SOPHOS
Cybersecurity evolved.

RELATÓRIO DE AMEAÇAS 2021 DA SOPHOS

Navegando pela segurança virtual em um mar de incertezas

Por **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response, Sophos AI, Cloud Security**

CONTEÚDO

O PODER DE COMPARTILHAR

Joe Levy, CTO, Sophos

“Se quiser ir depressa, vá sozinho, mas se quiser ir longe, sigam juntos.”

Este provérbio africano não poderia ser mais verdadeiro quando se trata da indústria cibernética. Se trabalharmos coletivamente, como uma verdadeira equipe, poderemos chegar muito mais longe do que se tentarmos lutar contra o crime virtual como fornecedores individuais.

E apenas melhorando essa abordagem e compartilhando inteligência de ameaças de modo mais abrangente, e expandindo o grupo de participantes que contribuem para este compartilhamento e colaboração (e que deles se beneficiam), nós, fornecedores de segurança virtual, continuaremos a elevar os custos para os invasores e a fazer mudanças de impacto e duradouras.

Seguindo com esse mesmo espírito de cooperação no trabalho, em 2017 a Sophos se juntou à *Cyber Threat Alliance*, uma organização dedicada a pôr abaixo as barreiras que, por anos, impediam qualquer chance de a concorrência no setor de segurança da informação colaborar uns com os outros. A CTA foi muito além do seu preceito inicial de servir como um repositório de inteligência compartilhada contra ameaças e um lugar para resolver as diferenças e se tornou um tipo de ONU da indústria de segurança virtual.

Através dessa parceria com a CTA, a Sophos pode proteger melhor os seus clientes, graças aos alertas prévios e à troca de dados entre fornecedores, o que foi possível com a aliança. A Sophos também compartilha o encargo de proteger clientes de outros fornecedores ao contribuir com a sua própria inteligência de ameaças.

Em março de 2020, conforme o lockdown foi rapidamente instituído no mundo todo para conter a propagação e a COVID-19, o diretor científico da Sophos, Joshua Saxe, fez um apelo pelo Twitter. Estarrecido com grupos criminosos que começavam a incorporar referências à COVID-19 em suas campanhas criminosas, os analistas de segurança da informação – mais de 4.000 deles – se uniram em uma manifestação de repúdio e formaram a CCTC (COVID-19 Cyber Threat Coalition) em um canal do Slack criado naquele dia. Esse canal estabelece uma "casta comunitária" persistente para que a comunidade possa se respaldar em tempos de crise, e está cada vez mais perto de atingir o status de organização sem fins lucrativos sob o auspício da CTA.

Essas histórias de compartilhamento da inteligência de ameaças falam sobre muito mais do que simplesmente as organizações. Outra parábola – a dos cegos e o elefante – nos ensina que nenhum fornecedor pode oferecer por si só a verdade plena e absoluta apenas através de suas experiências subjetivas. A verdade sobre as dificuldades se forma com a união de nossas experiências. Essas iniciativas de colaboração protegeram milhões de pessoas de se tornarem vítimas do crime virtual, mas apenas isso não inferiu a *razão* de terem tido êxito. O sucesso veio porque a motivação central de seus membros e fundadores era, primeiramente, proteger a todos que estivessem em perigo. Sem motivos financeiros, apenas um desejo de defender aqueles em necessidade, quando os lobos pareciam estar batendo à porta.

Isso mostra que o modelo está correto – transpondo lacunas críticas de cobertura que nenhum de nós, sozinho, poderia unir – e que podemos fazer ainda mais. Como uma indústria, no futuro talvez também consideremos o compartilhamento de modelos de aprendizado de máquina, ou conjuntos de dados de treinamento, do mesmo modo que hoje compartilhamos listas de bloqueio ou regras Yara. Poderíamos também reforçar e contribuir com normas emergentes, como STIX e a estrutura ATT&CK. Poderíamos participar das ISACs e ISAOs específicas à indústria.

O futuro será mais conectado e estaremos mais bem preparados (e mais bem protegidos) para ele.

SUMÁRIO EXECUTIVO

O Relatório de Ameaças 2021 da Sophos cobre as áreas em que a Sophos adquiriu insight através dos mais de 12 meses de trabalho do SophosLabs em análise de spam e malware, e pelas equipes do Sophos Rapid Response, Cloud Security e Data Science. Esses aspectos do nosso trabalho diário em proteger os clientes nos dá um insight sobre o cenário da ameaça que pode indicar à equipe de resposta a incidentes e aos profissionais de segurança da TI onde devem canalizar seus esforços para defender redes e endpoints no ano que vem.

Segmentamos o relatório em quatro partes principais: Debates sobre como o ransomware se autotransformou e qual o seu rumo; análise sobre os ataques mais comuns que as organizações enfrentam e porque esses canários cantadores metafóricos se mantêm ameaças de grande significância; como o surgimento de uma pandemia global afetou a segurança da informação em 2020, e uma pesquisa do escopo dos ataques que visam plataformas tradicionalmente nunca antes consideradas parte de uma superfície de ataque da empresa.

Para resumir os pontos básicos deste relatório:

Ransomware

- Os golpistas com seus ransomwares continuam a inovar em tecnologia e no modus operandi do crime em ritmo acelerado
- Agora, mais grupos de ransomware se engajam no roubo de dados de modo que possam ameaçar suas vítimas com extorsões em troca de não publicar dados privados confidenciais
- Conforme os grupos de sequestro colocam mais esforços em ataques ativos contra as grandes organizações, os resgates que demandam subiram vertiginosamente
- Além disso, os grupos distintos de criminosos que se envolvem com sequestros e resgates parecem estar colaborando entre si mais de perto no submundo do ransomware, comportando-se mais como cartéis do crime cibernético do que grupos independentes
- Ataques de ransomware que antes levavam semanas ou dias agora levam, quando muito, apenas algumas horas para serem efetivados

Ameaças diárias

- Plataformas de servidor que executam Windows e Linux têm sido duramente castigadas por ataques, transformando-se um degrau para atingir as organizações
- Serviços comuns, como os concentradores de RDP e VPN, se mantêm o foco de ataque no perímetro da rede, e os invasores também usam o RDP para se mover internamente pelas redes violadas
- Mesmo os malwares de menor periculosidade podem levar a grandes violações, com as famílias de malwares se assemelhando cada vez mais a "redes de distribuição de conteúdo" de outros malwares
- A falta de atenção a um ou mais aspectos de higiene básica de segurança foi apontada como a causa primária de muitos dos ataques mais danosos que investigamos

COVID-19

- Trabalhar de casa apresenta novos desafios, estendendo o perímetro de segurança das organizações para milhares de redes domésticas protegidas por uma imensa variedade de níveis de segurança
- A computação na nuvem deu vazão ao ímpeto das empresas por ambientes de computação seguros, ainda que tenham seus próprios desafios únicos além daqueles de uma rede corporativa tradicional
- Os criminosos tentaram limpar sua reputação com a promessa de não atacar organizações que envolvessem operações de saúde e assistência médica, porém mais tarde voltaram atrás
- Empresas criminosas se ramificaram em prestadoras de serviços para facilitar o acesso para os novos criminosos
- Em 2020, os profissionais de segurança virtual em todo o mundo se organizaram rapidamente em uma força-tarefa para combater as ameaças que se aproveitavam do potencial da engenharia social para explorar qualquer coisa relacionada ao novo coronavírus

Plataformas não tradicionais

- Já virou rotina entre os criminosos se aproveitarem da riqueza de ferramentas e utilitários dos "red teams" se infiltrarem como teste de penetração em ataques ativos em tempo real
- Apesar dos esforços por parte das operadoras de plataformas móveis em monitorar aplicativos em busca de códigos maliciosos, os invasores continuam a comer pelas bordas, desenvolvendo técnicas para ludibriar essas varreduras de códigos
- Um software classificado anteriormente como "potencialmente indesejado", porque disparava uma pletora de anúncios publicitários (ainda que não maliciosos), agora se engaja em táticas que estão cada vez mais difíceis de distinguir de um malware evidente
- Os cientistas de dados vêm aplicando abordagens emprestadas da epidemiologia biológica para espalhar cargas de malwares e ataques como um método de ligar as lacunas na detecção

O FUTURO DO RANSOMWARE

Os ataques de ransomware lançados durante 2020 aumentaram o sofrimento de uma população já castigada. Conforme a pandemia devastou muitas vidas e o sustento de muitos, também o fez um rol de famílias de ransomware cujos esforços não se acanharam em atacar os setores de saúde e educação, mesmo com os hospitais virando verdadeiros campos de batalha da COVID-19 e as escolas tentando inventar uma maneira totalmente nova de educar nossas crianças e jovens desde março.

Você não consegue juntar muito só com quermesses durante uma pandemia para pagar um resgate, mas algumas escolas conseguiram se recuperar de ataques que pareciam visar o primeiro dia de aula com backups de segurança.

As operadoras de ransomware desbravaram novos caminhos para se esquivar de produtos de segurança de endpoint, se espalhar rapidamente e até mesmo criaram uma solução para o problema (pela perspectiva deles) de as empresas e indivíduos visados terem um bom material de backups, seguramente armazenado onde o ransomware não os poderia atingir.

Mas o que parece ser uma amplitude variada de ransomwares talvez não seja tão ampla assim. Conforme o tempo passou e investigamos um maior número de ataques, os analistas da Sophos descobriram que alguns códigos de ransomware pareciam ter sido compartilhados entre famílias, e que alguns dos grupos de ransomwares pareciam trabalhar em colaboração, mais do que competindo entre si.

Com tudo isso, fica difícil fazer qualquer tipo de previsão sobre o que os criminosos de ransomware farão a seguir. Os criadores e operadores de ransomwares gastaram horas e horas trabalhando nas suas defesas contra produtos de segurança de endpoint. Nós contra-atacamos suas medidas defensivas. Eles mostram criatividade e versatilidade em tramar novas táticas; nós mostramos tenacidade em estudar o que eles fazem e encontrar maneiras engenhosas de pará-los.

O roubo de dados cria um mercado secundário de extorsão

Até esse ano, o senso comum que regia as empresas de segurança que tinham alguma experiência em ransomware era bastante uniforme: embarreirar os métodos óbvios de entrada, como portas RDP voltadas à internet, manter bons backups offline e lidar com as pequenas infecções por malwares inofensivos, como Dridex ou Emotet, rapidamente, antes que pudessem avançar com suas cargas mortíferas.

Vários ataques de alta periculosidade, por exemplo, contra escolas municipais pelos Estados Unidos, falharam, ao menos em parte, porque os gerentes de TI mantinham cópias de backup de dados críticos.

Como uma medida preventiva contra o preparo de suas vítimas, várias famílias de ransomwares se apegaram ao lado diligente do design para aumentar a pressão em suas vítimas para pagar o resgate – mesmo que o backup de todos os dados essenciais estivesse protegido. Eles não apenas sequestravam a máquina, mas também roubavam os dados das máquinas e ameaçavam espalhar os dados pelo mundo se as vítimas se recusassem a pagar o proposto.

Durante os últimos seis meses, os analistas da Sophos observaram que os ransomwares se organizaram ao redor de um conjunto comum (e crescente) de ferramentas que utilizam para exfiltrar dados da rede das vítimas. Esse conjunto de ferramentas e utilitários legítimos e já conhecidos, a que qualquer um pode ter acesso, não é detectado por produtos de segurança de endpoint. A lista de famílias de ransomwares que se enquadram nessa prática continua a crescer e agora inclui Doppelpaymer, REvil, Clop, DarkSide, Netwalker, Ragnar Locker e Conti, entre muitos outros mais. Os invasores operam sites de "divulgação", onde tornam públicos os dados secretos que roubaram; o REvil permite que qualquer pessoa compre dados roubados diretamente no site.

Os criminosos se utilizam desse conjunto de ferramentas para copiar informações internas sigilosas, compactá-las em arquivos e transferi-las para fora da rede, e para longe do alcance da vítima. Essas são algumas das ferramentas que temos visto em uso até então:

- Total Commander (gerenciador de arquivos com cliente FTP interno)
- 7zip (software de compactação de arquivo)
- WinRAR (software de compactação de arquivo)
- psftp (cliente SFTP do PuTTY)
- Windows cURL

Quando se trata de roubo de dados, os golpistas são muito menos seletivos e exfiltram pastas inteiras, independentemente dos tipos de arquivos que estejam contidos nelas. (Normalmente, os ransomwares priorizam a parte de criptografia do ataque aos tipos principais de arquivos e excluem vários outros.)

Tamanho não é documento. Eles parecem não se importar muito com a quantidade de dados visada pela exfiltração. A estrutura de diretórios é exclusiva a cada empresa e alguns tipos de arquivo podem ser compactados melhor do que outros. Já vimos arquivos de 5 GB a 400 GB de dados compactados sendo roubados de uma vítima antes da implantação do ransomware.

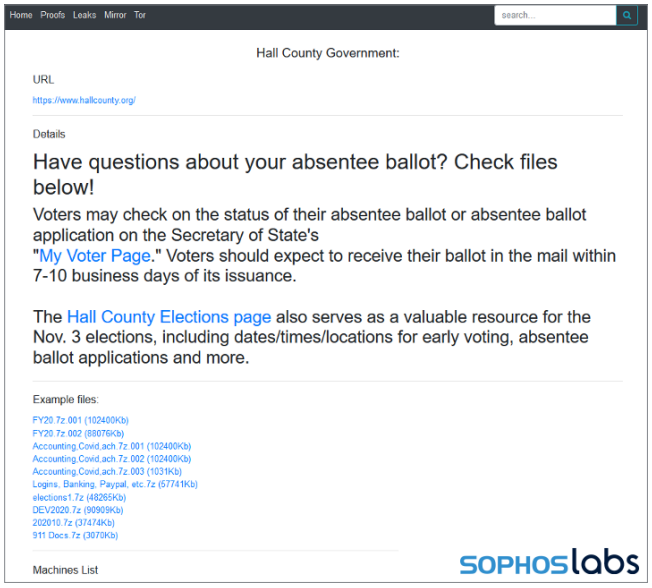


Fig.1. Em outubro de 2020, a página de divulgação de dados secretos do ransomware Doppelpaymer revelou que invasores haviam atingido as redes de dados de Hall County, um município no estado da Geórgia, nos EUA. Os dados secretos incluíam referências a um arquivo chamado "elections" que incluía as provas da cédula para a prévia eleitoral de 2020 e listas dos mesários dos serviços eleitorais de 2018 com seus números de telefone, entre outros arquivos confidenciais. A Associated Press divulgou que o ransomware criptografou o banco de dados de verificação de assinaturas que o município usa para validar cédulas eleitorais. Fonte: SophosLabs.

Geralmente, os criminosos enviam os dados exfiltrados para legalizar os serviços de armazenamento na nuvem, o que torna essa atividade mais difícil de localizar, pois esses são destinos comuns de tráfego na rede. Entre os invasores, os seguintes três serviços de armazenamento na nuvem são as rotas mais populares para o armazenamento de dados exfiltrados:

- Google Drive
- Amazon S3 (Simple Storage Service)
- Mega.nz
- Servidores FTP privados

Em um ato final de destruição, os ransomwares invasores buscam incessantemente pelos servidores locais que contêm backups de dados críticos: uma vez encontrados, eles apagam (ou criptografam independentemente) esses backups instantes antes de atacar e criptografar toda a rede.

Definitivamente, o mais importante é armazenar as suas cópias de backup essenciais offline. Se conseguirem encontrá-las, os criminosos virtuais as destruirão.

Resgates sobem e ataques aumentam

É difícil acreditar que apenas dois anos atrás os analistas da Sophos se admiraram com a bolada de US$ 6 milhões angariada pelos operadores do ransomware conhecido como SamSam. Em um ataque respondido pela Sophos em 2020, os operadores do ransomware começaram as suas negociações com um valor em dólares mais de duas vezes o valor angariado pela quadrilha do SamSam em 32 meses de operação.

