fonte: Cisco Security Research

À medida que os criminosos cibernéticos criam grandes redes de ataque, o setor de segurança precisa investigar maneiras de colaborar ao enfrentar uma ameaça como o SSHPsychos. Os principais provedores de domínios, ISPs, provedores de hospedagem, resolvedores de DNS e fornecedores de segurança não podem mais se omitir quando os criminosos on-line iniciam suas explorações nas redes destinadas a transportar apenas tráfego legítimo. Em outras palavras, quando os criminosos fornecem tráfego mal-intencionado de uma forma mais ou menos simples, o setor precisa remover as trajetórias mal-intencionadas dessas redes legítimas.

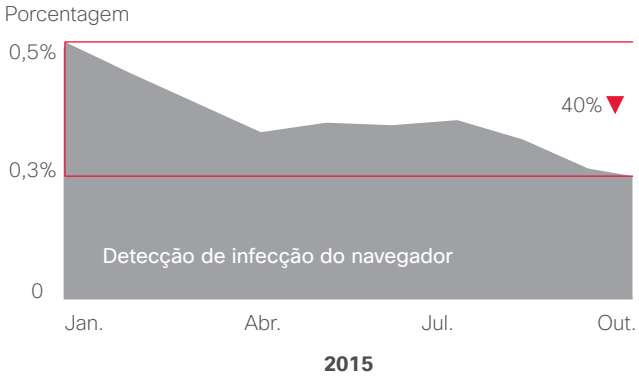
Para saber mais sobre a resposta da Cisco e da Level 3 Threat Research Labs à ameaça SSHPsychos, leia a postagem do blog Cisco Security "**Threat Spotlight: SSHPsychos.**"

Infecções do navegador: disseminadas– e uma grande fonte de vazamento de dados

Com frequência, as equipes de segurança veem os add-ons do navegador como uma ameaça de baixa severidade. Entretanto, elas devem fazer do monitoramento uma prioridade mais alta para que possam identificar rapidamente e atenuar esses tipos de infecções.

O motivo da urgência: nossa pesquisa indica que as infecções do navegador apresentam uma predominância muito maior do que muitas empresas imaginam. De janeiro a outubro de 2015, examinamos 26 famílias de add-ons de navegador mal-intencionados (figura 9). Ao analisar o padrão de infecções de navegador durante esses meses, foi possível perceber que o número de infecções parecia apresentar uma queda geral.

Figura 9. Infecções do navegador, janeiro a outubro de 2015



Fonte: Cisco Security Research

No entanto, esse padrão é enganoso. O volume crescente de tráfego HTTPS nesses meses dificultou a identificação dos indicadores de comprometimento geralmente associados às 26 famílias que acompanhamos, pois as informações de URL não estavam visíveis devido à criptografia. (Para saber mais sobre criptografia e os desafios criados por ela para os defensores, consulte "Criptografia: uma tendência crescente e um desafio para os defensores", na **página 30**.)

As extensões mal-intencionadas de navegador podem roubar informações e elas podem ser uma grande fonte de vazamento de dados. Cada vez que um usuário abre uma nova página da Web com um navegador comprometido, as extensões mal-intencionadas de navegador coletam dados. Elas extraem mais do que os detalhes básicos sobre cada página da Web interna ou externa que o usuário visita. Elas também coletam informações altamente confidenciais inseridas no URL. Essas informações podem incluir credenciais de usuário, dados do cliente e detalhes sobre as APIs internas e a infraestrutura de uma empresa.

As extensões mal-intencionadas multiuso de navegador são entregues por pacotes de software ou adware. Elas são projetadas para obter receita através da exploração de usuários de várias maneiras. Em um navegador afetado, elas podem levar os usuários a clicar em malvertising, como anúncios ou pop-ups. Elas também podem distribuir malware ao levar os usuários a clicar em um link comprometido ou fazer download de um arquivo infectado encontrado em malvertising. E podem sequestrar as solicitações de navegador dos usuários e injetar páginas da Web mal-intencionadas nas páginas dos resultados do mecanismo de pesquisa.

Nas 45 empresas que compõem nossa amostra, determinamos que em cada mês mais de 85% delas foram afetadas por extensões mal-intencionadas de navegador. Uma descoberta que enfatiza a escala massiva dessas operações. Como os navegadores infectados frequentemente são considerados uma ameaça relativamente menor, elas podem levar dias para serem detectadas ou resolvidas ou até mesmo semanas. Isso dá aos criminosos mais tempo e oportunidade para realizar suas campanhas (consulte "Tempo para detecção: a corrida para continuar limitando a janela," **página 60**).

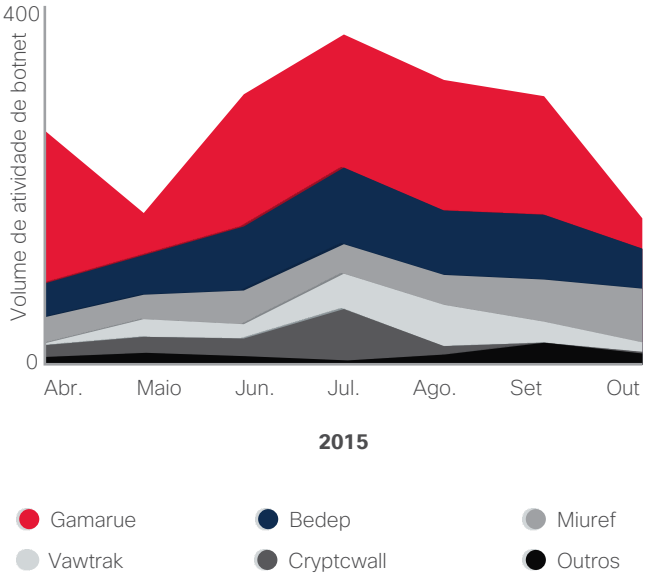
Por isso, sugerimos que vale a pena para as equipes de segurança dedicarem mais tempo e esforço ao monitoramento desse risco, e considerarem o maior uso da automação para ajudar a priorizar as ameaças.

Comando e controle de botnet: um resumo global

Os botnets são redes de computadores infectados por malware. Os criminosos podem controlá-los como um grupo e ordenar que executem uma tarefa específica, como o envio de spam ou o início de um ataque de DDoS. Eles têm crescido em tamanho e número há anos. Para entender melhor o panorama atual de ameaças em uma escala global, analisamos as redes de 121 empresas, de abril a outubro de 2015, para obter evidências de um ou mais dos oito botnets comumente observados. Os dados foram normalizados para fornecer um resumo da atividade de botnet (figura 10).

Durante esse período, descobrimos que o Gamarue, um ladrão de informações modular e multiuso que existe há anos, era a ameaça de comando e controle mais comum.

Figura 10. Crescimento de ameaças individuais (proporção de usuários infectados)



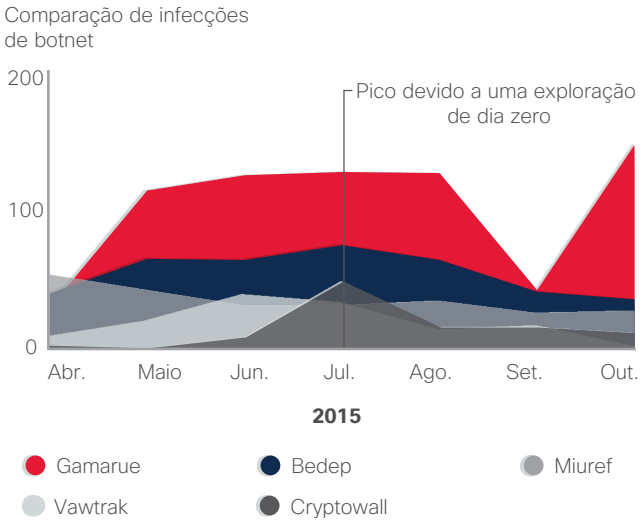
Fonte: Cisco Security Research

Um aumento significativo no número de infecções envolveu o ransomware Cryptowall 3.0, que foi identificado em julho. Essa atividade é amplamente atribuída ao kit de exploração Angler, que como se sabe, solta a carga Cryptowall. Conforme relatado no Relatório Semestral de Segurança da Cisco de 2015, os autores do Angler e de outros kits de exploração foram rápidos em explorar as "lacunas de correções de falha" com o Adobe Flash. O tempo entre o lançamento pela Adobe de uma atualização e quando os usuários realmente fazem a atualização.[2] Os pesquisadores de ameaças da Cisco atribuem o pico de julho de 2015 à exploração de dia zero do Flash, CVE-2015-5119, que foi exposta como parte dos vazamentos da Hacking Team.[3]

O kit de exploração Angler também entrega o Cavalo de Troia Bedep, que é usado para executar campanhas de fraudes de cliques. Um ligeiro aumento no predomínio dessa ameaça também foi observado em julho (figura 11).

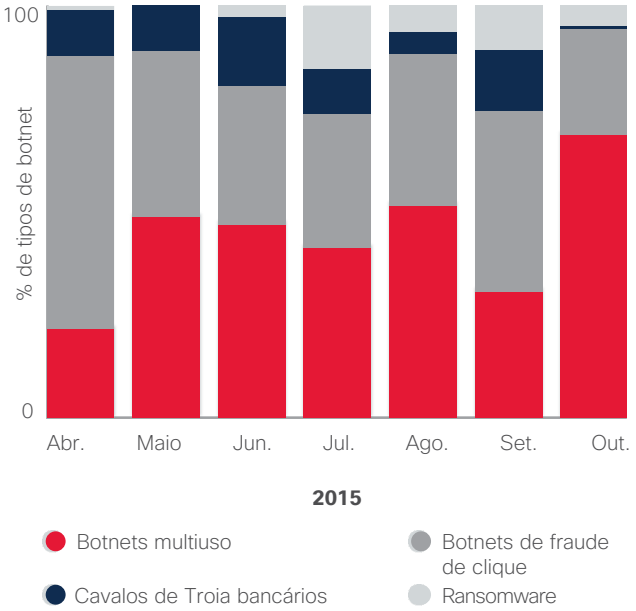
O Bedep, o Gamarue e o Miuref (outro Cavalo de Troia e sequestrador de navegador que pode executar fraudes de cliques) juntos representaram mais de 65% da atividade de comando e controle de botnet na base de usuários que analisamos.

Figura 11. Cobertura mensal de ameaças, com base no número de usuários infectados



Fonte: Cisco Security Research

Figura 12. Cobertura mensal de ameaças, com base nas categorias de ameaças



Fonte: Cisco Security Research

O percentual de infecções pelo Bedep permaneceu relativamente estável durante nosso período de análise. No entanto, foi observada uma redução nas infecções por Miuref. Nós atribuímos isso ao aumento no tráfego HTTPS, o que ajudou a ocultar os indicadores de comprometimento do Miuref.

A figura 12 mostra os tipos de botnets que foram responsáveis pela maioria das infecções durante o período em que monitoramos. Os botnets multiuso, como Gamarue e Sality, lideram o grupo, seguidos pelos botnets de fraudes de cliques. Os Cavalo de Troia bancários vieram em terceiro lugar, o que mostra que esse tipo de ameaça, embora antigo, ainda é bastante difundido.

COMPARTILHAR

[2] Relatório Semestral de Segurança da Cisco de 2015: **http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html**.
[3] "Adobe Patches Hacking Team's Flash Player Zero-Day," de Eduard Kovacs, *SecurityWeek*, 8 de julho 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day.**

O ponto cego de DNS: ataques com DNS para comando e controle

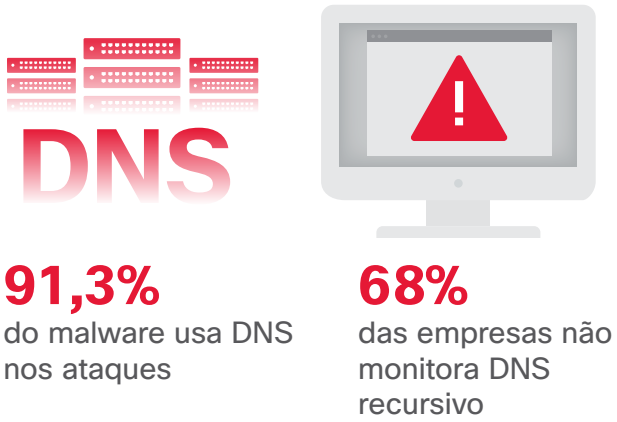
A análise de malwares validados como "sabidamente prejudiciais" pela Cisco descobriu que a maioria desses malwares, 91,3%, usa o Serviço de nomes de domínio de uma destas três maneiras:

- Para obter comando e controle
- Para extrair dados
- Para redirecionar o tráfego

Para chegar a esse percentual, analisamos todos os comportamentos de amostragem de várias sandboxes que temos. Os malwares que não usassem DNS de nenhuma forma, ou que usassem DNS simplesmente para realizar "verificações de integridade" da Internet eram removidos da amostra para análise. Os malwares restantes usavam DNS para se conectar a sites que eram considerados ruins ou suspeitos.

Apesar da confiança dos criminosos no DNS para ajudar nas campanhas de malware, poucas empresas monitoram o DNS para fins de segurança (ou nem monitoram o DNS). Essa falta de supervisão faz do DNS um caminho ideal para os invasores. De acordo com uma pesquisa recente que realizamos (consulte a figura 13), 68% dos profissionais de segurança relatam que suas empresas não monitoram ameaças de DNS recursivo. (Os servidores de nomes de DNS recursivo fornecem os endereços IP de nomes de domínio pretendidos para os hosts solicitantes.)

Figura 13. Monitoramento de ameaças de DNS recursivo



Fonte: Cisco Security Research

Por que o DNS é um ponto cego de segurança para tantas empresas? O principal motivo é que as equipes de segurança e os especialistas em DNS geralmente trabalham em grupos de TI diferentes em uma empresa e não interagem com frequência.

Mas deveriam. O monitoramento de DNS é essencial para identificar e conter as infecções por malware que já usam DNS para uma das três atividades listadas anteriormente. Também é uma primeira etapa importante no mapeamento de outros componentes que podem ser usados para investigar um ataque mais detalhadamente, da determinação do tipo de infraestrutura que apoia o ataque à descoberta de sua origem.

No entanto, o monitoramento de DNS usa mais do que a colaboração entre as equipes de segurança e de DNS. Isso exige o alinhamento da tecnologia e dos conhecimentos certos para a análise de correlação. (Para obter mais insight, consulte "A colaboração do setor ajuda a Cisco a contornar um kit de exploração de longo alcance e altamente lucrativo e uma campanha de ransomware" na **página 10**, para saber como a OpenDNS ajudou a Cisco a obter mais visibilidade de domínio para os IPs usados pelo Kit de exploração Angler.)

ANÁLISE RETROSPECTIVA DE DNS

A investigação retrospectiva da Cisco das consultas de DNS e do tráfego de TCP e UDP subsequente identifica algumas origens de malware. Isso inclui servidores de comando e controle, sites e pontos de distribuição. A investigação retrospectiva também detecta conteúdo com ameaças ao usar a inteligência de listas de ameaças, relatórios de ameaças da comunidade, tendências observadas nos comprometimentos digitais e conhecimento das vulnerabilidades exclusivas enfrentadas por um segmento de cliente.

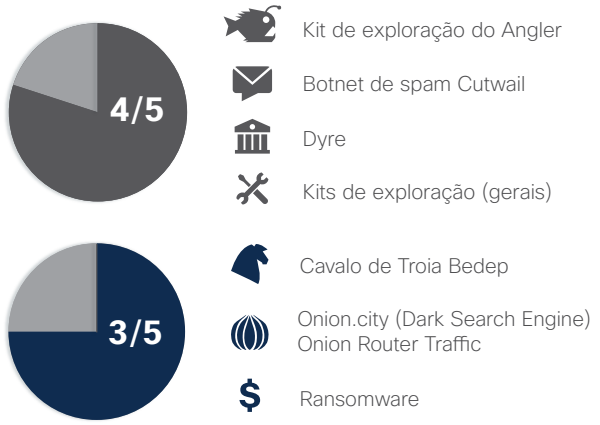
Nosso relatório retrospectivo ajuda a identificar tentativas de extração de dados "baixas e lentas" geralmente associadas ao comportamento de ameaças avançadas persistentes (APT) e que, em muitos casos, não é capturado pelas tecnologias tradicionais de detecção de ameaças. O objetivo da análise é identificar anomalias dentro da vasta quantidade de tráfego de comunicações de saída. Essa abordagem de "dentro para fora" pode revelar possíveis comprometimentos de dados e atividade de rede prejudicial que podem passar despercebidos.

É assim que descobrimos falsos resolvedores de DNS usados nas redes de clientes. Os clientes não sabiam que os resolvedores eram usados pelos seus funcionários como parte de sua infraestrutura de DNS. Se você não gerenciar e monitorar ativamente o uso de resolvedores de DNS, isso poderá causar comportamentos mal-intencionados, como envenenamento de cache de DNS e redirecionamento de DNS.

Além de descobrir e identificar resolvedores falsos de DNS, a investigação retrospectiva também revelou os seguintes problemas nas redes dos clientes:

- O espaço de endereço de cliente encontrado em spams de terceiros e listas de bloqueio de malware
- O sinalizador de espaço de endereço de cliente para servidores de comando e controle Zeus e Palevo conhecidos
- Campanhas de malware ativas, inclusive CTB-Locker, Angler e DarkHotel
- Atividade suspeita, inclusive o uso de Tor, encaminhamento automático de e-mails e conversão de documentos on-line
- Encapsulamento de DNS difundido para domínios registrados chineses
- "Typosquatting"[4] de DNS
- Clientes internos que ignoram a infraestrutura de DNS confiável do cliente

Quando examinamos uma amostra selecionada de clientes do Cisco Custom Threat Intelligence em vários verticais, também descobrimos os seguintes tipos de malware no respectivo percentual do total de clientes examinados:



[4] Typosquatting é o ato de registrar um nome do domínio que é semelhante a um nome do domínio atual; essa é uma estratégia usada pelos criminosos para atingir usuários que acidentalmente digitam nomes de domínio de modo incorreto.

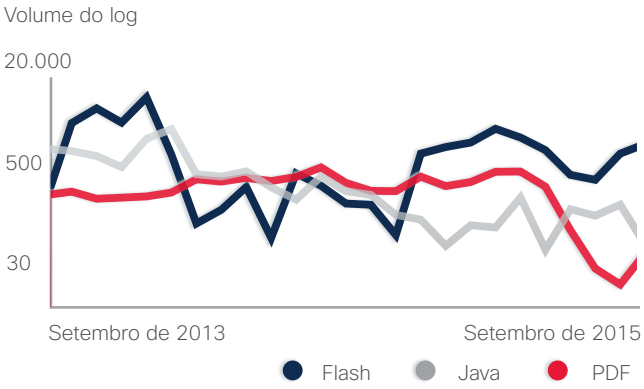
Análise de inteligência de ameaças

Vetores de ataque da Web

ADOBE FLASH: A CAMINHO DA SAÍDA, EVENTUALMENTE

Apesar do fato do volume geral de Flash ter diminuído no ano passado (consulte a próxima seção, "**Tendências de conteúdo de Adobe Flash e PDF**"), ele ainda é uma ferramenta preferencial dos desenvolvedores de kits de exploração. Na verdade, não houve uma tendência perceptível de aumento ou redução do malware Flash em 2015 (figura 14). O malware relacionado ao Flash provavelmente continuará um vetor primário de exploração por algum tempo: é importante ressaltar que os autores do kit de exploração Angler têm como objetivo principal as vulnerabilidades do Flash.

Figura 14. Compartilhamento de vetores de ataque - comparação de 2 anos



Fonte: Cisco Security Research

A pressão do setor para remover o Adobe Flash da experiência de navegação leva a uma redução na quantidade de conteúdo em Flash na Web (consulte a próxima seção, **"Tendências de conteúdo de Adobe Flash e PDF"**). Isso é semelhante ao que foi visto com o conteúdo Java nos últimos anos e que, por sua vez, levou a uma tendência regular de queda no volume de malware em Java. (Na verdade, os autores do Angler nem mesmo se incomodam mais em incluir explorações de Java). Enquanto isso, o volume de malware em PDF permaneceu relativamente constante.

O uso do Microsoft Silverlight como vetor de ataque também diminuiu, pois muitos fornecedores interromperam o suporte para a API utilizada pelo Silverlight para integração nos navegadores. Muitas empresas estão deixando de usar o Silverlight, enquanto adotam tecnologias baseadas em HTML5. A Microsoft indicou que não há nenhuma versão nova do Silverlight em produção e atualmente só emite atualizações relacionadas à segurança.

TENDÊNCIAS DE CONTEÚDO DE ADOBE FLASH E PDF

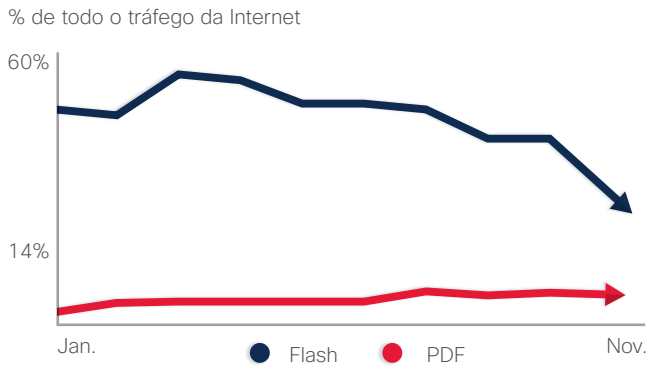
Os pesquisadores da Cisco têm observado uma queda geral na quantidade de conteúdo do Adobe Flash na Web (figura 15). As ações recentes da Amazon, Google e outros participantes importantes no espaço da Internet constituem um fator para a redução de conteúdo em Flash. Essas empresas não aceitam mais publicidade na Web que use Flash ou bloqueiam esse recurso.

Entretanto, o conteúdo em PDF permaneceu razoavelmente estável no ano passado e provavelmente continuará assim. Ele não é um vetor de ataque da Web importante há algum tempo.

A redução do conteúdo em Flash provavelmente continuará, e talvez sofra uma aceleração, a curto prazo, agora que a Adobe anunciou que encerrará o Flash.[5] Mas é provável que demore algum tempo até o conteúdo em Flash desaparecer. O Flash é integrado aos navegadores como Google Chrome, Microsoft Internet Explorer e Microsoft Edge e ainda é amplamente usado em conteúdos da Web, inclusive jogos e vídeos.

No entanto, nos próximos anos, à medida que novas tecnologias forem adotadas (como HTML5 e plataformas móveis), a tendência a longo prazo para vetores de ataque na Web como Java, Flash e Silverlight fica cada vez mais clara. Com o tempo, elas se tornarão menos comuns. Assim, é provável que se tornem vetores muito menos interessantes para criminosos voltados para o lucro, que se concentram em vetores que lhes permitem comprometer com facilidade grandes populações de usuários e gerar receita rapidamente.

Figura 15. Percentual de tráfego geral para Flash e PDF

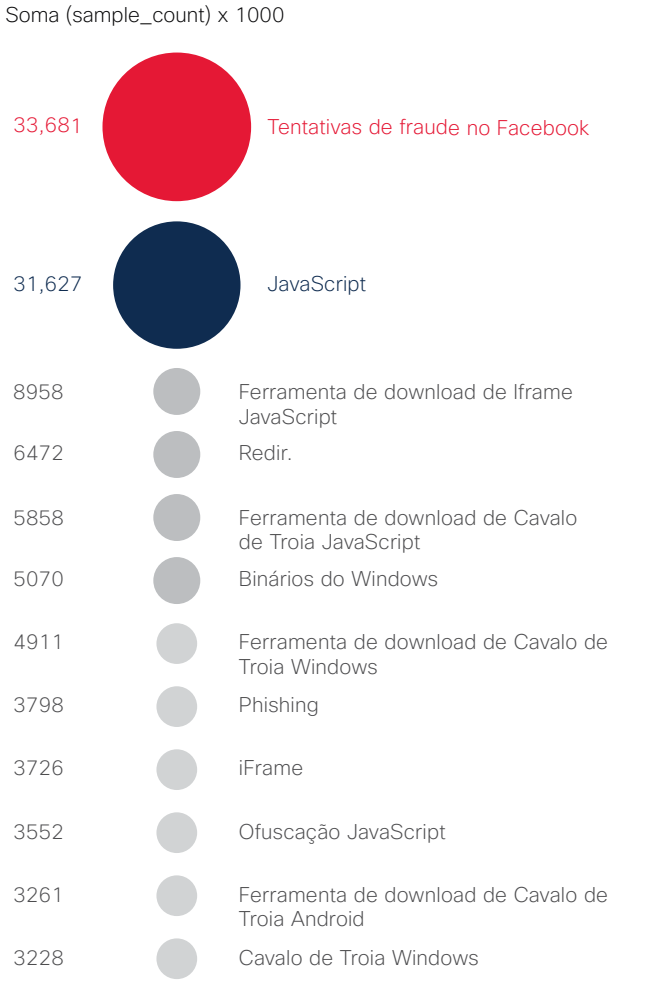


Fonte: Cisco Security Research

Métodos de ataque da Web

As figuras 16 e 17 mostram os diversos tipos de malware que os criminosos usam para acessar redes empresariais. A figura 16 mostra os tipos mais comumente observados de malware: adware, spyware, redirecionadores mal-intencionados, explorações de iFrame e phishing.

Figura 16. Malware observados com mais frequência



Fonte: Cisco Security Research

[5] "Adobe News: Flash, HTML5 and Open Web Standards," Adobe, 30 de novembro de 2015: **http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html**.

A figura 16 pode ser vista basicamente como um conjunto de tipos de malware que os criminosos usam para obter acesso inicial. Esses são os métodos testados, aprovados e mais econômicos de comprometer grandes populações de usuários com relativa facilidade. As explorações de JavaScript e as fraudes no Facebook (engenharia social) foram os métodos de ataque mais usados, de acordo com a nossa pesquisa.

A figura 17 mostra malware de menor volume. Observe que "volume menor" não significa "menos eficácia". De acordo com a Cisco Security Research, o malware de menor volume pode representar ameaças emergentes ou campanhas altamente direcionadas.

Muitas dessas técnicas mais sofisticadas foram projetadas para obter o maior valor possível dos usuários comprometidos. Eles roubam dados de alto valor ou sequestram ativos digitais para pedir resgate.

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

Figura 17. Exemplo de malware de menor volume observado

Fonte: Cisco Security Research

Atualizações de ameaças

LISTA DAS PRINCIPAIS VULNERABILIDADES DO ADOBE FLASH

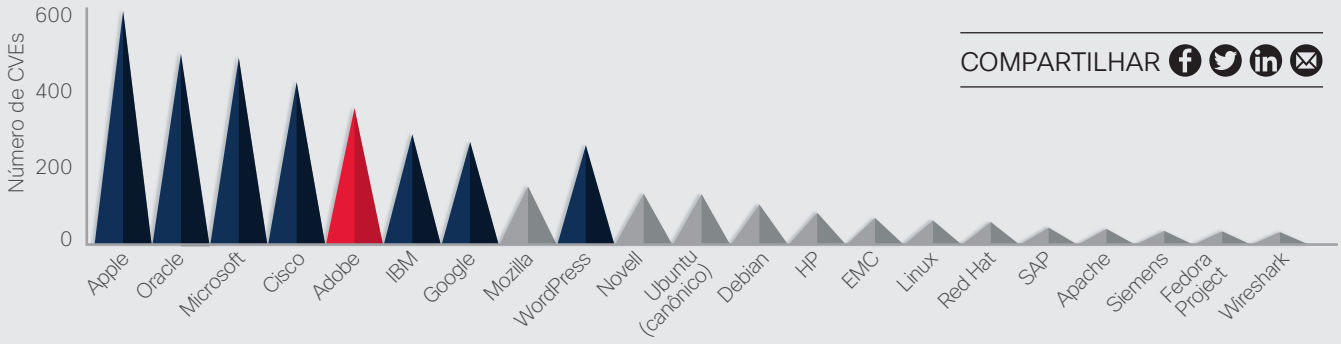
A plataforma Adobe Flash é um vetor de ataque popular para os criminosos há vários anos. As vulnerabilidades do Flash ainda aparecem com frequência nas listas de alertas de alta urgência. Em 2015, a boa notícia foi que os fornecedores de produtos nos quais essas explorações ocorrem comumente, como navegadores da Web, reconheceram essa vulnerabilidade e agora adotam ações para reduzir as oportunidades para os criminosos.

