Microsoft

RELATÓRIO DE INTELIGÊNCIA EM SEGURANÇA DA MICROSOFT

VOLUME 24
JANEIRO – DEZEMBRO 2018

Sumário

Este documento é apenas para fins informativos. A MICROSOFT NÃO OFERECE NENHUMA GARANTIA, EXPRESSA, IMPLÍCITA OU ESTATUTÁRIA, QUANTO ÀS INFORMAÇÕES NESTE DOCUMENTO.

Este documento é fornecido "no estado em que se encontra". As informações e as opiniões expressas neste documento, incluindo URLs e outras referências a sites, podem ser alteradas sem aviso prévio. Você assume o risco de utilização.

Os nomes de empresas e produtos reais aqui mencionados podem ser marcas registradas dos respectivos proprietários.

Autores e colaboradores

Abhishek Agrawal
Proteção de informações

David Fantham
Proteção de informações

Debraj Ghosh
Marketing de segurança da Microsoft

Diana Kelley
Grupo de soluções de segurança cibernética

Elia Florio
Defesa ativa do Windows

Eric Avena
Equipe de pesquisa do Windows Defender

Eric Douglas
Equipe de pesquisa do Windows Defender

Francis Tan Seng
Equipe de pesquisa do Windows Defender

Jonathan Trull
Grupo de soluções de segurança cibernética

Joram Borenstein
Grupo de soluções de segurança cibernética

Karthik Selvaraj
Equipe de pesquisa do Windows Defender

Kasia Kaplinska
Marketing de segurança da Microsoft

Kristina Laidler
Resposta a incidentes de segurança

Matt Duncan
Análise e engenharia de dados da defesa ativa do Windows

Mark Simos
Grupo de soluções de segurança cibernética

Paul Henry
Wadeware LLC

Pragya Pandey
Marketing de segurança da Microsoft

Ram Pliskin
Segurança do Azure

Ryan McGee
Marketing de segurança da Microsoft

Seema Kathuria
Grupo de soluções de segurança cibernética

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Equipe de pesquisa do Windows Defender

Volv Grebennikov
Bing

Yaniv Zohar
Segurança do Azure

Prefácio

Olá. Seja bem-vindo à 24ª edição do Relatório de Inteligência em Segurança (SIR) da Microsoft. Como profissional praticante e arquiteta de segurança, leio relatórios como este com o objetivo de entender um pouco melhor o panorama com a conclusão de recomendações práticas sobre como usar esse conhecimento para defender e proteger as organizações de forma mais eficiente.

A equipe do SIR traz o espírito de educação para o aprimoramento da resiliência cibernética a este relatório e conduziu análises ao longo de um ano de dados para selecionar as lições mais importantes.

O que você está lendo são os insights obtidos de um ano de análise de dados de segurança e as lições práticas aprendidas. Os dados analisados incluem 6,5 trilhões sinais de ameaça que passam pela nuvem da Microsoft todos os dias e as experiências de pesquisa do mundo real de nossos milhares de pesquisadores de segurança e entrevistados em todo o mundo. Em 2018, os invasores usaram uma grande variedade de truques mal-intencionados, tanto novos (mineração de moedas virtuais) quanto antigos (phishing), em sua missão contínua de roubar dados e recursos de clientes e organizações. Ataques híbridos, como a campanha Ursnif, combinaram abordagens sociais e técnicas. À medida que os defensores ficaram mais inteligentes contra ransomware, uma forma chamativa e inovadora de ataque, os criminosos se voltaram às mais "furtivas", mas ainda rentáveis mineradoras de moedas virtuais.

Essa mudança de foco pode ser frustrante, como se os invasores sempre estivessem um passo à frente. Mas, vista de outro ângulo, essa é uma história positiva. Os defensores e profissionais de segurança cibernética, como você, implementaram técnicas defensivas que forçaram os invasores a mudarem suas cargas preferenciais e se afastarem do ransomware.

Outra área em que os criminosos cibernéticos aumentaram sua atividade foi a cadeia de fornecedores. Um dos mais conhecidos, o surto da mineradora de moedas virtuais Dofoil, que começou em 6 de março de 2018, foi iniciado por um aplicativo ponto a ponto infectado. As preocupações da cadeia de fornecedores foram além dos aplicativos e da nuvem e incluíram extensões de navegador maliciosas, repositórios do Linux comprometidos e várias instâncias de módulos de backdoor. Para abordar essa ameaça, as organizações estão avançando em direção a um modelo de cadeia de fornecedores transparente e confiável.

Os dados são ótimos, mas às vezes é importante descobrir o que realmente aconteceu em uma organização. É por isso que incluímos as lições aprendidas no campo de nossa equipe de detecção e resposta (DART). Elas incluem como uma grande empresa de manufatura foi capaz de implementar controles para bloquear uma campanha de phishing de várias fases que a incomodava há meses e organizações de serviços financeiros finalmente conseguiram erradicar os agentes de ameaças de seus sistemas usando ferramentas avançadas de investigação e monitoramento de pontos de extremidade.

Por último, mas não menos importante, os cliques de phishing continuaram a aumentar, mas os modelos de machine learning estão melhorando na captura de phishing antes que chegue às caixas de entrada dos usuários e impedindo danos após possíveis cliques. Mais boas notícias? Um número crescente de empresas estão implementando soluções multifatoriais para limitar o sucesso de emails de phishing para roubo de credenciais.

Os invasores buscam oportunidades, por isso, quanto mais soubermos sobre as suas técnicas e táticas operacionais, melhor estaremos preparados para criar defesas e responder rapidamente. Pequenos passos importantes podem fazer uma enorme diferença na integridade geral da segurança cibernética de uma organização. É por isso que, juntamente com insights profundos sobre a mudança no cenário de malware e ataques, você encontrará os passos recomendados e outras orientações de práticas recomendadas neste relatório. Porque, quando eu era uma profissional praticante, isso era exatamente o que precisava na minha luta contra os bandidos. Esperamos que seja o que você precisa também.

Diana Kelley
CTO de campo da Microsoft Cybersecurity

P.S. Estamos sempre procurando melhorar o SIR. Se tiver comentários, entre em contato e conte-nos sua opinião.

SEÇÃO I

Ransomware, mineração de criptomoedas e dinheiro

Em sua maioria, as grandes histórias de segurança de 2017 envolveram ransomware. Surtos de alto perfil em todo o mundo de WannaCrypt e Petya impulsionaram o ransomware, um tipo de malware que bloqueia ou criptografa computadores e, em seguida, exige dinheiro para restaurar o acesso, para o conhecimento geral, e muitos especularam que o problema só aumentaria no futuro. Em vez disso, encontros de ransomware diminuíram significativamente em 2018.

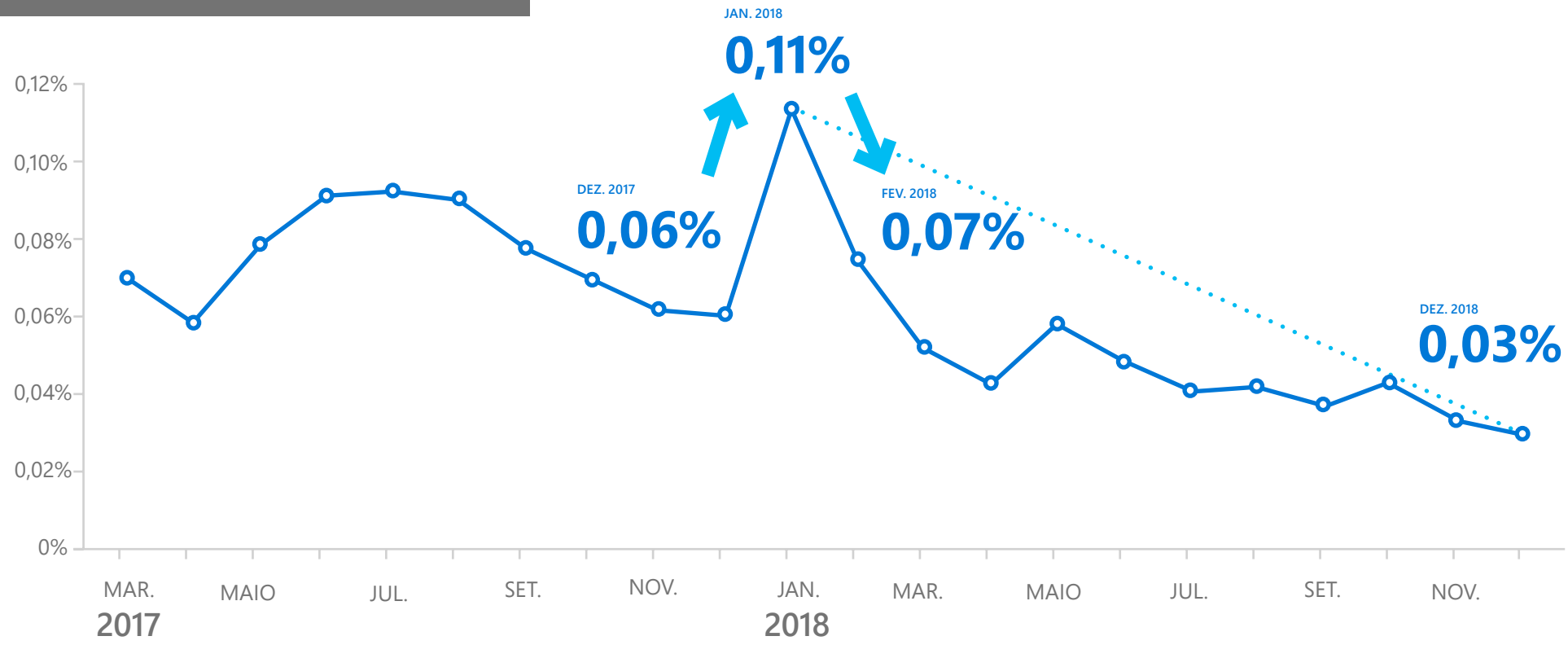
A diminuição dos encontros de ransomware foi devido, em parte, à melhoria na detecção e no treinamento, que tornaram mais difícil para os invasores lucrarem com isso. Como resultado, os invasores começaram a mudar seus esforços do ransomware para abordagens como a mineração de criptomoedas, que usa os recursos de computação das vítimas para fornecer dinheiro digital para os invasores. A mudança demonstra a natureza fundamentalmente oportunista da maioria dos criminosos cibernéticos orientados para o lucro: eles tendem a perseguir o dinheiro da forma mais fácil disponível, e, quando a economia do crime cibernético muda, eles são rápidos para acompanhar essa mudança.

