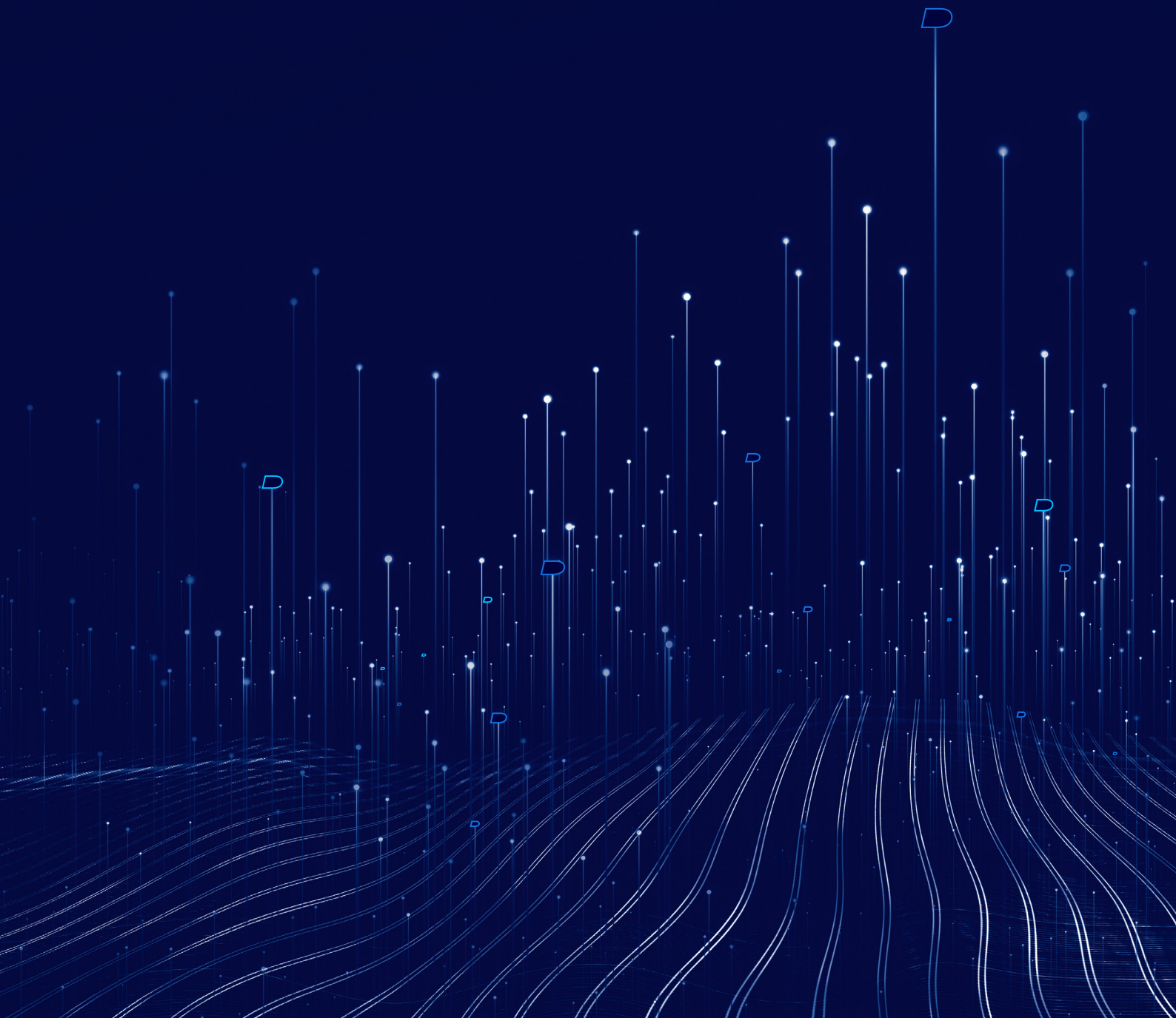
BlackBerry. Intelligent Security. Everywhere.

RELATÓRIO DE AMEAÇAS 2022



SUMÁRIO

INTRODUÇÃO

O Relatório de Ameaças BlackBerry 2022 não é uma simples retrospectiva dos ciberataques de 2021. É uma visão geral de questões que afetam a segurança cibernética no mundo, direta e indiretamente. Abrange elementos de violações em infraestruturas críticas, inteligência artificial (IA) adversarial, intermediadores de acesso inicial (IABs), gerenciamento de eventos críticos (CEM), detecção e resposta estendidas (XDR) e outras questões que moldam o ambiente de segurança atual.

Este relatório analisa os principais eventos de segurança de 2021 e como podem moldar o cenário de cibersegurança futuro.

Este relatório abrange temas enfrentados por pessoas e organizações no mundo inteiro. Como sempre, representa apenas uma peça no quebra-cabeça de segurança geral. Nossa meta é aprimorar a abordagem de segurança global, compartilhando nossas informações, previsões e experiências com todos. Para concretizar isso, o relatório analisa os principais eventos de segurança de 2021 e como podem moldar o cenário de cibersegurança futuro. Aprofunda-se nos problemas de cibersegurança que enfrentamos atualmente e oferece aos leitores informações adicionais e contexto para que elaborem sua própria análise detalhada.

Mas os leitores que esperam o nosso detalhamento anual dos 10 principais ataques de malware observados pela BlackBerry no ano passado não ficarão desapontados. Nem aqueles que aguardam ansiosamente a revisão do ano de resposta a incidentes (RI), atualizações legislativas anuais sobre cibersegurança e previsões de curto prazo. Muitas das seções de que os nossos leitores gostaram em relatórios de ameaças BlackBerry anteriores voltaram. Além disso, este ano, abordamos ataques à cadeia de suprimentos, novas linguagens de programação perigosas, segurança no Metaverso, computação quântica, campanhas de ransomware e outros temas em ascensão.

A fluidez dos ciberataques modernos pode exigir que as organizações repensem com frequência suas abordagens de cibersegurança e considerem novas opções. Devem avaliar constantemente novas tecnologias e abordagens que possam superar o desempenho das soluções antivírus (AV) legadas, incluindo IA com prevenção em primeiro e adoção de arquitetura Zero Trust. Assim, o Relatório de Ameaças BlackBerry 2022 oferece sugestões de estratégias de cibersegurança e tecnologias que poderiam ter prevenido as maiores falhas de segurança do ano anterior.

Esperamos sinceramente que as informações contidas neste relatório ajudem a proteger os usuários e a manter a segurança das organizações em 2022 e no futuro.

RESUMO EXECUTIVO

Os eventos cibernéticos mais amplamente divulgados de 2021 envolveram ataques de ransomware a empresas de infraestrutura crítica e tecnologia. O grupo de ameaças de ransomware REvil atacou a Acer, a JBS Foods e outras empresas, enquanto o DarkSide paralisou a Colonial Pipeline e o Avaddon invadiu a AXA. Em resumo, o alcance e o sucesso de vários grupos de ameaças no ano passado, principalmente contra empresas do setor privado consideradas parte da infraestrutura nacional, foram inquietantes. Os governos responderam aos ataques. Países do G7 e aliados da OTAN colocaram a cibersegurança como prioridade na agenda de políticas públicas. O presidente dos EUA, Joe Biden, promulgou uma ordem executiva sobre "Melhoria da Segurança Cibernética da Nação" e o Departamento de Justiça estabeleceu uma Força-Tarefa de Ransomware e Extorsão Digital.

Com o passar do ano, uma vulnerabilidade de dia zero do Microsoft® Exchange Server deu origem a uma crise quando o grupo HAFNIUM explorou a falha. Outros agentes de ameaças aproveitaram rapidamente a oportunidade, fazendo engenharia reversa do patch e visando organizações em todo o mundo. A rápida proliferação de ataques no estilo HAFNIUM reforçou a importância de que pessoas e organizações mantenham os softwares atualizados. No entanto, atualizar softwares como uma prática reativa não salva a vítima inicial de um ataque – também conhecida como "cordeiro sacrificial". Isso faz com que muitas organizações busquem abordagens de segurança alternativas, como Zero Trust, XDR e IA com prevenção em primeiro lugar.

No final de 2020, um ataque à cadeia de suprimentos contra a SolarWinds ganhou as manchetes internacionais. O mesmo estilo de ataque ressurgiu em 2021, quando o software VSA da Kaseya foi comprometido, afetando mais de 1.000 empresas. Os ataques a cadeias de suprimentos geralmente contam com a confiança já estabelecida entre fornecedores e clientes para se propagar – oferecendo outro forte argumento para a adoção de uma estrutura Zero Trust. Embora os ataques a grandes organizações tenham se destacado nos meios de comunicação em 2021, as pequenas e médias empresas (PMEs) também sofreram inúmeros ataques, tanto diretamente quanto por meio da cadeia de suprimentos. Os pesquisadores de ameaças da BlackBerry descobriram PMEs com 11 a 13 ameaças por dispositivo em média, um número muito maior do que nas grandes empresas.

Os agentes de ameaças devem seu sucesso em 2021 a uma variedade de fatores. Muitos aprenderam a adotar e imitar as capacidades do setor privado usando fornecedores de ransomware como serviço (RaaS), infraestrutura como serviço (IaaS) e malware como serviço (Maas) para potencializar ataques maliciosos. Outros criaram uma camada de ofuscação entre eles e seus alvos usando IABs e fingindo ser outros grupos de ameaças. Novas linguagens de programação foram exploradas com algum efeito, com destaque para Go, D, Nim e Rust em todo o cenário de ameaças. O Cobalt Strike permaneceu ativo como uma ferramenta fundamental para redes de comando e controle para proliferar malwares e ataques.

300%

de aumento nos ataques de phishing (smishing) por SMS na América do Norte no ano passado.

Houve progresso na integração da segurança em veículos conectados com a International Organization for Standardization (ISO), a Society of Automotive Engineers (SAE) e a Organização das Nações Unidas (ONU) fornecendo orientações firmes às fabricantes automotivas. Os aplicativos móveis permaneceram notoriamente inseguros. O aplicativo SHAREit vulnerável, que permitia a execução remota de código, foi baixado mais de um bilhão de vezes. Estudos recentes descobriram que 63% dos aplicativos móveis testados usam código-fonte aberto com vulnerabilidades conhecidas. Somando-se aos problemas dos usuários de smartphones, os ataques de phishing (smishing) por SMS aumentaram 300% na América do Norte no ano passado.

Os ciberataques de 2021 afetaram pessoas em todos os níveis, desde grandes organizações a indivíduos que usam telefones celulares. Os relatórios internos da BlackBerry mostram que todos os setores estão abertos a ciberataques. Os mesmos problemas de cibersegurança que ameaçam organizações sem fins lucrativos também são riscos para empresas de transporte, organizações públicas, serviços públicos, organizações de saúde, instituições financeiras e outras. Ninguém está seguro. Quando se trata de ciberataques, a imunidade é zero. No entanto, existem várias inovações e abordagens de cibersegurança que oferecem proteção mais forte às organizações. Por exemplo, as organizações que buscam novas medidas de segurança eficazes devem considerar a adoção de uma estrutura Zero Trust. Também poderiam usar a tecnologia de prevenção em primeiro lugar, migrar para uma plataforma XDR ou envolver serviços gerenciados de XDR.

FEVEREIRO

Uma usina de tratamento de água em Oldsmar, Flórida foi comprometida quando um atacante tentou envenenar o suprimento de água.

A CD Projekt Red foi atacada pelo ransomware HelloKitty.

MARÇO

A Channel Nine na Austrália teve transmissões interrompidas por ciberataques.

A University of Highlands and Islands foi atacada com Cobalt Strike.

A CNA Insurance foi atacada por Evil Corp.

As Buffalo Public Schools em Nova York foram atacadas com ransomware.

Os Microsoft Exchange Servers foram atacados por HAFNIUM.

ABRIL

O time de basquete Houston Rockets (NBA) foi atacado por Babuk.

MAI

A Colonial Pipeline foi atacada pelo DarkSide.

A AXA foi atacada por Avaddon.

A Brenntag (distribuidora química) foi atacado pelo DarkSide.

A Acer foi atacada por REvil.

A JBS Foods foi atacada por REvil.

O Health Service Executive (HSE) da Irlanda foi atacado por Conti.

JULHO

Ataques de ransomware ocorreram em Chile, Itália, Taiwan e Reino Unido pelo grupo de ameaças LockBit.

A Kaseya sofreu um ataque à cadeia de suprimentos por REvil.

NOVEMBRO

A plataforma de trading Robin Hood foi invadida e informações sobre sete milhões de contas de usuários vazaram.

DEZEMBRO

A vulnerabilidade de Log4j foi revelada e explorada por vários agentes de ameaças.

LINHA DO TEMPO DE CIBERATAQUES DE ALTA VISIBILIDADE EM 2021

Entre os ciberataques de alta visibilidade que foram destaque nas notícias em 2021, alguns dos incidentes mais divulgados incluem:

Esses ataques conhecidos foram notícia nacional ou internacional devido à sua considerável escala, sofisticação, agressividade ou exigências de resgate. No entanto, suas histórias não refletem o verdadeiro preço que o crime cibernético cobrou de organizações públicas e privadas. Mais de 70% das PMEs sofreram ciberataques, de acordo com um estudo do Instituto Ponemon. Entre as atacadas, 60% fecham as portas em seis meses. Órgãos governamentais e grandes empresas podem sobreviver a um ciberataque. Mas, para PMEs, muitas vezes é uma sentença de morte.

Os ciberataques de 2021 atingiram diversos setores, afetaram organizações de todos os portes e são lembretes enfáticos de que ninguém está seguro. Não há imunidade contra agentes de ameaças dedicados e qualquer pessoa que opere no cenário digital pode ser o próximo alvo. Com tentativas maliciosas de hackers ocorrendo a cada 39 segundos, uma organização vai se esgotar se depender de medidas de segurança reativas. Felizmente, ferramentas que priorizam a prevenção, tecnologias preditivas de IA e estruturas Zero Trust podem oferecer às organizações uma alternativa eficaz às soluções tradicionais de cibersegurança.

CIBER AMEAÇAS

COBALT STRIKE

Nenhum relatório de ameaças estaria completo sem pelo menos um comentário sobre o Cobalt Strike. Este ano, a BlackBerry reuniu insights e tendências de um conjunto de dados interno de mais de 7.000 Cobalt Strike Team Servers e 60.000 Beacons.

Rastrear e monitorar os Cobalt Strike Team Servers que estão em circulação pode ajudar muito no ciclo de vida da inteligência de ameaças. Fornece informações valiosas para ajustar as soluções de segurança e ajudar nas investigações de incidentes. Uma análise detalhada da inteligência de ameaças obtida com a análise do Cobalt Strike está disponível no novo eBook da BlackBerry Threat Research and Intelligence Team, *"Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence"*.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

Nossa revisão anual da atividade do Cobalt Strike começa com algumas das estatísticas mais interessantes sobre implementações do Team Server.

Por exemplo, observe os 10 principais números de sistemas autônomos (ASNs) e netblocks (intervalos de endereços IP consecutivos) responsáveis por hospedar o payload imensamente versátil do Beacon do Cobalt Strike. Isso revela uma tendência fascinante: os agentes de ameaças estão ampliando o uso de provedores de nuvem legítimos para hospedagem. Isso permite que os operadores de malware ocultem seu tráfego dos sistemas de monitoramento, o que torna a tarefa de bloqueio automatizado mais complicada. Além das dificuldades de detecção, várias empresas grandes e respeitáveis são encontradas na lista dos 20 principais provedores. A Figura 1 mostra os 10 principais ASNs que hospedaram o Beacon do Cobalt Strike:

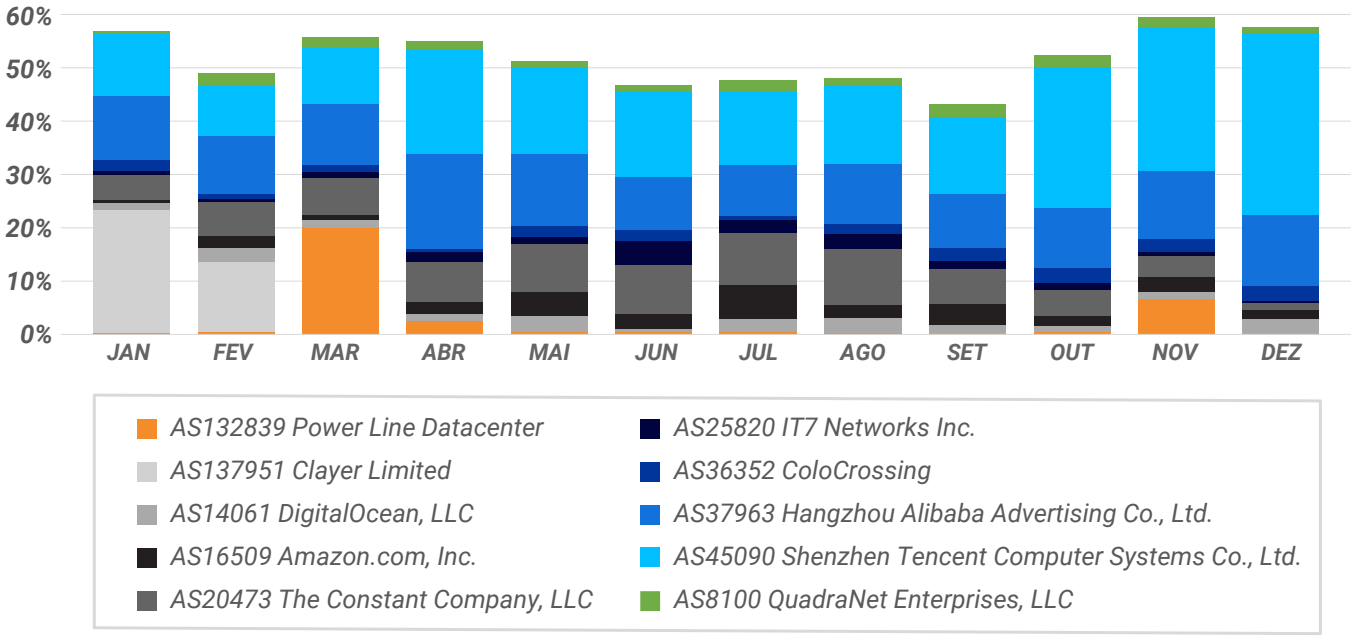


Figura 1 - 10 principais ASNs responsáveis por hospedar o payload do Beacon do Cobalt Strike

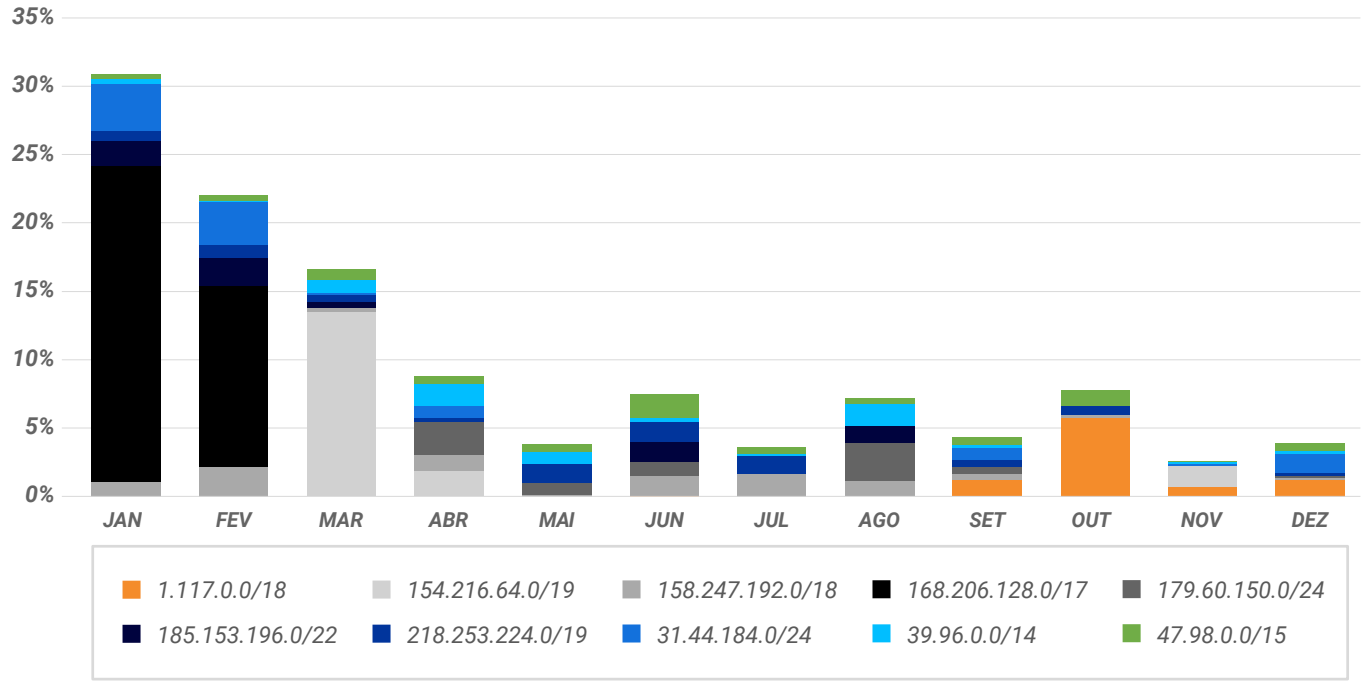


Figura 2 - 10 principais netblocks responsáveis por hospedar Beacons

De uma perspectiva geográfica, os seguintes países são os 10 principais usados para hospedar Beacons:

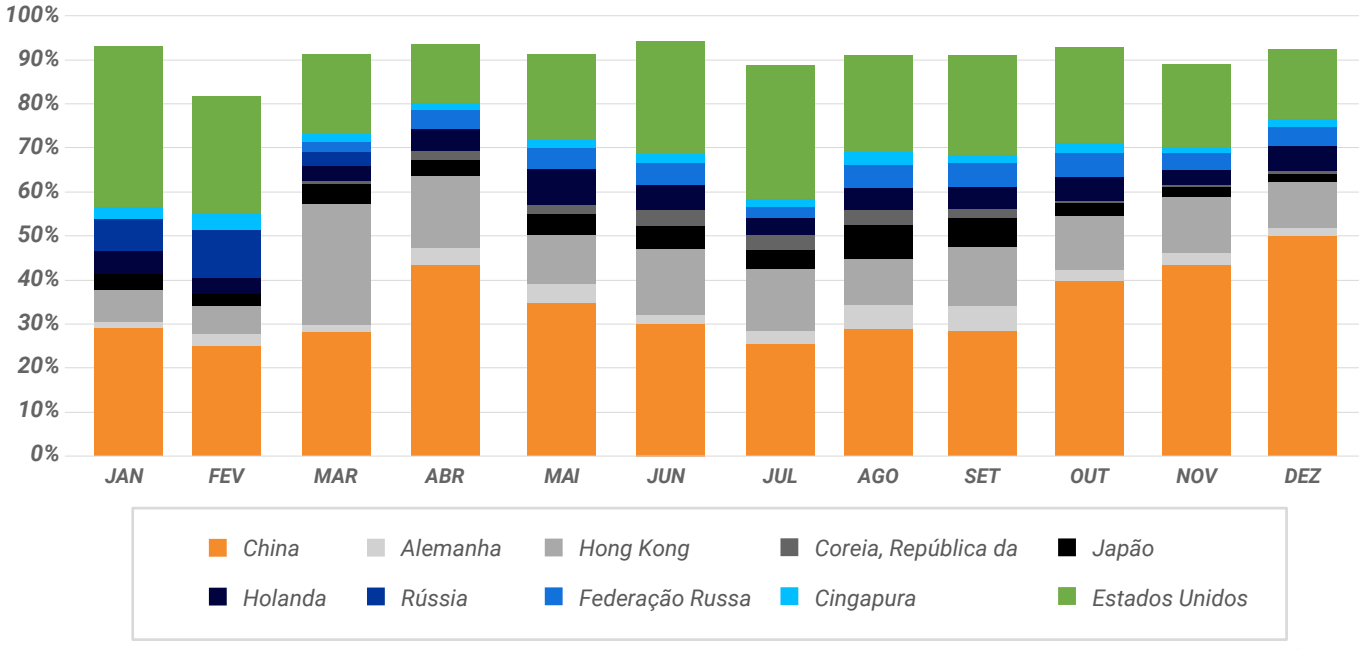


Figura 3 - 10 principais países que hospedaram Team Servers para Cobalt Strike

As portas 80, 443 e 8080 destacam-se (ver Figura 4) como acesso a payloads de Beacons de Team Servers. Essas portas em geral ficam abertas na maioria dos ambientes e se tornam uma escolha óbvia para roteamento de tráfego de comando e controle (C2).

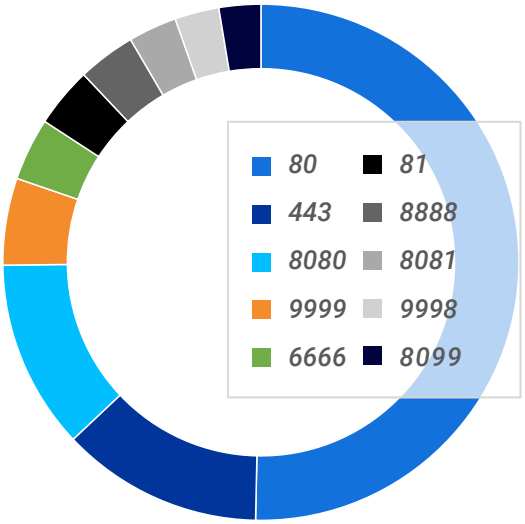


Figura 4 - 10 principais portas usadas para payloads de Beacons

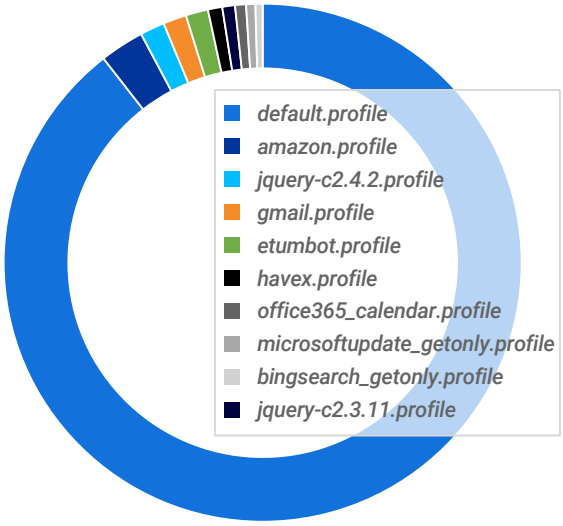


Figura 5 - 10 principais perfis maleáveis usados por Beacons do Cobalt Strike

Os Beacons do Cobalt Strike são altamente configuráveis por meio de perfis C2 maleáveis, que especificam como um Beacon age e se manifesta no ambiente de destino. Esses perfis também especificam quais parâmetros são usados em seu protocolo de comunicação e o método que o Beacon usa para injeção em outros processos. Os 10 principais perfis maleáveis observados ao longo de 2021 são mostrados na Figura 5.

