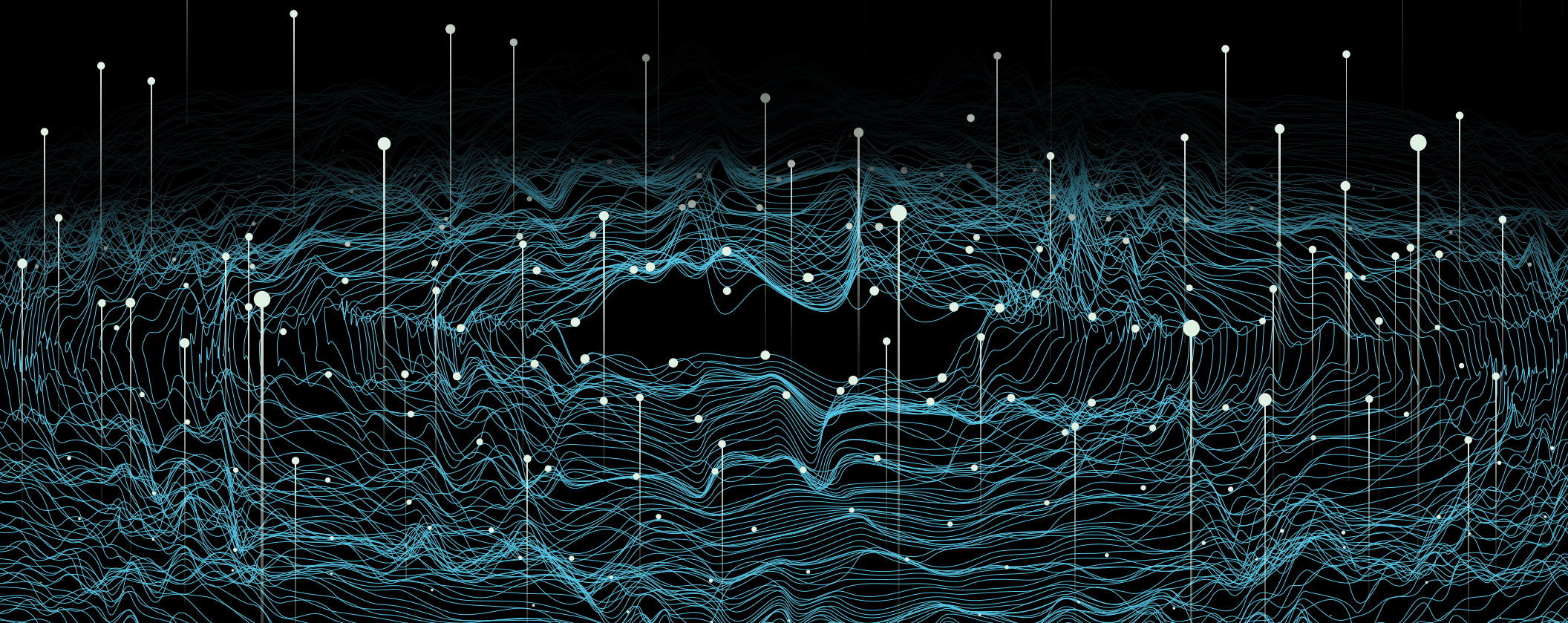
Microsoft

RELATÓRIO DE INFORMAÇÕES DE SEGURANÇA DA MICROSOFT

VOLUME 24
JANEIRO – DEZEMBRO 2018



Índice

Autores e colaboradores . . . 3

Prefácio . . . 4

SECÇÃO I: Ransomware, mineração de criptomoedas e dinheiro . . . 6

Declínio dos ataques de ransomware . . . 7

Mineração de criptomoedas em crescimento . . . 10

Mineradores de criptomoedas baseados no browser: um novo tipo de ameaça . . . 11

Impacto da mineração não solicitada de criptomoedas . . . 12

SECÇÃO II: Cadeias de fornecimento de software em risco . . . 13

Confiança em risco . . . 16

Para lá do software: compromisso da cadeia de fornecimento através de objetos na cloud . . . 17

Investigação de ciberincidentes: Serviços profissionais . . . 18

SECÇÃO III: O phishing ainda prevalece . . . 19

O phishing continua a ser um vetor de ataque preferencial em 2018 . . . 20

Investigação de ciberincidentes: Indústria . . . 23

SECÇÃO IV: Malware em todo o mundo . . . 24

Investigação de ciberincidentes: Serviços financeiros . . . 27

Orientação . . . 28

Origens de Dados . . . 33

Este documento é fornecido meramente para efeitos informativos. A MICROSOFT NÃO OFERECE QUAISQUER GARANTIAS, EXPRESSAS, IMPLÍCITAS OU LEGAIS, RELATIVAMENTE ÀS INFORMAÇÕES DESTE DOCUMENTO.

Este documento é fornecido "tal como está". As informações e visões expressas neste documento, incluindo os URLs e outras referências a Web sites da Internet, podem ser alteradas sem aviso prévio. O utilizador é o único responsável pela utilização destas informações.

Copyright © 2019 Microsoft Corporation. Todos os direitos reservados.

Os nomes de produtos e empresas reais mencionados no presente documento poderão ser marcas registadas dos respetivos 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 Cibersegurança

Elia Florio
Defesa Ativa do Windows

Eric Avena
Equipa de Investigação do Windows Defender

Eric Douglas
Equipa de Investigação do Windows Defender

Francis Tan Seng
Equipa de Investigação do Windows Defender

Jonathan Trull
Grupo de Soluções de Cibersegurança

Joram Borenstein
Grupo de Soluções de Cibersegurança

Karthik Selvaraj
Equipa de Investigação do Windows Defender

Kasia Kaplinska
Marketing de Segurança da Microsoft

Kristina Laidler
Resposta a Incidentes de Segurança

Matt Duncan
Engenharia e Análise de Dados da Defesa Ativa do Windows

Mark Simos
Grupo de Soluções de Cibersegurança

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 Cibersegurança

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Equipa de Investigação do Windows Defender

Volv Grebennikov
Bing

Yaniv Zohar
Segurança do Azure

Prefácio

Olá e bem-vindo(a) à 24.ª edição do Relatório de Informações de Segurança da Microsoft (SIR). Como profissional e arquiteto de segurança, leio relatórios como este na esperança de compreender um pouco melhor o ambiente, elaborando conselhos práticos sobre como utilizar esses conhecimentos para defender e proteger as organizações de forma mais eficaz.

A equipa SIR incorpora neste relatório o espírito da formação para melhorar a resiliência informática, tendo analisado um ano de dados de modo a apurar as lições mais importantes.

O que está a ler são insights selecionados ao longo de um ano de análise de dados de segurança e de aprendizagem de lições práticas. Os dados analisados incluem os 6,5 biliões de sinais de ameaça que atravessam diariamente a Cloud Microsoft e a pesquisa e experiências do mundo real dos nossos milhares de investigadores de segurança e inquiridos a nível mundial. Em 2018 os atacantes utilizaram uma variedade de golpes baixos, tanto novos (mineração de moedas) como velhos (phishing), na tentativa permanente de roubar dados e recursos a clientes e organizações. Ataques híbridos, como a campanha Ursnif, misturaram abordagens sociais e técnicas. Com os defensores a responderem melhor ao ransomware, uma forma de ataque visível e disruptiva, os criminosos viraram-se para os mais "discretos", mas bastante rentáveis, mineiros de moedas.

Esta "viragem" pode parecer frustrante, uma vez que os atacantes estão sempre um passo à frente. Mas vista de uma perspetiva diferente, esta evolução até é positiva. Os defensores e os profissionais de cibersegurança implementaram técnicas defensivas que forçaram os atacantes a mudar as suas payloads preferenciais, afastando-se do ransomware.

Outra área onde aumentou a atividade dos cibercriminosos foi a cadeia de fornecimento. Um dos ataques mais notáveis, o surto de mineração de moeda Dofoil que ocorreu a 6 de março de 2018, foi espoletado por uma aplicação peer-to-peer manipulada. As preocupações com a cadeia de fornecimento ultrapassaram as aplicações e chegaram à cloud, incluindo extensões de browser maliciosas, repositórios de Linux comprometidos e múltiplas instâncias de backdoor de módulos. Para resolver estas ameaças, as organizações estão a passar para um modelo de cadeia de fornecimento transparente e fiável.

Os dados são ótimos, mas às vezes é útil descobrir o que realmente aconteceu numa organização. Foi por isso que incluímos lições aprendidas no terreno pela nossa Equipa de Deteção e Resposta (DART). Essas lições incluem a forma como uma grande empresa industrial conseguiu implementar controlos para bloquear uma campanha de phishing multifaseada que a tinha atormentado durante meses, assim como instituições financeiras que foram finalmente capazes de erradicar os autores de ameaças dos seus sistemas utilizando ferramentas avançadas de investigação e monitorização do endpoint.

Por último, mas não menos importante, os cliques de phishing continuaram a aumentar, mas os modelos de machine learning estão a permitir melhorar a deteção de phishing antes que atinja as caixas dos utilizadores, e anular os danos pós-clique, caso lá chegue. Mais boas notícias? Um número crescente de empresas está a implementar soluções multifator para limitar o sucesso dos e-mails de phishing de roubo de credenciais.

Os atacantes procuram oportunidades, pelo que quanto mais soubermos sobre as suas técnicas e artifícios, melhor preparados estaremos para criar defesas e reagir rapidamente. Pequenos passos importantes podem fazer uma enorme diferença no estado geral de cibersegurança de uma organização. É por isso que, juntamente com insights aprofundados sobre a evolução do malware e dos cenários de ataque, encontrará neste relatório ações recomendadas e outras orientações de melhores práticas. Porque nos meus tempos de profissional era exatamente isto o que eu precisava na minha luta contra os criminosos. Esperamos que seja também o que precisa.

Diana Kelley
Diretora Operacional de Cibersegurança da Microsoft

P.S. Estamos sempre a tentar melhorar o SIR. Se tiver feedback, entre em contacto e dê-nos a sua opinião.

SECÇÃO I

Ransomware, mineração de criptomoedas e dinheiro

Em 2017, as principais histórias de segurança envolveram maioritariamente ransomware. Por todo o mundo, os surtos em destaque de WannaCrypt e Petya colocaram o ransomware (um tipo de malware que bloqueia ou encripta os computadores, exigindo depois dinheiro para restaurar o acesso) na consciência global, e muitos especularam que o problema tenderia a agravar-se no futuro. Em vez disso, as ocorrências de ransomware diminuíram de forma significativa em 2018.

