Defenda-se contra as maiores ameaças dos dias de hoje

Relatório de ameaças de fevereiro de 2019

CISCO

Conteúdo

Olhe para trás, siga em frente

Quando se trata do cenário de ameaças, é importante olhar pelo espelho retrovisor de vez em quando.

Assim como ao dirigir, você precisa poder não só enxergar o que está atrás de você, mas também identificar rapidamente o que está prestes a acontecer.

Essa é a ideia deste relatório de ameaças. Selecionamos cinco casos importantes do ano passado, não apenas porque foram grandes eventos, mas porque achamos que essas ameaças, ou ameaças parecidas, poderiam muito bem aparecer em um futuro próximo.

Veja as ameaças modulares como Emotet e VPNFilter, por exemplo. São as ameaças que podem oferecer uma variedade de ataques e ameaças sob demanda, dependendo do dispositivo infectado ou do objetivo do invasor. Vimos muitas dessas ameaças modulares recentemente e não seria surpreendente se víssemos mais no futuro.

O e-mail continua sendo o método de entrada preferido dos invasores, com as ameaças de cryptomining e Emotet utilizando-o para se disseminarem. Também é muito provável que outras ameaças, como perfil MDM não autorizado, também sejam usadas. Isso mostra como é fundamental ficar atento ao que chega à caixa de entrada.

Modus operandi

A geração de receita continua a ser a principal motivação para os invasores: o malware persegue o dinheiro. As ameaças de cryptomining, por exemplo, estão muito voltadas para esse objetivo. Enquanto isso, o Emotet se transformou em uma rede de distribuição de ameaças, aproveitando uma série de opções para ganhar dinheiro.

A extração de dados também já esteve em destaque. Ela foi o principal motor de muitas ameaças recentes, como VPNFilter, que parece ter sido criada para roubar informações. O Emotet, além de roubar credenciais de rede para ajudá-lo a se espalhar, também já espalhou Trickbot, outro conhecido Cavalo de Troia para roubo de informações bancárias.

Escolhemos cinco casos para mostrar por que essas ameaças, ou outras similares, podem aparecer novamente.

Por fim, algumas ameaças apenas querem provocar tumulto, como é o caso do Olympic Destroyer. Observamos uma série de ameaças como essa no ano passado, mas nenhuma mereceu tanto destaque nas manchetes como um ataque cujo único propósito parece ter sido atrapalhar as Olimpíadas de Inverno.

Ao olharmos novamente para algumas das ameaças mais impactantes de 2018, é importante saber o que as tornou tão famosas. Muitas delas podem ser passado agora, mas será que elas realmente ficaram para trás ou só estão tomando novo fôlego para burlar seus recursos de proteção e jogar por terra sua estratégia de segurança?

Quando se trata do cenário de ameaças, é importante olhar pelo espelho retrovisor de vez em quando. Assim como ao dirigir, você precisa poder não só enxergar o que está atrás de você, mas também identificar rapidamente o que está prestes a acontecer.

Tipos de ataque e proteção

Sempre é aconselhável ter uma abordagem de segurança em camadas. Incluímos ícones no final de cada caso para indicar os principais vetores de ameaças usados (ou suspeitos de serem usados) e as ferramentas que podem ajudar a protegê-los em cada caso. Abaixo, decodificamos os ícones e discutimos as vantagens de implantar os vários tipos de proteção como parte de uma arquitetura de segurança integrada.

A tecnologia de detecção e proteção contra malware avançado (como a do Cisco Advanced Malware Protection, ou AMP) consegue rastrear arquivos desconhecidos, bloquear os arquivos mal-intencionados mais conhecidos e impedir a execução do malware nos endpoints e dispositivos de rede.

Recursos de segurança de rede, como o Cisco Next-Generation Firewall (NGFW) e o Next-Generation Intrusion Prevention System (NGIPS), podem detectar arquivos mal-intencionados que tentam entrar pela Internet ou se mover dentro da rede. A visibilidade de rede e as plataformas de análise de segurança, como o Cisco Stealthwatch, conseguem detectar anomalias internas da rede que podem significar que existe malware ativandoo a carga útil. Por fim, a segmentação pode impedir a movimentação lateral de ameaças em uma rede e conter a propagação do ataque.

Fazer a varredura da Web em um Secure Web Gateway (SWG) ou **Secure Internet Gateway (SIG)**, como o Cisco Umbrella, pode impedir que os usuários se conectem a domínios, IPs e URLs mal-intencionados, independentemente de estarem ou não na rede corporativa. Isso pode evitar que as pessoas inadvertidamente deixem o malware acessar a rede e ajudar a impedir que ele entre através da conexão a um servidor de comando e controle (C2).

A **tecnologia de segurança de e-mail** (como a do Cisco Email Security), implantada no local ou na nuvem, bloqueia e-mails mal-intencionados enviados pelos agentes de ameaças como parte de suas campanhas. Isso reduz a quantidade total de spam, remove spam mal-intencionado e verifica todos os componentes de um e-mail (por exemplo, remetente, assunto, anexos e URLs incorporadas) para encontrar as mensagens contendo ameaças. Esses recursos são importantes, pois o e-mail ainda é o principal vetor usado pelos agentes de ameaças para iniciar ataques.

A **tecnologia de detecção e proteção contra malware avançado**, como a do Cisco AMP para Endpoints, impede a execução do malware no endpoint. Também ajuda a isolar, investigar e corrigir endpoints infectados nos 1% dos ataques que passam até mesmo pelas defesas mais robustas.