Utilizando Perfis C2 Maleáveis, o Beacon do Cobalt Strike pode ser configurado para realizar uma técnica conhecida como domain fronting. É usada para rotear o tráfego HTTPS por redes confiáveis de entrega de conteúdo de terceiros. Os 10 principais hosts usados para domain fronting em 2021 foram:

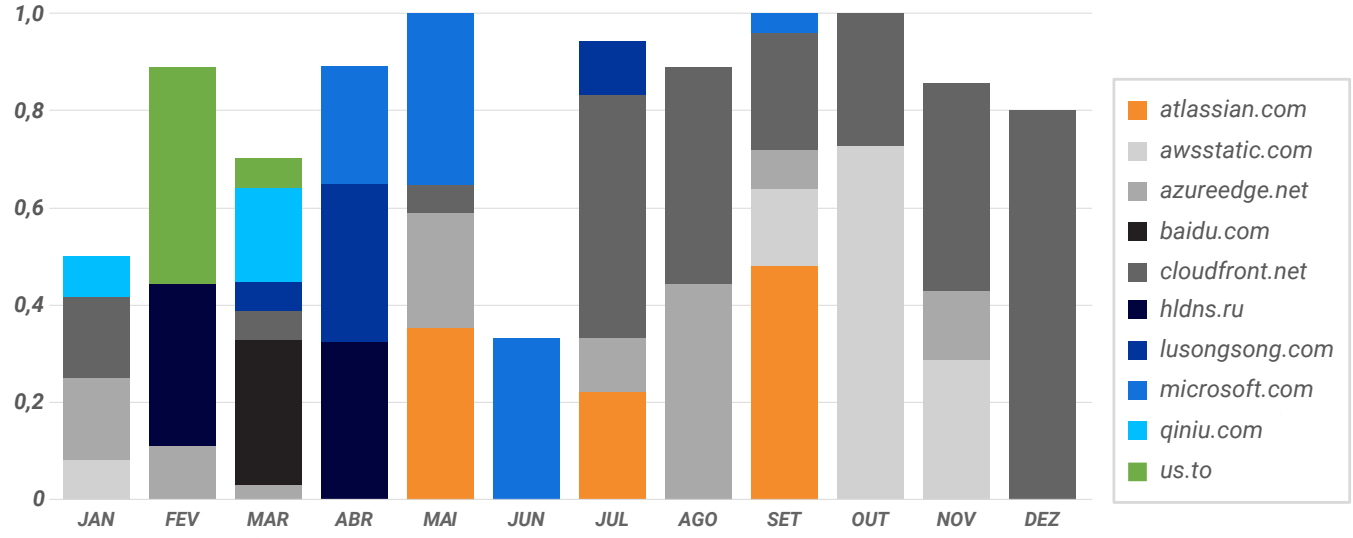


Figura 6 - 10 principais hosts usados pelo Beacon do Cobalt Strike para domain fronting e masquerading

O Beacon do Cobalt Strike pode ser configurado para usar redirecionadores de DNS para encaminhar tráfego C2 para um Team Server. A Figura 7 mostra os 10 principais protocolos IP de redirecionamento de DNS em 2021.

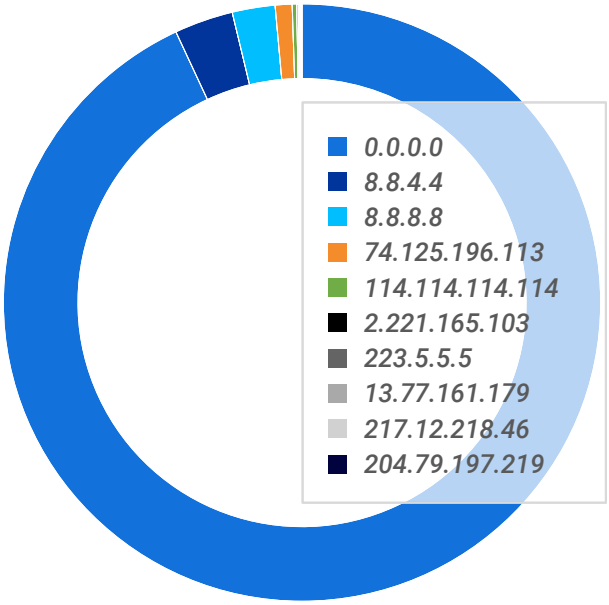


Figura 7 - 10 principais IPs de redirecionamento de DNS usados pelo Cobalt Strike

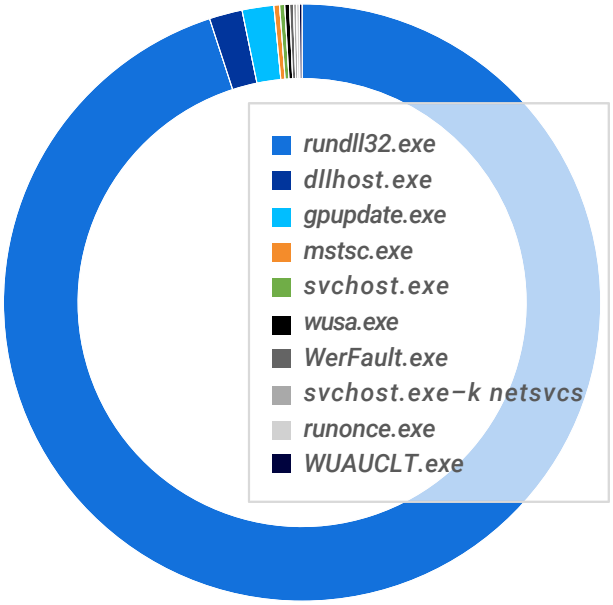


Figura 8 - Processos gerados que foram criados para injeções de Cobalt Strike

O Beacon do Cobalt Strike gera processos e injeta neles os payloads de bibliotecas de vínculo dinâmico. Esses processos podem ser configurados para funcionar em diferentes arquiteturas (x86/x64) com a opção SPAWNTO. O processo padrão e mais popular é rundll32.exe. Consulte a Figura 8.

Além dos certificados Secure Sockets Layer (SSL) implementados no Team Server, os Beacons também são empacotados com uma chave pública SSL adicional. Isso faz parte de um par de chaves pública/privada que é gerado no servidor sempre que alguém instala o Cobalt Strike. A chave pública é posteriormente incorporada em todos os Beacons gerados no mesmo servidor e usada para check-ins C2. É importante observar que esse par de chaves é totalmente diferente do par de chaves SSL usado para o certificado HTTPS no Team Server.

Diferente das marcas d'água, a chave pública SSL armazenada na configuração de um Beacon oferece uma opção fantástica para agrupar Beacons. É praticamente garantido que as chaves sejam exclusivas por instalação do Team Server, mas muitas vezes são reutilizadas, por exemplo, com reimplementações de máquinas virtuais. Em outros casos, os agentes de ameaças usarão um único Team Server para configurar payloads para implementação de outros servidores sob seu controle. Isso facilita consideravelmente a identificação, o rastreamento e o monitoramento de sua infraestrutura.

As 10 principais chaves públicas SSL pertencem principalmente a compilações vazadas do Cobalt Strike Team Server:

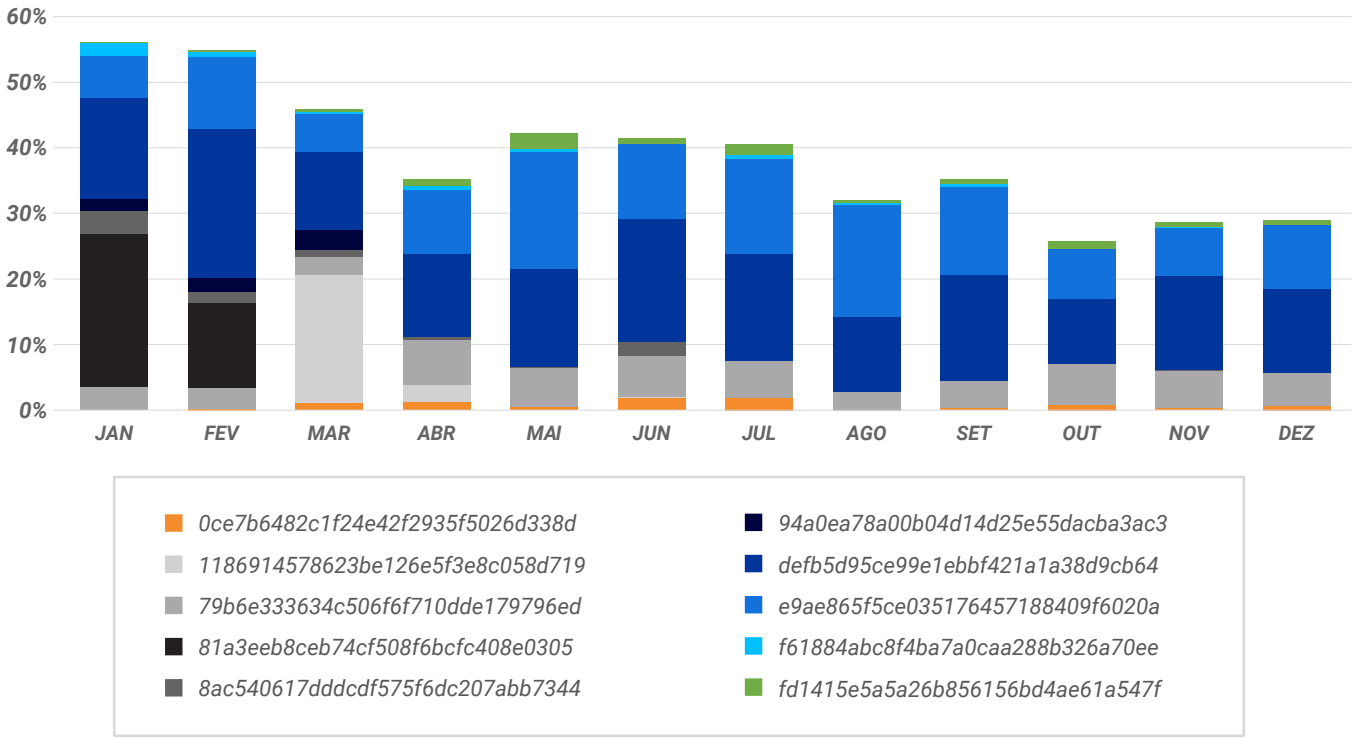


Figura 9 - As 10 principais chaves públicas de Cobalt Strike Team Servers

Por fim, é possível rastrear as compilações do Team Server por meio de uma configuração chamada PROCINJ_STUB, que contém um hash de algoritmo de resumo de mensagem (MD5) do arquivo Java Cobalt Strike (cobaltstrike[.]jar). Este arquivo contém o componente do lado do servidor que fornece aos operadores do Team Server uma interface gráfica de usuário para gerar, operar, implementar e controlar payloads de Beacon.

O hash MD5 do pacote cobaltstrike.jar nos permite determinar várias coisas. Ao correlacioná-lo com seu arquivo Java correspondente comumente encontrado em repositórios de malware online, como o VirusTotal, descobrimos:

- A versão exata do Team Server usado
- Se o Team Server em operação é uma versão vazada, craqueada ou de avaliação
- Se o Team Server é uma versão privada, licenciada

Mesmo que o arquivo Java não esteja disponível para ajudar a identificar a versão, ainda é um mecanismo de cluster extremamente valioso, especialmente no caso de compilações privadas e personalizadas.

Os 10 principais builds do Team Server em 2021 (com base no valor de hash de PROCINJ_STUB) foram:

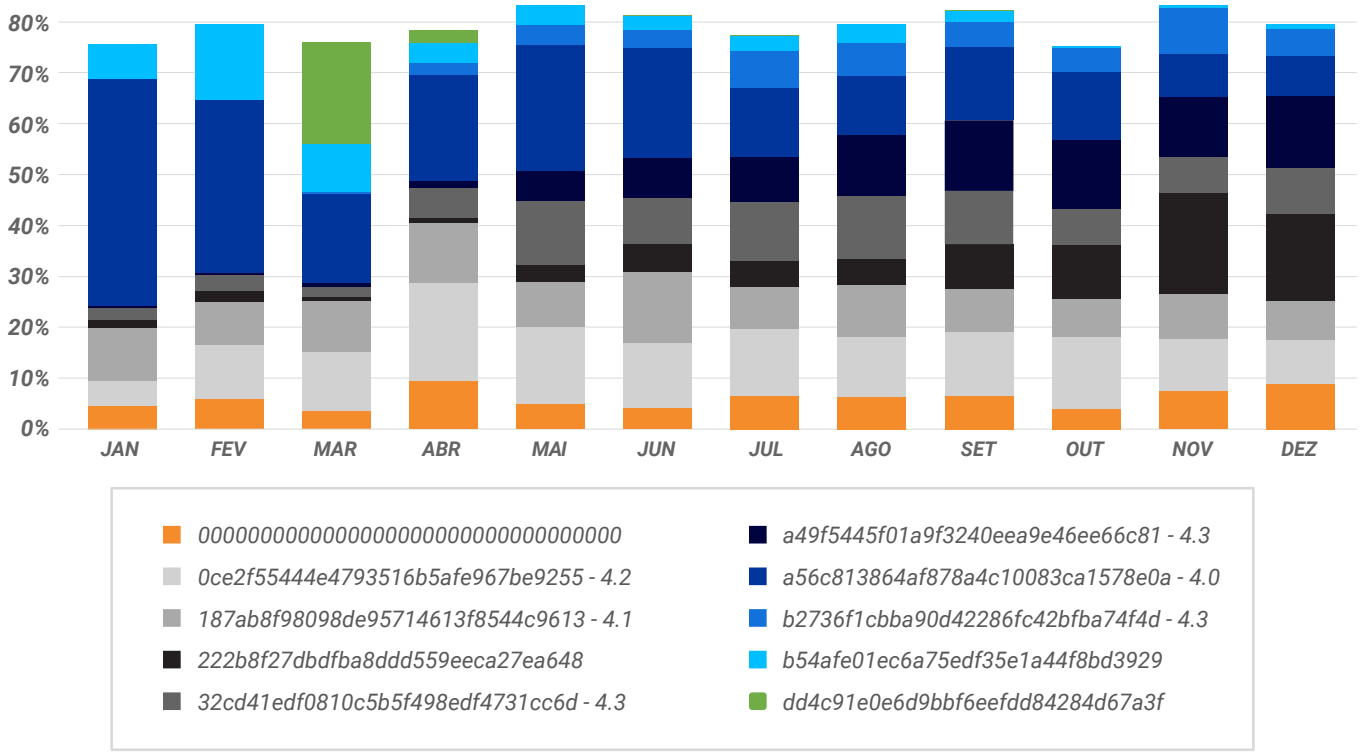


Figura 10 - 10 principais builds do Team Server em 2021

Além de nossa pesquisa, a Agência de Segurança Cibernética e Infraestrutura (CISA) do Departamento de Segurança Interna dos EUA divulgou um relatório sobre o Beacon do Cobalt Strike em maio de 2021. O documento inclui uma lista de recomendações que usuários e organizações podem adotar para minimizar a exposição a essa ameaça.

ATAQUES À CADEIA DE SUPRIMENTOS

Os ataques à cadeia de suprimentos não são um conceito recente. No entanto, a cadeia de suprimentos de software tem sido cada vez mais usada como um vetor de ataque nos últimos anos. Por quê? Um dos motivos é que o impacto potencial e a disseminação de um ataque à cadeia de suprimentos pode ser muito maior do que ter como alvo uma vítima individual. O potencial para danos varia, dependendo da base de clientes do produto. A relação entre produtor e consumidores é essencialmente um para muitos, com um único ponto de falha. Isso significa que, quanto maior a base de clientes, também é maior a base potencial para o ataque.

Os agentes de ameaças sabem que explorar a confiança que as pessoas têm na integridade e segurança de sua cadeia de suprimentos é mais fácil do que invadir alvos fortificados. Os adversários em geral procuram o caminho com menos resistência: a cadeia de suprimentos representa a evolução mais recente nessa técnica.

O QUE É UM ATAQUE À CADEIA DE SUPRIMENTOS?

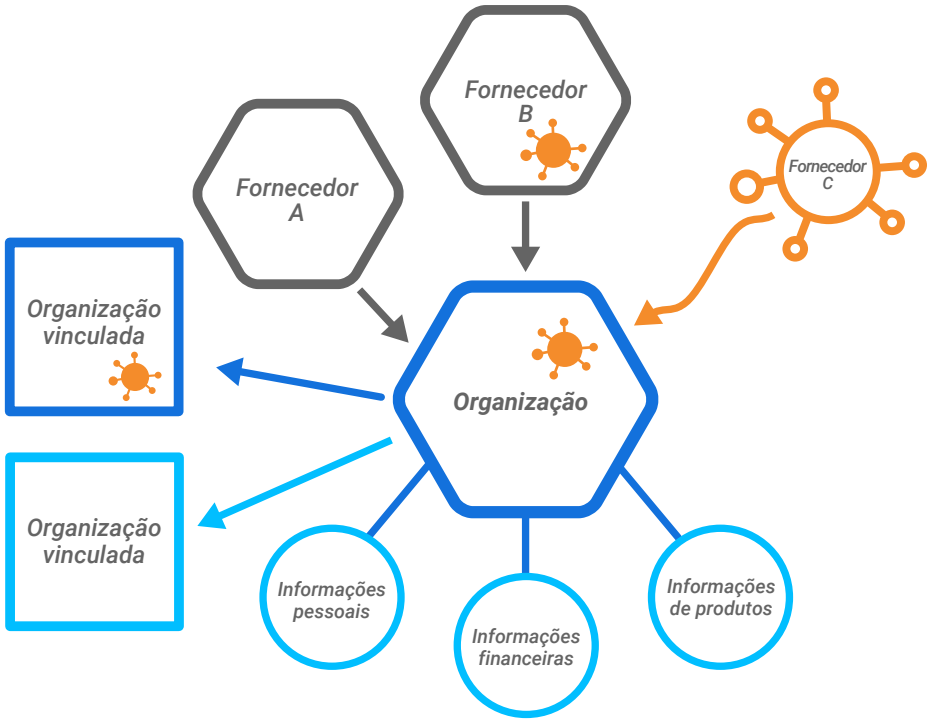


Figura 11 - Exibição topológica de um ataque à cadeia de suprimentos

Para entender melhor os ataques à cadeia de suprimentos, veja a representação topológica de interações da empresa na Figura 11. Os ataques à cadeia de suprimentos ocorrem quando uma organização depende de outra para parte de seu desenvolvimento de produtos, equipamentos, softwares ou outros serviços.

O Departamento de Defesa dos EUA define um risco de cadeia de suprimentos como uma situação em que o adversário pode "sabotar, incluir maliciosamente uma função indesejada, ou de outra forma subverter design, integridade, fabricação, produção, distribuição, instalação, operação ou manutenção de um sistema para espionar, negar, interromper ou de outra forma degradar a função, o uso ou a operação de sistemas".

Olhe a Figura 11 outra vez. A organização central depende dos Fornecedores A até C para diferentes requisitos. Tudo vai bem, até que o Fornecedor C é invadido e uma presença é estabelecida no ambiente. O ciclo de vida de desenvolvimento de produtos do Fornecedor C é comprometido e um componente malicioso é incluído no produto.

O produto, em estado comprometido, é distribuído para a organização, onde atua como ponto de entrada para que adversários maliciosos se infiltrem e comprometam.

Depois que os atacantes entrarem, todas as informações que acessarem podem ser extraídas, incluindo informações sobre produtos, informações financeiras e dados pessoais. Se a organização comprometida tem uma abordagem de segurança fraca, a propagação adicional desse ataque poderá se espalhar para organizações vinculadas e suas bases de clientes.

IMPACTO POTENCIAL

Dependendo do tamanho da base de clientes da organização comprometida, o impacto de um ataque à cadeia de suprimentos pode ser imenso.

Identificar quais clientes foram afetados, e em qual extensão, pode ser complicado. Como resultado, assim que uma violação for identificada, os clientes devem ser notificados para que possam iniciar seus próprios esforços de remediação. As organizações devem se planejar para o pior nesses cenários: pressupor que os clientes foram invadidos e que o risco de danos adicionais à reputação é iminente. Quanto mais tempo se passar até a identificação da ameaça e a resposta, maior o risco de que os atacantes obtenham uma presença persistente em ambientes de clientes.

Também existe a possibilidade de um efeito dominó, em que, se a violação não for contida, outras organizações também podem ser afetadas.

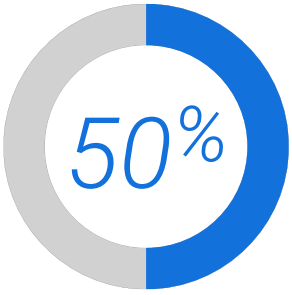
ATAQUES RECENTES A CADEIAS DE SUPRIMENTOS

Os ataques à cadeia de suprimentos parecem ser perigosos. E são. Muitos preferem não acreditar na ideia de que uma fonte confiável possa ser o ponto de comprometimento inicial. Mas isso ocorre. Alguns exemplos de ataques históricos a cadeias de suprimentos de software incluem:

- **Os ataques de ransomware NotPetya em 2017.** Os atacantes comprometeram o software tributário ucraniano MEDoc e causaram bilhões de dólares em perdas e danos a gigantes farmacêuticas.
- **A violação da SolarWinds em 2020.** O software de gestão e monitoramento Orion IT foi comprometido e enviado para diversas organizações de alta visibilidade.
- **Kaseya em 2021.** Um exploit de dia zero permitiu que os atacantes implementassem uma atualização em todos os clientes que executavam seu software de administração virtual de sistemas (VSA). A atualização era ransomware puro e criptografou uma grande parcela da base de clientes de VSA da Kaseya.

A Agência de Cibersegurança da União Europeia publicou recentemente um relatório sobre 24 ataques à cadeia de suprimentos entre janeiro de 2020 e julho de 2021. O relatório revelou algumas estatísticas claras:

- Os fornecedores não sabiam ou não informaram como foram comprometidos em 66% dos ataques à cadeia de suprimentos.
- Grupos de ameaças persistentes avançadas (APTs) receberam o crédito por realizar 50% dos ataques à cadeia de suprimentos.
- A exploração da confiança no fornecedor correspondeu a quase 62% dos ataques a clientes.



Em 24 ataques recentes a cadeias de suprimentos, os grupos de ameaças persistentes avançadas (APTs) receberam o crédito por realizar 50% deles.

COMO OS ATAQUES À CADEIA DE SUPRIMENTOS EVADEM A DETECÇÃO?

Na essência, um ataque à cadeia de suprimentos é um abuso de confiança. Pressupõe-se que um fornecedor confiável terá normas de segurança rigorosas. Por exemplo, um analista que responde a alertas que mostram o tráfego de rede C2 pode ter um viés, dependendo do seu nível de confiança em um aplicativo. Pode ver um domínio de interesse específico no tráfego de rede ou em seus certificados SSL. No entanto, como vem de um aplicativo confiável, é pressuposto que o indicador de ameaça é legítimo.

Esse viés destaca os benefícios de uma abordagem Zero Trust e como a confiança implícita pode ser uma grande vulnerabilidade. Também reforça a necessidade de investigar e analisar aplicativos de terceiros com mais detalhes. Uma corrente tem a força de seu elo mais fraco: se uma parte quebrar, o sistema inteiro pode falhar.

COMO MELHORAR A PROTEÇÃO?

Muitas questões de segurança podem ser superadas com uma abordagem holística para a segurança e adotando os princípios de Zero Trust. Todos os vetores de ameaças precisam ser cobertos, incluindo fontes geralmente consideradas benignas.

Muitas questões de segurança podem ser superadas com uma abordagem holística para a segurança e adotando os princípios de Zero Trust.

A equipe de resposta a incidentes de segurança de produtos (PSIRT) da organização também é um componente essencial para aprimorar sua abordagem de segurança. Por exemplo, uma PSIRT pode trabalhar de perto com outras equipes, comunicando insights de segurança valiosos ao longo do ciclo de vida de desenvolvimento de software (SDLC). À medida que sua inclusão no SDLC continuar, a PSIRT alcançará novos níveis de maturidade e ficará mais proativa. Isso ajuda a garantir que os produtos e processos de compilação tenham o máximo de segurança possível. O risco de um ataque à cadeia de suprimentos é reduzido quando as linhas de comunicação entre as equipes estão bem constituídas.

Para analistas de segurança, é importante reduzir a tendência natural de favorecer aplicativos e serviços com confiança. Embora assinatura com certificados, proveniência, build tooling e outras medidas que podem ser adotadas tenham valor de segurança, é imperativo que as equipes de operações de segurança (SecOps) sempre se mantenham céticas. A rapidez para divulgação e contenção de uma violação também é crítica para proteger as organizações e os clientes que dependem de seus produtos ou serviços.

EXPLOITS DE LOG4J/LOG4SHELL

O Log4j é um pacote de logging de código aberto usado por inúmeros aplicativos e frameworks importantes, incluindo Apache Struts2. No fim de 2021, uma vulnerabilidade neste componente de software que os atacantes podem explorar enviando texto especial foi descoberta. Os ataques que têm como alvo esta vulnerabilidade, também denominados exploits de Log4Shell, permitem que agentes de ameaças obtenham código em um servidor remoto e executem o código remotamente (RCE, Remote Code Execution). Como o Log4j não é malware, não é suscetível às medidas de cibersegurança e ferramentas com foco exclusivamente em detectar código malicioso.

A vulnerabilidade de Log4j, reportada pela primeira vez por Chen Zhaojun em 24 de novembro, é descrita adicionalmente em CVE-2021-44228. Em 10 de dezembro, a vulnerabilidade foi divulgada publicamente no National Vulnerability Database, mantido pelo National Institute of Standards and Technology (NIST). A revelação desta vulnerabilidade levou a um aumento rápido em ataques que em breve chegaram a milhões por hora.

A vulnerabilidade de Log4j é particularmente problemática, pois é difícil para as organizações saberem quais aplicativos e serviços estão em risco. Um aplicativo autônomo usando Log4j pode ser fácil de identificar, mas e os casos em que o pacote tem seis níveis de profundidade na cadeia de dependências? O uso generalizado do Log4j e a natureza complexa das dependências de software indicam que essa vulnerabilidade representará uma ameaça nos próximos anos.

Embora as medidas antimalware não sejam úteis para detectar e corrigir a vulnerabilidade do Log4j, outras estratégias de cibersegurança podem reduzir a exposição de uma organização a esse risco. Por exemplo, adotar uma estrutura Zero Trust pode limitar o uso da vulnerabilidade por um atacante, restringindo o acesso de processos invadidos. Os ambientes Zero Trust podem reduzir ainda mais os riscos, aplicando políticas de acesso com privilégios mínimos em todo o ambiente. Além disso, como muitos ciberataques dependem da entrega de um payload malicioso, as ferramentas antimalware podem impedir ataques baseados em arquivos resultantes do exploit.

CACHORROS VELHOS, TRUQUES NOVOS – LINGUAGENS DE PROGRAMAÇÃO OBSCURAS

A BlackBerry Threat Research and Intelligence Team tem rastreado e monitorado o cenário de ameaças em relação a quatro linguagens de programação obscuras:

- **Go**
- **D**
- **Nim**
- **Rust**

Essas linguagens estão sendo observadas atualmente para monitorar seu uso e adoção por agentes de ameaças. A seleção dessas linguagens foi motivada parcialmente por um aumento no uso inadequado para atividades maliciosas. Outro fator é seu papel cada vez maior em famílias de malware criadas e reveladas no cenário de ameaças geral.