ATAQUES DE RANSOMWARE EM DECLÍNIO

Há mais de uma década, os hackers e os usuários pregando peças que dominavam o sub-mundo inicial do malware foram substituídos pelo crime organizado e por outros interesses orientados para o lucro. Considerando que os surtos de malware iniciais eram muitas vezes chamativos e óbvios, era muito mais provável que o malware orientado para o lucro operasse silenciosamente e evitasse atrair a atenção, a fim de continuar a desempenhar a sua função (envio de spam, roubo de informações confidenciais, condução de ataques de negação de serviço e outras atividades maliciosas) pelo máximo de tempo possível.

O ransomware rejeitou essa tendência. Em vez de tentar continuar não detectado, o ransomware nega abertamente às vítimas o acesso aos seus computadores e arquivos importantes até que a vítima pague pelo resgate (e mesmo depois disso, os invasores muitas vezes não liberaram o controle dos computadores, mesmo depois que o resgate é pago). Enquanto o ransomware estava no auge em 2017, parecia que este estilo de ataque aberto poderia representar uma nova fase nas técnicas dos invasores. Mas os dados mais recentes sugerem que o ransomware pode estar em declínio, com os invasores cada vez mais retornando ao modo de operação mais furtivo que empregaram no passado, buscando voar abaixo do radar, a fim de conduzir ataques de forma mais eficiente, como a mineração de criptomoedas. Embora tenha havido um declínio na taxa de encontros de ransomware, isso não significa necessariamente que a gravidade dos ataques diminuiu.

Taxa de encontros de ransomware



As taxas de encontro de ransomware diminuíram em aproximadamente 60% entre março de 2017 e dezembro de 2018, com aumentos intermitentes em todo esse período.

FIGURA 1.

Encontros de ransomware de março de 2017 a dezembro de 2018

Provavelmente, há muitas causas para esse declínio em geral, embora os pesquisadores de segurança da Microsoft suspeitem que um dos principais fatores é que os usuários finais e as organizações estão se conscientizando mais e lidando de forma mais inteligente com ameaças de ransomware, inclusive ao agir com maior cautela e fazer backup de arquivos importantes para que possam ser restaurados se forem criptografados por ransomware. Além disso, como descrito anteriormente, os criminosos cibernéticos são oportunistas.

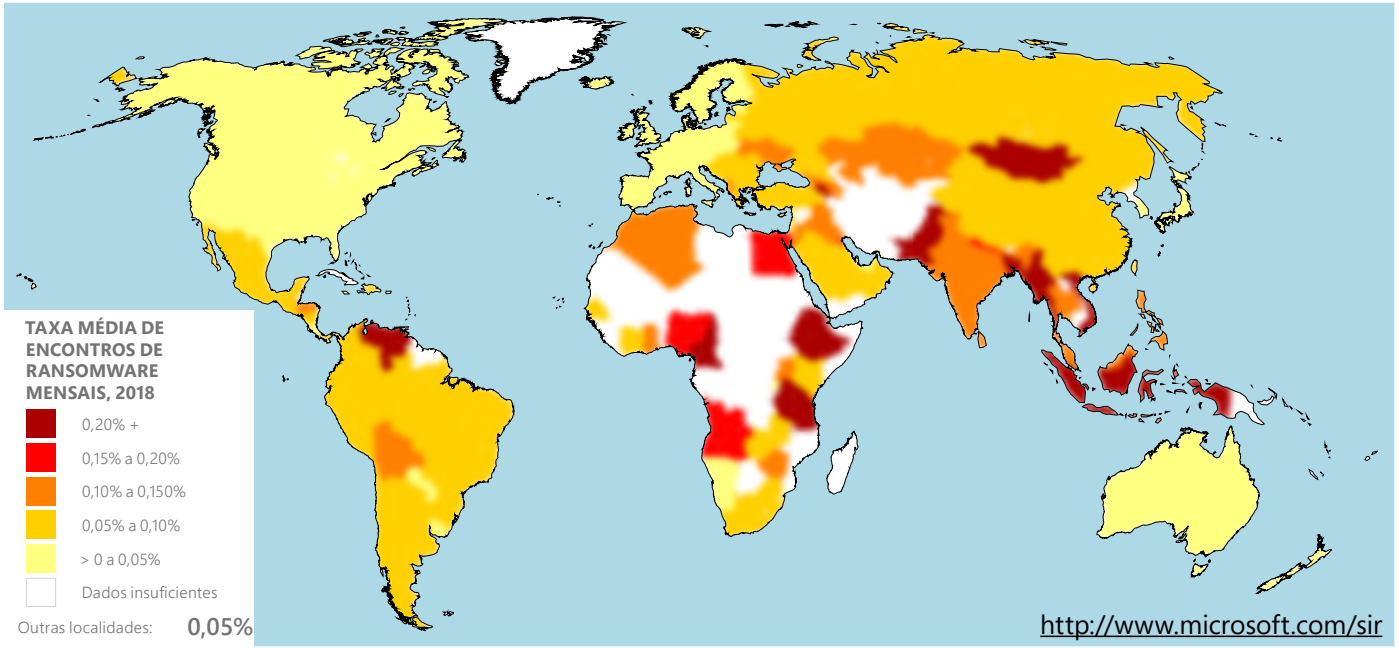
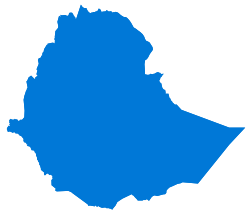


FIGURA 2.

Taxas médias de encontros de ransomware mensais em todo o mundo por país/região em 2018

PAÍS MAIS AFETADO POR RANSOMWARE: ETIÓPIA



Taxa média de encontros mensais: **0,77%**

Os cinco locais com as maiores taxas médias de encontros de ransomware mensais em 2018 foram Etiópia (taxa média de encontros de ransomware mensais de 0,77%), Mongólia (0,46%), Camarões (0,41%), Myanmar (0,33%) e Venezuela (0,31%), cada um deles com uma taxa média de encontros de ransomware mensais de 0,31% ou superior durante o período.1 Há alguns anos, os encontros de ransomware tinham a tendência de se concentrarem em países e regiões ricos na Europa e na América do Norte. Porém, como o ransomware começou a perder popularidade com os invasores, o padrão de encontros passou a ficar mais parecido com o malware como um todo.

Os locais com as menores taxas de encontros de ransomware em 2018 foram Irlanda (0,01%), Japão (0,01%), Estados Unidos (0,02%), Reino Unido (0,02%) e Suécia (0,02%), cada um deles com uma taxa média de encontros de ransomware mensais de 0,02% ou inferior durante o mesmo período. Locais com baixas taxas de encontros tendem a ter infraestruturas de segurança cibernética maduras e programas bem estabelecidos para proteger infraestruturas críticas e se comunicar com os cidadãos sobre segurança básica.

NOTAS DE RODAPÉ

[1] A taxa de encontros é a porcentagem de computadores que executam produtos de segurança da Microsoft em tempo real e relatam um encontro de malware. Encontrar uma ameaça não significa que o computador tenha sido infectado. Somente computadores cujos usuários optaram por fornecer dados à Microsoft são considerados ao calcular as taxas de encontro.

MINERAÇÃO DE CRIPTOMOEDAS EM ASCENSÃO

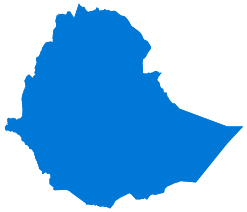
A criptomoeda é o dinheiro virtual que pode ser usado para comprar e vender bens e serviços de forma anônima, tanto online como no mundo físico. Existem muitos tipos diferentes de criptomoedas, mas todos baseados na tecnologia de blockchain, em que cada transação é registrada em um registro distribuído que é mantido por milhares ou milhões de computadores em todo o mundo. Novas moedas são criadas, ou "mineradas", por computadores que executam cálculos complexos que também desempenham a função de verificar as transações de blockchain.

A mineração de moedas pode ser muito lucrativa. Em 2018, uma única moeda de Bitcoin, a criptomoeda mais antiga e mais popular, valia vários milhares de dólares americanos. No entanto, fazer os cálculos necessários pode exigir um uso intensivo dos recursos, que se torna cada vez mais intensivo a cada nova moeda minerada. Para moedas populares, como Bitcoin, a mineração de moedas de forma lucrativa é quase impossível sem o acesso a imensos recursos de computação que estão fora do alcance para a maioria dos indivíduos e pequenos grupos. Por isso, os invasores que buscam lucros ilícitos têm cada vez mais recorrido ao malware, que permite usar os computadores das vítimas para ajudá-los a minerar criptomoedas. Essa abordagem permite que eles aproveitem o poder de processamento de centenas de milhares de computadores em vez de um ou dois. Mesmo quando uma infecção menor é descoberta, a natureza anônima da criptomoeda complica os esforços de rastreamento das partes responsáveis.

Em 2018, a taxa média de encontros de mineração de criptomoedas mensais no mundo todo foi de 0,12%, em comparação com apenas 0,05% de ransomware. Muitos fatores contribuem para o aumento da popularidade da mineração como uma carga para malware. Ao contrário do ransomware, a mineração de criptomoedas não requer a entrada do usuário: ela funciona em segundo plano, enquanto o usuário está realizando outras tarefas ou está longe do computador e pode não ser notada, a menos que prejudique suficientemente a performance do computador. Como resultado, é menos provável que os usuários executem qualquer ação para remover a ameaça, e ela pode continuar a mineração para o benefício do invasor por um período prolongado.

A disponibilidade de produtos prontos para uso para a mineração oculta de muitas criptomoedas é outro fator da tendência. A barreira para entrada é baixa por causa da ampla disponibilidade de softwares de mineração de moedas, que os criminosos cibernéticos reempacotam como malware para entregas aos computadores dos usuários desavisados. Em seguida, os mineradores equipados são distribuídos às vítimas usando muitas das mesmas técnicas que os invasores usam para entregar outras ameaças, como engenharia social, explorações e drive-by downloads. Depois que o software de mineração é instalado, ele é executado em segundo plano nos computadores da vítima para executar as computações de blockchain, com o invasor aproveitando as recompensas.

