2023 de agosto

Relatório de cenário de ameaças global

Um relatório semestral da FortiGuard Labs

FORTINET

Índice

Resumo executivo. 3

Visão geral do 1º semestre de 2023 3

Olhando para trás: tendências de ameaças em cinco anos 5

Entrando na área de risco 6

Da previsão da exploração ao surto 8

Mapa de calor global ATT&CK 9

Insights técnicos da telemetria de endpoint 11

Protegendo sua empresa contra ameaças em evolução 12

Conclusão e perspectiva final 14

Resumo executivo

O cenário de ameaças e as superfícies de ataque das organizações estão em constante transformação. E a capacidade dos cibercriminosos de projetar e adaptar rapidamente suas técnicas para explorar esse ambiente em evolução continua a representar riscos significativos para empresas de todos os portes, independentemente do setor ou da localização geográfica.

À medida que examinamos a atividade no primeiro semestre de 2023, vemos organizações de crimes cibernéticos e grupos de ciberofensivos de estados-nação adotando rapidamente novas tecnologias. Notavelmente, alguns desses atores operam como empresas tradicionais, com responsabilidades, entregas e objetivos bem definidos. Essa estrutura organizacional, combinada com bolsos profundos resultantes de explorações passadas ou patrocinadores de estados-nação, facilita sua postura ofensiva, permitindo que eles experimentem e incorporem tecnologias revolucionárias, como a nova IA generativa, que tornam seus ataques mais complexos e difíceis de detectar.

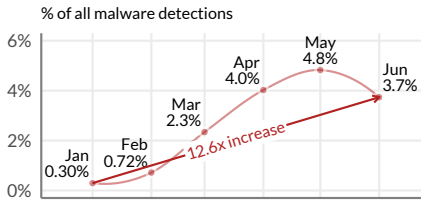
Um aumento significativo na sofisticação de atores maliciosos está especialmente evidente no domínio da cibersegurança, onde as ameaças aumentaram em frequência e complexidade. Isso é caracterizado por um aumento nos ataques altamente direcionados em vários setores, incluindo campanhas complexas de ransomware, violações de dados substanciais e uma mudança notável nas táticas MITRE ATT&CK, conforme observado por meio de nossos recursos globais de detecção aprimorados por IA.

Visão geral do 1º semestre de 2023

Grupos de APT

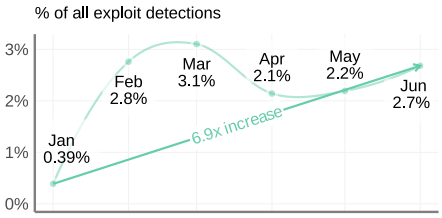
A atividade foi detectada para 41 de 138 (30%) grupos de APT identificados pelo MITRE. Esses ataques são mais focados e planejados e também ocorrem em "ondas" rápidas, portanto, é preocupante ver um terço de todos os grupos de APT categorizados ativos.

Ransomware



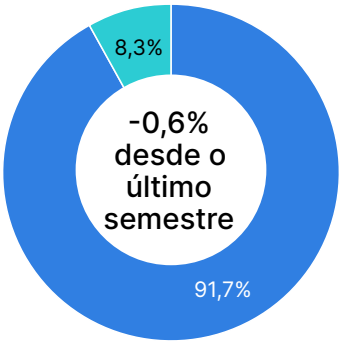
A montanha-russa do ransomware continuou, terminando o 1º semestre de 2023 13x maior do que começou. Menos organizações estão detectando ransomware com sucesso do que no passado (13% versus 22%), reforçando que o ransomware também está se tornando mais sofisticado e direcionado.

Ataques de ICS e OT



Os ataques direcionados a sistemas de controle industrial (Industrial Control Systems, ICS) e tecnologias operacionais (OT) não ocorreram em alto volume, mas aumentaram no primeiro semestre de 2023. Metade das organizações sofreu explorações de ICS ou OT, sendo que energia e serviços públicos estiveram entre os principais alvos.

Entrando na área de risco



A porcentagem de todas as vulnerabilidades de endpoint visadas pelos invasores permaneceu relativamente estável (cerca de 8%) no primeiro semestre de 2023 em comparação com o período anterior.

Tempo para exploração

327x

Nossa análise mostra que as principais vulnerabilidades mais exploráveis, identificadas pelo EPSS, têm 327 vezes mais chances de serem atacadas em uma semana do que outras no seu radar.

Visitas do ATT&CK

Usando nossas tecnologias de detecção, observamos a atividade de dois terços de todas as técnicas conhecidas de MITRE ATT&CK ao longo do primeiro semestre de 2023.