De forma geral, novas linguagens de programação com frequência são desenvolvidas para aprimorar diversos aspectos ou carências nas atuais. Isso, em consequência, também pode torná-las uma opção atraente para abuso por agentes de ameaças. As novas linguagens podem ser usadas como wrapper ou loader para uma família de malware existente, para reescrever malwares existentes ou desenvolver malwares totalmente novos. Essa tendência foi observada no passado com o uso de VB6 e Delphi para desenvolver wrappers para malwares existentes.

Cachorros velhos, truques novos: atacantes adotam linguagens de programação exóticas

Mais recentemente, em março de 2021, a família de malware BazarLoader foi reescrita na linguagem de programação Nim e chamada de Nimzaloader. Vários meses depois, em maio, apareceu o RustyBeur, uma variante do malware Buer-loader reescrito em Rust.

Do ponto de vista de um agente de ameaças, o uso de linguagens de programação exóticas fornece muitas vantagens. Elas incluem:

- Desempenho aprimorado
- Indisponibilidade de ferramentas de análise
- Desconhecimento dos analistas sobre sua composição
- Maior capacidade para impedir a detecção por antivírus baseado em assinaturas

Poderíamos dizer que essas linguagens atuam como uma camada de ofuscação. Sua novidade e a indisponibilidade de ferramentas de análise significam que podem parecer muito originais para pesquisadores inexperientes.

A BlackBerry observou que essas linguagens estavam sendo usadas no desenvolvimento de uma quantidade crescente de droppers e loaders. Foram usadas como novos malwares de primeiro estágio projetados para colocar/decodificar, carregar e implantar famílias de malware comerciais comumente vistas. As ameaças que usam essas novas linguagens atualmente incluem os cavalos de Troia de acesso remoto Remcos e NanoCore, e Beacons do Cobalt Strike.

Muitas dessas linguagens também podem ter compilação cruzada para ter como alvo vários sistemas operacionais. Agentes de ameaças abusaram implacavelmente desse poderoso recurso. Especificamente, o grupo APT29 da Rússia e seu malware Wellmess, que foi escrito em Go e compilado para atacar sistemas operacionais Windows® e Linux®. Um exemplo adicional disso foi o surgimento do malware ElectroRAT em janeiro de 2021. Também foi desenvolvido em Go e depois compilado cruzadamente para atacar todos os principais sistemas operacionais: Windows, macOS® e Linux.

Nim e Go já foram usados em diferentes partes da mesma cadeia de ataque para aumentar a capacidade de evasão de detecção do atacante. Por exemplo, o grupo de ameaças APT28 utilizou um downloader baseado em Nim para recuperar um payload baseado em Go no malware Zebrocy.

Os benefícios e a popularidade dessas linguagens resultaram em aumento de sua adoção pela comunidade de segurança. Devido às vantagens ofensivas, são úteis especialmente no desenvolvimento das ferramentas de Red Team. No fim de 2020, a FireEye revelou que um agente de ameaças havia obtido acesso não autorizado a algumas de suas ferramentas de Red Team. Como contramedida, eles divulgaram uma declaração junto com um repositório GitHub composto por várias assinaturas de detecção para ajudar a identificar as ferramentas roubadas. Nesse repositório, a FireEye revelou que sua Red Team vinha usando uma combinação de ferramentas publicamente disponíveis modificadas e ferramentas personalizadas internas. Algumas dessas ferramentas da Red Team haviam sido escritas em DLang, Rust e Go.

Os binários maliciosos criados nessas linguagens atualmente constituem uma pequena parte dos que estão sendo usados por agentes de ameaças. No entanto, seu uso em ciberataques é uma tendência que provavelmente aumentará na próxima década.

INTERMEDIADORES DE ACESSO INICIAL (IABS)

A BlackBerry Threat Research and Intelligence Team tem monitorado um IAB que ainda não havia sido documentado e a BlackBerry chamou de Zebra2104. Nossa investigação descobriu uma massa de infraestrutura maliciosa interligada que apresentou uma conexão incomum entre vários grupos de ameaças aparentemente não relacionados.

A primeira revelação ocorreu em abril de 2021, com a descoberta de um domínio servidor de Beacon do Cobalt Strike que também atuava como servidor C2. Ao seguir uma trilha de navegação, encontramos várias sobreposições com uma infraestrutura de malspam documentada anteriormente. Essa infraestrutura entregou vários payloads, incluindo o Dridex, no ano passado. Também foi associada com uma campanha de phishing voltada para entidades na Austrália, privadas e governamentais.

Pesquisas adicionais identificaram vínculos com uma invasão do ransomware MountLocker por meio de informações de registrante de domínio compartilhado para o domínio supercombinating[.]com. Mais investigações revelaram outro domínio relacionado, mentiononecommon[.]com, que resolvia para o mesmo IP em alternância com supercombinating[.]com durante vários meses. A inteligência de código aberto confirmou que esse domínio havia sido marcado anteriormente como servidor C2 do StrongPity em junho de 2020.

O Promethium (também conhecido como StrongPity) é um grupo de APTs com atuação desde 2012. Em geral, usa ataques de watering hole para entregar versões trojanizadas de utilitários comumente usados. WinRAR, CCleaner e Internet Download Manager são alguns dos utilitários que foram reformulados maliciosamente para distribuir o malware do grupo.

Ao buscar mais evidências para comprovar que esses dois grupos díspares cooperaram de alguma forma, nossos pesquisadores encontraram outro indício interessante. Um tweet do The DFIR Report em agosto de 2020 avisou que ransomware adicional estava sendo distribuído por supercombinating[.]com. Desta vez, o malware era da família Phobos e não MountLocker.

Isso motivou mais perguntas sobre a conexão entre esses grupos de ameaças. Estavam relacionados ou só compartilhavam a mesma infraestrutura? Havíamos descoberto algum tipo de sistema de distribuição? O elo perdido que reunia esses grupos seria um IAB?

Um IAB é uma entidade cujo objetivo é obter acesso ilegal à rede de uma organização. Estabelece uma presença, geralmente instalando um backdoor, e depois vende o acesso ilícito na dark web. Os preços desses serviços podem variar desde apenas US$ 25 até milhares de dólares. Depois de obter acesso, com frequência os compradores implementam malware no ambiente da vítima.

Embora diferentes grupos de ransomware possam compartilhar infraestrutura, nossa pesquisa durante esta investigação indica que isso não ocorria aqui. Em vários casos, foi observado um retardo entre o comprometimento inicial com Cobalt Strike e a distribuição de ransomware adicional. Esses fatores nos levaram a inferir que a infraestrutura sobreposta não era de MountLocker, Phobos ou Promethium. Pertence a um quarto grupo que atuou como intermediário para facilitar as operações dos três primeiros. Esse acordo foi alcançado fornecendo/vendendo acesso inicial ou pelo fornecimento de IaaS.

Além disso, os domínios encontrados nessa infraestrutura sobreposta usada para resolução para IPs eram fornecidos por um único ASN da Bulgária, pertencente à Neterra LTD.

O fato de que todos os IPs estavam agrupados no mesmo ASN adiciona credibilidade à teoria de que pertencem ao mesmo grupo de ameaças. Esse grupo provavelmente também lançou as bases para que os outros agentes de ameaças acessassem redes invadidas pelo IAB.

CHACHI

A BlackBerry Threat Research and Intelligence Team tem monitorando um cavalo de Troia de acesso remoto (RAT) Golang sem nome que visava sistemas Windows. Batizamos esse RAT de ChaChi. O RAT tem sido usado por operadores do ransomware PYSA (também conhecido como Mespinoza) como parte do conjunto de ferramentas para atacar vítimas globalmente. Recentemente, o malware tem visado organizações de educação.

O PYSA adora o ChaChi: um novo RAT GoLang

O ChaChi foi observado em circulação desde o primeiro semestre de 2020, sem receber muita atenção do setor de cibersegurança. A primeira variante conhecida do ChaChi foi usada em ataques às redes de autoridades locais do governo na França. Foi listada como um indicador de comprometimento (IOC) em uma publicação da CERT França na época dos ataques.

Desde então, os analistas da BlackBerry observaram versões mais refinadas do ChaChi implementadas por operadores do ransomware PYSA. A campanha tinha foco em instituições educacionais nos EUA, o que fica evidente por um aumento recente de atividade, conforme reportado pelo FBI.

TIPOS DE ATAQUES

RANSOMWARE

REVIL

O FBI acusou o REvil, grupo RaaS afiliado à Rússia (e também conhecido como Sodin ou Sodinokibi), de ter realizado os ataques ao maior fornecedor de carnes do mundo, a JBS. Esses ataques ameaçaram a cadeia de suprimentos de alimentos mundial e são um lembrete sobre o estado vulnerável da infraestrutura crítica no mundo inteiro.

O REvil foi anunciado pela primeira vez em fóruns russos de crimes cibernéticos e está associado ao agente de ameaças Unknown (também conhecido como UNKN).

O malware atua como RaaS e tornou-se prolífico depois que outro grupo de RaaS, o GandCrab, desativou suas operações. Os pesquisadores de segurança identificaram muitas semelhanças e reutilização de código entre REvil e GandCrab. O REvil foi anunciado pela primeira vez em fóruns russos de crimes cibernéticos e está associado ao agente de ameaças Unknown (também conhecido como UNKN).

O REvil é mais conhecido por estar associado a ataques recentes ao setor de seguros de viagem, à Acer e a fabricantes de computadores. Atuando como RaaS, o REvil depende de afiliados ou parceiros para realizar seus ataques. Os desenvolvedores do REvil recebem um percentual de toda a receita dos pagamentos de resgates. Como o ransomware é distribuído por diferentes entidades, o vetor inicial de infecção pode variar. Em geral, a infecção é alcançada com campanhas de phishing, ataques de força bruta para comprometer o protocolo RDP ou vulnerabilidades de software. O REvil também é distribuído por outros malwares, como o IcedID.

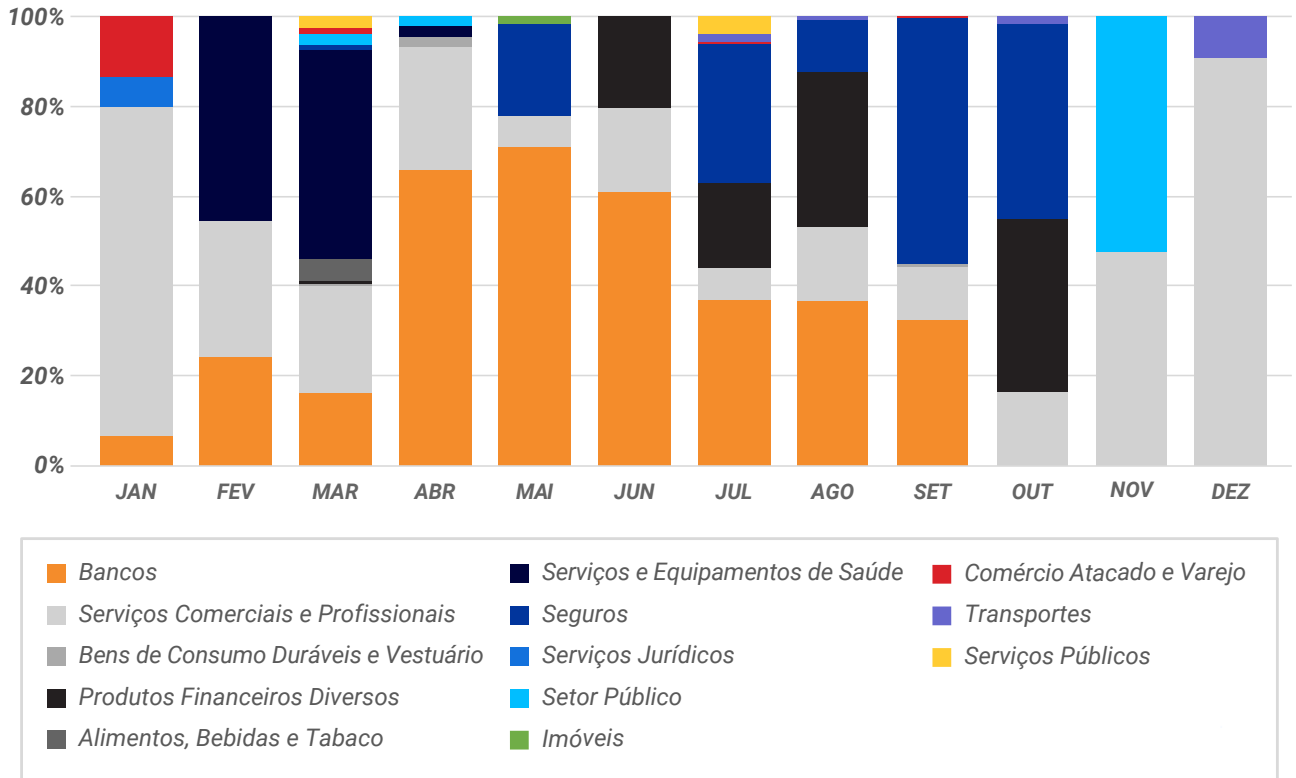


Figura 12 - Setores atacados pelo REvil, 2021

DARKSIDE

A variante de ransomware DarkSide apareceu pela primeira vez em meados de 2020. É distribuído como um RaaS usado para ataques direcionados. O DarkSide ataca máquinas com Windows e Linux. Foi notícia em 2021 com o ataque à Colonial Pipeline, que administra um sistema de oleodutos dos EUA.

O DarkSide usa um esquema de extorsão dupla, em que os dados são criptografados localmente e exfiltrados antes da solicitação de resgate. Se a vítima se recusar a pagar, os dados são publicados em um site na dark web.

Após o ataque à Colonial Pipeline, o DarkSide Group declarou que não pretendia afetar hospitais ou instalações médicas, educacionais, sem fins lucrativos ou sistemas de governos. O DarkSide Group foi desativado em maio de 2021, possivelmente pelo Comando Cibernético dos Estados Unidos.

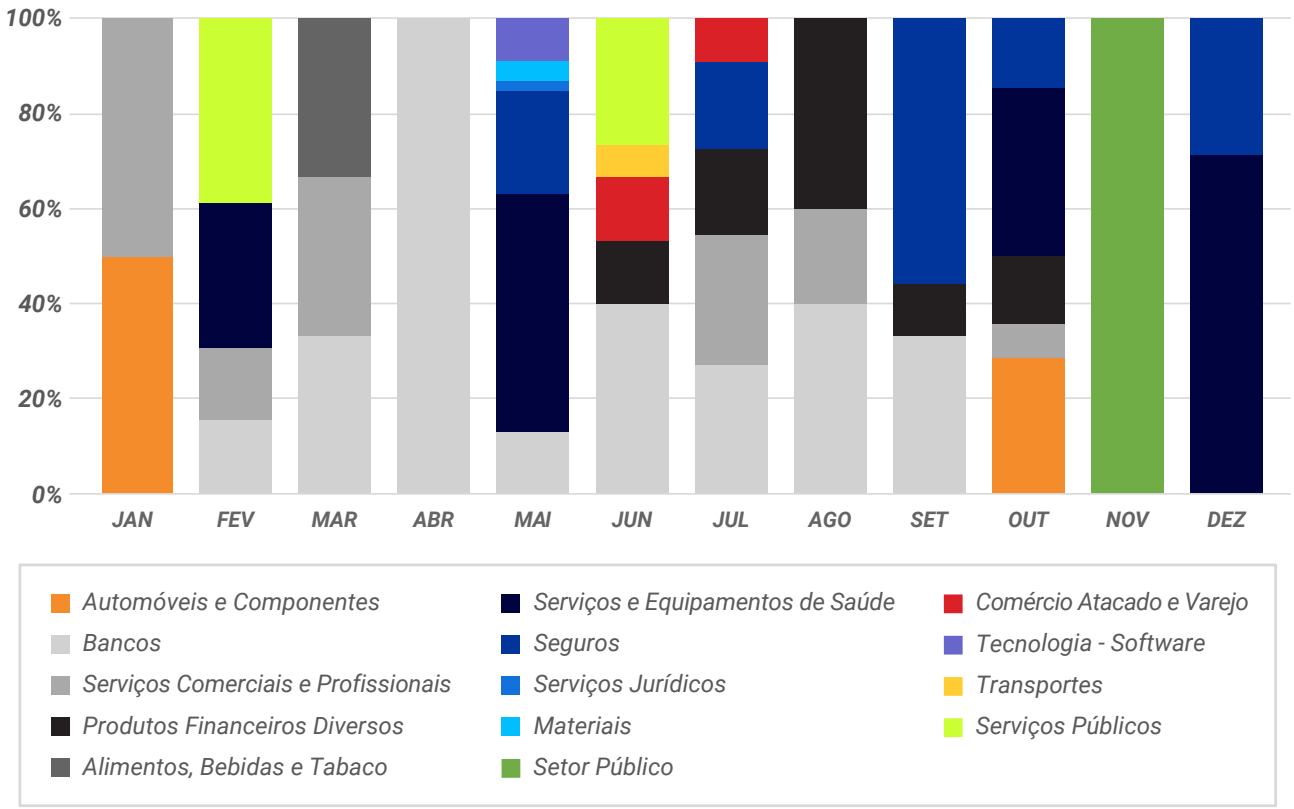


Figura 13 - Setores atacados pelo DarkSide, 2021

Muitos analistas consideram o Conti como o ransomware que substituiu o Ryuk, e o avaliam como uma das ameaças de ransomware mais potentes em circulação.

CONTI

O ransomware Conti foi notícia internacional após sua descoberta inicial em meados de 2020. Os pesquisadores da BlackBerry observaram ataques do Conti contra prestadores de serviços de fabricação, seguros e saúde no Japão, na Europa e nos EUA.

O Conti é oferecido como RaaS, que é uma maneira popular de os agentes de ameaças distribuírem e venderem seus serviços maliciosos em fóruns clandestinos. Como essa ameaça é oferecida como serviço para venda, é personalizável e, portanto, sua funcionalidade pode ser alterada de uma infecção para outra. Em maio de 2021, agentes de ameaças lançaram um decodificador para essa ameaça, que pode ajudar a recuperar arquivos alterados por uma cepa específica de Conti.

A popularidade do Conti aumentou depois que o famoso ransomware Ryuk aparentemente encerrou as operações. Muitos analistas consideram o Conti como o ransomware que substituiu o Ryuk, e o avaliam como uma das ameaças de ransomware mais potentes em circulação.

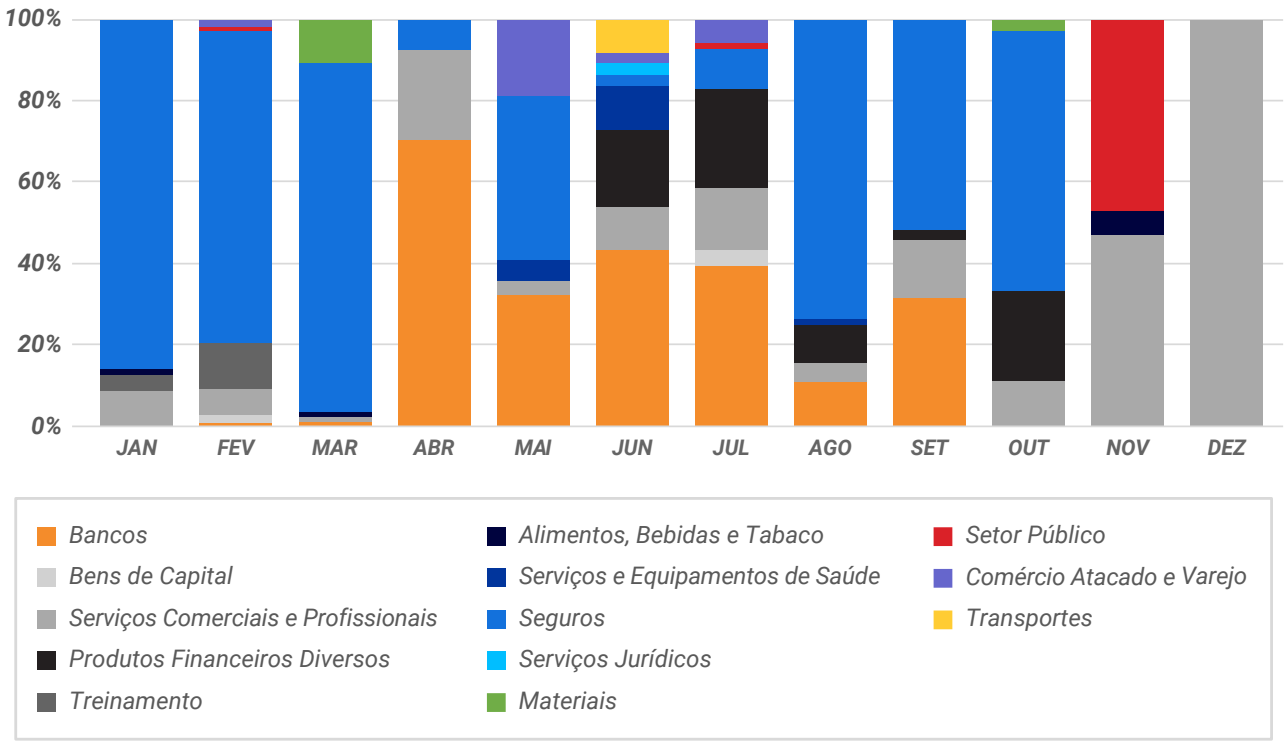


Figura 14 - Setores atacados pelo Conti, 2021

AVADDON

A variante de ransomware Avaddon apareceu pela primeira vez no início de 2020. Foi notícia internacional devido a ataques recentes contra organizações australianas e uma empresa de seguros cibernéticos com sede na Ásia, a AXA. O FBI e o Australian Cyber Security Center divulgaram avisos sobre um ataque em andamento dessa família de malware.

Como os ransomwares DarkSide e REvil, o Avaddon também usa um esquema de extorsão dupla, em que os dados são criptografados localmente e exfiltrados antes da solicitação de resgate. Se a vítima se recusar a pagar, os dados são publicados em um site na dark web. No entanto, o Avaddon vai um passo além. Para incentivar ainda mais a conformidade, os atacantes também sujeitam as vítimas a um ataque distribuído de negação de serviço (DDoS) até que o resgate seja pago.

Depois de chamar a atenção por seu papel em vários incidentes de ransomware de alta visibilidade, o grupo por trás do Avaddon parece estar encerrando suas operações atuais. Os esforços policiais para rastrear os operadores de malware aumentaram visivelmente após o ataque à Colonial Pipeline, que também levou o DarkSide a encerrar as operações. O Avaddon divulgou os decodificadores para a versão mais recente de sua ameaça.

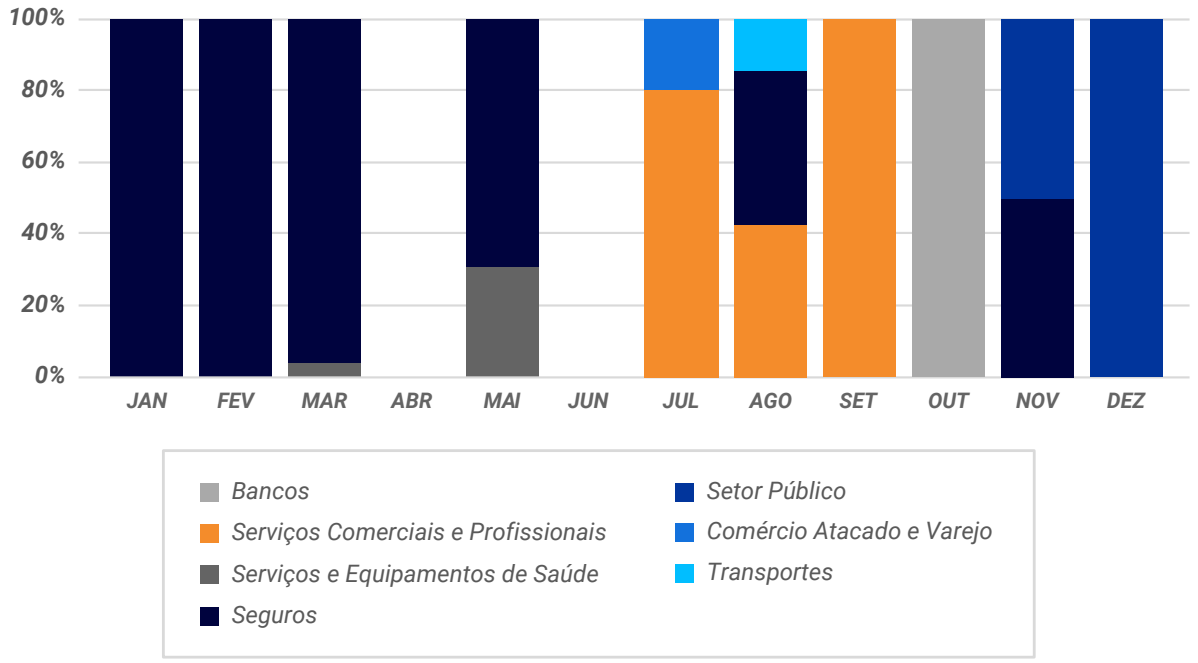


Figura 15 - Setores atacados pelo Avaddon, 2021

1,5TB

O grupo Ragnar Locker afirma ter exfiltrado 1,5 TB de dados de uma vítima de alta visibilidade.

RAGNAR LOCKER

O ransomware Ragnar Locker foi notícia internacional pelos ataques contra uma fabricante taiwanesa de módulos DRAM de alto desempenho e produtos NAND Flash. A primeira variante dessa família apareceu no fim de 2019.

Como muitas outras variantes de ransomware conhecidas (por exemplo, DarkSide, Avaddon e REvil), a variante atual do Ragnar Locker também usa uma técnica de extorsão dupla para pressionar as vítimas a pagar.

O site do Ragnar Locker na dark web relaciona as vítimas mais recentes em um "hall da vergonha". Atualmente, afirma ter exfiltrado 1,5 TB de dados de uma vítima de alta visibilidade. De acordo com o website, essa informação foi coletada furtivamente durante muito tempo.

HIVE

Vista pela primeira vez em junho de 2021, a família de ransomware Hive foi notícia por atacar o Altus Group, uma empresa de software imobiliário comercial. Essa ameaça também usa técnicas de extorsão dupla. As vítimas que se recusam a cooperar com o agente de ameaças correm o risco de ter seus dados publicados no site do grupo, o Hive Leaks.

As amostras de Hive são escritas na linguagem de programação Go e compiladas para máquinas de 32 e 64 bits. São empacotadas em UPX para redução do tamanho, porque os binários Go tendem a ser muito grandes.