TAXAS MÉDIAS DE ENCONTROS MENSAIS DOS PAÍSES MAIS AFETADOS PELA MINERAÇÃO DE CRIPTOMOEDAS



Etiópia: **5,58 %**

Tanzânia: **1,83%**

Paquistão: **1,47%**

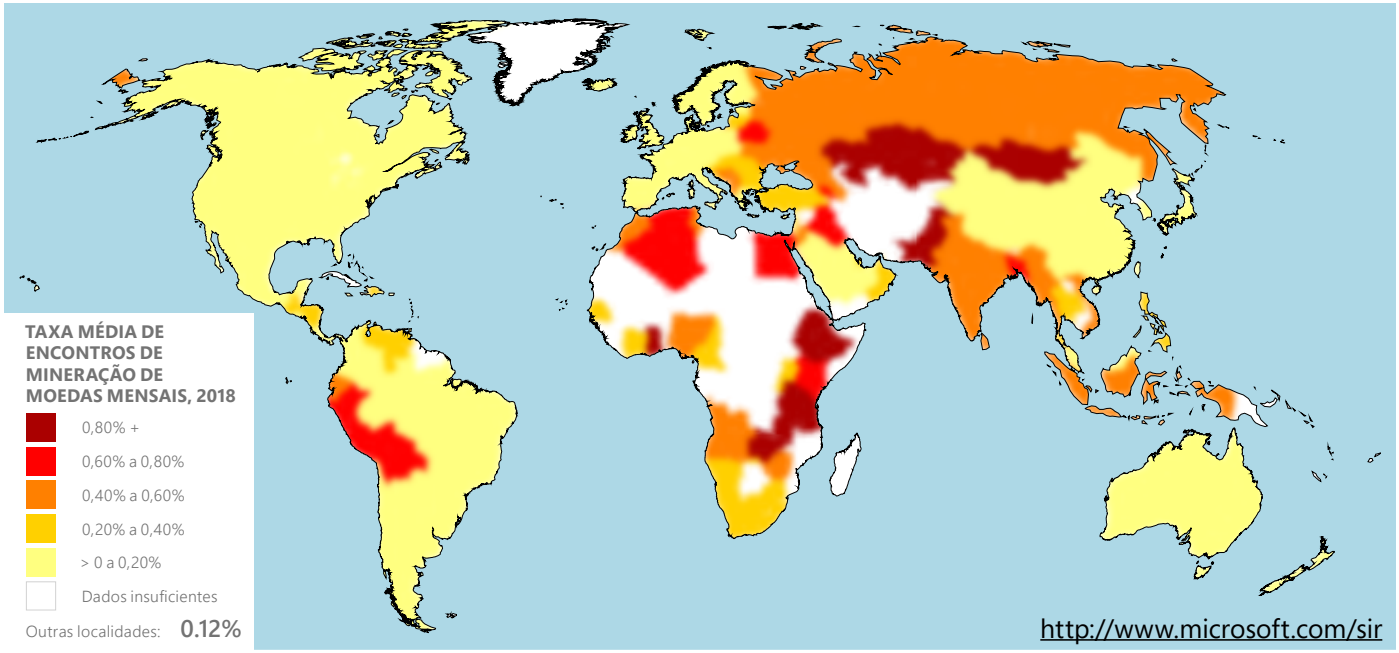


FIGURA 3.

Taxas médias de encontros de mineração de moedas mensais em todo o mundo por país/região em 2018

Os cinco locais com as maiores taxas de encontros de mineração de criptomoedas em 2018 foram Etiópia (5,58%), Tanzânia (1,83%), Paquistão (1,47%), Cazaquistão (1,24%) e Zâmbia (1,13%), cada um deles com uma taxa média de encontros de mineração de moedas mensais de aproximadamente 1,13% ou superior durante o período. Os locais com as menores taxas de encontros de mineração de moedas em 2018 foram Irlanda, Japão, Estados Unidos e China, cada um deles com uma taxa média de encontros de mineração de moedas mensais de aproximadamente 0,02% durante o período.

MINERADORES DE CRIPTOMOEDAS COM BASE EM NAVEGADOR: UM NOVO TIPO DE AMEAÇA

As estatísticas apresentadas nesta seção envolvem mineradores de criptomoedas mal-intencionados que são projetados para serem instalados nos computadores das vítimas como malware. Mas algumas das ameaças mais significativas da mineração de criptomoedas se baseiam inteiramente em navegadores da web e nunca precisam ser instaladas. Vários serviços anunciam a mineração de criptomoedas com base em navegador como uma forma de os proprietários de sites monetizarem o tráfego para seus sites sem depender da publicidade. Os proprietários de sites devem adicionar código JavaScript às suas páginas que mineram criptomoedas em segundo plano enquanto um usuário está acessando

TAXAS MÉDIAS DE ENCONTROS MENSAIS DOS PAÍSES MENOS AFETADOS PELA MINERAÇÃO DE CRIPTOMOEDAS

Irlanda: 0,02%

Japão: 0,02%

Estados Unidos: 0,02%

Taxa de encontros de Brocoiner

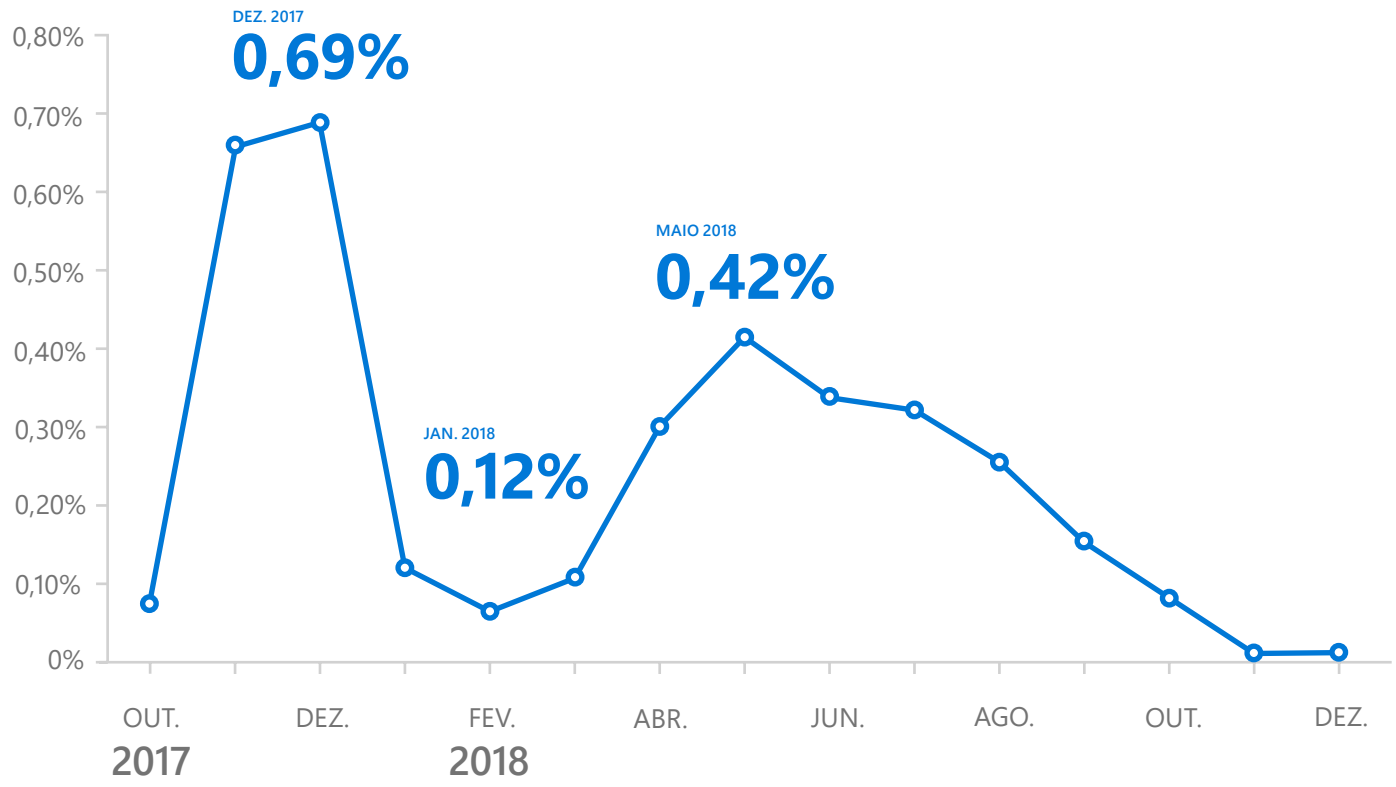


FIGURA 4.

Taxa de encontros de Brocoiner, o minerador de criptomoedas com base em navegador mais predominante

o site, com os rendimentos divididos entre o proprietário do site e o serviço. Infelizmente, os invasores têm sido rápidos em se aproveitarem desses serviços para minerar criptomoedas sem obter o consentimento dos usuários finais, muitas vezes comprometendo sites legítimos e inserindo o código de mineração em seu código-fonte maliciosamente. Esses mineradores com base em navegador não exigem nenhum comprometimento do computador do usuário final e serão executados em qualquer plataforma com um navegador da Web compatível com JavaScript. Como os trojans de mineração de criptomoedas, os mineradores com base em navegador podem prejudicar significativamente a performance do computador e desperdiçar eletricidade enquanto um usuário acessa uma página da Web afetada.

O IMPACTO DA MINERAÇÃO DE CRIPTOMOEDAS NÃO SOLICITADA

A ameaça mais óbvia que as vítimas enfrentam com a mineração de criptomoedas mal-intencionada é o consumo de recursos de computação, que pode desperdiçar eletricidade e prejudicar significativamente a performance do computador. Usuários e organizações também enfrentam outros riscos com a mineração de moedas, incluindo:

- **Obtendo uma base para causar danos ainda maiores no futuro.** Assim como outras formas de malware, a mineração de criptomoedas pode ser um ponto de entrada para os invasores. Enquanto o computador está minerando criptomoedas em segundo plano, os criminosos cibernéticos podem aprender sobre o ambiente e, possivelmente, descobrirem lacunas na segurança para explorar para outros fins.
- **Os dispositivos conectados à Internet podem ser comprometidos e transformados em bots para mineração de criptomoedas.** Muitos desses dispositivos não possuem segurança interna, como a detecção de ameaças de malware, o que pode torná-los alvos desejáveis para os invasores.
- **Prejudicando computadores.** Os softwares de mineração de criptomoedas em execução contínua durante meses ou mais tempo podem prejudicar a performance, e o calor gerado pelo consumo excessivo de energia e pela utilização da CPU pode danificar os computadores.

SEÇÃO II

Cadeias de fornecedores de software em risco

Há anos, a Microsoft tem rastreado os agentes de ameaças que usam o comprometimento da cadeia de fornecedores como um ponto de entrada para ataques. Em um ataque da cadeia de fornecedores, o invasor se concentra em comprometer o processo de desenvolvimento ou atualização de um fornecedor de software legítimo.

Se for bem-sucedido, o invasor pode incorporar um componente comprometido em um aplicativo ou pacote de atualização legítimo que, em seguida, é distribuído aos usuários do software. Em seguida, o código malicioso é executado com as mesmas permissões e confiança do software. O aumento no número de ataques da cadeia de fornecedores de software nos últimos anos tornou-se um assunto importante em muitas conversas sobre segurança cibernética e é a principal fonte de preocupação em muitos departamentos de TI.

FIGURA 5.