Em 2016, é mais provável que os criminosos se concentrem em explorações e ataques aos usuários do Adobe Flash. Algumas dessas vulnerabilidades do Flash têm explorações disponíveis on-line, publicamente ou para venda, como parte dos kits de exploração. (Conforme indicado na **página 21**, o volume de conteúdo relacionado ao Flash caiu, mas esse recurso ainda é um dos principais vetores de exploração.)

Acompanhando as táticas usadas para reduzir o impacto do Java, outro vetor comum de ameaças, muitos navegadores da Web bloqueiam o Flash ou usam sandbox como uma forma de proteger os usuários. Embora esse seja um desenvolvimento positivo, é importante lembrar que os invasores ainda conseguirão iniciar explorações por algum tempo. Pode ser que os usuários não consigam atualizar seus navegadores conforme necessário, e os criminosos continuarão a iniciar explorações que visam as versões mais antigas de software do navegador.

No entanto, os pesquisadores da Cisco acreditam que agora, as proteções integradas em alguns navegadores da Web e sistemas operacionais comumente usados reduzirão a confiança dos criminosos no Flash. Como os invasores on-line querem obter os melhores resultados possíveis (por exemplo, a alta lucratividade) para conquistar a maior eficiência, eles não se empenham tanto em ataques com menor probabilidade de fornecer um retorno no investimento.

Figura 18. Número total de CVEs por fornecedor



COMPARTILHAR

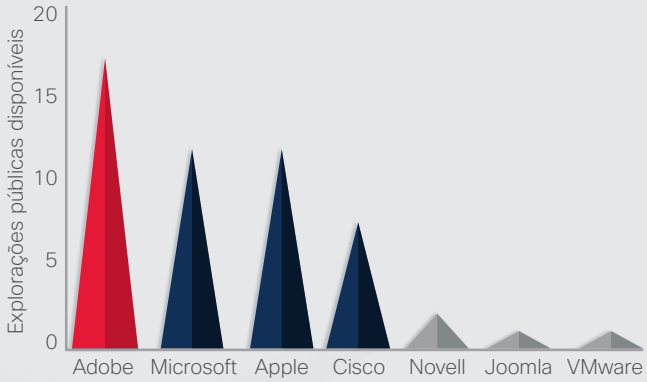
Fonte: Cisco Security Research, Banco de dados nacional de vulnerabilidade

O gráfico acima mostra o número total de CVEs publicados em 2015 por fornecedor. Observe que a Adobe não tem tanto destaque neste gráfico quanto no gráfico à direita, que mostra as vulnerabilidades para as quais há explorações disponíveis.

Além disso, o WordPress mostra apenas 12 vulnerabilidades em 2015 para seu próprio produto. As 240 vulnerabilidades adicionais vêm de plug-ins e scripts criados por terceiros.

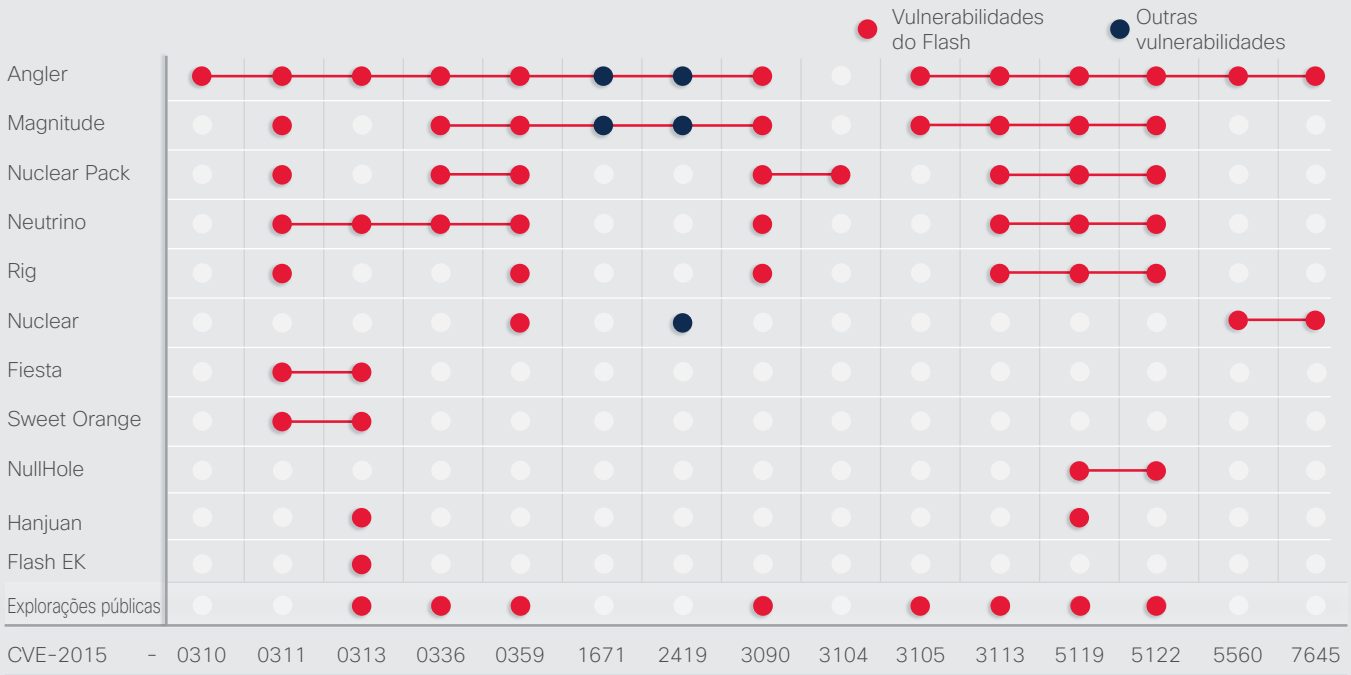
Conforme indicado na figura 20, listas de vulnerabilidades e explorações relacionadas podem fornecer orientação para profissionais de segurança. Eles podem usá-las para gerenciar e priorizar as vulnerabilidades de alto risco e as mais comuns e corrigi-las mais rapidamente do que as de baixo risco. Consulte o site de Detalhes de CVE **(https://www.cvedetails.com/top-50-products.php)** para obter mais informações sobre CVEs por fornecedor.

Figura 19. Número de explorações públicas disponíveis por vulnerabilidade de fornecedor



Fonte: Cisco Security Research, Metasploit, Exploit DB

Figura 20. Vulnerabilidades comuns



Fonte: Cisco Security Research

A figura 20 mostra vulnerabilidades de alto risco e indica se elas fazem parte de um kit de exploração para contratação (veja a linha "Flash EK") ou têm explorações publicamente disponíveis (veja a linha "Explorações públicas"). As vulnerabilidades para as quais explorações funcionais estão disponíveis são uma alta prioridade para correção de falhas.

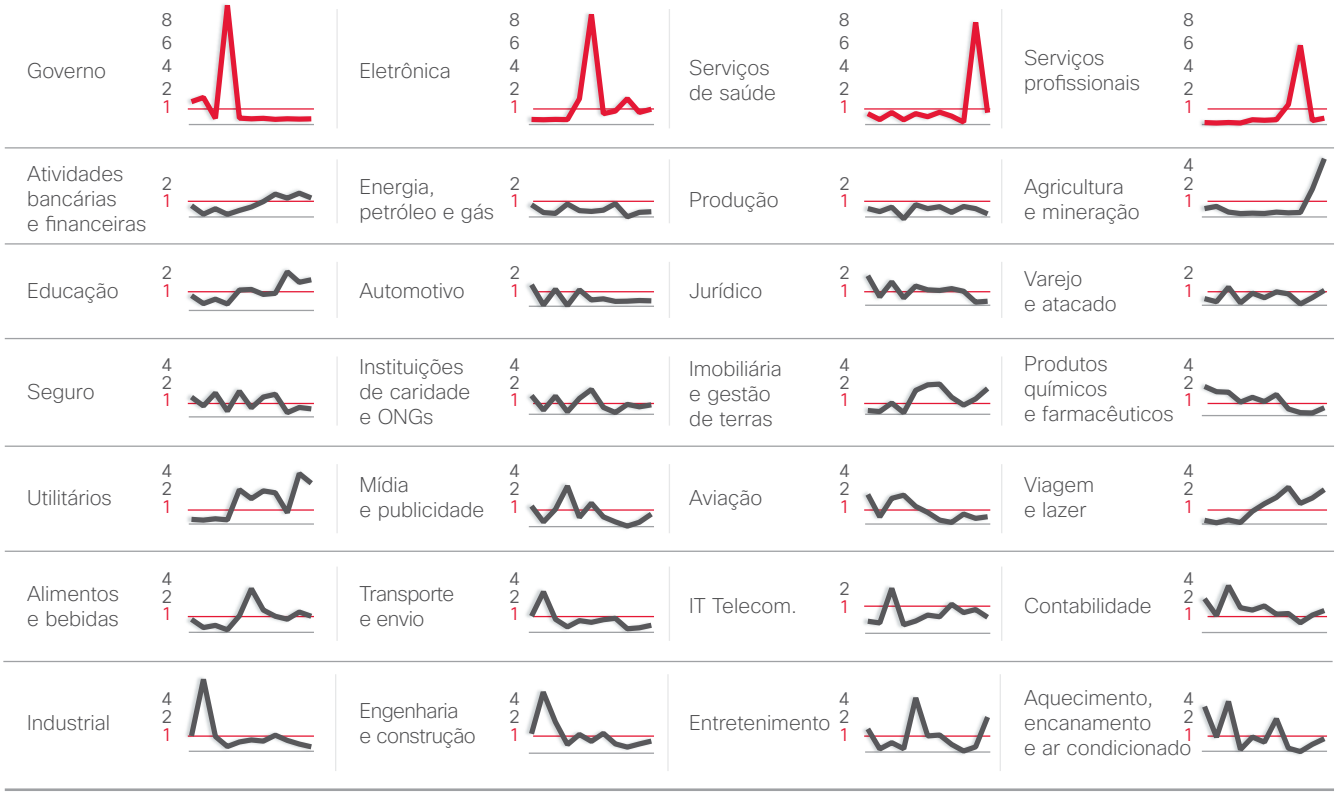
Essa lista pode ser usada para ajudar os profissionais de segurança a priorizar suas atividades de correção de falhas. A existência de uma exploração para um determinado produto, publicamente ou dentro de um kit de exploração, não indica necessariamente a ocorrência de ataques.

O risco vertical das descobertas de malware

Para rastrear verticais de alto risco para descobertas de malware da Web, examinamos os volumes relativos de tráfego de ataque ("taxas de bloqueio") e tráfego "normal" ou esperado.

A figura 21 mostra os 28 principais setores e sua atividade de bloqueio relativa como uma proporção do tráfego de rede normal. Uma proporção de 1,0 significa que o número de bloqueios é proporcional ao volume de tráfego observado. Qualquer coisa acima de 1,0 representa taxas de bloqueio maiores que o esperado, e qualquer coisa abaixo de 1,0 representa taxas de bloqueio menores que o esperado.

Figura 21. Taxas de bloqueio de verticais mensais, novembro de 2014 a setembro de 2015



Fonte: Cisco Security Research

A figura 22 mostra como o foco dos criminosos em verticais específicos pode ser passageiro. (Zero representa a ausência de mudanças globais.) De janeiro a março de 2015, o governo foi o vertical com a mais alta atividade de taxa de bloqueio. De março a maio, foi o setor de eletrônicos. No verão, os serviços profissionais experimentaram o maior número de bloqueios. E no outono de 2015, o setor de saúde foi o vertical com o maior número de taxas de bloqueio.

De acordo com a nossa pesquisa, os quatro verticais com a maior atividade de bloqueio em 2015 sofreram ataques relacionados a Cavalos de Troia. O vertical do governo também enfrentou um alto número de ataques de injeção de PHP, enquanto o vertical de serviços profissionais foi atingido por um alto número de ataques de iFrame.

Figura 22. Taxas de bloqueio relativas de verticais, comparação mês a mês

Fonte: Cisco Security Research

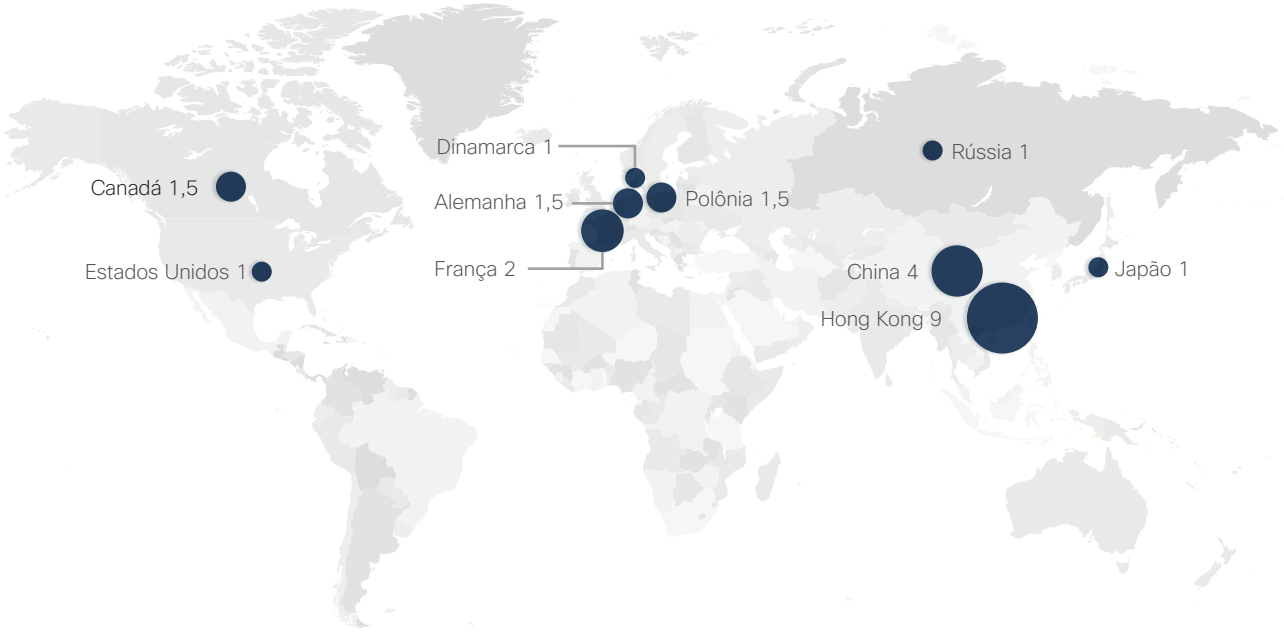
COMPARTILHAR

Atividade de bloqueio da Web: resumo geográfico

Também examinamos onde a atividade de bloqueio baseada em malware é originada por país ou região, conforme visto na figura 23. Os países foram selecionados para o estudo com base no seu volume de tráfego na Internet. Uma taxa de bloqueio de 1,0 indica que o número de bloqueios observados é proporcional ao tamanho da rede.

Países e regiões com atividade de bloqueio que consideramos mais alta que o normal provavelmente têm muitos hosts e servidores da Web com vulnerabilidades não corrigidas em suas redes. Agentes mal-intencionados não respeitam fronteiras de países e hospedarão o malware onde for mais eficiente.

Figura 23. Bloqueios da Web por país ou região



Atividade de bloqueio = tráfego mal-intencionado/tráfego previsto

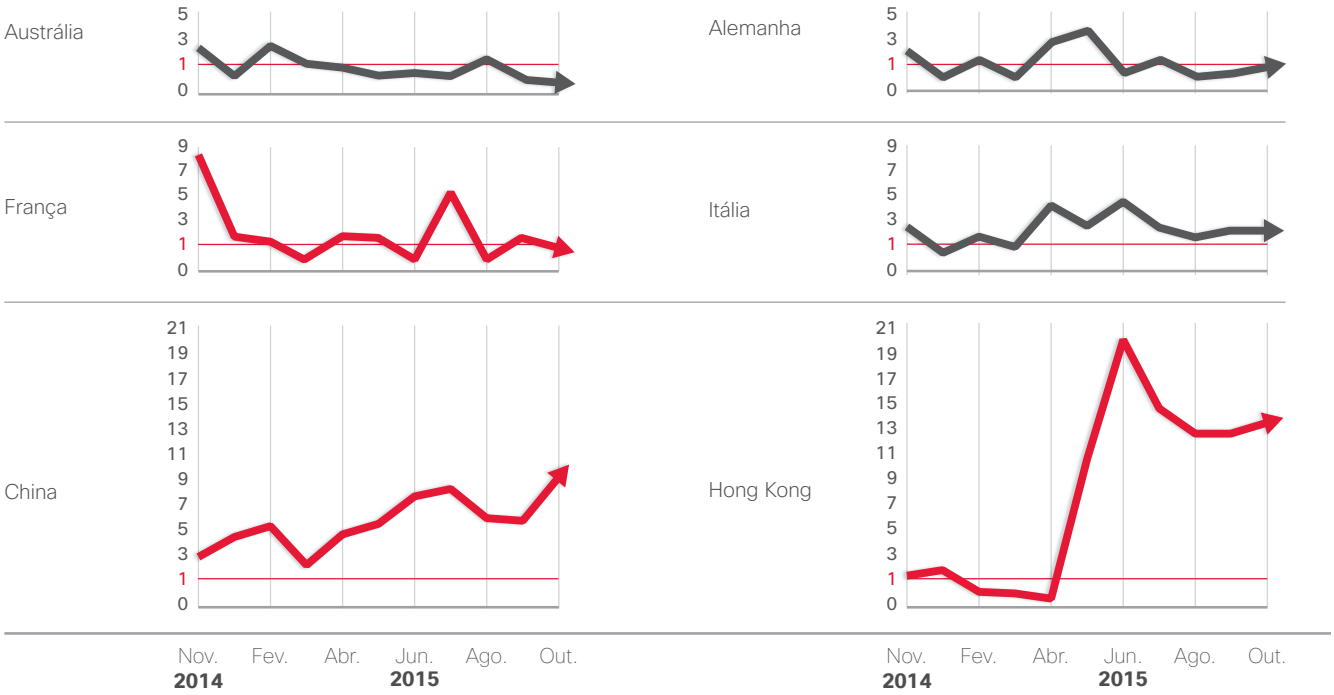
Fonte: Cisco Security Research

Uma presença em redes grandes e comercialmente viáveis nas quais trafega um grande volume de Internet é outro fator para a alta atividade de bloqueio, que é um motivo pelo qual Hong Kong lidera nossa lista.

A figura 24, que mostra uma comparação mês a mês dos bloqueios da Web por país ou região, de novembro de 2014 a outubro de 2015, fornece mais contexto para esses rankings.

Observe que foi detectada uma atividade de bloqueio da Web mais alta do que o normal em Hong Kong, iniciada na primavera de 2015. O mesmo ocorreu na França. Desde então, ambos os locais observaram uma queda significativa na atividade de bloqueio da Web, mas como as taxas mais altas de atividade no início desse ano estavam tão distantes da linha de base, a queda recente na atividade ainda deixou Hong Kong em uma posição bem mais alta no final do ano do que no início. O pico na atividade de bloqueio na França voltou aos níveis normais no verão.

Figura 24. Bloqueios da Web por país ou região, comparação mês a mês entre novembro de 2014 e outubro de 2015



Fonte: Cisco Security Research

Insights do setor

Insights do setor

A Cisco fornece pesquisa e análise sobre tendências e práticas de segurança. Paradoxalmente, algumas dessas tendências e práticas podem tornar mais difícil a capacidade dos defensores de rastrear ameaças e acabar colocando as empresas e os usuários em maior risco de comprometimento ou ataque.

Criptografia: uma tendência crescente e um desafio para os defensores

A criptografia faz sentido. As empresas precisam proteger sua propriedade intelectual e outros dados confidenciais, os anunciantes querem preservar a integridade do conteúdo de seus anúncios e da análise de back-end, e as firmas estão mais preocupadas em proteger a privacidade de seus clientes.

No entanto, a criptografia também cria problemas de segurança para as organizações, inclusive um falso senso de segurança. As empresas aprimoraram a criptografia de dados para a transmissão entre entidades, mas os dados armazenados frequentemente ficam sem segurança. Muitas das violações mais notáveis nos últimos anos aproveitaram os dados não criptografados armazenados no data center e em outros sistemas internos. Para os invasores, isso é como seguir um caminhão de suprimentos protegido até um depósito destrancado.

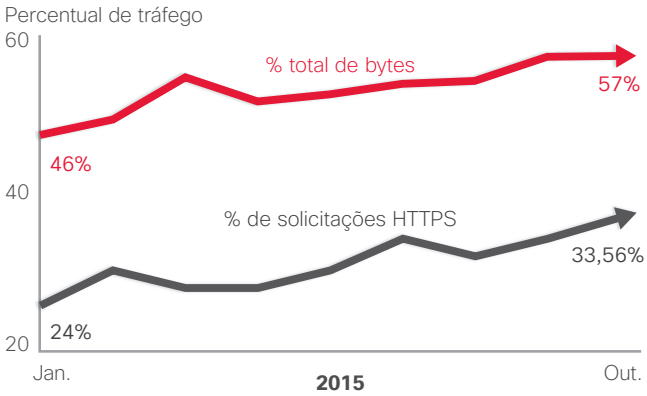
Também é importante que as empresas entendam que a criptografia de ponta a ponta pode diminuir a eficácia de alguns produtos de segurança. A criptografia oculta os indicadores de comprometimento usados para identificar e rastrear atividades mal-intencionadas.

Porém não há motivos para deixar dados confidenciais sem criptografia. As ferramentas de segurança e seus operadores precisam se adaptar a este “admirável mundo novo” coletando cabeçalhos e outras partes não criptografadas do fluxo de dados, junto com outras fontes de informações contextuais, para analisar o tráfego criptografado. As ferramentas que dependem da visibilidade de carga, como a captura de pacotes completos, tornam-se cada vez menos eficazes. Agora, a execução do Cisco NetFlow e de outras análises baseadas em metadados é essencial.

COMPARTILHAR

Ao observar as tendências de 2015, nossos pesquisadores sugerem que o tráfego criptografado, particularmente HTTPS, atingiu um ponto crítico. Embora ainda não seja a maioria das transações, em breve essa será a forma dominante de tráfego na Internet. Na verdade, nossa pesquisa mostra que ele já representa consistentemente mais de 50% dos bytes transferidos (figura 25) devido à sobrecarga de HTTPS e ao conteúdo maior que é enviado via HTTPS, como transferências para sites de armazenamento de arquivos.

Figura 25. Percentuais de SSL



Fonte: Cisco Security Research

Para realizar qualquer transação na Web, alguns bytes são enviados (saída) e recebidos (entrada). As transações HTTPS têm solicitações de saída maiores do que as solicitações de saída HTTP: cerca de 2000 bytes extras. As solicitações de entrada HTTPS, por sua vez, também têm sobrecarga, mas isso se torna menos significativo com respostas maiores.

Ao combinar os bytes de entrada e saída por transação da Web, podemos determinar o percentual geral de todos os bytes envolvidos por transação da Web criptografada com HTTPS. Devido ao aumento no tráfego HTTPS e à sobrecarga extra, determinamos que os bytes HTTPS representaram 57% de todo o tráfego da Web em outubro de 2015 (figura 25), acima dos 46% em janeiro.

Através de análises de tráfego da Web, também determinamos que as solicitações HTTPS aumentaram gradativamente, mas de modo significativo, desde janeiro de 2015. Conforme mostra a figura 25, 24% das solicitações de janeiro usaram o protocolo HTTPS; as outras usaram o protocolo HTTP.

Em outubro, 33,56% das solicitações observadas foram HTTPS. Além disso, nós descobrimos que o percentual de bytes de HTTPS de entrada havia aumentado. Essa tendência se manteve durante todo o ano. À medida que o volume de tráfego de HTTPS aumenta, é necessária mais largura de banda. São necessários mais de 5 Kbps por transação.

Nós atribuímos o aumento geral no tráfego da Web criptografado basicamente a estes fatores:

- Mais tráfego móvel de aplicativos, com criptografia inerente
- Mais solicitações de usuários para fazer download de vídeo criptografado
- Mais solicitações para servidores de armazenamento e backup que guardam "dados armazenados" confidenciais, que os adversários estão ansiosos em obter

A figura 26 mostra que as solicitações HTTPS para recursos on-line de armazenamento e backup aumentaram 50% desde o início de 2015. Os serviços de transferência de arquivo também aumentaram significativamente no mesmo período: 36%.

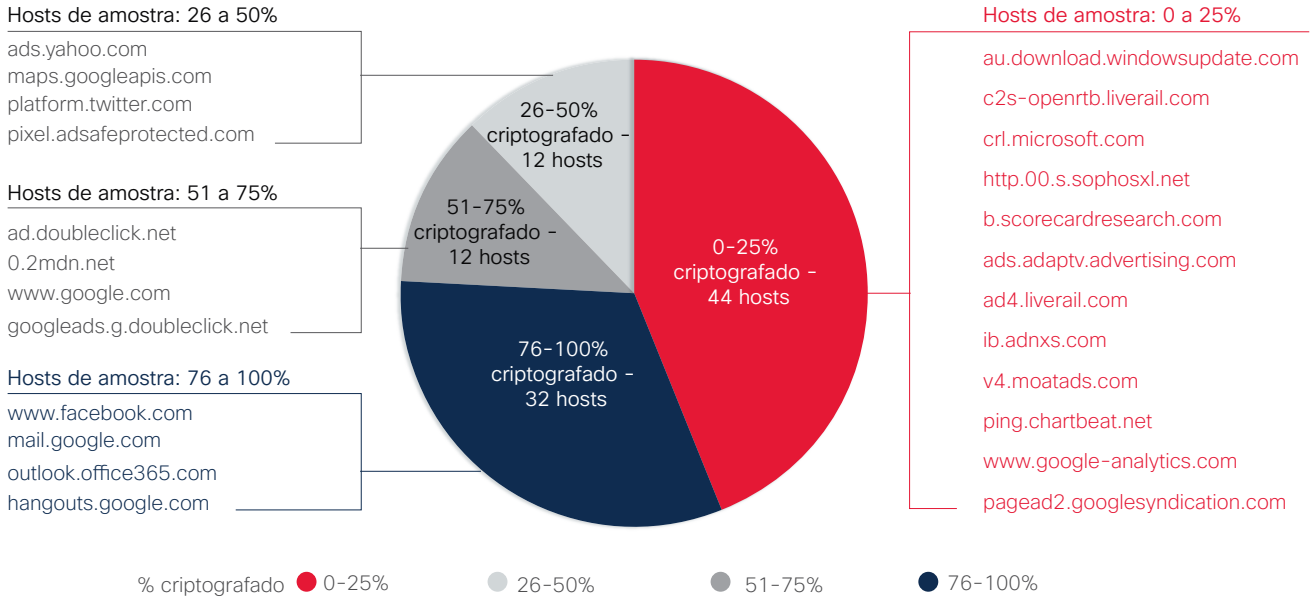
Por fim, há um aumento na atividade criptografada que ocorre tanto no número de transações com criptografia quanto no número de bytes criptografados em cada transação. Cada um apresenta seu próprio benefício e seu próprio risco potencial, indicando a necessidade de uma defesa integrada contra ameaças que ajude a aumentar a visibilidade.