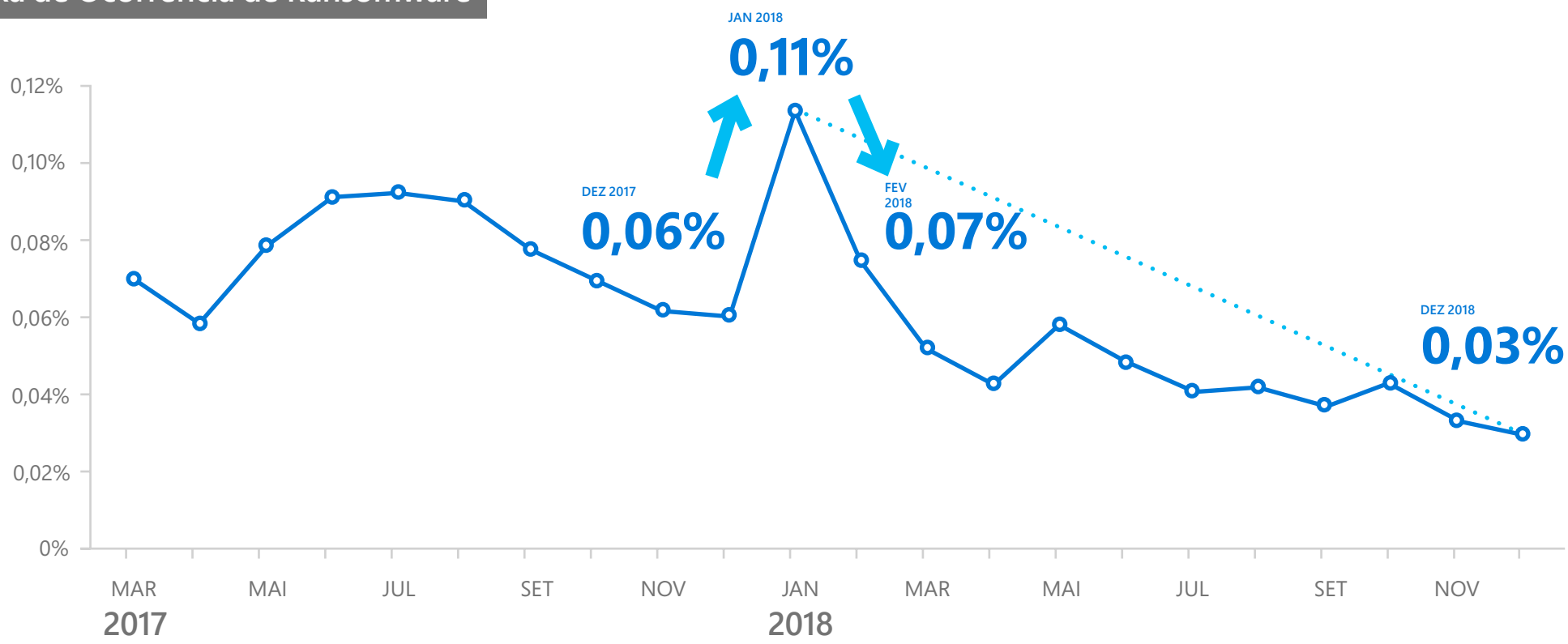
O declínio das ocorrências de ransomware ficou em parte a dever-se à melhoria da deteção e formação, que tornou mais difícil a obtenção de lucros por parte dos atacantes. Em resultado, os atacantes começaram a deslocar os seus esforços do ransomware para abordagens como a mineração de criptomoedas, que utiliza os recursos informáticos das vítimas para criar dinheiro digital para os atacantes. Esta alteração demonstra a natureza fundamentalmente oportunista da maioria dos cibercriminosos que visam a obtenção de lucro: eles tendem a perseguir o dinheiro mais facilmente disponível, e quando a economia do cibercrime muda, eles acompanham rapidamente a mudança.

DECLÍNIO DOS ATAQUES DE RANSOMWARE

Há mais de uma década, os hackers e os brincalhões que dominaram o início do malware foram suplantados pelo crime organizado e por outros interesses orientados para o lucro. Enquanto os surtos iniciais de malware eram muitas vezes chamativos e óbvios, o malware orientado para o lucro operava com mais frequência de forma silenciosa e evitava atrair as atenções, a fim de continuar a desempenhar a sua função: o envio de spam, o roubo de informações confidenciais, a realização de ataques de negação de serviço e outras atividades maliciosas, durante o máximo de tempo possível.

O ransomware inverteu esta tendência. Em vez de tentar permanecer oculto, o ransomware nega abertamente o acesso das vítimas aos seus computadores e ficheiros importantes até que a vítima pague o resgate (e muitas vezes mesmo depois: é frequente os atacantes não abdicarem do controlo dos computadores, mesmo após o pagamento do resgate). Como o ransomware atingiu um pico em 2017, parecia que este estilo de ataque aberto poderia representar uma nova fase das técnicas de ataque. Mas dados mais recentes sugerem que o ransomware poderá estar em declínio, com os atacantes a regressarem cada vez mais aos modos de operação mais furtivos que utilizaram no passado, procurando ocultar-se dos radares a fim de levarem a cabo ataques mais eficazes, como a mineração de criptomoedas. Embora tenha havido um declínio na taxa de ocorrência de ransomware, isso não significa necessariamente que a gravidade dos ataques tenha diminuído.

Taxa de Ocorrência de Ransomware



As taxas de ocorrência de ransomware diminuíram em cerca de 60% entre março de 2017 e dezembro de 2018, com aumentos intermitentes ao longo desse período.

FIGURA 1.

Ocorrências de ransomware entre março de 2017 e dezembro de 2018

Provavelmente há muitas causas para este declínio global, embora os investigadores de segurança da Microsoft suspeitem que um fator principal é que tanto os utilizadores finais como as organizações se estão a tornar mais conscientes e a lidar de forma mais inteligente com as ameaças de ransomware, tendo mais cuidado e fazendo cópias de segurança dos ficheiros importantes para que os possam restaurar caso sejam encriptados por ransomware. Além disso, conforme descrito anteriormente, os cibercriminosos são oportunistas.

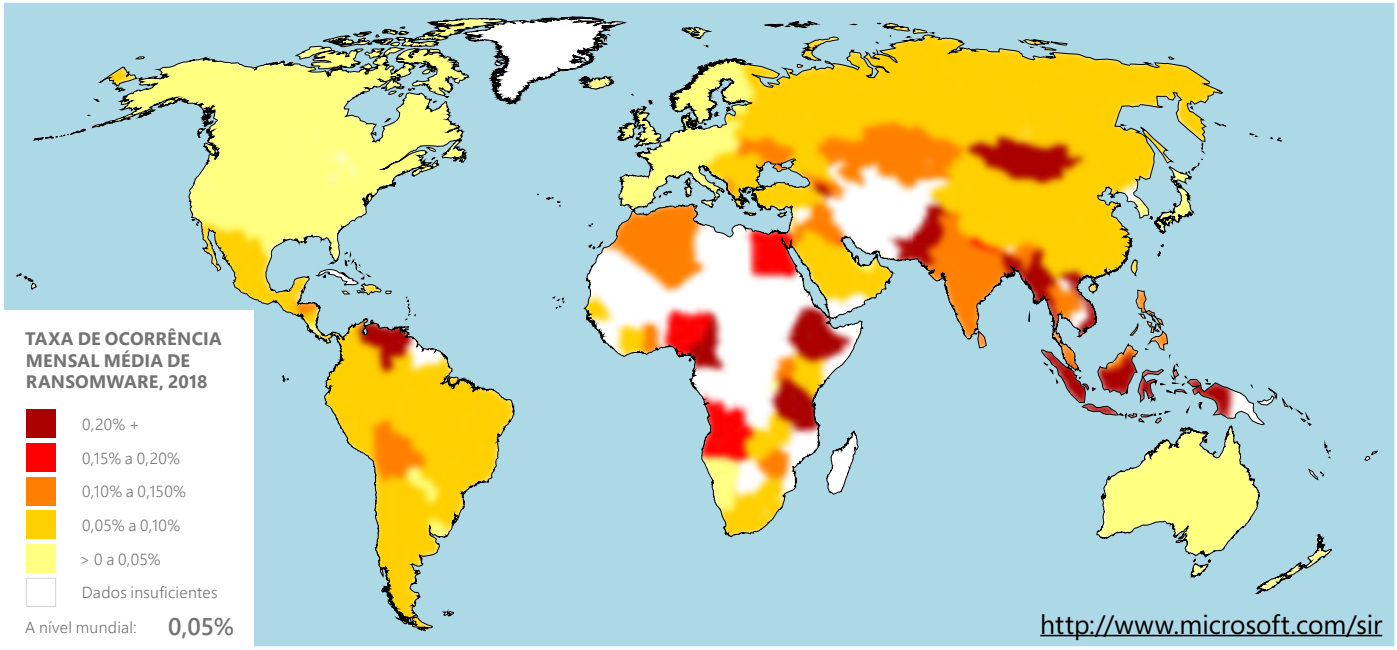
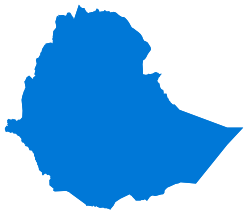


FIGURA 2.

Taxas de ocorrência mensal média de ransomware a nível mundial, por país/região, em 2018

PAÍS MAIS AFETADO PELO RANSOMWARE: ETIÓPIA



Taxa de ocorrência mensal média: **0,77%**

Em 2018, os cinco países com a maior taxa de ocorrência mensal média de ransomware foram a Etiópia (taxa mensal média de 0,77%), Mongólia (0,46), Camarões (0,41), Myanmar (0,33) e Venezuela (0,31), cada um dos quais com uma taxa de ocorrência mensal média de ransomware de 0,31% ou superior durante o período.[1] Há alguns anos, as ocorrências de ransomware tendiam a agrupar-se em países e regiões ricas da Europa e América do Norte, mas com o declínio da utilização do ransomware por parte dos atacantes, o padrão de ocorrências tornou-se mais parecido com o do malware em geral.

Em 2018, os países com as menores taxas de ocorrência de ransomware foram a Irlanda (0,01%), Japão (0,01), Estados Unidos (0,02), Reino Unido (0,02) e Suécia (0,02), cada um dos quais com uma taxa de ocorrência mensal média de ransomware de 0,02% ou inferior durante o mesmo período. Os locais com baixas taxas de ocorrência tendem a ter infraestruturas de cibersegurança maduras e programas bem estabelecidos para proteger as infraestruturas críticas e comunicar com os cidadãos sobre segurança básica.