Ataques da cadeia de fornecedores de software em 2017 e 2018

PRINCIPAIS ATAQUES DA CADEIA DE FORNECEDORES DE SOFTWARE EM 2017

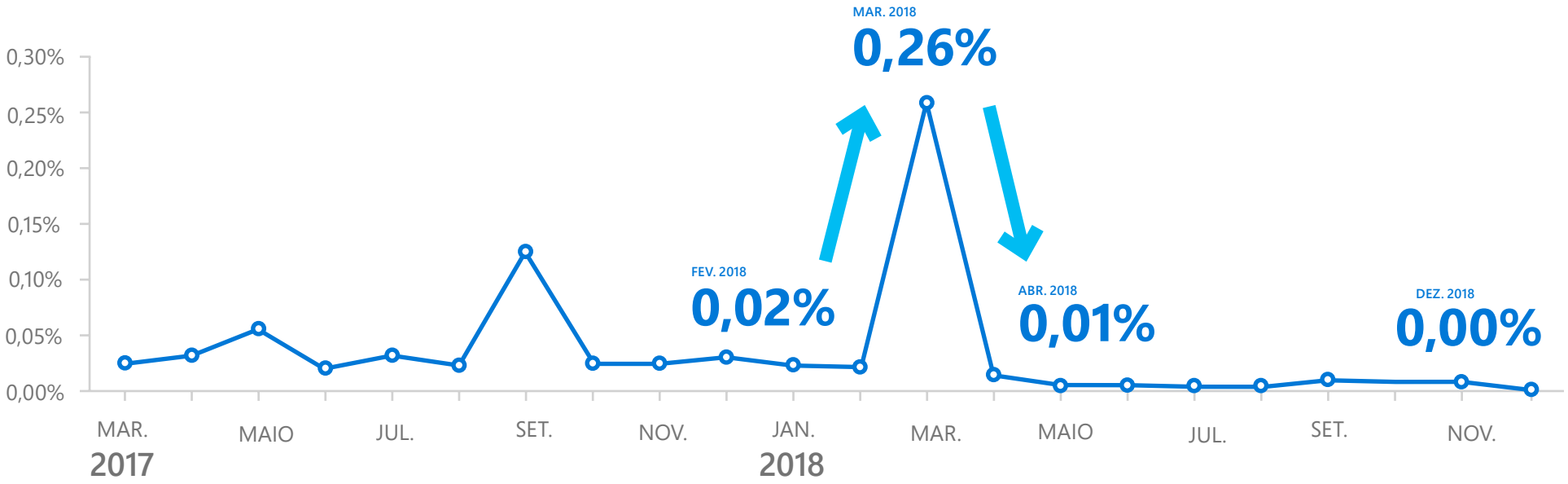
Em 2017, os ataques da cadeia de fornecedores foram responsáveis por vários incidentes proeminentes, mais notavelmente o surto de ransomware Petya em junho, que foi rastreado para infecções iniciais em um processo de atualização comprometido de um aplicativo de contabilidade fiscal popular na Ucrânia. Em maio, a operação WilySupply comprometeu o atualizador de software de um editor de texto para instalar um backdoor em organizações selecionadas nos setores financeiro e de TI. Em julho, um backdoor chamado ShadowPad estava oculto em um pacote de software de gerenciamento de servidores e permitiu que os invasores instalassem cargas de malware adicionais para roubo de dados e outras atividades maliciosas. Em setembro, a infraestrutura da ferramenta popular de freeware CCleaner foi comprometida e uma versão de backdoor foi entregue à sua base de usuários.

O primeiro grande incidente de ataque da cadeia de fornecedores de software de 2018 ocorreu em 6 de março, quando o Windows Defender ATP bloqueou uma enorme campanha para entregar o trojan Dofoil (também conhecido como Smoke Loader). A enorme campanha de malware foi rastreada para um aplicativo ponto a ponto infectado. O pacote de atualização do aplicativo foi substituído por um outro mal-intencionado que fez download do código comprometido, que, posteriormente, instalou o malware Dofoil. O trojan sofisticado levava uma carga de mineração de moedas e exibia técnicas avançadas de injeção entre processos, mecanismos de persistência e métodos de evasão.

FIGURA 6.

As tendências de encontros de Dofoil (Smoke Loader) em 2018 mostram o pico de instâncias bloqueadas em março

Taxa de encontros de Dofoil



Nas primeiras 12 horas da campanha, o Windows Defender Antivírus bloqueou mais de 400.000 tentativas de infecção em todo o mundo. A Rússia representou 73% dos encontros mundiais, com a Turquia e a Ucrânia registrando 18% e 4%, respectivamente.

Vários outros ataques foram detectados usando cadeias de fornecedores de software comprometidas como mecanismos de entrega em 2018, incluindo os descritos na tabela a seguir:

Período	Ataque	Descrição	Software afetado
Março de 2018	Campanha de mineração de moedas de Dofoil (relatado pela Microsoft).	Os invasores infectaram o processo de atualização de um aplicativo ponto a ponto para instalar o Dofoil, que, por sua vez, instalou o malware de mineração de moedas.	Aplicativo ponto a ponto.
Julho de 2018	Cadeia de fornecedores comprometida em uma cadeia de fornecedores (relatado pela Microsoft).	Os invasores comprometeram a infraestrutura compartilhada entre um fornecedor de um aplicativo editor de PDF e um de seus fornecedores parceiros de software.	Aplicativo editor de PDF e fornecedor parceiro de terceiros.
Agosto de 2018	Programa de suporte remoto comprometido (operação Red Signature, relatado por Trend Micro e IssueMakersLab).	O servidor de atualização de um provedor de soluções de suporte remoto foi comprometido para entregar uma ferramenta de acesso remoto chamada 9002 RAT.	Programa de suporte remoto.
Outubro de 2018	Solução de painel de controle de hospedagem comprometida (relatado pela ESET).	O script de instalação para uma solução de painel de controle de hospedagem foi alterado para roubar credenciais.	Solução de painel de controle de hospedagem.

FIGURA 7.

Outros ataques da cadeia de fornecedores de software em 2018

CONFIANÇA EM RISCO

Os ataques da cadeia de fornecedores são insidiosos porque se aproveitam da confiança que os usuários e os departamentos de TI colocam no software usado. O software comprometido muitas vezes é assinado e certificado pelo fornecedor e talvez não dê nenhuma indicação de que algo está errado, o que torna significativamente mais difícil detectar a infecção. Eles podem prejudicar a relação entre as cadeias de fornecedores e seus clientes, sejam eles usuários corporativos ou domésticos. Ao infectar o software e minar as infraestruturas de entrega ou atualização, os ataques da cadeia de fornecedores podem afetar a integridade e a segurança dos bens e serviços que as organizações fornecem.

Os ataques da cadeia de fornecedores afetaram uma ampla gama de softwares e organizações selecionadas em diferentes setores e localizações geográficas. A ameaça dos ataques da cadeia de fornecedores é um problema de toda a indústria que requer atenção de várias partes interessadas, incluindo os fornecedores e desenvolvedores de software que escrevem o código, os administradores de sistema que gerenciam as instalações de software e a comunidade de segurança da informação que encontra esses ataques e cria soluções para proteger as pessoas e os softwares.

ALÉM DO SOFTWARE: COMPROMETIMENTO DA CADEIA DE FORNECEDORES POR MEIO DE OBJETOS DE NUVEM

A capacidade dos ataques da cadeia de fornecedores de minar a confiança aumenta e torna-se ainda mais complexa na nuvem. Vários incidentes de objetos de nuvem, serviços e infraestruturas comprometidos em 2018 destacam essa complexidade:

- Extensões do Chrome infectadas que instalaram malware de fraude por clique (relatado pela ICEBRG)
- Vários repositórios do Linux comprometidos (relatado em alguns fóruns online)
- Plug-ins maliciosos do WordPress usados para várias atividades maliciosas, incluindo permitir que os invasores publiquem conteúdo em sites do WordPress (relatado pelo Wordfence)
- Imagens do Docker maliciosas que continham um script para fazer download do malware de mineração de criptomoedas e eram carregadas na conta do Docker Hub (relatado por Fortinet e Kromtech)
- Um pacote malicioso de typosquatting no repositório oficial Python. O pacote continha um script malicioso que faz download do malware usado para sequestrar endereços de mineração de moedas na área de transferência (relatado no Medium)
- Script comprometido no StatCounter que permitia que os invasores injetassem um script malicioso em sites que usam o StatCounter (relatado pela ESET)
- Vários incidentes de módulos npm de backdoor (Blog do npm, Medium) que, se explorados, poderiam resultar em situações em que, por exemplo, um invasor poderia inserir um código arbitrário em um servidor em execução e executá-lo.

Esses incidentes demonstram como o comprometimento da cadeia de fornecedores pode ampliar muito uma superfície de ataque. Se não protegidos, os objetos de nuvem podem ser vetores de entrada inesperados. Por exemplo, o incidente do Hub do Docker envolveu uma conta maliciosa que carregava imagens do Docker que continham um backdoor de mineração de moedas oculto. As imagens do Docker ficaram hospedadas no Docker Hub por quase um ano e foram obtidas milhões de vezes e usadas por administradores e usuários desavisados.

Os riscos da cadeia de fornecimento se estendem a códigos na nuvem, Open Source, bibliotecas da Web, contêineres e outros objetos na nuvem. Esses riscos, juntamente com o alto grau de variação entre os incidentes de comprometimento da cadeia de fornecimento de software e hardware que vieram à tona, fazem com que os ataques da cadeia de fornecimento uma ampla categoria de ameaças. Embora não haja uma solução única para todo o espectro desses tipos de ataques, as organizações precisam criar proteção preventiva e detecção pós-violação de ataques da cadeia de fornecedores provenientes de fornecedores de hardware e software, provedores e aquisições, fornecedores de software Open Source, bem como fornecedores de serviços de nuvem e infraestrutura comprometidos.

Investigação de incidentes cibernéticos com a DART

A equipe de detecção e resposta (DART) da Microsoft é uma equipe global de especialistas em segurança cibernética e profissionais responsáveis por respostas a incidentes que ajuda as organizações na detecção, na investigação e na resposta a incidentes de segurança cibernética. Esta seção destaca alguns dos casos de clientes com os quais a DART lidou no último ano. Ela ilustra as tendências comuns de invasores e como a Microsoft e os clientes conseguiram frustrá-las.

ORGANIZAÇÃO DE SERVIÇOS PROFISSIONAIS PASSOU POR UM ATAQUE DE ESTADO-NAÇÃO QUE EXTRAIU DADOS

Uma organização de serviços profissionais foi afetada por uma sofisticada ameaça persistente avançada (APT), patrocinada pelo Estado, que obteve acesso a credenciais privilegiadas da organização. Os invasores obtiveram acesso à rede usando um ataque de spray de senha, no qual utilizaram um pequeno número de senhas fracas ou amplamente usadas (como "p@ssword" ou "123456") para visar um grande número de contas de usuários e obter credenciais administrativas do Office 365. (Ataques de spray de senha são usados para evitar a detecção ao limitar o número de tentativas de login para cada conta.) Após infiltrar na rede, a APT executou a extração elaborada e automatizada de dados de caixas de correio dos funcionários. Apesar de várias tentativas para expulsá-los, o adversário permaneceu na rede por mais de 200 dias. Como parte do ataque, o adversário aproveitou o software da cadeia de fornecedores da organização e automatizou a extração de dados.