Agora os ransomwares vêm em classes de peso: peso-pesado, que ataca as redes das grandes empresas, peso meio-médio, que ataca sociedades civis (segurança pública e governos locais) e pequenas e médias empresas, e peso-pena, que visa computadores pessoais e usuários domésticos. Ainda que conquistar um distintivo da mais alta classe impressione, de um modo dúbio, não parece justo comparar altos pedidos de regaste com aqueles que se originam na parte mais indistinta do espectro do ransomware.

A Sophos tem uma equipe dedicada que investiga os ataques de ransomware, e que frequentemente também trabalha com seus alvos. A equipe pode reconstituir a cena forense dos eventos de um ataque após o ocorrido e, às vezes, interromper ataques que ainda estejam em andamento. A equipe do Sophos Rapid Response se envolve em casos quando existe uma chance de parar ou limitar os estragos, mas às vezes o ataque acontece tão rápido que não há nada que se possa fazer, ficando a critério do usuário-alvo decidir se pagará ou não o resgate, e, a partir desse ponto, a Sophos não se envolve mais.

É aqui que as firmas como a Coveware entram em cena. A firma representa os alvos de ransomwares no papel de negociador de alto calibre com os invasores. Alex Holdtman, CTO da Coveware, confirmou nossas suspeitas: os ransomwares pesos-pesados são o principal fator propulsor na demanda por resgastes estratosféricos.

Média paga por resgaste, trimestral

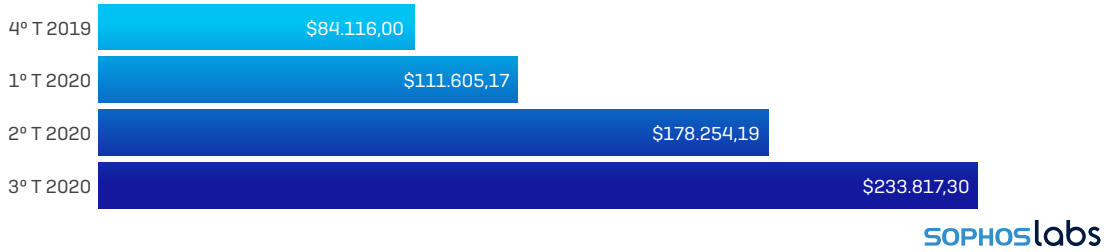


Fig.2. A demanda média de resgaste aumentou 21% no último trimestre, e quase triplicou no último ano. Fonte: Coveware.

Apenas no trimestre passado, a média de pagamento de resgate subiu 21%, mas a Coveware acredita que as médias podem ter sido distorcidas com base em um ou dois ataques com resgates incrivelmente altos. A média de pagamento de resgate no trimestre que acabou de fechar equivale a US$ 233.817,30, pagável em criptomoeda. Um ano atrás, a média de pagamento era de US$ 84.116,00.

Os agentes de ransomwares sabem como o período de inatividade pode sair caro, e já vêm testando o limite máximo que conseguem extorquir em um sequestro.

Várias famílias de ransomwares têm aplicado seus golpes usando o lado confuso do processo para extorquir suas vítimas e fechar a negociação. Como mencionado anteriormente em nosso relatório, grupos como Netwalker e outros se utilizam dessa tática. Dessa forma, mesmo que o alvo do ataque tenha cópias de backup perfeitamente recuperáveis de seus dados, ele poderá acabar forçado a pagar o resgaste na esperança de que os criminosos não publiquem suas informações internas para o mundo.

Até mesmo na parte não tão "nobre" do espectro de ransomwares, as demandas têm aumentado, mas, como diz Holdtman, eles estão apenas se aproximando. Existe uma infinidade de pequenas empresas e indivíduos que são atingidos, mas para estes as demandas de resgaste se mantêm relativamente estáveis.

Dias na vida de um membro da equipe de resposta rápida a ransomwares

Quando uma organização se viu na posição de alvo do ainda ativo ransomware Maze, ela foi direto para a equipe do Sophos Rapid Response. Nós investigamos e ativamente encontramos o ataque enquanto ainda estava em andamento. A seguir você verá um resumo do dia a dia de um ataque, conforme se desenrola.

Antes do Dia 1
Em algum momento antes de o ataque ficar ativo, os operadores comprometeram um computador na rede do alvo.

Esse computador foi usado como "cabeça de ponte" na rede. Em múltiplas ocasiões, o invasor se conectará daquele a outros computadores usando Remote Desktop Protocol (RDP).

Dia 1
A primeira evidência da atividade maliciosa desponta quando um beacon SMB Cobalt Strike é instalado como um serviço em um Controlador de Domínio (DC) desprotegido. Os invasores são capazes de controlar o DC a partir do computador previamente comprometido explorando a conta Domain Admin com uma senha fraca.

Dia 2
Os invasores criam, executam e apagam uma série de tarefas agendadas e scripts em batch. Pelos indícios observados pelos investigadores, as tarefas eram semelhantes a uma técnica usada posteriormente para implantar ataques de ransomware. É possível que os invasores estejam testando o método que planejam utilizar.

Usando a conta Domain Admin comprometida e o acesso RDP, os invasores movimentam-se internamente pela rede e para outros servidores críticos.

Eles usam uma ferramenta de varredura de rede legítima, o Advanced IP Scanner, para começar a mapear e fazer listas de endereços IP que, mais tarde, serão infectados com a implantação do ransomware. Os invasores criam uma lista separada dos endereços IP pertencentes aos computadores usados pelos administradores de TI do alvo.

A seguir, os invasores usam a ferramenta ntdsutil da Microsoft para o despejo do banco de dados de credenciais com hash do Active Directory.

Os invasores executam vários comandos WMI para coletar informações sobre máquinas comprometidas e depois passam a fazer a exfiltração dos dados: Eles identificam um servidor de arquivo e, usando a conta Domain Admin comprometida, o acessam remotamente por RDP. Eles começam a compactar as pastas localizadas nele.

Os invasores movem os arquivos compactados para o controlador de domínio e tentam instalar o aplicativo de armazenamento na nuvem Mega no DC. Isso é impedido pela segurança, assim eles passam a usar uma versão baseada na web e carregam os arquivos compactados.

Dia 3
A exfiltração de dados para o Mega continua durante o dia todo.

Dia 4 e 5
Nenhuma atividade maliciosa é observada durante este período. Em incidentes anteriores, observamos ataques de ransomware aguardando pelo lançamento no fim de semana ou em um feriado, quando a equipe de segurança de TI não está trabalhando ou prestando muita atenção ao que está acontecendo na rede.

Dia 6
Um domingo. O primeiro ataque do ransomware Maze é lançado, usando uma conta Domain Admin comprometida e listas de endereços IP que foram identificados. Mais de 700 computadores são alvo do ataque, que é imediatamente detectado e bloqueado pela segurança. Ou os invasores não se dão conta de que o ataque foi interceptado ou eles esperam que com os dados roubados que têm em mãos já tenham o suficiente para chantagear a vítima, porque esse é o momento quando eles lançam o pedido de resgate de US$ 15 milhões.

Dia 7
A equipe de segurança instala segurança adicional e passa a monitorar ameaças 24 horas, 7 dias. A investigação de resposta a incidentes começa e rapidamente identifica a conta admin comprometida, descobre vários arquivos maliciosos e bloqueia a comunicação entre o invasor e as máquinas infectadas.

Dia 8
Mais ferramentas e técnicas usadas pelos invasores são descobertas, além de indícios relacionados à exfiltração de dados. Mais arquivos e contas são bloqueados.

Dia 9
Apesar da atividade defensiva, os invasores mantêm o acesso à rede e outra conta comprometida, lançando um segundo ataque. Esse ataque é semelhante ao primeiro: executa comandos em um DC, circulando pelas listas de endereços IP contidas em arquivos txt.

O ataque é rapidamente identificado. O ransomware é detectado automaticamente, e a conta comprometida e a carga de malware são desativadas e excluídas. Nenhum arquivo é criptografado.

Claramente não querendo desistir, os invasores tentam novamente. A terceira tentativa acontece poucas horas depois do segundo ataque.

Nesse ponto eles parecem estar desesperados, pois esse ataque visa um único computador. Esse é o principal servidor de arquivos de onde os dados foram exfiltrados.

Os invasores Maze seguem uma nova abordagem: implementam uma cópia completa de uma máquina virtual (VM) e um instalador de hipervisor VirtualBox, um ataque detalhado no SophosLabs Uncut em setembro de 2020.

O resultado do terceiro ataque é o mesmo de antes: a equipe do Sophos Rapid Response detectou e impediu o ataque, sem nenhum arquivo criptografado. A equipe ajudou o cliente a bloquear o grupo criminoso e os invasores não foram capazes de prosseguir com o ataque.

AMEAÇAS DIÁRIAS ÀS EMPRESAS – O CANÁRIO CANTADOR

Se tudo o que você sabe sobre ataques virtuais vem dos noticiários, você está perdoado. Os ataques que visam as grandes organizações acontecem diariamente, mas nem todos eles são eventos desproporcionais, como uma ultra violação de dados que pode levar o capital da empresa (ou o preço das ações) morro abaixo e gerar uma péssima publicidade. Muitos ataques são bem mais mundanos e envolvem malwares que a equipe do SophosLabs monitora em uma lista do tipo "Procurados" para encontrar os "Os Suspeitos".

Mas apesar de esses ataques, e alguns dos malwares que infiltram, serem conhecidos e facilmente refreados, cada um deles traz em si o potencial de piorar muito a situação caso não seja resolvido com rapidez e eficácia. Seguindo na metáfora do canário, esses ataques diários rotineiros representam o canário na mina, a indicação de um presença tóxica que poderia rapidamente espiralar fora de controle.

Ataques direcionados a servidores Windows e Linux

Enquanto a vasta maioria dos incidentes de segurança aos quais respondemos em 2020 envolveu computadores desktop ou notebooks executando variações do Windows, vimos um crescimento estável nos ataques em servidores Windows e outros. Em geral, os servidores têm sido alvos atraentes de ataque por uma série de motivos: frequentemente são deixados de lado, operando sem supervisão alguma; servidores geralmente têm mais capacidade de CPU e memória do que notebooks individuais, e servidores podem ocupar um espaço privilegiado na rede, frequentemente com acesso aos dados mais sigilosos e valiosos às operações de uma organização. Isso faz deles uma atraente base de operações para um invasor persistente. Essas características não mudarão em 2021 e a Sophos prevê que o volume de ataques que visam servidores continuará a crescer.

A maioria dos ataques que visa servidores se enquadra em um destes três perfis: ransomware, criptomineração e exfiltração de dados, cada qual com um conjunto correspondente distinto de táticas e técnicas que os invasores empregam. Uma das práticas recomendadas aos administradores de servidores é evitar que aplicativos desktop convencionais, como clientes de e-mail ou navegadores, sejam executados nos servidores como uma defesa contra infecções, de modo que os ataques que visam servidores tenham que necessariamente aplicar mudanças às suas táticas.

Os servidores que atendem a internet executando o Windows recebem uma descarga incessante de tentativas de força bruta por RDP, uma tática de ataque que, durante os últimos três anos, tem sido mais comumente associada com ataques de ransomware, sendo também um modo de prognóstico. A equipe do Sophos Rapid Response observa com frequência que a causa primária dos ataques de ransomware que investiga envolve um acesso inicial à rede da vítima por meio de RDP, seguindo então para o uso dessas máquinas para obter acesso à base de operações que reside na rede e tomar o controle dos servidores DC, a partir dos quais pode formar o resto do ataque.

Em contraste, os ataques de criptojacking costumam visar uma gama maior de vulnerabilidades no Windows e em aplicativos que normalmente são executados no hardware do servidor, como softwares de bancos de dados.

Por exemplo, um método utilizado pelo criptominer Lemon_Duck envolve um ataque de força bruta contra os servidores voltados para a internet que executam o Microsoft SQL Server. Assim que o invasor desvenda a senha correta do banco de dados, ele usa o próprio banco de dados para reagrupar a carga do criptojacker, gravá-la no sistema de arquivos do servidor e executá-la. A máquina infectada tenta explorar as vulnerabilidades EternalBlue e/ou SMBGhost em uma corrida para disseminar o criptojacker.

O Lemon_Duck é um invasor que opera de modo equivalente e que pode infectar servidores Linux. O malware aplica força bruta às senhas SSH obtidas de uma lista relativamente pequena. Se bem-sucedidos, os invasores carregam shellcodes maliciosos e estabelecem a persistência, aproveitando-se dos pontos de escape de um serviço chamado Redis. O criptojacker também pode se esconder por trás da execução dos comandos para inicializar de dentro de clusters Hadoop.

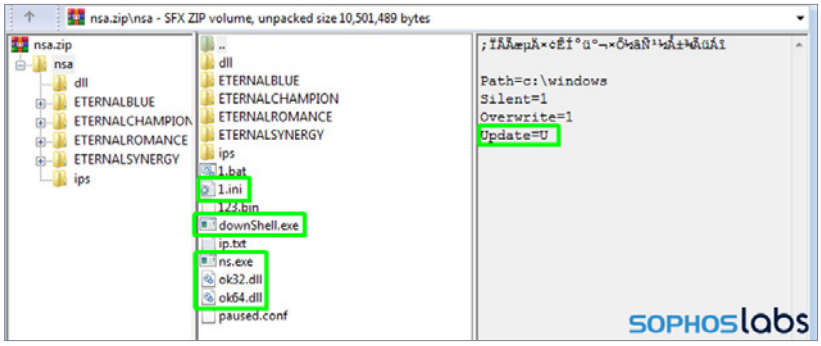


Fig.3. Um dos criptojackers mais prolíficos, chamado MyKings, distribuiu os componentes responsáveis pela instalação do botnet (destacado em verde) dentro de um arquivo Zip juntamente com vários dos exploits que vazaram da NSA pela Shadow Brokers. Fonte: SophosLabs.

Ocasionalmente, os invasores visam servidores porque, em vez de fazer dinheiro rápido ou minerar criptomoedas de modo constante, o que eles querem é roubar os dados de valor neles armazenados. Em 2020, a Sophos descobriu um agente que visava servidores Linux usando o malware que chamamos de Cloud Snooper. Os servidores em questão estavam hospedados em um cluster de computação na nuvem, burlando a detecção com um sistema inteligente de retransmissores de mensagem que inventaram e que pegava carona nas mensagens de comando e controle em conexões HTTP rotineiras.