Dinâmica do Emotet: de bancos à distribuição

O Emotet estava em segundo plano há anos. Essa tática foi muito útil.

Muitas vezes no contexto de ameaças, as histórias que viram manchetes nas primeiras páginas são de pessoas que inovam: uma vulnerabilidade é descoberta, afetando uma grande quantidade de dispositivos, ou quando ocorre um ataque contra uma grande empresa.

No entanto, nem sempre as ameaças predominantes são as que ficam em evidência. Elas podem se basear em métodos testados, em vez de nas melhores e mais recentes técnicas. E isso chega às mãos dos invasores. Algo que passa despercebido poder crescer, e nem sempre isso acontece com algo que chama a atenção.

O Emotet é um exemplo perfeito. Com as manchetes tomadas por discussões sobre ameaças como WannaCry e NotPetya, o Emotet ficou em segundo plano durante anos. Essa tática deu certo, pois ele se tornou uma das mais bem-sucedidas ameaças modernas.

O sucesso do Emotet está no modo como ele evolui. No início apenas um " humilde" um Cavalo de Troia em sistemas bancários, os agentes se mobilizaram rapidamente para transformar a ameaça em uma plataforma modular, capaz de realizar uma série de ataques diferentes. No cenário atual, outras linhas de ameaças que já foram vistas como concorrentes, agora o utilizam para espalhar seus produtos. E à medida que o cenário de ameaças muda novamente, o Emotet parece estar chamando a atenção de todos.

De modesto para modular

Quando o Emotet apareceu, ele era um dos vários Cavalos de Troia bancários. A ameaça foi disseminada por meio de campanhas de spam, geralmente usando e-mails sobre faturas ou boletos referentes a algum pagamento. Ele era frequentemente anexado como documentos do Office habilitados para macro, arquivos JavaScript ou incluídos como um link mal-intencionado. As técnicas de distribuição variavam, embora muitas das campanhas tinham como alvo bancos em regiões específicas, especialmente, países de língua alemã na Europa e nos EUA.

A princípio, a ameaça estava concentrada principalmente em roubar informações bancárias: nomes de usuários, senhas,

E-mail: o vetor mais comum de ameaças

Um recurso presente na maioria das principais ameaças de hoje é o e-mail. Ele continua sendo o vetor de infecção mais comum para os agentes de ameaças distribuírem seus produtos e, provavelmente, vai continuar a ser no futuro próximo.

Veja o Emotet, por exemplo. Toda semana, os invasores por trás dessa ameaça lança novas campanhas de phishing.

O mesmo se aplica à criptografia mal-intencionada, em que campanhas de spam constantantemente enganam os usuários para que baixem malware nos computadores.

Em termos de ameaças de gerenciamento de dispositivo móvel (MDM), parece plausível a teoria de que os ataques tenham começado por e-mail de engenharia social.

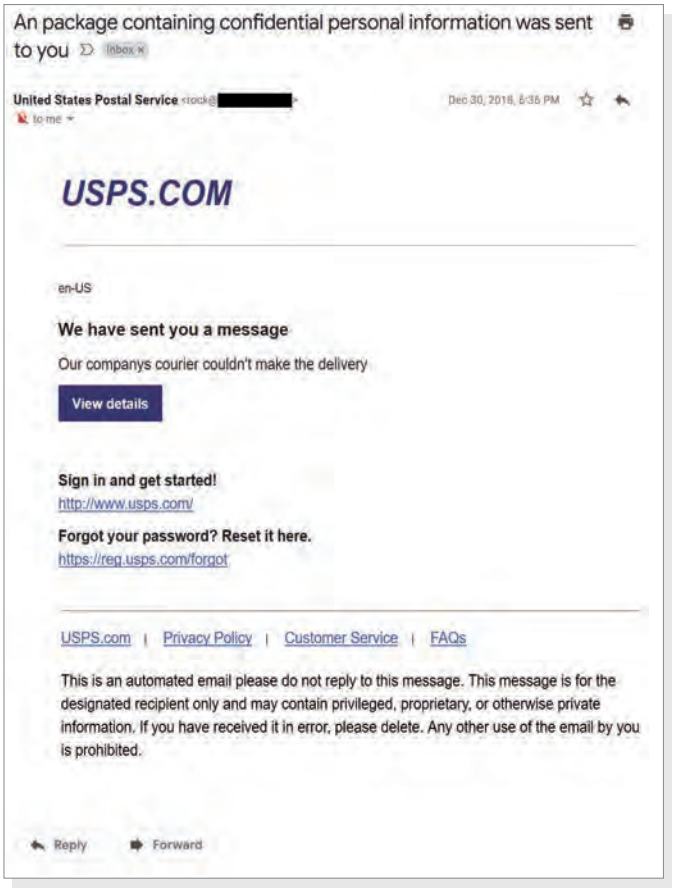
(continuação)

endereços de e-mail e outros detalhes financeiros. Com o tempo, o Emotet começou a se espalhar para um público mais geral. Uma nova versão da ameaça originou a configuração modular que vemos hoje, contendo diferentes ferramentas para diferentes funções. Alguns módulos roubam credenciais de e-mail, porém outros se concentram em nomes de usuário e senhas armazenadas no navegador. Alguns fornecem recursos de negação de serviço distribuído (DDoS), enquanto outros podem espalhar ransomware.

E não é de estranhar também, devido à aparência convincente de muitos e-mails de phishing, especialmente se visualizados no celular. Para um usuário ocupado, a urgência transmitida pelo e-mail podem levar ao risco de o destinatário agir imediatamente, ignorando os sinais reveladores de uma ameaça à espreita.