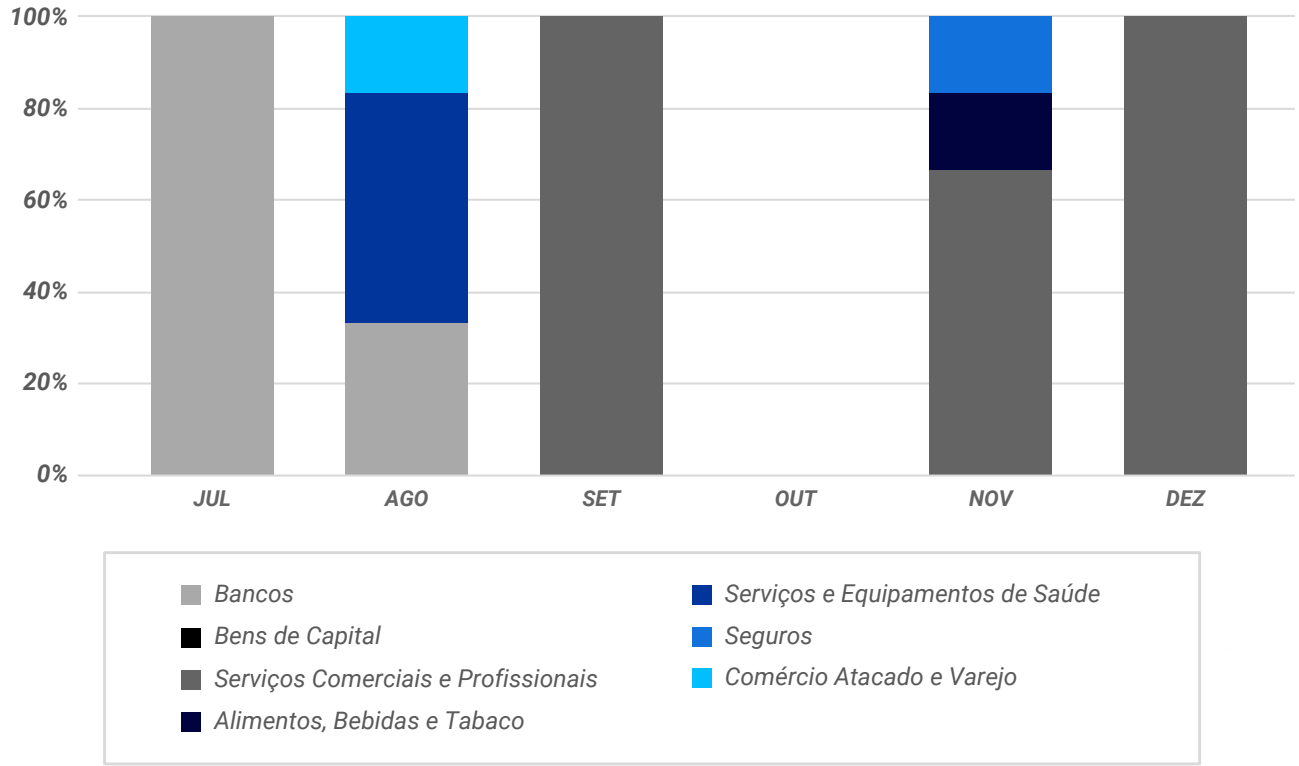


Figura 16 - Setores atacados pelo Hive, 2021

INFOSTEALERS

O RedLine é uma família de infostealers distribuída em campanhas de e-mail de phishing com temas de COVID-19.

REDLINE

O RedLine é uma família de infostealers distribuída em campanhas de e-mail de phishing com temas de COVID-19. Foi uma ameaça ativa ao longo de 2020. Em 2021, foi entregue em anúncios maliciosos no Google e campanhas de spear phishing contra artistas 3D ou digitais usando tokens não fungíveis (NFTs). Os NFTs são tokens digitais vinculados a ativos que podem ser comprados, vendidos e negociados.

O RedLine é extremamente versátil e apareceu como diversos serviços trojanizados, jogos, cracks e ferramentas. Muitas amostras do RedLine também aparecem com certificados digitais de aparência legítima.

Após o estabelecimento da conexão com seu painel C2, o malware RedLine tem uma ampla gama de aplicativos e serviços. Em todos os casos, tenta exfiltrar ilicitamente os dados das vítimas. O malware coleta informações de navegadores de Internet, clientes de FTP, aplicativos de mensagens instantâneas, carteiras de criptomoedas, serviços de VPN e clientes de games. Também tem funcionalidade remota para entregar e executar outros malwares na máquina da vítima.

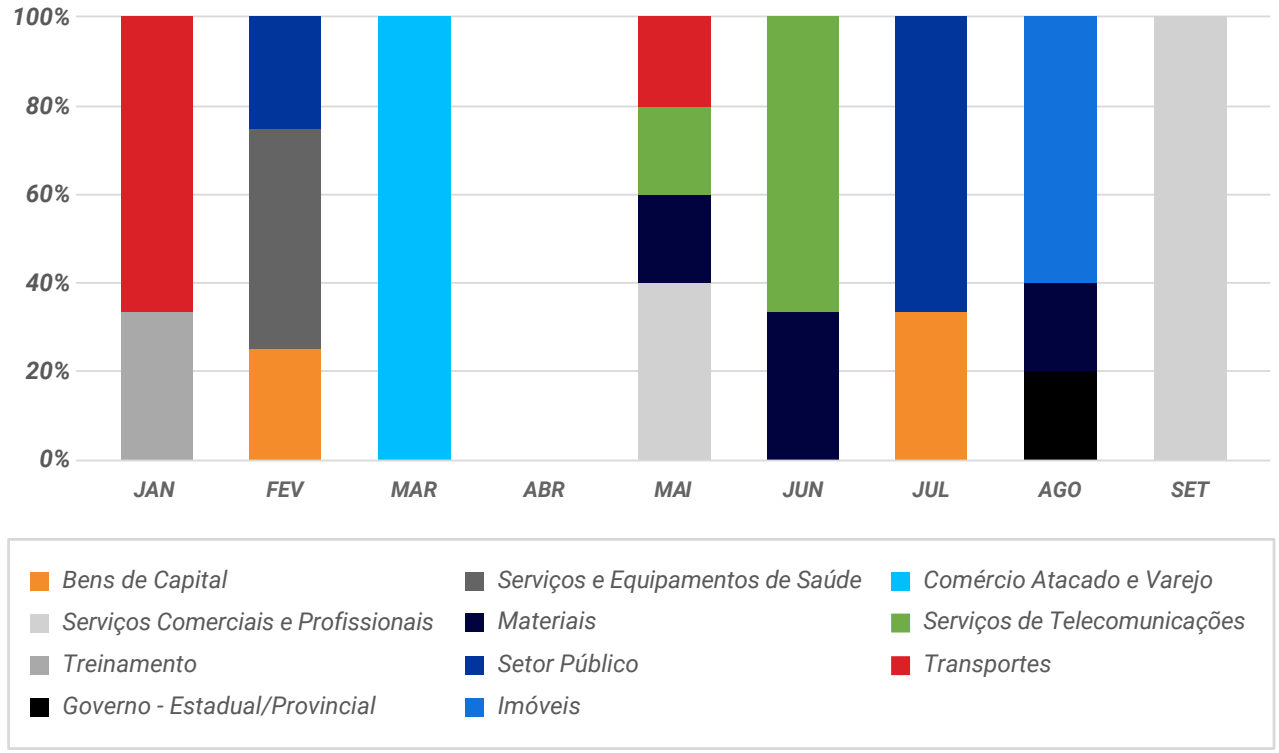


Figura 17 - Setores atacados pelo RedLine, 2021

O infostealer Agent Tesla tem sido consistentemente usado por cibercriminosos em diversas companhas, com frequência usando e-mails de spam para facilitar a infecção.

AGENT TESLA

Observado em circulação pela primeira vez em 2014, o Agent Tesla é compilado em .NET e contém uma gama de recursos potentes para furto de informações. Inicialmente, estava disponível para compra em um website e o autor do malware oferecia diversas licenças com prazo fixo de uso.

Desde então, o infostealer Agent Tesla tem sido consistentemente usado por cibercriminosos em diversas companhas, com frequência usando e-mails de spam para facilitar a infecção.

O malware evoluiu para coletar informações sobre um perfil de Wi-Fi de usuário, potencialmente como mecanismo de propagação. Esse upgrade ocorreu após um aprimoramento similar na variante de malware Emotet, que também recebeu um spreader de Wi-Fi.

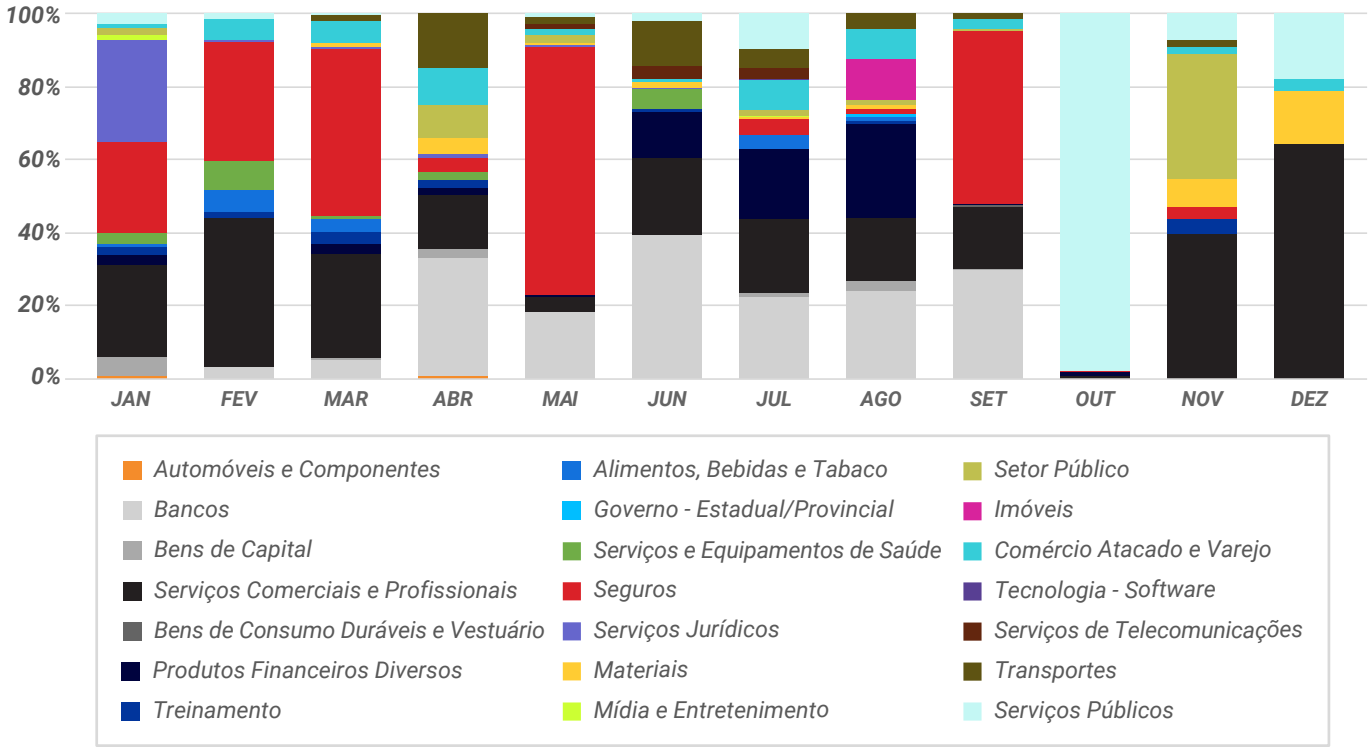


Figura 18 - Setores atacados pelo Agent Tesla, 2021

O Ficker é um infostealer malicioso que encaminha as vítimas para páginas que ofereciam downloads gratuitos de serviços pagos legítimos, como Spotify e YouTube Premium™.

FICKER

O Ficker é um infostealer malicioso que é vendido e distribuído em fóruns underground russos por um agente de ameaças que usa o alias [at]ficker. Este MaaS foi identificado em circulação pela primeira vez em 2020.

O Ficker foi distribuído anteriormente com links da web trojanizados e websites comprometidos. Por exemplo, podia encaminhar as vítimas para páginas que ofereciam downloads gratuitos de serviços pagos legítimos, como Spotify e YouTube Premium™. Também foi implementado pelo Hancitor, um downloader de malware conhecido.

Programado em Rust, o Ficker tem diversos alvos para suas atividades de furto de informações, incluindo:

- Navegadores de Internet
- Informações de cartões de crédito
- Carteiras de criptomoedas
- Clientes de FTP
- Outros aplicativos

O Ficker usa verificações antianálise e pode implementar funcionalidades adicionais e fazer download de malware adicional depois que um sistema é comprometido com êxito.

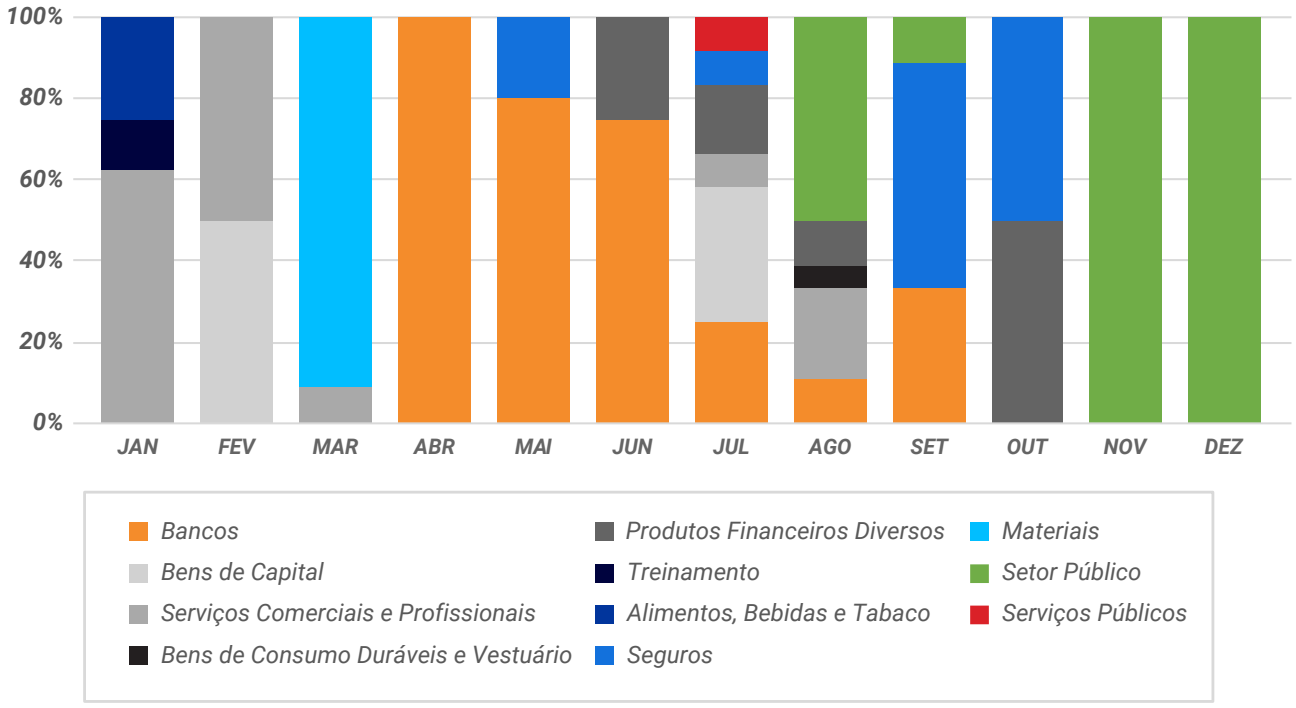


Figura 19 - Setores atacados pelo Ficker, 2021

HANCITOR

O Hancitor (também conhecido como Chanitor) foi descoberto em circulação pela primeira vez em 2013. Dissemina-se por técnicas de engenharia social, como aparentar ser do DocuSign®, um serviço legítimo de assinatura de documentos. Depois que as vítimas são enganadas para permitir que seu código malicioso de macro seja executado, infecta os sistemas.

Em seguida, o Hancitor se conecta com sua infraestrutura C2 e tenta fazer download de diversos componentes maliciosos, de acordo com as necessidades da campanha do operador. Este ano, o Hancitor foi observado fazendo download da conhecida família de malwares Ficker (também conhecido como FickerStealer) e também de um payload de Beacon do Cobalt Strike.

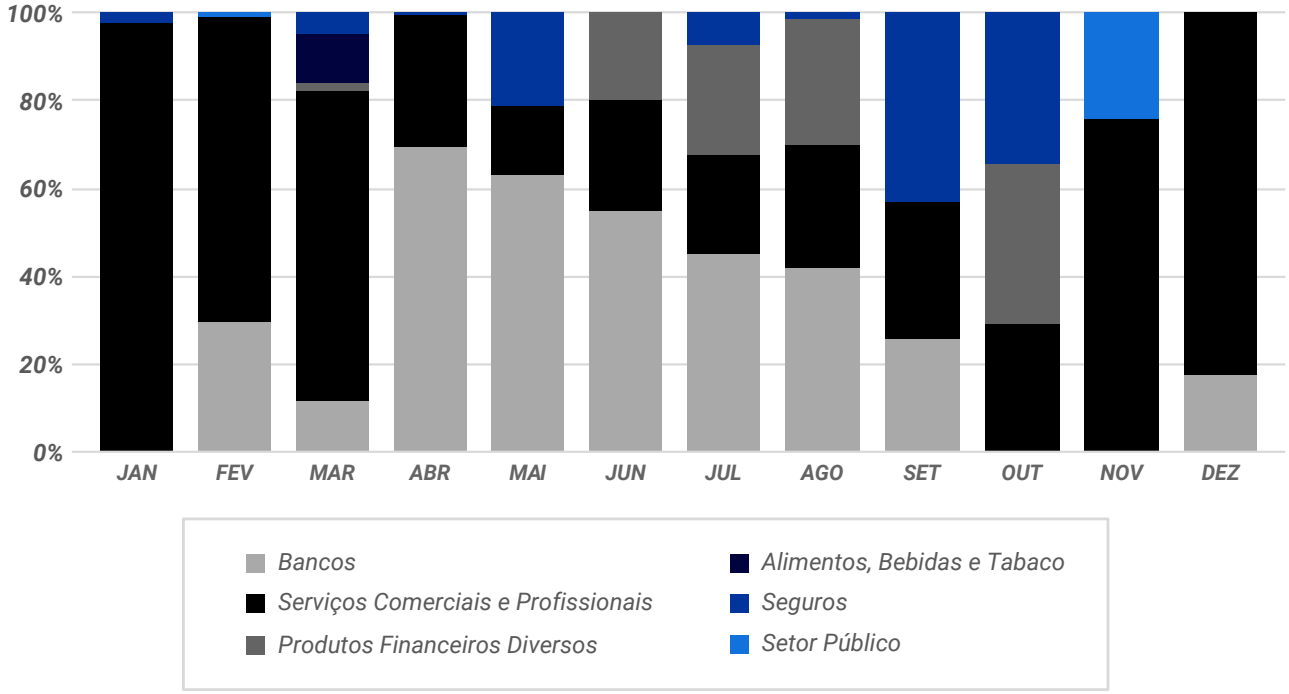


Figura 20 - Setores atacados pelo Hancitor, 2021

AS 10 PRINCIPAIS AMEAÇAS

OCORRÊNCIAS DAS 10 PRINCIPAIS AMEAÇAS EM 2021

A Figura 21 mostra a prevalência mensal de cada família de malware, de acordo com dados internos da BlackBerry.

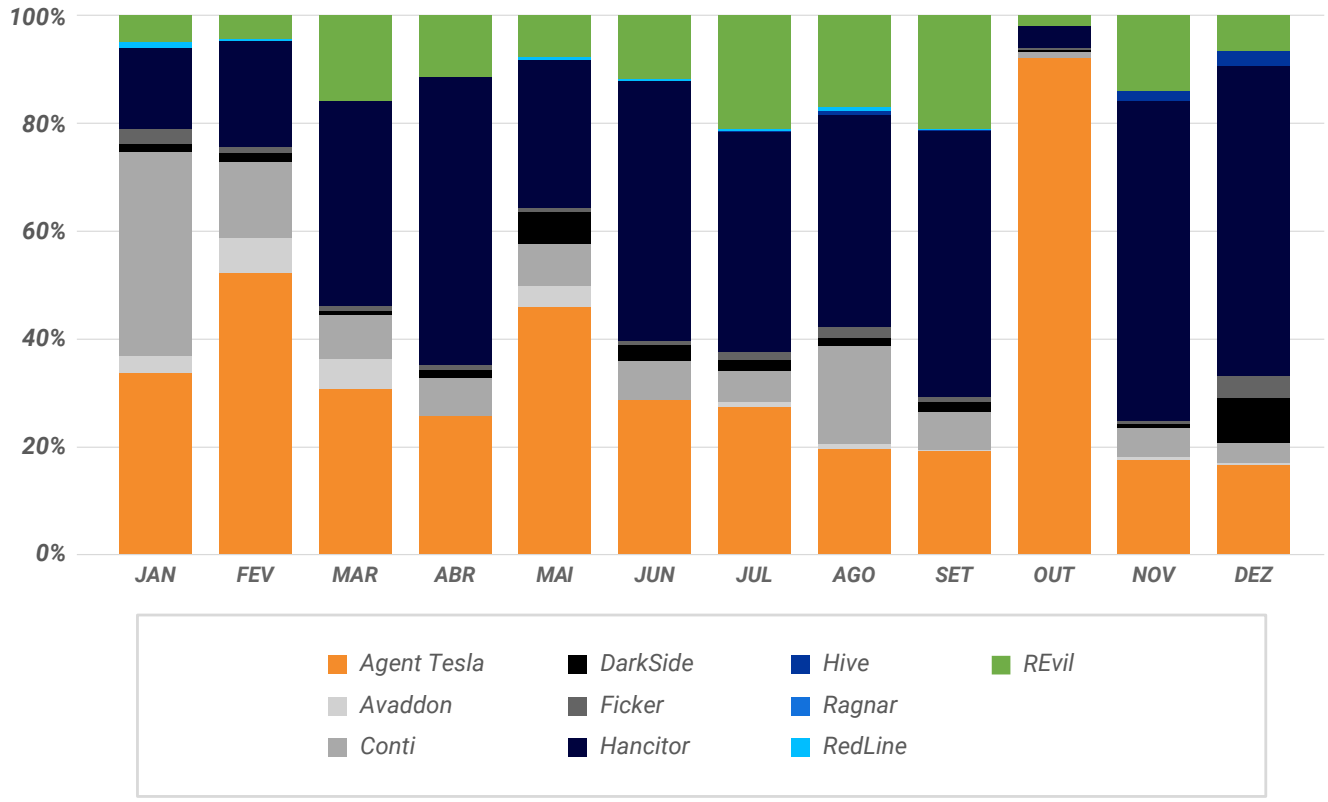


Figura 21 - Prevalência das 10 principais ameaças de malware, 2021

10 PRINCIPAIS X VANTAGEM PREDITIVA DA BLACKBERRY

Ninguém quer ser o paciente zero para uma ameaça nova. Ao aprender lições da rotina do mundo abrangente das ameaças, as organizações não precisam ser.

Com modelos preditivos de detecção de ameaças, os modelos de cibersegurança voltados para o futuro migraram de métodos de detecção legados para técnicas orientadas por aprendizado de máquina (AM). Treinar os modelos de AM extensivamente sobre malwares atuais permite que as soluções orientadas por IA prevejam como as ameaças se apresentarão e se comportarão no futuro. As soluções BlackBerry® desenvolvidas usando Cylance® AI aprendem a prever famílias de malware e variantes emergentes com base em amostras existentes obtidas do cenário de ameaças. Essa abordagem fornece à cibersegurança orientada por IA a capacidade para detectar ameaças conhecidas e de dia zero antes que possam impactar seus alvos.

A Vantagem Preditiva mede retroativamente quanto tempo antes da descoberta um modelo orientado por IA teria detectado e prevenido uma nova ameaça.

O QUE É VANTAGEM PREDITIVA?

A Vantagem Preditiva mede retroativamente quanto tempo antes da descoberta um modelo orientado por IA teria detectado e prevenido uma nova ameaça. Por exemplo, se um modelo de AM protege contra uma ameaça que aparece um ano após a criação do modelo, isso corresponde a uma vantagem preditiva de 12 meses. A medição usa um algoritmo de previsão local offline para testes, sem qualquer atualização ou conexão de Internet. Isso garante que o modelo de AM tenha desempenho exatamente igual ao de sua data de lançamento original, sem aprimoramentos ou upgrades.

A BlackBerry fez um teste de vantagem preditiva para avaliar as nossas detecções em relação às 10 principais famílias de malware descritas neste relatório anual. Isso ilustra quanto tempo antes o modelo de IA ofereceria proteção em relação às maiores ameaças enfrentadas pelos nossos clientes em 2021.

O modelo de IA representado neste teste foi criado em outubro de 2015. Foi implementado com o agente BlackBerry® Protect versão 1320. Os números na Figura 22 mostram com quantos meses de antecedência o nosso modelo poderia ter protegido os clientes contra cada ameaça antes que fosse descoberta.

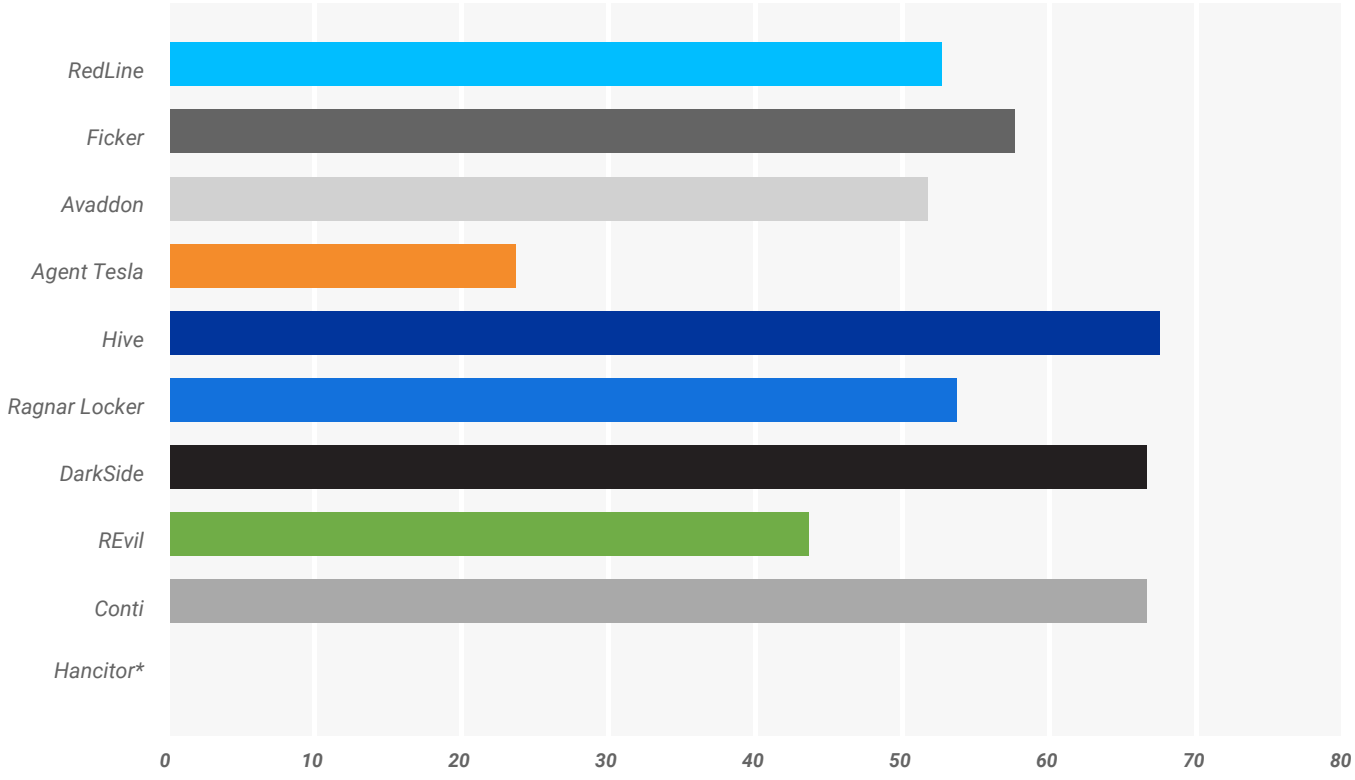


Figura 22 - Vantagem Preditiva da BlackBerry, em meses, em relação às 10 principais ameaças contra nossos clientes
**OBS.: O Hancitor não está representado no gráfico porque foi descoberto antes de outubro de 2015.*

CIÊNCIA DE DADOS

IA E ATAQUES ADVERSARIAIS

Como os exemplos anteriores de Vantagem Preditiva indicam, inteligência artificial e aprendizado de máquina podem ser armas potentes na luta contra o crime cibernético. Infelizmente, também têm potencial para uso inadequado ou abuso nas mãos de agentes sofisticados e sem escrúpulos com intenção maliciosa.