NOTAS DE RODAPÉ

[1] A taxa de ocorrência é a percentagem de computadores que executam produtos de segurança em tempo real da Microsoft que relatam uma ocorrência de malware. Encontrar uma ameaça não significa que o computador tenha sido infetado. Apenas os computadores cujos utilizadores optaram por fornecer dados à Microsoft são tidos em consideração para calcular as taxas de ocorrência.

MINERAÇÃO DE CRIPTOMOEDAS EM CRESCIMENTO

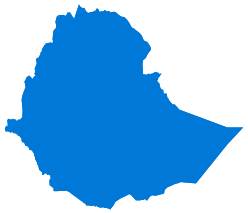
As criptomoedas constituem dinheiro virtual que pode ser utilizado para comprar e vender bens e serviços de forma anónima, tanto online como no mundo físico. Existem muitos tipos diferentes de criptomoedas, mas todos se baseiam na tecnologia blockchain, em que cada transação é registada num ficheiro de controlo distribuído, mantido por milhares ou milhões de computadores em todo o mundo. As novas moedas são criadas, ou "mineradas", por computadores que executam cálculos complexos, que servem também 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 popular, valia vários milhares de dólares americanos), mas a execução dos cálculos necessários pode consumir muitos recursos e com a mineração de cada nova moeda a sobrecarga para os recursos aumenta. Para as moedas populares, como a Bitcoin, a mineração de moedas de forma lucrativa é quase impossível sem acesso a vastos recursos de computação, muito fora do alcance da maioria dos indivíduos e pequenas organizações. Por este motivo, os atacantes que procuram obter lucros ilícitos têm recorrido cada vez mais ao malware, que lhes permite utilizar os computadores das vítimas para os ajudar a minerar criptomoedas. Esta abordagem permite que aproveitem a capacidade de processamento de centenas de milhares de computadores, em vez de um ou dois. Mesmo quando é detetada uma infeção menor, a natureza anónima das criptomoedas complica os esforços para descobrir os responsáveis.

Em 2018, a taxa de ocorrência mensal média de mineração de criptomoedas a nível mundial foi de 0,12%, em comparação com apenas 0,05% para o ransomware. Muitos fatores contribuem para o aumento da popularidade da mineração como payload de malware. Ao contrário do ransomware, a mineração de criptomoedas não requer a participação do utilizador: funciona em segundo plano, enquanto o utilizador realiza outras tarefas ou está longe do computador, e pode nem sequer ser notada a menos que degrade de forma notória o desempenho do computador. Por esse motivo, é menos provável que os utilizadores tomem qualquer ação para remover a ameaça, pelo que a mineração poderá continuar a beneficiar o atacante durante muito tempo.

A disponibilidade de produtos "prontos a usar" para mineração encoberta de muitas criptomoedas é outro fator que explica a tendência. A barreira à entrada é baixa dada a ampla disponibilidade de software de mineração de moedas, que os cibercriminosos voltam a empacotar como malware para entregar aos computadores dos utilizadores desprevenidos. Os mineradores armados são então distribuídos às vítimas utilizando muitas das técnicas que os atacantes usam para distribuir outras ameaças, como a engenharia social, exploits e downloads drive-by. Após a instalação do software de mineração, este é executado em segundo plano nos computadores das vítimas, executando os cálculos de blockchain e permitindo ao atacante obter as recompensas.

TAXAS DE OCORRÊNCIA MENSAL MÉDIA DOS PAÍSES MAIS AFETADOS PELA MINERAÇÃO DE CRIPTOMOEDAS



Etiópia: 5,58%

Tanzânia: 1,83%

Paquistão: 1,47%

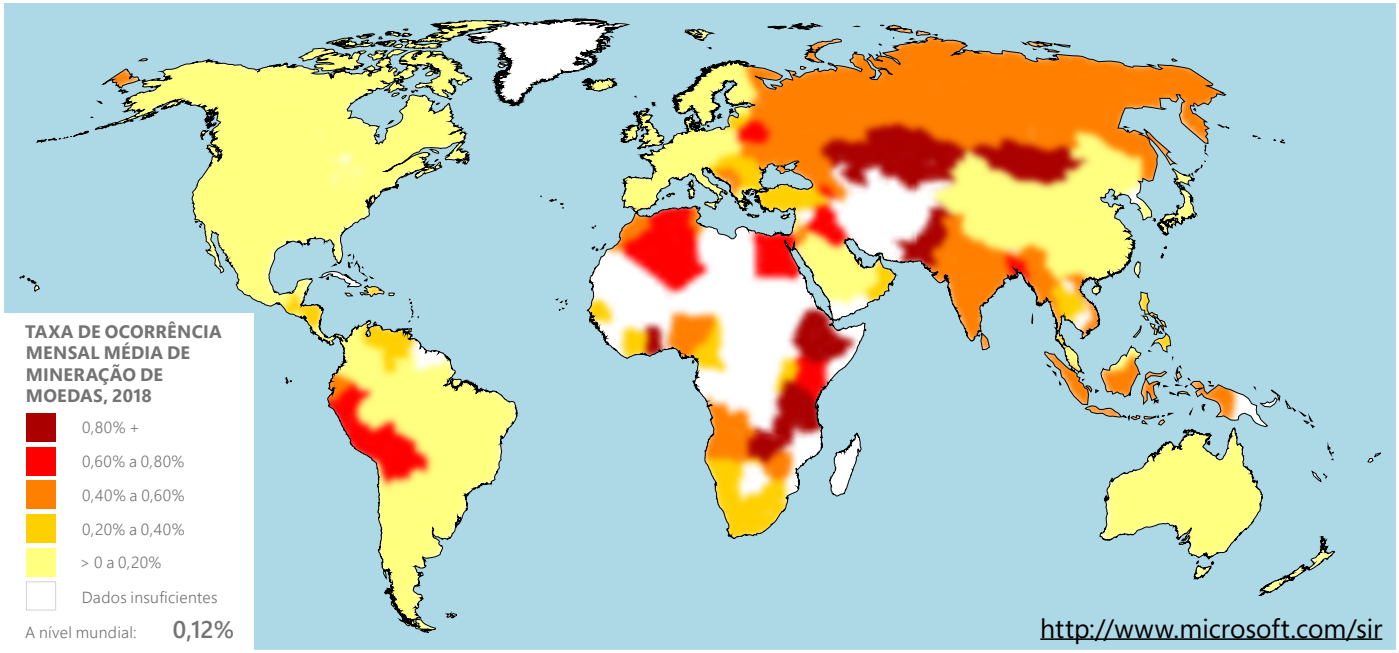


FIGURA 3.

Taxas de ocorrência mensal média de mineração de moedas a nível mundial, por país/região, em 2018

TAXAS DE OCORRÊNCIA MENSAL MÉDIA DOS PAÍSES MENOS AFETADOS PELA MINERAÇÃO DE CRIPTOMOEDAS

Irlanda: 0,02%

Japão: 0,02%

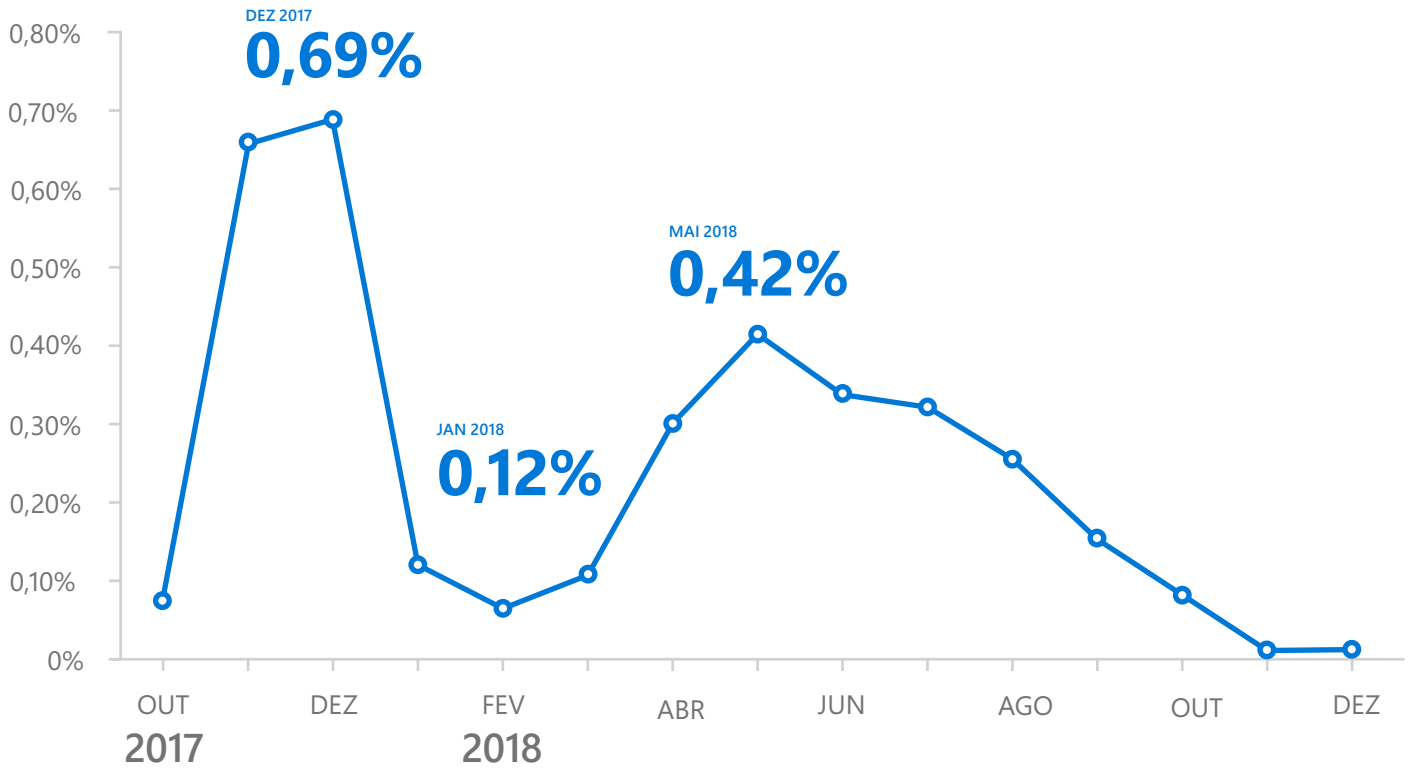
Estados Unidos: 0,02%

Em 2018, os cinco países com as maiores taxas de ocorrência de mineração de criptomoedas foram a Etiópia (5,58%), a Tanzânia (1,83), o Paquistão (1,47), o Cazaquistão (1,24) e a Zâmbia (1,13), cada um dos quais com uma taxa de ocorrência mensal média de mineração de moedas de aproximadamente 1,13% ou superior durante o período. Em 2018, os países com as menores taxas de ocorrência de mineração de moedas foram a Irlanda, Japão, Estados Unidos e China, cada um dos quais com uma taxa de ocorrência mensal média de mineração de moedas de aproximadamente 0,02% durante o período.