Não é de admirar que os invasores continuem a usar o e-mail para propagar o malware.

Figura 1 Um exemplo de e-mail de spam do Emotet



Cadê o dinheiro?

O objetivo principal do Emotet é descobrir uma forma de rentabilizar o computador, que é por onde entram os módulos. Parece que os módulos instalados em um dispositivo específico dependem de como eles podem rentabilizar melhor o dispositivo infectado. Considere os seguintes cenários:

- O histórico do navegador do computador mostra frequentes visitas a sites bancários? Implante módulos de bancos para roubar credenciais e transferir o dinheiro.
- O dispositivo é um notebook top de linha e é provável que indique que o alvo tem dinheiro? Implante módulos de distribuição de malware e instale o software de ransomware ou cryptomining.
- A máquina é um servidor em uma rede de grande largura de banda? Instale módulos para distribuição no e-mail e na rede e dissemine ainda mais o Emotet.

Honra entre ladrões

O que realmente diferencia o Emotet de muitas outras ameaças no atual cenário não é apenas seu alcance e modularidade, mas o fato de que os agentes parecem estar vendendo a ameaça como um canal de distribuição para outros grupos de ataque.

Por exemplo, observamos situações onde o Emotet infecta um computador apenas para soltar Trickbot no sistema como a carga útil. Neste caso aparentemente contraditório, o Emotet, com reputação de um Cavalo de Troia em sistemas bancários, na realidade está soltando outro Cavalo de Troia, em vez de utilizar os próprios módulos de roubo de informações. O mais interessante é que o Trickbot, depois de ser lançado pelo Emotet, às vezes, também distribui o ransomware Ryuuku.

Por mais estranho que isso pareça, a impressão que dá é de que a cooperação entre grupos ocorre simplesmente porque trabalhar juntos aumenta o lucro. Se o Emotet não puder utilizar um dispositivo para se espalhar mais, o Trickbot poderá roubar os registros bancários. Caso nenhum registro bancário seja encontrado, o Ryuk pode criptografar o dispositivo e exigir um resgate. Obviamente, ninguém sabe até quando essa aliança vai durar.

O que esperar do futuro

Claro que uma ameaça que cresce raramente fica sob o radar. Nos últimos dois meses de 2018, o setor de segurança começou a prestar atenção no tamanho do Emotet. O que o fez ficar em evidência é que os distribuidores de e-mail de spam parecem

Os agentes por trás do Emotet agora parecem estar vendendo a ameaça como um canal de distribuição para outros grupos de ataque.

ter mudado de cargas úteis de cryptomining para a distribuição do Emotet e dos Cavalos de Troia de acesso remoto (RATs). O impacto está sendo percebido. Na verdade, alguns ataques do Emotet deram um prejuízo de até US$ 1 milhão para serem resolvidos, de acordo com US CERT.

É pouco provável que o Emotet desapareça e pode muito bem dominar o cenário de ameaças do futuro. Se o passado for um sinalizador do futuro, haverá menos incidência do Emotet, apenas para ser substituído por outro agente dominante no cenário de ameaças.

Para uma visão mais detalhada sobre esse assunto:

https://blog.talosintelligence.com/2019/01/Return-of-emotet.html

https://www.US-CERT.gov/ncas/Alerts/TA18-201A

https://Duo.com/Decipher/The-Unholy-Alliance-of-emotet-trickbot-and-the-Ryuk-ransomware

https://blog.talosintelligence.com/2018/12/cryptocurrency-Future-2018.html

Manobras de IoT: o caso do VPNFilter

Imagem: Talos

O VPNFilter permanece como um precursor do que inevitavelmente ainda está por vir.

Na última década, houve um grande número ameaças relacionadas à Internet das Coisas (IoT). Houve o botnet da Mirai, que infectou câmeras IP e roteadores para realizar ataques de DDoS. E quem consegue esquecer os hacks de monitoramento de bebês, onde os pais entram no berçário e ouvem os hackers conversando com seus filhos depois de invadirem o dispositivo?

Gostem ou não, seja nos assistentes inteligentes ou em dispositivos hospitalares conectados à Internet, a IoT entrou de vez em nossas casas e empresas. Infelizmente, em muitos casos as práticas de segurança adequadas têm sido negligenciadas nesse processo. Como resultado, já vimos esses dispositivos sendo alvo de agentes mal-intencionados.

No entanto, nada foi tão prejudicial quanto o VPNFilter. Essa ameaça tinha como alvo uma ampla gama de roteadores de diversos fabricantes, provavelmente para atacar vulnerabilidades não corrigidas e prejudicá-los. Um de seus propósitos parecia ser a extração de dados confidenciais das redes comprometidas, mas o VPNFilter também continha um sistema modular que lhe permitia fazer muito mais do que isso, o que o tornava bastante preocupante.

Para se ter uma ideia, a ameaça infectou, pelo menos, meio milhão de dispositivos em 54 países. Felizmente, os pesquisadores do grupo Cisco Talos tomaram conhecimento dela logo no início. Quando as infecções dispararam, eles estavam prontos para interrompê-las de imediato. Hoje, a ameaça representada pelo VPNFilter diminuiu significativamente graças ao trabalho dos parceiros de inteligência contra ameaças do setor público e privado e às autoridades policiais. O VPNFilter permanece como um precursor do que inevitavelmente ainda está por vir.