Considere o caso do aprendizado profundo, uma das tecnologias mais empolgantes da década passada. Apesar de sua promessa para o setor, também apresenta outro alvo para comprometimento por agentes de ameaças.

APRENDIZADO PROFUNDO E ATAQUES ADVERSARIAIS

Na década passada, a ascensão do aprendizado profundo (também conhecido como redes neurais) proporcionou um grande benefício para as indústrias técnicas. Essa tecnologia disruptiva tem permitido às empresas melhorar seus produtos e otimizar indicadores-chave de desempenho, identificando padrões antes ocultos em seus dados internos. Esses algoritmos permitiram que as empresas realocassem mão de obra que antes se dedicava a tarefas tediosas de análise: especificamente, as tarefas em que grandes quantidades de conjuntos de regras ou outras heurísticas eram geradas manualmente.

Todo um campo conhecido como aprendizagem adversarial emergiu como uma ameaça a todos os produtos que utilizam algoritmos preditivos.

Infelizmente, esse progresso teve um custo. Todo um campo conhecido como aprendizagem adversarial emergiu como uma ameaça a todos os produtos que utilizam algoritmos preditivos. O objetivo principal deste campo é descobrir maneiras pelas quais as redes neurais podem ser ensinadas a enganar outros algoritmos preditivos alterando sutilmente os dados de entrada. Por exemplo, algoritmos adversariais foram usados para determinar como aplicar pedacinhos de fita a um sinal de parada para torná-lo invisível aos algoritmos de classificação. Para imagens ou áudio, ataques adversariais podem ser usados para fazer alterações quase indetectáveis em uma amostra para enganar algoritmos de previsão altamente precisos.

Em cibersegurança, esses algoritmos têm sido usados para modificar arquivos maliciosos para permitir que ignorem as defesas heurísticas e apoiadas por AM. Não é simples fazer alterações arbitrárias em arquivos (que têm estrutura e regras estruturais próprias); portanto, a maioria desses ataques usa uma estratégia iterativa em massa. Utilizando esta técnica, os algoritmos fazem milhares (ou até centenas de milhares) de pequenas adições a um arquivo que individualmente não têm impacto na sua funcionalidade. No entanto, cada mudança pode empurrar as decisões de um algoritmo preditivo sobre a classificação da ameaça na direção benigna. De forma preocupante, os arquivos gerados por esses algoritmos adversariais parecem poder serem transferidos entre modelos. Isso significa que um ataque treinado em uma defesa pode ser capaz de contornar dúzias de produtos comerciais de cibersegurança.

Apesar do perigo representado por esses algoritmos, o ritmo de pesquisa nessa área está se acelerando, em grande parte devido a incentivos desalinhados. O aprendizado profundo é um campo extremamente competitivo e popular, que oferece aos acadêmicos e às grandes empresas de tecnologia motivação forte para publicar o máximo de pesquisas possível. Como resultado, o campo de ataques adversariais é extremamente ativo. Por exemplo, uma busca por ataques adversariais no Google Scholar™ para 2020 retorna milhares de entradas, das quais algumas centenas têm foco em cibersegurança.

De forma semelhante, os engenheiros de AM que procuram entrevistas em empresas de tecnologia de alto nível geralmente são incentivados a criar pacotes úteis de código aberto para demonstrar suas habilidades. Uma busca rápida por aprendizado adversarial no GitHub retorna quase 5.000 repositórios separados, alguns com mais de 1.000 estrelas (ou curtidas). Os incentivos baseados na carreira tiveram o efeito líquido de democratizar e comoditizar os algoritmos adversariais, tornando-os onipresentes e reduzindo as barreiras de entrada.

DEFESAS ALGORÍTMICAS

Um campo secundário, conhecido como aprendizado adversarial ou defesas adversariais, foi criado pouco depois da descoberta dos ataques adversariais. Essas defesas geralmente têm foco em arquitetar ou treinar modelos, ou pré-processar dados antecipadamente, para mitigar os efeitos dos ataques adversariais.

Este campo ainda está correndo atrás em termos de eficácia geral. Nenhuma defesa adversarial parece ser robusta em ataques de caixa branca, em que o atacante tem pleno conhecimento do tipo de modelo e defesa que estão sendo usados. No entanto, muitas defesas adversarial parecem ser bastante robustas para ataques caixa-preta. Assim, as organizações podem prevenir ataques de caixa-branca e forçar os atacantes a usar ataques de caixa-preta menos eficientes usando algumas técnicas. Podem ofuscar a saída de uma defesa, principalmente reduzindo sua precisão, ou estrangulando a capacidade dos atacantes para consultar uma defesa em massa.

Como foi mencionado antes, os exemplos adversariais com frequência são transferíveis, e são potencialmente capazes de evadir inúmeras defesas, como publicações recentes confirmaram.

No entanto, esses ataques evitaram apenas produtos que não empregavam defesas adversarial geradas por aprendizado profundo. A BlackBerry verificou internamente que os ataques gerados dessa maneira têm pouca probabilidade de contornar os modelos que utilizam vários esquemas defensivos robustos de aprendizado profundo.

Além disso, ataques adversariais contra arquivos precisam adotar abordagens iterativas que não costumam ser usadas em outras áreas (como os modelos visuais ou auditivos). Como resultado, muitos kits de ferramentas de ataque adversarial de código aberto não podem ser modificados facilmente para ter foco em defesas de cibersegurança. Infelizmente, uma consulta no GitHub resulta em algumas páginas contendo o que parecem ser esforços amadores para geração de exemplos adversariais. Isso não é um bom presságio para o que pode acontecer à medida que o campo amadurece.

PERSPECTIVAS

No curto prazo, as perspectivas nesta área são mistas. O campo de ataques adversariais ainda está em alta, e os softwares de código aberto reduziram bastante a barreira de entrada para pessoas que procuram gerar exemplos adversariais. A expertise necessária para gerar desvios ainda é bastante alta. Diante disso, não esperamos um uso generalizado dessa tecnologia nos próximos dois anos.

Quaisquer pacotes adversariais de código aberto provavelmente ainda precisarão contar com abordagens em massa para gerar ataques. Isso significa que as empresas de cibersegurança têm um caminho razoável para o futuro, que pode ser resumido da seguinte forma:

- Contratar pessoas que entendam de aprendizado profundo adversarial
- Usar diversos esquemas defensivos robustos (mesmo para produtos que usam defesas heurísticas)
- Manter os esquemas defensivos em segredo/somente internos
- Impedir que os atacantes consultem rapidamente as defesas para encontrar buracos sutis

Nada em segurança é garantido. No entanto, para as organizações que seguem essas regras, os ataques adversariais deverão ser um vetor de ameaças administrável em curto prazo.

INSIGHTS DE CIBERSEGURANÇA

REVISÃO DO ANO DE RESPOSTA A INCIDENTES E TENDÊNCIAS

O ransomware continuou a ser destaque para a BlackBerry Incident Response Team no ano passado. Como foi discutido no Relatório de Ameaças BlackBerry de 2021, a estratégia de dupla extorsão de resgate e exfiltração de dados agora se tornou o padrão. Na verdade, a tendência aumentou, com instâncias de extorsão tripla (adicionando assédio) e quádrupla (ataques disruptivos, como DDoS). Como resultado dessas estratégias de agentes de ameaças em expansão, há um aumento crescente no vazamento de dados públicos.

A evolução dos métodos de extorsão criou um alinhamento estreito entre as táticas usadas pelos agentes de ameaças de APTs que são estados-nação e as organizações criminosas com fins lucrativos. Suas abordagens e objetivos operacionais são surpreendentemente semelhantes, embora as motivações centrais, os níveis de perícia técnica e os métodos de execução variem. Assim, a grande maioria dos ataques que ocorrem atualmente seguem um padrão semelhante, conforme detalhado na Figura 23.

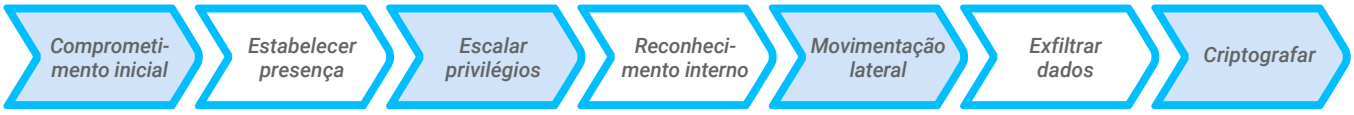


Figura 23 - Fluxo típico de ataque por agente de ameaças

Uma das principais diferenças entre os grupos de APTs e as organizações de ransomware é quanto tempo cada grupo planeja permanecer ativo no ambiente. Isso, por sua vez, afeta o sigilo com que atuam. Os grupos de APTs com frequência planejam residências de longa duração no ambiente das vítimas. Os grupos de ransomware são mais como invasores de casas que quebram a janela e levam o que encontram.

Por exemplo, as APTs muitas vezes preferem a abordagem "live off the land", usando recursos legítimos do sistema, de modo que sua atividade é difícil de distinguir das operações diárias. Dedicam tempo para estudar cuidadosamente um ambiente e entender as medidas de segurança em vigor antes de executar qualquer ação maliciosa. Os ataques de ransomware são mais oportunistas e, portanto, operam com mais rapidez e imprudência. Como resultado, costumam gerar mais ruído, que pode ser detectado por uma plataforma de proteção de endpoints (EPP) ou ferramentas de detecção e resposta em endpoints (EDR). Por exemplo, podem usar ferramentas como PowerShell, scripts em lotes do Windows ou WMI para tentar desativar produtos antivírus, soluções de backup e outros processos de sistema.

Outra diferença importante é que os grupos de estados-nação geralmente procuram informações específicas para exfiltrar. Podem ter fins de espionagem, muitas vezes em busca de vantagens políticas ou econômicas. Por outro lado, os grupos de ransomware geralmente procuram qualquer item valioso que possa aumentar a probabilidade de serem pagos. Os favoritos frequentes incluem bancos de dados que podem conter informações de clientes ou financeiras.

Aos olhos do público, o tamanho realmente importa quando se trata de notícias e vazamento de dados. Portanto, os agentes de ameaças com fins lucrativos tentarão obter o máximo que puderem enquanto estiverem no sistema ou rede.

Como resultado, a BlackBerry observou algumas abordagens automatizadas de "metralhadora" para exfiltração de dados por grupos de ransomware no ano passado. Algumas têm scripts com engenharia sofisticada que visam tipos de arquivos específicos para coleta: em geral, documentos Microsoft® Word, Excel® e PDF com menos de um ano de idade. Os dados furtados são carregados na infraestrutura do atacante. Em outras instâncias, a BlackBerry identificou agentes de ameaças que tentam compactar unidades compartilhadas inteiras de nível superior nas organizações, para tenta pegar tudo o que está disponível.

Além de grupos de ransomware como Conti, DarkSide, BlackMatter e outros que são destaque nas notícias atualmente, há um novo influxo de operações de ransomware ocorrendo por RaaS. A BlackBerry observou diversos incidentes em que empresas foram atacadas usando uma variante de um ransomware conhecido. No entanto, as táticas, técnicas e procedimentos (TTPs) usados pelo atacante não tinham sofisticação ou profundidade. Em diversos incidentes, a BlackBerry identificou agentes de ameaças que deixavam arquivos de texto de playbook contendo IOCs com comandos exatos, endereços IP, listas de alvos e mais. Isso sugere que os autores dessas famílias sofisticadas de ransomware não são as pessoas que estão realizando os ataques.

Os atacantes com motivação financeira ainda têm foco nos alvos de acesso mais fácil para a fase de comprometimento inicial do ataque.

Os atacantes com motivação financeira ainda têm foco nos alvos de acesso mais fácil para a fase de comprometimento inicial do ataque. Infelizmente, houve uma superabundância de alvos no ano passado devido ao uso contínuo de tecnologias e infraestruturas mais antigas em ambientes de vítimas, como servidores locais. Por exemplo, ProxyLogon e ProxyShell, nomes comuns de dois conjuntos de vulnerabilidades com impacto em muitos Microsoft Exchange Servers no local, foram amplamente explorados ao longo de 2021. O grupo de APTs HAFNIUM foi o primeiro a explorar as vulnerabilidades em diversas organizações. Após a publicação da vulnerabilidade do ProxyLogon e de exploits de prova de conceito, outros agentes de ameaças começaram a examinar e infectar rapidamente diversos hosts Exchange no local. Os agentes de ameaças que exploravam essas vulnerabilidades com frequência instalaram backdoors adicionais, em geral na forma de web shells China Chopper, um web shell cada vez mais popular que tem grande alcance em pacote pequeno.

O RDP acessível externamente continua a ser um favorito duradouro; no entanto, está se tornando menos comum em comparação com outras técnicas. As vulnerabilidades que afetam appliances, especialmente VPNs, firewalls e dispositivos de rede de perímetro, continuam sendo a causa raiz de muitos incidentes. Embora essas vulnerabilidades sejam frequentemente datadas e bem documentadas, a BlackBerry observou vários incidentes em que os dispositivos permaneceram sem correção.

Em outros casos, os dispositivos rede anteriormente vulneráveis foram corrigidos, mas só depois que já tinham sido comprometidos. Esses incidentes resultaram em roubo de credenciais ou instalação de backdoors. O grande número de ambientes e credenciais comprometidos reforçaram os florescentes marketplaces da dark web, onde as contas de administrador de domínio valem mais. No entanto, não é difícil encontrar credenciais de empresas ou particulares que também estejam disponíveis gratuitamente.

Além das técnicas mencionadas anteriormente, a BlackBerry observou vários incidentes envolvendo ataques de watering hole. Os ataques de watering hole proporcionam aos agentes de ameaças uma forma única de obter presença e estabelecer acesso persistente em um ambiente. Esses ataques visavam usuários que faziam pesquisas legítimas de material relacionado a negócios, uma prática comum no local de trabalho. Nesses incidentes, os resultados de pesquisa retornavam o URL do watering hole perto do início da primeira página da pesquisa no Google™. O site de watering hole apresentava ao usuário o que parecia ser uma publicação útil em fórum, contendo um link para exatamente o que eles precisavam. Incluía vários comentários falsos, alegando que o link de arquivo era uma correspondência exata para a consulta.

No entanto, se os usuários abrem o documento armamentizado, um malware é baixado e instala um Beacon do Cobalt Strike, com que os agentes de ameaças obtêm presença no ambiente.

O REvil é um dos grupos de ataques mais conhecidos que usam esse estratagema atualmente. Este grupo de ameaças foi identificado inicialmente em 2019. É um dos grupos de ransomware dominantes e assume a responsabilidade por alguns dos ataques de ransomware mais famosos dos últimos anos. Também tinha vínculos próximos com o DarkSide Group, responsável pelo ataque à Colonial Pipeline. Esse grupo ligado à Rússia esteve sob vigilância recentemente e passou à clandestinidade em várias ocasiões, mas depois reaparecia.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

O uso cada vez maior do Cobalt Strike é outra tendência observada no ano passado. A BlackBerry observa seu uso como kit de ferramentas pós-exploit altamente eficaz e popular há vários anos. Seu abuso continuou a aumentar a ponto de não ser incomum encontrar evidências de uso durante um engajamento de resposta a incidentes. Para quem não conhece ainda, a BlackBerry recomenda ler o novo livro sobre o Cobalt Strike, publicado pela BlackBerry Threat Research and Intelligence Team em novembro de 2021.

CICLO DE VIDA DOS ATAQUES

A Red Team da BlackBerry analisa o ciclo de vida completo do ataque como parte de nossa missão e do portfólio de ofertas de serviços. Nossa simulação adversarial de ponta a ponta fornece um ponto de vista único sobre o agente de ameaças, permitindo observar a eficácia das diferentes defesas em uma variedade de organizações. Essas experiências nos levaram a revelar alguns dos ataques mais comuns e as defesas eficazes que encontramos.

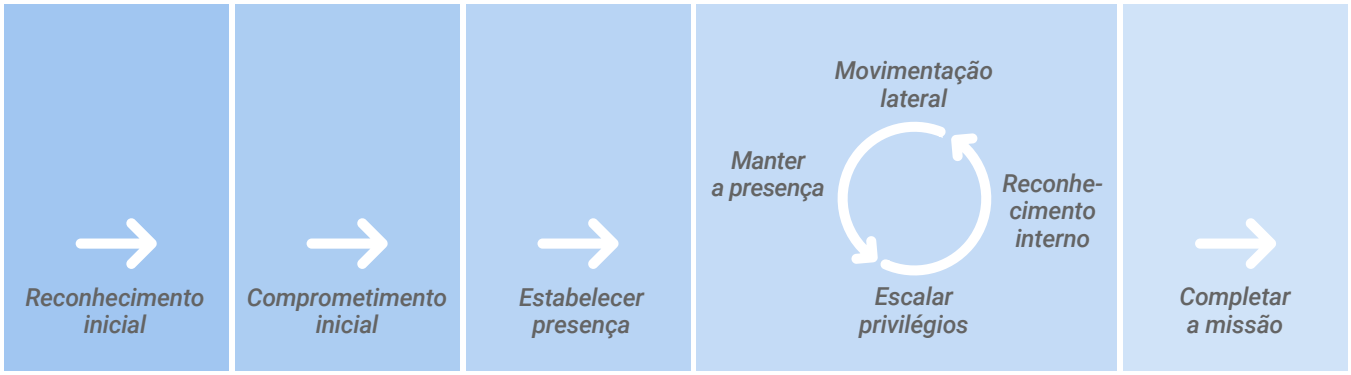


Figura 24 - Ciclo de vida típico dos ataques

RECONHECIMENTO INICIAL

O reconhecimento inicial de um atacante pode ser passivo, ativo ou ambos. Como o reconhecimento passivo não toca nos sistemas do alvo, pode ser difícil de detectar. No entanto, depois que o reconhecimento migra para atividades mais ativas e intrusivas, como sistemas de sondagem de vulnerabilidades, os defensores devem ser alertados. As principais estratégias defensivas para esta fase envolvem conhecer os ativos da organização, varredura proativa, patching, monitoramento e redução da superfície de ataque.

COMPROMETIMENTO INICIAL E ESTABELECIMENTO DA PRESENÇA

Depois que uma vulnerabilidade é descoberta durante a fase de reconhecimento, os atacantes exploram a vulnerabilidade e estabelecem a presença no host. A partir daí, os agentes de ameaças podem voltar a entrar posteriormente e acessar outros sistemas na rede. Esta atividade deve ser detectada e bloqueada pelas organizações por meio de uma defesa em camadas, com rede baseada em IA, visibilidade de hosts e bloqueio.

ENCAMINHAMENTO

Os atacantes em geral obtêm acesso equivalente ao do aplicativo que invadiram e usam para comprometer o host. Este é um dos muitos motivos pelos quais o princípio de menor privilégio é importante. Além de seguir as melhores práticas, o software EPP deve conter camadas de defesa para incluir bloqueio de scripts e proteção de memória.

O objetivo é tornar extremamente difícil para um atacante atingir cada etapa do ciclo de vida do ataque. Retardar o progresso do adversário também ganha tempo para os defensores detectarem e bloquearem o ataque.

RECONHECIMENTO INTERNO E MOVIMENTAÇÃO LATERAL

Depois que um atacante obtiver privilégios suficientes, vai percorrer a rede e se posicionar para atingir o alvo. Uma das melhores defesas nesta situação é usar segmentação de rede e procurar anomalias que resultem do uso de credenciais roubadas. Nesta fase, as equipes de defesa podem se beneficiar muito de usar tecnologia de defesa habilitada por IA, como autenticação contínua usando biometrias passivas. As biometrias passivas são atividades de baixa carga de usuário (como padrões de uso de teclado e mouse) que identificam usuários com exclusividade. Um algoritmo de AM pode ser aplicado a esses metadados para criar uma pontuação de risco. Em seguida, as organizações podem usar ações, como forçar reautenticação ou bloquear usuários, quando a pontuação de risco excede o limiar definido para a organização.

Formas como os agentes de ameaças podem obter pagamento

Vender dados roubados

Ameaçar vender dados roubados

Desbloquear dados criptografados

COMPLETAR A MISSÃO

Antes que a Red Team da BlackBerry faça um exercício de simulação adversarial, definimos os objetivos junto com os clientes. Isso quase sempre inclui algum tipo de exfiltração (ou flag) de dados, porque muitos agentes de ameaças têm motivação financeira. Os agentes de ameaças podem ser pagos de muitas formas, como vendendo dados furtados, ameaçando vender dados furtados ou bloqueando dados criptografados.

CONCLUSÃO

Estas são algumas verdades universais úteis que devemos ter em mente sobre o ciclo de vida de ataques e a cadeia de ataque digital:

- Seja proativo. "Quanto mais à esquerda" você estiver no ciclo de vida do ataque (ver a Figura 24), mais fácil e barato é identificar e bloquear um ataque.
- Qualquer medida inferior a monitoramento 24 horas não é suficiente.
- A missão da maioria dos agentes de ameaças atualmente é exfiltrar dados e lançar ransomwares para obter lucros.
- As defesas baseadas em IA ajudam as organizações a evitar ser um paciente zero e são imunes ao atraso gerado pela criação de assinaturas que ocorre com as defesas tradicionais.
- Os esforços defensivos devem sempre ser contínuos, devido às vulnerabilidades recém-descobertas e à evolução constante do cenário de ameaças.
- Prevenção é essencial. A capacidade para se recuperar com backups não aborda a tática de extorsão dupla derivada da ameaça de venda de dados furtados pelos atacantes.

PROTEÇÃO DE INFRAESTRUTURA CRÍTICA

Todas as organizações, em todos os verticais, correm o risco de violação, implantação de ransomware e extorsão. No entanto, no mundo real, poucas têm o mesmo risco de ciberataques como no setor de infraestrutura crítica. O público espera que serviços públicos como energia, gás, água e tratamento de resíduos estejam sempre aptos a fornecer esses serviços essenciais. Como resultado, essas organizações estão significativamente motivadas a atender a essas expectativas, o que as torna alvos lucrativos para resgate e extorsão.

Infelizmente, os desafios para esse setor não se resumem a serem alvos de alto valor. Os seguintes fatores geralmente agravam o problema:

- Dispositivos mais antigos, intrinsecamente vulneráveis e sensíveis
- Sistemas operacionais legados
- A necessidade de ambientes offline/desconectados

Todas as organizações, em todos os verticais, correm o risco de violação, implantação de ransomware e extorsão. No entanto, no mundo real, poucas têm o mesmo risco de ciberataques como no setor de infraestrutura crítica.

Muitos sistemas e dispositivos de infraestrutura crítica existem há muito tempo e foram originalmente projetados para comunicação serial, mas posteriormente adaptados para redes TCP/IP ubíquas. Essa adaptação de conectividade pode não incluir necessariamente um upgrade de segurança. Como esses ambientes podem ser difíceis e caros de modernizar, em geral executam sistemas operacionais mais antigos e com frequência sem suporte.

A necessidade de proteger os ambientes costuma resultar em segmentação de outras redes e, espera-se, também da Internet. No entanto, essa segmentação apresenta desafios adicionais de administração e proteção.

Em resumo, as proteções precisam ser ampliadas para dispositivos mais antigos, que executam sistemas operacionais legados e estão desconectados das redes e da Internet. Uma solução possível é o uso de proteção de endpoints baseada em aprendizado de máquina que reside no próprio endpoint. Esse tipo de software de plataforma de proteção de endpoints (EPP) pode ser executado em sistemas operacionais legados como Windows XP/2003. Se for leve, não vai sobrecarregar o hardware antiquado. O modelo matemático localizado deve ser projetado para evitar a necessidade constante de implementação de atualizações de assinaturas.

Os softwares AV legados exigem a criação de assinaturas para as ameaças mais recentes. Em alguns casos, são lançadas a cada hora. É difícil acompanhar isso, mesmo em equipamentos modernos e hosts conectados à Internet. Portanto, é inadequado para infraestrutura crítica que está desconectada e exigiria uma abordagem de “sneakernet” para distribuição de atualizações de assinaturas. As defesas baseadas em IA permitem um tempo de espera muito mais longo antes de exigir atualizações, pois identificam ameaças usando milhões de atributos, e não por meio de assinaturas conhecidas.

A infraestrutura crítica é um ambiente desafiador para proteger, mas a situação não é desesperadora. Como outros setores, simplesmente precisa evoluir além da dependência de tecnologia defensiva herdada que não pode ser redimensionada para evitar ciberataques modernos.

IA COM PREVENÇÃO EM PRIMEIRO LUGAR

IA e AM oferecem muitas capacidades e vantagens para proteger as organizações contra ciberataques. Embora os termos IA e AM sejam frequentemente usados de forma intercambiável, são conceitos diferentes em alguns aspectos essenciais. IA descreve a capacidade de computadores e máquinas para realizar atividades que imitam o comportamento humano inteligente. AM é um subconjunto da IA que se baseia em algoritmos matemáticos para atingir o comportamento e a função da IA. O processo por trás do treinamento de AM requer acesso a grandes quantidades de dados históricos como base para o aprendizado. Em várias fases, novos dados são introduzidos para aprimorar as funções de aprendizagem do modelo de AM, até que se torne um componente de IA.