MINERADORES DE CRIPTOMOEDAS BASEADOS NO BROWSER: UM NOVO TIPO DE AMEAÇA

As estatísticas apresentadas nesta seção envolvem mineradores maliciosos de criptomoedas concebidos para serem instalados nos computadores das vítimas como malware. Mas algumas das mais significativas ameaças de mineração de criptomoedas são inteiramente baseadas nos browsers, sem precisarem de qualquer tipo de instalação. Diversos serviços anunciam a mineração de criptomoedas baseada no browser como uma forma de os proprietários dos sites monetizarem o respetivo tráfego sem recorrerem à publicidade. Supostamente, os proprietários dos sites adicionam às suas páginas código JavaScript que minera criptomoeda em segundo plano enquanto os utilizadores visitam o site, sendo as receitas divididas entre o proprietário do site e o serviço. Infelizmente, os atacantes têm sido rápidos a tirar partido desses serviços

Taxa de Ocorrência do Brocoiner



para minerar criptomoeda sem obter o consentimento dos utilizadores finais, comprometendo muitas vezes sites legítimos e inserindo de forma maliciosa o código de mineração no respetivo código fonte. Esses mineradores baseados no browser não exigem comprometer o computador do utilizador final, sendo executados em qualquer plataforma com browsers compatíveis com JavaScript. Tal como os trojans de mineração de criptomoedas, os mineradores baseados no browser podem degradar de forma significativa o desempenho do computador e desperdiçar eletricidade enquanto o utilizador visita uma página Web afetada.

FIGURA 4.

Taxa de ocorrência do Brocoiner, o principal minerador de criptomoedas baseado no browser

IMPACTO DA MINERAÇÃO NÃO SOLICITADA DE CRIPTOMOEDAS

A ameaça mais evidente que as vítimas da mineração maliciosa de criptomoedas enfrentam é o consumo de recursos de computação, que pode desperdiçar eletricidade e degradar de forma significativa o desempenho do computador. Os utilizadores e as organizações enfrentam também outros riscos da mineração de moedas, incluindo:

- **Obtenção de um ponto de apoio para provocar maiores danos no futuro.** Como outras formas de malware, a mineração de criptomoedas pode constituir um ponto de entrada para os atacantes. Enquanto o computador está a minerar criptomoedas em segundo plano, os cibercriminosos podem conhecer o seu ambiente e, possivelmente, descobrir falhas de segurança para explorar para outros fins.
- **Os dispositivos ligados à Internet podem ser comprometidos e transformados em bots para mineração de criptomoedas.** Muitos desses dispositivos não possuem segurança interna, como deteção de ameaças de malware, o que os pode tornar em alvos desejáveis para os atacantes.
- **Danificação das máquinas.** A execução de forma contínua do software de mineração de criptomoedas ao longo de meses ou anos pode prejudicar o desempenho, e o calor gerado pelo consumo energético e pela utilização excessiva da CPU pode danificar os computadores.

SECÇÃO II

Cadeias de fornecimento de software em risco

Durante anos, a Microsoft tem seguido o rasto dos atacantes que utilizam o compromisso das cadeias de fornecimento como ponto de entrada para os ataques. Num ataque de cadeia de fornecimento, o atacante concentra-se em comprometer o processo de desenvolvimento ou atualização de um editor de software legítimo.

Se for bem sucedido, o atacante poderá incorporar um componente comprometido numa aplicação ou pacote de atualização legítimo, que é em seguida distribuído aos utilizadores do software. Em seguida, o código malicioso é executado com a mesma confiança e permissões que o software. O número crescente de ataques na cadeia de fornecimento de software nos últimos anos tornou-se num tópico importante em muitos debates sobre cibersegurança, constituindo uma fonte primária de preocupação em muitos departamentos de informática.

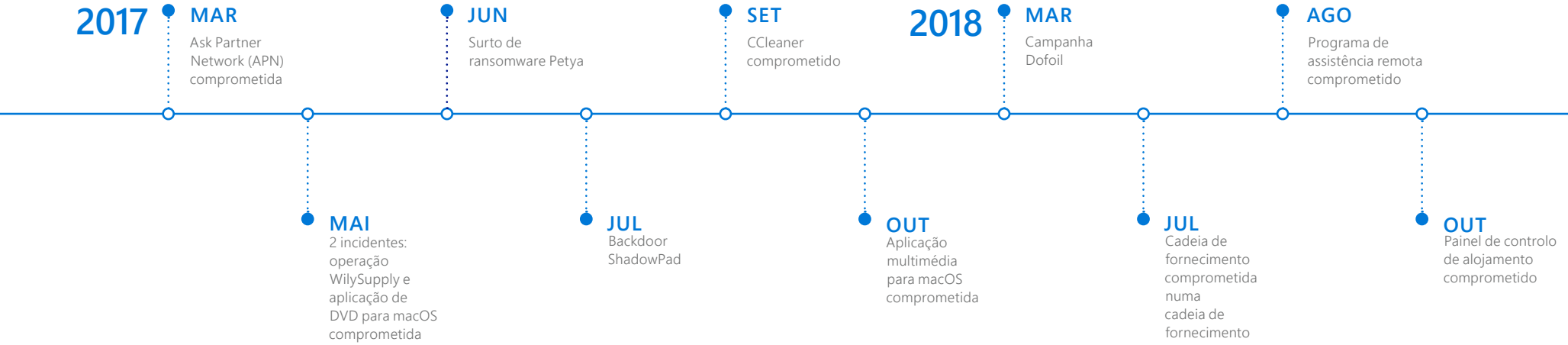


FIGURA 5.

Ataques de cadeia de fornecimento de software em 2017 e 2018

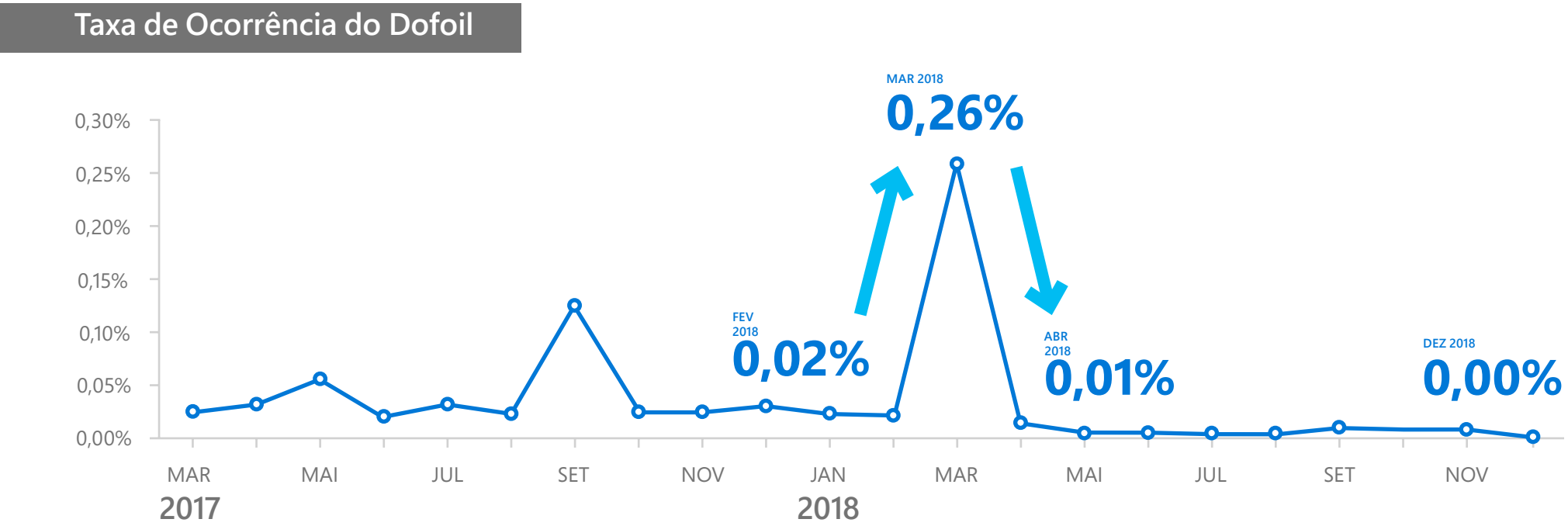
PRINCIPAIS ATAQUES DE CADEIA DE FORNECIMENTO DE SOFTWARE EM 2017

Em 2017 os ataques de cadeia de fornecimento foram responsáveis por um conjunto de incidentes importantes, especialmente o surto de ransomware Petya, em junho, cujas infeções iniciais foram detetadas num processo de atualização comprometido de uma popular aplicação de contabilidade fiscal na Ucrânia. Em maio, a Operação WilySupply comprometeu a ferramenta de atualização de software de um editor de texto, instalando um backdoor em organizações alvo dos setores financeiro e informático. Em julho, um backdoor chamado ShadowPad foi ocultado num pacote de software de gestão de servidores, permitindo aos atacantes instalar payloads adicionais de malware para roubo de dados e outras atividades maliciosas. Em setembro a infraestrutura da popular ferramenta freeware CCleaner foi comprometida, distribuindo uma versão com backdoor à sua base de utilizadores.

O primeiro ataque de cadeia de fornecimento de grandes dimensões de 2018 ocorreu a 6 de março, quando o Windows Defender ATP bloqueou uma campanha massiva de entrega do trojan Dofoil (também conhecido como Smoke Loader). A campanha massiva de malware foi detetada numa aplicação peer-to-peer contaminada. O pacote de atualização da aplicação foi substituído por um pacote malicioso que fazia download de código comprometido que, posteriormente, instalava o malware Dofoil. O trojan sofisticado possuía um payload de mineração de criptomoedas e apresentava técnicas avançadas de injeção de processos cruzados, mecanismos de persistência e métodos de evasão.

FIGURA 6.

Tendência de ocorrência do Dofoil (Smoke Loader) em 2018 revela um pico de instâncias bloqueadas em março



Nas primeiras 12 horas da campanha, o Antivírus do Windows Defender bloqueou mais de 400.000 tentativas de infeção em todo o mundo. A Rússia representou 73% das ocorrências a nível mundial, com a Turquia e a Ucrânia a registarem 18% e 4%, respetivamente.

Foram detetados diversos outros ataques em 2018 utilizando cadeias de fornecimento de software comprometidas como mecanismo de entrega, incluindo os descritos na seguinte tabela:

FIGURA 7.