Como ele é feito

Etapa 1 – O VPNFilter tem três componentes principais, ou " etapas", que compõem a ameaça. O objetivo central da primeira etapa é estabelecer uma espera persistente em um dispositivo. Até surgir o VPNFilter, malware direcionado a dispositivos de IoT normalmente podia ser eliminado apenas com a reinicialização do dispositivo. No caso de um componente da primeira etapa do VPNFilter, o malware sobrevive a tal tentativa. A etapa um também inclui várias opções para se conectar ao servidor de comando e controle (C2), que informa ao malware o que ele deve fazer.

Etapa 2 – A segunda etapa, que é o componente principal usado para atingir as metas mal-intencionadas do VPNFilter, conta com recursos como coleta de arquivos, execução de comandos, extração de dados e gerenciamento de dispositivos. Algumas versões da etapa dois incluíam um “kill switch”, que se ativado, poderia deixar o dispositivo infectado permanentemente inutilizável.

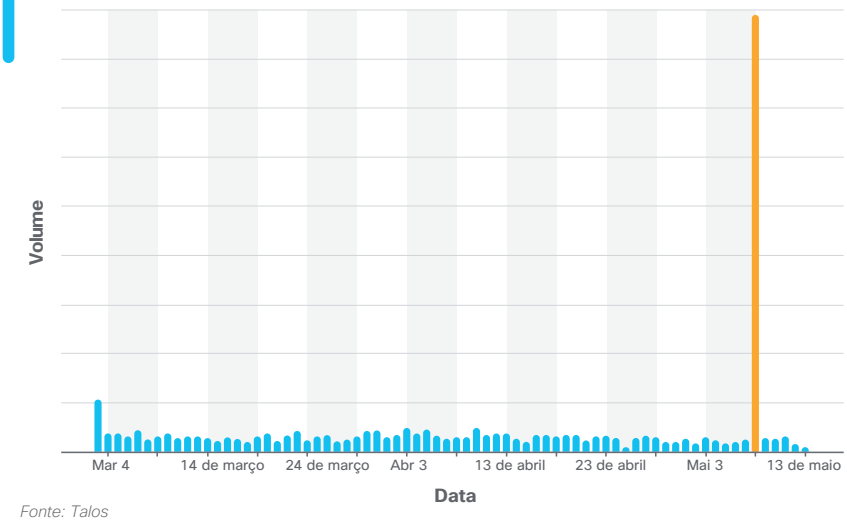
Etapa 3 – A terceira etapa amplia a funcionalidade da segunda, oferecendo plug-ins para disponibilizar ainda mais ações mal-intencionadas. Alguns desses plug-ins incluem a funcionalidade para:

- Monitorar o tráfego de rede
- Roubar várias credenciais
- Monitorar o tráfego de um dispositivo de IoT industrial específico
- Criptografar a comunicação com o servidor C2
- Mapear redes
- Explorar sistemas de endpoint
- Espalhar para outras redes
- Realizar ataques DDoS
- Construir uma rede proxy que pode ser usada para ocultar a origem de ataques futuros

VPNFilter (quase) tem êxito

Talos pesquisa o VPNFilter por vários meses e conclui que a taxa de infecção ficou razoavelmente estável. A equipe monitorou e examinou os dispositivos infectados para entender melhor a ameaça e os recursos contidos no malware.

Figura 2 Novas infecções por VNPFilter por dia



Fonte: Talos

Isso ocorreu até 8 de maio de 2018, quando houve um pico de atividade de infecção. Além disso, a maioria das infecções aconteceu na Ucrânia. Um segundo pico de infecções do VPNFilter na Ucrânia ocorreu em 17 de maio, perto do aniversário de um ano do NotPetya. Devido ao histórico de ataques destrutivos na Ucrânia, o Talos achou melhor abordar esse ataque de infraestrutura o mais rápido possível, mesmo que a pesquisa permanecesse em andamento.

O Talos continuou pesquisando e divulgando informações sobre o botnet até que, em setembro de 2018, conseguiu declarar a ameaça como neutralizada.

Desaparecido, mas não esquecido

Infelizmente, embora o VPNFilter possa ser uma ameaça do passado, vulnerabilidades continuam sendo descobertas em dispositivos de IoT. Porém, é inevitável que futuramente ocorra outra ameaça que tenha como alvo a IoT.

Defender-se contra essas ameaças é difícil. Os dispositivos de IoT, como roteadores, geralmente são conectados diretamente à Internet. Junte-se a isso o fato de que muitos usuários não têm o conhecimento técnico para repará-los ou não os consideram uma ameaça, e a situação se torna muito perigosa.

E no final das contas, a IoT como parte da rede só tende a aumentar. O VPNFilter mostra o que pode acontecer caso não sejam tomadas medidas adequadas para proteger esses dispositivos no futuro.