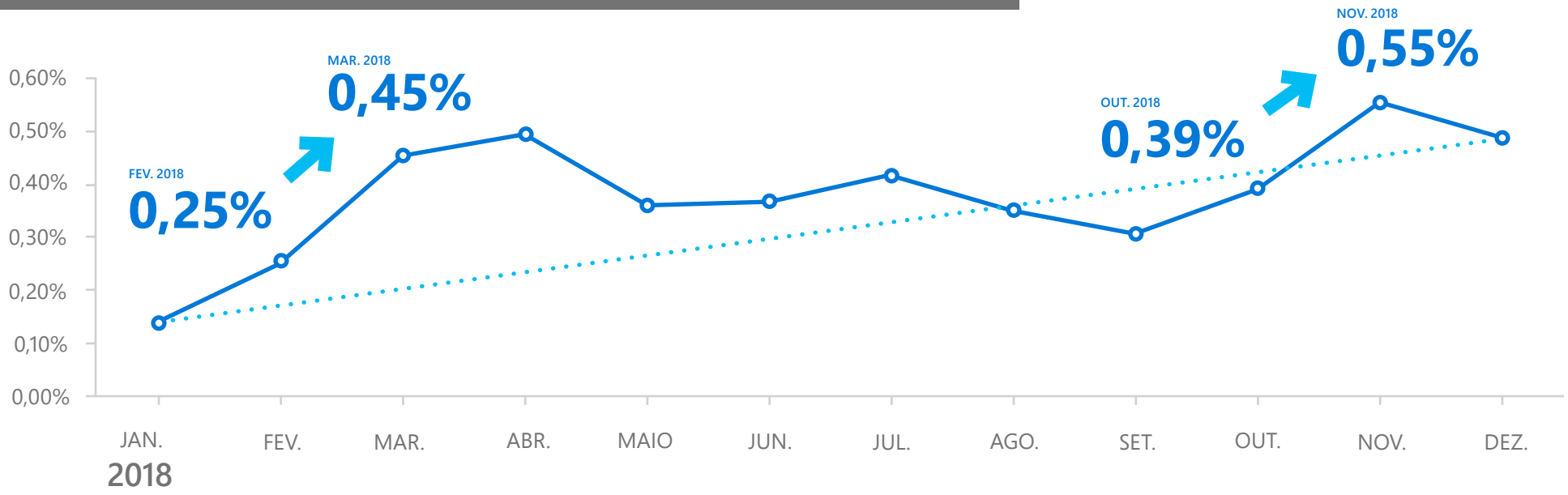
Como havia a suspeita de uma violação de dados dos clientes, a organização contratou a equipe DART para investigar e ajudar a evitar mais danos. A DART identificou como alvo pesquisas da caixa de correio do Office 365, contas comprometidas e canais de comando e controle do invasor. As principais lições do cliente nesse incidente foram para implantar controles para proteger os serviços de nuvem contra ameaças baseadas em identidade e invasores. A organização adotou a autenticação multifatorial (MFA), as políticas de acesso condicional para determinados aplicativos de nuvem e o registro em log do Office 365. Para se proteger ainda mais contra ameaças semelhantes no futuro, a organização também pode adotar uma solução de resposta e detecção de ponto de extremidade (EDR) para detectar invasores que podem estar tentando explorar sua rede. Além disso, recomendamos que essa organização indique uma entidade de governança de nuvem ou uma equipe de identidade global que vai gerenciar e impor as políticas adequadas de autenticação de usuários, para que a organização supervisione sua postura de segurança e possa reduzir riscos de forma mais eficiente.

SEÇÃO III

Phishing ainda é predominante

Em 2018, os analistas de ameaças da Microsoft perceberam evidências de que os invasores continuam a usar phishing como um método de ataque preferencial. O phishing promete continuar a ser um problema durante o futuro próximo, porque envolve decisões e julgamentos humanos perante esforços persistentes de criminosos cibernéticos para atrair vítimas.

As taxas de phishing ainda estão em ascensão
Percentual do total de emails de entrada que são emails de phishing



PHISHING CONTINUA A SER UM VETOR DE ATAQUE PREFERENCIAL EM 2018

A Microsoft analisa e verifica no Office 365 mais de 470 bilhões de mensagens de email todo mês para ver se há phishing e malware, o que fornece aos analistas insights consideráveis sobre as tendências e técnicas de invasores. A quantidade de emails de entrada que eram mensagens de phishing aumentou 250% entre janeiro e dezembro de 2018. O phishing continua sendo um dos principais vetores de ataque usados para entregar cargas de dia zero maliciosas aos usuários. A Microsoft continua a se fortalecer contra esses ataques com recursos adicionais de proteção, detecção, investigação e resposta anti-phishing para ajudar a proteger os usuários.

▲ **FIGURA 8.**

Emails de phishing em 2018

Evolução em métodos de ataque de phishing

À medida que as ferramentas e técnicas usadas para proteger as pessoas contra o phishing tornam-se mais sofisticadas, os invasores são forçados a se adaptar. Os ataques de phishing tornaram-se cada vez mais polimórficos, o que significa que os invasores não usam um único URL, domínio ou endereço IP para enviar emails, mas sim usam uma infraestrutura variada com vários pontos de ataque. A natureza dos ataques também evoluiu, com campanhas de phishing modernas que vão desde ataques de curta duração que ficam ativos por apenas alguns minutos até campanhas de grande volume de duração muito mais longa. Outros são ataques de variantes de série, em que os invasores enviam um pequeno volume de emails em vários dias sucessivos.

Além disso, a Microsoft observou uma tendência dos invasores a usar uma infraestrutura hospedada e outra infraestrutura de nuvem pública, o que torna mais fácil evitar a detecção, escondendo-se entre sites e ativos legítimos. Por exemplo, os invasores usam cada vez mais sites e serviços populares de compartilhamento e colaboração de documentos para distribuir cargas maliciosas e formulários de login falsos que são usados para roubar credenciais de usuário. Também houve um aumento no uso de contas comprometidas para distribuir ainda mais emails maliciosos dentro e fora de uma organização.

As campanhas de phishing variam, desde ataques direcionados até de base ampla

Da mesma maneira que ocorre a distribuição de malware em geral, as campanhas de phishing variam, desde ataques direcionados até genéricos de base ampla. Embora ataques altamente sofisticados produzam maiores ganhos monetários por conta vítima de phishing, os ataques mais genéricos geram menos dinheiro por conta comprometida, mas visam um conjunto mais amplo de usuários.

Um exemplo de campanha sofisticada e direcionada é a Ursnif, na qual os invasores localizavam o nome de arquivo do documento para ser específico de uma organização conhecida ou da indústria do alvo. Esses ataques são bastante diferentes das campanhas de base ampla e parecem ser mais legítimos e confiáveis.

Algumas das campanhas de base ampla em 2018 foram relacionadas ao comprometimento de emails de negócios (BEC) e à usurpação de identidade de marcas, domínios ou usuários conhecidos dentro das organizações selecionadas e campanhas de falsificação sofisticadas. A usurpação de identidade de domínios é uma tática de ataque comum usada para fazer as organizações acreditarem que o email é confiável e deve ser aberto.

Truques de phishing vêm em muitas formas

Os pesquisadores da Microsoft descobriram que muitos tipos diferentes de cargas ou truques de phishing estão sendo utilizados em campanhas, incluindo:

- **Falsificação de domínio** (o domínio da mensagem de email é uma correspondência exata ao nome do domínio original)
- **Usurpação de identidade de domínio** (o domínio da mensagem de email é semelhante ao nome do domínio original)[2]
- **Usurpação de identidade de usuário** (a mensagem de email parece ser proveniente de alguém em quem você confia)
- **Truques de SMS** (a mensagem de texto parece ser proveniente de uma fonte legítima, como um banco, órgão governamental ou outra empresa, para transmitir legitimidade às alegações e geralmente pede à vítima para fornecer informações confidenciais, como nomes de usuário, senhas ou dados financeiros confidenciais)
- **Links de phishing de credenciais** (a mensagem de email contém um link para uma página que é semelhante a uma página de logon de um site legítimo, para que os usuários insiram suas credenciais de logon)
- **Anexos de phishing** (a mensagem de email contém um anexo de arquivo malicioso que o remetente instiga a vítima a abrir)
- **Links para locais de armazenamento em nuvem falsos** (a mensagem de email parece vir de uma fonte legítima e instiga o usuário a conceder permissão e/ou inserir informações pessoais, como credenciais em troca de acesso a um local de armazenamento em nuvem falso)

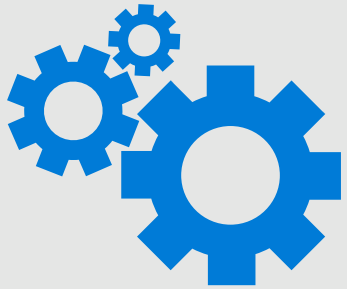
Essa variedade de truques que podem ser utilizados por invasores aumenta a complexidade das ameaças de phishing que as organizações devem enfrentar.

NOTAS DE RODAPÉ

[2] A usurpação de identidade de domínio pode ser semelhante à falsificação de domínio (correspondência exata ao nome do domínio original) no caso excepcional em que o domínio aparece no nome de exibição do email.

Investigação de incidentes cibernéticos com a DART

GRANDE ORGANIZAÇÃO DE MANUFATURA ATINGIDA POR INCIDENTES DE PHISHING DIRECIONADOS



Uma organização de manufatura enfrentou uma campanha de phishing de várias fases em um período de alguns meses. Essa abordagem não é incomum. Durante a primeira fase, o invasor realizará o reconhecimento e, na segunda fase, visará ativos de alto valor. A primeira fase dessa campanha utilizou uma tentativa de phishing bem conhecida que foi baseada em um link de página da Web incorporado em um email enviado para um pequeno grupo direcionado na organização. O email indicava que o alvo tinha um documento eletrônico importante em espera para ser analisado, e tudo que o destinatário tinha que fazer era autenticar com suas credenciais de domínio para obter acesso. Essa página de aterrissagem falsa configurada para o alvo analisar o chamado "documento importante" na verdade coletava as credenciais e permitia que o invasor acessasse contas do Office 365 em qualquer lugar do mundo. A segunda fase da campanha de phishing foi destinada a enviar emails de phishing semelhantes para ativos de alto valor na organização de manufatura selecionada, com o objetivo de obter acesso a dados mais valiosos. A Microsoft se envolveu com esse cliente durante a segunda fase da campanha de phishing. As principais lições do cliente nesse incidente foram:

o phishing continua a ser um dos métodos de ataque mais eficientes, e os usuários ainda são o elo mais fraco. Treinar os usuários para desconfiar de tentativas de phishing, ter ferramentas preparadas para identificar invasores e agir e corrigir o sistema regularmente são todas medidas importantes. Se a organização não abordar alguma delas, poderá ficar vulnerável.