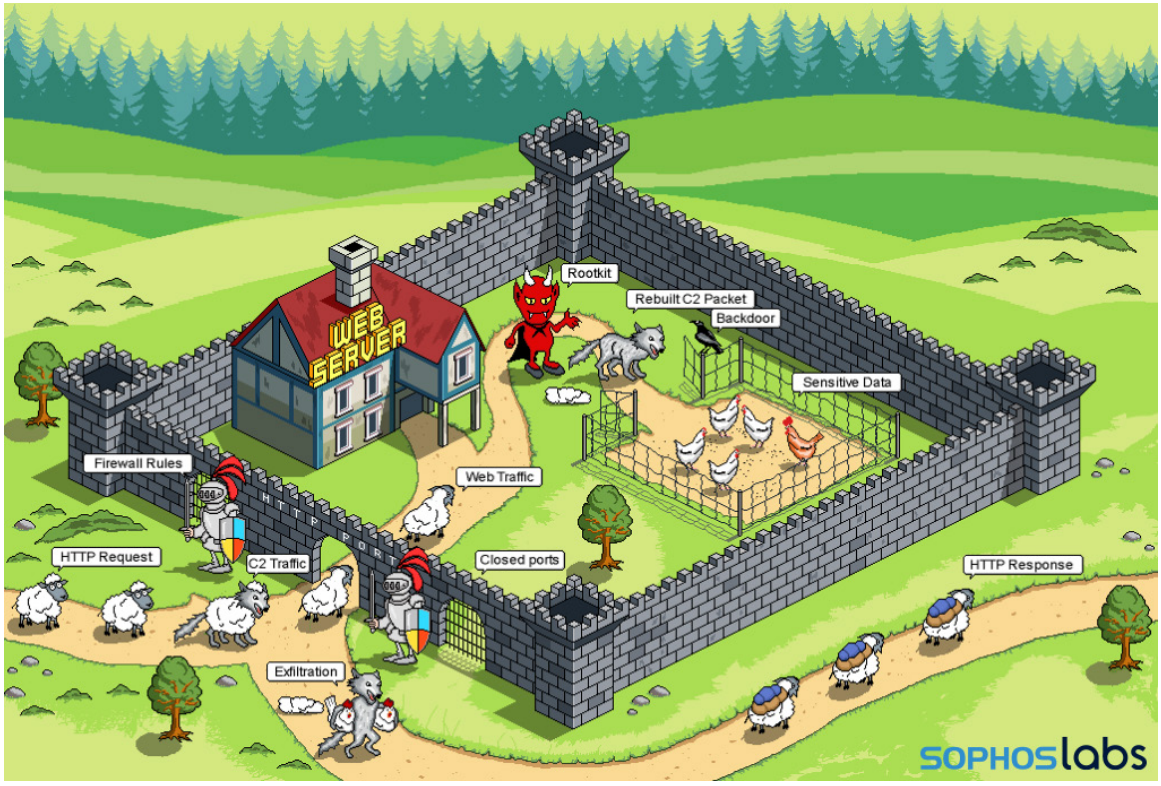


Fig.4. A metáfora do "lobo em pele de cordeiro" ilustra como o malware Cloud Snooper APT dissimulou seus comandos e exfiltrou dados na forma de solicitações e respostas de HTTP convencionais com a ajuda de uma ferramenta que monitorava o tráfego da rede e reescrevia os pacotes TCP/IP em tempo real. Fonte: SophosLabs.

Historicamente, os administradores de servidores nunca instalaram produtos de proteção de endpoint em servidores, mas com o advento desses tipos de ataque essa convenção mudou.

Subestimando malwares por sua conta e risco

Nem todos são atingidos por uma vulnerabilidade de dia zero com uma ameaça avançada persistente (APT) respaldada por um estado-nação. A maioria dos ataques envolve malwares ordinários entregues por meios convencionais – normalmente um e-mail de spam, um anexo ou link com aparência benigna e bastante incentivo à vítima para abrir o anexo. A Sophos recebe milhares de dados de telemetria todo mês sobre malwares comuns, normalmente com uma indicação de que o computador protegido por um de nossos produtos bloqueou o ataque.

Em computadores desprotegidos, onde o malware pode se expressar por completo, ele irá criar um perfil do computador visado e extrair credencias de login ou senhas salvas de sites que controlam algo de valor (normalmente, mas sem se limitar a, contas de serviços financeiros e bancários); depois enviará as informações de volta a seus operadores e aguardará por novas instruções, as quais podem chegar em alguns segundos... ou vários dias depois.

Mas não se engane com o fato de essas famílias de malwares serem ***meramente costumeiras***, deixando-se levar por uma falsa sensação de segurança. Esses cavalos de batalha maliciosos podem causar grandes problemas se conseguirem se sustentar. Como mencionado anteriormente em nosso relatório, a equipe do SophosLabs mantém uma lista de "Procurados" com analistas dedicados às famílias de malwares que teimosamente conseguem persistir. Fizemos um pequeno resumo de alguns deles.

Dridex e Zloader

Um dos tipos de malware mais comuns é o *loader*. Os loaders apresentam características que giram em torno da entrega de outra carga de malware em nome de seus operadores ou de pessoas que firmam contrato com os operadores. As famílias de malwares Dridex e Zloader são plataformas de loader bem-estabelecidas. Os invasores usam o Dridex e o Zloader para coletar informações sobre o sistema na mira e as enviam de volta aos criminosos, que vão então decidir a seu bel-prazer quais componentes ou cargas úteis eles entregarão com base nas informações que o bot enviou.

A função central do loader Dridex é contatar seu servidor de comando e controle (C2), tomar uma ou mais cargas criptografadas e implantá-las. É bastante difícil para os analistas pegarem essas cargas úteis, porque os agentes da ameaça só as distribuem de acordo com a necessidade, seja como um aplicativo de controle remoto VCN ou um proxy SOCKS. Essas cargas úteis dão aos invasores a capacidade de fazer coisas no contexto do dispositivo do usuário. Elas também permitem que os criminosos acessem recursos no sistema da vítima que não são diretamente acessíveis se partindo de seus próprios sistemas.

A lógica do lado do servidor que determina o que acontece durante uma infecção pode ser impenetrável, mas podemos inferir algumas regras, porque os bots não querem infectar computadores usados por analistas de malware. O bot envia a seus operadores uma lista dos programas instalados; se houver ferramentas de análise, ou componentes de máquinas virtuais, os bots não entregam as cargas úteis naquela máquina. No caso do Zloader, os operadores do bot disseminam o malware por meio de uma mensagem de spam; se você demorar muito para infectar o seu computador, de 8 a 12 horas após o spam ser enviado, eles param de enviar cargas.

A máquina também tem que estar superlimpa, mas tampouco pode estar muito limpa. Uma instalação simples do Windows não irá dispará-lo, tal qual uma máquina abarrotada de ferramentas.

Agent Tesla e RATicate, infostealers e RATs

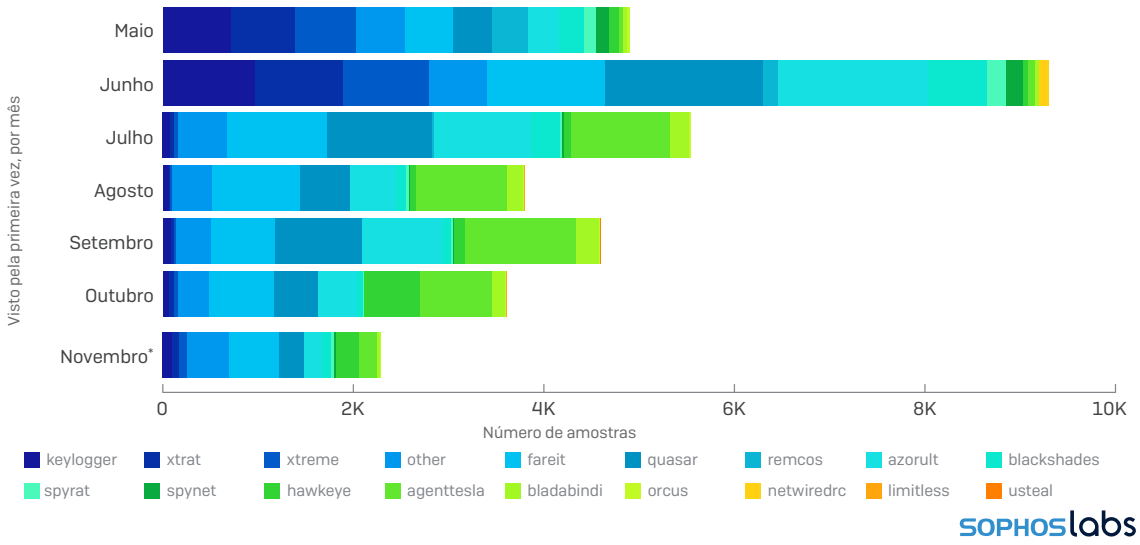


Fig.5. Executamos todas as amostras de malwares cavalo de troia de acesso remoto (RAT) recém-descobertos através do nosso sistema interno de sandbox. Esta tabela ilustra quantas novas amostras exclusivas encontramos durante um período de 7 meses, que posteriormente classificamos como uma das 18 famílias mais comuns de RAT, separadas por nome de família. * Dados de um mês parcial. Fonte: SophosLabs.

Cavalos de troia de acesso remoto, ou RATs, e infostealers estão entre os mais antigos malwares. RATs dão aos invasores a capacidade de controlar um computador infectado remotamente. Infostealers se engajam no roubo e exfiltração de credenciais, certificados e outras informações sigilosas. Duas das famílias de "Procurados" com as quais lidamos no ano passado são Agent Tesla (um infostealer) e RATicate (um RAT).

Como os loaders, os RATs geralmente também têm um mecanismo através do qual podem entregar cargas adicionais, incluindo versões atualizadas deles mesmos. Observamos o RATicate distribuindo outros malwares, inclusive o Agent Tesla. Vimos também essas famílias de RATs servidas pelos – ou se comunicando com – mesmos endereços IP ou servidores, o que sugere que algo foi compartilhado entre grupos que, em outras condições, não estariam relacionados entre si.

Desarmamento do Trickbot

Trickbot é um malware irritantemente persistente que está em cena há pelo menos quatro anos. O infame botnet foi o precursor de muitos do que hoje aceitamos como comportamentos e características comuns: por exemplo, ele se comunicava com sua infraestrutura de C2 usando TLS. O bot está implicado em vários ataques de ransomware de alto escalão, sendo por si só um exímio ladrão de credenciais.

Fig.6. O trickbot foi desarmado com uma única linha de código. Fonte: SophosLabs.

Em outubro de 2020, enquanto preparávamos este relatório, a Microsoft e o Departamento de Justiça dos EUA anunciaram que haviam capturado vários servidores e enviado um comando através do sistema de comando e controle do botnet que fez com que cerca de 90% do botnet interrompessem a comunicação com a infraestrutura de comando e controle.

Os investigadores conseguiram carregar uma configuração "envenenada" para a infraestrutura do Trickbot que todos os bots baixaram. A configuração enganou o botnet, fazendo com que acreditasse que seu principal servidor de comando e controle era a máquina infectada em que estava sendo executado. O botnet acabou por perder contato com os verdadeiros servidores C2 e não pôde mais obter cargas e instruções.

Esse esforço teve um grande impacto no operador do Trickbot, mas o mundo já espera que, lentamente, e consequentemente, ele retome sua operação normal.

Mecanismos de entrega

Existe um número limitado de caminhos que malwares ou invasores podem seguir para acessar um computador ou penetrar em uma rede. Os métodos da maioria dos ataques de malware seguem por um caminho bastante trilhado que pode incluir o uso de um e-mail contendo links a arquivos maliciosos ou um arquivo malicioso anexado, ou o invasor pode assumir um papel mais dinâmico e visar o RDP ou outro serviço vulnerável hospedado no perímetro da rede, do lado da internet pública.

RDP, o vetor de ataque Nº 1 de ransomware

O Windows Remote Desktop Protocol, ou RDP, é um serviço padrão disponível em todas as versões correntes do Windows. Como pouquíssimo esforço, o RDP oferece aos administradores de TI ou usuários de computador a capacidade de fazer login em um computador sem estar fisicamente em sua presença, o que é excelente no caso de uma pandemia, quando todos repentinamente são forçados a trabalhar de casa. Infelizmente, nos últimos três anos, os agentes de ameaças de ransomware brutalizaram (a uma velocidade estonteante) essa mesma plataforma de acesso remoto como um modo de ter acesso à base de operações das empresas e lhes causar danos de grande escala, o que se converte no pagamento de uma boa fatia dos ganhos das organizações atingidas.

Tentativas de login do RDP por honeypot

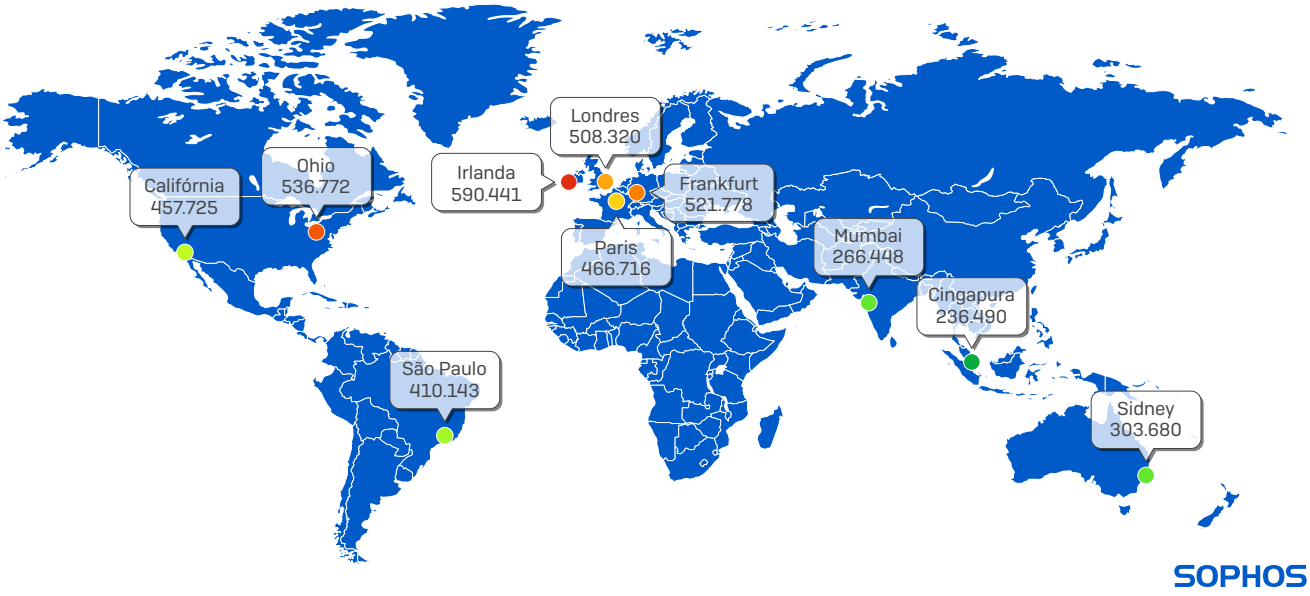


Fig.7. Distribuímos honeypots por datacenters em todo o mundo e permitimos que os invasores tentassem abrir caminho pela força bruta. As máquinas honeypot foram descobertas "organicamente", sem serem anunciadas de forma alguma. Esse mapa ilustra quantos ataques cada localidade do honeypot recebeu durante nosso um mês de testes.

O impacto do lockdown da era COVID-19 exacerbou o problema, com um número crescente de organizações e trabalhadores forçados pelas circunstâncias a depender do RDP para se manterem em operação. O principal risco aqui é que o RDP não foi destinado a resistir à fúria dos ataques que pode se originar na internet. Se a senha do RDP for fraca, fácil de adivinhar ou puder ser descoberta por força bruta através de tentativas de login automatizadas, o invasor se instala na rede e passa a explorá-la como lhe convier.

A equipe da Sophos que lida com resposta a grandes incidentes informa que o RDP se mantém entre os primeiros lugares entre as "causas primárias" dos eventos de ransomware com que se deparam. O alerta aos gerentes de TI permanece o mesmo de sempre: o RDP nunca deveria ficar voltado para a internet pública, e, sim, ser alocado entre o firewall que exige a conexão dos usuários através de uma VPN ou outro recurso zero trust primeiro – e os administradores deveriam fortalecer suas políticas de senha do Windows para exigir senhas longas e um token ou aplicativo de autenticação multifator.

Em uma pesquisa realizada antes do lockdown entrar em vigor, a Sophos instalou honeypots em 10 datacenters distribuídos mundialmente para compreender melhor quanto o problema tinha piorado. Durante um período de 30 dias, os honeypots receberam uma média de 467.000 tentativas de login do RDP – cerca de 600 por hora por localidade. A pesquisa revelou que cada honeypot recebia uma frequência de tentativas vorazes de login que aumentava gradativamente, até que finalmente tiramos o plugue da tomada.

5 nomes de usuário mais usados em todas as tentativas de login malsucedidas

NOME DE USUÁRIO	TENTATIVAS DE LOGIN MALSUCEDIDAS
administrador	2.647.428
admin	376.206
user	79.384
ssm-user	53.447
test	42.117

Fig.8. As tentativas de força bruta de um Desktop Remoto visam os nomes de usuário mais comuns no Windows, incluindo a conta padrão "administrator". Fonte: SophosLabs.