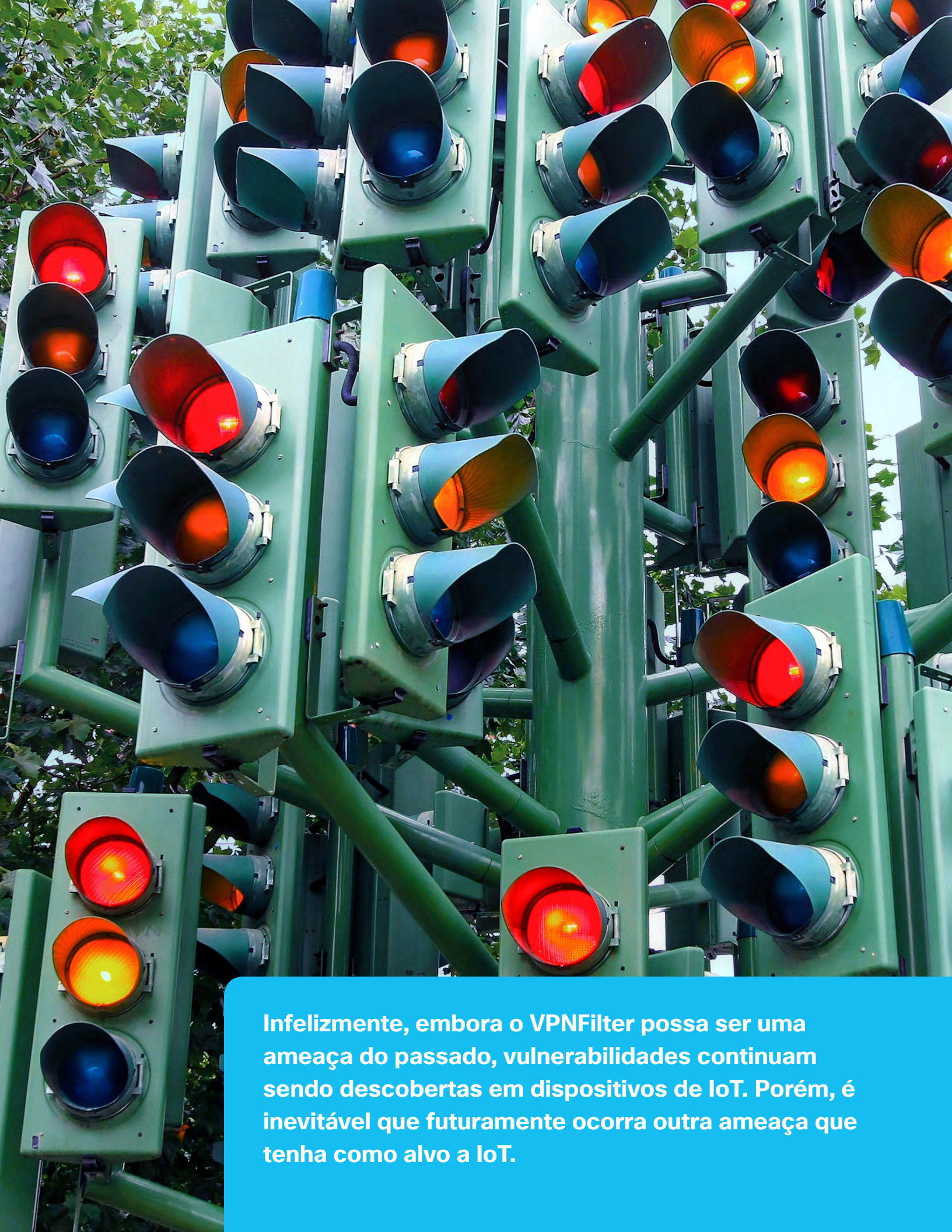
Para uma visão mais detalhada sobre esse assunto:

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-Most-PROMINENT.html



Infelizmente, embora o VPNFilter possa ser uma ameaça do passado, vulnerabilidades continuam sendo descobertas em dispositivos de IoT. Porém, é inevitável que futuramente ocorra outra ameaça que tenha como alvo a IoT.

Gerenciamento de dispositivos móveis: a salvação e a maldição

O Talos descobriu que agentes mal-intencionados descobriram como usar o MDM para fins criminosos.

A funcionalidade de gerenciamento de dispositivos móveis (MDM) foi um benefício para as empresas. Ela permite que as empresas tenham muito mais controle sobre os dispositivos na rede. No entanto, conforme descobrimos em 2018, também abriu portas para agentes mal-intencionados com bastante recurso financeiro.

Quando se trata de malware móvel, pode ser difícil atingir os sistemas operacionais. A cerca criada em torno de todo o sistema operacional móvel, na maior parte do tempo, o protegeu contra aplicativos mal-intencionadas.

Isso não quer dizer que os agentes mal-intencionados não tentaram atacar celulares. Houve aplicativos mal-intencionados descobertos nas lojas de aplicativos oficiais, mas na maioria dos casos, os invasores foram confinados a dispositivos comprometedores que foram desbloqueados ou "destravados" ou, se disponíveis, permitiram a entrada de aplicativos de terceiros.

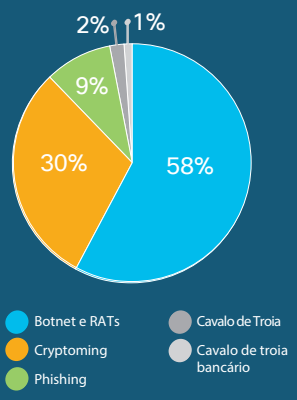
Portanto, ao mesmo tempo em que o jardim murado é seguro, ele também pode ser uma prisão. A desvantagem desse nível de restrição e da segurança que ele oferece é que você só pode instalar aplicativos de uma loja de aplicativos oficial ou, se disponível, deixar o dispositivo aberto para qualquer aplicativo de terceiros. Isso se torna um problema para as empresas que criam aplicativos proprietários que só permitem acesso dos funcionários, mas que desejam manter seus dispositivos seguros.

A introdução do MDM

Para lidar com essa necessidade, foram introduzidos os sistemas MDM. Isso permite que uma empresa tenha celulares corporativos, instale perfis registrados na empresa e, por fim, instale os aplicativos preferidos. O MDM frequentemente oferece outros recursos empresariais, como a capacidade de controlar as configurações do dispositivo, impedir o acesso a sites indesejados ou encontrar dispositivos perdidos.