Figura 26. Solicitações HTTPS: maiores desafios de janeiro a setembro de 2015

Fonte: Cisco Security Research

COMPARTILHAR

Figura 27. Principais hosts que criptografam o tráfego HTTPS



Fonte: Cisco Security Research

Quando examinamos os principais domínios pelas solicitações (figura 27), observamos que muitas das principais páginas de conteúdo do Google e do Facebook são criptografadas. Normalmente, apenas 10% do tráfego de publicidade é criptografado.

Apesar dos desafios, a criptografia de dados é um requisito no atual panorama de ameaças. Os invasores conseguem enganar cada vez mais o controle de acesso fazendo com que usuários deixem informações importantes desprotegidas em qualquer estágio do armazenamento ou da transferência.

Por isso, é fundamental que as equipes de segurança monitorem os padrões de tráfego da Web para certificarem-se de que as solicitações HTTPS não estejam chegando ou indo para locais suspeitos. Cuidado: não procure tráfego criptografado em um conjunto predefinido de portas. Conforme discutido na próxima seção, nossa pesquisa mostra que é provável que o malware inicie comunicações criptografadas em um conjunto diversificado de portas.

O FATOR DE ENTROPIA

A alta entropia é uma boa indicação de transferências de arquivo ou comunicação criptografados ou compactados.[6] A boa notícia para as equipes de segurança é que a entropia é relativamente fácil de monitorar porque não exige conhecimentos dos protocolos criptográficos básicos.

Durante um período de 3 meses iniciado em 1 de junho de 2015, os pesquisadores de segurança da Cisco observaram 7.480.178 fluxos de 598.138 amostras de malware com "pontuação de ameaça: 100" enviadas. Houve 958.851 fluxos de alta entropia nesse período ou 12,82%.

Também identificamos 917.052 fluxos com o protocolo TLS (Transport Layer Security) (12,26 %). Além disso, 8419 fluxos de TLS passaram por uma porta diferente da 443, que é a porta padrão para HTTP protegido. Algumas das portas que o malware observado usou para comunicação foram as portas 21, 53, 80 e 500.

À medida que o nível de tráfego criptografado da Internet continuar aumentando, será cada vez mais importante que as empresas adotem uma arquitetura de defesa integrada contra ameaças (consulte "Os seis princípios da defesa integrada contra ameaças" na **página 62**). As soluções pontuais não são eficazes na identificação de possíveis ameaças no tráfego criptografado. As plataformas de segurança integradas fornecem às equipes de segurança mais visibilidade em relação ao que acontece nos dispositivos ou redes, portanto, elas podem identificar com mais facilidade os padrões suspeitos de atividade.

[6] Entropia: em computação, entropia (falta de ordem ou previsibilidade) é a aleatoriedade coletada por um sistema operacional ou aplicação para uso na criptografia ou outras utilizações que exigem dados aleatórios.

A mudança para a criptografia: dados de caso

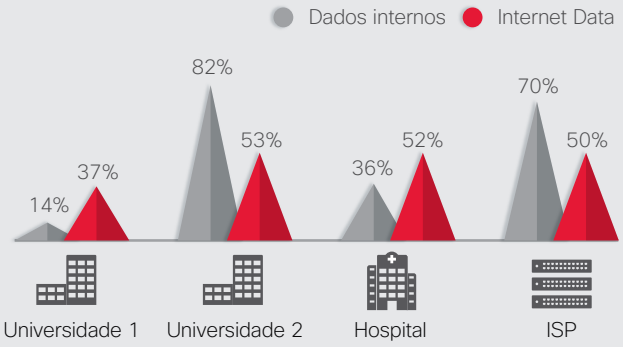
A Lancope, uma empresa da Cisco, examinou as taxas de criptografia tanto de tráfego interno quanto da Internet em três setores empresariais (duas universidades, um hospital e um provedor de ISP, sediados nos Estados Unidos).

Em uma das universidades, a Lancope constatou que quase todo o tráfego interno era criptografado (82%). Além disso, 53% do tráfego de Internet da universidade era criptografado. Essas descobertas estão de acordo com as tendências que a Lancope observou em outros setores.

Somente 36% dos dados internos do hospital eram criptografados. Contudo, mais da metade (52%) do tráfego da Internet era criptografado.

No provedor de ISP, 70% do tráfego interno era criptografado, e 50% do tráfego da Internet também.

O estudo da Lancope indica uma ampla adoção da criptografia para dados em movimento em vários setores. A Cisco sugere que um foco semelhante deva ser aplicado agora à criptografia de dados armazenados para limitar os impactos dos comprometimentos empresariais.



Fonte: Lancope Threat Research Labs

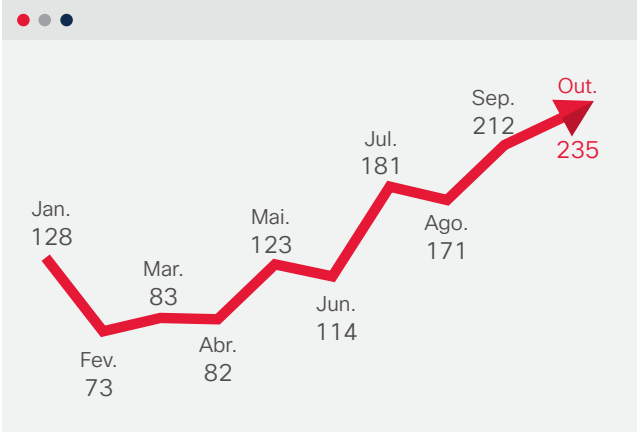
Os criminosos on-line aumentam a atividade do servidor no WordPress

Conforme discutido na introdução a este relatório, os criminosos on-line estão sempre à procura de métodos para adicionar eficiência e economia às suas operações, além de novas maneiras de escapar da detecção. Cada vez mais, os criminosos cibernéticos encontram essa eficiência em sites criados com o WordPress, uma plataforma popular de desenvolvimento de sites e blogs. Nos sites do WordPress, os invasores podem assumir o controle de um fluxo contínuo de servidores comprometidos para criar uma infraestrutura com suporte para ransomware, fraude bancária ou ataques de phishing. A Internet está cheia de sites abandonados criados com o WordPress que não passam por manutenção de uma perspectiva de segurança; conforme novos problemas de segurança surgem, com frequência, esses sites são comprometidos e incorporados em campanhas de ataque.

Ao analisar os sistemas usados para oferecer suporte a ransomware e outros malwares, os pesquisadores de segurança da Cisco descobriram que muitos criminosos on-line estão deslocando a atividade on-line para servidores comprometidos do WordPress. O número de domínios do WordPress usados pelos criminosos aumentou 221% entre fevereiro e outubro de 2015 (veja a figura 28).

Os pesquisadores da Cisco acreditam que essa mudança de local aconteceu por alguns motivos. Quando o ransomware usa outras ferramentas para transmitir chaves de criptografia ou outras informações de comando e controle, essas comunicações podem ser detectadas ou bloqueadas, o que impede a conclusão do processo de criptografia. No entanto, as comunicações que transmitem chaves de criptografia através de servidores comprometidos do WordPress podem parecer normais, o que aumenta as chances de conclusão da criptografia de arquivos. Em outras palavras, os sites do WordPress atuam como agentes de transmissão.

Figura 28. Número de domínios do WordPress usados por autores de malware



Fonte: Cisco Security Research

Para contornar as desvantagens de outras tecnologias, os criminosos se voltaram para o WordPress, que usam para hospedar cargas de malware e servidores de comando e controle. Os sites do WordPress oferecem várias vantagens. Por exemplo, os muitos sites abandonados oferecem aos criminosos mais oportunidades para comprometer sites com proteções de segurança baixas.

O risco de usar sistemas comprometidos para executar uma operação de malware é que um dos servidores invadidos poderá ser inativado quando o comprometimento for descoberto. Se isso acontecer no meio de uma campanha, a ferramenta de download de malware talvez não consiga recuperar sua carga ou o malware pode ser incapaz de se comunicar com seus servidores de comando e controle. Os pesquisadores de segurança da Cisco observaram que o malware superou isso usando mais de um servidor do WordPress; a Cisco descobriu até listas de servidores comprometidos do WordPress armazenados em sites de compartilhamento de dados, como o Pastebin.

O malware usou essas listas para encontrar servidores de comando e controle funcionais, o que lhe permitiria operar até mesmo se um servidor comprometido falhasse. Os pesquisadores também identificaram ferramentas de download de malware que continham uma lista de sites do WordPress que armazenavam cargas. Se um site de download não estivesse funcionando, o malware se dirigia ao próximo e fazia o download de cargas mal-intencionadas do servidor do WordPress funcional.

Com frequência, os sites comprometidos do WordPress não executavam a versão mais recente do WordPress, tinham senhas de admin fracas e usavam plug-ins sem os patches de segurança.

Essas vulnerabilidades permitiam que os invasores cooptassem servidores do WordPress e os utilizassem como infraestrutura de malware (veja a figura 29).

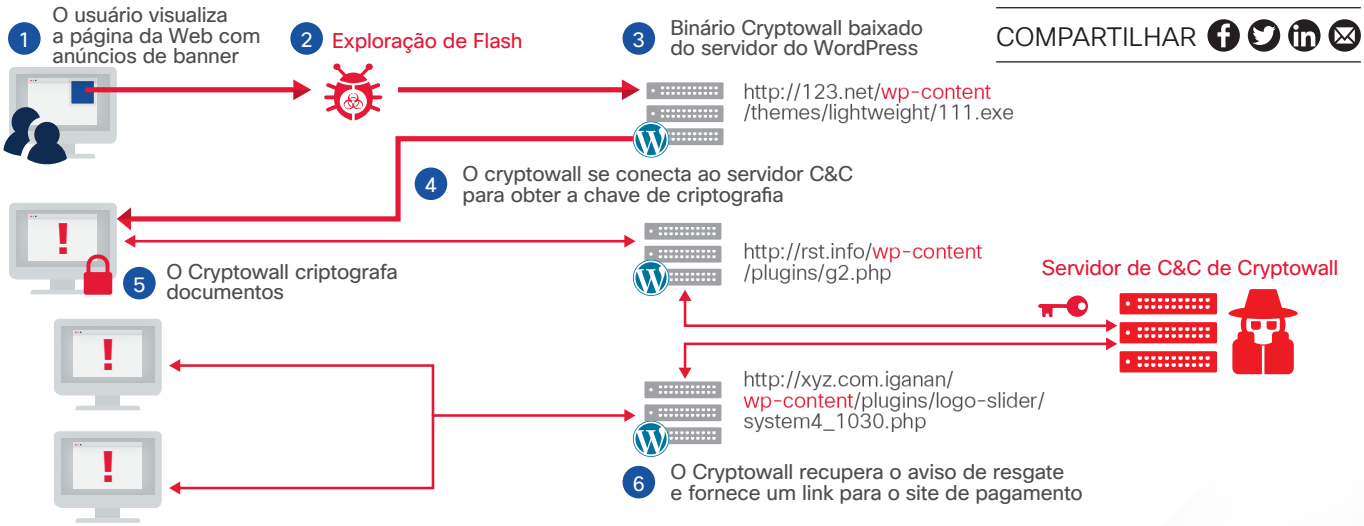
Os pesquisadores da Cisco identificaram alguns dos tipos de software e arquivo geralmente hospedados nos sites comprometidos do WordPress:

- Arquivos executáveis que são cargas para ataques de kit de exploração
- Arquivos de configuração para malware, como Dridex e Dyre
- Código proxy que transmite comunicação de comando e controle para ocultar a infraestrutura de comando e controle
- Páginas da Web de phishing para coleta de nomes de usuário e senhas
- Scripts HTML que redirecionam o tráfego para servidores do kit de exploração

Além disso, os pesquisadores da Cisco identificaram muitas famílias de malware que usam sites não comprometidos do WordPress como infraestrutura:

- Infostealer Dridex
- Ladrão de senhas Pony
- Ransomware TeslaCrypt
- Ransomware Cryptowall 3.0
- Ransomware TorrentLocker
- Botnet de spam Andromeda
- Droper de Cavalo de Troia Bartallex
- Infostealer Necurs
- Páginas de login falsas

Figura 29. Como os sites do WordPress são comprometidos



Fonte: Cisco Security Research

Os profissionais de segurança preocupados com as ameaças representadas pela hospedagem realizada pelos criminosos no WordPress devem buscar uma tecnologia de segurança da Web que examine o conteúdo proveniente de sites criados pelo WordPress. Esse tráfego poderá ser considerado incomum se a rede fizer o download de programas de sites do WordPress, em vez de apenas páginas da Web e imagens (embora os sites do WordPress possam hospedar programas legítimos também).

Infraestrutura envelhecida: um problema em 10 anos

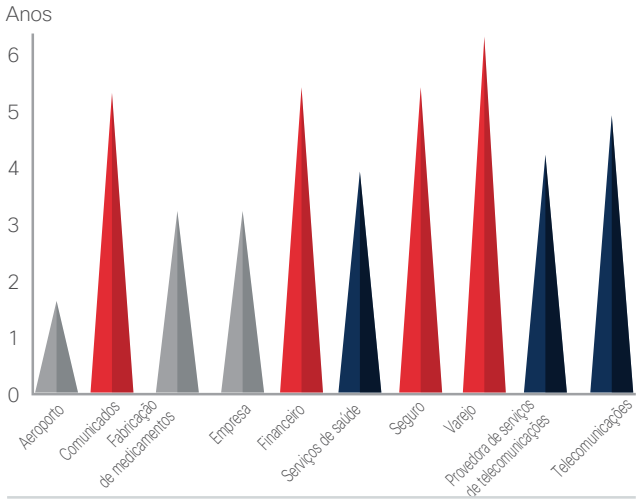
Até certo ponto, todas as empresas atuais são empresas de TI, pois dependem da infraestrutura de TI e TO (tecnologia operacional) para serem conectadas, digitalizadas e bem-sucedidas. Isso significa que precisam fazer da segurança de TI uma prioridade. Porém, muitas empresas dependem de infraestruturas de rede criadas com base em componentes antigos, desatualizados e que executam sistemas operacionais vulneráveis. E não têm resiliência digital.

Recentemente, nós analisamos 115.000 dispositivos Cisco na Internet e nos ambientes de clientes como uma forma de chamar a atenção para os riscos de segurança da infraestrutura envelhecida atual e da falta de atenção com as correções de falhas de vulnerabilidades.

Para identificar os 115.000 dispositivos em nossa amostragem de um dia, verificamos a Internet e depois olhamos os dispositivos por uma perspectiva "de fora para dentro" (da Internet para a empresa). Através de nossa verificação e análise, descobrimos que 106.000 dos 115.000 dispositivos tinham vulnerabilidades conhecidas no software que executavam. Isso significa que 92% dos dispositivos Cisco na Internet em nossa amostragem são suscetíveis a vulnerabilidades conhecidas.

A Cisco também descobriu que a versão do software executado por esses dispositivos tinha em média, 26 vulnerabilidades. Além disso, descobrimos que muitas empresas executavam software desatualizado em sua infraestrutura de rede (figura 30). Nós descobrimos que alguns clientes nos setores financeiro, de saúde e de varejo usam versões de nosso software que têm mais de 6 anos.

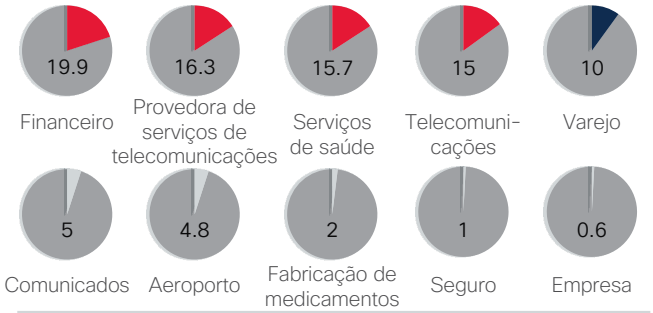
Figura 30. Idade média do software em anos



Fonte: Cisco Security Research

Também descobrimos que muitos dos dispositivos de infraestrutura que analisamos atingiram seu último dia de suporte (LDoS). Isso significa que não é possível atualizá-los e nem torná-los mais seguros (figura 31). Esses dispositivos nem mesmo recebem correção de falhas para vulnerabilidades conhecidas, portanto, não recebem informações sobre novas ameaças. Os clientes foram informados a respeito desse problema.

Figura 31. Percentual de LDoS para dispositivos de infraestrutura



Fonte: Cisco Security Research

Para saber mais sobre esse tópico, leia as postagens do blog Cisco Security:

"Segurança de TI: quando a maturidade é superestimada"

"Evolução dos ataques em dispositivos Cisco IOS"

"SYNful Knock: detecção e atenuação de ataques de software Cisco IOS"

Além disso, 8% dos 115.000 dispositivos que analisamos em nossa amostra atingiram seu estágio de fim da vida útil, e outros 31% atingirão o fim do suporte dentro de um a quatro anos.

A infraestrutura de TI envelhecida e desatualizada é uma vulnerabilidade para as empresas. Conforme nos aproximamos da Internet das Coisas (IoT) – e da Internet de Todas as Coisas (IoE) – se torna cada vez mais importante que as empresas verifiquem se estão utilizando uma infraestrutura de rede segura, para garantir a integridade dos dados e das comunicações que passam pela rede. Isso é essencial para o sucesso da IoE emergente.

Muitos clientes Cisco criaram sua infraestrutura de rede há uma década. Nessa época, muitas empresas simplesmente não consideravam o fato de que seriam 100% dependentes dessa infraestrutura. Nem previram que sua infraestrutura se transformaria no alvo principal de criminosos.

As empresas tendem a evitar a realização de atualizações de infraestrutura, pois isso é caro e requer tempo de inatividade da rede. Em alguns casos, uma simples atualização não será suficiente. Alguns produtos são tão antigos que não podem ser atualizados para incorporar as soluções de segurança mais recentes, necessárias para proteger a empresa.

Esses fatos indicam a importância da manutenção da infraestrutura. As empresas precisam se planejar para fazer atualizações regulares e reconhecer o valor de assumir o controle proativo de sua infraestrutura básica, antes que um criminoso faça isso.

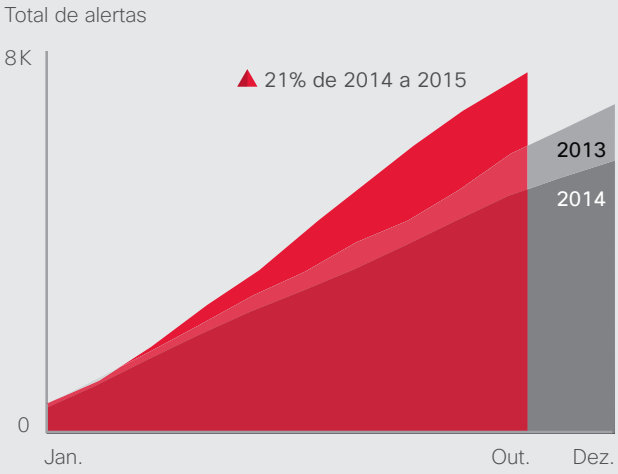
O total de alertas acumulado mostra o comprometimento crescente para o gerenciamento das vulnerabilidades

A confiança na infraestrutura envelhecida abre a porta para invasores. No entanto, a elevação dos alertas acumulados, que incluem vulnerabilidades do produto em soluções de código aberto e proprietárias, é um sinal positivo de que o setor de tecnologia está se esforçando bastante para eliminar as oportunidades de invasão.

O total de alertas acumulados aumentou 21% de 2014 a 2015. De julho a setembro de 2015, o aumento foi notavelmente alto. Em grande parte, esse aumento pode ser atribuído às grandes atualizações de software de fornecedores como a Microsoft e a Apple, pois as atualizações de produtos levaram a mais relatos de vulnerabilidades de software.

Agora, os grandes fornecedores de software lançam patches e atualizações em maior volume e são mais transparentes em relação a essa atividade. O volume crescente é uma grande motivação para as empresas automatizarem seu gerenciamento de vulnerabilidades através do uso da inteligência de segurança e de plataformas de gerenciamento que ajudem a administrar o volume do sistema e o inventário de software, a vulnerabilidade e as informações de ameaça. O uso desses sistemas e interfaces de programação de aplicações (APIs) permite o gerenciamento de segurança mais eficiente, oportuno e eficaz entre empresas de pequeno e grande porte.

Figura 32. Totais acumulados de alertas anuais



Fonte: Cisco Security Research

COMPARTILHAR

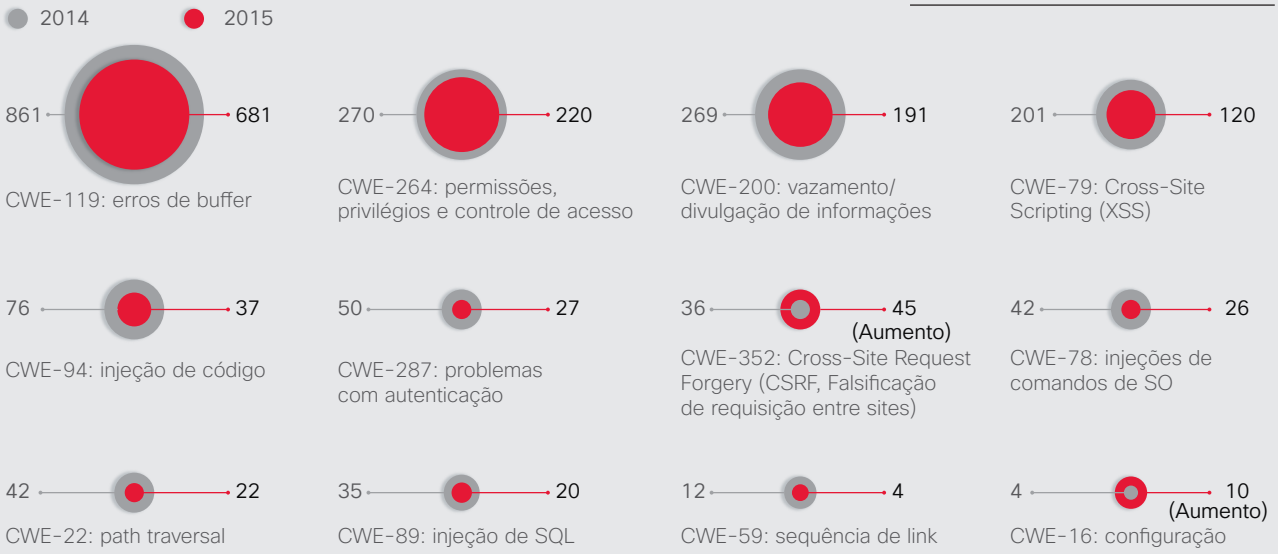
Categorias de ameaças: redução nos erros de buffer, vazamentos e divulgações de informações

Ao examinar as categorias de vulnerabilidades comuns, as vulnerabilidades de scripts entre sites (XSS) caíram 47% de 2014 a 2015 (figura 33). Essa redução pode ter ocorrido em virtude da maior atenção dada aos testes de vulnerabilidade. Os fornecedores ficaram mais habilidosos em identificar essas vulnerabilidades específicas e corrigi-las antes do lançamento de seus produtos.

As vulnerabilidades de vazamento de informações ou divulgação de informações caíram 15% em 2015. Essas vulnerabilidades envolvem divulgações involuntárias para partes que não têm acesso explícito. Os fornecedores ficaram atentos a controles que permitem ou proíbem o acesso a dados, o que tornou essa vulnerabilidade conhecida menos frequente.

Figura 33. Número de vulnerabilidades nas categorias comuns

COMPARTILHAR



Fonte: Cisco Security Research

As empresas de pequeno e médio porte são a parte mais frágil da segurança corporativa?

As SMBs desempenham um papel fundamental nas economias dos países. Quando os clientes confiam seus dados a elas, as SMBs também têm a responsabilidade de proteger essas informações de invasores on-line. No entanto, conforme detalhado no Estudo comparativo de recursos de segurança da Cisco 2015 (consulte a **página 41**), as SMBs mostram sinais de que suas defesas contra invasores são mais fracas do que seus desafios exigem. Por sua vez, esses pontos fracos podem colocar em risco os clientes corporativos de pequenas e médias empresas. Os invasores que podem violar uma rede de SMB também podem encontrar um caminho para uma rede corporativa.

Com base nos resultados do Estudo comparativo de recursos de segurança da Cisco 2014, agora, as SMBs usam menos processos para analisar comprometimentos e menos ferramentas de defesa contra ameaças do que no passado. Por exemplo, 48% das SMBs afirmaram em 2015 que utilizavam segurança da Web, em comparação com 59% em 2014. Apenas 29% disseram que usaram correção de falhas e ferramentas de configuração em 2015, em comparação com 39% em 2014.

Além disso, dos entrevistados de SMB que não têm um executivo responsável pela segurança, praticamente um quarto não acredita que suas empresas sejam alvos de grande valor para criminosos on-line. Essa crença indica uma confiança excessiva na capacidade de suas empresas de enfrentar os sofisticados ataques on-line atuais. Ou, muito provavelmente, que ataques nunca acontecerão a suas empresas.

É MENOS PROVÁVEL QUE AS SMBS USEM EQUIPES DE RESPOSTA A INCIDENTE

Em muitos casos, as SMBs apresentam menor probabilidade do que as grandes empresas de ter equipes de resposta a incidente e inteligência de ameaças. Talvez isso se deva a restrições orçamentárias: os entrevistados destacaram os problemas de orçamento como um dos maiores obstáculos à adoção de processos e tecnologia de segurança avançada. 72% das grandes empresas (aquelas com mais de 1000 funcionários) têm as duas equipes, em comparação com 67% das empresas com menos de 500 funcionários.

As SMBs também usam menos processos para analisar comprometimentos, eliminar as causas de um incidente e restaurar os sistemas aos níveis anteriores ao incidente (figura 35). Por exemplo, 53% das empresas com mais de 10.000 funcionários utilizam a análise de fluxo de rede para analisar os sistemas comprometidos, em comparação com 43% das empresas com menos de 500 funcionários. 60% das empresas com mais de 10.000 funcionários corrigem e atualizam as aplicações consideradas vulneráveis, em comparação com 51% das empresas com menos de 500 funcionários.

O uso pelas SMBs de certas defesas contra ameaças parece estar diminuindo. Por exemplo, em 2014, 52% das SMBs usaram segurança móvel, mas apenas 42% fizeram isso em 2015. Além disso, em 2014, 48% das SMBs usaram verificação de vulnerabilidade, em comparação com 40% em 2015 (veja a figura 36).

Figura 34. Maiores obstáculos das SMBs

Quais dos itens a seguir você considera os maiores obstáculos à adoção de processos de segurança avançada e tecnologia?

Porte da empresa	250-499	500-999	1000-9999	10,000+
Restrições de orçamento	40%	39%	39%	41%
Problemas de compatibilidade com sistemas legados	32%	30%	32%	34%
Prioridades concorrentes	25%	25%	24%	24%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 36. Redução nas defesas das SMB em 2015

Quais (se houver) destes tipos de defesas para ameaças de segurança sua empresa usa no momento?	2014	2015
Segurança móvel	52%	42%
Sem fio seguro	51%	41%
Varredura de vulnerabilidades	48%	40%
VPN	46%	36%
Segurança das informações e gerenciamento de eventos (SIEM)	42%	35%
Teste de penetração	38%	32%
Peritagem judicial na área de redes	41%	29%
Correção de falhas e configuração	39%	29%
Análise de endpoint	31%	23%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 35. As SMBs usam menos processos de segurança do que as grandes empresas

Quais destes processos (se houver) sua empresa usa para analisar os sistemas comprometidos?