Comprometimento de e-mail empresarial e falsificação de e-mail empresarial

O comprometimento de e-mail empresarial, formalmente chamado de Business Email Compromise (BEC), é o termo usado para referir-se a um tipo específico de golpe que se concentra em uma solicitação fraudulenta de dinheiro. Em um ataque BEC, o golpista envia mensagens elaboradas de modo a parecer que foram originadas por um executivo de alto escalão da empresa, instruindo alguém em um cargo inferior a realizar algum tipo de transação financeira ou aquisição em nome do executivo. Os golpistas fazem isso falsificando a aparência dos e-mails internos (às vezes chamado de Business Email Spoofing), ou eles podem tentar assumir o controle das contas no servidor de e-mail da própria organização e usar essa conta para enviar a solicitação fraudulenta.

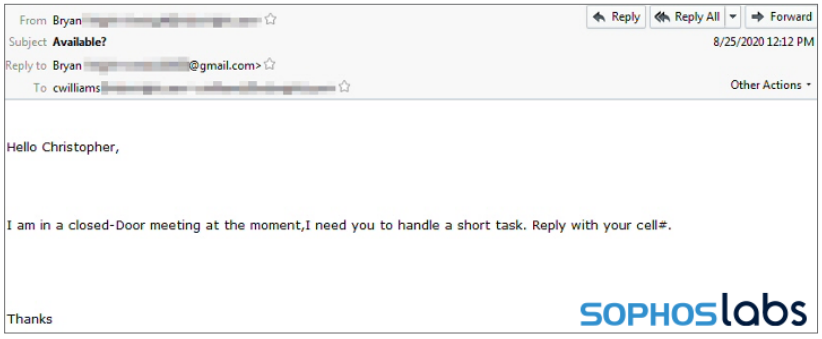


Fig.9. Neste exemplo do mundo real de uma tentativa de comprometimento de e-mail empresarial, os impostores se passam por um executivo pedindo a um funcionário que responda a uma solicitação urgente. O e-mail apresenta endereços de resposta diferentes no campo Responder para: (em uma conta Gmail) e no campo De:, um indício absoluto de que há algo de estranho – isso se o destinatário estiver atento aos campos do e-mail. Fonte: SophosLabs.

Os golpistas de BEC que se passam pelo executivo podem pedir a funcionários-alvo para comprar cartões-presente caros ou efetivar uma transação financeira de algum tipo. Em geral, os ataques são altamente adaptados aos indivíduos e às organizações. As mensagens de e-mail de BEC não se parecem em nada com uma mensagem mal-intencionada, pois não seguem o padrão das mensagens de spam: (geralmente) não contêm anexos ou links maliciosos e tentam parecer que foram originadas de dentro da organização visada, por vezes até mesmo incorporando as "assinaturas" típicas da organização ou outros elementos que possam ser familiares aos funcionários, para deixá-las mais convincentes para os destinatários do que os tradicionais spams mal-intencionados.

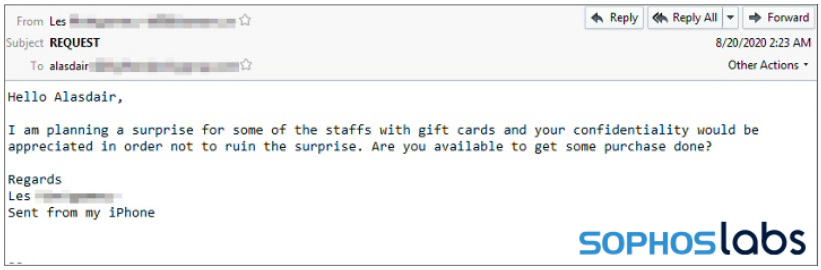


Fig.10. Após o alvo confirmar a solicitação inicial, o golpista faz o "pedido", com um pretexto que soa plausível. Fonte: SophosLabs.

Os golpes BEC depositam suas esperanças no fato de o alvo do scam (o funcionário) estar fisicamente distante do sujeito do scam (o executivo), mas dependem também da ação rápida do alvo – antes que alguém possa perceber o que está acontecendo e interrompa a compra de cartões-presente ou as transferências bancárias. Os golpistas de BEC podem preparar a mensagem para quando sabem que o executivo estará fora, a trabalho.

Esses tipos de solicitações fraudulentas geralmente envolvem uma conversação entre o impostor e o alvo. A conversa pode começar com um simples pedido para o alvo responder ao impostor e progredir em uma série de mensagens que acabaram levando a um "pedido" para fazer uma compra baseado em um pretexto que soa plausível.

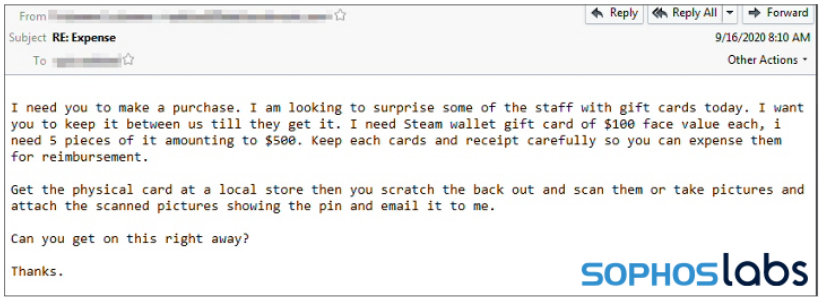


Fig.11. Em um determinado momento durante o ataque, o impostor do BEC fará a solicitação, até certo ponto plausível, de uma transferência bancária repentina a uma conta desconhecida pelo alvo do golpe. Isso oferece outra oportunidade para o funcionário prudente questionar a natureza da solicitação: por que o executivo precisa da foto do verso do cartão-presente com o PIN raspado se a ideia é dar de presente? Fonte: SophosLabs.

Nos tempos em que a maioria de nós trabalhava em escritórios, a proximidade física entre o alvo e o sujeito teria colocado o golpe imediatamente em evidência. Mas nosso atual ambiente de trabalho distribuído, onde tanto o executivo como o funcionário dificilmente estarão na mesma proximidade física que antes, diminui as oportunidades de as pessoas simplesmente caminharem até a mesa de alguém e pedir que confirme a solicitação.

Os golpes BEC existem desde antes da era da COVID-19, e com mais pessoas trabalhando remotamente, os impostores andam à espreita. Como um ataque contra as pessoas de boa índole que simplesmente querem ajudar, esse tipo de golpe é particularmente ofensivo. Se você vir e-mails como esses, confie em seus instintos e fale diretamente com o sujeito em questão, se puder, ou peça ajuda a alguém caso não consiga contatar o sujeito. Quanto mais funcionários reais se envolverem nessas solicitações, maior a probabilidade de o golpe ser descoberto antes de causar estragos.

A ciência do fatídico: uma antiga falha do Office que volta a atacar

Quando se trata de documentos do Office mal-intencionados (maldocs) e dos exploits que eles tentam implantar, os materiais antigos são usados e reusados, transitam bastante depois que a Microsoft cria uma atualização e (às vezes) ressurgem. Por anos, o SophosLabs vem rastreando como os invasores incorporam com rapidez uma ampla variedade de mutações de exploits em maldocs. Vulnerabilidades recém-desvendadas geralmente são bem-recebidas entre os criminosos que usam maldocs como ponto de partida para a entrega de uma carga de malware, isso porque nem todos instalam patches logo que são lançados, e às vezes demora um certo tempo para as empresas de segurança criarem uma "rede de segurança" para uma defesa eficaz com base no comportamento ou outras características do novo vetor.

A maioria dos maldocs que encaramos no ano passado foi construída usando ferramentas chamadas construtores, o que dá aos invasores um sistema de menus do tipo apontar e clicar que lhes permite decidir exatamente o exploit a incorporar no documento mal-intencionado. Como as ferramentas de proteção de endpoint ficam cada vez melhores em identificar exploits mais modernos, que em geral envolvem um script que foi incorporado no documento, os criadores de maldocs parecem ter mergulhado fundo para achar um bug superantigo que ajuda a ocultar macros ou outro conteúdo malicioso nos documentos.

O bug é conhecido como exploit **VelvetSweatshop**, ainda que não seja um exploit. De fato, o VelvetSweatshop foi introduzido no Microsoft Office 2003 pela Microsoft, embora não se tenha notado nenhum revés até 2013, quando as pastas de trabalho do Excel que exploravam a vulnerabilidade CVE-2012-0158 eram disfarçadas com a ajuda de uma falha. Uma planilha do Excel ou um arquivo .doc do Word marcado como "somente leitura" é simplesmente um documento protegido por uma senha padrão, e adivinhe qual é a senha padrão? VelvetSweatshop.

Este ano, vimos muitas planilhas maliciosas do Excel entregues que utilizam a técnica como uma forma de burlar a detecção de ameaças avançadas. Devido à criptografia, o conteúdo verdadeiramente malicioso estará oculto por trás de uma forte criptografia que os recursos de varredura não conseguem decodificar, tampouco conseguem verificar, a menos que haja suporte ao algoritmo mais recente utilizado pelos invasores. Devido ao uso da senha padrão, o Excel abre o conteúdo decodificado sem pedir uma senha, portanto, do ponto de vista de execução, a criptografia é transparente. Programas de segurança de endpoint adicionaram suporte a criptografia e a senha padrão, mas os criminosos continuam a encontrar algoritmos de criptografia adicionais têm a mesma funcionalidade e (ainda) não estão implementados por varreduras antivírus.

Foi uma grande surpresa descobrir um bug que, se fosse um ser humano, estaria acabando a escola. Porém não surpreende que os criadores dos construtores de documentos minados tentariam tirar proveito dele.

Segurança da informação: 20 anos em retrospectiva

Um relatório anual nos dá a oportunidade de vermos os eventos mais importantes que aconteceram no ano que passou, mas achamos que um retrospecto mais a fundo – das últimas duas décadas – nos daria mais contexto sobre como chegamos a esse atual cenário de ameaças. A virada do milênio foi um grande marco, quando a segurança da informação se tornou um ofício e uma indústria genuína. Esta linha do tempo de ameaças e eventos representa momentos de grande importância na evolução do comportamento da ameaça.

Como tanto as empresas quanto os indivíduos adotaram a internet para negócios e lazer, as grandes rede eram alvos propícios para o surgimento dos prolíficos worms – malwares de propagação automática. Cumulativamente, os worms infectaram dezenas de milhões de sistemas em todo o mundo, custando mais de US$ 100 bilhões em danos e remediação

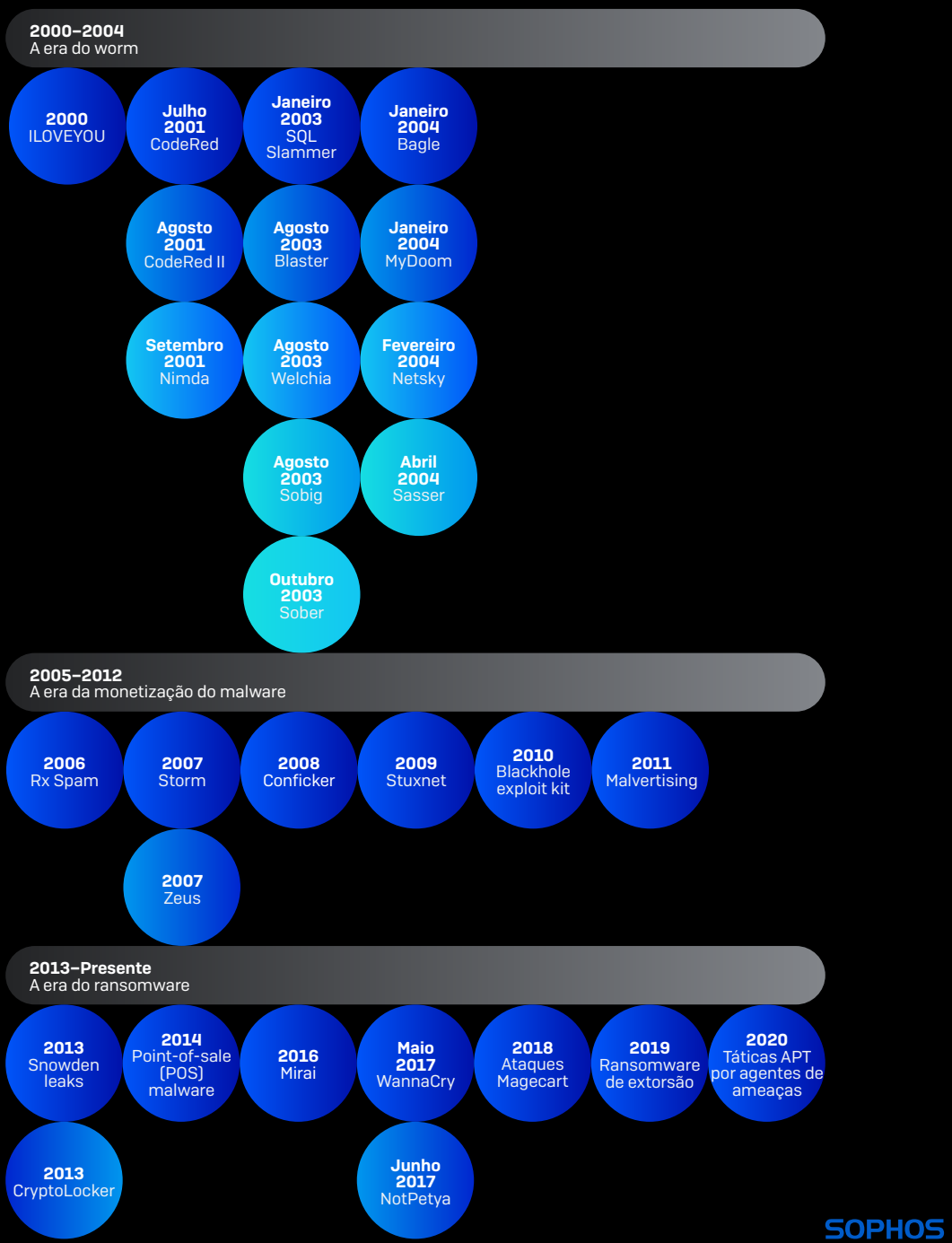


Fig.12. Fonte: Sophos

2000–2004 – A era do worm

2000 – ILOVEYOU
O worm ILOVEYOU usava um truque de engenharia social que persiste até os dias de hoje: ele chegou como um anexo de e-mail de spam e acabou infectando cerca de 10% de todos os computadores Windows conectados à internet.

Julho de 2001 – CodeRed
Assim chamado em referência ao sabor da bebida Mountain Dew que seus descobridores estavam bebendo "na hora do crime", o CodeRed usa uma vulnerabilidade de estouro de buffer no IIS para se disseminar e desfigurar websites. Um mês depois, seguiu-se uma versão atualizada que instalava um backdoor nos computadores em rede.

Agosto de 2001 – CodeRed II

Setembro de 2001 – Nimda

Janeiro de 2003 – SQL Slammer
Com apenas 376 bytes, o Slammer explorou o estouro de buffer nos aplicativos de bancos de dados Microsoft. Dobrando suas infecções a cada 8,5 segundos, o Slammer colocou abaixo grande parte da internet em apenas 15 minutos.

Agosto de 2003 – Blaster
O Blaster foi criado pela engenharia reversa de um patch da Microsoft dois meses antes do primeiro Patch Tuesday. Ele explorava uma vulnerabilidade de estouro de buffer no serviço RPC do Windows XP e sistemas 2000 e lançava um ataque DDoS contra o windowsupdate.com se o dia do mês fosse maior que 15 ou se o mês fosse setembro ou posterior.