Um resumo dos incidentes de segurança

Quais são os incidentes de segurança mais comuns que as empresas estão enfrentando? Nossos colegas do grupo de inteligência cognitiva da Cisco processaram os números. Aqui está uma amostra das cinco principais categorias, obtida em julho de 2018.



Em geral, botnets e RATs dominam os incidentes de segurança. Ameaças como Andromeda e Xtrat estão inclusas nesta categoria.

A segunda maior categoria de ameaça é cryptomining, que contém incidentes que revelaram os invasores não autorizados Monero e Coinhive, entre outros.

O que é mais notável nesse resumo é como os Cavalos de Troia de sistemas bancários representam uma pequena proporção. Sem dúvida, isso vai mudar com o aumento da atividade do Emotet.

Vamos analisar mais uma vez essa métrica em relatórios futuros, para saber como isso muda.

Imagem: Talos

Não há dúvida que o MDM é uma ferramenta poderosa. Tão poderosa que o Talos constatou que agentes mal-intencionados descobriram como usá-lo para fins criminosos.

Isso começou na Índia

Nossos pesquisadores do Talos descobriram dispositivos na Índia que foram comprometidos por meio de um código aberto do sistema MDM. Os invasores conseguiram criar perfis mal-intencionados nos dispositivos e enviar aplicativos com o objetivo de interceptar dados, roubar mensagens SMS, baixar fotos e contatos e rastrear a localização dos dispositivos, entre outras ações.

Os aplicativos incluíam versões modificadas de aplicativos muito utilizados, como WhatsApp e Telegram, que tinham recursos extras adicionados, ou eram carregados neles (" sideloaded"), permitindo que os invasores monitorassem as conversas em cada dispositivo comprometido.

Como esses dispositivos foram atacados continua sendo um mistério. É possível que os invasores tivessem acesso físico aos dispositivos, o que lhes permitiria instalar um perfil que lhes desse controle. No entanto, também é possível que eles tenham usado engenharia social para enganar os usuários e instalar o perfil.

Esse alerta mal-intencionado pode ter chegado por e-mail ou mensagem de texto, tentando enganar o usuário, fazendo-o pensar que era necessário instalar o perfil mal-intencionado. Mesmo assim, o usuário precisa seguir uma série de instruções e clicar em vários prompts antes que o dispositivo seja totalmente comprometido.

Cuide do seu jardim

Não há dúvida de que esse é um método de ataque potente e preocupante. Felizmente, também é raro. A campanha de ataque descoberta pelo Talos é a única publicamente

Dada a potencial recompensa que eles oferecem, estamos propensos a ver mais desses ataques no futuro sendo realizados por agentes com bastante recurso financeiros.

conhecida desse tipo específico. Também é difícil de ser bem-sucedida, considerando o número de etapas que um usuário precisa realizar para configurar um dispositivo para atividades mal-intencionadas. Por causa da possível recompensa, o Talos já observa cada vez mais ataques a dispositivo móvel, realizados por agentes de ameaças com bastante recurso financeiro.

Ironicamente, a melhor proteção contra um MDM mal-intencionado é...MDM.

As empresas precisam garantir que os dispositivos tenham perfis implantados, capazes de monitorar e impedir a instalação de perfis ou aplicativos mal-intencionados de lojas de aplicativos de terceiros.

Também é importante que os usuários estejam cientes do processo de instalação de MDM, e que eles sejam informados sobre esses ataques para que não instalem um MDM mal-intencionado.

Para uma visão mais detalhada sobre esse assunto:

https://blog.talosintelligence.com/2018/07/Mobile-malware-Campaign-uses-malicious-MDM.html

https://blog.talosintelligence.com/2018/07/Mobile-malware-Campaign-uses-malicious-MDM-part2.html

O que aconteceu com o ransomware?

Em 2017, parecia que o ransomware dominaria o cenário de ameaças por muito tempo. Ameaças como SamSam e Bad Rabbit geravam avisos, exigindo pagamentos em moeda criptografada, senão haveria perda de todos os dados.

Depois de pouco mais de um ano, certamente houve uma mudança.

O ransomware perdeu o trono, em grande parte para o cryptomining mal-intencionado.

Por que a mudança repentina? Com o ransomware, apenas uma pequena porcentagem das vítimas paga o resgate. Mesmo que paguem, é um pagamento único, não uma fonte de receita recorrente.

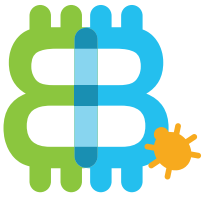
Ainda mais arriscado, os órgãos de segurança pública em todo o mundo começaram a combater os invasores que usam ransomware. Como as prisões associadas ao ransomware aumentaram, os criminosos foram atraídos pelos tipos de ataque menos arriscados.

Isso não quer dizer que o ransomware tenha desaparecido, vimos algumas dessas ameaças aparecendo em 2018. O GandCrab continuou a fazer sua presença percebida, e o Ryuk foi disseminado através de infecções por Emotet e Trickbot. Portanto, embora o ransomware já não reine soberano, ele ainda existe, e demanda de vigilância para evitar ataques.

Cryptomining: um lobo em pele de cordeiro não deixa de ser um lobo

De longe, o esquema mais proeminente de ameaças financeiras de 2018 foi o cryptomining mal-intencionado. Esse é um tópico que o grupo de inteligência de ameaças Cisco Talos tem pesquisado há algum tempo. Na mente de um invasor, é quase o crime perfeito: mineradores trabalham frequentemente em segundo plano sem o conhecimento dos usuários, roubando a capacidade de computação e gerando receita para o invasor.