No primeiro semestre de 2023, observamos uma atividade significativa entre os grupos de Ameaça Persistente Avançada (Advanced Persistent Threat, APT), um aumento na frequência e na complexidade do ransomware, uma maior atividade de botnet, uma mudança nas técnicas MITRE ATT&CK usadas pelos invasores, e muito mais.

No entanto, apesar das mudanças no cenário de ameaças, nem tudo são más notícias para os defensores. Neste relatório, também analisaremos de perto as vulnerabilidades e ofereceremos conselhos sobre como priorizar seus esforços de correção. E como grande parte da atividade do cenário de ameaças que estamos vendo é familiar, há muitas oportunidades para implementar estratégias para se defender efetivamente dos agentes mal-intencionados. Por fim, abordaremos várias etapas práticas que você pode adotar hoje, como aproveitar a threat intelligence para proteger melhor sua organização.

Um terço de todos os grupos de APT categorizados estavam ativos no 1º semestre de 2023

Vale a pena reservar um momento para destacar os agentes mal-intencionados por trás dessas tendências que estamos analisando. Como parte de seus esforços para apoiar a estrutura ATT&CK, a MITRE rastreia 138 grupos de ameaças cibernéticas.[1] O monitoramento da atividade coletiva desses grupos é um componente essencial do mapeamento e da análise do cenário de ameaças. De janeiro a junho de 2023, observamos atividade atribuída a 41 desses grupos (30%). Dentre eles, Turla, StrongPity, Winnti, OceanLotus e WildNeutron foram os mais ativos com base na análise de código genético de malware.

O Turla é possivelmente um dos grupos de ameaças mais eficientes que existem. Há quase duas décadas, ele vem operando sob vários pseudônimos (Snake, Venomous Bear e Blur Python, para citar alguns). Ele foi associado a mais de 45 ataques notáveis, afetando agências governamentais, meios de comunicação, organizações do setor energético e embaixadas em todo o mundo. Durante anos, o grupo conseguiu violar organizações e passar despercebido, mesmo em ambientes altamente monitorados, e dado o agravamento do conflito russo-ucraniano, não ficamos surpresos ao ver o aumento da atividade desse grupo em particular.

No entanto, também há boas notícias: nos últimos seis meses, a atividade do grupo de APT impactou apenas um pequeno subconjunto de todas as organizações, indicando que a atividade de APT ainda está bastante na mira, pelo menos por enquanto. Isso faz sentido já que o grupo não irá desperdiçar suas armas cibernéticas em ataques de pulverização.

A montanha-russa do ransomware continua

Embora o ransomware exista há décadas, nos últimos anos, vimos agentes mal-intencionados usando cepas mais sofisticadas e complexas para se infiltrar em redes, em grande parte graças ao aumento das operações de ransomware como serviço (Ransomware-as-a-Service, RaaS).[2] E como a atividade de ransomware continua desenfreada, os líderes empresariais em todo o mundo estão cada vez mais preocupados com essa ameaça. Em uma pesquisa recente realizada pela Fortinet, dos 78% dos líderes que afirmaram que suas empresas estavam preparadas para um ataque, metade ainda foi vítima deles.[3]

O ransomware não mostra sinais de desaceleração, sendo que as atividades de ransomware terminaram 13 vezes mais altas do que no início de 2023 como proporção de todas as detecções de malware. Mas também estamos em um ponto mais baixo na montanha-russa para o número de organizações impactadas. Quase um quarto (22%) das empresas detectou atividade de ransomware em suas respectivas redes há cinco anos. Isso agora caiu para 13% ao examinarmos o primeiro semestre de 2023. Infelizmente, essa aparente diminuição na atividade não indica que a atividade de ransomware está diminuindo. Em vez disso, é um sinal de que a distribuição de ransomware se tornou mais concentrada à medida que as gangues de ransomware avançam em seus modelos de negócios, realizando ataques mais direcionados usando cartilhas rapidamente adaptáveis e sofisticadas.

A imagem a seguir mostra informações sobre as famílias de malware mais prevalentes observadas por meio de nossa telemetria no primeiro semestre de 2023. Ela compartilha as principais famílias de cada categoria em criptomineradores, infostealers, ransomware e Trojans de Aacesso Remoto (Remote Access Trojans, RATs).