Agosto de 2003 – Welchia

Agosto de 2003 – Sobig

Outubro de 2003 – Sober

Janeiro de 2004 – Bagle

Janeiro de 2004 – MyDoom
Estima-se que 25% de todos os e-mails enviados em 2004 originaram-se com o worm MyDoom, o qual se autoenviava por e-mail para novas vítimas de modo prolífico e se engajava em um ataque de negação de serviço (DDoS).

Fevereiro de 2004 – Netsky

Abril de 2004 – Sasser

2005-2012 – A era da monetização do malware

Até cerca de 2005, os incidentes de malware eram esboçavam curiosidade ou ruptura. O malware Botnet, criado para ações furtivas e lucrativas, dominou. Essa era também viu o início do chamado spam pharmacy. A explorações de vulnerabilidade de software tornaram-se componentes-chave do malware, o qual permitiu o malvertising. Onde quer que houvesse potencial para ganho financeiro, os criminosos virtuais estavam lá para explorar a oportunidade.

2006 – Rx Spam
O que era um mero aborrecimento (ou uma forma de propagar worms), passou a ser um negócio lucrativo de venda de medicamentos sem receita, na sua maioria falsificados e anunciados por meio de spam. Estima-se que os golpistas da farmácia tenham feito bilhões de dólares vendendo medicamentos que com uma simples consulta médica poderiam ser obtidos.

2007 – Storm

2007 – Zeus

2008 – Conficker
Conficker infectou rapidamente milhões de computadores mundo afora, mas não causou muito estrago. Continuamos sem saber qual a verdadeira finalidade do worm, mas milhares de hosts permanecem infectados até hoje, e, rotineiramente, o tráfego de varredura do Conficker é detectado como parte da "radiação de fundo" da internet.

2009 – Stuxnet
Stuxnet foi uma das primeiras armas a visar um sistema físico: centrífugas para refinamento nuclear usadas pelo Irã para enriquecer urânio O legado que perdura do Stuxnet é que ele abriu permanentemente as portas para o uso de malware de estado-nação como uma arma de guerra.

2010 – Blackhole Exploit Kit
Exploit Kits – kits de ferramentas que visam vulnerabilidades de software – unem diferentes partes do ecossistema do crime cibernético. Crimeware como um Serviço surgiu quando os criadores do Blackhole Exploit Kit começaram a oferecer seus serviços.

2011 – Malvertising

2013–Presente – A era do ransomware

O ransomware foi o que causou mais impacto nesta era. Enquanto worms, banking trojans, malvertising e spams persistem, nada se equipara à força destrutiva de um ransomware. Os danos estimados causados por ataques de ransomwares nos últimos sete anos chegam à casa dos trilhões de dólares. O ransomware também é, muito provavelmente, a primeira forma de malware ligada à morte de um ser humano. Além disso, muitas das ameaças de hoje acabam entregando um ransomware e, como os exploit kits, deu um impulso ainda maior ao ecossistema do crime cibernético.

2013 – Snowden leaks

2013 – CryptoLocker
Durante a sua curta existência, o CryptoLocker deu aos futuros criminosos uma fórmula vencedora ao casar duas tecnologias existentes: criptografia e criptomoeda. O cenário das ameaças mudou para sempre como o CryptoLocker, e o estremecimento que ele causou é sentido até hoje. Três meses após seu lançamento, a carteira de bitcoin usada pelo CryptoLocker continha quase US$ 30 milhões.

2014 – Malware Point-of-sale (POS)

2016 – Mirai

Maio de 2017 – WannaCry
WannaCry, o híbrido de ransomware e worm mais difundido já visto, demonstrou (novamente) como um lapso em um patch pode ter terríveis consequências. Ele operava com exploits roubados da NSA e lançados a público pelo Shadow Brokers. Os ataques forçaram a Microsoft a lançar atualizações fora de banda de produtos sem suporte.

Junho de 2017 – NotPetya
NotPetya mutilou algumas das maiores empresas de entrega e logística do mundo, registrando danos de mais de US$ 10 bilhões. Algumas das empresas ainda não se recuperaram plenamente.

2018 – Ataques Magecart

2019 – Ransomware de extorsão
Em um ataque contra a cidade de Johannesburgo, África do Sul, os criminosos por trás do ransomware Maze foram os primeiros a explorar o uso da extorsão. Eles não apenas criptografaram e roubaram os dados, mas também ameaçaram publicar os dados roubados se as empresas não pagassem. Essa tática foi copiada por muitas outras quadrilhas de ransomware como uma autodefesa contra os backups de qualidade de suas vítimas.

2020 – Táticas APT por agentes de ameaças
A adoção de táticas e ferramentas de estado-nação, que começou nos últimos dois anos, se consolidou em 2020. Quadrilhas de profissionais do crime cibernético utilizam ferramentas sofisticadas, como o Cobalt Strike, para criar efeitos devastadores; já outros grupos (Dharma) estão fazendo o pé de meia com kits de ferramentas do tipo aponte e clique, um grande auxílio aos novatos.

COVID-19 COMO MULTIPLICADOR DE FORÇA DOS ATAQUES

Com o novo coronavírus, a COVID-19 afetou drasticamente cada um dos aspectos da segurança virtual. Os invasores sentiram-se incitados a atacar a nova força de trabalho que se ergueu nos lares. Um nível já bastante elevado de ansiedade e medo que permeia a esfera pública foi exacerbado apenas por ondas de campanhas de spam, ransomwares que visavam instituições enfraquecidas ou destituídas pelo momento ou sociedades civis que se encontravam sob pressão financeira, e qualquer outra forma de obter dinheiro de modo fraudulento e lucrar da escassez de qualquer coisa, de EPI a papel higiênico.

O lar é o novo perímetro

O normal acabou em março de 2020, quando os profissionais que podiam trabalhar remotamente, e os estudantes em praticamente qualquer grau, foram mandados para casa em uma tentativa desvairada de conter a envergadura da COVID-19 e aliviar a pressão nos hospitais superlotados. De repente, estávamos trabalhando em casa e morando no trabalho.

Muitas pessoas tiveram dificuldade para aceitar o novo normal: você não vai ao escritório, o escritório vem a você. Surge assim a necessidade repentina de serviços de acesso a VPN e autenticação multifator. Chromebooks se tornam raridades. O Zoom passou por um crescimento evolutivo de dez anos em um período de dois meses. Em meio a tudo isso, a Microsoft, Adobe, Apple e Google lançando atualizações e patches de manutenção para uma infinidade de plataformas.

O aumento em e-mails de scam sobre COVID-19 e coronavírus

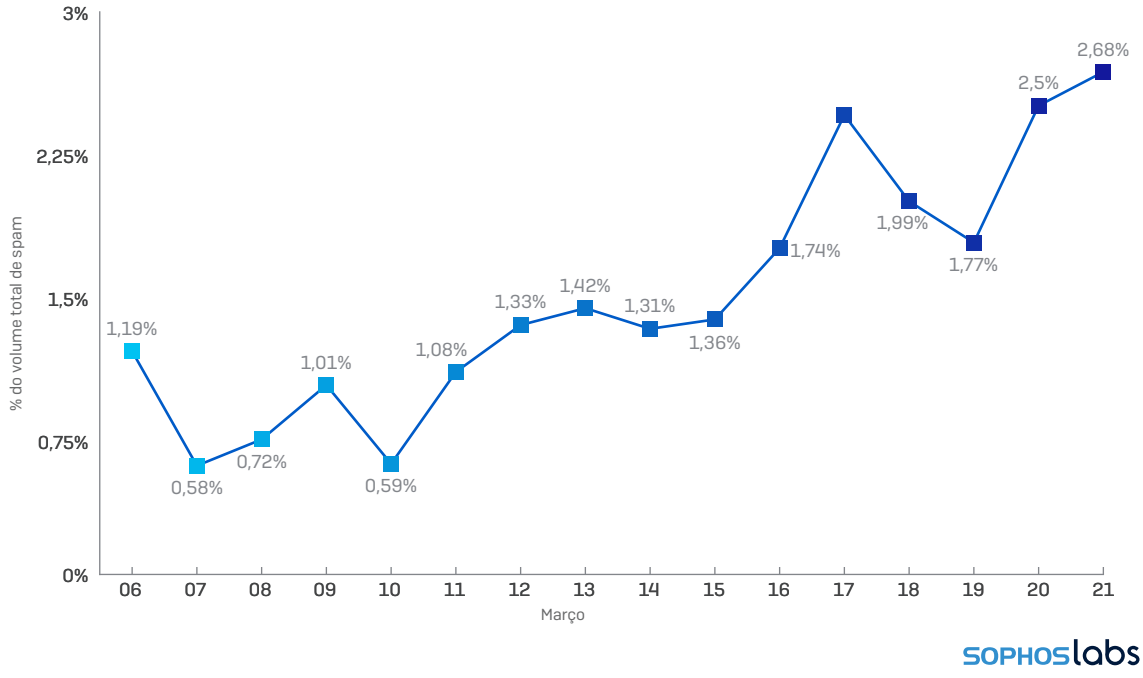


Fig.13. Mundialmente, uma parte significativa dos e-mails de spam mencionavam COVID-19 ou coronavírus nas semanas que se seguiram ao lockdown. Fonte: SophosLabs.

A COVID-19 fez de nós o nosso próprio departamento de informática, gerenciando patches, atualizações de segurança e resolvendo problemas de conectividade que nos impedem de participar de reuniões – ou os estudantes de participar das aulas virtuais. A procura por microfones, fones de ouvido, luminárias e proteção mais leve e mais segura para redes e endpoints entrou em surto. Isso sem falar nos cursos rápidos para jovens e crianças em phishing, spam, trolls online, bullying cibernético e malwares disfarçados de cópias grátis do seu game favorito, pronto para jogar.

Não tem sido fácil, e continuamos longe de operar como operávamos em fevereiro de 2020, mas muitas pessoas começam a ver que o novo normal pode, de certa maneira, ser uma melhora. Mais empresas decidiram manter o trabalho remoto mesmo após o término do lockdown, mesmo dada às pessoas a possibilidade de regressar ao escritório se assim desejassem, o que trará um grande benefício ao meio ambiente e à qualidade de vida das pessoas.

Conforme o perímetro do espaço de trabalho se estende e se expande para englobar maiores volumes da força de trabalho em suas localidades remotas, as circunstâncias acentuaram a seriedade com que olhamos para nossas redes domésticas como nossa última linha de defesa. O modem na entrada de casa passou agora a ser o perímetro da rede. Precisamos repensar completamente como oferecer uma estrutura de defesa com mais afinco.

Crimeware como um serviço

Tente pensar nos criadores de malwares como uma forma de startup de software. Inicialmente desconexos, os criadores bem-sucedidos acabam conquistando seguidores fiéis. Podem existir tantos modelos de negócios para softwares maliciosos quanto para softwares legítimos.

O termo "crimeware" é intencionalmente abrangente: alguns criadores de malwares – ou de ferramentas que possibilitam que o malware seja entregue com facilidade ou que seja melhorado com novos recursos – não vendem seus produtos imediatamente, mas usam licenças, do mesmo modo que você compraria uma licença de uso de 1 ano do Adobe Creative Suite. A essa classe de modelo de negócios chamamos "crimeware-como-um-serviço" (CaaS), a qual parece estar prestes a se tornar o novo normal.

Um dos exemplos mais notórios de um malware CaaS é o Emotet. O cavalo de troia que entrega esse spam já se encontra entre nós há anos, parecendo girar em torno de uma experiência tranquila para os pretensos criminosos. O Emotet é uma classe de malware coletivamente chamada, entre os pesquisadores de segurança, de loaders. O Emotet existe essencialmente para colocar outro malware no computador de uma vítima. Ele efetua seu trabalho através de uma rede sofisticada que distribui e-mails de spam minados a grandes volumes de alvos.

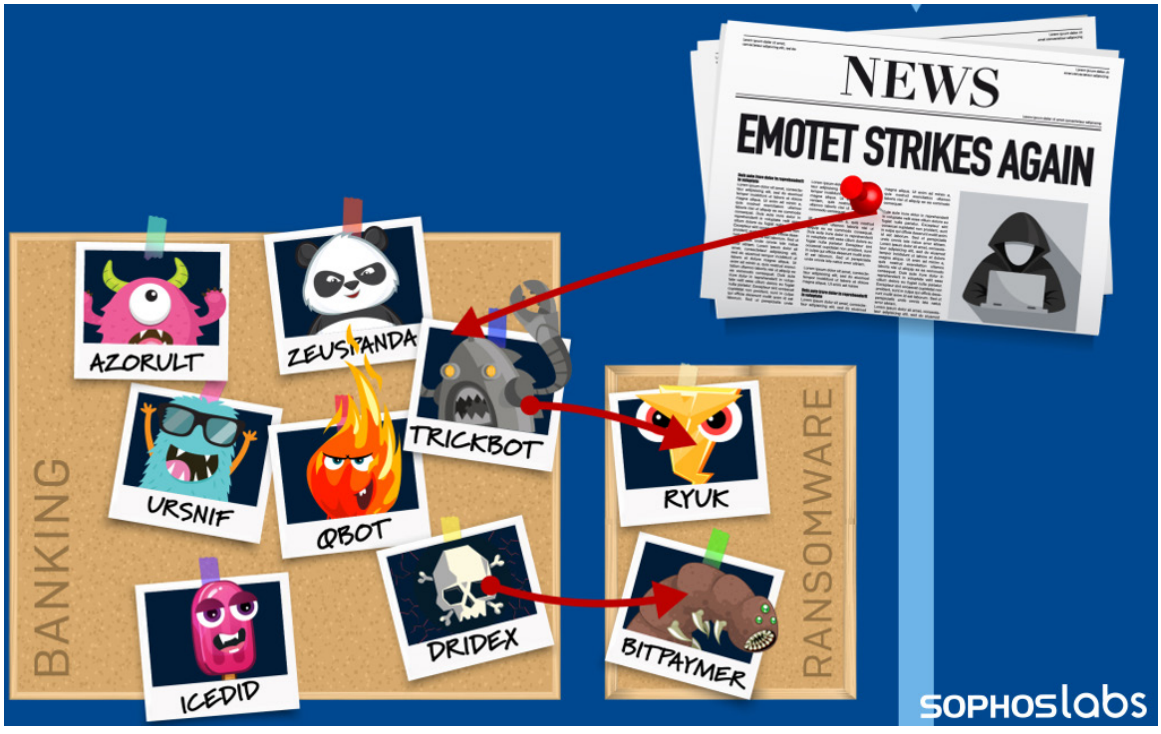


Fig.14. Fonte: SophosLabs.

Contudo, o Emotet passou por dois episódios negros este ano. O malware se manteve em comunicação com seus servidores C2 por um período de quase cinco meses, durante o qual os e-mails de spam que normalmente distribuíam ataques evaporaram completamente. Misteriosamente, os e-mails de spam que distribuíam o Emotet voltaram em julho.

O ransomware Dharma é outro malware CaaS que vale mencionar. Diferentemente de seus caros comparsas, o Dharma mantém um valor de resgate baixo e fixo. O resgate segue o modelo de negócios do Dharma: um ransomware com rodinhas, para os criminosos aspirantes em início de carreira. Basicamente, esses criminosos pagam uma taxa de assinatura para obter cargas úteis dos criadores do Dharma, depois dividem o produto dos ataques com eles.

Como os invasores se ramificando em especialidades e subespecialidades, a impressão que temos é de que o modelo de negócios sob o qual os criminosos operam com contratados, autônomos e afiliados independentes não dá mostras de que desaparecerá.

Spams, scams e promessas quebradas

Os lockdowns pelo mundo foram acompanhados por uma enchente de mensagens fraudulentas de golpes fomentadas por e-mails de spam. Nos tempos de outrora, as campanhas de spam mais eficazes traziam em um senso de urgência que fazia os destinatários agirem a favor da mensagem. Esse é um truque psicológico bastante conhecido, porque se você demorar uns segundos a mais pensando sobre o conteúdo da mensagem de spam, provavelmente se dará conta de que é falsa. Se o golpista lhe incutir o medo, você reagirá antes de pensar, e cairá na armadilha.