Porte da empresa	250-499	500-999	1000-9999	10.000+
Análise de memória	30%	34%	34%	37%
Análise de fluxo de rede	43%	47%	52%	53%
Análise de log/evento correlacionado	34%	34%	40%	42%
Equipes de análise/resposta a incidentes externas (ou terceirizadas)	30%	32%	34%	39%
Análise de log do sistema	47%	51%	55%	59%
Análise do registro	43%	43%	49%	52%
Detecção de IOC	31%	34%	37%	36%

Quais processos sua empresa usa para restaurar os sistemas afetados para níveis operacionais anteriores ao incidente?

Correção e atualização de aplicativos considerados vulneráveis	51%	53%	57%	60%
Implementação de controles de detecção novos ou adicionais	49%	55%	57%	61%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

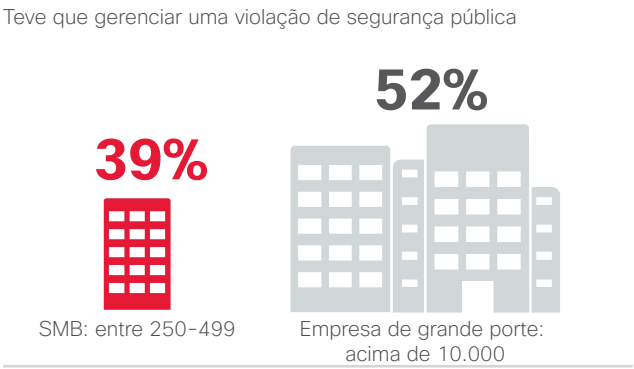
Por que é importante que as SMBs tenham a tendência de usar menos defesas do que as empresas de maior porte? Em um ambiente de segurança em que os invasores desenvolvem táticas mais sofisticadas para entrar nas redes e evitar a detecção, nenhuma empresa pode deixar suas redes desprotegidas ou abrir mão de processos que possam oferecer insights sobre como um comprometimento ocorreu, para que seja possível evitá-lo no futuro.

Além disso, as SMBs talvez não percebam que sua própria vulnerabilidade se transforma em risco para os clientes de empresas maiores e suas redes. Com frequência, os criminosos de hoje entram em uma rede para encontrar um ponto de entrada para outra, que seja mais lucrativa, e a SMB pode ser o ponto de partida para esse ataque.

MENOR PROBABILIDADE DE TER PASSADO POR VIOLAÇÕES DE DADOS PÚBLICOS

As SMBs apresentam menor probabilidade do que as grandes empresas de ter lidado com uma violação de segurança pública, possivelmente em virtude de seu menor espaço ocupado de um ponto de vista de rede. Enquanto 52% das empresas com mais de 10.000 funcionários já gerenciaram as consequências de uma violação de segurança pública, apenas 39% das empresas com menos de 500 funcionários já fizeram isso.

Figura 37. AS SMBs relatam menos violações públicas

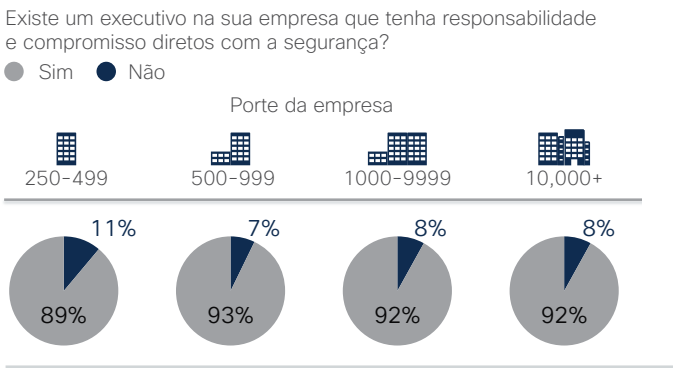


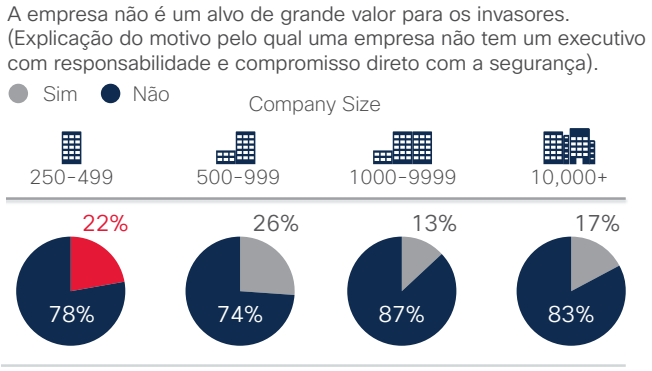
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Obviamente, as violações de segurança pública causam interrupções e são prejudiciais para uma empresa, mas oferecem uma vantagem: com frequência, elas incentivam as empresas a prestar mais atenção em sua segurança e pensar no fortalecimento de suas proteções. Os dados da pesquisa da Cisco (consulte a **página 74**) mostram que quando grandes empresas sofrem uma violação de dados públicos, elas fazem atualizações significativas de sua tecnologia de segurança e implementam processos mais fortes.

Figura 38. As SMBs não se consideram alvos de alto risco





Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

A visão das SMBs de suas empresas como alvos de criminosos cibernéticos pode demonstrar uma lacuna em sua percepção do panorama de ameaças. Conforme ilustrado acima, na figura 38, 22% das empresas com menos de 500 funcionários afirmaram não ter um executivo com responsabilidade direta pela segurança, pois não se consideram alvos de grande valor.

SMBs APRESENTAM MAIOR PROBABILIDADE DE TERCEIRIZAR FUNÇÕES DE SEGURANÇA EM 2015

Embora a pesquisa mostre que em geral, mais SMBs terceirizam algumas de suas funções de segurança, as SMBs apresentam menor probabilidade do que as grandes empresas de terceirizar certos serviços, como consultoria. Por exemplo, 55% das grandes empresas terceirizam os serviços de consultoria, em comparação com 46% das empresas com menos de 500 funcionários. 56% das grandes empresas terceirizam as tarefas de auditoria de segurança, em comparação com 42% das empresas com menos de 500 funcionários (veja a figura 39).

Entretanto, em 2015, mais SMBs estão terceirizando pelo menos alguns serviços de segurança. Em 2014, 24% das SMBs com menos de 499 funcionários afirmaram não terceirizar serviços. Em 2015, apenas 18% das SMBs disseram o mesmo.

O fato de que mais SMBs estão adotando a terceirização como uma forma de gerenciar a segurança é uma boa notícia. Isso indica que as SMBs estão em busca de ferramentas flexíveis para proteger as redes que não aumentem a carga de suas pequenas equipes ou de orçamentos mais conservadores. Entretanto, as SMBs podem acreditar incorretamente que a terceirização de processos de segurança reduzirá bastante a probabilidade de uma violação de rede. Ou podem transferir o ônus da segurança para terceiros. Esse ponto de vista pode ser uma ilusão, pois apenas um sistema de defesa contra ameaças realmente integrado, que examine e atenue os ataques e ainda, os evite, pode fornecer proteção de segurança em nível empresarial.

Figura 39. Mais SMBs terceirizam serviços de segurança em 2015

Quando se trata de segurança, quais dos seguintes tipos de serviços, se houver, são terceirizados total ou parcialmente?

Porte da empresa	250-499	500-999	1000-9999	10,000+
Conselho e consultoria	46%	51%	54%	55%
Monitoramento	45%	46%	42%	44%
Auditoria	42%	46%	46%	56%
Resposta a incidentes	39%	44%	44%	40%
Inteligência de ameaças	35%	37%	42%	41%
Correção	33%	38%	36%	36%
Nenhuma	18%	12%	11%	10%

Por que sua empresa (SMB 250-499) opta por terceirizar esse(s) serviço(s)?

Porque é mais econômico	Porque deseja um insight independente	Resposta mais oportuna a incidentes	Falta de recursos internos (software, mão de obra)	Falta de experiência interna
51%	45%	45%	31%	30%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Estudo comparativo de recursos de segurança da Cisco

Estudo comparativo de recursos de segurança da Cisco

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 suas percepções de procedimentos e recursos de segurança. O Estudo comparativo de recursos de segurança da Cisco 2015 apresenta insights sobre o nível de maturidade das operações de segurança e das práticas de segurança em uso no momento, e também compara esses resultados com o estudo inicial de 2014.

Queda na confiança entre os sinais de preparo

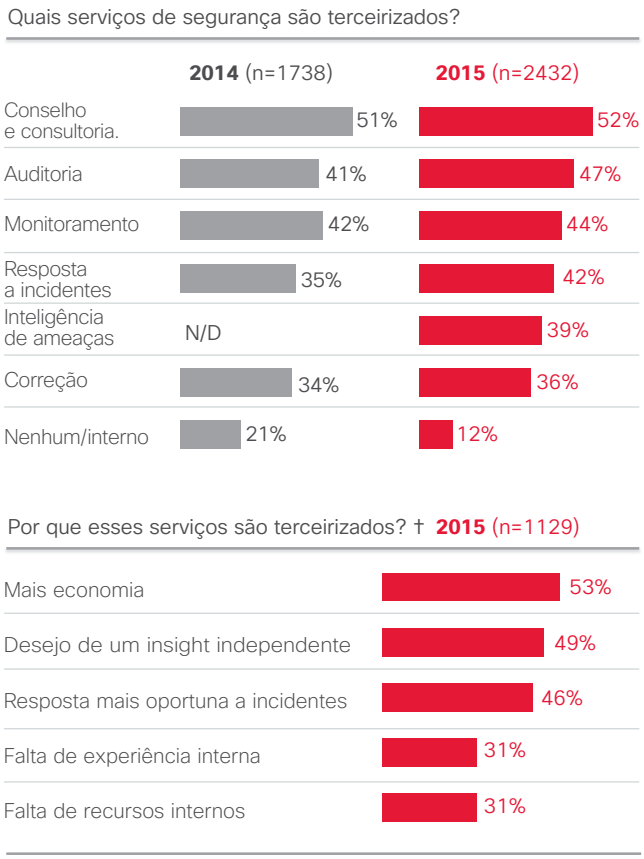
Diante de ameaças mais sofisticadas, o estudo da Cisco sugere que a confiança dos profissionais de segurança parece estar caindo. Por outro lado, as preocupações mais profundas com a segurança alteram o modo como esses profissionais protegem as redes. Por exemplo, observamos mais treinamento em segurança, um aumento nas políticas formais por escrito e ampliação da terceirização de tarefas como auditorias de segurança, consultoria e resposta a incidentes. Em resumo, os profissionais de segurança dão sinais de que estão reagindo para combater as ameaças que aparecem em suas redes.

Os movimentos na direção do treinamento e da terceirização são positivos, mas o setor de segurança não pode parar aí. Ele deve continuar aumentando o uso de ferramentas e processos para melhorar a detecção, a contenção e a atenuação de ameaças. Dadas as barreiras das limitações orçamentárias e a compatibilidade de soluções, o setor também precisa explorar soluções eficazes que fornecem uma defesa integrada contra ameaças. O setor também deve fazer um trabalho melhor de colaboração com outras empresas quando violações públicas ocorrerem (por exemplo, com o botnet SSHPsychos; consulte a **página 14**), pois o compartilhamento de conhecimentos pode ajudar a evitar futuros ataques.

RECURSOS: HÁ GRANDE POSSIBILIDADE DE TERCEIRIZAÇÃO PELAS EMPRESAS

À medida que os profissionais de segurança tomam conhecimento das ameaças, eles podem aprimorar suas defesas, por exemplo, com a terceirização de tarefas de segurança que podem ser gerenciadas com mais eficiência por consultores ou fornecedores. Em 2015, 47% de nossas empresas pesquisadas terceirizaram auditorias de segurança, um aumento de 41% em 2014. Também em 2015, 42% terceirizaram os processos de resposta a incidente, em comparação com 35% em 2014 (figura 40).

Figura 40. Resumo dos serviços terceirizados



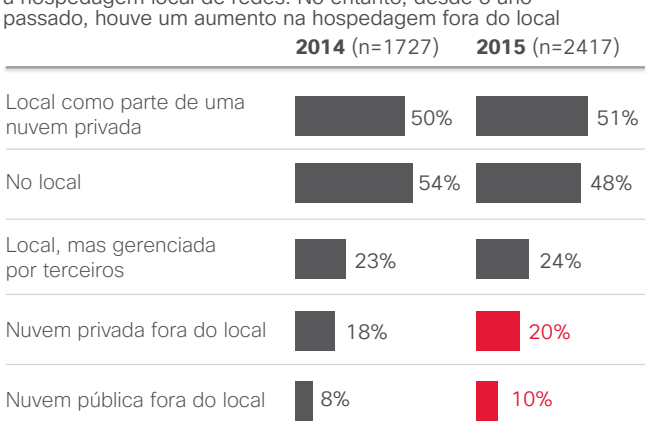
† Entrevistados da pesquisa de segurança que terceirizaram serviços de segurança (2015; n=2129)

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Além disso, mais profissionais de segurança terceirizam pelo menos algumas funções de segurança. Em 2014, 21% dos entrevistados da pesquisa afirmaram que não terceirizaram nenhum serviço de segurança. Em 2015, esse número caiu significativamente, para 12%. 53% disseram que terceirizaram os serviços porque isso era mais econômico, enquanto 49% disseram ter feito isso para obter insights independentes.

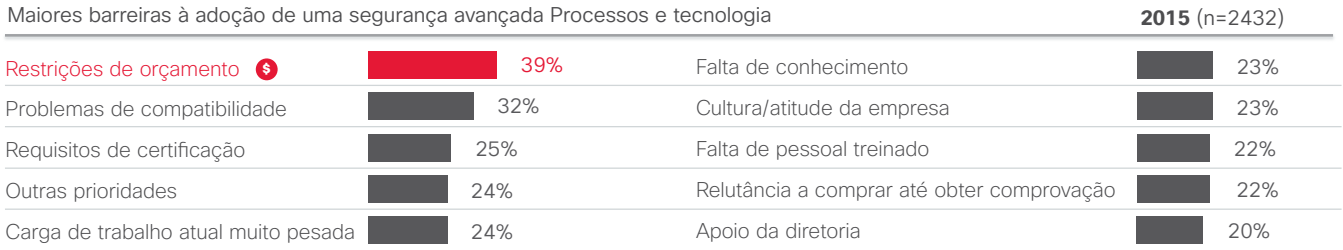
Para adicionar proteção às suas redes e dados,os profissionais de segurança indicaram que estão receptivos ao conceito de hospedagem de rede fora do local. Embora a hospedagem no local ainda seja a opção preferida, o número de profissionais que usa soluções fora do local aumentou. Em 2015, 20% usaram soluções de nuvem privada fora do local, em comparação com 18% em 2014 (figura 41).

Figura 41. Hospedagem fora do local em alta



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

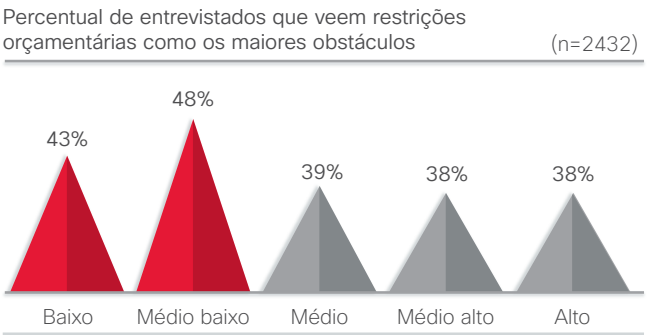
Figura 42. As restrições orçamentárias são a principal barreira para atualizações de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

As equipes de segurança pesquisadas pela Cisco estão mais inclinadas a proteger suas redes de modo mais eficaz, mas podem ter limitada sua capacidade de realizar seus planos. Os profissionais de segurança afirmaram que restrições orçamentárias (39%) lideram a lista de motivos prováveis para escolher ou recusar os serviços e as ferramentas de segurança. Em seguida, vêm os problemas de compatibilidade tecnológica (32%; veja a figura 42). As restrições orçamentárias se tornaram um grande problema para as empresas que estão nos níveis de maturidade baixa e baixa-intermediária (veja a figura 43). Nas respostas de todos os profissionais de segurança, 39% citam as restrições orçamentárias como um obstáculo à adoção de processos de segurança avançada. Esse número representa 43% das empresas no intervalo de maturidade baixa, e 48% no intervalo de maturidade baixa-intermediária.

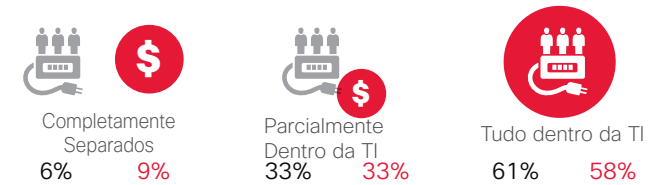
Figura 43. As restrições orçamentárias são o maior obstáculo para as empresas de baixa maturidade



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Um sinal de que algumas empresas pensam cada vez mais em seus recursos de segurança é o modo como estruturam seu orçamento de segurança. A pesquisa mostra um ligeiro aumento no número de empresas que separam o orçamento de segurança do orçamento geral de TI. Em 2014, 6% dos profissionais afirmaram que tinham separado completamente os orçamentos de segurança e de TI; em 2015, esse número aumentou para 9% (veja a figura 44).

Figura 44. Ligeiro aumento no número de empresas com orçamentos de segurança separados



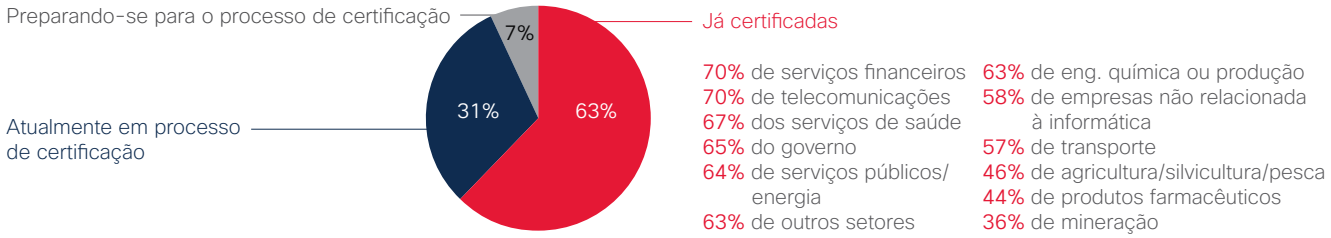
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Quando as empresas padronizam as políticas de segurança ou buscam certificação, elas mostram um compromisso com o aumento da segurança. Cerca de dois terços dos profissionais de segurança afirmaram que suas empresas têm certificação em políticas ou práticas padrão de segurança, ou estão em processo de certificação (figura 45). Esse é outro sinal positivo de que as empresas enxergam valor no aprimoramento de seu conhecimento de segurança e resposta a ameaças.

Figura 45. Muitas empresas têm certificações ou estão em busca de certificação

A empresa segue uma prática de política de segurança da informação padronizada (**2015** n=1265)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Ao examinar o uso de defesas de segurança, descobrimos que os firewalls são as ferramentas de segurança mais comumente usadas pelas empresas (65%), seguidas pela prevenção a perda de dados (56%) e pelas ferramentas de autenticação (53%; veja a figura 46). Em 2015, as empresas apresentaram uma probabilidade ligeiramente menor de confiar em ferramentas baseadas em nuvem. Embora os profissionais de segurança tenham mostrado disposição para terceirizar os serviços de segurança (consulte a **página 43**), eles estão inclinados a seguir uma tendência de implantação interna de ferramentas. (Consulte a **página 71** para obter a lista completa.)

Figura 46. Os firewalls e a prevenção contra perda de dados são as ferramentas de segurança mais usadas

Defesas contra ameaças à segurança usadas pela empresa	**2014** (n=1738)	**2015** (n=2432)	Defesas administradas através de serviços em nuvem (entrevistados da pesquisa de segurança que usam defesas contra ameaças de segurança) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevenção contra perda de dados	55%	56%		
Autenticação	52%	53%		
Criptografia/privacidade/proteção de dados	53%	53%		
Segurança de e-mail/envio de mensagens	56%	52%	37%	34%
Segurança da Web	59%	51%	37%	31%
Rede, segurança, firewalls e prevenção contra intrusões*	60%	N/D	35%	

*Firewall e a prevenção contra intrusões foram unificados em um código em 2014: " Segurança de rede, firewalls e prevenção contra intrusões".

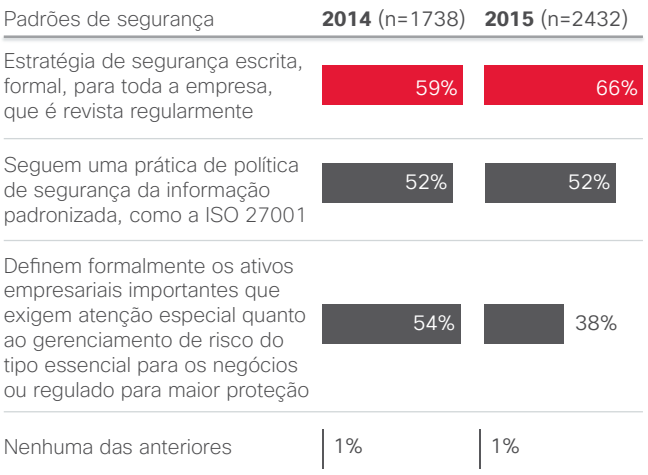
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

RECURSOS: A CONFIANÇA ESTÁ EM BAIXA

Em 2015, os profissionais de segurança tinham menos certeza do que em 2014, de que sua infraestrutura segura estava atualizada. Essa queda na confiança se deve, sem dúvida, aos rumores persistentes de ataques de alto perfil nas grandes empresas, ao roubo correspondente de dados privados e às desculpas públicas de empresas cujas redes foram violadas.

No entanto, essa queda na confiança é acompanhada por um interesse crescente no desenvolvimento de políticas mais fortes. Conforme visto na figura 47, mais empresas (66%) têm uma estratégia de segurança escrita formal em 2015 do que em 2014 (59%).

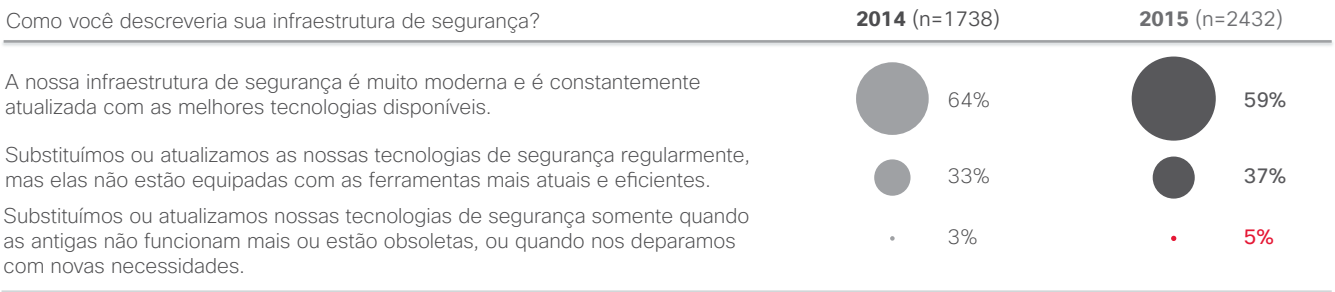
Figura 47. Mais empresas criam políticas de segurança formais



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Figura 48. A confiança é menor em 2015

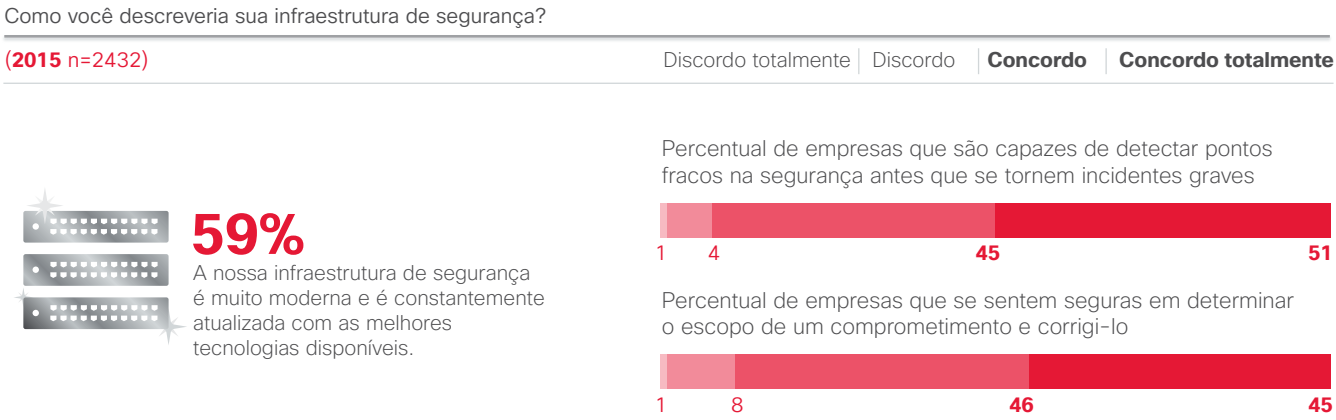


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Como um sinal de queda no nível de confiança, os profissionais de segurança mostram confiar um pouco menos em suas tecnologias. Em 2014, 64% afirmaram que sua infraestrutura de segurança estava atualizada. Em 2015, esse número caiu para 59% (figura 48). Além disso, em 2014, 33% afirmaram que suas empresas não tinham as ferramentas de segurança mais recentes; esse número aumentou para 37% em 2015.

A confiança é ligeiramente maior entre os CSOs, que estão mais otimistas do que os gerentes de operações de segurança: 65% dos CSOs acreditam que sua infraestrutura de segurança está atualizada, em comparação com 54% dos gerentes de SecOps. A confiança dos gerentes de SecOps provavelmente será afetada porque eles respondem aos incidentes de segurança diários, o que lhes dá uma visão menos favorável de sua prontidão para a segurança.

Figura 49. Pouca confiança na capacidade de detecção de comprometimentos

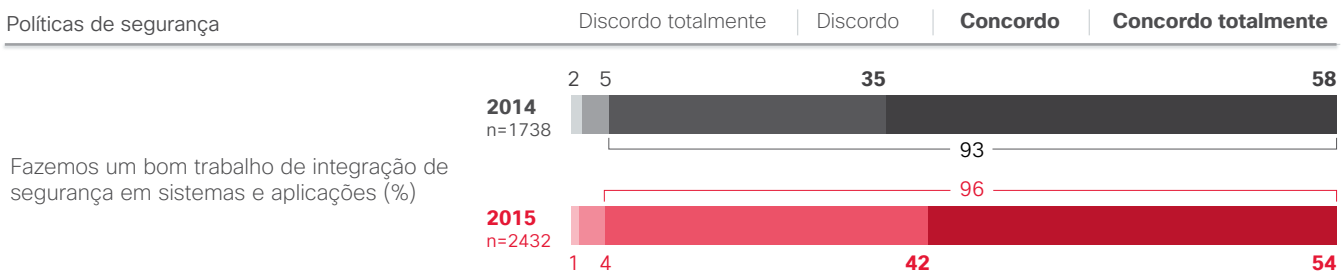


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Os profissionais de segurança também mostram níveis combinados de confiança em termos de sua capacidade de impedir ataques. 51% acreditam com firmeza que podem detectar pontos fracos de segurança antes que eles se tornem incidentes; apenas 45% confiam em sua capacidade de determinar o escopo de um comprometimento de rede, e de minimizar os danos (veja a figura 49).