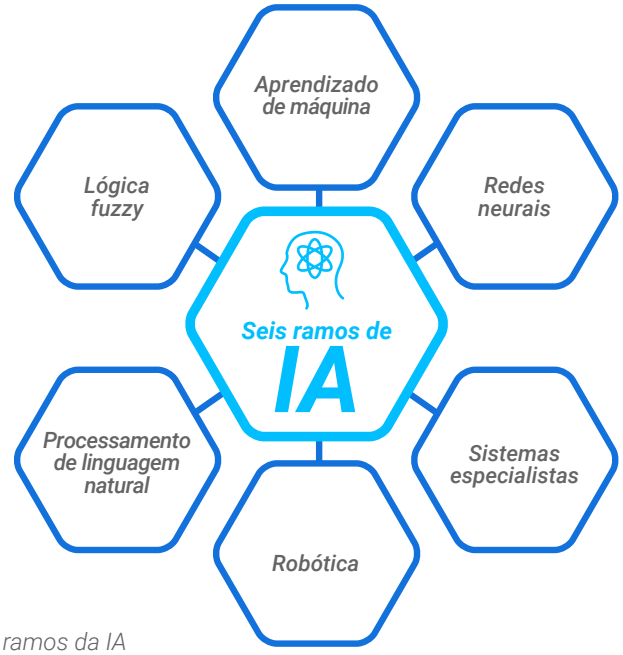


Figura 25 - Os seis ramos da IA

Na verdade, o AM é apenas um dos seis ramos da IA. Os outros ramos são: redes neurais, sistemas especialistas, processamento de linguagem natural, lógica fuzzy e robótica. O Cylance IA da BlackBerry, por exemplo, associa AM e redes neurais para identificar e prevenir ciberataques antes que sejam executados. Como os agentes de segurança de IA são bem treinados e extremamente leves, podem residir nos endpoints dos usuários sem afetar os recursos. Esses agentes de segurança no dispositivo protegem os dispositivos online e offline. A BlackBerry dedicou esforço e financiamento de pesquisa e desenvolvimento consideráveis para desenvolver o Cylance IA. Temos centenas de patentes em IA, AM, segurança e análise forense, o que nos coloca ao lado de outras empresas líderes em IA, como Google, Facebook e Amazon.

O AM é classificado em duas categorias: supervisionado e não supervisionado. Essas classificações descrevem como os modelos de AM aprendem a classificar os dados de entrada com as suposições de saída corretas; em outras palavras, como fazem previsões corretas.

O aprendizado supervisionado é um processo assistido em que o algoritmo matemático é orientado para prever os resultados da entrada de um conjunto de dados de treinamento. Com esse método, pessoas supervisionam o AM, rotulando manualmente os conjuntos de dados de treinamento. O AM supervisionado é como uma criança aprendendo a andar de bicicleta com rodinhas. Um adulto oferece orientação, até que a criança esteja pronta para remover as rodinhas e andar sozinha. O aprendizado supervisionado requer quantidades imensas de dados de treinamento e orientação antes que os modelos matemáticos possam avaliar as entradas e retornar as saídas desejadas.

O AM não supervisionado classifica os dados com as suposições de saída corretas sem intervenção humana ou dados rotulados. O aprendizado não supervisionado é geralmente o segundo estágio de treinamento de modelos matemáticos, depois que ingerem grandes quantidades de dados de entrada com conjuntos de treinamento supervisionado. Essa fase permite que os cientistas de dados vejam como os modelos matemáticos são executados por conta própria e como criam as saídas desejadas. Voltando à alegoria da bicicleta, o aprendizado não supervisionado é o adulto removendo as rodinhas e vendo se criança consegue andar de bicicleta sem ajuda.

IA + AM

Na BlackBerry, nossos modelos matemáticos de IA usam AM supervisionado e não supervisionado para treinar como identificar um binário bom e diferenciá-lo de um binário ruim.

Na BlackBerry, nossos modelos matemáticos de IA usam AM supervisionado e não supervisionado para treinar como identificar um binário bom e diferenciá-lo de um binário ruim. Os conjuntos de dados são extensos e baseados em milhões de características de arquivos. Ao determinar o perigo de um arquivo, suas características (tudo o que compõe o arquivo) são extraídas para fornecer essencialmente seu DNA digital. Essas características são correlacionadas com aproximadamente 2,7 milhões de outras, em que os nossos modelos matemáticos já foram treinados anteriormente. Ao treinar com um conjunto tão grande de recursos de arquivos, o Cylance IA aprendeu a identificar rapidamente o que é um arquivo bom ou ruim (também conhecido como malicioso).

O BlackBerry Protect, que foi desenvolvido usando Cylance IA, pode executar essa correlação de recursos em até 100 milisegundos ou menos. E, o que é mais importante, antes da execução. Isso significa que pode bloquear a ameaça antes que seja executada. O BlackBerry Protect impede a execução de arquivos maliciosos, não importa se são malwares conhecidos ou uma ameaça nunca antes vista. Essa capacidade para bloquear malwares novos e de dia zero é conhecida como Vantagem Preditiva da BlackBerry. É alcançada com a precisão de nossos modelos matemáticos, que conseguem identificar corretamente arquivos maliciosos, muitas vezes anos antes de serem vistos em circulação.

COMO A EXTRAÇÃO/VETORIZAÇÃO DE CARACTERÍSTICAS É REALIZADA?

Para que as máquinas interpretem as associações de extração de características de AM e produzam uma saída, é necessário que a vetorização ocorra. Vetorização é o processo de converter dados de entrada em vetores matemáticos usando um formato legível por algoritmos de AM e computadores.

A vetorização existe desde que os computadores foram criados. É como os modelos matemáticos de AM podem correlacionar e agrupar as boas características de arquivos, separando-as das ruins. Formata informações de características de arquivos de uma forma que computadores e modelos matemáticos entendam, e habilita que forneçam

saídas. Quando uma característica de arquivo, como código esperado em uma área específica da memória, é extraída de um arquivo, é convertida em um valor matemático de 1s e 0s. Isso permite que os algoritmos de AM do BlackBerry Protect identifiquem se um arquivo é seguro. Se for, é liberado para execução. Os arquivos maliciosos são bloqueados e colocados em quarentena.

Deve-se observar que o BlackBerry Protect, nas fases iniciais do processo de aprendizagem de algoritmos, identificou cerca de 300 milhões de características de arquivos. Desde então, isso foi reduzido a 2,7 milhões de características críticas que podem ser usadas para categorizar e etiquetar a segurança de arquivos. As características referem-se tanto ao que é encontrado em arquivos como ao que é esperado. Por exemplo, caso seja esperado que dados específicos constem em uma parte específica do DNA de um arquivo, mas não estão presentes, isso também é uma característica.

Uma IA bem treinada oferece uma vantagem incrível sobre as contrapartes humanas para fazer esse trabalho de análise e previsão. Um analista humano pode levar um tempo considerável para identificar 150 a 200 características de um arquivo. Algoritmos de AM treinados podem identificar, correlacionar e avaliar milhões de características de arquivos e determinar a ameaça de um arquivo em milissegundos.

UMA ABORDAGEM DE PREVENÇÃO EM PRIMEIRO LUGAR PARA PROTEGER A FORÇA DE TRABALHO CADA VEZ MAIS HÍBRIDA

É tentador colocar a culpa pelo aumento maciço de ciberataques nos últimos 18 meses na pandemia de COVID-19 e na migração resultante para uma força de trabalho distribuída. Uma pesquisa da IBM recente parece apoiar essa visão:

US$ 1,07 milhão

Aumento em custos com violações (de US$ 3,89 milhões para US$ 4,96 milhões) quando o trabalho remoto era um fator.

58 dias

Mais tempo para identificar e conter uma violação quando 50% ou mais dos funcionários trabalham remotamente.

É verdade que expandir a rede corporativa para abranger o ambiente doméstico e os dispositivos pessoais cria novas brechas de segurança para os adversários explorarem. Mas se nossas tecnologias e práticas de segurança atuais fossem robustas o suficiente para facilitar o redimensionamento, a transição poderia ter sido muito menos disruptiva para muitas organizações do que acabou sendo.

Spear phishing e abuso de credenciais eram grandes problemas antes da pandemia. Continuam a responder pela maioria das invasões hoje. Produtos de infraestrutura de desktop virtual e VPN eram vulneráveis a exploits antes da COVID-19. Continuam sendo atualmente. E o mesmo ocorre com servidores não corrigidos e ameaças causadas por pessoas internas maliciosas, ou por usuários com higiene cibernética ruim.

O verdadeiro problema é que as abordagens de segurança atuais são insustentáveis, porque são inerentemente reativas e irrealistas. Não se deve esperar que um funcionário de recursos humanos responsável por examinar currículos o dia inteiro saiba quando um documento está armamentizado e evite abri-lo. Não se pode esperar que os profissionais de SecOps e NetOps responsáveis por proteger uma infraestrutura complexa e que muda rápido possam prever e bloquear manualmente todos os ataques possíveis.

O problema não pode ser solucionado treinando todos os funcionários para que também se tornem especialistas em cibersegurança. E não pode ser corrigido adicionando mais uma ferramenta ou camada de segurança a uma arquitetura de segurança fundamentalmente reativa. A BlackBerry acredita que uma solução mais realista é a transição para uma estratégia de segurança com prevenção em primeiro lugar. Ao alavancar soluções inteligentes, com foco em bloquear e impedir ciberataques, os funcionários podem se concentrar no trabalho para o qual foram contratados.

No nível do dispositivo, isso significa bloqueio e combate tradicional. Sistemas vulneráveis devem ser corrigidos e atualizados. As defesas reativas baseadas em assinaturas devem ser substituídas com proteção de endpoints com tecnologia de IA que impede a execução de malwares conhecidos e de dia zero.

Em seguida, controles de segurança com foco no usuário devem ser implementados em cada ponto de entrada de aplicativos de rede e nuvem da empresa para evitar que funcionários remotos abusem de suas credenciais ou violem as políticas de segurança, de forma intencional ou acidentalmente. O acesso de cada usuário aos recursos deve ser controlado dinamicamente, com base em avaliações de risco em tempo real de seu comportamento atual. Para preservar a produtividade, esse processo de autenticação contínua deve ser o mais transparente possível para os usuários, mas não permitir soluções alternativas ou evasões.

Ferramentas que dependem de análise baseada em regras estáticas não conseguem fazer isso. Simplesmente não é possível conceber regras que prevejam cada gradação de comportamento arriscado ou anômalo. E a análise retrospectiva que costumam produzir chega tarde demais para impedir a exploração. Isso requer soluções construídas com IA que aprendam a avaliar os riscos e evitar a exploração de forma proativa, e não respondam após o fato quando o dano já estiver em andamento.

Com implementação adequada, a estratégia de prevenção em primeiro lugar preserva os benefícios de flexibilidade e produtividade de ter uma força de trabalho remota ou híbrida.

Prevenção e produtividade em equilíbrio: o melhor dos dois mundos.

DETECÇÃO E RESPOSTA ESTENDIDAS (XDR)

As equipes de segurança enfrentam diversos desafios atualmente. Os atacantes estão executando rapidamente ataques mais sofisticados, furtivos e multivetoriais em várias superfícies de ataque, incluindo endpoints, nuvem, redes, aplicativos e dispositivos móveis. As soluções de detecção e resposta em endpoints (EDR) criaram um plano de defesa, ao fornecer recursos avançados de detecção de ameaças e resposta a incidentes para endpoints. No entanto, é necessária uma proteção mais proativa e abrangente em toda a superfície do ataque.

Essa demanda impulsionou a criação do XDR. É uma evolução do EDR, unificando a proteção no endpoint com outras ferramentas de segurança. Oferece aos analistas de segurança: visibilidade aprimorada, detecção de alta eficácia, correlação, investigação e resposta mais eficazes.

O XDR é uma evolução do EDR e unifica a proteção no endpoint com outras ferramentas de segurança. Oferece aos analistas de segurança: visibilidade aprimorada, detecção de alta eficácia, correlação, investigação e resposta mais eficazes.

O QUE É XDR?

Os produtos XDR são, na essência, estratégias para inclusão e enriquecimento de dados. Isso significa que incorporam informações coletadas em suas próprias plataformas de produtos e as integram com a telemetria ingerida de parceiros e outras fontes. Esses dados são combinados para criar contexto adicional, que é compartilhado como inteligência de ameaças cibernéticas (CTI) acionável no produto.

Quando usada para caçar ameaças, a combinação com essa nova inteligência permite que os fornecedores de XDR aprimorem os recursos do produto e aumentem as oportunidades de mercado. Essa inteligência de ameaças permite que os produtos corrijam os riscos de forma proativa e informem os clientes sobre as ações adotadas para proteger suas organizações. Uma melhor inteligência contra ameaças também permite que o desenvolvimento de produtos seja proativo, de acordo com as necessidades e solicitações dos clientes.

QUAIS SÃO OS BENEFÍCIOS DO XDR?

A inteligência de ameaças enriquecida, reunida em toda a superfície de ataque, pode ser contextualizada para melhorar as ações de resposta humanas e automatizadas. Por exemplo, um analista de segurança pode perder um tempo considerável analisando alertas e dados de ameaças relatados de várias fontes. Uma plataforma XDR pode correlacionar de forma inteligente os dados de ameaças de todo o ambiente e encaminhar informações de alto valor para os analistas, eliminando o ruído. Com dados XDR enriquecidos, o analista tem uma melhor compreensão do ambiente e mais tempo para tomar decisões de segurança informadas e eficazes.

Fornecedores de XDR como a BlackBerry entendem os dados e seu significado para a comunidade de segurança e para nossos clientes, independentemente da estrutura, origem ou localização. Mantemos os dados em uma estrutura com suporte para acesso fácil e processamento compartilhado, para que possam ser utilizados por todas as partes de nossa plataforma.

Os fornecedores de XDR podem garantir que oferecerão alertas de eventos com a mais alta fidelidade, contando com especialistas que entendem e verificam os dados que fluem de vários sensores. Os dados com curadoria profissional habilitam respostas automatizadas para evitar ameaças e fornecer remediação que continua a melhorar, mesmo à medida que os ataques se tornam mais sofisticados.

QUAL É A DIFERENÇA ENTRE XDR E SIEM?

A abordagem típica da equipe do centro de operações de segurança (SOC) de ter informações de segurança e gerenciamento de eventos (SIEM) em acréscimo a todos os produtos de detecção tem muitas desvantagens. As soluções SIEM são boas para coletar e armazenar registros para ajudar na conformidade e em casos de uso forense, mas não podem gerar alertas de detecção de alta fidelidade.

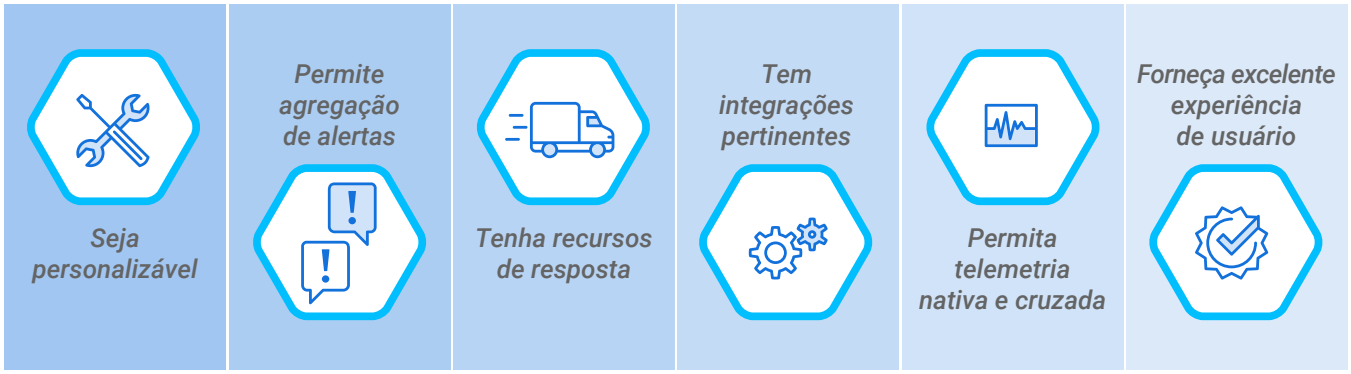
As soluções SIEM não produzem e coletam dados nativamente. Simplesmente consomem dados, sem coletar ou considerar o contexto. As equipes de SOC devem coletar e correlacionar manualmente a telemetria produzida isoladamente, o que resulta em alertas de baixa fidelidade.

Uma nova abordagem de arquitetura é necessária para resolver alguns desses problemas modernos de SOC. É aqui que o XDR entra em jogo. O sensor e o agente de segurança de um fornecedor produzem e coletam a maior parte da telemetria na superfície de ataque e centralizam em uma plataforma de nuvem. Isso fornece um repositório de dados valiosos sobre ameaças sem exigir ingestão, correlação e enriquecimento manuais de dados.

Quando ocorrem incidentes, os analistas de SOC geralmente são forçados a desperdiçar tempo de resposta crítico, costurando manualmente a telemetria para criar um resumo da linha do tempo necessário para determinar a intenção de um atacante. As soluções XDR podem habilitar a caça automatizada de ameaças com histórias de ataque pré-criadas. Essa automação reduz o tempo necessário para detectar e responder.

O QUE UMA BOA SOLUÇÃO XDR DEVE TER?

XDR é uma plataforma que unifica os recursos de vários produtos diferentes em uma experiência única, simples, robusta e personalizável. Representa a fusão de inteligência entre produtos nativos e de terceiros, habilitando os recursos de resposta necessários. Em resumo, os produtos XDR eficazes devem:



É claro que mesmo as melhores soluções XDR não podem parar as ameaças sozinhas. Algumas plataformas XDR podem incluir tecnologias de prevenção em primeiro lugar, análise assistida por IA e automação, mas os especialistas humanos ainda devem determinar o que se qualifica como uma ameaça em seu ambiente. Toda

a telemetria de ameaças que o XDR coleta de soluções primárias e de terceiros deve ser interpretada por analistas treinados. Isso pode tornar os serviços gerenciados de XDR uma opção atraente para organizações que operam com orçamentos menores de segurança cibernética.

600%

Tamanho do aumento em crimes cibernéticos devido à COVID-19.

EVOLUÇÃO DOS SERVIÇOS DE DETECÇÃO E RESPOSTA GERENCIADOS

Ameaças cibernéticas cada vez mais complexas e sofisticadas estão mudando como as organizações abordam a segurança cibernética. Alguns atacantes estão mudando seu foco de comprometimento da infraestrutura para ataques a indivíduos, com aumentos nas campanhas de phishing direcionadas. Essa mudança, entre outras, significa que as defesas tradicionais são inadequadas para abordar a diversidade de vetores de ameaças explorados pelos adversários contemporâneos. As organizações que procuram parceiros de detecção e resposta atualmente precisam de fornecedores que possam atender a uma ampla variedade de ciberataques avançados. Uma breve olhada no cenário de ameaças mostra que as organizações enfrentam uma batalha difícil:

- 667 milhões de novas detecções de malware foram descobertas no mundo em 2020.
- Houve um aumento de 600% nos crimes cibernéticos durante a pandemia de COVID-19.
- 4 milhões de trabalhadores de cibersegurança adicionais são necessários globalmente.
- 1 milhão de alertas diários de segurança são vistos em 25% dos SOCs.

As organizações estão operando em um ambiente que muda constantemente, enquanto os agentes de ameaças as tocaiam silenciosamente, procurando uma oportunidade para atacar. As organizações devem encontrar um caminho em que não se exponham a ciberataques oportunistas. Os serviços gerenciados de detecção e resposta (MDR) podem ajudar as organizações a navegar com segurança pelas águas turbulentas da tecnologia insegura e de uma força de trabalho híbrida ou móvel. As plataformas de MDR oferecem suporte profissional 365 dias por ano, 24 horas por dia, 7 dias por semana para detecção de invasões, resposta a incidentes e eliminação de ameaças.

O ataque HAFNIUM de janeiro de 2021 oferece um exemplo perfeito de como o MDR ajuda as organizações. Durante a campanha, no mínimo 30.000 organizações nos EUA foram comprometidas por uma unidade de ciberespionagem chinesa, conhecida como HAFNIUM. Esses ataques foram amplamente automáticos e visavam Microsoft Exchange Servers sem patches.

Uma equipe MDR poderia combater o HAFNIUM coletando e pesquisando extensivamente todos os feeds de inteligência de ameaças disponíveis. As informações coletadas poderiam incluir IOCs, linhas de comando, processos em execução, chaves de registro, solicitações de DNS e mais. Em seguida, a equipe MDR faria caça a ameaças adicional. Por exemplo, as equipes BlackBerry continuariam a pesquisar ameaças usando ferramentas como o InstaQuery, que é implementado via API.

Com coleta de informações e caça a ameaças, uma equipe MDR experiente pode identificar rapidamente uma ciberameaça específica. E fornecer rapidamente aos clientes as instruções para correção e práticas recomendadas, além de atualizações à medida que novas informações forem disponibilizadas. As equipes MDR proativas poderiam até configurar uma série de regras específicas para o HAFNIUM diretamente em uma ferramenta EDR, aplicando as técnicas da estrutura MITRE ATT&CK®, por exemplo.

Considerando o cenário de ameaças em evolução e sofisticado, a necessidade de os analistas terem visibilidade holística e telemetria nas ferramentas de segurança aumentou. O XDR gerenciado baseia-se na estrutura de serviços de MDR, incorporando a visibilidade do XDR em toda a empresa. As plataformas XDR unificam as detecções de endpoints relevantes para a segurança, coletando e contextualizando a telemetria de ameaças em ferramentas de terceiros. Por exemplo, uma plataforma XDR pode coletar e analisar dados de fontes de rede e SIEM, segurança de e-mail, gerenciamento de identidade e acesso, firewall de próxima geração e muito mais. O XDR Gerenciado é nativo da nuvem e construído em uma infraestrutura de Big Data para fornecer flexibilidade, escalabilidade e oportunidades de automação para as equipes de segurança. Um XDR gerenciado pode oferecer às PMEs um nível de proteção que poucas organizações podem pagar. Por exemplo, um XDR gerenciado pode fornecer:

O XDR gerenciado pode oferecer às organizações acesso 24 horas por dia a profissionais experientes de segurança cibernética usando ferramentas de detecção e resposta de ameaças de última geração. Isso pode dar às organizações uma tranquilidade considerável e permitir que se concentrem em sua missão principal em vez de se preocupar com ataques cibernéticos.

EXPANSÃO DO PAPEL DA SEGURANÇA DE REDE E IA/AM PARA PREVENIR ATAQUES DE DIA ZERO

A rede foi a portadora das vulnerabilidades mais direcionadas e altamente exploradas de 2020 e 2021. Em 2020, várias dessas vulnerabilidades afetaram o trabalho remoto, VPNs ou tecnologias baseadas em nuvem. Em 2021, os cibercriminosos maliciosos continuaram a atacar e comprometer dispositivos de perímetro. Vulnerabilidades altamente exploradas foram descobertas em muitas plataformas populares, incluindo as da Microsoft, Pulse, Accellion, VMware e Fortinet. Essa série de ataques bem-sucedidos resultou em um foco maior na segurança e proteção da conectividade de rede.

As organizações estão adotando abordagens mais novas de cibersegurança, como Zero Trust Network Access (ZTNA), Secure Access Service Edge e XDR. Em nível macro, a estrutura MITRE ATT&CK também forneceu recursos que melhoram a cobertura do ataque para vulnerabilidades específicas da rede. Ataques de dia zero estimularam os analistas de segurança a combinar defesas e tecnologias para fortalecer as medidas de segurança. Entre as abordagens usadas, estão:

- Tecnologia de prevenção em primeiro lugar
- Abordagens de proteção em primeiro lugar
- Análise baseada em assinaturas
- Detecção de ameaças e anomalias com base em AI e ML na camada de rede
- Correlação avançada entre várias fontes de telemetria

O tecido da rede também está passando por grandes mudanças. As soluções de VPN baseadas em IPSec têm sido um ponto de ignição para vários exploits recentes, destacando a necessidade de pilhas TCP/IP seguras e modernas. Da mesma forma, uma abordagem de malware puramente baseada em assinaturas exige que pelo menos um usuário seja infectado para que uma amostra maliciosa possa ser obtida. Isso impulsionou a ascensão das abordagens de IA e AM, que podem analisar ameaças na camada de rede e impedir ataques de dia zero.

O PAPEL DE AI E ML

Em detecção de ameaças de rede, IA e AM desempenham um papel importante ao modelar o comportamento normal da organização e seus usuários. Em seguida, detectam anomalias que não correspondem ao comportamento de nenhum usuário autorizado. Também podem prever se um comportamento de rede específico tem menor ou maior probabilidade de ser associado a um usuário específico. Isso fornece uma maneira eficaz de identificar beacons C2, por exemplo, e diferenciá-los do processo benigno e do uso de rede iniciado pelo usuário. Essa capacidade de detecção de anomalias e previsão com base em usuários específicos, orientada por IA e baseada em modelo, pode reduzir falsos positivos e falsos negativos.

A PESSOA INTERNA MALICIOSA

Para pessoas internas maliciosas, a detecção de acesso anômalo e a modelagem de comportamento preditivo podem ser menos eficazes, se usadas sozinhas. Em geral, a pessoa interna maliciosa mantém seu comportamento passado e pode compartilhar muitas características com o acesso normal do usuário e da organização. No entanto, comportamentos abertamente maliciosos, aberrantes ou suspeitos ainda podem chamar a atenção.

A PESSOA EXTERNA MALICIOSA

A modelagem de IA é altamente eficaz contra pessoas externas maliciosas, como as que acessam um dispositivo desbloqueado clandestinamente ou obtêm acesso ilícito a credenciais legítimas de usuários. É muito menos provável que o comportamento de uma pessoa externa mal-intencionada esteja continuamente em conformidade com o comportamento modelado de usuário comprometido. Também é provável que o comportamento da pessoa externa entre em conflito com o da organização como um todo. Pode se conectar fora do horário normal de trabalho, acessar novos recursos, ou realizar ações atípicas, como tentar fazer download de bancos de dados que os identifiquem rapidamente como ameaças.

MALWARE

Assim como acontece com pessoas externas mal-intencionadas, o acesso anômalo ou de baixa probabilidade ao endpoint por malware pode desencadear detecções. Alertar o usuário legítimo sobre a atividade maliciosa permite que interrompa o acesso e relate o problema ao SOC. Além disso, o malware e seu C2 associado apresentam padrões de rede que são anômalos em relação ao comportamento legítimo de usuários. Para proteção adicional, o comportamento de ameaças pode ser modelado separadamente para aumentar a detecção. A configuração de ações automatizadas de resposta para o comportamento de ameaça modelado protege o ambiente em casos em que o usuário legítimo não rejeita tentativas de acesso suspeitas.

DETECÇÃO DE AMEAÇAS DE REDE HABILITADA POR REGRAS

A proteção de rede holística inclui uma combinação de tecnologia de IA e AM e detecção de ameaças de rede baseada em regras. Por exemplo, o tráfego IDS/IPS pode ser usado para analisar, avaliar e filtrar comunicações. O tráfego pode ser avaliado por regras criadas previamente, como SNORT, implementadas para prevenir e detectar tráfego malicioso. Uma regra pode ser associada a uma ação de resposta correspondente, como alertar, permitir ou bloquear. Em geral, os administradores do SOC mantêm a visibilidade das ações executadas pelo SNORT ou regras semelhantes. A detecção baseada em regras por si só pode aumentar significativamente a cobertura da MITRE ATT&CK em áreas como escalonamento de privilégios, movimento lateral, comando e controle, exfiltração de dados, etc.

MICROSOFT HAFNIUM

O HAFNIUM, um agente de ameaças patrocinado por governo, utilizou vulnerabilidades de patches em Microsoft Exchange Servers locais para comprometer contas de e-mail. Em poucos dias, outros agentes maliciosos além do HAFNIUM começaram a atacar sistemas sem patches e instalar malwares para garantir acesso de longo prazo a ambientes comprometidos.