A COVID-19 já deixou tudo mundo a ponto de bala, portanto os golpistas não precisaram se esforçar muito para isso.

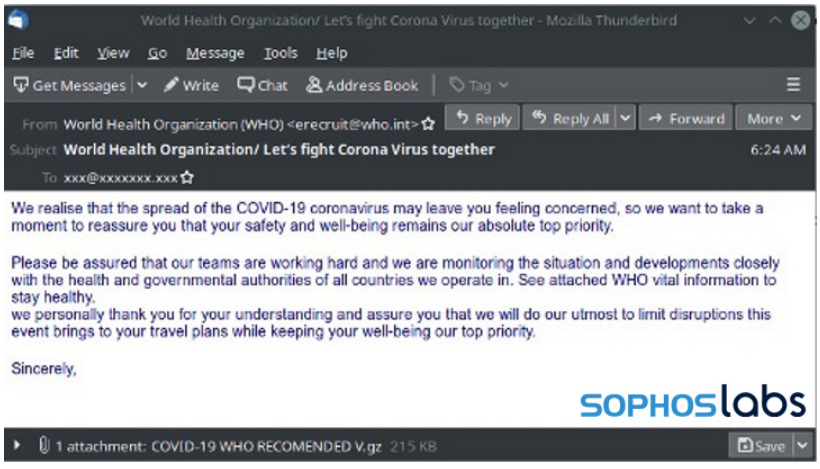


Fig.15. Fonte: SophosLabs.

Algumas semanas em lockdown e decidimos dar uma olhada mais de perto em outro fenômeno que se intensificava: o registro de domínios. Em semanas as pessoas estavam registrando milhares de novos nomes de domínio por dia que continham diferentes combinações das strings *COVID-19*, *Corona* ou *vírus*.

Domain	First Seen	Nameserver	Ns Ip
coronavirusshaquilleoneal.com	2020-03-14 07:00:38	ns-cloud-b1.googledomains.com	216.239.32.107

SOPHOSlabs

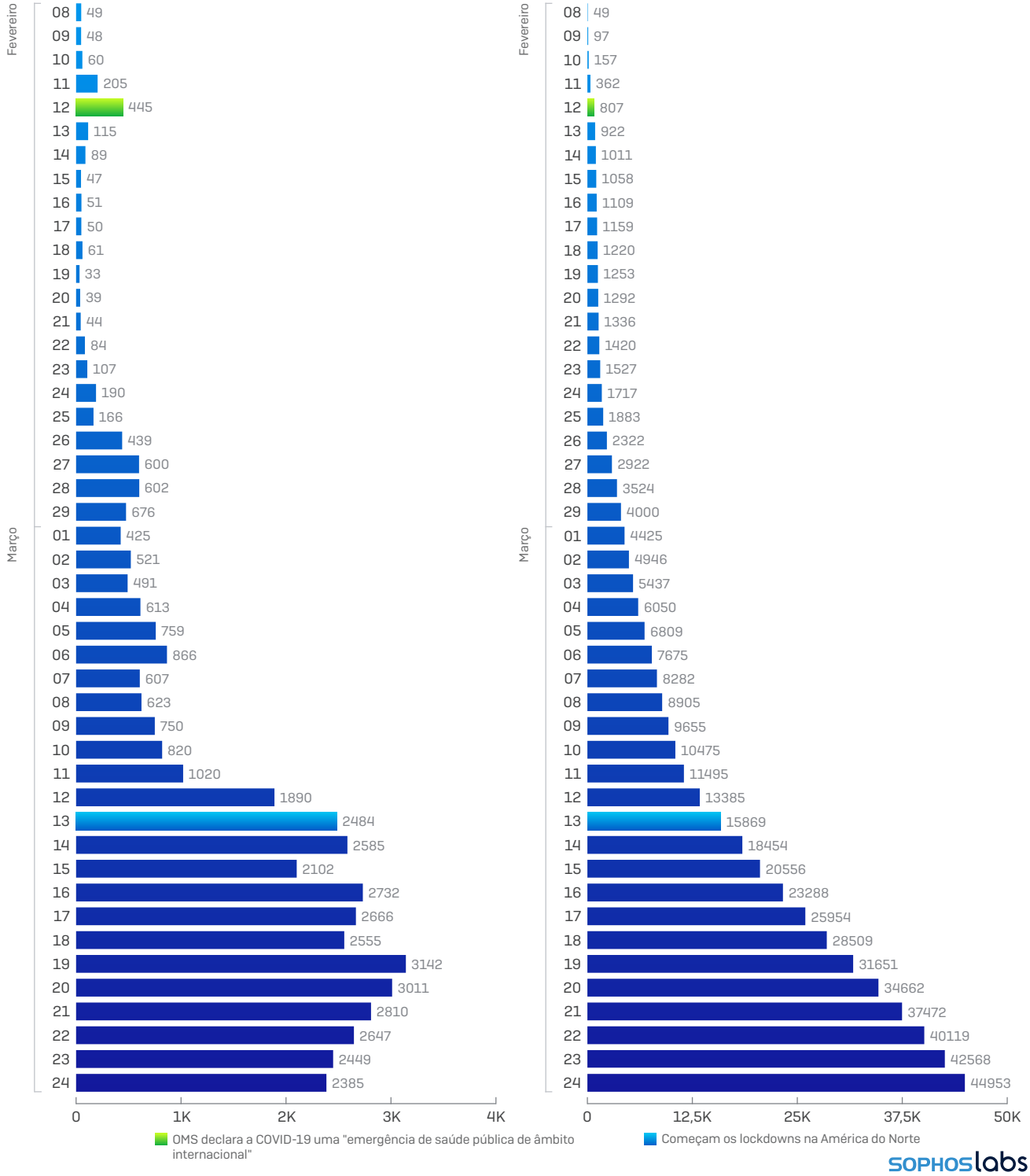
Fig.16. Fonte: SophosLabs.

Alguns dos sites obviamente eram piada, já outros eram confusos e semelhantes àqueles usados por autoridades de saúde locais e nacionais legítimas.

Também saímos no encalço de domínios e subdomínios relacionados com COVID-19 em logs de transparência de certificado TLS. Os logs de transparência de certificado são úteis para rastrear subdomínios que têm seus próprios certificados TLS – informação que não aparece nos dados brutos do registro do domínio – e nomes de domínio.

Novos registros do domínio COVID, por dia a data

Total de novos nomes do domínio COVID, até



SOPHOSlabs

Fig.17. Durante os primeiros meses da crise da COVID-19, as pessoas registraram milhares de domínios e licenciaram pelo menos o mesmo tanto de certificados TLS por dia cujos nomes continham a string "COVID-19" ou "corona". Fonte: SophosLabs.

Novos certificados TLS por mês com nomes de host "COVID-19" ou "Corona"

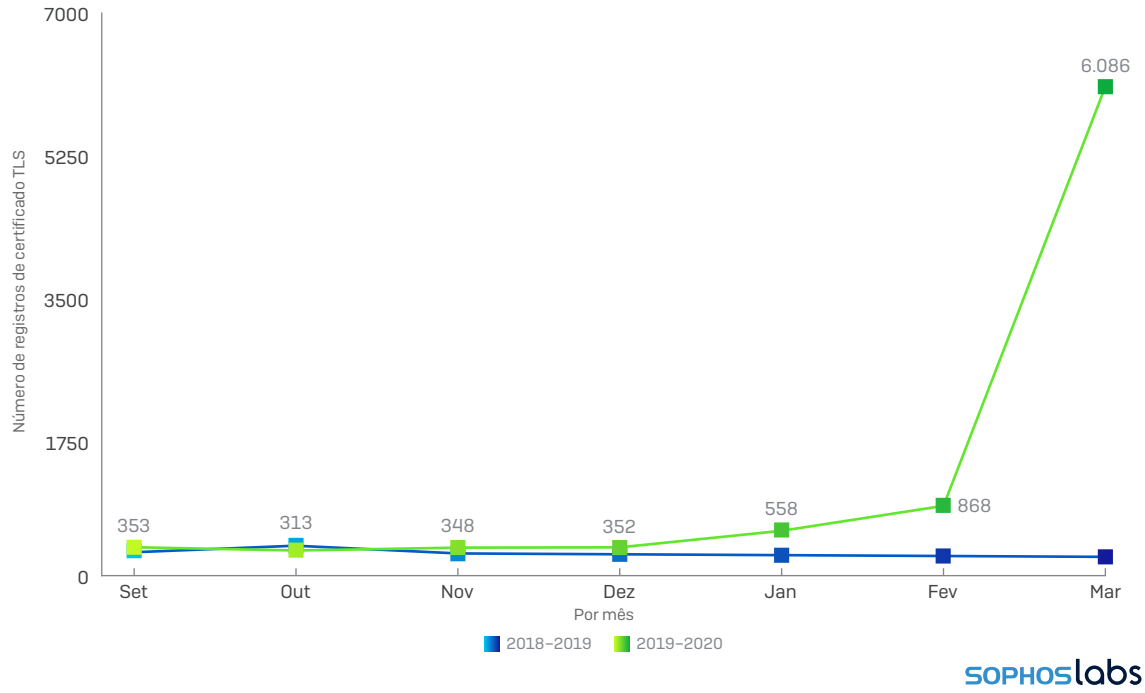


Fig.18. Registro de certificados TLS que se referem à pandemia tem seu pico ao mesmo tempo que os registros de domínio. Fonte: SophosLabs.

Vimos uma média de mais de 200 solicitações de certificado por domínios COVID-19 por dia em março, e a taxa continuou a subir nos meses subsequentes. Em junho, a média havia chegado a 625 por dia. Em outubro, essa taxa atingiu seu pico: 951 novos certificados TLS eram solicitados diariamente.

A maioria desses domínios mantém sua legitimidade, enquanto outros domínios continuam estacionados e sem conteúdo – um sinal de que o registrador está deixando o "domínio maturar", reservando-o para verificações futuras de reputação.

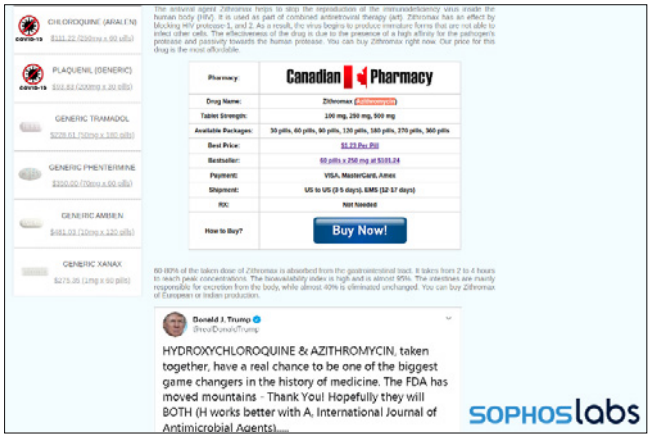


Fig.19. Até mesmo as fábricas de medicamentos irregulares não resistiram à tentação e colocaram à venda o milagre da cura no Twitter, chegando a usar postagens de tweets em suas propagandas.
Fonte: SophosLabs.

Uma pequena porcentagem (abaixo de 1%) foi identificada como estando associada com phishing ou malware. Muitas são efêmeras, com nomes de hosts que não podendo mais ser resolvidos depois de apenas um dia.

O trabalho remoto salienta a importância da computação na nuvem segura

Quando o lockdown da COVID-19 começou, em março de 2020, as pessoas e os escritórios deram início a uma transição rápida e inédita que se estende até hoje. O modo como trabalhamos, vamos à escola, participamos de eventos e conferências e nos entretemos pode ter mudado para sempre, e a computação na nuvem foi um elemento essencial para essa rápida evolução, porém com muitos desafios.

O excesso no provisionamento de permissões de acesso, a visibilidade limitada a informações e recursos na nuvem, e a falta de auditoria podem tornar os ambientes de nuvem mais vulneráveis a ameaças virtuais, e um malware é tão mau para a nuvem como para qualquer outro ambiente computacional. Por exemplo, o criptojacking é um problema crescente na nuvem. Os processos de criptomineração nos sistemas de computação de alta demanda são suficientemente danosos quando executados em máquinas físicas – além de subir a conta de eletricidade –, e criam um efeito colateral ainda mais danoso quando executados em instâncias na nuvem: a vítima é faturada pelo provedor da nuvem pelo ciclos de CPU consumidos por suas estações de trabalho virtuais realizando altos cálculos, necessários para extrair alguns míseros centavos em criptomoeda.

Ademais, muitas forças de trabalho remotas e dispersas foram atingidas por ataques de ransomware, em que criminais bloquearam a infraestrutura da nuvem da mesma forma que fazem com máquinas físicas. Afinal, um ransomware pode criptografar um armazenamento de objeto ou unidade de disco virtual com a mesma facilidade que um armazenamento físico. Organizações cuja infraestrutura de nuvem é atacada por um ransomware podem acabar pagando não apenas pela conta de ciclos de CPU criptografando dados, mas também pelo resgate.

Organizações que sofreram incidentes de segurança no ano passado

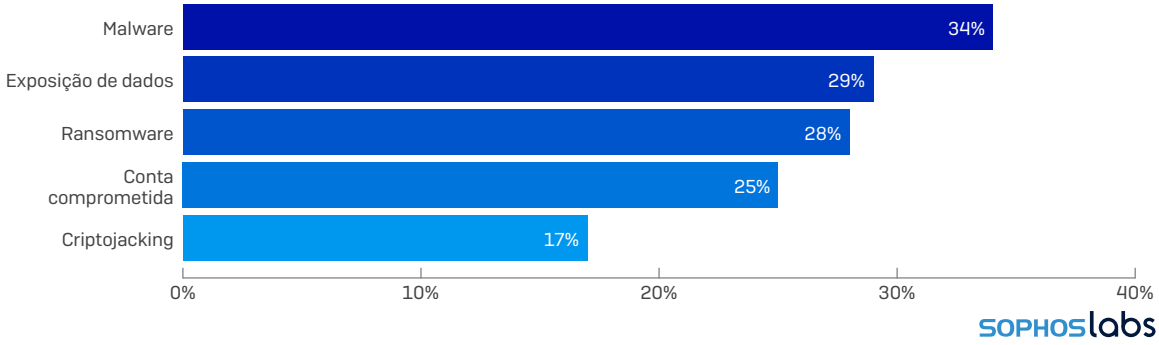


Fig.20. Em nosso Relatório de Segurança da Nuvem de 2020, a Sophos entrevistou mais de 3.500 profissionais de TI sobre suas experiências com o uso da nuvem e constatou que muitos dos problemas de segurança que empesteiam as redes físicas passaram para as redes virtuais. Fonte: SophosLabs.

No lockdown, os departamentos de TI precisavam de uma forma de suprir um helpdesk virtual com os mesmos recursos que o faziam antes dos muitos escritórios fecharem. As grandes mudanças que a COVID-19 exigiu veio em ondas.

Nas primeiras semanas depois que o lockdown começou, a primeira onda – uma onda de acesso – começou a tomar forma. Milhões de trabalhadores, de repente, se viram impossibilitados de ir para o trabalho, e a necessidade de acessar recursos dentro do ambiente organizacional aumentou aceleradamente a demanda por redes virtuais privadas (VPN), enquanto outras funcionalidades de acesso zero trust exauriram seus recursos. Além de VPNs, as organizações perceberam que precisavam adicionar novos firewalls e outros equipamentos de segurança, e implantações de sistemas unificados de gerenciamento de ameaças modernos complementaram os rudimentares firewalls de 3 camadas oferecidos pelos serviços de nuvem.

No mundo pré-COVID-19, as VPNs se acostumaram ao uso moderado, pois o número de trabalhadores locais superava os trabalhadores remotos e em trânsito. Março passou e chegamos a maio e junho e, para esses trabalhadores, a VPN se transformou em um meio de contato vital (se não no único meio) que mantém as organizações em operação.