Outros ataques de cadeias de fornecimento de software em 2018

Período	Ataque	Descrição	Software afetado
Março de 2018	Campanha de mineração de moeda Dofoil (reportado pela Microsoft).	Os atacantes corromperam o processo de atualização de uma aplicação peer-to-peer para instalar o Dofoil, que por sua vez instalava malware de mineração de moedas.	Aplicação peer-to-peer.
Julho de 2018	Cadeia de fornecimento comprometida dentro de uma cadeia de fornecimento (reportado pela Microsoft).	Os atacantes comprometeram a infraestrutura partilhada entre o fornecedor de uma aplicação de edição de PDF e um dos seus parceiros fornecedores de software.	Aplicação de edição de PDF e parceiro fornecedor externo.
Agosto de 2018	Programa de assistência remota comprometido (Operação Red Signature, reportado pela Trend Micro e IssueMakersLab).	O servidor de atualizações de um fornecedor de soluções de assistência remota foi comprometido para distribuir uma ferramenta de acesso remoto chamada 9002 RAT.	Programa de assistência remota.
Outubro de 2018	Solução de painel de controlo de alojamento comprometida (reportado pela ESET).	O script de instalação de uma solução de painel de controlo de alojamento foi alterado para roubar credenciais.	Solução de painel de controlo de alojamento.

CONFIANÇA EM RISCO

Os ataques às cadeias de fornecimento são insidiosos porque tiram partido da confiança que os utilizadores e os departamentos de informática depositam no software que utilizam. O software comprometido é muitas vezes assinado e certificado pelo fornecedor, podendo não dar qualquer indicação de que algo está errado, o que dificulta significativamente a deteção da infeção. Isso pode prejudicar a relação entre as cadeias de fornecimento e os seus clientes, quer estes sejam utilizadores empresariais ou domésticos. Ao corromper o software e minar as infraestruturas de distribuição ou atualização, os ataques à cadeia de fornecimento podem afetar a integridade e a segurança dos bens e serviços que tais organizações fornecem.

Os ataques à cadeia de fornecimento afetaram uma vasta gama de software e visaram organizações de diferentes setores e localizações geográficas. A ameaça dos ataques a cadeias de fornecimento constitui um problema de todo o setor, exigindo a atenção de múltiplos intervenientes, incluindo os programadores e fornecedores de software que escrevem o código, os administradores de sistemas que gerem as instalações de software e a comunidade de segurança da informação que deteta esses ataques e cria soluções para deles proteger as pessoas e o software.

PARA LÁ DO SOFTWARE: COMPROMISSO DA CADEIA DE FORNECIMENTO ATRAVÉS DE OBJETOS NA CLOUD

A capacidade dos ataques à cadeia de fornecimento para minar a confiança é amplificada e torna-se ainda mais complexa na cloud. Diversos incidentes de objetos, serviços e infraestrutura na cloud comprometidos em 2018 destacam esta complexidade:

- Extensões do Chrome corrompidas que instalaram malware de fraude de cliques (reportado pela ICEBRG).
- Vários repositórios de Linux comprometidos (reportado em diversos fóruns online)
- Plug-ins maliciosos do WordPress utilizados para diversas atividades maliciosas, incluindo permitir que os atacantes publicassem conteúdo em sites WordPress (reportado pela Wordfence).
- Imagens maliciosas do Docker que continham um script para download de malware de mineração de criptomoedas carregado na conta do Docker Hub (reportado pela Fortinet e Kromtech).
- Um pacote malicioso de digitação no repositório oficial do Python; o pacote continha um script malicioso que fazia download de malware utilizado para sequestrar endereços de mineração de moeda na área de transferência (reportado na Medium).
- Script comprometido no StatCounter que permitia aos atacantes injetar um script malicioso em sites que utilizam o StatCounter (reportado pela ESET).
- Múltiplos incidentes de backdoor em módulos npm (The npm Blog, Medium) que, se explorados, poderiam resultar em situações como, por exemplo, um atacante poder inserir e executar código arbitrário num servidor em execução.

Estes incidentes demonstram a forma como cadeias de fornecimento comprometidas podem ampliar de forma considerável uma superfície de ataque. Se não estiverem protegidos, os objetos na cloud podem constituir vetores de entrada inesperados. Por exemplo, o incidente Docker Hub envolveu uma conta maliciosa que carregava imagens do Docker contendo um backdoor de mineração de moedas oculto. As imagens do Docker estiveram alojadas no Docker Hub durante quase um ano e o seu download foi feito milhões de vezes, sendo utilizadas por administradores e utilizadores desprevenidos.

Os riscos da cadeia de fornecimento estendem-se ao código na cloud, open source, bibliotecas da Web, containers e outros objetos na cloud. Estes riscos, juntamente com o elevado grau de variabilidade dos incidentes de comprometimento da cadeia de fornecimento de software e hardware que vieram à luz, tornam os ataques de cadeia de fornecimento numa ampla categoria de ameaça. Embora não exista uma solução única para todo o espetro deste tipo de ataques, as organizações devem promover a proteção preventiva e deteção pós-falha de ataques da cadeia de fornecimento de fornecedores de hardware e software comprometidos, fornecedores e aquisições, fornecedores de software open source, bem como de fornecedores de infraestruturas e serviços cloud.

Investigação de ciberincidentes com a DART

A Equipa de Deteção e Resposta (DART) da Microsoft é uma equipa global de especialistas em cibersegurança e resposta a incidentes que ajuda as organizações na deteção, investigação e resposta a incidentes de cibersegurança. Esta secção destaca alguns dos casos de clientes que a DART processou no último ano, ilustrando as tendências comuns dos ataques e a forma como a Microsoft e os clientes os conseguiram impedir.

ORGANIZAÇÃO DE SERVIÇOS PROFISSIONAIS ENFRENTOU ATAQUE COORDENADO DE CAPTAÇÃO DE DADOS PATROCINADO POR UM ESTADO

Uma organização de serviços profissionais foi afetada por uma sofisticada ameaça persistente avançada (APT), patrocinada por um estado, que obteve acesso a credenciais privilegiadas da organização. Os atacantes obtiveram acesso à rede utilizando um ataque de pulverização de palavras-passe, no qual usaram um pequeno número de palavras-passe inseguras ou utilizadas habitualmente (como "p@ssword" ou "123456") para visar um grande número de contas de utilizador e obter credenciais administrativas do Office 365. (Os ataques de pulverização de palavras-passe são utilizados para evitar a deteção, limitando o número de tentativas de início de sessão em cada conta.) Após se infiltrar na rede, a APT executou a captação elaborada e automatizada de dados das caixas de correio dos colaboradores. Apesar de múltiplas tentativas de o expulsar, o adversário permaneceu na rede durante mais de 200 dias. Como parte do ataque, o adversário alavancou o software da cadeia de fornecimento da organização e automatizou a captação de dados.

Como suspeitava de uma violação dos dados dos seus clientes, a organização envolveu a equipa DART para investigar e ajudar a evitar mais danos. A DART identificou as pesquisas alvo de caixas de correio do Office 365, as contas comprometidas e os canais de comando e controlo do atacante. As principais lições deste incidente para o cliente foram a implementação de controlos para proteger os serviços cloud contra atacantes e ameaças baseadas em identidade.
A organização adotou a autenticação multifator (MFA), políticas de acesso condicional para determinadas aplicações na cloud e o registo do Office 365. Para se proteger ainda melhor contra ameaças semelhantes no futuro, a organização poderá também adotar uma solução de deteção e resposta a ameaças de endpoint (EDR) para detetar atacantes que possam estar a tentar explorar a sua rede. Além disso, recomendamos que a organização nomeie um corpo de gestão da cloud ou uma equipa global de identidade que fique encarregue de gerir e impor políticas adequadas de autenticação de utilizador, para que possa supervisionar o seu posicionamento de segurança e mitigar os riscos de forma mais eficaz.

SECÇÃO III

O phishing ainda prevalece

Em 2018, os analistas de ameaças da Microsoft viram evidências de que os atacantes continuam a utilizar o phishing como um método de ataque preferencial. O phishing promete continuar a ser um problema no futuro previsível, porque envolve decisões humanas e o julgamento em face de esforços persistentes por parte dos cibercriminosos para fazer as vítimas caírem nas suas artimanhas.

As taxas de phishing ainda continuam a crescer

Percentagem do total de e-mails recebidos que são e-mails de phishing

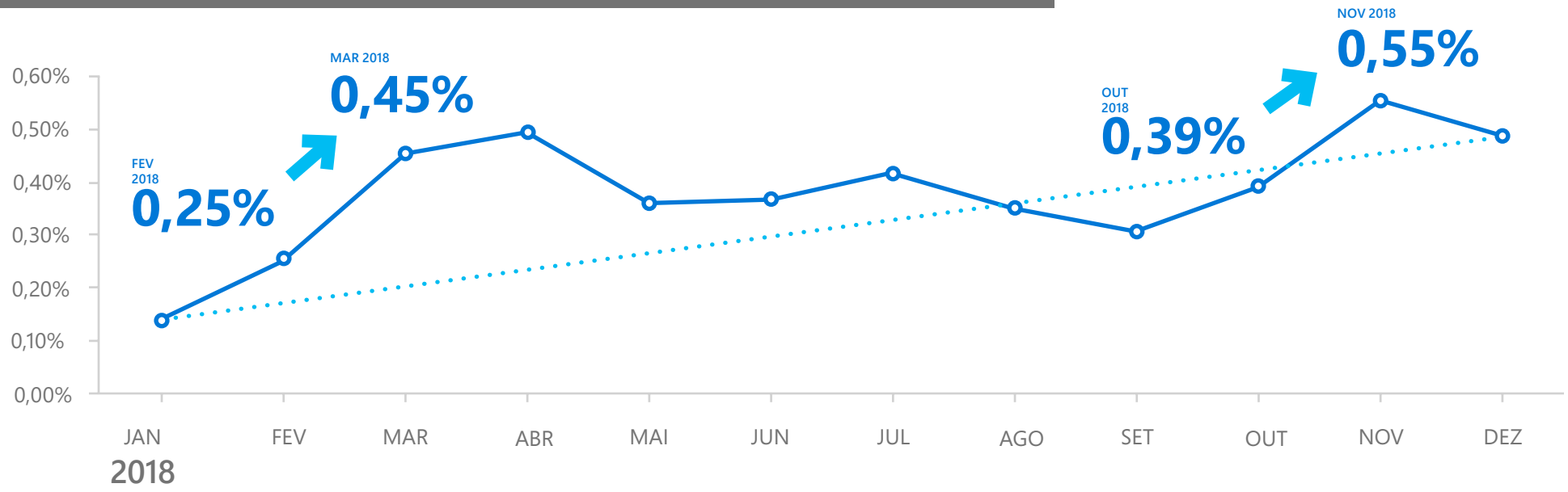


FIGURA 8.