Uma combinação de segurança cibernética com prevenção em primeiro lugar e tecnologia de detecção rápida pode impedir ataques no estilo HAFNIUM. Especificamente, as vulnerabilidades exploradas pelo HAFNIUM poderiam ter sido protegidas por:

- Princípios ZTNA
- Uma abordagem de privilégio mínimo para acesso
- Uma plataforma de rede com reconhecimento de identidade
- Autenticação contínua e tecnologia de acesso adaptável
- Soluções de trabalho remoto que autenticam o acesso a aplicativos individuais, não a toda a rede

EXPLOITS DE VPN

Os exploits de VPN de dia zero inundaram o setor em 2021, com destaque para Sonic VPN, Pulse Secure e Fortinet VPN. Embora várias dessas vulnerabilidades já existissem há algum tempo, as tendências recentes de trabalho em casa e acesso remoto ampliaram sua atuação. À medida que uma tecnologia atrai mais usuários e organizações, torna-se cada vez mais valiosa para os agentes de ameaças.

Para evitar exploits de VPN com uma força de trabalho remota e móvel, as organizações devem considerar a adoção de:

- Uma arquitetura de rede Zero Trust definida por software
- Uma rede construída sobre uma pilha TCP/IP robusta
- Proteção da conectividade usando os princípios de acesso com privilégios mínimos
- Soluções que oferecem controle de acesso de rede segmentado para separar o tráfego de rede profissional e pessoal
- Controles de acesso dinâmicos que podem fornecer acesso just-in-time a uma plataforma que oferece visibilidade total do tráfego de rede em recursos locais e na nuvem

AMEAÇAS MÓVEIS E SEGURANÇA

76%

De acordo com estudos recentes, impressionantes 76% dos aplicativos móveis testados armazenam dados de forma insegura.

A segurança de dispositivos móveis deve ser uma preocupação séria para todas as organizações. Considere a situação atual do mercado de smartphones, que está dividido entre dispositivos Android™ e iPhone®. De acordo com estudos recentes, impressionantes 76% dos aplicativos móveis testados armazenam dados de forma insegura. Aplicativos inseguros ameaçam as organizações que têm políticas de "traga seu próprio dispositivo" ou que oferecem suporte para trabalhadores móveis ou remotos. O risco aumenta quando os funcionários usam cada vez mais dispositivos pessoais não gerenciados para realizar tarefas profissionais. Quando recursos de negócios e aplicativos vulneráveis ocupam o mesmo dispositivo e se conectam a várias redes, há muitas oportunidades para desastres.

Os apps vulneráveis não são a única ameaça móvel que as organizações enfrentam. Quando os dispositivos pessoais armazenam ou acessam recursos da organização, existe risco de que dados corporativos sejam expostos involuntariamente. Os vazamentos podem ser tão simples quanto encaminhar e-mails confidenciais para o endereço errado ou tão graves quanto revelar credenciais de usuários e informações de identificação pessoal. O vazamento de dados também pode ocorrer por outras vias; por exemplo, dispositivos de Internet das Coisas (IoT) emparelhados e pontos de acesso de rede não gerenciados (como Wi-Fi público).

Softwares sem patches e desatualizados também geram um risco grave para dispositivos móveis. Em março de 2021, foi identificado que o SHAREit, um aplicativo de compartilhamento de arquivos para Android, continha vulnerabilidades que permitiam a execução remota de código. Os pesquisadores de ameaças estavam cientes do problema e notificaram os desenvolvedores em dezembro de 2020, mas nenhuma atualização foi lançada. Quando os pesquisadores de ameaças revelaram publicamente as vulnerabilidades, o SHAREit tinha mais de um bilhão de downloads.

Os dispositivos móveis na América do Norte tiveram um aumento de 300% nos ataques de smishing, ou ataques de phishing via SMS, no terceiro trimestre de 2020. Esse aumento saltou para 700% nos primeiros seis meses de 2021. Os ataques de smishing chegam como uma mensagem de texto SMS, supostamente proveniente de um contato confiável, e geralmente contêm links maliciosos. Por exemplo, a vítima pode receber um texto supostamente de seu banco, informando que a conta está com saldo negativo. O texto contém um link malicioso e solicita que a vítima clique no link para obter detalhes. Se clicar no link, a vítima pode iniciar um download de malware ou ter suas informações capturadas. Esses ataques são fáceis de executar, porque o atacante só precisa ter o número de telefone da vítima. As mensagens de SMS também truncam os URLs, tornando-os mais difíceis de inspecionar visualmente em busca de sinais de alerta.

Recentemente, as práticas enganadoras de phishing e smishing evoluíram para uma ameaça ainda maior – aplicativos maliciosos se passando por programas legítimos. Essa tendência tem sido particularmente perceptível com aplicativos de bancos, criptomoedas e trading. Os aplicativos maliciosos instalados pelos usuários desfrutam dos benefícios da confiança implícita do usuário. Como o aplicativo recebe a permissão do usuário para instalação e execução, a detecção pelas abordagens tradicionais de segurança cibernética pode ser dificultada. A detecção pode ser ainda mais complicada quando aplicativos maliciosos são baixados de plataformas confiáveis.

A IA BLOQUEIA AMEAÇAS MÓVEIS

As organizações enfrentaram muitos desafios de segurança ao tentar oferecer suporte para uma força de trabalho remota e móvel quando ocorreram os lockdowns devido à COVID-19. Desde então, a força de trabalho permaneceu em fluxo e muitas organizações continuam procurando maneiras eficazes de combater ameaças móveis.

Uma abordagem promissora é adotar soluções orientadas por IA que usam modelagem matemática e análise preditiva para detectar e prevenir vários tipos de ameaças. Por exemplo:

- **Código vulnerável em aplicativos.** A IA pode extrair recursos de arquivo de um aplicativo antes que ele seja executado e bloquear aqueles que contêm código malicioso ou explorável. Isso protege os usuários contra malware, bem como aplicativos com bugs que dependem de código aberto vulnerável ou código de terceiros.
- **Vazamento de dados.** As plataformas de gateway inteligente podem oferecer recursos de túnel completo/dividido que criptografam as comunicações para dados confidenciais, mas deixam as comunicações triviais abertas. A IA desempenha um papel vital na seleção de como o tráfego de rede é classificado, eliminando o risco de erro humano causar vazamentos de dados não intencionais.
- **Softwares desatualizados.** A IA pode monitorar dispositivos para identificar versões de software desatualizadas e configurações incorretas. Essas verificações garantem que o SO, as bibliotecas do sistema e o firmware permaneçam atualizados.
- **Pontos de acesso vulneráveis.** A IA pode analisar a segurança de pontos de acesso Wi-Fi para garantir que o tráfego móvel não atravesse redes públicas ou privadas inseguras.
- **Ataques de phishing/smishing.** A IA pode determinar rapidamente a segurança de URLs, impedindo que os usuários naveguem inadvertidamente em locais inseguros.
- **Aplicativos maliciosos.** A IA pode detectar aplicativos maliciosos antes de serem carregados ou executados em um dispositivo móvel. Essa capacidade proativa de bloquear malware é uma característica da cibersegurança com prevenção em primeiro lugar.

Embora nenhuma solução seja 100% eficaz contra todos os ataques, a IA pode abordar efetivamente muitas das ameaças enfrentadas pela tecnologia móvel. A IA pode tomar continuamente decisões informadas relacionadas à segurança em segundo plano, permitindo que os usuários se concentrem na produtividade. A IA também pode monitorar conexões e tráfego de rede para garantir que as comunicações permaneçam protegidas enquanto os usuários viajam para onde quer que seus empregos exijam – ou trabalhem onde quer que sua viagem exija. Como a IA é uma tecnologia adaptável, é adequada para responder tanto a ameaças conhecidas quanto àquelas que surgem em períodos conturbados.

VEÍCULOS CONECTADOS–ÊNFASE EM SEGURANÇA

Para esses sistemas eletrônicos em que a segurança é crítica, qualquer modificação no comportamento para evitar ataques maliciosos (incluindo a inclusão de uma nova prevenção) requer uma nova certificação do sistema.

As mudanças transformacionais que estão ocorrendo no transporte pessoal ressaltam a necessidade de atender aos requisitos de segurança dessas plataformas de dados de rede móvel. A indústria automobilística está explorando usos construtivos para a IA, incluindo sua capacidade de executar tarefas críticas de segurança cibernética.

Entender como a segurança cibernética de IA com prevenção em primeiro lugar se integra à direção conectada é mais fácil desdobrando a tecnologia nos elementos individuais de prevenção e IA. Cada um pode ser implementado independentemente do outro. Da mesma forma, há trabalho que deve ser realizado em cada elemento para implementá-los adequadamente na direção conectada.

PREVENÇÃO DE ATAQUES DE CIBERSEGURANÇA

O primeiro passo para proteger qualquer sistema é projetá-lo e construí-lo de forma a minimizar a probabilidade de vulnerabilidades de segurança. Esse sentimento reflete-se em algumas diretrizes recentes estabelecidas pela ISO e pela ONU:

- ISO/SAE 21434, publicada em agosto de 2021, define a norma para tratamento da segurança durante projeto, fabricação, uso e descomissionamento de veículos.
- UN R155 determina que a cibersegurança seja considerada, não apenas nas plataformas automotivas, mas também na infraestrutura circundante.

No entanto, a prevenção e a detecção de ameaças não são diametralmente opostas. Existem vulnerabilidades que não serão encontradas durante o projeto e desenvolvimento de sistemas. Impedir que essas vulnerabilidades não identificadas sejam exploradas envolve detectar um ataque contra o sistema e impedir que progrida. As possibilidades de prevenção de comportamentos maliciosos serão afetadas pelo fato de a segurança ser crítica em sistemas eletrônicos.

Alguns sistemas eletrônicos em veículos modernos precisam ter certificação de segurança. A ISO 26262 define os níveis de integridade em segurança automotiva (ASIL, Automotive Safety Integrity Levels) de A até D. Os eventos perigosos são classificados de acordo com sua gravidade, exposição e capacidade de controlar o veículo se o evento ocorrer. Para esses sistemas eletrônicos em que a segurança é crítica, qualquer modificação no comportamento para evitar ataques maliciosos (incluindo a inclusão de uma nova prevenção) requer uma nova certificação do sistema. A recertificação envolve a realização de uma análise de riscos para cada ação de prevenção implementada. Para sistemas eletrônicos que não são críticos em termos de segurança, alterar o comportamento do sistema para prevenir atividades maliciosas contínuas é mais simples.

Em geral, a implementação de detecção de invasões precede a prevenção de invasões em novos ambientes. Habilita o monitoramento e o refinamento do sistema sem consequências adversas, até que tenhamos confiança em sua operação e possamos habilitar abordagens baseadas na prevenção.

USO DE IA

Com IA, ocorre a mesma distinção importante entre sistemas em que a segurança é crítica e outros sistemas veiculares. O uso de IA em sistemas em que a segurança é crítica ainda está sendo debatido. Um dos desafios de usar IA em um contexto de segurança é entender o comportamento do sistema resultante. A garantia de segurança depende do entendimento de como o sistema responderá às suas entradas. Um sistema de IA baseado em AM, onde o comportamento não é bem compreendido, introduz dívida intelectual. Um sistema com dívida intelectual é profundamente preocupante para os engenheiros de segurança responsáveis pela certificação. Ataques como aprendizado de máquina adversarial destacam a incapacidade do projetista para entender completamente como todas as entradas podem afetar as ações do sistema de IA. Os dados usados para treinar o sistema também podem ser alvo de ataque ou não representar as mudanças nas condições do mundo real. Portanto, é fundamental não tratar os novos sistemas de IA como infalíveis e entender por que eles falham quando falham.

Reconstruir o estado de um sistema usando IA para fazer análises após incidentes e descobrir por que falhou exigirá significativamente mais recursos em muitas áreas. Um trabalho considerável ainda precisa ser feito para reduzir a dívida intelectual relacionada à IA. O Grupo de Trabalho de Segurança de Sistemas Autônomos publicou orientações sobre garantia de segurança de sistemas autônomos. ISO TC 22/SC 32 tem vários grupos de trabalho (WG13 e WG14) que estão examinando a segurança da IA e da direção autônoma. Os problemas com o uso de IA baseada em ML em um sistema crítico em segurança incluem ameaças à própria IA e aos dados usados para treinamento ou em produção.

Portanto, esperamos que a segurança cibernética baseada em IA encontre caminhos fora dos componentes do veículo em que a segurança é crítica antes da inclusão nesses componentes. A plataforma BlackBerry IVY™ foi projetada para facilitar a introdução de IA no veículo, fornecendo insights inteligentes para aprimorar as experiências do motorista e do passageiro.

O veículo é apenas um componente na rede de veículos conectados. Outros sistemas incluem infraestrutura de recarga, interseções conectadas e até localização de rotas.

ÁREAS ADICIONAIS QUE PRECISAM DE ATENÇÃO

O veículo é apenas um componente na rede de veículos conectados. Outros sistemas na rede de veículos conectados incluem infraestrutura de recarga, interseções conectadas e até localização de rotas. Atualmente, a maior parte da localização de rotas é feita por meio de smartphones, em vez de ser integrada ao veículo. A direção autônoma em níveis mais altos exigirá que a localização de rotas seja incorporada ao veículo. Em todas essas redes de apoio, a IA pode ser usada para tomar decisões com base nos dados. Também existe a possibilidade de ataques cibernéticos nessas redes. Fatores como segurança continuarão a influenciar as decisões sobre como proteger melhor essas redes contra ameaças de segurança cibernética.

A cibersegurança de IA com prevenção em primeiro lugar não precisa ter foco exclusivamente em ambientes de produção. Prevenir a introdução de vulnerabilidades durante o design e o desenvolvimento de softwares, incluindo sistemas de IA, é outro caminho pelo qual a segurança cibernética pode ser aprimorada. O uso de IA continua sendo pesquisado para fuzzing e outras ferramentas de análise de teste de segurança de aplicativos estáticos/dinâmicos (SAST/DAST).

A ISO e a SAE estão trabalhando para determinar o nível de garantia de segurança cibernética necessário para vários componentes do veículo, com base nas ameaças cibernéticas que podem enfrentar. Maior garantia é decorrente de mais foco em projeto, desenvolvimento e testes adequados de sistemas. Isso garantirá que a probabilidade de que vulnerabilidades permaneçam não descobertas seja minimizada.

O foco ampliado em design, desenvolvimento e testes adequados de software não é exclusivo para veículos conectados. Com campanhas cibernéticas maliciosas sendo cada vez mais realizadas contra os setores público e privado, o foco na melhoria da segurança cibernética se estende a todos os softwares críticos.

GERENCIAMENTO DE EVENTOS CRÍTICOS–PREPARE-SE PARA TUDO

Para muitas organizações, a pandemia trouxe a realidade de que eventos críticos massivamente disruptivos podem ocorrer a qualquer momento. No entanto, a pandemia não foi a única interrupção nos últimos 12 meses. Interrupções na cadeia de suprimentos, distúrbios civis, interrupções de serviços públicos, desastres naturais e causados pelo homem e até mesmo condições climáticas extremas ocorreram de forma consistente ao longo do ano e em todo o mundo. Além dos eventos físicos, ciberataques e outras disrupções de TI atingiram sistemas críticos de negócios, de acordo com um relatório da Aberdeen. As interrupções na cadeia de suprimentos e em serviços públicos do passado eram muitas vezes o resultado de problemas de logística ou transmissão de energia "upstream e downstream". Atualmente, cada vez mais os ciberataques têm um papel nessas interrupções.

A Colonial Pipeline Company, proprietária do maior oleoduto dos EUA, foi vítima do ransomware DarkSide em maio de 2021, e forçada a desligar seu sistema de oleodutos por vários dias.

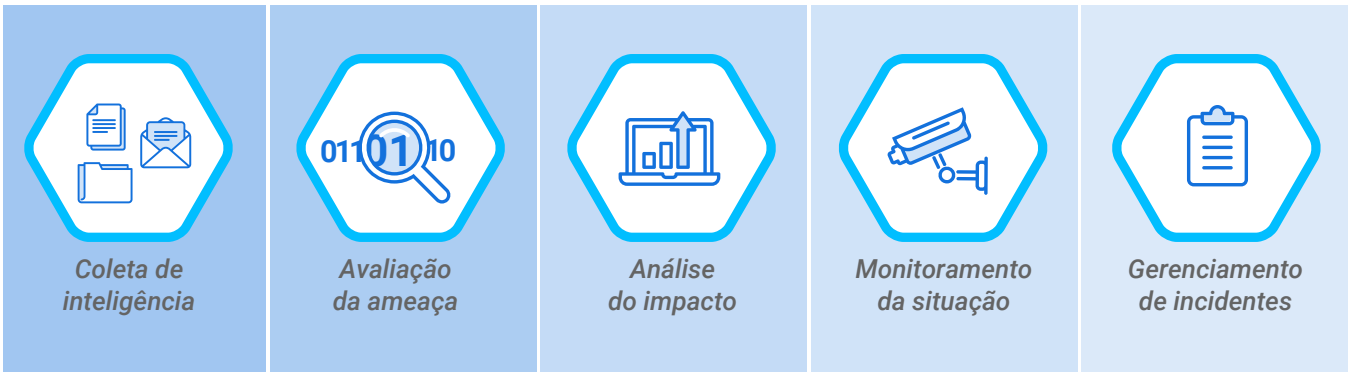
Vários incidentes de segurança cibernética de alta visibilidade foram relatados no primeiro semestre de 2021, incluindo:

- **Colonial Pipeline.** A Colonial Pipeline Company, proprietária do maior oleoduto de combustível dos EUA, foi vítima do ransomware DarkSide em maio de 2021. Os ataques interromperam as operações e forçaram a empresa a fechar seu sistema de dutos por vários dias. A Colonial Pipeline pagou US$ 5 milhões em resgate, dos quais US$ 2,3 milhões foram recuperados posteriormente.
- **Suprimento de água da Flórida.** Em fevereiro de 2021, um criminoso cibernético se infiltrou no sistema da usina de tratamento de água da cidade de Oldsmar. O atacante tentou envenenar os moradores da cidade, aumentando o teor de hidróxido de sódio no abastecimento de água para níveis perigosos. Um operador da usina identificou o aumento dos níveis de hidróxido de sódio e reverteu o ataque antes que alguém fosse ferido. As autoridades federais ainda estão procurando o atacante.

- **Channel Nine da Austrália.** A TV australiana Channel Nine teve seus programas retirados do ar por um ciberataque em março de 2021. A empresa lutou contra o problema durante várias horas, até encontrar uma solução alternativa que permitisse a transmissão novamente.
- **Ataque à cadeia de suprimentos do Accellion.** Atacantes invadiram o sistema de transferência de arquivos Accellion no início de 2021. Com essa violação, criminosos cibernéticos conseguiram roubar dados de várias organizações.

Infelizmente, muitas organizações não estão preparadas para esses tipos de eventos críticos. Os ataques às cadeias de suprimentos e infraestrutura crítica que foram destaques nas notícias em 2021 levantaram algumas questões sérias para organizações em todo o mundo. É possível prevenir esses tipos de incidentes no futuro? Como? Quais medidas as organizações poderiam ter adotado para estarem melhor preparadas para responder a eles?

Para abordar incidentes cibernéticos semelhantes, as organizações voltadas para o futuro estão investindo em recrutamento e treinamento, e equipando seus analistas de segurança para atuar em centros de operações mistos (“fusion”). Esses centros lidam com eventos críticos de segurança cibernética e TI, e também com questões não técnicas. Suas responsabilidades combinadas abrangem eventos críticos tradicionalmente gerenciados por um centro de operações de emergência, como distúrbios civis, desastres naturais e incidentes de segurança. Trabalham 24 horas por dia, executando funções importantes, incluindo:



Operar um centro de operações misto bem equipado é apenas um aspecto da resposta a eventos críticos. Existem outros desafios que devem ser considerados. As organizações ainda precisam garantir que existam processos confiáveis para alcançar as partes interessadas, sistemas de resposta interoperáveis e sistemas integrados não SOC.

O gerenciamento de eventos críticos (CEM) bem-sucedido depende de comunicação e colaboração rápidas com todas as partes interessadas afetadas. Todos os funcionários e terceirizados envolvidos precisam estar familiarizados com os procedimentos operacionais padrão da organização antes que um evento crítico ocorra. Realizar exercícios simulados de gerenciamento de crises pode aumentar a conscientização, a preparação e, em última análise, reduzir os impactos de eventos críticos.

O CEM não se limita a desastres em grande escala: inclui abordar eventos com potencial de deterioração e escalada para situações graves. Ter uma plataforma CEM segura, confiável e de ponta a ponta pode ajudar a mitigar possíveis descuidos que, posteriormente, podem custar caro. Garante que os riscos sejam entendidos e abordados, que as partes interessadas estejam adequadamente preparadas, que os feeds de monitoramento de ameaças sejam integrados com eficácia e que os recursos possam ser distribuídos rapidamente.

O CEM não se limita a desastres em grande escala: inclui abordar eventos com potencial de deterioração e escalada para situações graves.

É necessário considerar a crescente frequência e gravidade dos ataques de ransomware. Durante um ataque, os dados críticos de uma organização são criptografados e, em alguns casos, exfiltrados. Os agentes de ameaças exigem o pagamento de um resgate pela chave de criptografia para desbloquear os dados e garantir que os dados não serão mais divulgados. Se a organização não obedecer, os atacantes podem usar os dados para chantagem, deixá-los criptografados ou divulgá-los ao público. E confiar que os agentes da ameaça manterão sua parte no acordo após o pagamento de um resgate é, obviamente, uma aposta.

Usando uma plataforma CEM nesta situação, as partes interessadas pré-identificadas já estariam familiarizadas com os procedimentos de resposta esperados. À medida que o incidente se desenvolve, os analistas de segurança tentarão rastrear a fonte inicial e identificar os endpoints afetados. Um fluxo de trabalho automatizado pode enviar notificações para usuários potencialmente afetados. Essas notificações podem incluir a natureza do incidente, sinais de alerta específicos, formas de relatar problemas e quaisquer medidas para solução alternativa. Um status de progresso pode até ser incorporado para fornecer uma visão geral rápida para auxiliar o gerente de incidentes.

Externamente, reguladores, autoridades policiais, usuários de serviços identificados ou outros parceiros podem ser notificados sobre o andamento atual do incidente. Suponha que a organização afetada seja um prestador de cuidados críticos, como um hospital ou uma organização de segurança pública. Uma plataforma CEM significaria ter capacidade para garantir com eficácia que os serviços críticos possam continuar operando. Por exemplo, o terminal de dados móvel de bordo de uma ambulância pode ser integrado para garantir o envio contínuo de informações críticas, como localização e dados do paciente. Isso poderia ocorrer enquanto a organização luta simultaneamente para conter e resolver um grande evento disruptivo, como um incidente cibernético. Uma plataforma CEM oferece a capacidade para administrar melhor as interrupções operacionais e garante a entrega contínua de serviços quando as ameaças se materializam.

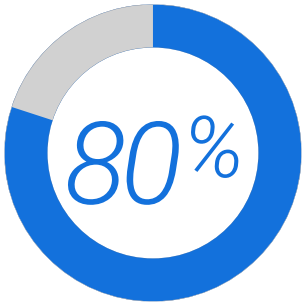
De acordo com a pesquisa com CIOs do Gartner de 2021, 64% dos funcionários podem trabalhar em casa e 40% já estão fazendo isso. Para esse grupo de partes interessadas, a capacidade para comunicar e receber informações vitais durante um incidente cibernético ou outro evento crítico é crucial. Embora os riscos não possam ser totalmente eliminados, a adoção da tecnologia CEM ajuda a ampliar as iniciativas atuais de preparação e prevenção e melhora a resiliência organizacional.

Para organizações sem uma plataforma CEM, ou que desejam ampliar suas capacidades, adquirir capacidades CEM como um serviço gerenciado pode ser uma opção atraente.

NOVAS INICIATIVAS LEGISLATIVAS E REGULATÓRIAS EM CIBERSEGURANÇA E PREVISÃO

A cibersegurança agora está como prioridade na pauta de políticas públicas para países do G7 e aliados da OTAN. Os ciberataques sucessivos e cada vez mais frequentes contra oleodutos, hospitais, empresas aéreas, cadeias de suprimentos e serviços essenciais destacam a necessidade urgente de proteger infraestruturas críticas, empresas e cidadãos. Em 2020/2021, governos de EUA, Reino Unido, França, Japão, Itália, Austrália e Alemanha prometeram coletivamente bilhões de dólares e lançaram novas medidas para fortalecer sua resiliência cibernética.

Nos EUA, o Governo Biden promulgou uma Ordem Executiva em maio de 2021 com o objetivo de reforçar as iniciativas de segurança cibernética em todo o governo federal. O presidente Biden nomeou um diretor cibernético nacional para supervisionar a política de segurança digital e lançou novas medidas para proteger e ampliar a segurança dos sistemas de informação federais. Também fortaleceu a autoridade da Agência de Segurança Cibernética e Segurança de Infraestrutura (CISA) do Departamento de Segurança Interna (DHS) para responder a grandes incidentes cibernéticos. Paralelamente, o Congresso dos EUA aprovou uma lei para codificar e financiar alguns desses esforços.



Mais de 80% dos CEOs canadenses mencionam a segurança cibernética como uma grande ameaça às perspectivas de crescimento de suas empresas.

A União Europeia está considerando uma abrangente legislação de segurança cibernética que inclua redes, infraestrutura crítica e novas certificações de segurança para produtos IoT. No Canadá, o governo federal se comprometeu a elaborar uma nova estratégia nacional de segurança cibernética, aprovar uma nova lei para levar os criminosos cibernéticos à justiça e aumentar as capacidades cibernéticas federais. No entanto, empresas e grupos setoriais estão pedindo ao governo federal que faça mais, tornando a segurança cibernética uma prioridade política. O apoio a medidas mais fortes é alto, com 92% dos canadenses dizendo que o governo deve priorizar o investimento em segurança cibernética. Mais de 80% dos CEOs canadenses mencionam a segurança cibernética como uma grande ameaça às perspectivas de crescimento de suas empresas.

De fato, a implementação das leis promulgadas em 2021, incluindo investimentos significativos em segurança cibernética, continuará em 2022 e incluirá:

- Requisitos de segurança para softwares de cadeia de suprimentos
- Programas de etiquetamento de segurança cibernética orientados para o consumidor
- Conformidade relacionada à proteção de setores de infraestrutura crítica
- Medidas para proteger redes governamentais e infraestrutura crítica contra ciberataques
- Melhorias na colaboração público-privada em iniciativas de segurança cibernética
- Aceleração dos esforços para equipar as agências governamentais com os recursos cibernéticos necessários para responder a riscos cibernéticos e ameaças cibernéticas em rápida evolução

Empreiteiros governamentais e empresas em setores regulamentados (como energia, transporte, finanças, saúde e defesa) provavelmente serão os primeiros a ter requisitos adicionais de segurança cibernética implementados. Os governos tendem a considerar que esses setores apresentam o maior risco de ameaças cibernéticas que podem resultar em amplo impacto econômico, de segurança nacional e social.

ESTADOS UNIDOS

Como 2020, 2021 foi outro ano marcante para incidentes de segurança cibernética e, portanto, iniciativas de políticas de segurança cibernética nos EUA. Conforme observado acima, o presidente Biden emitiu uma Ordem Executiva sobre "Melhoria da Segurança Cibernética da Nação" (EO 14028). A Ordem Executiva definiu e originou novas orientações sobre como melhorar a segurança da cadeia de suprimentos de software, entre outras iniciativas importantes de segurança cibernética. Lançou um processo com várias agências federais para determinar a estrutura apropriada para exigir uma Lista de Materiais de Software para aplicativos vendidos ao governo federal. A Ordem Executiva também instruiu as agências do governo federal dos EUA a fazer a transição para uma arquitetura de TI Zero Trust mais segura, entre outras medidas.