Os profissionais de segurança também mostram níveis de confiança mais fracos em sua capacidade de defender as redes contra ataques. Por exemplo, em 2015, menos profissionais acreditam com firmeza que fazem um bom trabalho na elaboração de procedimentos de segurança para adquirir, desenvolver e manter sistemas (54% em 2015, em comparação com 58% em 2014; veja a figura 50). (Consulte a **página 76** para obter a lista completa.)

Figura 50. Menor confiança na capacidade de integrar a segurança aos sistemas



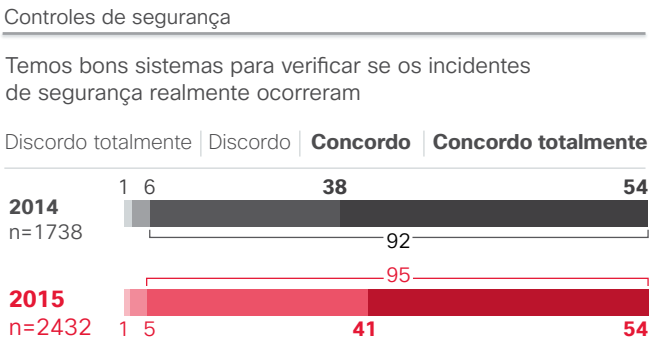
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Em algumas áreas, os níveis de confiança nos recursos de segurança não são muito altos. Por exemplo, em 2015, apenas 54% dos entrevistados disse acreditar que tinham um bom sistema para verificar se os incidentes de segurança realmente ocorreram (veja a figura 51). (Consulte a **página 77** para obter a lista completa.)

Os entrevistados não têm certeza se seus sistemas podem definir o escopo desses comprometimentos e detê-los. 56% afirmaram que analisam e melhoram as práticas de segurança regularmente, formalmente e estrategicamente; 52% acreditam que suas tecnologias de segurança estão bem integradas e funcionam bem em conjunto (veja a figura 52). (Consulte a **página 79** para obter a lista completa.)

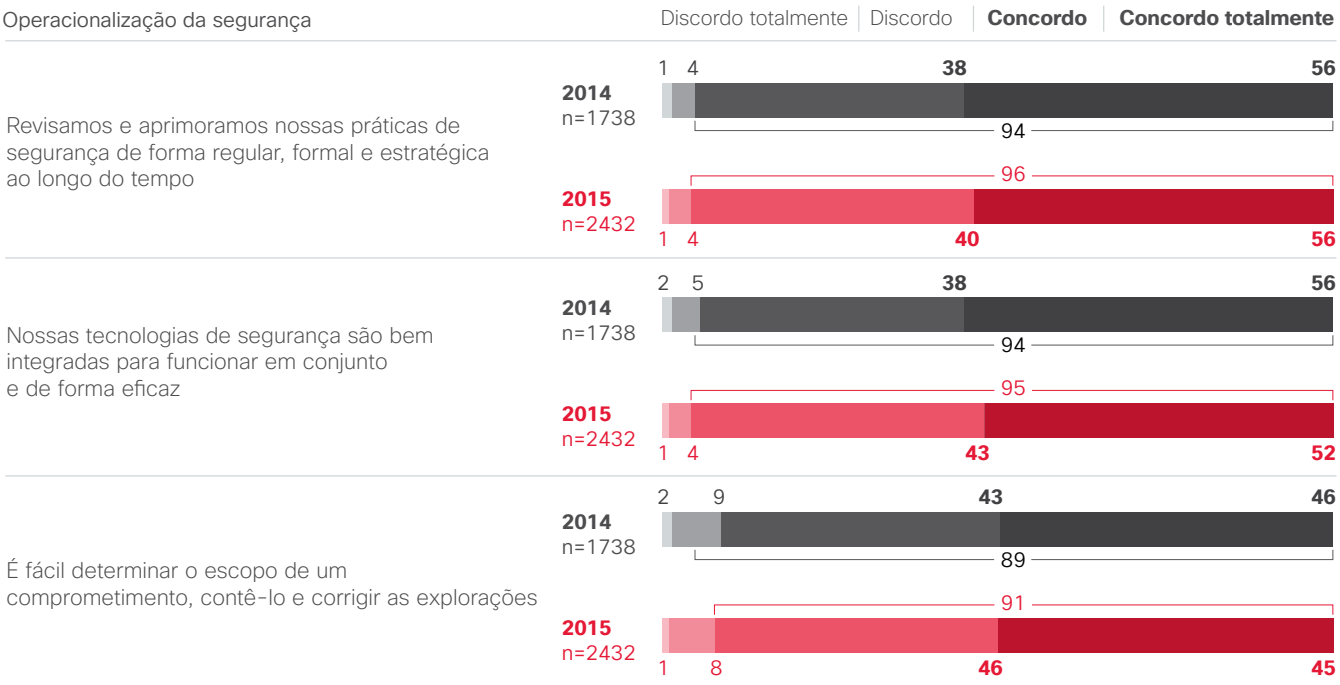
Figura 51. As empresas acreditam que têm bons controles de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

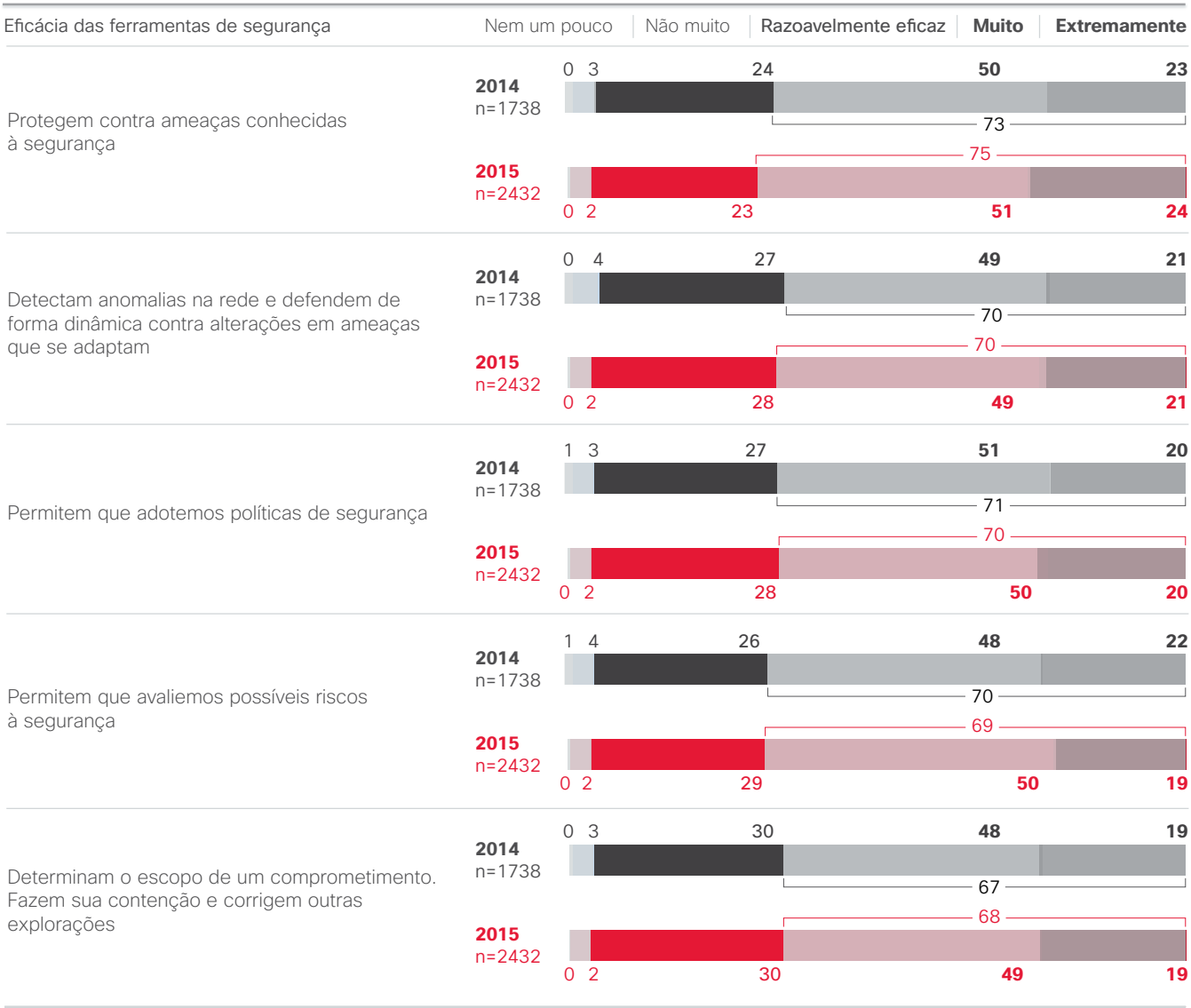
COMPARTILHAR

Figura 52. As empresas mostram pouca confiança na capacidade de evitar o comprometimento



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 53. Um quarto das empresas acreditam que as ferramentas de segurança são pouco eficazes



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

De modo semelhante aos entrevistados de 2014, mais de um quarto dos profissionais de segurança em 2015 disseram ter percebido que suas ferramentas de segurança eram apenas um pouco eficazes (figura 53).

As violações de segurança pública tendem a ser um momento determinante para as empresas. Quando ocorrem, as empresas parecem perceber melhor a necessidade de evitar futuras violações. No entanto, em 2015, menos profissionais de segurança disseram que suas empresas tiveram que lidar com violações de segurança pública: foram 53% dos profissionais em 2014 e 48% em 2015 (figura 54).

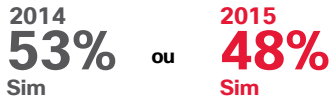
Os profissionais reconhecem o valor das violações em termos de chamar a atenção sobre a importância do fortalecimento de processos de segurança: 47% dos profissionais de segurança afetados pelas violações públicas disseram que essas violações resultaram em políticas e procedimentos melhores. Por exemplo, 43% dos entrevistados disseram que aumentaram o treinamento de segurança depois de uma violação pública, e 42% disseram ter aumentado os investimentos em tecnologias de defesa de segurança.

A boa notícia é que as empresas que sofreram uma violação pública apresentam uma probabilidade cada vez maior de fortalecer seus processos de segurança. Em 2015, 97% dos profissionais de segurança afirmaram realizar treinamento de segurança pelo menos uma vez por ano, um sólido aumento sobre os 82% de 2014 (veja a figura 90 na **página 82**).

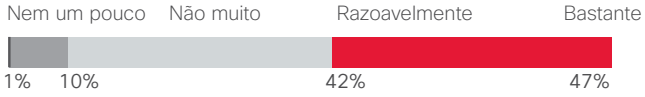
COMPARTILHAR

Figura 54. As violações públicas podem melhorar a segurança

A sua empresa já teve que lidar com as críticas resultantes de uma violação de segurança? (n=1701) (n=1347)



Qual foi a quantidade de aprimoramentos que a violação gerou nas suas políticas de defesa contra ameaças de segurança? Procedimentos ou tecnologias? (n=1134)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 55. Mais empresas realizam treinamento de segurança

Em 2015, 43% dos entrevistados disseram ter aumentado o treinamento de segurança depois de uma violação pública.

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

MATURIDADE: AS RESTRIÇÕES ORÇAMENTÁRIAS OCUPAM POSIÇÕES PRIORITÁRIAS EM CADA NÍVEL

Conforme as empresas implantam práticas e políticas de segurança mais sofisticadas, suas percepções sobre a própria preparação de segurança podem mudar. O Estudo comparativo de recursos de segurança da Cisco de 2015 classifica os participantes da pesquisa e suas empresas em cinco categorias de maturidade, com base nas respostas sobre seus processos de segurança (figura 56). O estudo examina como características diferentes, como recursos, setores e países, podem afetar os níveis de maturidade.

Curiosamente, empresas com níveis de maturidade diferentes parecem compartilhar alguns obstáculos à implementação de processos e ferramentas de segurança mais sofisticados. Embora os percentuais exatos possam variar, o desafio das restrições orçamentárias está no início da lista em todos os níveisde maturidade (figura 57).

Figura 56. O modelo de maturidade classifica as empresas com base em processos de segurança

A Cisco explorou várias opções de segmentação de amostra antes de selecionar uma solução de cinco segmentos com base em uma série de perguntas relativas a processos de segurança. A solução de cinco segmentos mapeia de forma razoavelmente estreita para o Capability Maturity Model Integration (CMMI).

	Nível	Solução baseada em 5 segmentos	
Otimização	1	Foco na melhoria dos processos	Alto
Gerenciada de forma quantitativa	2	Processos mensurados quantitativamente e controlados	Superior-médio
Definida	3	Processos caracterizados pela empresa; geralmente proativos	Médio
Pode ser repetida	4	Processos caracterizados por projetos: geralmente reativos	Médio-baixo
Inicial	5	Processos ad hoc, imprevisíveis	Baixo

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 57. Quais dos itens a seguir você considera os maiores obstáculos à adoção de processos de segurança e tecnologia de ponta?

Quais dos itens a seguir você considera os maiores obstáculos à adoção de processos de segurança avançada e tecnologia?

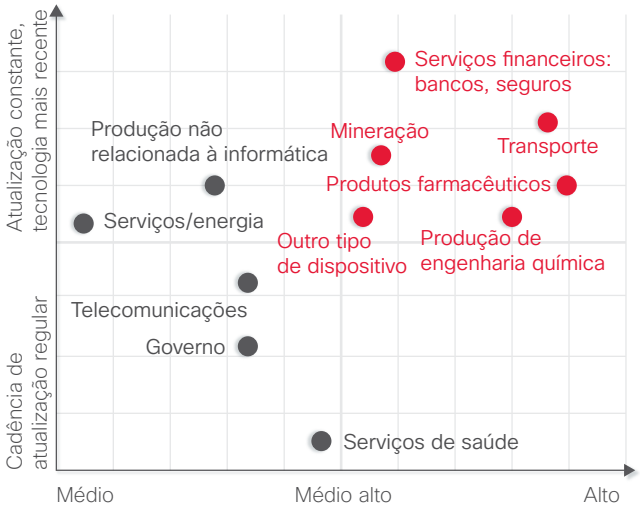
Nível de sofisticação	Baixo	Médio baixo	Médio	Superior-médio	Alto
Restrições de orçamento	43%	48%	39%	38%	38%
Apoio da diretoria	14%	20%	20%	22%	19%
Prioridades concorrentes	19%	27%	26%	26%	22%
Falta de pessoal treinado	21%	27%	22%	19%	23%
Falta de conhecimento sobre processos de segurança avançada e tecnologia	31%	20%	25%	23%	22%
Problemas de compatibilidade com sistemas antigos	21%	28%	29%	34%	33%
Requisitos para a certificação	14%	17%	26%	27%	25%
Atitude da cultura empresarial sobre segurança	31%	23%	23%	22%	21%
Relutam em comprar até obter a comprovação do mercado	12%	25%	24%	25%	19%
A carga de trabalho atual é muito pesada para assumir novas responsabilidades	36%	23%	25%	25%	22%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

O gráfico à direita mapeia a qualidade da infraestrutura de segurança e os níveis de maturidade de vários setores. Ele se baseia nas percepções dos entrevistados a respeito de seus processos de segurança. Os setores exibidos no quadrante superior direito mostram os mais altos níveis de maturidade e qualidade de infraestrutura.

O gráfico abaixo mostra o posicionamento nos níveis de maturidade da Cisco por setor. Em 2015, aproximadamente metade das empresas de transporte e farmacêuticas pesquisadas estavam no segmento de alta maturidade. As empresas de telecomunicações e do setor público apresentam menos probabilidade de estar no segmento de alta maturidade em 2015, em comparação com 2014. Os resultados se baseiam nas percepções dos entrevistados a respeito de seus processos de segurança.

Figura 58. Avaliação da maturidade de segurança por infraestrutura e setor

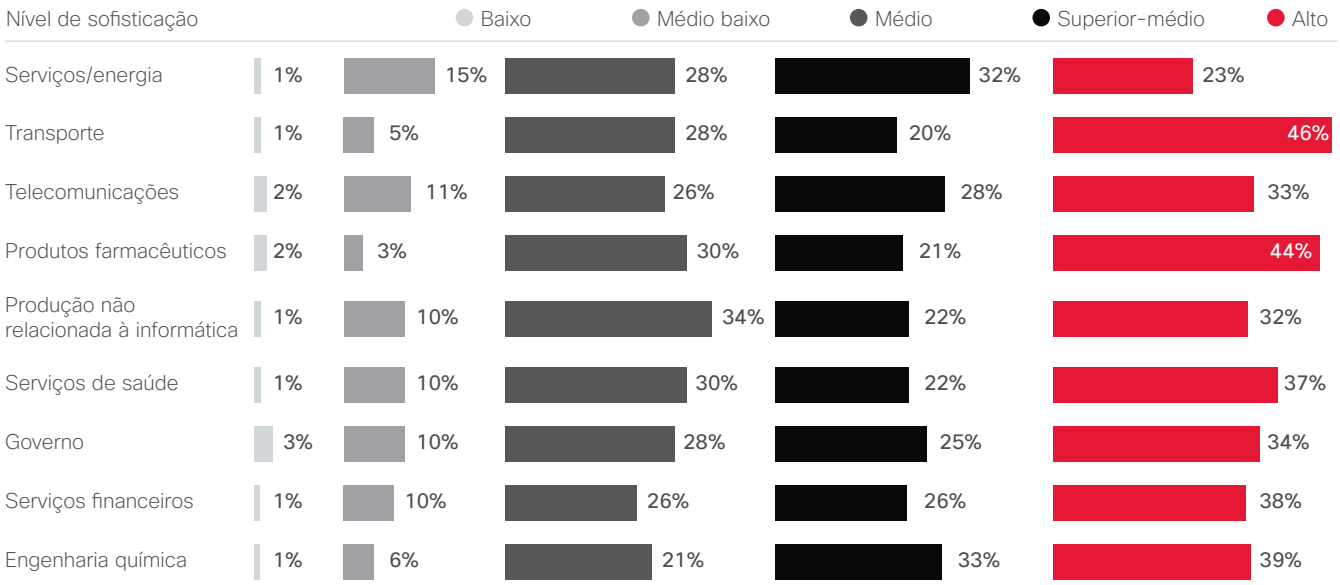


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

COMPARTILHAR

Figura 59. Níveis de maturidade por setor

Distribuição de segmento por setor



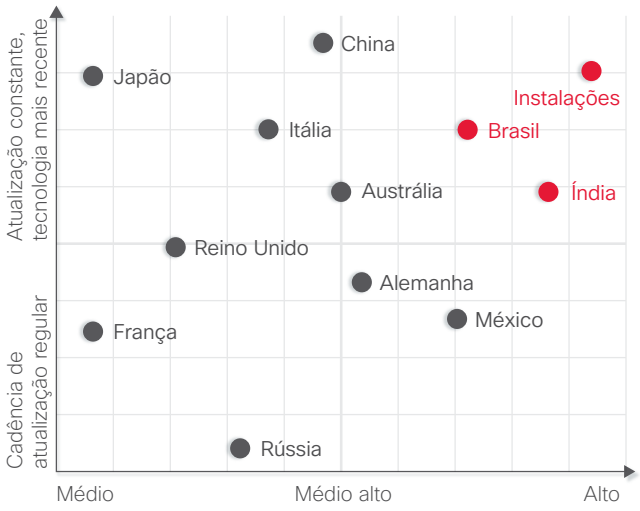
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

O gráfico à direita mapeia a qualidade da infraestrutura de segurança e os níveis de maturidade de vários países. Os países exibidos no quadrante superior direito mostram os mais altos níveis de maturidade e qualidade de infraestrutura. É importante observar que essas descobertas se baseiam nas percepções dos profissionais de segurança de sua prontidão para a segurança.

O gráfico abaixo mostra o posicionamento nos níveis de maturidade da Cisco por país. Os resultados se baseiam nas percepções dos entrevistados a respeito de seus processos de segurança.

COMPARTILHAR

Figura 60. Avaliação da maturidade de segurança por infraestrutura e país



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 61. Níveis de maturidade por país

Distribuição de segmento por setor — **2014** (n=1637) — **2015** (n=2401)

Nível de sofisticação	2014	Baixo	Médio baixo	Médio	Superior-médio	Alto
Instalações	3% / 2%	10% / 4%	27% / 22%	16% / 27%	44% / 45%	
Brasil	2% / 1%	5% / 9%	24% / 24%	35% / 26%	34% / 40%	
Alemanha	1% / 1%	4% / 12%	27% / 24%	25% / 24%	43% / 39%	
Itália	1% / 4%	23% / 3%	13% / 36%	25% / 23%	38% / 34%	
Reino Unido	8% / 0%	8% / 14%	25% / 32%	18% / 22%	41% / 32%	
Austrália	9% / 1%	7% / 5%	19% / 29%	35% / 36%	30% / 29%	
China	0% / 0%	3% / 6%	32% / 37%	29% / 25%	36% / 32%	
Índia	7% / 1%	3% / 4%	20% / 21%	16% / 34%	54% / 40%	
Japão	7% / 2%	15% / 16%	14% / 34%	40% / 16%	24% / 32%	
México	6%	8%	20%	16%	50%	
Rússia	1%	14%	27%	26%	32%	
França	1%	15%	35%	20%	29%	

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

RECOMENDAÇÕES: RESPOSTA A VERIFICAÇÕES DE REALIDADE

Como mostra nosso Estudo comparativo de recursos de segurança, a realidade chegou para os profissionais de segurança. A confiança dos profissionais de segurança em sua capacidade de bloquear invasores oscila. Entretanto, a dura realidade proveniente das explorações públicas teve um efeito positivo no setor, a julgar pelo aumento do treinamento em segurança e o desenvolvimento de uma política formal. Além disso, a mais frequente terceirização de auditorias e serviços de resposta a incidentes indica que os defensores estão em busca de ajuda especializada.

As empresas devem continuar elevando seu conhecimento em relação à preparação da segurança, e os profissionais de segurança devem liderar o crescimento de investimentos orçamentários para apoiar a tecnologia e seus funcionários. Além disso, a confiança aumentará quando os profissionais de segurança implantarem ferramentas que não só possam detectar ameaças, como também detenham seu impacto e aumentem o entendimento sobre maneiras de impedir ataques futuros.

Um olhar para o futuro

Um olhar para o futuro

Os especialistas em geopolítica da Cisco oferecem insights sobre o panorama em constante mudança do controle da Internet, inclusive as alterações na legislação de transferência de dados e o debate sobre o uso de criptografia. Esta seção também apresenta as descobertas específicas de dois estudos da Cisco. Um deles aborda as preocupações dos executivos com a segurança digital. O outro enfatiza as percepções dos tomadores de decisões de TI em relação aos riscos de segurança e credibilidade. Também apresentamos um resumo da importância de uma arquitetura de defesa integrada contra ameaças e fornecemos uma atualização sobre o progresso da Cisco na redução do tempo de detecção (TTD).

Perspectiva geopolítica: incerteza no panorama de controle da Internet

Na era pós Edward Snowden, o panorama geopolítico do controle da Internet mudou radicalmente. Atualmente, uma incerteza onipresente ronda o livre fluxo de informações entre fronteiras. O caso histórico do ativista de privacidade austríaco Max Schrems contra o gigante das redes sociais Facebook talvez tenha sido o mais impactante, levando o Tribunal de Justiça da União Europeia (CJEU) a anular o acordo de Safe Harbor com os EUA em 6 de outubro de 2015.[7]

Em virtude disso, as empresas agora são forçadas a confiar em mecanismos e formas de proteção legais diferentes do Safe Harbor quando transferem dados da UE para os Estados Unidos que, por sua vez, estão sujeitos à investigação. As empresas de dados ainda tentam avaliar as consequências dessa mudança. Embora as autoridades da União Europeia e dos EUA tenham trabalhado na obtenção de uma alternativa para o Safe Harbor nos últimos dois anos, o novo mecanismo previsto já desperta preocupações. É possível que essa alternativa não se concretize até janeiro de 2016 ou, o que é mais provável, não seja capaz de recuperar a confiança do mercado caso não aborde todas as preocupações do CJEU e, mais uma vez, esteja em risco de invalidação.[8]

Os especialistas em proteção de dados esperam que o Safe Harbor 2.0 cause tanta polêmica quanto a versão anterior. É possível que também seja contestado no tribunal e declarado inválido.[9]

A criptografia de ponta a ponta – o modo como ela beneficia consumidores e empresas e os desafios que cria para os órgãos de segurança pública em suas investigações de atividades criminosas e terroristas – também será um assunto de destaque nos debates entre os governos e o setor neste ano. Devido aos ataques terroristas em Paris, ocorridos em novembro de 2015, alguns políticos estão pressionando ainda mais para que se dê acesso ao conteúdo das comunicações criptografadas aos investigadores[10]. Isso pode impulsionar muito o desenvolvimento do Safe Harbor 2.0, já que as preocupações com os direitos civis cedem espaço para as preocupações com segurança.

[7] "The Court of Justice declares that the Commission's U.S. Safe Harbour Decision is invalid", CJEU, 6 de outubro de 2015: **http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.**

[8] "Safe Harbor 2.0 framework begins to capsize as January deadline nears" de Glyn Moody, *Ars Technica*, 16 de novembro de 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[9] "Safe Harbor 2.0 framework begins to capsize as January deadline nears" de Glyn Moody, *Ars Technica*, 16 de novembro de 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[10] "Paris Attacks Fan Encryption Debate," de Danny Yadron, Alistair Barr e Daisuke Wakabayashi, *The Wall Street Journal*, 19 de novembro de 2015: **http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407**.

Em um cenário de incertezas, o que as empresas devem perguntar aos provedores de dados para assegurarem que seus negócios estejam em conformidade com os regulamentos de transferência de dados? A curto prazo, elas devem buscar garantias dos fornecedores de que as Cláusulas do contrato modelo da UE ou as Regras corporativas associadas estão sendo seguidas, e não só o Safe Harbor, na transferência de dados para fora da UE.

Outro problema geopolítico importante que as empresas devem monitorar está relacionado às vulnerabilidades e explorações. Alguns governos mostram grande preocupação com o aumento de um mercado para vulnerabilidades sem correções, o assim chamado software como arma (weaponized software). Essas ferramentas são fundamentais para a comunidade de pesquisa de segurança, pois buscam maneiras de proteger as redes ao redor do mundo. No entanto, em mãos erradas, particularmente no caso de regimes repressivos, essa tecnologia criada para o bem poderá ser usada para crime financeiros, roubo de segredos nacionais e corporativos, eliminação de dissidentes políticos ou desorganização da infraestrutura principal.

Como restringir o acesso a vulnerabilidades não corrigidas sem impedir o progresso de pesquisas vitais é uma questão que os governos claramente enfrentarão em um futuro próximo. Ao tentarem lidar com esse problema complexo, os governos precisam avaliar com atenção como suas decisões políticas afetam a segurança. Por exemplo, a incerteza a respeito das leis que regem a transmissão de informações sobre vulnerabilidades não publicadas pode deter o avanço da pesquisa de ameaças de segurança ou incentivar a publicação de vulnerabilidades antes que os fornecedores tenham uma oportunidade de corrigi-las. Qualquer abordagem para resolver essa incerteza deverá ser compatível em todo o mundo.