Nesse caso, a preocupação mais importante do cliente foi uma necessidade imediata de bloquear o acesso às contas comprometidas. Em parceria com as equipes do Azure Identity e do Office 365, a DART concebeu um plano para erradicar o invasor da rede e monitorar todo tráfego no canal de comando e controle ao usar a solução recém-implantada Microsoft Azure Log Analytics. A equipe foi capaz de ajudar a resolver a situação em apenas três horas. O acesso do invasor foi bloqueado, e a organização pôde voltar sua atenção para a avaliação e a recuperação de danos. A DART usou as ferramentas do Azure Log Analytics para caçar o comportamento do invasor, o que ajudou a descobrir muitos desafios de configuração para a organização. Por exemplo, a DART identificou lacunas na correção de servidores críticos, descobriu computadores na rede que se comunicavam com hosts ruins conhecidos na Internet e também encontrou vários servidores importantes sem proteção contra malware.

SEÇÃO IV

Malware ao redor do mundo

O malware representa riscos para as organizações e os indivíduos na forma de usabilidade prejudicada, perda de dados, roubo de propriedade intelectual, perda monetária e estresse emocional e pode até mesmo colocar vidas humanas em risco. A Microsoft usa uma ampla variedade de ferramentas e técnicas para identificar, bloquear e erradicar infecções de malware onde quer que sejam encontradas.

As taxas de encontros de malware variaram de cerca de 5% até mais de 7% em 2017. No início de 2018, elas aumentaram antes de diminuir durante a maior parte do ano para pouco acima de 4%. Algumas possíveis razões para a redução geral nas taxas de encontros de malware em 2018 são o crescimento na adoção do Windows 10 e o aumento no uso do Windows Defender para proteção. A taxa de encontros é a porcentagem de computadores com o Windows Defender Antivírus que relataram encontrar malware durante o mês, incluindo as tentativas de infecção que o Defender bloqueou.

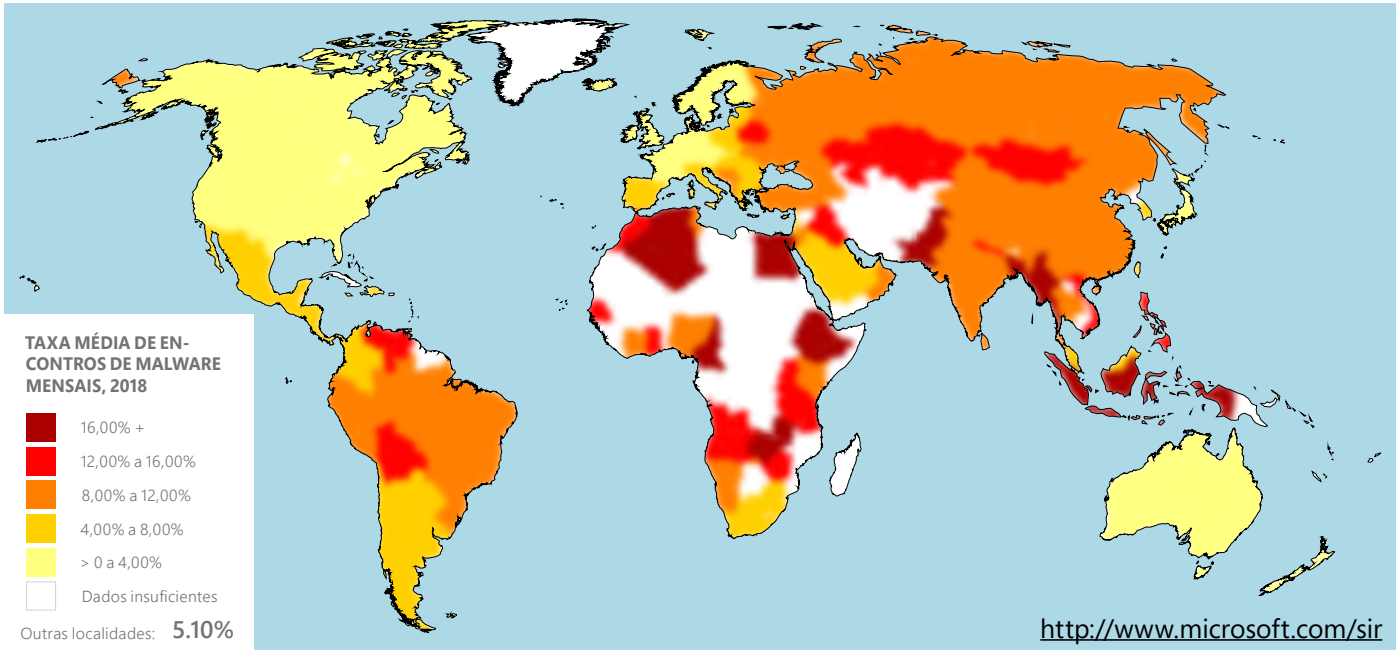


FIGURA 9.

Taxas médias de encontros de malware mensais em todo o mundo por país/ região em 2018

Os cinco locais com as maiores taxas de encontros de malware durante o período de janeiro a dezembro de 2018 foram Etiópia (taxa média de encontros mensais de 26,33%), Paquistão (18,94%), territórios palestinos (17,50%), Bangladesh (16,95%) e Indonésia (16,59%). Todos tiveram uma taxa média de encontros mensais de aproximadamente 16,59% ou superior durante o período. As taxas de infecção tendem a se correlacionar fortemente com fatores de desenvolvimento humano e preparação tecnológica em uma sociedade. Todos os locais com as maiores taxas de encontros em 2018 foram classificados nas últimas posições dos 40% dos países e regiões no Índice de tecnologias de informação e comunicação (ICT) de 2017, publicado pela United Nations International Telecommunication Union (ICT).

Os cinco locais com as menores taxas de encontros de malware durante esse mesmo período foram Irlanda (1,26%), Japão (1,51%), Finlândia (1,74%), Noruega (1,79%) e Holanda (1,82%). Todos tiveram uma taxa média de encontros mensais de 1,82% ou inferior durante o período. Esses locais tendem a ter infraestruturas de segurança cibernética maduras e programas bem estabelecidos para proteger infraestruturas críticas e se comunicar com os cidadãos sobre segurança básica.

TAXAS MÉDIAS DE ENCONTROS MENSAIS DOS PAÍSES MAIS AFETADOS PELO MALWARE

Etiópia: **26,33%**

Paquistão: **18,94%**

Territórios palestinos: **17,50%**

Investigação de incidentes cibernéticos com a DART

VÁRIAS ORGANIZAÇÕES DE SERVIÇOS FINANCEIROS SOFRERAM ATAQUES DE ESTADO-NAÇÃO QUE INTERROMPERAM AS OPERAÇÕES

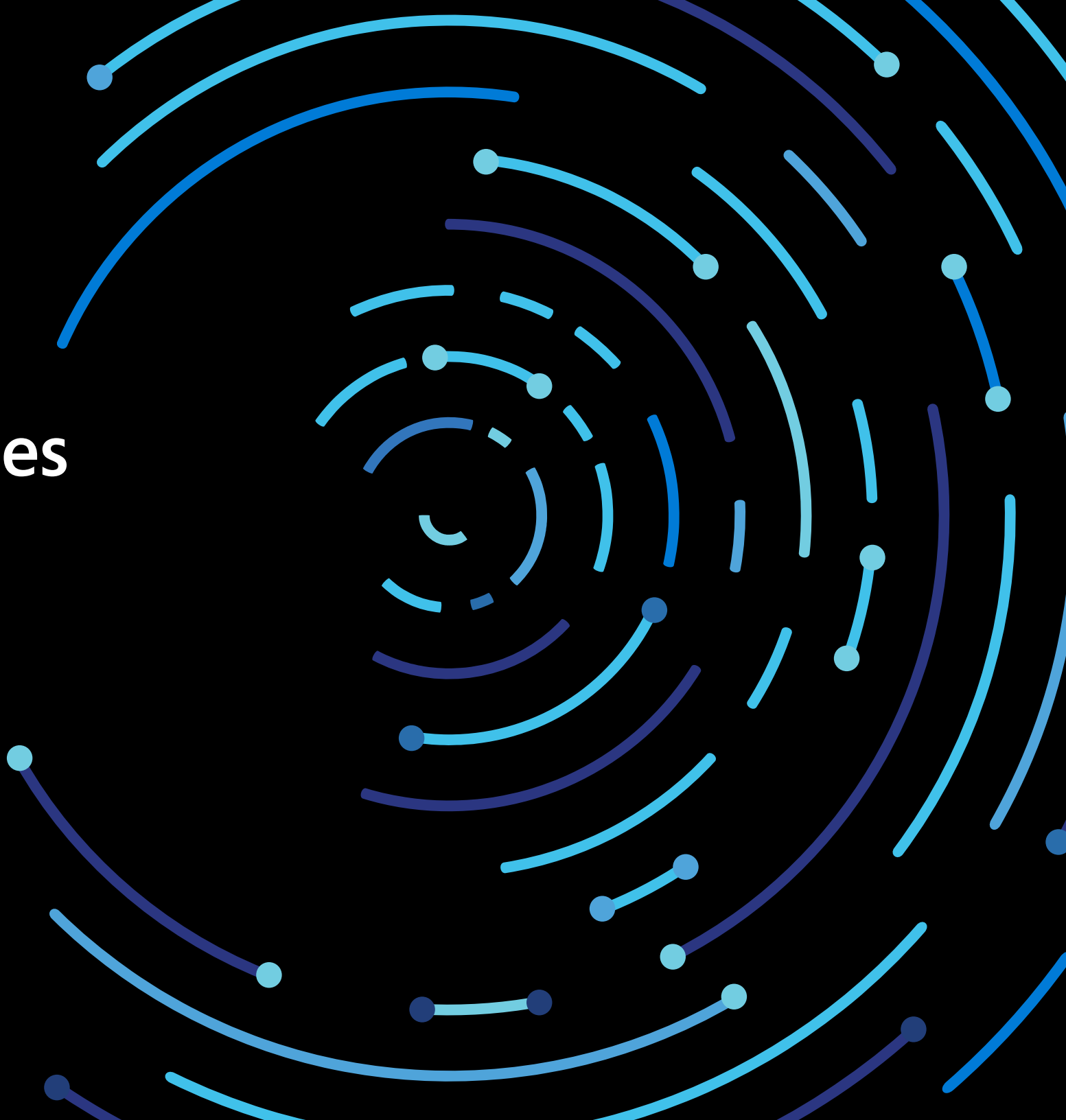
Em um dos incidentes mais destrutivos que a DART já viu, várias organizações de serviços financeiros foram alvo de uma APT patrocinada pelo Estado (um grupo diferente daquele que visou a organização de serviços profissionais mencionada anteriormente) que agiu de forma semelhante.