À medida que as empresas se aperfeiçoaram em lidar com ransomware e os órgãos de segurança em todo o mundo começaram a reprimir os invasores de ransomware, cada vez mais invasores foram atraídos para a perspectiva menos arriscada de vender software de cryptomining mal-intencionado.



Há pouca diferença entre o software de cryptomining que um usuário instala sozinho e o software de cryptomining instalado por um agente mal-intencionado.

Os cordeiros encontram o lobo

Geralmente, há pouca ou nenhuma diferença entre o software de cryptomining que um usuário instala sozinho e o software de cryptomining instalado por um agente mal-intencionado. A diferença está no consentimento, e o software de crytomining mal-intencionado está funcionando sem o conhecimento do proprietário. Há um atrativo óbvio para os invasores neste caso, onde eles podem aproveitar os benefícios sem o conhecimento das vítimas.

No jogo de risco e recompensa, o cryptomining tem menor probabilidade de chamar a atenção da polícia. Por outro lado, qualquer software executado em um dispositivo sem o conhecimento do proprietário é motivo de preocupação.

E o cryptomining, mal-intencionado ou não, pode render um bom dinheiro. Nos últimos anos e na primeira metade de 2018, o valor da criptomoeda disparou. Como qualquer item valioso e relacionado a software, ele atraiu a atenção de agentes mal-intencionados, especialmente porque coincidiu com uma queda no ransomware. O cryptomining gera receita recorrente, enquanto o ransomware geralmente resulta em um pagamento único da vítima.

Os perigos do cryptomining mal-intencionado

Na perspectiva do defensor, há muitas razões para se preocupar com o cryptomining mal-intencionado. Como qualquer parte do software em um computador, o cryptomining vai ter um impacto no desempenho geral do sistema e precisar de energia extra. Pode não causar grande impacto em um único sistema, mas ao multiplicarmos o custo pelo número de endpoints em uma empresa, o aumento nos gastos com energia pode ser considerável.

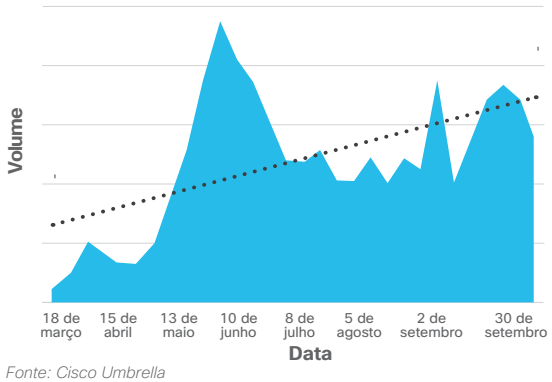
Além disso, pode haver implicações de conformidade com as normas quando os cryptominers estiverem obtendo receita nas redes corporativas. Isso vale especialmente para quem é do setor financeiro, onde regras rigorosas podem ser aplicadas às receitas geradas usando recursos corporativos, estejam ou não os responsáveis conscientes da prática.

Talvez o mais preocupante é que a presença de uma infecção mal-intencionada de cryptomining, sem o conhecimento dos que administram a rede, poderia indicar falhas de segurança na configuração ou nas políticas gerais de segurança. Tais falhas poderiam ser facilmente exploradas pelos invasores por outros meios. Basicamente, se uma infecção de cryptomining for encontrada na rede, o que vai impedir que outras ameaças mal-intencionadas explorem essas mesmas vulnerabilidades para realizar outras atividades mal-intencionadas?

O que está acontecendo agora?

Embora, conforme observado pela Cisco na camada de DNS, tenha havido altos e baixos nítidos no volume total de tráfego relacionado ao cryptomining, a conclusão é que o cryptomining está em ascensão com o passar do tempo.

Figura 3 Volume de tráfego de cryptomining de DNS corporativo



Fonte: Cisco Umbrella

O interessante é que o valor de muitas criptomoedas conhecidas diminuiu durante o mesmo período, com tendência de queda. Por exemplo, a Monero, uma moeda popular usada em cryptomining mal-intencionado.

Figura 4 Valores de fechamento da Monero

Fonte: coinmarketcap.com

Agentes mal-intencionados continuam a enviar cryptomining mal-intencionado devido à facilidade de implantação e ao baixo risco, caso sejam descobertos. O fato é que, uma vez instalado em um dispositivo, ele continua gerando dinheiro para o agente mal-intencionado durante o período de permanência.

Como o cryptomining mal-intencionado entra em um sistema?

Há várias maneiras de o cryptomining mal-intencionado entrar no ambiente. Ele pode:

- Explorar vulnerabilidades
- Enviar e-mails com anexos mal-intencionados
- Utilizar botnets
- Aproveitar o cryptomining no navegador da Web
- Utilizar ameaças adware que instalam plug-ins de navegador
- Ser um agente interno mal-intencionado

Infelizmente, o cryptomining mal-intencionado ainda vai demorar um tempo para desaparecer. Os distribuidores de spam continuarão a enviar ameaças de cryptomining.

A presença de cryptomining, sem o conhecimento dos administradores de rede, pode indicar outras brechas de segurança na rede.

O dinheiro é, e provavelmente sempre será, um dos principais estímulos para os agentes mal-intencionados. Em muitos aspectos, o cryptomining mal-intencionado pode ser visto como uma forma de os invasores obterem lucro rápido com poucos aborrecimentos. Isso é especialmente verdadeiro, já que os alvos estão menos preocupados com cryptomining do que com outras ameaças em seus dispositivos. É uma situação perfeita para os lobos vestirem-se em pele de cordeiro e desfrutarem dos lucros.