As preocupações com a segurança digital pesam nas mentes dos executivos

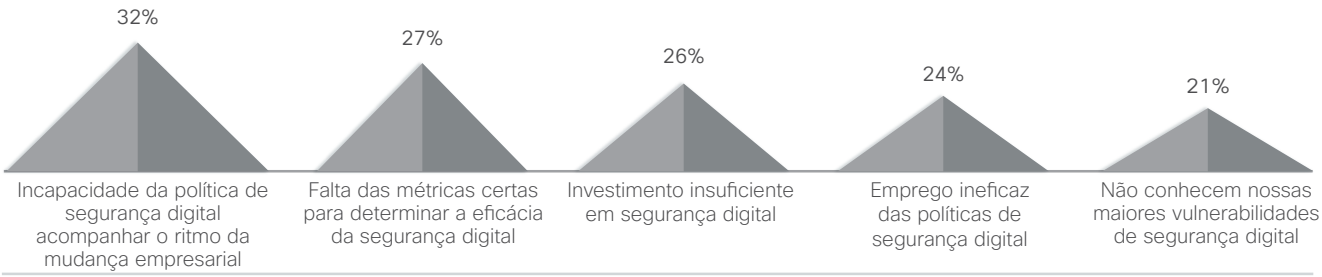
Obviamente, a segurança abrangente pode ajudar as empresas a evitar violações e ataques desastrosos. Mas ela pode ajudar a aumentar as chances de sucesso de uma empresa? De acordo com um estudo da Cisco de outubro de 2015 sobre o papel da segurança digital na estratégia digital e de negócios com executivos de finanças e linha de negócios, os executivos entendem que proteger suas empresas contra ameaças pode definir seu sucesso ou fracasso. À medida que as empresas se tornam mais digitais, o crescimento passa a depender da sua capacidade de proteger a plataforma digital.

Como mostra a pesquisa, a segurança digital é uma preocupação crescente para os executivos: 48% afirmaram estar muito preocupados e 39% disseram estar moderadamente preocupados com as violações de segurança digital. Essa preocupação é cada vez maior; 41% afirmaram se preocupar muito mais com as violações de segurança agora do que há três anos, e 42% disseram estar um pouco mais preocupados do que antes.

Os líderes empresariais também antecipam que os investidores e reguladores farão perguntas mais difíceis sobre os processos de segurança, assim como fazem perguntas sobre outras funções de negócios. 92% dos entrevistados concordaram que os reguladores e investidores vão esperar que as empresas forneçam mais informações sobre a exposição ao risco de segurança digital no futuro.

As empresas também parecem ter uma noção mais clara dos desafios de segurança digital que enfrentam. A incapacidade das políticas de segurança digital acompanharem a mudança empresarial foi o desafio mais comumente citado, seguido pela falta de métrica para determinar a eficácia da segurança (figura 62).

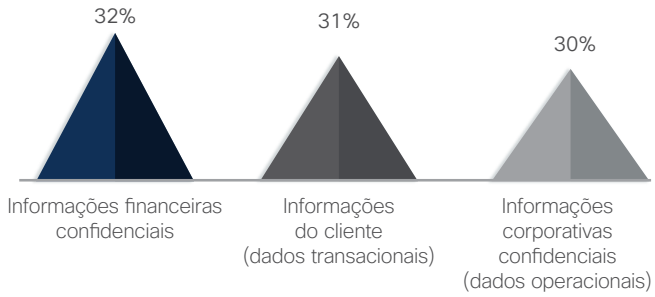
Figura 62. As empresas enfrentam difíceis desafios de segurança digital



Fonte: Cisco Security Research

Mais de um terço dos executivos também mostrou preocupação com a capacidade de proteger dados essenciais. Quando foi pedido que citassem os tipos de informações mais difíceis de proteger, 32% selecionaram a opção de "informações financeiras confidenciais". Os entrevistados citaram em segundo lugar "informações de cliente" e "informações corporativas confidenciais" como os dois tipos de dados mais difíceis de proteger (veja a figura 63).

Figura 63. Executivos preocupados em proteger dados importantes



Fonte: Cisco Security Research

Estudo de credibilidade: esclarecimento dos riscos e desafios para empresas

O aumento implacável das violações de segurança da informação enfatiza a necessidade de as empresas garantirem a segurança de seus sistemas, parceiros de negócios de dados, clientes e cidadãos. Nós observamos que a confiança se tornou um fator primordial para as empresas durante a seleção da infraestrutura de TI e redes. Na realidade, muitas exigem que a segurança e a credibilidade sejam integradas em todo o ciclo de vida do produto das soluções que compõem sua infraestrutura.

Em outubro de 2015, a Cisco realizou um estudo para avaliar as percepções dos responsáveis pelas decisões de TI sobre os desafios e riscos à segurança e também para determinar a função que a credibilidade do fornecedor de TI desempenha em seus investimentos em TI. Nossa pesquisa abrange tanto tomadores de decisões de segurança da informação, quanto de outros tipos de segurança em empresas de vários países. (Consulte o **Apêndice** para obter mais detalhes sobre o Estudo sobre o risco à segurança e credibilidade, inclusive nossa metodologia.)

ALGUMAS DESCOBERTAS DE 5NOSSA PESQUISA SÃO APRESENTADAS A SEGUIR:

Descobrimos que 65% dos entrevistados acham que a empresa onde trabalham enfrenta um nível significativo de risco à segurança, principalmente em decorrência do uso, na empresa, de soluções móveis, de segurança de TI e em nuvem (figura 64).

Figura 64. Percepções de risco à segurança

65%
dos entrevistados acham que suas empresas estão ameaçadas

A empresa acredita que as seguintes áreas de sua infraestrutura correm o risco de sofrer uma violação de segurança:

50%
de mobilidade

43%
de segurança de TI

42%
de dados em nuvem

Fonte: Estudo sobre o risco à segurança e confiabilidade, Cisco

COMPARTILHAR

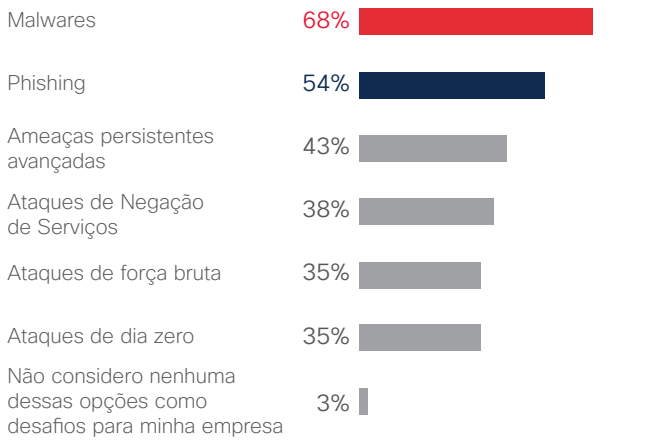
68% dos participantes do nosso estudo identificaram o malware como o principal desafio de segurança externa enfrentado pelas organizações. O phishing e outras ameaças avançadas persistentes completam a lista das três principais respostas: em 54% e 43%, respectivamente (veja a figura 65).

Quanto aos desafios de segurança interna (veja a figura 66), mais da metade (54%) dos participantes citaram downloads de software mal-intencionado como a principal ameaça, seguido por violações de segurança interna praticadas pelos funcionários (47%) e vulnerabilidades de hardware e software (46%).

Nós também verificamos que a maioria das empresas (92%) emprega uma equipe de segurança dedicada interna. 88% dos entrevistados relataram ter uma estratégia de segurança formal para toda a empresa, que é renovada regularmente. No entanto, apenas 59% padronizaram as políticas e os procedimentos em vigor para comprovar a credibilidade de fornecedores de TI (veja a figura 67).

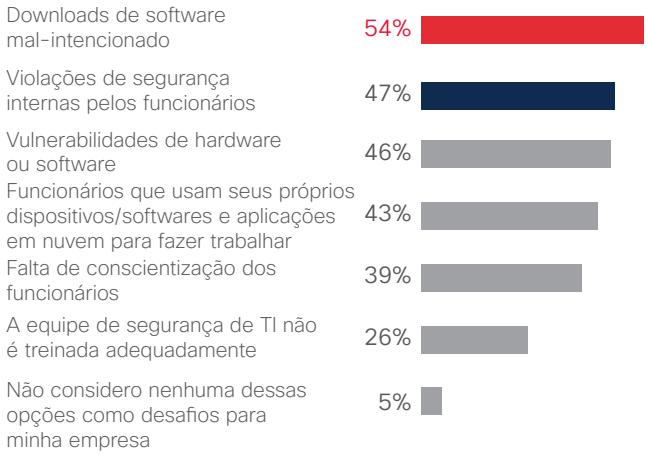
Além disso, cerca de metade (49%) das grandes empresas mantém a segurança de sua infraestrutura atualizada com as tecnologias mais recentes, e muitas outras atualizam sua infraestrutura regularmente. De acordo com nosso estudo, muito poucas esperam para atualizar apenas quando a tecnologia que utilizam fica obsoleta.

Figura 65. Desafios externos enfrentados (total de entrevistados)



Fonte: Estudo sobre o risco à segurança e confiabilidade, Cisco

Figura 66. Desafios internos de segurança enfrentados (total de entrevistados)



Fonte: Estudo sobre o risco à segurança e confiabilidade, Cisco

Figura 67. A grande maioria das empresas tem uma equipe interna dedicada à segurança

Fonte: Estudo sobre o risco à segurança e confiabilidade, Cisco

COMPARTILHAR

Como os fornecedores podem demonstrar credibilidade

No atual cenário centralizado em ameaças, a confiança nos processos do fornecedor, nas políticas, nas tecnologias e nas pessoas – e a capacidade de verificá-los – são a base para criar uma relação duradoura e de confiança entre os fornecedores e as empresas.

Os fornecedores de tecnologia demonstram credibilidade ao:

- Integrar segurança em suas soluções e na cadeia de valores desde a concepção
- Ter e seguir políticas e processos em vigor que possam reduzir o risco
- Criar uma cultura de conscientização de segurança
- Responder as violações de forma rápida e transparente
- Fornecer a correção rápida e a vigilância constante depois de um incidente

Obviamente, é uma boa prática atualizar a infraestrutura. Empresas de todos os tamanhos precisam implantar uma infraestrutura segura e confiável na qual a segurança esteja integrada em todos os aspectos da rede. No entanto, elas também podem ajudar a reduzir a superfície de ataque ao incentivarem uma cultura deconscientização da segurança aberta.

Para criar essa cultura, é necessário que as empresas implementem políticas e processos sólidos e abrangentes que assegurem a segurança presente em todos os aspectos da empresa. Elas devem trabalhar para ampliar essa mentalidade focada na segurança para seu ecossistema de parceiros e fornecedores e se esforçar o tempo todo para demonstrar transparência e responsabilidade com os clientes, parceiros e outros envolvidos.

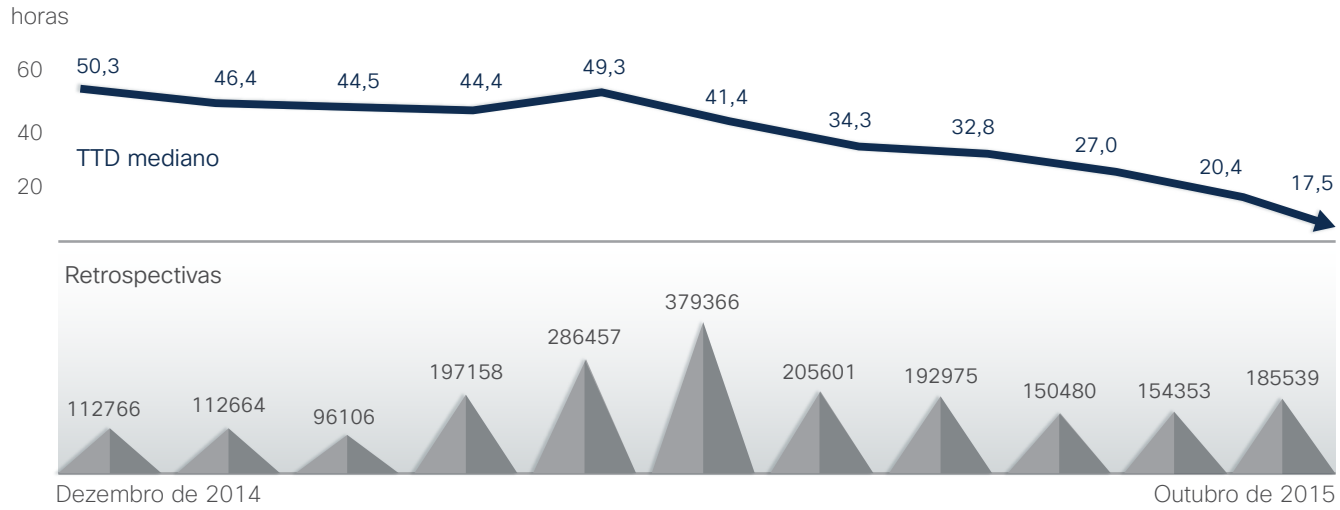
Tempo para detecção: a corrida para continuar a reduzir as opções

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

A categoria "retrospectivas" na Figura 68 mostra o número de arquivos que a Cisco categorizou inicialmente como "desconhecidos" e que depois foram considerados "reconhecidamente não confiáveis".

Conforme indicado no Relatório Semestral de Segurança da Cisco de 2015, o TTD médio foi de cerca de dois dias (50 horas).

Figura 68. Tempo para detecção, dezembro de 2014 a outubro de 2015



Fonte: Cisco Security Research

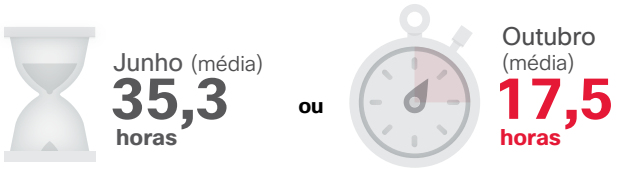
De janeiro a março, o TTD médio foi aproximadamente o mesmo: entre 44 e 46 horas, com ligeira tendência de queda. Em abril, ele subiu um pouco, para 49 horas. No entanto, no final de maio, o TTD da Cisco diminuiu para cerca de 41 horas.

Desde então, o TTD médio está em rápido declínio. Em outubro, a Cisco havia reduzido o TTD médio para cerca de 17 horas. Menos de um dia. Isso supera muito a estimativa atual de TTD do setor (100 a 200 dias). A velocidade se deve à inclusão de mais detalhes sobre como as infecções de curta duração são corrigidas.

A industrialização da invasão e o maior uso da base de malware desempenharam um papel importante em nossa capacidade de limitar as opções no TTD. Assim que uma ameaça ocorre em escala industrial, ela se torna mais disseminada e, portanto, é mais fácil detectá-la.

No entanto, também sugerimos que a combinação de defesas sofisticadas contra ameaças e a colaboração próxima aos talentosos pesquisadores de segurança talvez tenha sido ainda mais importante para nossa capacidade de reduzir, de modo significativo e consistente, o TTD médio no decorrer de 2015.

Figura 69. Comparação do tempo para detecção, dezembro de 2014 a outubro de 2015



Fonte: Cisco Security Research

A comparação do TTD na figura 69 mostra que, em junho, muitas ameaças foram detectadas em cerca de 35,3 horas. Já em outubro, mais ameaças foram interrompidas em cerca de 17,5 horas. Novamente, atribuímos em parte a redução no TTD médio a uma identificação mais rápida da base de malware, como Cryptowall 3.0, Upatre e Dyre. A integração de novas tecnologias, como as da ThreatGRID, uma empresa da Cisco, é outro fator.

No entanto, até mesmo com a janela de tempo menor para TTD, ainda é mais difícil detectar algumas ameaças do que outras. As ferramentas de download que visam usuários do Microsoft Word geralmente são as mais fáceis de detectar (<20 horas). As inserções de adware e do navegador estão entre as ameaças mais difíceis de detectar (<200 horas).

Um dos motivos para que essas últimas ameaças sejam tão difíceis de detectar é que, em geral, elas são consideradas como de prioridade mais baixa pelas equipes de segurança e, portanto, frequentemente ignoradas na corrida para deter o início dos ataques de dia zero praticados pelos criminosos (consulte "Infecções de navegador: disseminadas – e uma grande fonte de vazamento de dados" na **página 16**).

A figura 70 apresenta um resumo dos tipos de ameaças que geralmente são descobertas em 100 dias.

Figura 70. Nuvem (tag) por 100 dias

Fonte: Cisco Security Research

COMPARTILHAR

Os seis princípios da defesa integrada contra ameaças

No Relatório Semestral de Segurança da Cisco de 2015, os especialistas em segurança da Cisco sugerem que a necessidade de soluções adaptáveis levará a mudanças significativas no setor de segurança nos próximos cinco anos. Os resultados serão a consolidação do setor e um movimento unificado na direção de uma arquitetura de defesa contra ameaças integrada e escalável. Essa arquitetura fornecerá visibilidade, controle, inteligência e contexto em muitas soluções.

Essa estrutura de " detecção e resposta" permitirá uma resposta mais rápida tanto para ameaças conhecidas como para as emergentes. No núcleo dessa nova arquitetura haverá uma plataforma de visibilidade que fornece conscientização contextual completa e é atualizada o tempo todo para avaliar ameaças, correlacionar a inteligência local e global, e otimizar as defesas. A intenção dessa plataforma é criar uma base com a qual todos os fornecedores possam operar e contribuir. Com a visibilidade, há mais controle, o que leva a uma melhor proteção contra mais vetores de ameaças e a capacidade de contornar mais ataques.

Abaixo, apresentamos os seis princípios de defesa integrada contra ameaças para ajudar as empresas e seus fornecedores de segurança a compreenderem melhor o objetivo e os potenciais benefícios dessa arquitetura:

1. **Uma arquitetura de rede e segurança mais completa é necessária para abordar o volume crescente e a sofisticação dos agentes de ameaças.**

   Nos últimos 25 anos, o modelo tradicional de segurança foi algo como "se você vir um problema, compre uma caixa". No entanto, essas soluções, com frequência um conjunto de tecnologias de muitos fornecedores de segurança diferentes, não falam umas com as outras de maneira eficiente. Elas produzem informações e inteligência sobre eventos de segurança, que são integrados em uma plataforma de eventos e depois analisados por profissionais de segurança.

   Uma arquitetura integrada de defesa contra ameaças é uma estrutura de detecção e resposta que oferece mais recursos e suporte a respostas para ameaças com maior rapidez ao coletar mais informações da infraestrutura implementada de uma forma eficiente e automatizada. A estrutura observa o ambiente de segurança de modo mais inteligente. Em vez de apenas alertar as equipes de segurança sobre eventos suspeitos e violações de política, ela pode definir um cenário claro da rede e do que acontece nela para informar melhor os tomadores de decisões sobre a segurança.

2. **Apenas a melhor tecnologia não é suficiente para enfrentar o panorama atual e futuro de ameaças; ela só aumenta a complexidade do ambiente de rede.**

   As empresas investem nas melhores tecnologias de segurança, mas como sabem se essas soluções são realmente eficientes? As manchetes do ano passado sobre grandes violações de segurança são uma prova de que muitas tecnologias de segurança não funcionam bem. E quando elas falham, falham de verdade.

   A proliferação de fornecedores de segurança que oferecem as melhores soluções não ajuda a melhorar o cenário, a menos que esses fornecedores ofereçam soluções radicalmente diferentes (e não um pouco diferentes) das oferecidas pela concorrência. No entanto, atualmente, não há grandes diferenças entre os muitos produtos dos principais fornecedores na maioria das áreas de segurança.

3. **A maior quantidade de tráfego criptografado exigirá uma defesa integrada contra ameaças que pode convergir em atividade mal-intencionada criptografada, tornando determinados produtos ineficazes.**

   Como discutido neste relatório, o tráfego da Web criptografado está aumentando. Naturalmente, há bons motivos para o uso da criptografia, mas esse recurso também torna o rastreamento de ameaças um desafio para as equipes de segurança.

   A resposta para o "problema" da criptografia é ter mais visibilidade do que acontece nos dispositivos ou redes. As plataformas integradas de segurança podem ajudar nisso.

4. **As APIs abertas são essenciais para uma arquitetura integrada de defesa contra ameaças.**

   Os ambientes de vários fornecedores precisam de uma plataforma comum que ofereça maior visibilidade, contexto e controle. A criação de uma plataforma de integração de front-end pode oferecer suporte para uma melhor automação e aumentar a conscientização em relação aos próprios produtos de segurança.

5. **Uma arquitetura de defesa integrada contra ameaças requer a instalação e o gerenciamento de menos equipamentos e software.**

   Os fornecedores de segurança devem se esforçar para oferecer plataformas que tenham o maior número possível de recursos e que ofereçam funções extensivas em cada plataforma. Isso ajudará a reduzir a complexidade e a fragmentação no ambiente de segurança, que cria muitas oportunidades para o acesso fácil e a ocultação dos criminosos.

6. **Os aspectos de automação e coordenação de uma defesa integrada contra ameaças ajudam a reduzir o tempo para a detecção, contenção e correção.**

   A redução de falsos positivos ajuda as equipes de segurança a se concentrar no que é mais importante. A contextualização oferece suporte a uma análise da linha de frente dos eventos em curso, ajuda as equipes a avaliar se esses eventos exigem atenção imediata e pode produzir respostas automatizadas e análise mais profunda.

A força dos números: a importância da colaboração do setor

A colaboração do setor é essencial não só para o desenvolvimento de uma arquitetura futura para defesa integrada contra ameaças que permitirá uma resposta mais rápida às ameaças, como também para acompanhar o ritmo atual da comunidade global de agentes de ameaças cada vez mais audaciosos, inovadores e persistentes. Cada vez mais os criminosos implantam campanhas difíceis de detectar e altamente lucrativas. Agora, muitos deles empregam recursos legítimos na infraestrutura para embasar suas campanhas. E fazem isso com grande sucesso.

Dado esse panorama, é de ses esperar que os defensores pesquisados no nosso Estudo comparativo de recursos de segurança da Cisco de 2015 tenham menos confiança em sua capacidade de ajudar a proteger sua empresa. Sugerimos que os defensores considerem o poderoso impacto que a colaboração proativa e contínua do setor pode ter para revelar a atividade dos criminosos cibernéticos, minar sua capacidade de gerar receita e reduzir a oportunidade de iniciar ataques futuros.

Como amplamente discutido anteriormente neste relatório (consulte “Artigos” a partir da **página 10**), a colaboração entre um Colaborador parceiro da Cisco e dentro do nosso ecossistema Cisco Collective Security Intelligence (CSI), e a cooperação com os provedores de serviços foram fatores significativos na capacidade da Cisco de revelar, verificar e contornar as operações globais que envolvem o kit de exploração Angler e enfraquecer um dos maiores botnets de DDoS que nossos pesquisadores já viram, o SSHPsychos.

Sobre a Cisco

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 operacionalizada com centrada em ameaças da Cisco reduz a complexidade e a fragmentação, proporcionando maior visibilidade, controle constante e proteção avançada contra ameaças antes, durante e depois de um ataque.

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

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

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

Colaboradores do Relatório Anual de Segurança da Cisco de 2016

TALOS SECURITY INTELLIGENCE E RESEARCH GROUP

Talos é a empresa que cuida da inteligência de ameaças da Cisco, um grupo de de especialistas em segurança de elite dedicado a fornecer mais proteção para os 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 conhecidas e emergentes. O Talos mantém os conjuntos de regras oficiais de Snort.org, ClamAV, SenderBase.org e SpamCop e é a principal equipe a contribuir com informações de ameaças para o ecossistema Cisco CSI.

EQUIPE DE OTIMIZAÇÃO, TRANSFORMAÇÃO DE TI E SERVIÇOS AVANÇADOS EM NUVEM

A equipe fornece recomendações e otimiza as redes, o data center e as soluções de nuvem para os maiores provedores de serviços e empresas do mundo. Essa oferta de consultoria enfatiza a maximização da disponibilidade, do desempenho e da segurança das soluções mais importantes dos clientes. O serviço de otimização é fornecido a mais de 75% das empresas da Fortune 500.

EQUIPE DO ACTIVE THREAT ANALYTICS

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

CISCO THOUGHT LEADERSHIP ORGANIZATION

A Cisco Thought Leadership Organization identifica as oportunidades globais, as transições de mercado e as principais soluções que transformam as empresas, os setores e as experiências. A empresa fornece uma visão incisiva e preditiva do que as empresas podem esperar em um mundo que muda rapidamente, e como elas podem melhorar seu desempenho nas competições. Grande parte dos líderes de pensamento da equipe se concentram em ajudar as empresas a se tornar digitais ao unir os ambientes físico e virtual, de modo perfeito e seguro, para inovar com mais rapidez e atingir os resultados comerciais desejados.

COGNITIVE THREAT ANALYTICS

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

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 pró-tecnologia e regulamentos. Ao trabalhar de modo colaborativo com as partes interessadas do setor e os parceiros de 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 moldar decisões políticas em um nível global, nacional e local. A equipe da Global Government Affairs é formada por ex-representantes eleitos, parlamentares, reguladores, 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.

EQUIPE DO INTELLISHIELD

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

LANCOPE

A Lancope, uma empresa da Cisco, é líder no fornecimento de visibilidade de rede e inteligência de segurança para proteger as empresas contra as principais ameaças atuais. Ao analisar o NetFlow, o IPFIX e outros tipos de telemetria de rede, o Lancope's StealthWatch® System oferece análise de segurança com reconhecimento de contexto para detectar rapidamente uma ampla gama de ataques de APTs e DDoS a malware de dia zero e ameaças internas. Ao combinar o monitoramento lateral contínuo nas redes empresariais com reconhecimento de usuário, dispositivo e aplicação, a Lancope acelera a resposta a incidentes, aprimora as investigações forenses e reduz o risco corporativo.

OPENDNS

A OpenDNS, uma empresa da Cisco, é a maior plataforma de segurança fornecida na nuvem do mundo, e atende a mais de 65 milhões de usuários por dia, distribuídos em mais de 160 países. A OpenDNS Labs é a equipe de pesquisa de segurança da OpenDNS que oferece suporte para a plataforma de segurança. Para obter mais informações, visite **www.opendns.com** ou **https://labs.opendns.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 missões essenciais da empresa incluem proteger os clientes públicos e privados da Cisco, permitir e assegurar os esforços de Cisco Secure Development Lifecycle e Trustworthy Systems no portfólio de produtos e serviços da Cisco e proteger a empresa Cisco contra ameaças digitais 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 foco 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**.

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 inova para oferecer novos serviços, como Cisco's Custom Threat Intelligence (CTI), que pode identificar os indicadores de comprometimento que não foram detectados ou atenuados pelas infraestruturas de segurança atuais.

2Colaborador de parceiro da Cisco

LEVEL 3 THREAT RESEARCH LABS

A Level 3 Communications é um provedor de comunicações global premier com sede em Broomfield, Colorado, que fornece serviços de comunicações para empresas, governos e clientes de operadoras. Apoiada por grandes redes de fibra óptica em três continentes e conectada por instalações submarinas, nossa plataforma de serviços globais conta com recursos metropolitanos distribuídos que operam em mais de 500 mercados em mais de 60 países. A rede da Level 3 oferece uma visão abrangente do panorama global de ameaças.