Mas essas organizações rapidamente também se deram conta de que os funcionários não deveriam usar dispositivos pessoais domésticos para acessar a VPN, e o abastecimento de novos notebooks criou um novo desafio para organizações que já enfrentam as necessidades de computação da força de trabalho agora distribuída. Sem máquinas físicas suficientes naquele exato momento, as organizações se voltaram para a interminável fonte de recursos das máquinas virtuais para atender à necessidade de um espaço de trabalho computacional seguro. Isso deu início à segunda onda – a onda do desktop virtual.

Conforme mais e mais funcionários faziam a transição para um desktop corporativo virtual, a mudança para hospedar esses desktops na rede fazia sentido em termos práticos e financeiros, mas continuava a exigir proteção.

De repente, os departamentos de TI tinham centenas ou milhares de VMs empregadas e precisavam de ferramentas de visibilidade para poder controlá-las e configurar com segurança a sua federação crescente de estados na nuvem de servidores virtuais, desktops virtuais e outros serviços de rede – a onda do gerenciamento de rede.

Cronograma de ataque

Fig.21. Um ataque de criptojacking que investigamos começou quando um programador incorporou inadvertidamente suas credenciais da nuvem em uma linha de código em um repositório público.
O invasor descobriu e usou as credenciais para atacar, usando as APIs nativas do provedor de rede – e colocou centenas de instâncias de VM para coletar bitcoins. Ao mesmo tempo, automatizou os recursos nas instâncias para dificultar sua terminação. Mais tarde, revogou o acesso a outros usuários legítimos.
Fonte: SophosLabs.

A era da COVID-19 foi marcada por grandes transformações em cada um dos aspectos da vida humana, inclusive como muitos de nós trabalhamos. Em uma recente pesquisa realizada pela Reuters, 97% dos CEOs e CTOs entrevistados disseram que os lockdowns aceleraram a transição a novas tecnologias. Mas em tempos de orçamentos apertados e incertezas, quase um em cada três CTOs disse que sua função era implementar essas mudanças com a melhor relação de custo e benefício possível.

No recente Relatório de Segurança da Nuvem da Sophos, constatamos que a maioria dos incidentes de segurança envolvendo a computação em nuvem se resumiram em duas principias causas primárias: roubo ou phishing de credenciais, ou erros de configuração que levavam a violações. Sete de cada dez dos mais de 3.700 profissionais de TI entrevistados para o relatório disseram que a infraestrutura de rede à qual davam suporte tinha passado por uma violação nos 12 meses que antecederam à pesquisa.

O que significa o CCTC para uma resposta rápida a ameaças de grande escala

Fig.22. Fonte: Sophos.

Cerca de uma semana depois do início do lockdown da COVID-19, o diretor científico da Sophos, Joshua Saxe, faz um chamado global por voluntários. A brigada de incêndio virtual rapidamente passou a ser a CCTC (COVID-19 Cyber Threat Coalition), uma organização que conta com mais de 4.000 membros a serviço de um objetivo único: empenhar um esforço especial no contragolpe a qualquer tipo de ameaça ou engenharia social que tente se aproveitar da apreensão do público em relação à COVID-19, por nome ou inferência.

"Eu não sou bombeiro, portanto não saberia como apagar o fogo de um prédio em chamas, mas posso ajudar uma equipe trabalhando nas defesas de uma infraestrutura crítica, como hospitais", disse Nick Espinosa do CCTC, analista de segurança e podcaster sediado em Chicago.

Esse foi um esforço absolutamente necessário. Desde os primeiros sinais do período de lockdown, o invasores disseminaram spams, malwares e uma diversidade de outras ameaças que faziam referência, de uma forma ou de outra, ao medo: o novo linguajar pandêmico. Como citado no relatório principal, em um certo ponto as pessoas estavam registrando milhares de novos domínios com palavras como COVID-19, corona ou CoV no nome, diariamente. A Sophos rastreou domínios conectados a certificados TLS com as mesmas strings de texto que nos dados do certificado e encontrou outros milhares deles.

Aumento da associação ao COVID-19 Cyber Threat Coalition

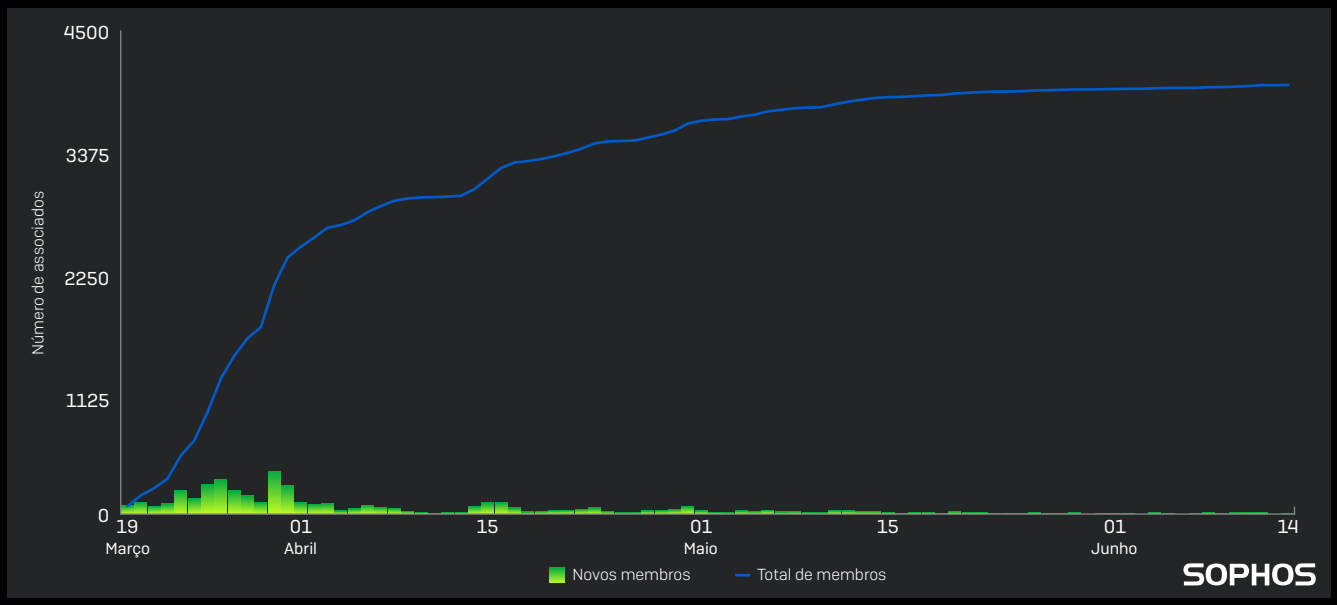


Fig.23. Fonte: Sophos.

Devido à natureza única que a ameaça da COVID-19 representa, spams maliciosos que usurpam a crise global são particularmente conspícuos e ofensivos. "Presenciamos uma explosão de hackers criminosos usando a COVID-19 como chamariz", disse Espinosa. Campanhas de spam espiralaram vertiginosamente, em que os impostores criaram mensagens com aparência de comunicados oficiais da Organização Mundial da Saúde, do CDC dos Estados Unidos, do NHS do Reino Unido, de empresas farmacêuticas ou de autoridades nacionais de saúde de outros países.

Os analistas se depararam também com referências à COVID-19 em strings dentro de binários e usadas como variáveis nos chamados living-off-the-land, LOLscripts.

Os participantes do CCTC compartilharam amostragens e inteligência sobre todos os modos de incidentes usando um canal no Slack configurado às pressas. Caótica a princípio, rapidamente a organização formou uma estrutura rudimentar. "Tantas pessoas se juntaram, e traziam tantas informações", disse Espinosa.

O produto do CCTC, o resultado final, é um feed de inteligência que traz indicadores de comprometimento recém-obtidos. O feed é gratuito, para qualquer um. Esses IoCs complementam as tecnologias defensivas já em uso, sem considerar fornecedores. Quando o CCTC formou a parceria com a Cyber Threat Alliance, os fornecedores de segurança que participavam do CTA amplificaram o efeito protetor da inteligência de ameaça do CCTC ingerindo e defendendo contra aquelas ameaças.

A rápida coalescência dos profissionais de segurança, compartilhando um objetivo comum, foi comovente, disse Espinosa. "Talvez parecêssemos um bando de perdidos", disse ele, "mas o grupo se organizou rápido". O estabelecimentos da plataforma de compartilhamento do CCTC significa que qualquer um que precise responder a uma pandemia como a COVID-19 no futuro não precisará reinventar a roda e poderá responder às ameaças mais bem preparado – uma metáfora da saúde por analogia ao sistema imunológico.

NÃO BAIXE A GUARDA: AMEAÇAS ATRAVÉS DE PLATAFORMAS NÃO TRADICIONAIS

Vivemos em um mundo cercado por dispositivos computadorizados que não se parecem com computadores ou servidores: roteadores, telefones celulares, firewalls, TVs Smart, caixas de streaming, caixas VoIP, câmeras e campainhas com câmera, unidades NAS, algumas marcas de eletrodomésticos e assim por diante.

Mas simplesmente porque não se parecem com computadores tradicionais não significa que não podem ser usados e brutalizados da mesma forma.

Malware Joker do Android aumenta em volume

Os usuários de Android se viram em meio a uma corrida armamentista entre o Google (proprietária da plataforma Android e de seu principal Google Play Store) e os criadores de malwares que queriam que seus malwares fossem listados para download no Google Play Store. O Google gastou anos desenhando um sistema para inspecionar códigos fonte dos aplicativos Android submetidos para inclusão no Google Play Store, que busca porções de código que indicam uma intenção maliciosa ou um resultado indesejável para o usuário de Android. Desenvolvedores de aplicativos de malware tiveram que trabalhar duro para escapar das verificações de código do Google Play Store.

Joker, também chamado de Bread, é um SMS premium e um aplicativo fraudulento de cobrança, um dos exemplos de maior sucesso de uma família de malwares que evoluiu a ponto de driblar essas verificações de código. O Google removeu milhares desses aplicativos maliciosos modificados pelo Joker do Google Play Store desde o ano passado, quando os pesquisadores o descobriram, inicialmente. Apesar da quantidade de esforços que pusemos para nos livrar do malware, o Joker continua a voltar.

O Joker aparece disfarçado de diferentes de aplicativos: utilitários e ferramentas, papéis de parede, tradutores e serviços de mensagem – vários clones de aplicativos populares. Lembre-se, o Joker pode, na verdade, estar incorporado em um aplicativo com aparência e funcionamento exatamente iguais ao da versão real de praticamente todos os seus aplicativos. Os aplicativos Joker têm uma pequena rotina de código de malware incrustada em um dos aplicativos de biblioteca de terceiros que os criadores rotineiramente compilam em seus aplicativos por razões legítimas e variadas.

Há alguns motivos por que o Joker consegue burlar com êxito as verificações de código de segurança do Google Play Store:

1. Os aplicativos maliciosos usam a ofuscação, da simples substituição de uma string aos complexos empacotadores comerciais, para retardar a análise e enganar o Google Play Store.
2. Quando o "programador" do Joker lança o aplicativo, ele não contém absolutamente nenhum código malicioso. Isso estabelece o histórico de que o aplicativo está limpo quando entra no Google Play Store. Somente mais tarde é que o código aparece no aplicativo, em uma atualização.
3. O aplicativo decodificava sua carga útil em tempo de execução ou faz o download dinamicamente, posteriormente.

O malware Joker usa código nativo (JNI) em vez do DEX, que é mais comum. O código nativo usa C para programação, o que desacelera a análise de códigos maliciosos. Comparativamente, o DEX, sendo uma variação de código Java, é muito mais fácil de descompilar em algo legível aos olhos humanos. O malware usa esse código JNI para enviar mensagens SMS, para fazer dinheiro e como uma mensagem só de ida para contatar sua rede de comando e controle. O uso de JNI e sinalização fora da banda pela rede telefônica em vez da internet pode ajudar o Joker a burlar as varreduras dex automatizadas que não falam JNI.

Está claro que o Joker tem uma vantagem na batalha contra o código automatizado do Google nos novos aplicativos, e não vemos sinais de que o Joker diminuirá sua presença em 2021, e ainda poderá ter a companhia da concorrência muito em breve.

Novembro, 2020

Anúncios e PUAs cada vez mais parecidos com malwares

Propagandas maliciosas (malvertising) continuam sendo a maior fonte de ameaças a um grande número de dispositivos. Recentemente, investigamos duas tendências correntes em ameaças de malvertising que estão fora do império dos ataques de malware: golpes de suporte técnico usando páginas da web "bloqueadas pelo navegador" e anúncios que visam dispositivos móveis que são vinculados a aplicativos "fleeceware" ou fraudulentos. A Sophos os classifica como ataques "alerta falso" – malvertisements que tentam amedrontar as suas vítimas e levá-las a ações que enriquecerão os golpistas por trás dos ataques.

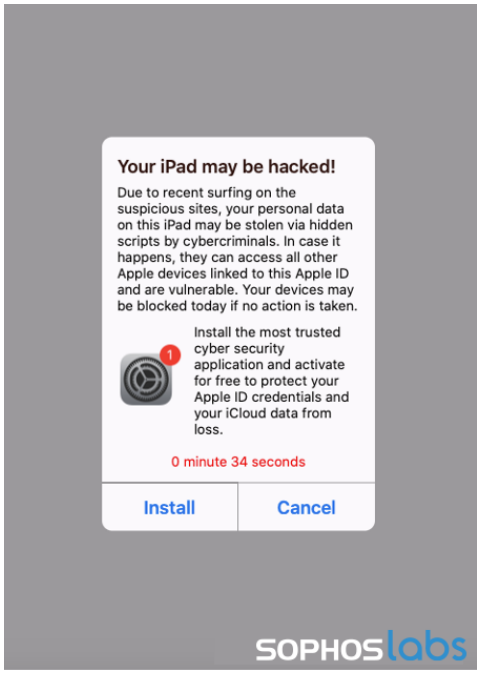


Fig.24. Fonte: SophosLabs

Golpes de suporte técnico são tipicamente tentativas de levar as possíveis vítimas a fornecer acesso remoto a seus computadores e então convencê-las a adquirir um software e serviços de suporte técnico a preços exorbitantes, ou obter seus dados de cartão de crédito para fins fraudulentos. Enquanto no passado muitos desses golpes se respaldavam nas chamadas diretas de telemarketing, vários operadores de scam mudaram para o modelo "pull", usando propagandas maliciosas na web que tentam convencer o usuário que seu computador foi bloqueado por diferentes motivos e instruindo-o a chamar os próprios golpistas.

Para chegar a isso, os impostores lançam kits de websites contendo scripts criados para dificultar a navegação para fora da página – incluindo variações do "evil cursor" (fazendo parecer que o ponteiro do mouse está apontando para algo que na verdade não está, ou tornando-o invisível) e ataques "infinite download" que esgotam o navegador – enquanto tentam se assemelhar a um alerta da Microsoft ou da Apple. Alguns dos kits que encontramos exploravam um bug que a equipe de segurança ofensiva do SophosLabs descobriu no Firefox no começo do ano, enquanto outros executavam ataques semelhantes em outros navegadores – todos eles disseminados através de anúncios "pop-under" maliciosos na web.