Para uma visão mais detalhada sobre esse assunto:

https://blogs.cisco.com/security/cryptomining-a-sheep-or-a-wolf

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

https://blog.talosintelligence.com/2018/12/cryptomining-Campaigns-2018.html

No radar

Para este relatório, podemos ver uma ampla variedade de ameaças a serem consideradas. Embora nem tudo tenha sido incluído no relatório, planejamos analisar os tópicos a seguir nos próximos meses por meio de nossa série de blogs de Ameaça do mês. Aqui está uma amostra do que está por vir:

Extorsão digital. Uma das campanhas de phishing mais atuais se baseia no medo dos destinatários em relação à extorsão de pagamentos em Bitcoin. Algumas campanhas afirmam que flagraram o destinatário na câmera olhando sites de pornografia. Outros incluem ameaças falsas de bomba. Em última análise, as ameaças são completamente fabricadas, tudo na esperança de enganar um número suficiente de destinatários para encher com Bitcoin as carteiras dos invasores.

Pishing no Office 365. Outra campanha significativa de phishing gira em torno do roubo de credenciais das contas do Microsoft Office 365. Os invasores usaram vários métodos para fazer isso. Vamos descrever diferentes campanhas e como reconhecê-las na nossa postagem do blog.

Para ficar a par da série de blogs Ameaça do mês, inscreva-se na nossa lista de e-mails e acesse a página de Ameaça do mês.

Assine: http://cs.co/9002ERAWM

Ameaça do mês: http://cisco.com/go/threatofthemonth

O inverno estava chegando: Olympic Destroyer

Imagem: Talos

Embora o ataque dos Jogos Olímpicos possa ter sido único, o grupo por trás dele não vai parar.

O ano passado começou com uma explosão. Especialistas em segurança digital ainda estavam sentindo os efeitos dos ataques de WannaCry e NotPetya, e esperavam por um começo mais tranquilo do ano. Essas aspirações foram rapidamente por água abaixo quando o Talos descobriu que as interrupções na cerimônia de abertura dos Jogos Olímpicos de Inverno de 2018 em Pyeongchang, Coreia do Sul, foram causadas por malware.

O malware era altamente destrutivo e adaptado para o ambiente em que estava. O nome pode estar ligado a uma ocasião histórica, mas a ameaça do Olympic Destroyer continua viva.

Durante as cerimônias de abertura, o Wi-Fi parou de funcionar no estádio e nas áreas de mídia das Olimpíadas de Inverno e o site oficial dos jogos saiu do ar. Uma interrupção em grande escala como essa apresenta vários desafios, incluindo riscos de privacidade de dados, prejuízo para a reputação de marca e uma queda no nível de satisfação do cliente.

Por fim, ficou claro que essa interrupção era um ataque cibernético, e uma investigação de longo prazo mostraria que o malware exibia duas características: 1) era um malware de limpeza projetado para destruir ativos (em vez de ser executado como ransomware, por exemplo) e 2) mais interessante, foi criado para esconder sua origem e enganar pesquisadores. Esse foi um ataque avançado que combinava técnicas sofisticadas de malware com uma estratégia desonesta.

Como exatamente o Olympic Destroyer causa destruição?

O método de disseminação do Olympic Destroyer ainda não é conhecido. O que está claro é que, uma vez dentro de uma rede de destino, ele se move rapidamente.

Nossa melhor análise no rescaldo do ataque de Pyeongchang é que ele se moveu como um worm: de um jeito rápido e altamente destrutivo. O arquivo rouba senhas, apaga os dados de backup e mira nos dados armazenados nos servidores, causando máxima devastação no menor tempo possível.

O Olympic Destroyer era altamente destrutivo e projetado para destruir informações.

Os invasores usaram ferramentas legítimas para realizar movimentos laterais, neste caso, o PsExec (um protocolo do Windows que permite a execução de programas em computadores remotos). Devido ao momento muito específico do ataque, para coincidir com a cerimônia de abertura das Olimpíadas, ele foi acionado remotamente.

O Olympic Destroyer provavelmente queria criar uma negação plausível para seus autores usando partes do código antigo que foram anexadas a outros agentes de ameaça. Alguns pesquisadores de segurança também ficaram confusos com esse ataque, enquanto outros foram ágeis para relatá-lo.

Há mais inverno chegando...

Quaisquer que sejam os motivos reais, o Cisco Talos encontrou os marcadores de um agente sofisticado no malware Olympic Destroyer. Isso nos mostra que, embora o Olympic Destroyer fosse um ataque sob medida, o grupo por trás dele não vai descansar. Ele provavelmente vai usar esse método altamente eficaz mais uma vez para provocar caos ou realizar furtos ou outras ações nefastas. Portanto, precisamos estar atentos ao procurar por malware dessa natureza.

E foi assim que 2018 começou. Que em 2019 não traga nada mal-intencionado e sofisticado para nenhum outro evento importante.

Para uma visão mais detalhada sobre esse assunto:

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

https://blog.talosintelligence.com/2018/02/who-wasn ' t-responsável-para-olympic.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

Sobre a Serie de Relatórios de Cibersegurança

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes forneciam detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados no banner **Serie de Relatórios de Cibersegurança**. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profundidade e amplitude da experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças e o Relatório de Referência do CISO, e outros ainda virão ao longo do ano.

Para obter mais informações, acesse www.cisco.com/br/securityreports.

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

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

Sede - Europa
Cisco Systems International BV Amsterdam,
Holanda

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

Publicado em fevereiro de 2019 THRT_01_0219_r2