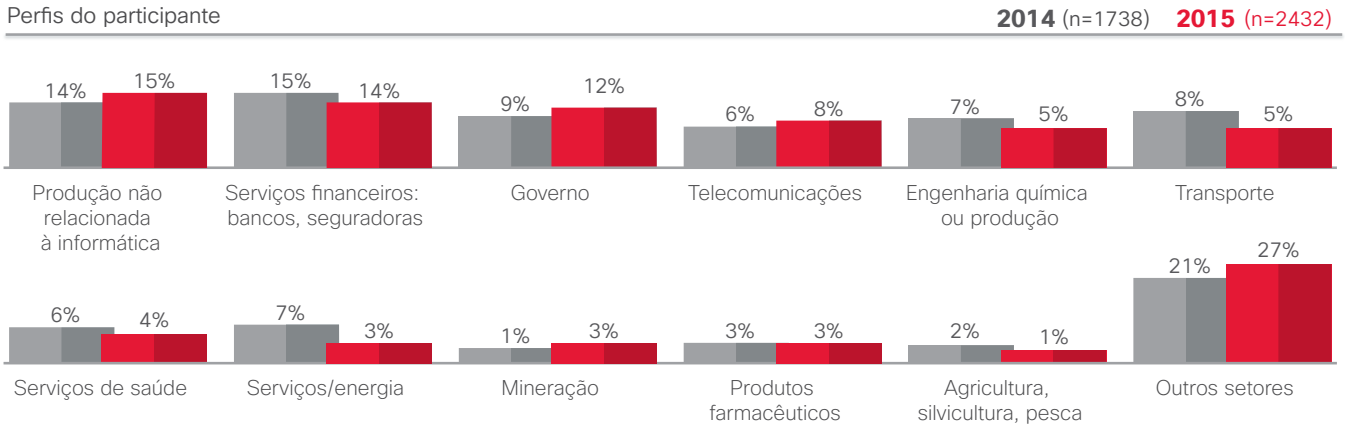
A Level 3 Threat Research Labs é o grupo de segurança que analisa proativamente o panorama global de ameaças e correlaciona informações entre fontes internas e externas para ajudar a proteger os clientes da Level 3, sua rede e a Internet pública. O grupo se associa regularmente aos líderes do setor, como Cisco Talos, colaborando na pesquisa e na atenuação de ameaças.

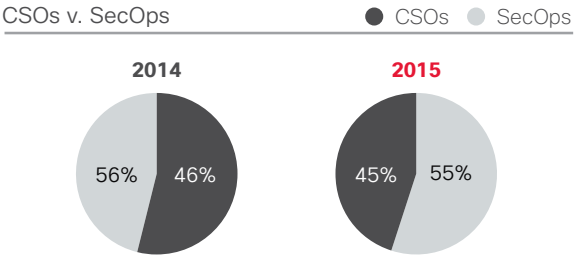
Apêndice

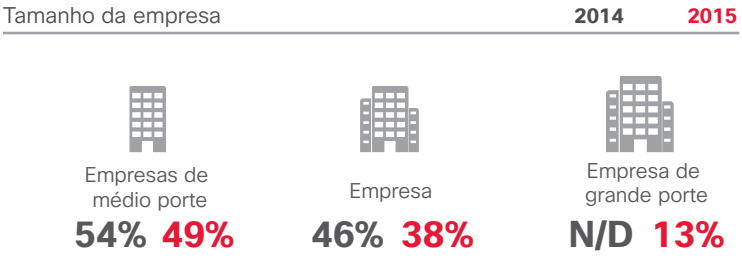
Apêndice

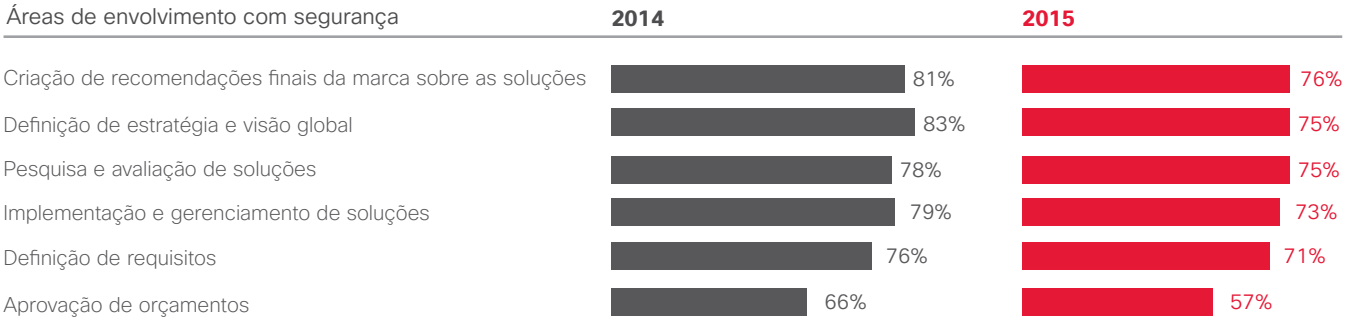
Estudo comparativo de recursos de segurança da Cisco de 2015: Perfis dos participantes e recursos

Figura 71. Perfis dos participantes





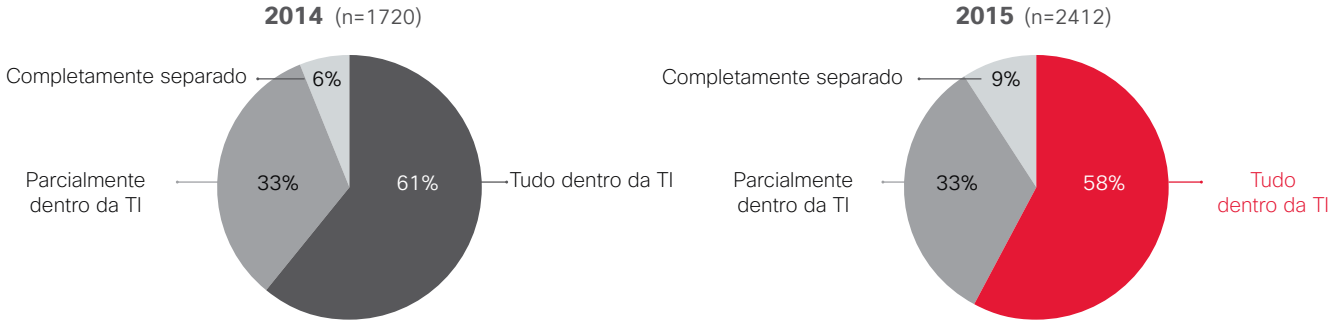




Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 72. Embora apenas 9% tenham um orçamento de segurança separado do orçamento de TI, essa tendência aumentou de modo significativo em 2014

O orçamento de segurança faz parte do orçamento de TI? (Membros do departamento de TI)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 73. Cargos: participantes e seus gerentes

Membros do departamento de TI

2014 **97%** ou 2015 **98%**

Departamento ou equipe dedicada à segurança

Membros de uma equipe de segurança

Cargo		Cargo de gerente	
Diretor de segurança	22%	Diretor executivo	34%
CTO	18%	Presidente/Proprietário	18%
Diretor ou Gerente de TI	16%	Diretor de segurança	16%
CIO	13%	CIO	6%
Diretor de operações de segurança	7%	CTO	6%
VP de segurança de TI	5%	Diretor ou Gerente de TI	4%
Diretor de risco e conformidade	4%	VP de segurança de TI	4%
Gerente de operações de segurança	4%	VP de TI	2%
Arquiteto de segurança	4%	Conselho executivo	2%
VP de TI	3%	Diretor de operações	1%
Diretor de operações	3%	Chefe do escritório financeiro	1%
Outro cargo	2%	Outro cargo	0%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 74. O firewall é a ferramenta de defesa contra ameaças de segurança mais comumente usada; poucas defesas contra ameaças de segurança são administradas por meio de serviços em nuvem em 2015, em comparação com 2014

Defesas contra ameaças à segurança usadas pela empresa	**2014** (n=1738)	**2015** (n=2432)	Defesas administradas através de serviços em nuvem (entrevistados da pesquisa de segurança que usam defesas contra ameaças de segurança) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Prevenção contra perda de dados	55%	56%		
Autenticação	52%	53%		
Criptografia/privacidade/proteção de dados	53%	53%		
Segurança de e-mail/envio de mensagens	56%	52%	37%	34%
Segurança da Web	59%	51%	37%	31%
Proteção de endpoints/antimalware	49%	49%	25%	25%
Controle de acesso/autorização	53%	48%		
Administração de identidades/provisionamento de usuários	45%	45%		
Prevenção contra intrusões*	N/D	44%		20%
Segurança da mobilidade	51%	44%	28%	24%
Sem fio seguro	50%	41%	26%	19%
Varredura de vulnerabilidades	48%	41%	25%	21%
VPN	48%	40%	26%	21%
Segurança das informações e gerenciamento de eventos	43%	38%		
Defesa contra DDoS	36%	37%		
Teste de penetração	38%	34%	20%	17%
Correção de falhas e configuração	39%	32%		
Peritagem judicial na área de redes	42%	31%		
Análise de endpoint	31%	26%		
Rede, segurança, firewalls e prevenção contra intrusões*	60%	N/D	35%	
Nenhuma das anteriores	1%	1%	13%	11%

*Firewall e a prevenção contra intrusões foram unificados em um código em 2014

*Segurança de rede, firewalls e prevenção contra intrusões.

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

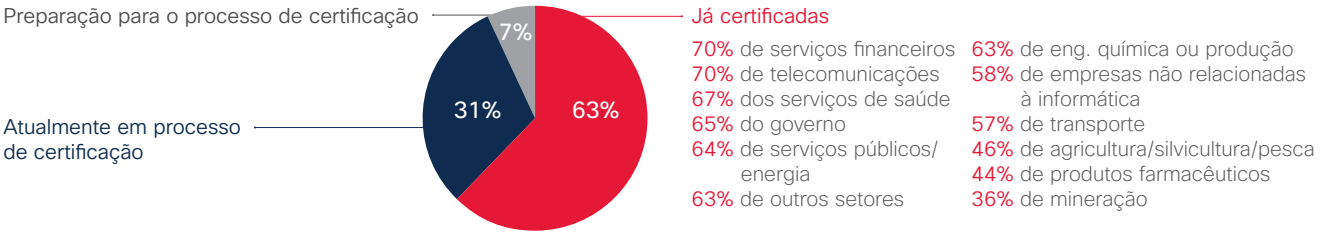
Terceirização

Figura 75. A consultoria ainda é o serviço de segurança mais terceirizado

Observação de aumentos significativos na terceirização de auditoria e resposta a incidente. A terceirização é vista como mais econômica.

Metade (52%) segue uma prática de política de segurança padronizada, como ISO 27001, a mesma do ano passado. Dessas, a grande maioria já obteve certificação ou está em processo de obtenção.

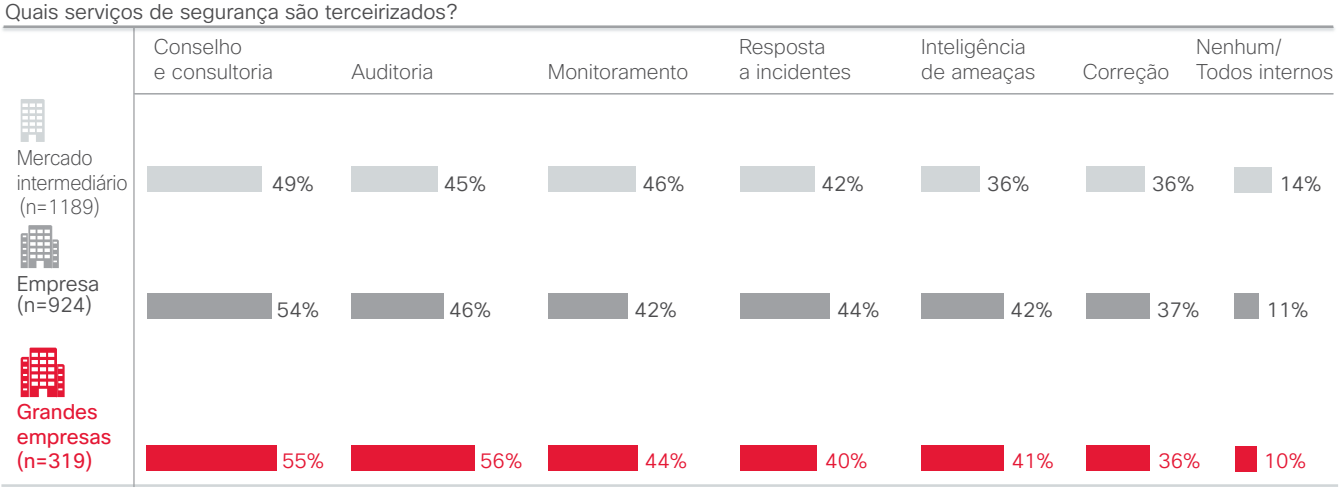
Prática de política de segurança padronizada
A empresa segue uma prática política de segurança de informações padronizada (**2015**: n=1265)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 76. Visão empresarial da terceirização: as grandes empresas apresentam cada vez mais probabilidade de terceirizar auditorias e consultorias

Quais serviços de segurança são terceirizados?



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

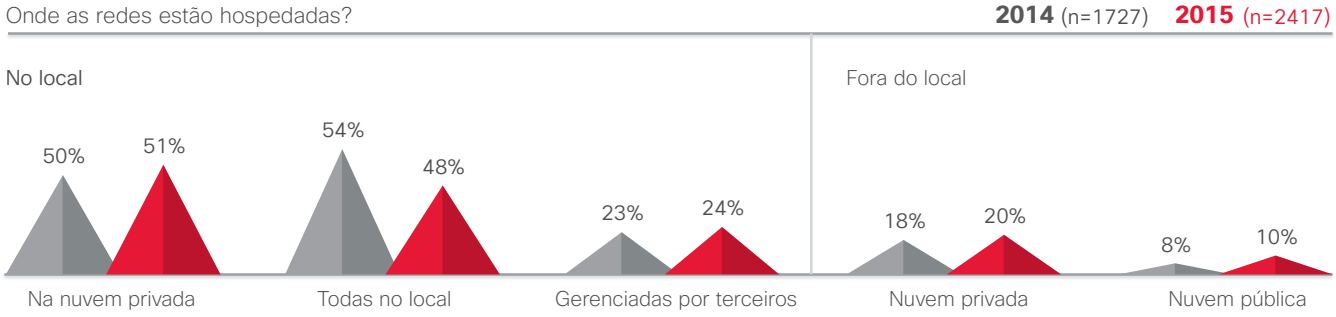
Figura 77. Visão da terceirização por país: o Japão apresenta uma probabilidade significativamente maior de terceirizar a consultoria

Quais serviços de segurança são terceirizados?

	TOTAL	Instalações	Brasil	Alemanha	Itália	Reino Unido	Austrália	China	Índia	Japão	México	Rússia	França
Conselho e consultoria	52%	52%	51%	49%	51%	44%	54%	52%	54%	64%	58%	41%	55%
Auditoria	47%	50%	55%	38%	48%	50%	36%	33%	51%	41%	63%	40%	59%
Monitoramento	44%	48%	49%	32%	39%	41%	52%	31%	51%	51%	49%	37%	50%
Resposta a incidentes	42%	46%	39%	32%	38%	43%	53%	34%	49%	53%	45%	27%	54%
Inteligência de ameaças	39%	42%	40%	37%	46%	36%	16%	36%	48%	47%	44%	42%	39%
Correção	36%	34%	32%	38%	34%	31%	47%	37%	41%	40%	21%	41%	41%
Nenhum/Todos internos	12%	18%	9%	18%	13%	19%	4%	19%	12%	10%	3%	16%	4%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 78. A hospedagem local das redes ainda é a situação mais comum. No entanto, a hospedagem fora do local aumentou desde o ano passado



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Violação de segurança pública

Figura 79. Em 2015, menos empresas relatam ter tido que gerenciar o escrutínio público de violações de segurança

As violações de segurança são fortes motivadores de aprimoramentos da segurança:

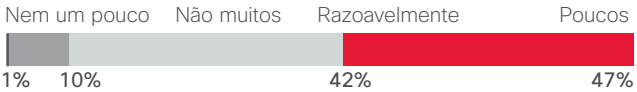
Em **2015** , menos empresas relataram ter tido que gerenciar o escrutínio público de violações de segurança, em comparação com o ano de **2014**.

2014 **53%** ou 2015 **48%**

Fonte: Estudo comparativo dos recursos de segurança da Cisco de 2015

Figura 80. As violações públicas podem melhorar a segurança

Quantos aprimoramentos a violação gerou nas suas políticas de defesa contra ameaças de segurança, procedimentos ou tecnologias? (n=1134)



Os CSOs mencionam mais aprimoramentos após a violação de segurança do que os gerentes de SecOps.

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Liderança e maturidade

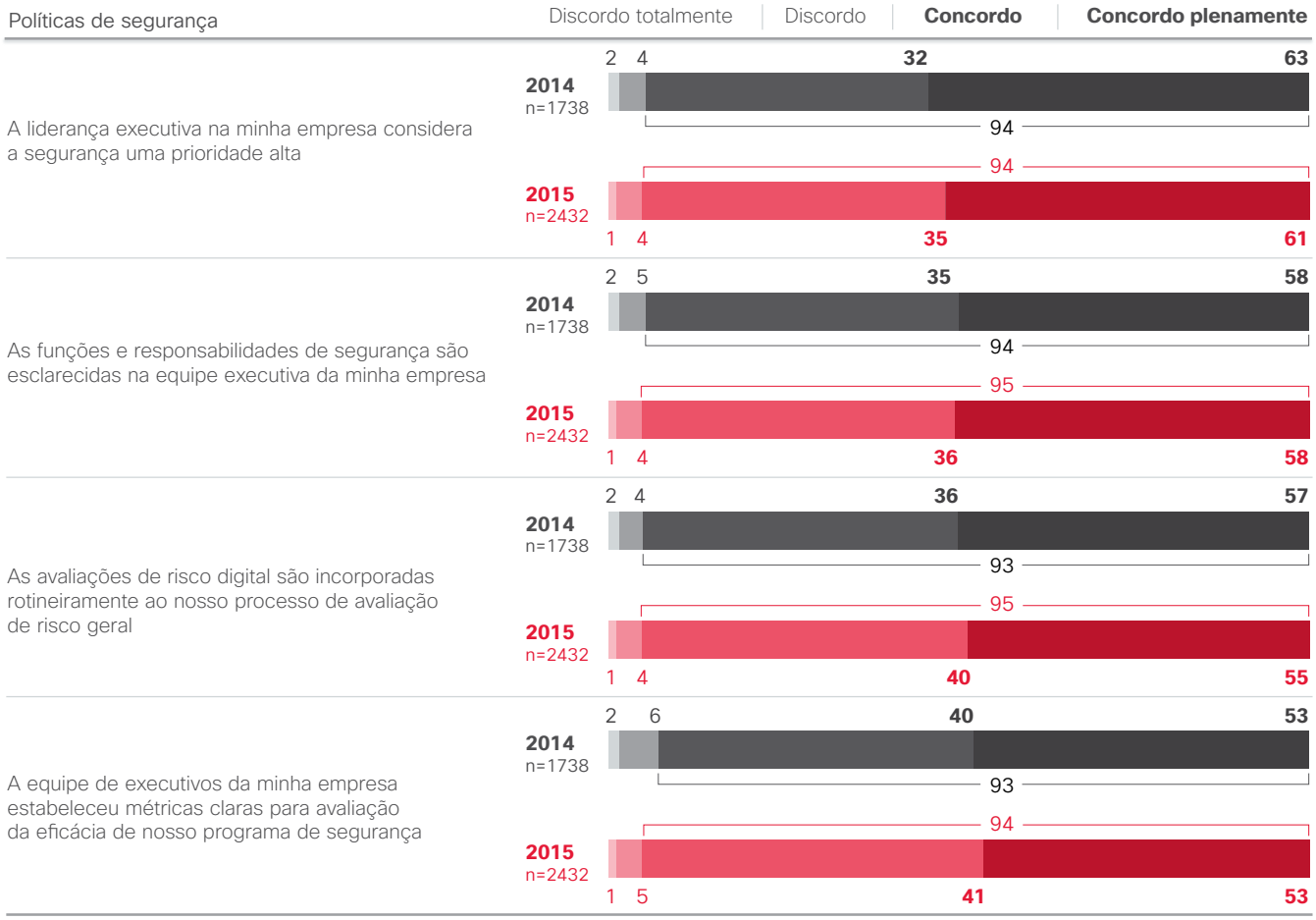
Figura 81. O modelo de 5 segmentos acompanha de perto o Security Capability Maturity Model (CMM)

Os segmentos refletem um padrão semelhante ao estudo do ano passado, em termos de maturidade em relação à prioridade de segurança e como isso se transforma em processos e procedimentos.

60% ou mais se adaptam mais aos perfis de segurança-maturidade. Isso é verdadeiro para a maior parte dos países e do setor.

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 82. Como em 2014, praticamente todos concordam ou concordam enfaticamente que a liderança executiva considera a segurança uma prioridade alta



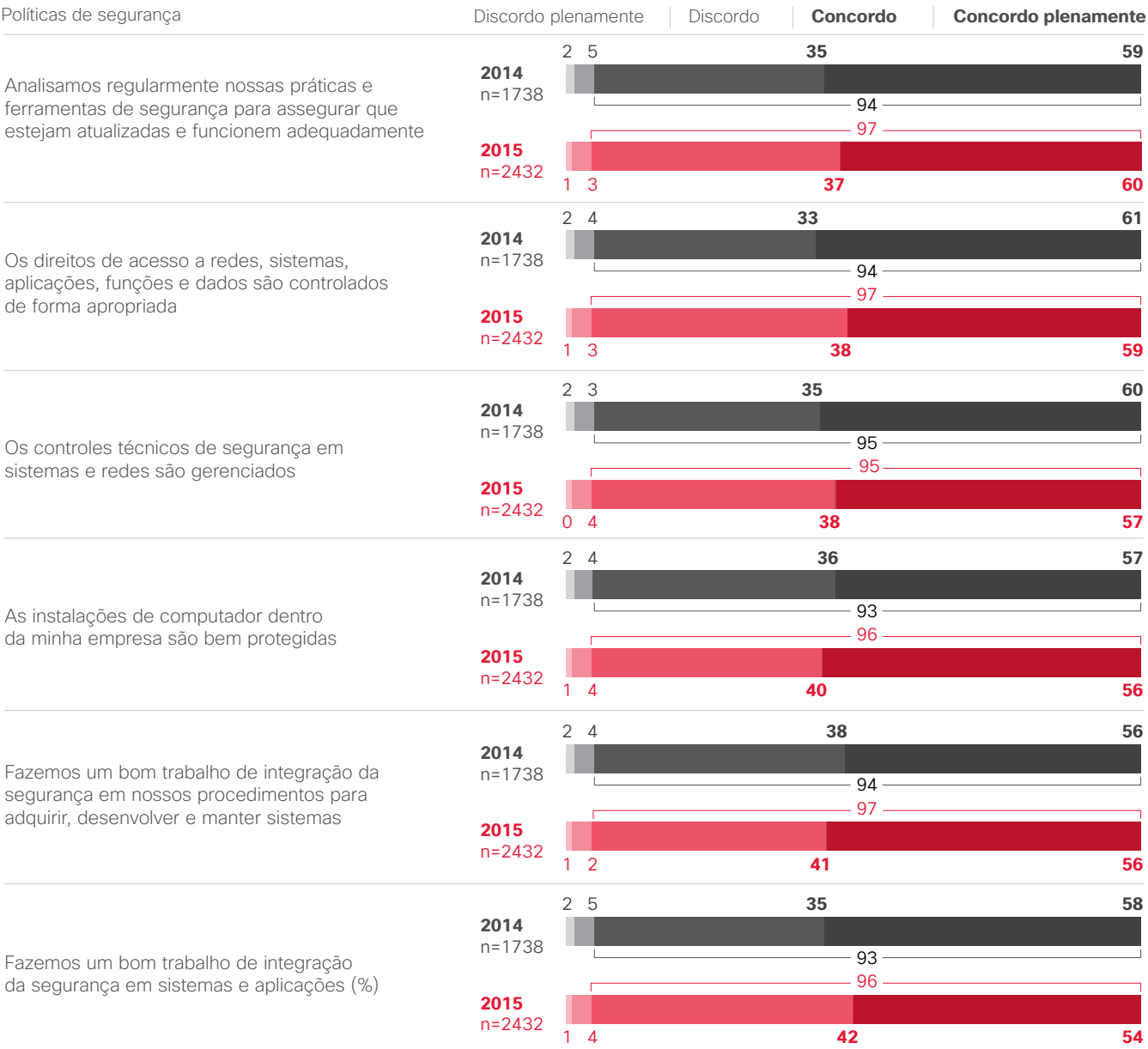
Um número significativo de farmacêuticos entrevistados respondeu que concorda enfaticamente com a declaração "a equipe executiva da minha empresa estabeleceu métricas claras para avaliar a eficácia de nosso programa de segurança" do que os profissionais da maioria dos outros setores.

Mais CSOs concordam com todas as declarações sobre o engajamento executivo, em comparação com SecOps.