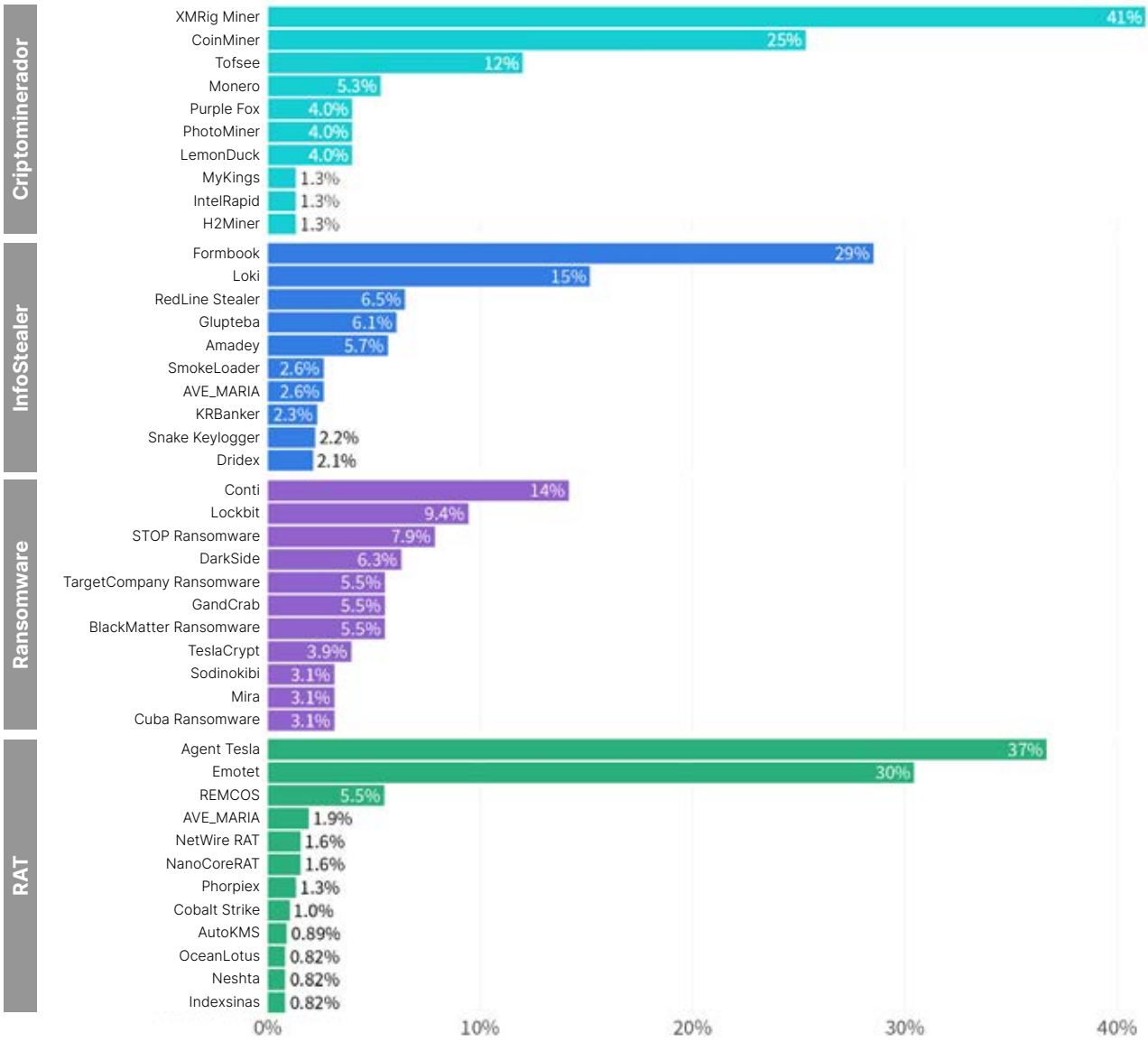


Figura 1: Principais famílias de malware por tipo

Os wipers estão diminuindo... por enquanto

Uma categoria de ransomware não listada acima é o malware wiper.[4] Os wipers ("limpadores") têm esse nome porque essa técnica de ataque destrutivo "limpa" os dados dos sistemas infectados. Observamos um aumento no uso de wipers no início de 2022, principalmente em conjunto com o conflito russo-ucraniano.[5] E, embora esse aumento tenha persistido pelo resto do ano, ele desacelerou no primeiro semestre de 2023.

Embora muitas vezes tenhamos observado que os wipers são usados principalmente por agentes do estado-nação em tempos de guerra, também vimos cibercriminosos usarem esse tipo de malware para atingir organizações em setores específicos, incluindo tecnologia, manufatura, governo, telecomunicações e saúde.

Olhando para trás: tendências de ameaças em cinco anos

Como profissionais de segurança, muitos de nós tendem a assumir que tudo sempre piora quando se trata de cibersegurança.