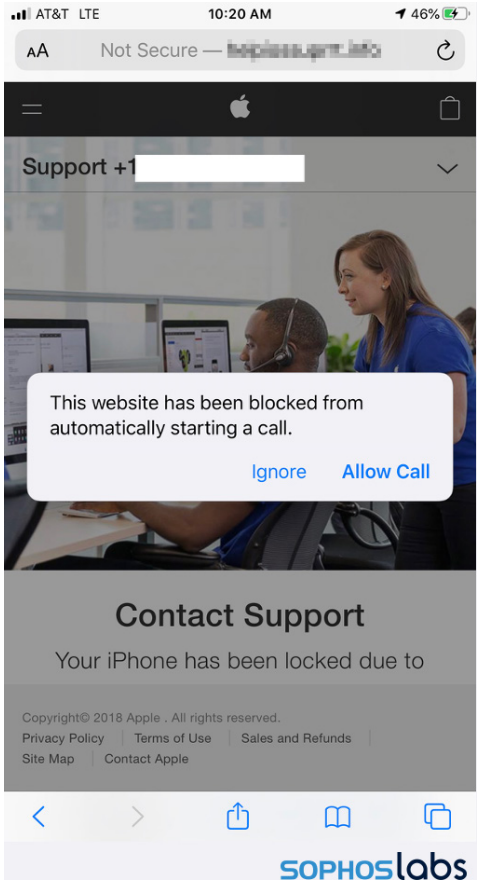


Fig.25. Fonte: SophosLabs

A mesma estrutura de rede que suporta esses ataques em navegadores no PC e Mac também serve aos golpes de suporte técnico e os alertas falsos que se vinculam a aplicativos móveis potencialmente indesejados, inclusive aplicativos que se dizem ser serviços de rede virtual privada e ferramentas de "limpeza" anunciadas como removedores de malware, com taxa de assinatura incluída (em alguns casos, um verdadeiro malware do Android). A Sophos encontrou um grupo de servidores de campanhas publicitárias que entregavam esses anúncios, usando um software comercial desenvolvido por um programador russo especificamente para executar tais campanhas.

Usando suas próprias forças contra você: criminosos brutalizam as ferramentas de segurança

Alguns ataques não envolvem malwares, ou aguardam para entregar o malware bem no final do ataque, em vez de utilizarem apenas as ferramentas nos sistemas operacionais que são executadas nos computadores em toda a rede. Outros criminosos aproveitam-se do poder das ferramentas usadas por dois grandes segmentos da indústria: resposta a incidentes e teste de penetração.

A comunidade de segurança da informação definiu o estilo dos ataques que envolvem muito pouco malware ou nenhum malware, mas que se aproveitam dos componentes existentes no sistema operacional ou pacotes de softwares populares, como living-off-the-land (LOL). Esses ataques geralmente envolvem um ou mais métodos de automação na forma de scripts nativos, como PowerShell, arquivos em batch ou scripts VBScript, coletivamente conhecidos por LOLscripts. Os invasores usam esses LOLscripts para executar sequências de comandos usando binários (aplicativos) living-off-the-land, coloquialmente chamados de LOLbins.

Originalmente desenhado pelo segmento "red team" da indústria, o software incorpora o método "bring your own attack". Nesse caso, os invasores implementam e usam as ferramentas de segurança vendidas nas lojas e que são comumente usadas pelos administradores de rede e pelo pessoal de testes de penetração. Incluem ferramentas como Cobalt Strike e elementos da estrutura Metasploit, criada para ser usada em avaliações de segurança e testes técnicos.

Conjunto de ferramentas do agente de ameaça Netwalker na matriz ATT&CK

ACESSO INICIAL	EXECUÇÃO	ESCALONA-MENTO DE PRIVILÉGIO	EVASÃO DE DEFESAS	ACESSO A CREDENCIAIS	DESCOBERTA	MOVIMENTO LATERAL	IMPACTO
Exploit Tomcat	Scripts PowerShell	CVE-2020-0796	Carga sem arquivo	mimikatz	SoftPerfect Network Scanner	psexec	Ransomware Netwalker
Exploit Weblogic	psexec	CVE-2019-1458	Eset AV Remover	Mimidogz	NLBrute	Teamviewer	Ransomware Zeppelin
E-mail de phishing		CVE-2017-0213	Gordon's Eset, restauração de senha	Mimikittenz		Anydesk	Ransomware Smaug
		CVE-2015-1701	Security Agent Uninstall Tool de Trend Micro	Windows Credentials Editor			Exfiltração de dados
			Desinstalação Microsoft Security Client	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

SOPHOSlabs

Fig.26. O conjunto de ferramentas usado pelo agente da ameaça envolvido nos ataques do ransomware Netwalker fazia uso de uma panóplia de códigos fonte abertos, freewares e utilitários comerciais em diferentes pontos durante o ataque. Fonte: SophosLabs.

Essas ferramentas são valiosas para os invasores for motivos diversos: Como frequentemente são usadas em uma posição legítima (para auditoria ou melhorar a segurança do sistema), pode ser difícil para as soluções de antivírus ou segurança detectarem ferramentas ou atividades por completo. Como tal, a Sophos precisa se respaldar mais profundamente nos estudos sobre comportamentos de LOLscripts para identificar possíveis atividades maliciosas. Logicamente, é mais fácil usar algo que já foi criado do que criar suas próprias ferramentas do zero.

Ainda que o uso de LOLscripts e reverse shells não fosse novidade no ano passado, em 2020 eles se tornaram um elemento onipresente em ataques complexos de invasão por ransomware operados manualmente. De fato, tanto a quantidade como a variedade das ferramentas de ataque que observamos durante os ataques parecem estar aumentando.

Killchain de ferramentas de ataque RaaS Dharma

ACESSO INICIAL	EXECUÇÃO	ESCALONAMENTO DE PRIVILÉGIO	EVASÃO DE DEFESAS	ACESSO A CREDENCIAIS	DESCOBERTA	MOVIMENTO LATERAL	EXFILTRAÇÃO	IMPACTO
Spray de credenciais RDP	PowerShell	CVE-2019-1388	Desativa a proteção contra malware	mimikatz	PCHunter	Objetos de política de grupo	Emailer de screenshot de PowerShell	Ransomware Dharma
Credenciais RDP roubadas	WMI	CVE-2018-8120	Revo Uninstaller	Remote Desktop Passview	Process Hacker	Desktop Remoto	TOR	
	AutoIT	CVE-2017-0213	IOBit Uninstaller	LaZagne	GMER	Gerenciamento remoto WinRM	dropmefiles[.]com	
	Linha de comando/RDP			NLBrute	Advanced IP Scanner			
				Hash Suite Tools	NS2.EXE			

SOPHOSlabs

Fig.27. Fonte: SophosLabs.

A grande diversidade de ferramentas de ataque varia de aplicativos disponíveis no mercado a repositórios GitHub de código aberto, com funcionalidades que podem incluir:

- Estruturas de comando e controle do tipo botnet
- Geração e ofuscação de shellcode
- Evasão de antivírus e detecção em sandbox
- Extração de senha ou credencial
- Kerberoasting (persistência de manutenção de privilégios Domain Admin)
- A habilidade de forçar abruptamente as senhas usadas por uma variedade de serviços
- Exfiltração de dados do sistema

A maioria desses tipos de ferramentas contém cargas benignas ou nenhuma carga em seu estado "original de uso", mas, no passado, fomos capazes de detectar várias dessas ferramentas se engajando em atividades maliciosas com base nas informações contextuais adquiridas por meio de nossas tecnologias de detecção comportamental.

De acordo com a nossa telemetria, as dez ferramentas de ataque que vimos mais comumente são, em ordem de uso: Metasploit, BloodHound, mimikatz, PowerShell Empire, Cobalt Strike, Veil Evasion, Hydra THC, Enigma, Nishang e Shellter. Metasploit foi, de longe, a ferramenta mais vista, aparecendo com cerca de duas vezes mais frequência que a ferramenta seguinte mais comum de ataque, BloodHound.

Ultimamente, a Sophos acompanha o uso de 99 diferentes ferramentas de ataque – e parece pouco provável que vejamos uma parada nos ataques, com os invasores continuando a tirar proveito dessas ferramentas muito bem elaboradas por todo ano de 2021.

Epidemiologia digital

Qual a porcentagem de dispositivos de computação que é infectada por malwares não detectados? Qual a porcentagem de execuções de linha de comando que é executada por adversários não detectados? Qual a porcentagem de e-mails de phishing direcionados que não é detectada? Como esses valores mudam em função da indústria, geolocalização e postura de rede?

Fazer essas perguntas é o mesmo que perguntar, "qual a porcentagem de pessoas infectadas com COVID-19?" em um contexto em que muitas dessas pessoas nunca farão o teste do vírus, sabendo-se ainda que os testes realizados podem apresentar um número elevado de falsos positivos e falsos negativos.

Em outras palavras, é difícil.

Apesar desses desafios, os epidemiologistas respondem perguntas cruciais sobre a COVID-19 diariamente. Infelizmente, os pesquisadores de segurança cibernética falharam em relação aos ataques cibernéticos. Temos uma grande defasagem em ferramentas, técnicas e procedimentos de operação sob circunstâncias incertas se nos compararmos com os epidemiologistas. E para isso não tem desculpa! É hora de criarmos as nossas próprias ferramentas para entendermos a natureza da ameaça que enfrentamos, providenciar dados precisos àqueles que nos defendem e tomar decisões sobre para onde dirigir nossos esforços.

Para ajudar nessa missão, a Sophos AI embarcou em um projeto para desenvolver um conjunto de modelos estatísticos inspirados pela epidemiologia para estimar a prevalência de infecções por malware no total. Combinamos um robusto pipeline para a coleta de dados de 100 milhões de endpoints com um conjunto de métodos estatísticos Bayesianos que nos permite lidar com essas difíceis perguntas de modo a traçar uma imagem completa do desempenho de nossos modelos "no campo".

Por exemplo, considere esta questão: "Quantos malwares estão em realidade afetando nossos clientes semana após semana, e quantos deles conseguimos detectar?"

Se já soubéssemos quais arquivos eram malwares e quais eram benignos para todos os arquivos, já estaríamos satisfeitos! Infelizmente, temos dois problemas.

1. Não sabemos, de fato, a verdade por trás de nenhum arquivo especificamente – todo produto de endpoint deixará escapar pelo menos alguns malwares, e o ocasional falso positivo (um arquivo normal que é sinalizado como malware) será inevitável
2. O balanço entre arquivos benignos e malignos é predominantemente a favor dos benignos, de modo que muito provavelmente não conseguiremos chegar a um valor com análises manuais – precisamos fazer uma análise profunda dos milhares de arquivos que o nosso produto de endpoint rotula como benignos para encontrar apenas um que seja malicioso

Para tratar desses problemas, recorremos à estatística Bayesiana. Colocando em termos extremamente simples, criamos um modelo "generativo" de dados: um programa matemático que pode supor parâmetros ("quantos malwares existem, realmente?") e reverter essas suposições em simulações de quantas detecções de endpoint poderemos ver. A partir disso, tentaremos diferentes suposições, veremos quais simulações correspondem à realidade observada e trabalharemos de modo reverso para encontrar valores plausíveis para o parâmetro em que estamos interessados.

Por exemplo, imagine que tenhamos 2.000 detecções de endpoint e uma boa estimativa de taxas do modelo de taxas de verdadeiros e de falsos positivos para uma semana em particular. Podemos simular mundos com taxas de malware de 0%, 2%, 5%, e assim por diante, e ver os prognósticos da simulação para as detecções de endpoint; se virmos algo perto das 2.000 detecções para algumas taxas de malware, aquele será, talvez, um valor plausível.

Fig.28. Proponha uma taxa de malware, faça amostragens, consulte se a simulação corresponde à realidade observada, registre as taxas que correspondem e repita. Fonte: SophosAI.

Você pode reiterar esse processo milhões de vezes para construir uma distribuição de valores plausíveis por taxa de malware, e porque usamos uma abordagem Bayesiana, barras de erro são "incorporadas" na estimativa. Em nosso exemplo, o modelo acha que o valor mais provável para "qual porcentagem de arquivos é malware?" é apenas um pouco acima de 3%, mas qualquer valor entre 2,75% a cerca de 3,35% é bastante plausível.

Assim que tivermos uma melhor noção desse número – quantos arquivos por cento têm a probabilidade de ser malware nos endpoints do cliente –, as falhas em detecções e falsos positivos ficarão relativamente mais fáceis de deduzir. Se examinarmos os dados do nosso sistema de detecção de malware baseado em ML com Deep Learning de uma semana em maio (sem nenhuma opção comportamental, heurística ou baseada em assinatura ativava), podemos lançar uma matriz de verdadeiros e falsos positivos e negativos, e completar a nossa imagem do desempenho do modelo. Nesse caso, vemos que, enquanto temos alguns falsos negativos, o número de falsos positivos é baixo, tendendo a zero, enquanto o número de positivos é alto e tende a 161.000 (o número total de resultados positivos na amostragem). Observando a escala, vemos que as três quantidades são tolhidas pelo número de verdadeiros negativos – arquivos benignos que nosso Machine Learning rotulou como benignos.

Nossa ferramenta inspirada na epidemiologia nos permitiu estimar, e até encontrar, as agulhas no nosso palheiro de arquivos PE.

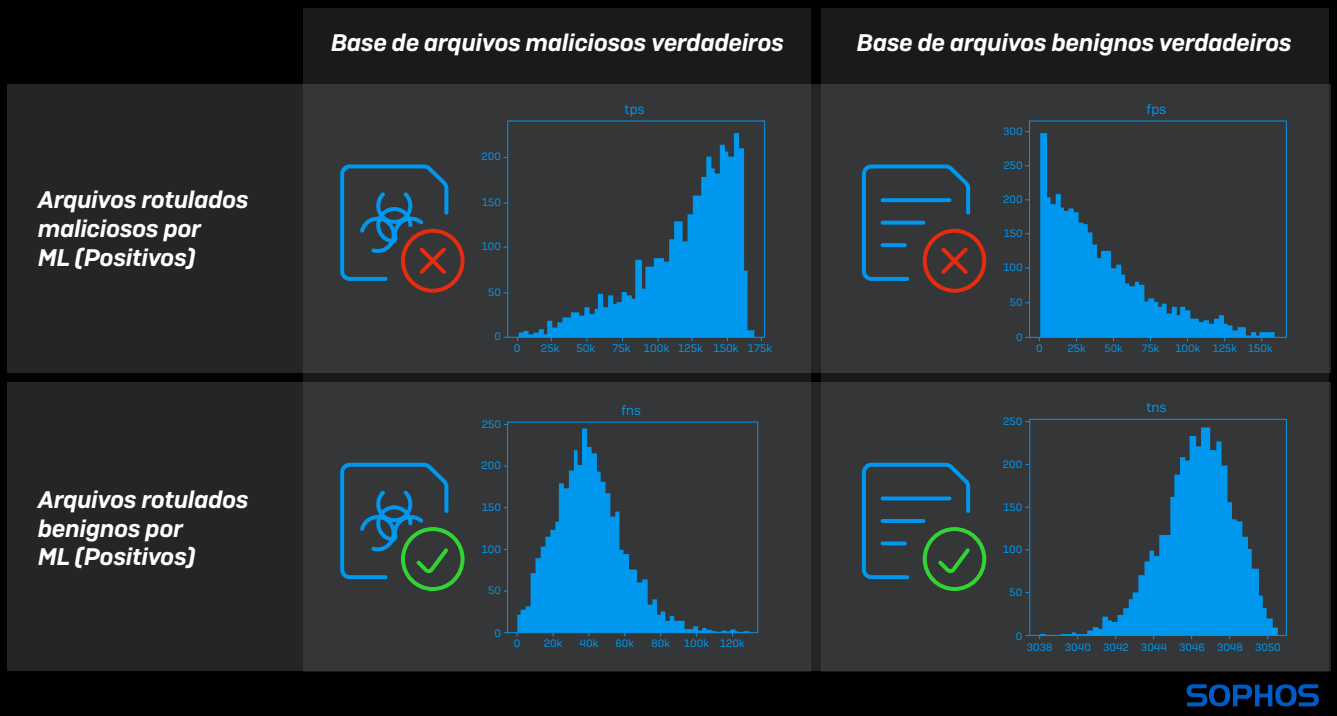


Fig.29. Análise de um modelo de Machine Learning de verdadeiros e falsos positivos no início de maio de 2020. Fonte: SophosAI.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

20-11-01 PTBR (DD)

SOPHOS