Essa APT obteve acesso administrativo após infectar um computador paciente zero com um implante de backdoor altamente direcionado e oculto, possivelmente entregue por meio de um email de spear phishing. Posteriormente, a APT executou várias transações fraudulentas, transferindo grandes quantias de dinheiro para contas bancárias estrangeiras. Em alguns casos, o invasor permaneceu não detectado por mais de 100 dias. Depois que o invasor percebeu que foi detectado, ele implantou rapidamente um ataque pré-configurado, entregando um malware destrutivo a mais da metade dos sistemas no ambiente. As operações desses clientes foram encerradas por vários dias.

Houve algumas lições importantes do cliente provenientes desses incidentes. A primeira foi que o gerenciamento do ciclo de vida do software é especialmente importante, o que inclui garantir que os sistemas estejam sendo atualizados (sistemas operacionais e de segurança), corrigidos e auditados regularmente. Em um dos casos, o ambiente do sistema Linux de uma organização que tinha um número excepcionalmente grande de workloads em execução foi completamente não gerenciado, colocando-o em risco de ataque notavelmente alto. A segunda lição foi que é importante manter backups de dados do sistema em um local offline caso os dados primários sejam perdidos. Outra lição foi que as soluções antivírus tradicionais podem não ser suficientes se você precisar saber mais sobre as atividades do adversário.

O retorno ao modo operacional normal era a maior prioridade para essas organizações. A DART ajudou a restaurar os serviços, primeiro ao investigar o impacto e, em seguida, ao tomar as medidas de mitigação necessárias, como remover o malware dos sistemas afetados e retorná-los a um estado íntegro. A equipe também treinou os clientes sobre como usar as ferramentas de investigação de ameaças da Microsoft, incluindo o EDR e outros, para que eles pudessem procurar comportamentos anômalos e atividades do invasor em sua rede. A DART enfatizou que o monitoramento de pontos de extremidade é crítico para a defesa contra ataques sofisticados e direcionados que podem não ser detectados por soluções antivírus tradicionais.

Orientações



Orientações

A criação da resiliência organizacional e a redução significativa de riscos exigem uma abordagem de segurança que inclua prevenção, detecção e resposta. Organizamos as seguintes sugestões de práticas recomendadas e controles de segurança nessas categorias.

PREVENÇÃO:

Os controles preventivos desempenham uma função fundamental em uma estratégia de defesa geral, pois os investimentos adequados podem aumentar o custo dos ataques para os criminosos cibernéticos e sustentar esse aumento nos custos de ataques ao longo do tempo (sem exigir que um analista especialista monitore e interprete o resultado). Os investimentos em controles preventivos devem ser direcionados às técnicas de menor custo para remover regularmente técnicas de ataque baratas e eficientes.

As quatro coisas a considerar para a prevenção são:

1. **A proteção de segurança é crítica. Como visto em alguns dos incidentes cibernéticos compartilhados neste relatório, problemas de proteção comuns podem prejudicar os recursos avançados de segurança. Portanto, seguir estas dicas pode ajudar a reduzir riscos:**

- Evite usar softwares desconhecidos gratuitos e/ou pirateados. Utilize apenas softwares de fontes confiáveis.
- Reduza o risco de roubo de credenciais, inclusive ao proteger contas de administrador privilegiadas.

  Para saber como, leia este blog, que descreve alguns princípios e ferramentas que a Microsoft usou para orientar e aprimorar nossa própria postura de segurança e alguns roteiros prescritivos para ajudá-lo a planejar suas próprias iniciativas.
- Aplique as linhas de base de configuração seguras fornecidas pelos fornecedores do software.
- Mantenha os computadores atualizados aplicando com rapidez as atualizações mais recentes aos seus sistemas operacionais e aplicativos e implante imediatamente as atualizações críticas de segurança para sistemas operacionais, navegadores e emails. Isole (ou desative) computadores que não podem ser atualizados nem corrigidos.
- Implemente proteções avançadas de emails e navegadores. Implante um gateway de email seguro que tenha recursos de proteção avançada contra ameaças para defesa contra variantes modernas de phishing.
- Habilite defesas de rede e antimalware de host para obter respostas de bloqueio da nuvem quase em tempo real (se disponível em sua solução).

2. **Implemente controles de acesso. Considere o seguinte:**

- Aplique o princípio de privilégio mínimo, que inclui a implementação da segmentação da rede, a remoção de privilégios de administrador local dos usuários finais e a cautela ao conceder permissões a aplicativos em execução no computador.
- Limite o download de aplicativos para apenas aqueles de fontes confiáveis (uma loja de aplicativos oficial).
- Implante políticas fortes de integridade de códigos, incluindo a restrição dos aplicativos que os usuários podem executar. Se possível, adote uma solução de segurança que restringirá o código que é executado no núcleo do sistema (kernel) e que possa bloquear scripts não assinados e outras formas de código não confiável. Use uma lista de permissões de aplicativos.
- Para saber mais sobre os ataques da cadeia de fornecedores de software e como protegê-las, leia este blog de pesquisadores da Microsoft.

3. **Guarde os backups.**

- Crie backups resistentes à destruição de seus sistemas e dados críticos.
- Use serviços de armazenamento em nuvem para backup automático de dados online. Para dados que estão na infraestrutura local, faça backup regularmente de dados importantes usando a regra de 3-2-1. Guarde três backups de seus dados em dois tipos de armazenamento diferentes e pelo menos um backup externo.

4. **Fique atento e tome medidas se suspeitar de algo.**

- Instrua os funcionários a serem cautelosos com comunicações suspeitas que solicitam informações confidenciais e oriente-os a reagir e reportá-las à equipe de operações de segurança da organização imediatamente. O treinamento também pode ajudar a reduzir ataques de spear phishing e engenharia social.
- Tenha cuidado ao clicar em links da Web. Colocar em prática hábitos seguros de navegação na Web e usar soluções que forneçam avisos ou bloqueiem o acesso a sites não seguros podem ajudar a reduzir a probabilidade de encontrar sites associados à mineração de criptomoedas.
- Se um computador estiver excepcionalmente lento, procure quaisquer arquivos suspeitos em execução e sinta-se à vontade para enviar uma amostra para o fornecedor do sistema operacional. Você pode enviar arquivos para análise de malware à Microsoft em https:// www.microsoft.com/wdsi/filesubmission.

DETECÇÃO E RESPOSTA:

A detecção e a resposta contribuem para a resiliência, limitando o tempo em que um invasor tem acesso aos seus recursos. Isso diminui o ROI do invasor, aumentando os custos do invasor (ele deve repetir ou modificar suas operações) e diminuindo o retorno (limita a probabilidade de alcançar seu objetivo).

A mesma tecnologia de nuvem que está permitindo que as organizações empresariais atendam melhor às necessidades do mercado também pode ajudar as operações de segurança a melhor combater os invasores.

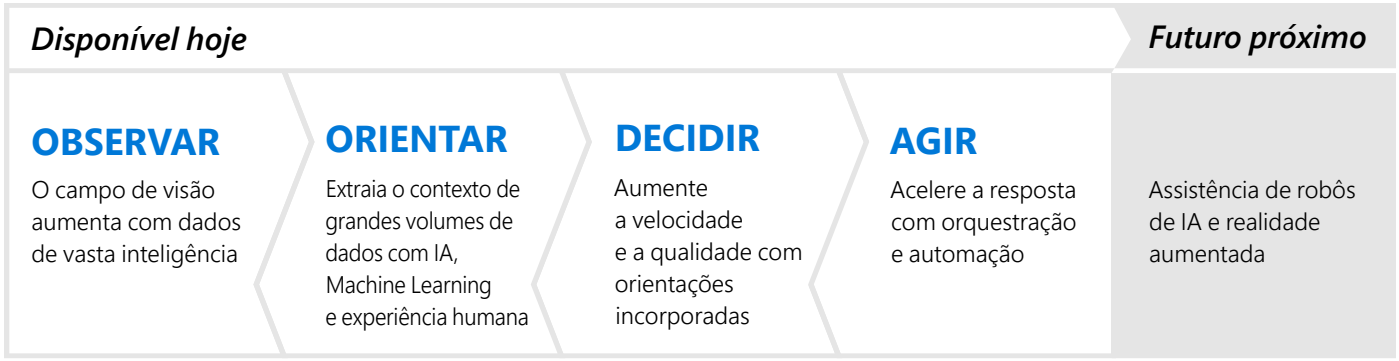


FIGURA 10.

Trajetória evolutiva dos centros de operações de segurança

Ao analisarmos a trajetória da evolução dos centros de operações de segurança (SOCs), percebemos que a tecnologia vem aumentando continuamente a velocidade e a qualidade das decisões e ações do SOC. Muitas dessas inovações podem ser mapeadas para cada etapa do "loop" Observar Orientar Decidir Agir (OODA) que foi documentado pelo Coronel da Força Aérea dos EUA John Boyd.[3]

OBSERVAR – Os SOCs podem explorar a vasta inteligência de segurança disponível (da Microsoft e de outras fontes), aumentando drasticamente seu campo de visão na organização e no ambiente externo.

ORIENTAR – À medida que essas novas fontes de dados são disponibilizadas para os SOCs já sobrecarregados, o machine learning (um subconjunto da inteligência artificial) torna-se uma ferramenta crítica para avaliar esses grandes conjuntos de dados e identificar anomalias que valem a pena investigar. Os fornecedores de segurança (incluindo a Microsoft) adotaram a tecnologia de machine learning para priorizar rapidamente os eventos (e ajudar a combinar esses eventos individuais a incidentes holísticos).

DECIDIR – Como a complexidade e o volume de ataques podem sobrecarregar rapidamente um SOC, os analistas e profissionais responsáveis por respostas a incidentes precisam tomar muitas decisões e agir com rapidez em resposta a alertas e detecções. A Microsoft e outros fornecedores têm recursos integrados de investigação automatizada, bem como orientações para ajudar os analistas a tomarem decisões adequadas rapidamente (para isolar dispositivos possivelmente infectados ou comprometidos, por exemplo). Por enquanto, a automação está se concentrando em resolver rapidamente incidentes de baixa prioridade para que habilidades especializadas possam ser aplicadas a problemas mais complexos.

AGIR – Respostas exigem uma execução rápida e exata em muitas tecnologias e plataformas, que é o que a orquestração de segurança e as tecnologias de automação de resposta permitem. A Microsoft e muitas outras empresas continuam a investir nessas tecnologias, incluindo soluções modernas de detecção de ameaças e resposta automatizada.