E-mails de phishing em 2018

O PHISHING CONTINUA A SER UM VETOR DE ATAQUE PREFERENCIAL EM 2018

A Microsoft analisa mensalmente mais de 470.000 milhões de mensagens de e-mail no Office 365, procurando phishing e malware, o que fornece aos analistas insights consideráveis sobre as tendências e técnicas dos atacantes. A parte dos e-mails recebidos que eram mensagens de phishing aumentou 250% entre janeiro e dezembro de 2018. O phishing continua a ser um dos principais vetores de ataque utilizados para entregar payloads maliciosos de dia zero aos utilizadores, e a Microsoft continuou a reforçar-se contra estes ataques com recursos adicionais de proteção, deteção, investigação e resposta ao phishing para ajudar a proteger os utilizadores.

Evolução dos métodos de ataque de phishing

Como as ferramentas e técnicas utilizadas para proteger as pessoas do phishing se tornam mais sofisticadas, os atacantes são forçados a adaptar-se. Os ataques de phishing tornaram-se cada vez mais polimórficos, o que significa que os atacantes não utilizam um único URL, domínio ou endereço IP para enviar os e-mails. Usam no entanto uma infraestrutura variada com múltiplos pontos de ataque. A natureza dos ataques também evoluiu, com modernas campanhas de phishing que vão desde ataques de curta duração que estão ativos durante apenas alguns minutos até campanhas de alto volume, muito mais longas. Outro tipo de ataques são os variantes de série, em que os atacantes enviam um pequeno volume de correio em vários dias sucessivos.

Além disso, a Microsoft observou uma tendência para os atacantes utilizarem infraestruturas alojadas e outras infraestruturas de cloud pública, o que dificulta a deteção, ocultando-se entre sites e recursos legítimos. Por exemplo, os atacantes utilizam cada vez mais sites e serviços populares de colaboração e partilha de documentos para distribuir payloads maliciosos e formulários de início de sessão falsos, utilizados para roubar credenciais de utilizador. Também ocorreu um aumento da utilização de contas comprometidas para distribuir e-mails maliciosos, dentro e fora de uma organização.

As campanhas de phishing variam entre direcionadas e abrangentes

Tal como no caso da distribuição de malware em geral, as campanhas de phishing variam entre ataques direcionados e ataques genéricos de base ampla. Embora os ataques altamente sofisticados produzam maiores ganhos monetários por conta comprometida pelo phishing, os ataques mais genéricos geram menos dinheiro por conta comprometida, mas visam um conjunto mais amplo de utilizadores.

Um exemplo de uma campanha sofisticada e direcionada é o Ursnif, no qual os atacantes localizam o nome de ficheiro do documento de modo a ser específico de uma organização familiar ou setorial do alvo. Tais ataques são bastante diferentes das campanhas de base ampla, parecendo ser mais legítimos e fiáveis.

Em 2018, algumas das campanhas de base ampla estavam relacionadas com o compromisso de e-mails empresariais (BEC) e com a representação de marcas, domínios ou utilizadores conhecidos dentro das organizações alvo e com campanhas de falsificação sofisticadas. A representação de domínios é uma tática de ataque comum utilizada para fazer as organizações crer que o e-mail é fidedigno e deve ser aberto.

A atração do phishing surge de diversas formas

Os investigadores da Microsoft descobriram que são utilizados muitos tipos diferentes de iscos ou payloads de phishing em campanhas, incluindo:

- **Falsificação de domínios** (o domínio da mensagem de e-mail corresponde exatamente ao nome do domínio original)
- **Representação de domínios** (o domínio da mensagem de e-mail é semelhante ao nome do domínio original)[2]
- **Representação de utilizadores** (a mensagem de e-mail parece vir de alguém em quem o utilizador confia)
- **Iscos de texto** (a mensagem de texto parece vir de uma fonte legítima, tal como um banco, departamento governamental ou outra empresa, de modo a transmitir legitimidade às suas reivindicações, e geralmente pede à vítima que forneça informações sensíveis tais como nomes de utilizador, palavras-passe ou dados financeiros sensíveis)
- **Ligações de phishing de credenciais** (a mensagem de e-mail contém uma ligação para uma página que se assemelha à página de início de sessão de um site legítimo, para que os utilizadores insiram as suas credenciais de início de sessão)
- **Anexos de phishing** (a mensagem de e-mail contém um ficheiro malicioso em anexo que o remetente convida a vítima a abrir)
- **Ligações para localizações falsas de armazenamento na cloud** (a mensagem de e-mail parece vir de uma fonte legítima e solicita ao utilizador que dê permissão e/ou insira informações pessoais, tais como credenciais, em troca do acesso a uma localização falsa de armazenamento na cloud)

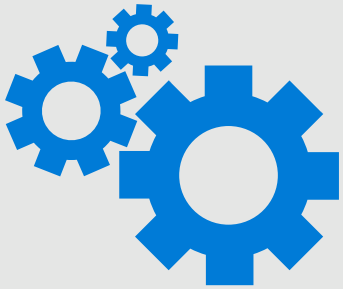
A variedade dos iscos que podem potencialmente ser utilizados pelos atacantes aumenta a complexidade das ameaças de phishing com as quais as organizações têm de lidar.

NOTAS DE RODAPÉ

[2] A representação de domínios pode assemelhar-se à falsificação de domínios (correspondência exata com o nome do domínio original) no caso excecional em que o domínio é apresentado no nome de apresentação do e-mail.

Investigação de ciberincidentes com a DART

GRANDE ORGANIZAÇÃO INDUSTRIAL ATINGIDA POR INCIDENTES DE PHISHING DIRECIONADO



Uma organização industrial enfrentou uma campanha de phishing em várias fases durante um período de alguns meses. Esta abordagem é frequente. Durante a primeira fase, o atacante realizará o reconhecimento; na segunda fase, visará ativos de valor elevado.
A primeira fase desta campanha aproveitou um esquema de phishing bem conhecido, baseado numa ligação para uma página da Web incorporada num e-mail enviado para um pequeno grupo alvo dentro da organização. O e-mail alegava que o alvo tinha um documento eletrónico importante a aguardar revisão, e que tudo o que o destinatário tinha de fazer era autenticar-se com as suas credenciais de domínio para obter acesso. A falsa página de destino configurada para o alvo rever o alegado "documento importante" recolhia na verdade as credenciais, permitindo ao atacante obter acesso a contas do Office 365 a partir de qualquer lugar. A segunda fase da campanha de phishing visava o envio de e-mails de phishing semelhantes a ativos de elevado valor dentro da organização industrial alvo, na esperança de obter acesso a dados mais valiosos. A Microsoft envolveu-se com este cliente durante a segunda fase da campanha de phishing. As principais lições deste incidente para o cliente foram: o phishing continua a ser um dos métodos de ataque mais eficazes e os utilizadores ainda constituem o elo mais fraco. A formação dos utilizadores para que sejam cautelosos com os esquemas de phishing, a implementação de ferramentas para identificar os atacantes e agir e a correção regular dos sistemas são elementos importantes; se a organização descurar qualquer um deles, poderá ficar vulnerável.

Neste caso, a preocupação mais importante do cliente foi a necessidade imediata de bloquear o acesso às contas comprometidas. Em parceria com as equipas de Identidade do Azure e do Office 365, a DART concebeu um plano para erradicar o atacante da rede e monitorizar todo o tráfego para o canal de comando e controlo, utilizando a recém-implementada solução do Microsoft Azure Log Analytics. A equipa conseguiu ajudar a resolver a situação em apenas três horas.
O acesso do atacante foi bloqueado e a organização pôde voltar a sua atenção para a avaliação e recuperação de danos. A DART utilizou as ferramentas do Azure Log Analytics para detetar o comportamento do atacante, o que ajudou a descobrir muitos desafios de configuração da organização. Por exemplo, a DART identificou falhas na correção de servidores críticos, detetou computadores na rede que comunicavam na Internet com hosts perigosos conhecidos e encontrou ainda diversos servidores importantes sem proteção contra malware.

SECÇÃO IV

Malware em todo o mundo

O malware representa riscos para as organizações e indivíduos sob a forma de limitação da usabilidade, perdas de dados, roubo de propriedade intelectual, perdas monetárias e perturbações emocionais, podendo até colocar vidas humanas em risco. A Microsoft utiliza um amplo conjunto de ferramentas e técnicas para identificar, bloquear e erradicar infeções de malware, onde quer que sejam encontradas.

Em 2017, as taxas de ocorrência de malware variaram entre cerca de 5% e mais de 7%. No início de 2018, subiram antes de diminuírem durante a maior parte do ano, para ligeiramente acima dos 4%. Alguns motivos potenciais para a redução global das taxas de ocorrência de malware em 2018 prendem-se com o crescimento da adoção do Windows 10 e com o aumento da utilização do Windows Defender para proteção. A taxa de ocorrência é a percentagem de computadores que executam o Antivírus do Windows Defender que reportou encontrar malware ao longo do mês, incluindo as tentativas de infeção que o Defender bloqueou.

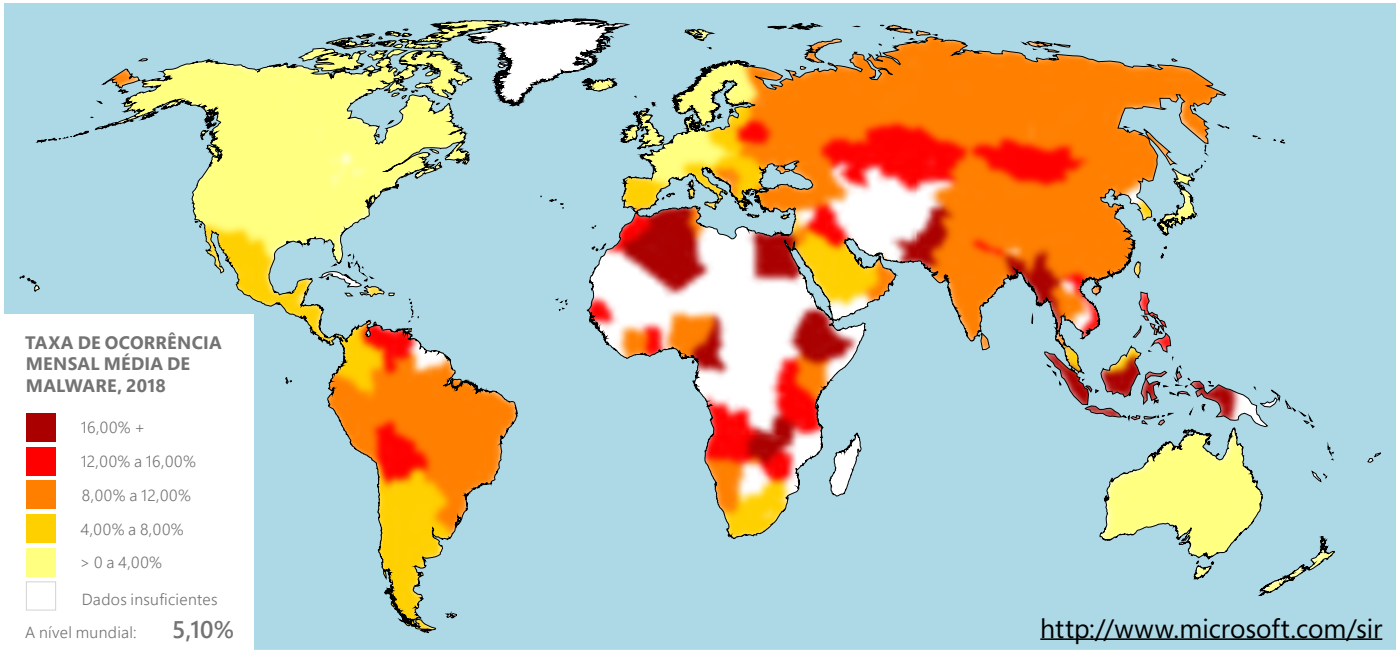


FIGURA 9.