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

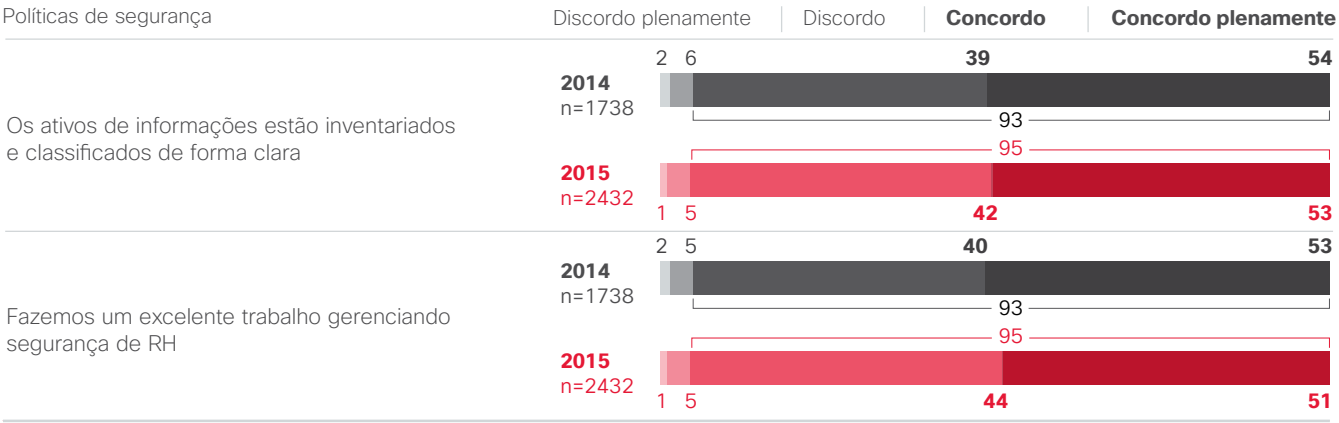
Processos

Figura 83. Menor confiança na capacidade de integrar a segurança aos sistemas



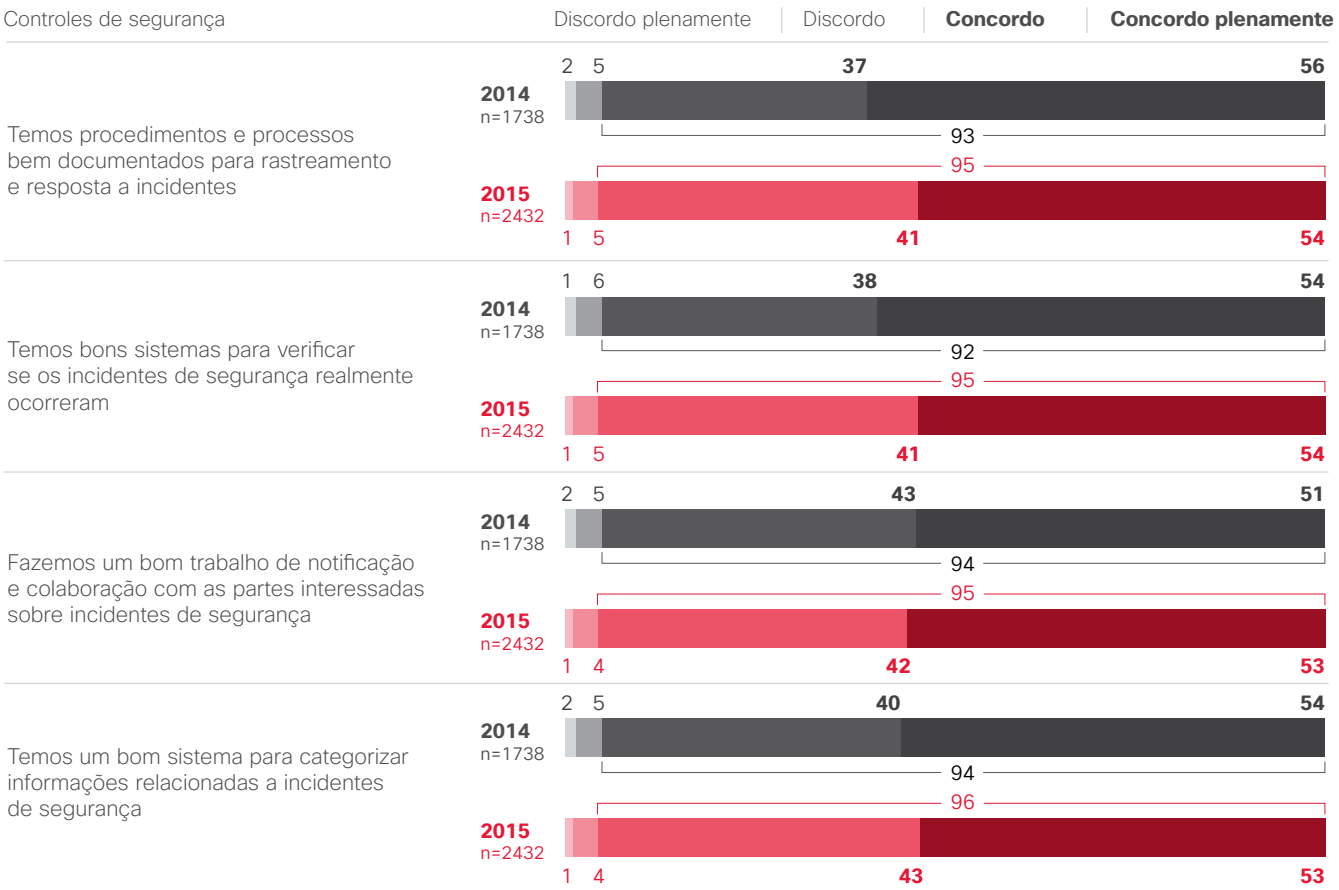
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 83. Menor confiança na capacidade de integrar a segurança aos sistemas (continuação)



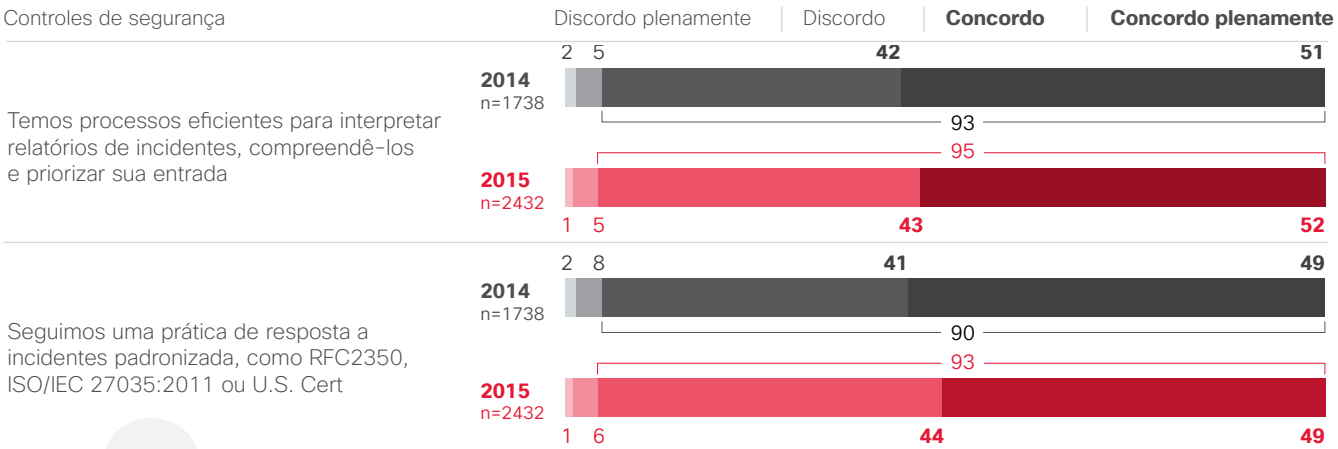
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 84. As empresas acreditam que têm bons controles de segurança



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 84. As empresas acreditam que têm bons controles de segurança (continuação)



Os entrevistados do setor de serviços financeiros apresentam maior probabilidade de concordar enfaticamente com a declaração "Temos um bom sistema para categorizar informações relacionadas a incidentes" do que os profissionais da maioria dos outros setores.

Com exceção da declaração "Fazemos um bom trabalho de notificação e colaboração com as partes interessadas sobre incidentes de segurança", os CSOs são mais positivos sobre os atributos que cercam os controles de segurança do que os gerentes de SecOps.

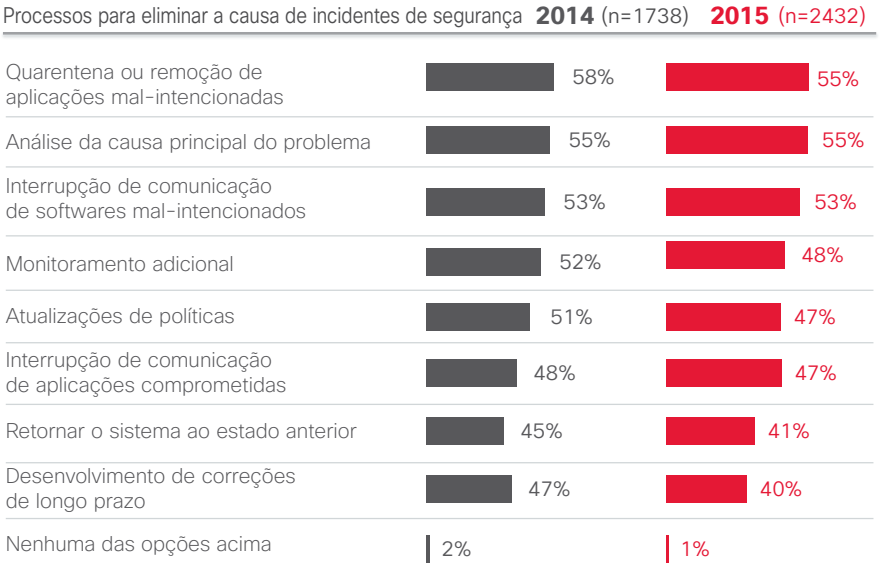
Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 85. A quarentena/remoção de aplicações mal-intencionadas e a análise da causa principal do problema ainda são os principais processos empregados

Mais entrevistados nos EUA respondem "nenhuma das opções acima" quando perguntados sobre processos para eliminar a causa de um incidente de segurança, em comparação com os entrevistados na maioria dos outros países.

Estados Unidos

Incidentes de segurança

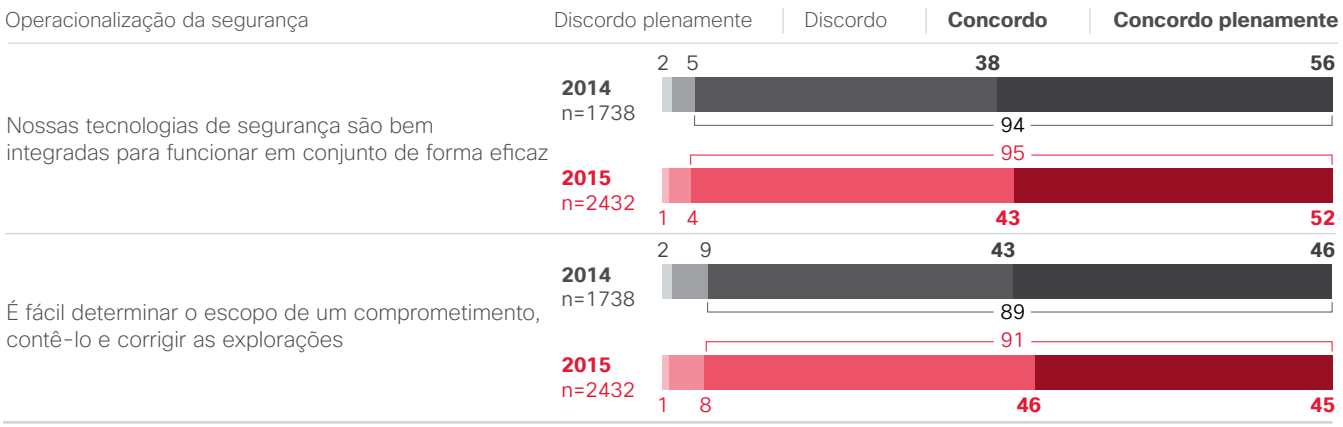


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 86. As empresas mostram pouca confiança na capacidade de evitar o comprometimento

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

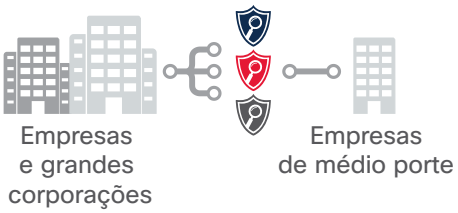
Figura 86. As empresas mostram pouca confiança na capacidade de evitar o comprometimento (continuação)

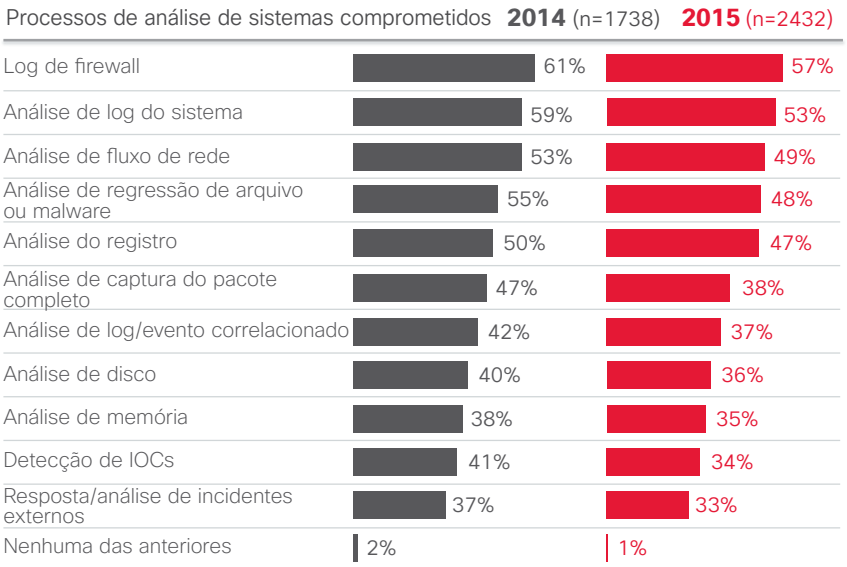


Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 87. Os logs de firewall e a análise de log de sistema continuam a ser os processos mais comumente usados para analisar os sistemas comprometidos

Empresas e grandes corporações relatam o uso de mais processos para análise de sistemas comprometidos do que empresas de médio porte.





Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 88. A restauração de um backup anterior ao incidente é o processo mais comum para restaurar os sistemas afetados em 2015

Os participantes na China dizem corrigir e atualizar aplicações de atualização consideradas vulneráveis com mais frequência do que os entrevistados em outros países pesquisados.

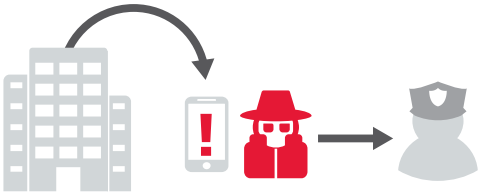
Processos para restaurar sistemas afetados	2014 (n=1738)	2015 (n=2432)
Restaurar usando um backup anterior ao incidente	57%	59%
Implementar controles e detecções novos ou adicionais, com base em pontos fracos identificados após o incidente	60%	56%
Correção de falhas e atualização de aplicações consideradas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

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 89. É mais provável que o CEO ou o presidente seja notificado sobre incidentes de segurança, seguido pelo departamento de operações e finanças

Mais entrevistados de grandes empresas mencionam que notificam autoridades externas em caso de um incidente do que os entrevistados de empresas de médio porte.

Empresa de grande porte



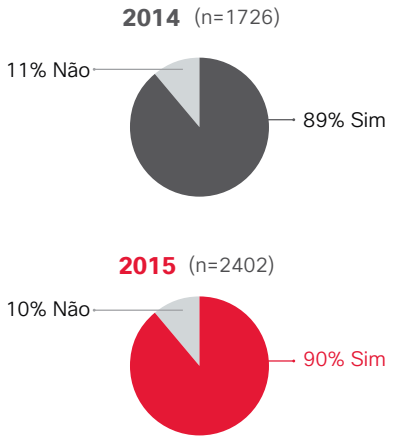
Grupos notificados em caso de incidente	2014 (n=1738)	2015 (n=2432)
Diretor executivo	N/D	45%
Operações	46%	40%
Departamento financeiro	N/D	40%
Parceiros de tecnologia	45%	34%
Engenharia	38%	33%
Recursos Humanos	36%	33%
Jurídico	36%	32%
Produção	33%	28%
Todos os funcionários	35%	27%
Relações públicas	28%	24%
Parceiros comerciais	32%	21%
Autoridades externas	22%	18%
Empresas de seguro	N/D	15%

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

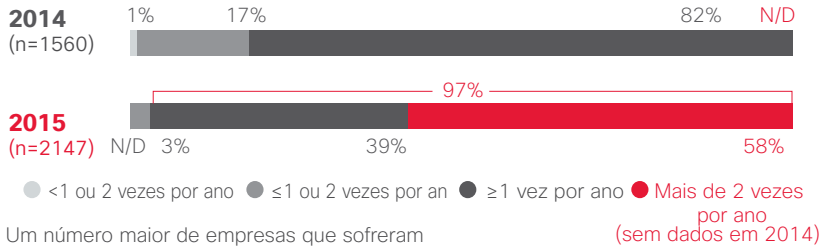
Treinamento

Figura 90. Quase todas as empresas (97%) oferecem treinamento em segurança pelo menos uma vez por ano

Os programas de treinamento e/ou conscientização da segurança são oferecidos à equipe de segurança regularmente? (Entrevistados dedicados à segurança)



Com que frequência é oferecido o treinamento de segurança? (Entrevistados cujas equipes de segurança recebem treinamento)



Um número maior de empresas que sofreram uma violação realiza regularmente programas de conscientização/treinamento de segurança (96%) do que as empresas que não sofreram uma violação (83%).

96% tem v. não tem **83%**

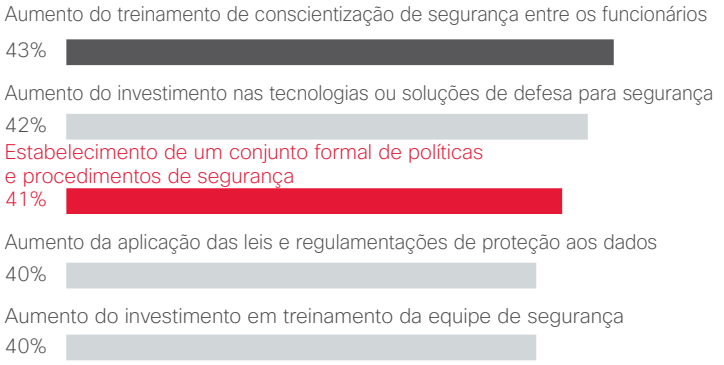
Um número maior de grandes empresas afirma realizar programas de conscientização/treinamento de segurança regularmente (93%), em comparação com empresas de médio porte (88%) e empresas (89%).

Empresa de grande porte **93%** Empresas **88%** de médio porte **89%**

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Figura 91. A frequência do treinamento para conscientização de segurança e a incidência de políticas de segurança formais estão ambas em alta desde 2014 – comprovação de ação

(5 principais menções) Participantes afetados por uma violação de segurança (**2015** n=1109)



Aumento do treinamento de conscientização de segurança entre os funcionários

Em 2015, 43% dos entrevistados disseram ter aumentado o treinamento de segurança depois de uma violação pública.

43%

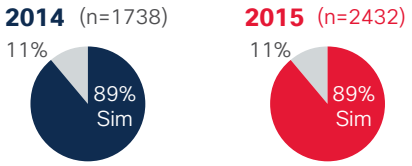
Em 2015, 41% dos entrevistados afirmaram ter estabelecido um conjunto formal de políticas e procedimentos de segurança.

41%

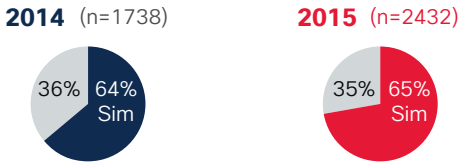
Fonte: Estudo comparativo dos recursos de segurança da Cisco de 2015

Figura 92. Desde 2014, praticamente 9 em 10 pessoas afirmam que sua equipe de segurança participa de conferências com foco em segurança ou treinamento

Os membros da equipe de segurança assistem a conferências e/ou fazem treinamentos externos para melhorar e manter suas qualificações profissionais? (Entrevistados dedicados à segurança)



Os funcionários trabalham em comitês ou conselhos do setor de segurança? (Entrevistados dedicados à segurança)



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2015

Estudo sobre risco à segurança e credibilidade

Figura 93. Histórico e metodologia

A Cisco está interessada em obter um entendimento mais profundo das percepções que os tomadores de decisões empresariais e de TI do provedor de serviços têm sobre os riscos e desafios de segurança da sua empresa, e da função que a credibilidade do fornecedor de TI desempenha nas compras de soluções de TI.

Os objetivos específicos incluem:

- Aprimorar o nível de risco de ameaças e vulnerabilidades externas e internas
- Entender as estratégias, políticas e soluções que estão sendo implementadas para diminuir os riscos à segurança
- Identificar o processo de compra de soluções de TI e a função de credibilidade de fornecedores de TI nesse processo
- Aprimorar o interesse em receber comunicados sobre como comprovar a credibilidade de fornecedores de TI
- Determinar se há diferenças nas perspectivas ou abordagens de risco à segurança para atenuar os riscos em todos os setores e no público

Metodologia: abordagem quantitativa e qualitativa

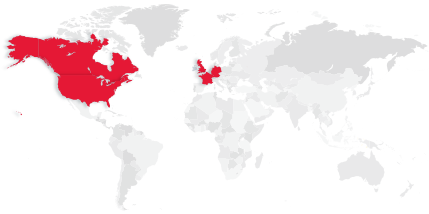
Duas metodologias foram usadas para fornecer insight em cada um desses objetivos de pesquisa:

(Todos os participantes envolvidos na tomada de decisão de compra de TI)

Pesquisa quantitativa na Web com
1050 ITDMs empresarias
(402 dos EUA, 282 do RU, 197 da Alemanha, 169 da França)

Entrevistas qualitativas detalhadas com
20 provedores de serviços
(7 dos EUA, 3 do Canadá, 3 do RU, 4 da Alemanha, 3 da França)

A pesquisa foi realizada. nos EUA, no Reino Unido, na França, na Alemanha e no Canadá (IDIs apenas)



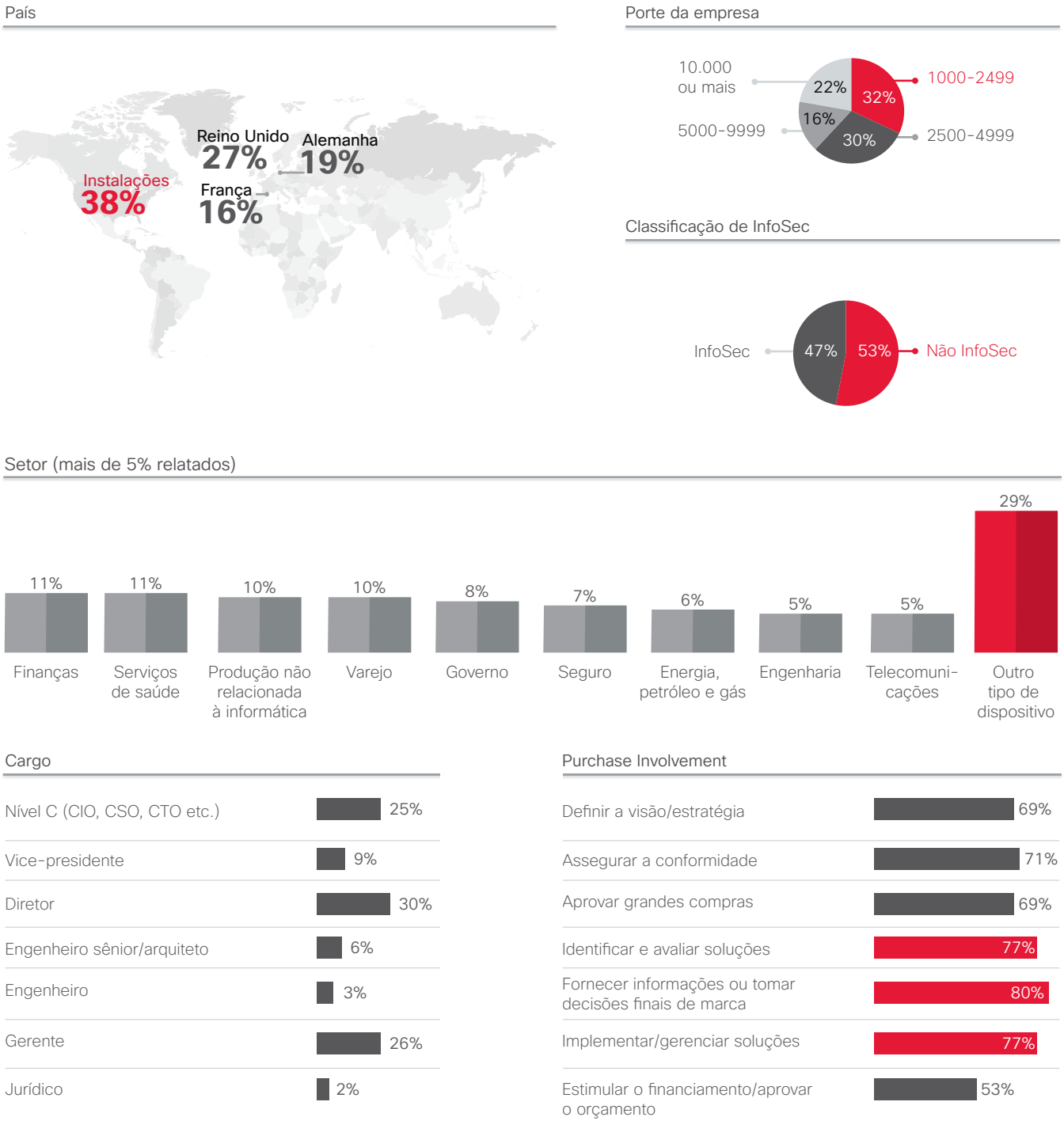
A coleta de dados ocorreu de agosto a setembro de 2015

20 Minuta da pesquisa com base na Web

45 Minuta das entrevistas detalhadas

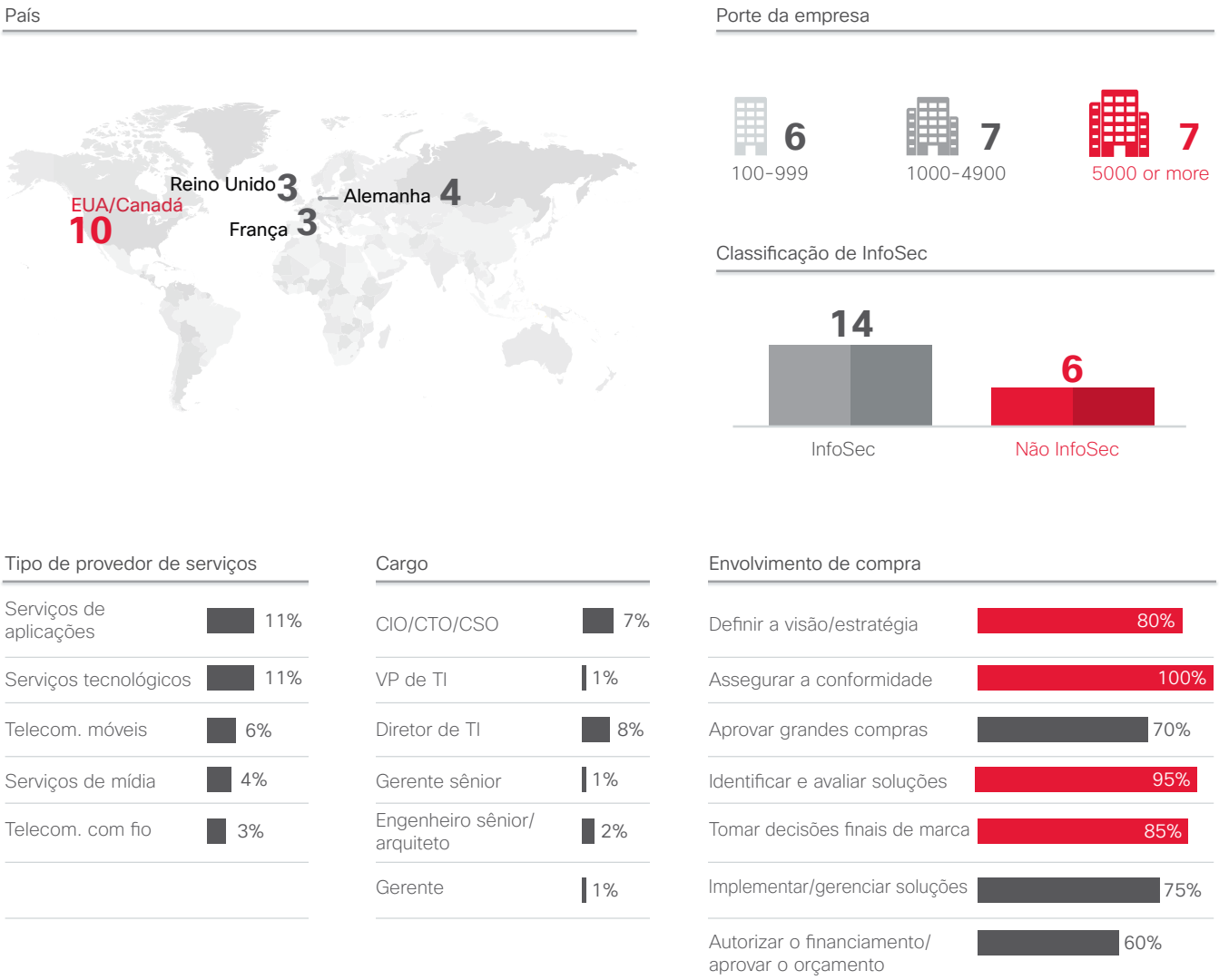
Fonte: Estudo sobre risco à segurança e credibilidade, Cisco

Figura 94. Perfil quantitativo do participante da empresa



Fonte: Estudo sobre risco à segurança e credibilidade, Cisco

Figura 95. Perfil do participante do provedor de serviços: qualitativo



Fonte: Estudo sobre risco à segurança e credibilidade, Cisco

Sede - América
Cisco Systems. Inc
San Jose. CA

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

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

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

Publicação: janeiro de 2016