NOTAS DE RODAPÉ

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Algumas outras tendências que se aplicam a um SOC moderno são:

- **Qualidade em vez da quantidade de feeds de alerta** – À medida que as organizações mudam do gerenciamento de "informações não suficientes" para o gerenciamento de "muitas informações", o tempo e a atenção dos analistas altamente especializados do SOC tornam-se cada vez mais valiosos. Isso impulsiona uma necessidade crescente de qualidade nos alertas que exigem o envolvimento de analistas de nível 1 e 2. Embora os feeds de dados adicionais sejam sempre úteis para investigações e caça proativa, o SOC corporativo de TI da Microsoft mede a verdadeira taxa positiva de feeds de alertas que exigem resposta do analista (e atualmente requer uma taxa positiva verdadeira de 90% ou superior).

- Gravidade dos dados – Análises de grandes conjuntos de dados (incluindo dados de segurança) são difíceis sem o acesso aos dados brutos subjacentes. À medida que mais dados de segurança são disponibilizados, torna-se mais econômico e prático executar a análise de segurança na nuvem em relação ao backhauling desses dados para um sistema na infraestrutura local. Isso provavelmente levará à evolução das arquiteturas do SIEM e do SOC que podem incluir abordagens híbridas do SIEM ou a adoção do SIEM nativo da nuvem como serviço.

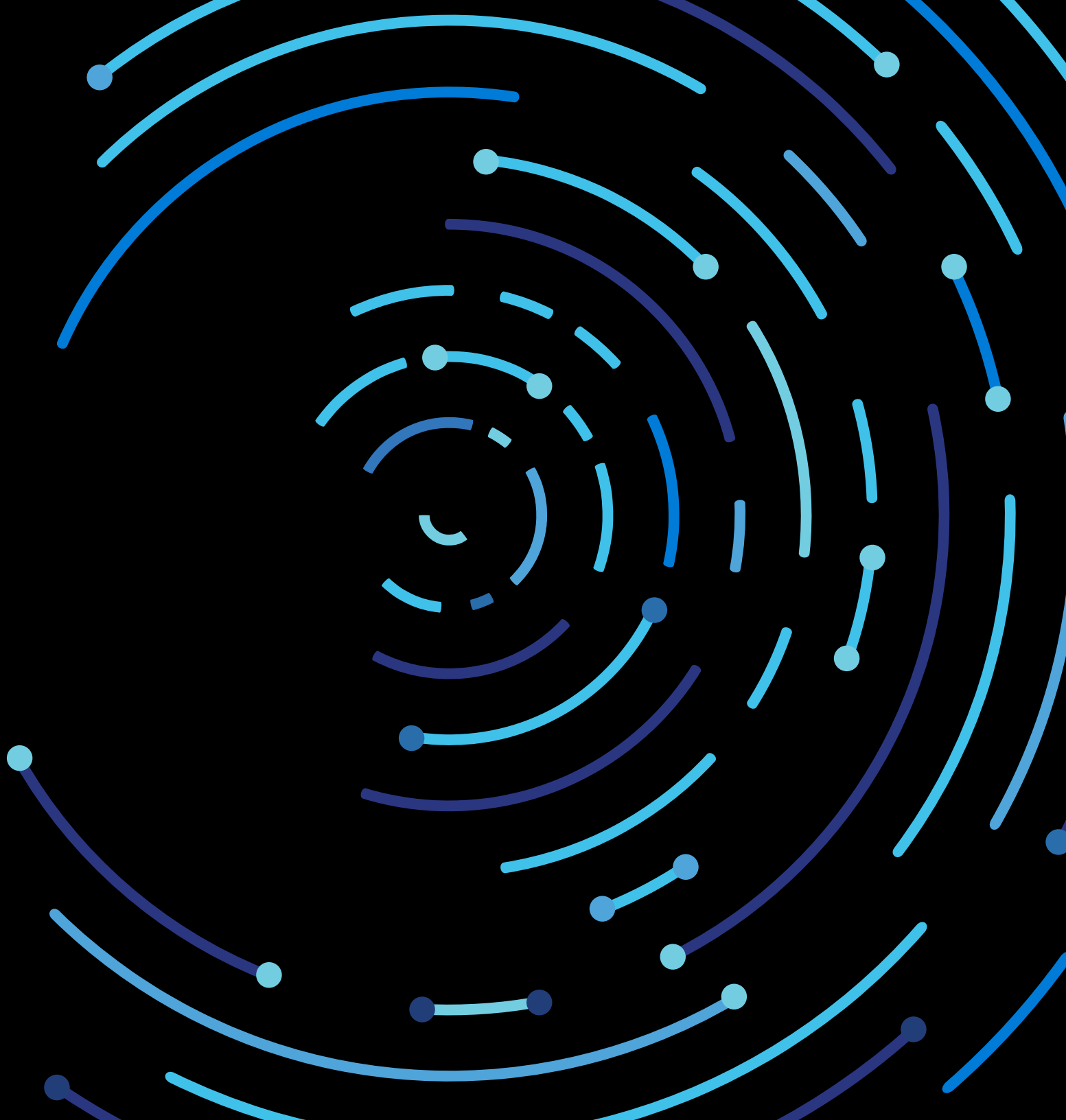
- **Alto contexto** – Estes tipos de detecções são muito mais úteis devido à sua capacidade de correlacionar conjuntos de dados de forma mais eficiente. Embora as detecções tradicionais baseadas em tráfego de rede ainda forneçam algum valor de segurança, o tráfego de rede bruto normalmente carece de contexto para diferenciar atividades legítimas e atividades anômalas. Estamos percebendo que os SOCs obtêm muito mais valor de detecções de contexto sofisticadas, como:

  - **Soluções de detecção e resposta de ponto de extremidade (EDR)** que têm um contexto aprofundado das atividades do host
  - Detecções baseadas em identidade que incluem insights sobre padrões normais de autenticação de usuários (locais, horários, serviços acessados etc.) e aplicam a análise de comportamento

Essas detecções ricas em contexto são mais difíceis de serem evitadas por adversários porque eles devem imitar uma operação muito mais complexa (em comparação com alguns atributos técnicos de tráfego IP).

Outra lição que aprendemos com grandes violações de clientes foi a dificuldade de responder com rapidez a incidentes quando as funções de TI são parcialmente ou totalmente terceirizadas. Recomendamos revisar seus contratos de terceirização de TI e contratos de nível de serviço (SLAs), bem como os fornecedores da cadeia de fornecedores para garantir que eles sejam compatíveis com a resposta de segurança rápida. Para obter mais aprendizados de nossas investigações de incidentes de clientes, consulte o Guia de Referência de Resposta a Incidentes (IRRG) em https://aka.ms/IRRG.

Fontes de dados



Fontes de dados

A Microsoft coletou os dados incluídos no Relatório de Inteligência em Segurança da Microsoft ao longo do fornecimento de uma ampla gama de seus produtos e serviços, conforme abordado na Política de Privacidade da Microsoft. Esses dados nos fornecem informações valiosas sobre a segurança e as operações de nossos produtos e serviços, bem como insights sobre o cenário de ameaças de segurança cibernética em geral. Esses dados incluem a análise das seguintes fontes:[4]

- **A Central de Segurança do Azure** é um serviço que ajuda as organizações a prevenir, detectar e responder a ameaças, proporcionando maior visibilidade da segurança dos workloads na nuvem e usando análises avançadas e a inteligência contra ameaças para detectar ataques.

- **O Bing** é o mecanismo de pesquisa e decisão que executa bilhões de verificações de páginas da Web por ano para procurar conteúdos maliciosos. Depois que esses conteúdos são detectados, o Bing exibe avisos aos usuários para ajudar a prevenir a infecção.

- **O Exchange Online** é o serviço de email e produtividade hospedado pela Microsoft. Os serviços antimalware e antispam do Exchange Online verificam bilhões de mensagens todo ano para identificar e bloquear spam e malware.

- **A Ferramenta de Remoção de Software Mal-Intencionado** (MSRT) é uma ferramenta gratuita que a Microsoft projetou para ajudar a identificar e remover famílias de malware predominantes e específicas de computadores de clientes. A MSRT é disponibilizada principalmente como uma atualização importante por meio do Windows Update, do Microsoft Update e das atualizações automáticas. Uma versão da ferramenta também está disponível no Centro de Download da Microsoft. A MSRT não substitui uma solução antivírus atualizada que funciona em tempo real.

- **O Verificador de Segurança da Microsoft** é uma ferramenta de segurança para download gratuito que fornece verificação sob demanda e ajuda a remover malware e outros softwares maliciosos. O Verificador de Segurança da Microsoft não substitui uma solução antivírus atualizada, porque não oferece proteção em tempo real e não pode impedir que um computador seja infectado.

NOTAS DE RODAPÉ

[4]Importante: esses dados sempre passam por limites rigorosos de privacidade e conformidade antes de serem usados para segurança.

- **O Microsoft Security Essentials** é um produto de proteção em tempo real gratuito e de fácil download que fornece proteção antivírus e antispyware básica e eficiente para o Windows Vista e o Windows 7.

- **O Microsoft System Center Endpoint Protection** (anteriormente Forefront Client Security e Forefront Endpoint Protection) é um produto unificado que fornece proteção contra malware e software indesejado para desktops, laptops e sistemas operacionais de servidores corporativos. Ele usa o Mecanismo de Proteção contra Malware da Microsoft e o banco de dados de assinatura antivírus da Microsoft para fornecer proteção em tempo real, programada e sob demanda.

- **O Office 365** é o serviço de assinatura do Microsoft Office para organizações e usuários domésticos. Alguns planos de assinatura incluem o acesso à Proteção Avançada contra Ameaças do Office 365.

- **A Segurança do Windows** no Windows 10 fornece verificação e remoção em tempo real de malware e software indesejado. Além disso, a versão mais recente do Windows utiliza dados contextuais avançados, como configuração de máquina, performance e integridade do dispositivo e outras informações desse tipo, para aumentar a segurança dos clientes. Ao mesmo tempo, capacitamos os clientes a serem mais informados sobre a privacidade no Windows 10. Leia este blog para saber mais sobre algumas das maneiras como a Microsoft faz isso.

- **A Proteção Avançada contra Ameaças do Windows Defender** é um serviço incorporado à Atualização de Aniversário do Windows 10 e versões posteriores que permite que os clientes corporativos detectem, investiguem e corrijam ameaças e violações de dados persistentes e avançadas nas suas redes.

- **O Windows Defender Offline** é uma ferramenta para download que pode ser usada para criar um CD, um DVD ou um pen drive inicializável para verificar se há malware e outras ameaças em um computador. Ele não oferece proteção em tempo real e não substitui uma solução antimalware atualizada.

- **O Windows Defender SmartScreen**, um recurso no Microsoft Edge e no Internet Explorer, oferece aos usuários proteção contra sites de phishing e sites que hospedam malware. A Microsoft mantém um banco de dados de sites de phishing e malware relatados por usuários do Microsoft Edge, do Internet Explorer e de outros produtos e serviços da Microsoft. Quando um usuário tenta acessar um site no banco de dados com o filtro habilitado, o navegador exibe um aviso e bloqueia a navegação para a página.