Taxas de ocorrência mensal média de malware a nível mundial, por país/região, em 2018

Os cinco países com as maiores taxas de ocorrência de malware durante o período de janeiro-dezembro de 2018 foram a Etiópia (taxa de ocorrência mensal média de 26,33%), Paquistão (18,94), Territórios Palestinianos (17,50), Bangladesh (16,95) e Indonésia (16,59), que tiveram uma taxa de ocorrência mensal média de aproximadamente 16,59% ou superior durante o período. As taxas de infeção tendem a correlacionar-se fortemente com os fatores de desenvolvimento humano e a prontidão tecnológica da sociedade. Todos os locais com as maiores taxas de ocorrência em 2018 estavam classificados nos 40% inferiores entre os países e regiões do Índice de Tecnologias de Informação e Comunicação (ICT) de 2017, publicado pela União Internacional de Telecomunicações das Nações Unidas (UIT).

Os cinco países com as menores taxas de ocorrência de malware durante o mesmo período foram a Irlanda (1,26%), Japão (1,51), Finlândia (1,74), Noruega (1,79) e Holanda (1,82), todos com uma taxa de ocorrência mensal média de 1,82% ou inferior durante o período. Estes locais tendem a ter infraestruturas de cibersegurança maduras e programas bem estabelecidos para proteger as infraestruturas críticas e comunicar com os cidadãos sobre segurança básica.

TAXAS DE OCORRÊNCIA MENSAL MÉDIA DOS PAÍSES MAIS AFETADOS PELO MALWARE

Etiópia: 26,33%

Paquistão: 18,94%

Territórios Palestinianos: 17,50%

Investigação de ciberincidentes com a DART

MÚLTIPLAS INSTITUIÇÕES FINANCEIRAS ENFRENTARAM ATAQUES PATROCINADOS POR ESTADOS QUE INTERROMPERAM AS OPERAÇÕES

Num dos incidentes mais destrutivos que a DART já viu, diversas instituições financeiras foram alvo de um APT patrocinado por um estado (um grupo diferente daquele que visou a organização de serviços profissionais referida anteriormente), que decorreu de forma semelhante.

Este APT obteve acesso administrativo após infetar uma máquina inicial com um implante backdoor ofuscado altamente direcionado, possivelmente entregue através de um e-mail de spear-phishing. Posteriormente, o APT executou múltiplas transações fraudulentas, transferindo valores elevados para contas bancárias estrangeiras. Nalguns casos, o atacante permaneceu sem ser detetado durante mais de 100 dias. Depois que o atacante perceber que tinha sido detetado, implementou rapidamente um ataque pré-preparado, distribuindo malware destrutivo a mais de metade dos sistemas do ambiente; as operações destes clientes foram suspensas durante vários dias.

Extraímos algumas lições chave para o cliente a partir destes incidentes. A primeira foi que a gestão do ciclo de vida do software é especialmente importante, o que inclui garantir que os sistemas sejam atualizados (sistemas operativos e segurança), corrigidos e auditados regularmente. Num dos casos, o ambiente de sistema Linux de uma organização que tinha um número excecionalmente grande de workloads em execução era totalmente não gerido, incorrendo num risco extraordinariamente elevado de ataque. A segunda lição foi que é importante manter cópias de segurança dos dados do sistema numa localização offline, para o caso de perda dos dados primários. Outra lição foi que as soluções antivírus tradicionais poderão não bastar se precisar de conhecer a atividade do adversário.

O regresso ao modo de funcionamento normal era a prioridade mais elevada destas organizações. A DART ajudou a restaurar os serviços, investigando primeiro o impacto e, em seguida, executando as ações de mitigação necessárias, tais como a remoção do malware dos sistemas afetados e a sua reposição num bom estado de funcionamento. A equipa também treinou os clientes sobre como utilizar as ferramentas de investigação de ameaças da Microsoft, incluindo o EDR e outras, para que pudessem procurar comportamentos anómalos e atividades de atacantes nas suas redes. A DART enfatizou que a monitorização de endpoints é crítica na defesa contra ataques sofisticados e direcionados, que as soluções antivírus tradicionais poderão não conseguir detetar.

Orientação

Orientação

A promoção da resiliência organizacional e a redução significativa de riscos exigem uma abordagem de segurança que inclua a prevenção, deteção e resposta. Organizámos as seguintes práticas e controlos recomendados de segurança nessas categorias.

PREVENÇÃO:

Os controlos preventivos desempenham um papel fundamental numa estratégia global de defesa, uma vez que os investimentos certos poderão aumentar o custo dos ataques para os cibercriminosos e manter esses custos adicionais dos ataques ao longo do tempo (sem exigir que um analista especializado monitorize e interprete o resultado). Os investimentos em controlos preventivos deverão ser direcionados para as técnicas de menor custo, de modo a remover constantemente as técnicas de ataque mais baratas e eficazes.

Há quatro elementos a levar em consideração na prevenção:

1. **As boas práticas de segurança são fundamentais. Conforme observado em alguns dos ciberincidentes partilhados neste relatório, a ausência de boas práticas de segurança poderá minar as capacidades de segurança avançada, pelo que seguir estas sugestões poderá ajudar a mitigar os riscos:**

- Evite utilizar software gratuito e/ou pirateado desconhecido. Utilize sempre software de origens fidedignas.
- Reduza o risco de roubo de credenciais, incluindo a proteção de contas de administrador privilegiadas. Para saber como proceder, leia este artigo de blogue que descreve alguns princípios e ferramentas que a Microsoft utilizou para orientar e melhorar a sua própria postura de segurança, assim como alguns roteiros prescritivos para o ajudar a planear as suas próprias iniciativas.
- Aplique as referências de configuração segura fornecidas pelos fornecedores de software.
- Mantenha os computadores atualizados, aplicando rapidamente as atualizações mais recentes dos seus sistemas operativos e aplicações, e implemente imediatamente as atualizações críticas de segurança dos sistemas operativos, browsers e e-mail. Isole (ou retire) os computadores que não possam ser atualizados ou corrigidos.
- Implemente proteções avançadas de e-mail e browsers. Implemente um gateway de e-mail seguro que possua recursos avançados de proteção contra ameaças para se defender das variantes modernas de phishing.
- Ative as defesas contra malware e de rede dos hosts para obter respostas de bloqueio quase em tempo real da cloud (se disponíveis na sua solução).

2. **Implemente controlos de acesso. Tenha em consideração o seguinte:**

- Aplique o princípio de menor privilégio, que inclui a implementação da segmentação de rede, a remoção dos privilégios de administrador local dos utilizadores finais e o exercício de cautela ao conceder quaisquer permissões a aplicações em execução no computador.
- Limite o download de aplicações apenas às de origens fiáveis (lojas de aplicações oficiais).
- Implemente políticas seguras de integridade de código, incluindo a restrição das aplicações que os utilizadores podem executar. Se possível, adote uma solução de segurança que restrinja o código executado no core do sistema (kernel) e que possa bloquear os scripts não assinados e outras formas de código não fidedigno. Utilize a aprovação de aplicações.
- Para saber mais sobre os ataques a cadeias de fornecimento de software e como se proteger contra os mesmos, leia este artigo de blogue de investigadores da Microsoft.

3. **Faça cópias de segurança.**

- Crie cópias de segurança resistentes à destruição, dos seus sistemas e dados críticos.
- Utilize serviços de armazenamento na cloud para efetuar cópias de segurança automáticas online dos dados. Para os dados on-premises, efetue regularmente cópias de segurança dos dados importantes utilizando a regra 3-2-1. Mantenha três cópias de segurança dos seus dados, em dois tipos de armazenamento diferentes, e pelo menos uma cópia de segurança externa.

4. **Esteja atento e aja se suspeitar de algo.**

- Ensine os colaboradores a serem cautelosos com comunicações suspeitas que solicitem informações confidenciais e instrua-os sobre como responder, reportando-as de imediato à equipa de operações de segurança da organização. A formação também poderá ajudar a mitigar os ataques de engenharia social e spear-phishing.
- Tenha cuidado ao clicar em ligações da Web. Desenvolva hábitos seguros de navegação na Web e utilize soluções que forneçam avisos ou bloqueiem o acesso a sites não seguros, de modo a reduzir a probabilidade de encontrar sites associados à mineração de criptomoedas.
- Se um computador estiver excecionalmente lento, procure ficheiros suspeitos que se encontrem em execução e não hesite em enviar uma amostra ao fornecedor do sistema operativo. Pode submeter ficheiros à Microsoft para análise de malware em https://www.microsoft.com/wdsi/filesubmission.

DETEÇÃO E RESPOSTA:

A deteção e resposta aumentam a resiliência, limitando o tempo em que um atacante tem acesso aos seus recursos. Isso permite diminuir o ROI dos atacantes, aumentando o custo dos ataques (os atacantes têm de repetir ou modificar as suas operações) e diminuindo o retorno (limitando a probabilidade de atingirem os seus objetivos).

A mesma tecnologia de cloud que permite que as empresas respondam melhor às necessidades do mercado também pode ajudar a melhorar a resposta das operações de segurança aos atacantes.