Além disso, as ações do governo dos EUA em 2021 incluíram novos requisitos de cibersegurança para proprietários e operadores de oleodutos críticos, passageiros de alto risco, operadores ferroviários de carga e de trânsito ferroviário, grandes aeroportos e operadores de aeronaves; uma Iniciativa de Cibersegurança de Sistemas de Controle Industrial pelo DHS, em coordenação com o Departamento de Comércio; estabelecimento de uma Força-Tarefa de Ransomware e Extorsão Digital pelo Departamento de Justiça; e uma série de sprints de 60 dias para resolver problemas de ransomware e segurança cibernética na força de trabalho. O presidente também convocou representantes de 30 países para uma cúpula na Casa Branca para discutir ações colaborativas para combater o ransomware.

Após as vulnerabilidades cibernéticas maciças expostas por SolarWinds, Microsoft Exchange, JBS Foods, Colonial Pipeline, Log4j e outros ataques cibernéticos de alta visibilidade e alto impacto, o Congresso continua buscando medidas para elevar o nível da segurança cibernética para proteger os setores público e privado.

Alguns dos desenvolvimentos de políticas públicas mais notáveis dos EUA que devem ser considerados pelos tomadores de decisões de segurança corporativa incluem:

- **Disposições relacionadas à segurança cibernética na Lei de Autorização de Defesa Nacional do exercício de 2022,** elaboradas com o objetivo de melhorar a capacidade do Departamento de Defesa (DOD) e do DHS para identificar, impedir, proteger, detectar e responder a campanhas cibernéticas maliciosas que ameaçam o setor público, e também infra-estrutura crítica de propriedade privada. Isso inclui exigir que o DOD desenvolva uma estratégia e arquitetura de modelo Zero Trust para sua Rede de Informações e expanda a elegibilidade para financiamento e suporte técnico do DOD para proprietários de infraestrutura crítica. O DHS, incluindo a CISA, também expandirão os esforços para abordar os riscos cibernéticos e aprimorar a resposta a incidentes cibernéticos, principalmente no que diz respeito aos sistemas de controle industrial. Será lançado um programa que fornece monitoramento e detecção contínuos de riscos de segurança cibernética para entidades de infraestrutura crítica, e estabelece um programa nacional de exercícios cibernéticos projetado para ajudar no planejamento de resposta a incidentes do governo e do setor privado.
- **Requisitos de segurança cibernética para fortalecer os setores de oleodutos, ferrovias e aviação** contra ameaças no espaço cibernético. Por exemplo, em dezembro de 2021, a Administração de Segurança de Transportes lançou novas regras exigindo que trens de alto risco, grandes aeroportos e operadores de aeronaves adotassem novos processos. Isso inclui relatar incidentes cibernéticos

à CISA, identificar um coordenador de segurança cibernética, realizar avaliações de vulnerabilidades e desenvolver planos de recuperação de contingência a serem implementados no caso de um ataque cibernético.

- **Novos requisitos de segurança da cadeia de suprimentos de software** incluídos na Ordem Executiva do Presidente estão começando a tomar forma à medida que várias agências governamentais passam a enfrentar esse problema desafiador. Essas regras afetarão inicialmente os empreiteiros federais. Embora focados em compras federais, os requisitos de segurança de software elevados provavelmente se espalharão também para as práticas e requisitos do setor privado.

US$ 1 bilhão

Montante autorizado na Lei de Empregos e Investimentos em Infraestrutura para financiar subsídios de segurança cibernética para governos estaduais e locais.

As iniciativas governamentais que provavelmente ganharão força em 2022 incluem o desenvolvimento de requisitos adicionais de segurança cibernética para os setores de transporte, energia, telecomunicações e financeiro. Caso novas regras ou leis sejam criadas, proprietários e operadores desses setores serão obrigados a dedicar mais recursos para cumprir os novos requisitos de segurança cibernética. Alguns congressistas pressionarão por mais consultas federais com as partes interessadas do setor para desenvolvimento desses requisitos. O setor privado também deve esperar propostas bipartidárias para promulgação de mandatos de notificações de incidentes de segurança cibernética e relatórios para operadores e proprietários de infraestrutura crítica, e possivelmente outras atividades. Várias dessas propostas foram debatidas em 2021 e provavelmente serão revistas em 2022.

Por fim, espera-se que o governo em todos os níveis continue a se mover rapidamente para investir na modernização de TI, incluindo a segurança cibernética. Esses fundos estão fluindo por meio da Lei do Plano de Resgate Americano, sancionada em março de 2021, que ampliou o Fundo de Modernização de Tecnologia, e a Lei de Investimentos e Empregos em Infraestrutura, sancionada em novembro de 2021. Várias disposições desta nova lei tornam o financiamento de infraestrutura dependente de investimento e planejamento para segurança cibernética pela primeira vez. Os governos locais e estaduais também vão se beneficiar de US$ 1 bilhão autorizado na Lei de Empregos e Investimentos em Infraestrutura para financiar subsídios de segurança cibernética para governos estaduais e locais.

CANADÁ

Assim como nos EUA, a segurança cibernética é um dos desafios mais prementes que o Canadá enfrenta. Durante décadas, especialistas alertaram sobre os perigos dos ataques cibernéticos. Atualmente, as violações cibernéticas tornaram-se desconcertantemente rotineiras. Com razão, os canadenses estão preocupados. Ser vítima de um ataque cibernético agora ocupa o segundo lugar, atrás de perder o emprego, na lista de coisas com as quais os canadenses mais se preocupam. No ano passado, no Canadá, empresas, hospitais, universidades, sistemas de transportes, cidades e serviços do governo passaram por ciberataques significativos.

Abordar as deficiências de segurança cibernética é uma alta prioridade para os canadenses, como parte integrante da construção de uma economia mais resiliente, inovadora, inclusiva e vibrante. Grupos setoriais estão levantando preocupações sobre o conjunto cada vez maior de ameaças cibernéticas. Estão reivindicando que o governo

invista em cibersegurança em nível equivalente ao do G7 e elaboraram recomendações detalhadas sobre como os setores público e privado podem colaborar para melhorar a segurança cibernética no Canadá.

O governo Trudeau assumiu o compromisso de elaborar uma nova Estratégia Nacional de Segurança Cibernética e desenvolver um Plano Nacional de Ação de Segurança Cibernética. Pretende promulgar leis para combater o crime cibernético e aprimorar as salvaguardas de privacidade, além de equipar o Canadian Security Establishment com as ferramentas necessárias para responder a um cenário de ameaças cibernéticas em rápida evolução. No entanto, muitos no setor, incluindo a Câmara de Comércio do Canadá, estão pressionando o Governo do Canadá a fazer mais para proteger a infraestrutura crítica, empresas e comunidades. Entre essas recomendações estão os apelos ao governo para:

- **Aumentar a resiliência cibernética da infraestrutura crítica.** Conforme observado no Relatório de Ameaças de 2021 da BlackBerry, a Estratégia de Infraestrutura Crítica do Canadá é antiga, remontando a 2009. A Public Safety Canada iniciou consultas para renovar e atualizar essa estratégia, mas isso pode levar vários anos para ser finalizado. Enquanto isso, a Infrastructure Canada está realizando uma Avaliação Nacional de Infraestrutura, que define as prioridades do governo para investimentos em infraestrutura nos próximos anos. Os ataques cibernéticos ao sistema de saúde de Terra Nova e Labrador e à autoridade de trânsito de Toronto em 2021 serviram como um "alarme" para o Canadá aumentar o investimento em segurança cibernética para infraestrutura crítica. A Transport Canada fez progressos na segurança cibernética de veículos, publicando orientações concretas e caracterizando a segurança cibernética como um elemento fundamental da segurança e proteção rodoviária. No entanto, mais orientações e regulamentações relacionadas à segurança cibernética são esperadas para os setores ferroviário, marítimo e de aviação, considerando a falta de atenção até o momento.
- **Ajudar as empresas canadenses a investir em segurança cibernética.** Em abril de 2021, o governo federal prometeu US$ 4 bilhões ao Programa de Adoção Digital do Canadá. Esses fundos destinam-se a ajudar 160.000 pequenas e médias empresas a comprar e adotar as novas tecnologias de que precisam para crescer. Foi uma iniciativa bem-vinda para muitos, porque a pandemia de COVID-19 pressionou as empresas para uma dependência sem precedentes da tecnologia digital para apoiar o trabalho remoto e o comércio eletrônico. No entanto, essas mesmas empresas experimentaram um aumento sem precedentes nos ataques cibernéticos. Para aproveitar plenamente o potencial do Programa de Adoção Digital, a segurança cibernética deve ser um elemento essencial desse programa. Ao alavancar a profunda experiência e o talento do setor privado, o Canadá pode elevar o nível de segurança cibernética e equipar pequenas e médias empresas com as melhores práticas e ferramentas necessárias para prosperar em uma economia orientada por dados. Isso também ajudará as empresas canadenses a cumprir uma nova lei federal de privacidade e proteção de dados, que provavelmente será proposta em 2022.
- **Melhorar a coerência e a ação de todo o governo em segurança cibernética.** Atualmente, as responsabilidades cibernéticas no Governo Federal estão distribuídas em pelo menos 12 departamentos e agências federais. Criar coerência em todo o governo para garantir que todos os departamentos operem com unificação

de esforço e propósito é essencial para promover a resiliência cibernética. A BlackBerry, juntamente com outras empresas líderes em tecnologia, instou o Canadá a considerar o estabelecimento de um cargo sênior no governo, como o novo Diretor Cibernético Nacional dos EUA. Esse cargo ajudaria a elevar a segurança cibernética nas políticas governamentais e promover a resiliência cibernética, aprimorando a coerência e a colaboração em todo o governo. Em 2022, esperamos maior atenção ao desenvolvimento de estratégias e mecanismos que facilitem a implementação de uma estratégia coesa de segurança cibernética em todo o governo. Isso ajudará o governo a passar de uma mentalidade reativa de resposta a incidentes para uma abordagem de prevenção em primeiro lugar que posicionará o Canadá como líder em segurança cibernética.

UNIÃO EUROPEIA

Em 2021, a UE manteve a abordagem proativa para abordar as vulnerabilidades da cibersegurança. A Estratégia de Cibersegurança da UE, publicada no final de 2020, introduziu novas medidas para aprimorar as capacidades cibernéticas coletivas. As medidas incluíram a criação de um novo centro de operações de segurança chamado Unidade Cibernética Conjunta, onde as autoridades públicas da UE podem trabalhar em rede e colaborar para responder a ciberataques. Além de novas iniciativas e requisitos de segurança cibernética para o governo, o setor será impactado por revisões da Diretiva de Segurança de Rede e Informação (NIS) da UE e da legislação que regulamenta os requisitos de relatórios de incidentes cibernéticos para operadores críticos.

Em 2022, será mantido o foco em:

- Uma proposta da Comissão para abordar as deficiências da diretiva de Segurança de Redes e da Informação (NIS). As mudanças de destaque incluem uma expansão no escopo das entidades cobertas pela diretiva. Agora, incluirão provedores de serviços baseados em nuvem, telecomunicações e comunicações eletrônicas, sistemas de transporte inteligentes e veículos autônomos, bem como tecnologia espacial. A diretiva também incluirá padrões mais restritivos de segurança cibernética e gestão de riscos. As alterações afetam a criptografia e a segurança da cadeia de suprimentos, além de exigir relatórios obrigatórios de incidentes cibernéticos dentro de prazos rígidos. Também estão previstas novas medidas de certificação de produtos de segurança cibernética para o setor privado. O descumprimento pode resultar em multas equivalentes à GDPR.
- Um quadro de certificação de cibersegurança em toda a UE, que especificará os níveis de garantia de segurança para produtos e serviços baseados em TIC para aplicações industriais e de consumo. As áreas de foco atuais incluem segurança na nuvem, segurança 5G, IoT e inteligência artificial.
- A UE também deve anunciar uma nova *Lei de Resiliência Cibernética* para estabelecer novos requisitos de dever de cuidado para software e dados em dispositivos de TIC para fabricantes. Esta proposta inclui softwares e dispositivos IoT. O objetivo é garantir a segurança em todo o ciclo de vida dos produtos de TIC, desde o desenvolvimento até o fim da vida útil.

PREVISÕES: AVALIAÇÃO PARA 2022 E O FUTURO

Embora seja impossível prever o futuro, solicitamos aos nossos experientes especialistas da BlackBerry que compartilhassem suas opiniões sobre problemas que em breve podem afetar a segurança cibernética. Estes são alguns dos temas que nossos profissionais estarão monitorando em 2022.

COMPUTAÇÃO QUÂNTICA

O avanço contínuo da computação quântica pode ser tão disruptivo para o espaço de segurança cibernética quanto a IA é hoje, principalmente quando os futuros computadores quânticos puderem quebrar esquemas de criptografia modernos em minutos ou segundos. Prever o impacto geral da computação quântica na segurança cibernética é difícil, mas pode-se começar imaginando que a criptografia não é mais um fator. Isso pode ser catastrófico, pois organizações públicas e privadas perderiam uma ferramenta valiosa para proteger dados roubados contra atacantes.

No entanto, há outra maneira de olhar para este problema. Dados e comunicações geralmente são criptografados devido à crença geral de que atacantes motivados chegarão a eles. Isso ignora a possibilidade de que outros aspectos da segurança cibernética possam melhorar a ponto de os dados permanecerem totalmente protegidos. Por exemplo, considere tecnologias que promovam uma forte abordagem de prevenção para a segurança, que identifique e encerre os ataques antes que sejam executados. Se os atacantes nunca conseguirem acessar os dados, não importa se estão criptografados ou não. Dessa forma, o avanço de outras tecnologias poderia compensar a perda iminente de criptografia devido à computação quântica.

É razoável pressupor que as tecnologias de rastreamento de COVID, que foram rapidamente desenvolvidas e implementadas, sejam alvos tentadores para os agentes de ameaças.

ATAQUES COM TEMAS DA COVID-19

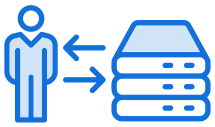
Não é difícil prever a continuação dos ataques com temas da COVID-19 persistindo durante a pandemia. Quando ocorre um evento disruptivo, sempre haverá algum elemento oportunista tentando lucrar ou ganhar com o caos resultante. O mais difícil é prever como serão os ataques inspirados na COVID-19 em 2022. Uma possibilidade é considerar as novas tecnologias relacionadas à COVID-19 que surgirão e antecipar ataques cibernéticos nessas frentes.

Por exemplo, é razoável supor que tecnologias de rastreamento de COVID continuarão a ser desenvolvidas durante a pandemia. Essas novas tecnologias terão sido desenvolvidas e implementadas rapidamente, tornando-as alvos tentadores para os agentes de ameaças. Da mesma forma, se os passaportes de imunização ou políticas semelhantes se estabelecerem nas regiões, a infraestrutura tecnológica por trás deles pode chamar a atenção dos agentes de ameaças.

GOVERNOS SOB PRESSÃO PARA SE ADAPTAREM

Os governos estão enfrentando uma pressão crescente para mudar sua abordagem no combate aos ataques cibernéticos. Os atacantes estão adotando rapidamente novos TTPs para ofuscar suas operações e explorar seus alvos. Estados-nação hostis, antes satisfeitos em conduzir sua própria guerra cibernética, agora frequentemente terceirizam seus ataques para serviços ou grupos de terceiros. Isso torna cada vez mais difícil atribuir um ataque específico a um agente de ameaça específico. Da mesma forma, alguns grupos de ameaças estudam os TTPs de outros adversários e, em seguida, imitam seus comportamentos e usam suas ferramentas para promover a identificação incorreta.

Os governos que dependem de tecnologias e abordagens legadas para segurança cibernética estão se encontrando continuamente na defesa. Diante de uma situação em que seus agressores são desconhecidos e sua tecnologia é reativa, torna-se cada vez mais provável que os governos adotem medidas mais agressivas. Não está claro quais devem ser essas medidas, mas poderiam incluir ferramentas de segurança de prevenção em primeiro lugar, estruturas Zero Trust e monitoramento mais intrusivo.



Mudanças futuras no SOC provavelmente se resumirão a dois componentes separados, mas interligados: pessoas e tecnologia.

MUDANÇAS NO SOC

Mudanças futuras no SOC provavelmente se resumirão a dois componentes separados, mas interligados: pessoas e tecnologia. Impulsionando as mudanças relacionadas às pessoas, os ataques cibernéticos tornaram-se cada vez mais sofisticados, o que significa que os analistas empregados para detectá-los também devem evoluir. A época em que o pessoal de segurança poderia ser considerado qualificado simplesmente por entender como interpretar um SHA-256 é passado. Os analistas de SOC de hoje e de amanhã precisam de uma compreensão mais profunda das técnicas adversariais. Não devem apenas ser capazes de detectar um ataque, mas também entender de onde ele veio e para onde está indo.

Essa necessidade de maior conhecimento impulsionará a mudança na tecnologia de SOC. Por exemplo, SOCs modernos se concentram menos em produtos singulares e mais em recursos. É por isso que o XDR e o XDR gerenciado estão chamando mais atenção. A capacidade de uma plataforma para integrar a telemetria de ameaças de várias fontes, incluindo soluções de terceiros, e entregá-la aos analistas é crucial. São necessários analistas que entendam ataques sofisticados e soluções que identifiquem e forneçam informações relevantes, independentemente de onde os dados de ameaças residam. Prevemos que o SOC continuará a favorecer analistas altamente treinados e plataformas de segurança que priorizam os recursos e não a força do produto individual em 2022.

SEGURANÇA NO METAVERSO

Muito poderia ser dito sobre a sabedoria de criar uma realidade híbrida onde as interações e o status das pessoas existem em grande parte em uma capacidade virtual. Do ponto de vista da segurança, é importante lembrar de uma verdade simples: as pessoas abrem mão da segurança em troca de conveniência. Um excelente exemplo disso pode ser visto no recurso de GPS dos smartphones. Qualquer pessoa pode negar a um atacante (ou empresa) informações sobre sua localização geográfica simplesmente desligando os serviços de localização GPS do telefone. No entanto, quem tentar isso descobre

rapidamente que muitos de seus aplicativos simplesmente param de funcionar. Isso significa que, por conveniência, as pessoas deixam o GPS ativado em seus telefones, mesmo que os aplicativos móveis sejam notoriamente inseguros.

Para que a segurança tenha sucesso no Metaverso, precisará ser implementada de forma robusta sem afetar negativamente a conveniência do usuário.

Agora, considere o quanto o risco aumenta quando não é apenas uma localização de celular, mas toda a vida de uma pessoa sendo monitorada. Se a informação pode ser usada de forma inadequada para lucro ou ganho, sempre haverá um elemento da sociedade esperando para roubá-la ou explorá-la. O Metaverso requer consideravelmente mais interação do usuário do que um telefone celular. Portanto, é razoável pressupor que coletaria muito mais informações e atrairia muito mais atacantes também. Para que a segurança tenha sucesso no Metaverso, precisará ser implementada de forma robusta sem afetar negativamente a conveniência do usuário.

O FUTURO DAS CIBERAMEAÇAS

Os atacantes continuarão a explorar eventos que fazem com que as organizações fiquem mais vulneráveis do que em geral. Isso se aplica tanto a crises globais imprevistas, como a pandemia de COVID-19, quanto a ocorrências mais previsíveis, como desastres naturais ou feriados programados. Quando as operações de segurança de uma organização são interrompidas, é mais provável que isso atraia a atenção dos agentes de ameaças que percebem uma oportunidade.

Os agentes de ameaças também continuarão imitando as estratégias e tendências bem-sucedidas que observam no mundo dos negócios. Por exemplo, estamos vendo mais malwares desenvolvidos para execução em arquitetura de nuvem. Ofertas como RaaS e IaaS malicioso estão se ampliando. Os IABs surgiram para ajudar criminosos comuns a executar campanhas com mais êxito, e para ajudar estados-nação e outras organizações poderosas que buscam realizar ataques cibernéticos clandestinamente e manter uma negação plausível. As organizações de ameaças estão se tornando cada vez mais resilientes, como podemos ver no Emotet, que retornou após uma derrubada completa do governo internacional em janeiro de 2021. Com base nesses fatores, prevemos que tecnologias e tendências cada vez mais favorecidas pelas organizações provavelmente continuarão sendo os principais alvos dos agentes de ameaças em 2022.

CONCLUSÃO

CONCLUSÃO

Ataques organizados a infraestruturas críticas e grandes organizações foram destaque nas notícias em 2021, com o ransomware desempenhando um papel fundamental. Os agentes de ameaças demonstraram sua capacidade para adotar e imitar os recursos do setor privado, alavancando serviços maliciosos (RaaS, IaaS, MaaS, etc.) e usando IABs. À medida que os atacantes continuam adotando rapidamente novas tecnologias e explorando as mudanças nas circunstâncias, torna-se cada vez mais importante que os analistas de ameaças acompanhem o ritmo. Isso pode exigir investimentos em plataformas XDR ou serviços XDR gerenciados que possam coletar telemetria de ameaças em produtos e dispositivos enquanto separam informações úteis de ruídos.

Os ataques à cadeia de suprimentos foram outro fator importante que moldou o cenário de ameaças em 2021. Os agentes de ameaças voltaram sua atenção para os provedores de serviços, comprometendo-os para lançar ataques downstream contra seus clientes. Dois ataques à cadeia de suprimentos, SolarWinds e Kaseya, trouxeram o problema à atenção do público, mas dezenas de outros ocorreram ao longo do ano passado. Quase dois terços desses ataques basearam-se na exploração da confiança do cliente em seu provedor de serviços – mais uma razão pela qual as organizações devem considerar a adoção de uma estrutura Zero Trust.

Uma vulnerabilidade em particular, a falha do Microsoft Exchange Server, causou estragos em todo o mundo. Foi explorada pela primeira vez pelo HAFNIUM. Vários outros grupos rapidamente se concentraram na falha e lançaram ataques usando as mesmas táticas contra várias organizações. Embora esses ataques se apoiassem em exploits de dia zero, poderiam ter sido evitados com algumas tecnologias existentes. Uma plataforma de rede com reconhecimento de identidade, autenticação contínua, acesso adaptável e soluções de trabalho remoto que autenticam por aplicativo reduzem bastante os riscos desse tipo de vulnerabilidade.

Os governos permanecem ativamente engajados no espaço de segurança digital, com países do G7 e aliados da OTAN colocando a cibersegurança como prioridade na agenda de políticas públicas. Uma Ordem Executiva para Melhorar a Cibersegurança da Nação foi emitida nos EUA, criando novos requisitos para relatórios de incidentes e segurança da cadeia de suprimentos de software. O Departamento de Justiça estabeleceu uma Força-Tarefa de Ransomware e Extorsão Digital. A União Europeia continua o trabalho estabelecido na Estratégia de Cibersegurança da UE de 2020. As medidas incluem a criação de um centro de operações de segurança da Unidade Cibernética Conjunta e a padronização de uma estrutura comum de certificação de segurança cibernética. A Transport Canada declarou que a cibersegurança é um elemento fundacional da segurança nas estradas. Os fabricantes automotivos receberam diretrizes de segurança cibernética da ISO, da SAE e da ONU sobre projeto, fabricação e uso de veículos conectados.

Os eventos de 2021 são um lembrete de que não há imunidade a ataques cibernéticos e ninguém está seguro. As PMEs em particular sofreram inúmeros ataques financeiramente dolorosos que nunca chegaram aos meios de comunicação. Ataques que afetam organizações de todos os portes foram infligidos diretamente e por meio de suas cadeias de suprimentos. Os dispositivos móveis, usados por uma população crescente de cidadãos do mundo, apresentam aplicativos que são extremamente inseguros. O aplicativo SHAREit vulnerável para dispositivos Android, que permite a execução remota de código, foi baixado mais de um bilhão de vezes antes que suas falhas fossem reveladas. Todos os participantes do espaço digital, desde empresas multinacionais até qualquer pessoa que possua um smartphone, permanecem expostos a riscos cibernéticos.

A BlackBerry dedica-se a fornecer soluções avançadas de cibersegurança para pessoas e organizações no mundo inteiro. Continuamos treinando e implementando modelos de IA cada vez mais eficazes e avançados, que preveem ameaças e usam a tecnologia de prevenção em primeiro lugar para impedir sua execução. Nossos modelos de segurança Cylance IA, implementados primeiro em endpoints, foram adaptados para detectar ameaças na rede, no comportamento de usuários e além.

PARA SABER MAIS SOBRE COMO A BLACKBERRY PODE PROTEGER A SUA ORGANIZAÇÃO, ACESSE BLACKBERRY.COM.

AGRADECIMENTOS:

O Relatório de Ameaças BlackBerry 2022 representa os esforços colaborativos de nossas equipes e pessoas talentosas. Em particular, gostaríamos de reconhecer:

Adam Lancaster
Baldeep Dogra
Brent Nicorvo
Brian Robison
Dan Ballmer
David Relyea
Dean Given
Eoin Wickens
Eric Milam
Ethan Fleisher
Gary Ng
Gina Regan
Ginger Espanola
Glenn Wurster
Goran Gotev
Grace Hu
Heather Spring
Ieva Rutkovska
Jim Simpson
John McClurg
John de Boer
Kristofer Vandercook
Lysa Myers
Marc Cormier
Marisa Goodrich
Marjorie Dickman
Mark Mariani
Mark Stevens
Marta Janus
Michelle Haynes
Natasha Rohner
Nigel Thompson
Patrick Slattery
Rajesh Rajamani
Robert Nusink
Sabrina Forgione
Samuel Spector
Sriram Krishnan
Steve Kovsky
Thom Ables
Tony Lee
Tom Bonner
Tracey Swanson
William L. Savastano
Willy Vega
Yi Zheng

As informações contidas no Relatório de Ameaças BlackBerry 2022 são apenas para fins educacionais. A BlackBerry não garante nem se responsabiliza pela precisão, integridade e confiabilidade de quaisquer declarações ou pesquisas de terceiros aqui mencionadas. A análise expressa neste relatório reflete o entendimento atual das informações disponibilizadas por nossos analistas de pesquisa e pode estar sujeita a alterações à medida que informações adicionais nos são divulgadas. Os leitores são responsáveis pela diligência devida ao aplicar essas informações em suas vidas privadas e profissionais. A BlackBerry não aprova qualquer uso malicioso ou abuso de informações apresentadas neste relatório.

BlackBerry Intelligent Security. Everywhere.

A BlackBerry (NYSE: BB; TSX: BB) fornece softwares e serviços de segurança inteligentes para empresas e governos no mundo inteiro. A empresa protege mais de 500 milhões de endpoints, incluindo 175 milhões de carros em circulação atualmente. Sediada em Waterloo, Ontário, Canadá, a empresa alavanca IA e aprendizado de máquina para entregar soluções inovadoras nas áreas de segurança digital, proteção e privacidade de dados, e é líder em gerenciamento de segurança de endpoints, criptografia e sistemas incorporados. A visão da BlackBerry é clara — proteger um futuro conectado em que você pode confiar.

Para obter mais informações, acesse BlackBerry.com e siga @BlackBerry.