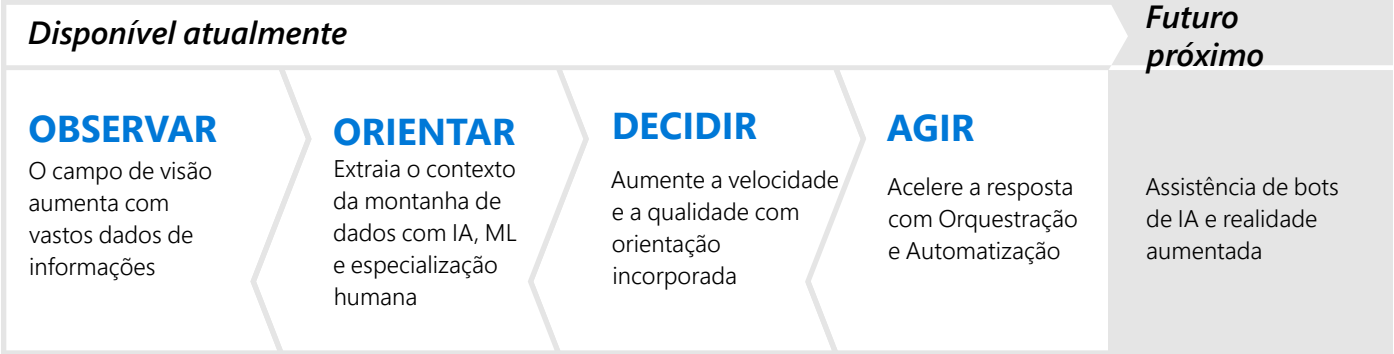


FIGURA 10.

Trajetória evolutiva dos SOCs

Ao observarmos a trajetória de evolução dos Centros de Operações de Segurança (SOCs), verificamos que a tecnologia faz aumentar de forma contínua a velocidade e a qualidade das decisões e ações dos SOC. Muitas destas inovações podem ser mapeadas para cada etapa do "ciclo" Observar - Orientar - Decidir - Agir (OODA), documentado pelo coronel da Força Aérea dos EUA, John Boyd.[3]

OBSERVAR – Os SOCs podem explorar a vastidão de informações de segurança disponíveis (da Microsoft e de outras fontes), aumentando drasticamente o seu campo de visão dentro da organização e sobre o ambiente externo.

ORIENTAR – Conforme essas novas origens de dados vão sendo disponibilizadas aos já sobrecarregados SOCs, o machine learning (um subconjunto da inteligência artificial) torna-se numa ferramenta fundamental para raciocinar sobre esses conjuntos maciços de dados, identificando anomalias que valha a pena investigar. Os fornecedores de segurança (incluindo a Microsoft) adotaram tecnologia de machine learning para atribuir rapidamente prioridades aos eventos (ajudando a fundir esses eventos individuais em incidentes holísticos).

DECIDIR – Como o volume e a complexidade dos ataques podem sobrecarregar rapidamente um SOC, os analistas e o pessoal de resposta a incidentes têm de tomar muitas decisões e agir rapidamente em resposta aos alertas e deteções. A Microsoft e outros fornecedores possuem capacidades integradas de investigação automatizada, bem como orientações para ajudar os analistas a tomarem rapidamente as decisões certas (por exemplo, isolando os dispositivos potencialmente infetados ou comprometidos).
De momento a automatização está focada em resolver rapidamente os incidentes de baixa prioridade, para que possam ser aplicadas capacidades especializadas a problemas mais complexos.

AGIR – A resposta exige uma execução rápida e precisa em muitas tecnologias e plataformas, o que é permitido pelas tecnologias de orquestração de segurança e automatização de respostas. A Microsoft e muitas outras entidades continuam a investir nessas tecnologias, incluindo a deteção de ameaças modernas e soluções automatizadas de resposta.

NOTAS DE RODAPÉ

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

Eis outras tendências aplicáveis a um SOC moderno:

- **Privilegiar a qualidade sobre a quantidade de feeds de alerta** – À medida que as organizações passam da gestão de "informação insuficiente" para a gestão de "demasiada informação", o tempo e a atenção dos analistas de SOC altamente especializados tornam-se cada vez mais valiosos. Isso origina uma maior necessidade 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 deteção pró-ativa, o SOC de informática empresarial da Microsoft mede a taxa de positivos verdadeiros nos feeds de alerta que exigem resposta dos analistas (exigindo atualmente uma taxa de positivos verdadeiros de 90% ou superior).

- Gravidade dos dados – A análise de grandes conjuntos de dados (incluindo dados de segurança) é difícil de realizar sem acesso aos dados brutos subjacentes. À medida que são disponibilizados mais dados de segurança, torna-se mais económico e prático executar a análise de segurança na cloud em vez de transferir esses dados para um sistema on-premises. Isso conduzirá provavelmente à evolução das arquiteturas de SIEM e SOC, que poderá incluir abordagens de SIEM híbridas ou a adoção de SIEM de cloud nativa como um serviço.

- **Contexto elevado** – Estes tipos de deteções são muito mais úteis devido à sua capacidade de correlacionar conjuntos de dados de forma mais eficaz. Embora as deteções tradicionais baseadas no tráfego de rede ainda forneçam algum valor de segurança, o tráfego de rede em bruto carece normalmente de contexto para diferenciar entre as atividades legítimas e as anómalas. Os SOCs estão a obter muito mais valor de deteções ricas em contexto, tais como:

  - **Soluções de Deteção e Resposta de Endpoint (EDR)** com um contexto profundo sobre as atividades do host
  - Deteções baseadas em identidade que incluem insights sobre os padrões normais de autenticação dos utilizadores (locais, horários, serviços acedidos, etc.) e que aplicam a análise comportamental

Essas deteções ricas em contexto são mais difíceis de iludir pelos adversários, pois têm que imitar uma operação muito mais complexa (em vez de alguns atributos técnicos do tráfego IP).

Outra lição que aprendemos com grandes falhas dos clientes foi a dificuldade de responder rapidamente aos incidentes quando os departamentos de informática são totalmente ou parcialmente externalizados. Recomendamos a revisão dos seus contratos de externalização de informática e dos contratos de nível de serviço (SLAs), bem como dos fornecedores da cadeia de fornecimento, de modo a garantir que sejam compatíveis com respostas de segurança rápidas. Para conhecer mais lições das nossas investigações de incidentes dos clientes, consulte o Guia de Referência de Resposta aos Incidentes (IRRG) em https://aka.ms/IRRG.

Origens de dados

Origens de dados

A Microsoft recolheu os dados incluídos no Relatório de Informações de Segurança no intuito de fornecer uma vasta gama de produtos e serviços Microsoft, conforme abordado na Declaração de Privacidade da Microsoft. Estes dados fornecem-nos informações valiosas sobre a segurança e funcionamento dos nossos produtos e serviços, assim como insights sobre o cenário global de ameaças de cibersegurança. Estes dados incluem a análise das seguintes fontes:[4]

- O **Centro de Segurança do Azure** é um serviço que ajuda as organizações a impedir, detetar e responder às ameaças, fornecendo maior visibilidade sobre a segurança dos workloads da cloud e utilizando análise de informações avançada e informações sobre ameaças para detetar ataques.

- O **Bing** é o motor de pesquisa e de decisão que executa milhares de milhões de verificações de páginas Web por ano para procurar conteúdos maliciosos. Quando são detetados tais conteúdos, o Bing avisa os utilizadores para ajudar a evitar infeções.

- O **Exchange Online** é o serviço de produtividade e e-mail alojado da Microsoft. Os serviços de antimalware e antispam do Exchange Online verificam milhares de milhões de mensagens por ano para identificar e bloquear spam e malware.

- A **Ferramenta de Remoção de Software Malicioso** (MSRT) é uma ferramenta gratuita concebida pela Microsoft para ajudar a identificar e a remover famílias de malware predominantes específicas dos computadores dos clientes. A MSRT é disponibilizada principalmente como uma atualização importante através do Windows Update, do Microsoft Update e das Atualizações Automáticas. Uma versão da ferramenta também está disponível no Centro de Transferências da Microsoft. A MSRT não constitui uma alternativa para uma solução atualizada de antivírus em tempo real.

- O **Analista de Segurança da Microsoft** é uma ferramenta de segurança de download gratuito que permite a verificação a pedido e ajuda a remover malware e outro software malicioso. O Analista de Segurança da Microsoft não é um produto de substituição para uma solução de antivírus atualizada, porque não oferece proteção em tempo real e não pode impedir que um computador seja infetado.

NOTAS DE RODAPÉ

[4]É importante destacar que estes dados estão sempre sujeitos a estritas normas de privacidade e conformidade antes de serem utilizados para fins de segurança.

- **Microsoft Security Essentials** é um produto de proteção em tempo real de download fácil, que oferece um antivírus básico e proteção antisspyware para o Windows Vista e o Windows 7.

- O **Microsoft System Center Endpoint Protection** (anteriormente conhecido como Forefront Client Security e Forefront Endpoint Protection) é um produto unificado que oferece proteção contra malware e software indesejado para computadores de secretária, portáteis e sistemas operativos de servidores empresariais. Utiliza o Mecanismo de Proteção de Malware e a base de dados de assinaturas antivírus da Microsoft para proporcionar proteção em tempo real, agendada e a pedido.

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

- A **Segurança do Windows** no Windows 10 fornece análise em tempo real e remoção de malware e software indesejado. Além disso, a versão mais recente do Windows aproveita dados contextuais avançados, tais como a configuração dos computadores, desempenho e estado dos dispositivos, bem como outras informações, para melhorar a segurança dos clientes. Ao mesmo tempo, capacitamos os clientes para que estejam melhor informados sobre a sua privacidade no Windows 10. Leia este artigo de blogue para saber mais sobre algumas das formas como a Microsoft faz este trabalho.

- A **Proteção Avançada contra Ameaças do Windows Defender** é um serviço incorporado na Atualização de Aniversário do Windows 10 e versões posteriores que permite que os clientes empresariais detetem, investiguem e remedeiem ameaças avançadas persistentes e falhas de segurança nas suas redes.

- O **Windows Defender Offline** é uma ferramenta para download que pode ser utilizada para criar um CD, DVD ou uma pen USB de arranque para verificar a existência de malware e outras ameaças num computador. Não oferece proteção em tempo real e não constitui uma alternativa a uma solução antimalware atualizada.

- O **Windows Defender SmartScreen**, uma funcionalidade do Microsoft Edge e do Internet Explorer, oferece proteção aos utilizadores contra sites de phishing e sites que alojam malware. A Microsoft mantém uma base de dados de sites de phishing e malware reportados por utilizadores do Microsoft Edge, do Internet Explorer e de outros produtos e serviços da Microsoft. Quando um utilizador tenta visitar um site na base de dados com o filtro ativado, o browser apresenta um aviso e bloqueia a navegação para a página.