Mas essa suposição é fato ou ficção? É importante dar um passo atrás ocasionalmente para examinar as tendências de longo prazo, o que pode nos dar a perspectiva necessária sobre o estado atual do cenário de ameaças. Vamos voltar um pouco no tempo e analisar as tendências de cinco anos em relação a explorações, malware e botnets.

Explorações	Malware	Botnets
10.042 detecções de explorações únicas ■ +68% nos últimos 5 anos **54** detecções de exploração por organização ■ 75% nos últimos 5 anos **69%** das organizações detectaram ataques graves ■ -10% nos últimos 5 anos	**44.886** variantes únicas ■ +172% nos últimos 5 anos **7.063** famílias diferentes ■ +135% nos últimos 5 anos **18** famílias de malware espalhadas por ≥1/10 de todas as organizações ■ +100% nos últimos 5 anos	**330** botnets únicos detectados ■ +27% nos últimos 5 anos **4,3** botnets ativos por sensor ■ +126% nos últimos 5 anos **83** dias de infecção em média ■ +1.085% nos últimos 5 anos

Variantes de explorações em ascensão

O número de detecções de explorações únicas aumentou 68% nos últimos cinco anos. Por um lado, isso indica que temos mais maneiras de detectar ataques maliciosos hoje do que anteriormente. Além disso, demonstra que os invasores estão se multiplicando e diversificando seus ataques. Mas, ao mesmo tempo, observamos uma queda de 75% nas tentativas de exploração por organização e uma queda de 10% nas explorações graves.

Embora essa queda nas tentativas de exploração possa inicialmente parecer promissora, é outro indicativo de que os invasores estão realizando ataques mais direcionados. As armas cibernéticas também podem se tornar maçantes se usadas com muita frequência, pois os recursos de detecção acabarão alcançando o ritmo delas, inutilizando a carga útil ao longo do tempo.

Aumento da atividade de malware impulsionada pelo crime cibernético organizado

As famílias e variantes de malware dispararam nos últimos cinco anos, aumentando 135% e 175%, respectivamente. Indiscutivelmente, o mais notável é que o número de famílias de malware que se infiltraram em pelo menos 10% das organizações globais (um limiar de prevalência crítico) dobrou. Isso é, sem dúvida, resultado de um número crescente de grupos de cibercriminosos e de estados-nação, bem como da expansão das operações daqueles que estão atualmente ativos.

À medida que esses invasores se tornam cada vez mais seletivos, precisos e destrutivos, eles representam uma ameaça progressivamente crescente, exigindo uma batalha interminável contra eles. Aproveitando os avanços tecnológicos mais recentes e significativos dos últimos anos, esses inimigos evoluíram rapidamente para se tornarem mais capazes, versáteis e secretos.

Os botnets se tornam mais persistentes

A maioria das famílias de malware modernas estabeleceu botnets para comunicações de Comando e Controle (Command and Control, C2). Dado o crescimento das famílias e variantes de malware, faz sentido que a atividade de botnet também aumente. Hoje, há botnets mais ativos (+27%) e uma maior taxa de incidência de infecção por botnets entre as organizações (+126%).

No entanto, o maior incentivo para as tendências de botnet é o aumento significativo no número total de "dias ativos", isto é, o tempo entre quando a atividade de botnet é detectada pela primeira vez e o último sensor "atingido". Isso mede o número médio de dias entre a detecção e o bloqueio das comunicações de botnet antes que elas mudem o curso após uma tentativa de violação malsucedida. Em certo sentido, isso pode aludir ao tempo para "conhecer e desinfetar" em média para os sensores que detectaram esse tipo de atividade. Nos últimos seis meses, essa média foi 83 de 183 dias (o último dia que medimos), quase metade do período. Isso representa um aumento de mais de 1.000 vezes em relação às medições feitas no início de 2018, indicando que os botnets se tornaram mais persistentes nos últimos cinco anos. O aumento geral na disponibilidade de vulnerabilidades e explorações para incorporar no "cinturão de armas de botnet" torna isso uma preocupação, pois eles são rápidos em se adaptar e aumentar a gama de dispositivos que podem violar e controlar automaticamente.

Entrando na área de risco

Introduzimos a "área de risco" em nosso Relatório de cenário de ameaças global do 2º semestre de 2022 para entender melhor a probabilidade (ou improbabilidade) de que os agentes mal-intencionados explorem uma vulnerabilidade específica.[6]

Embora vários fatores influenciem a relação entre Vulnerabilidades e Exposições Comuns (Common Vulnerabilities and Exposures, CVEs) em endpoints e CVEs visados por invasores, como práticas de gerenciamento de vulnerabilidades entre organizações ou desenvolvimentos em ferramentas adversárias, isso fornece uma visão valiosa do estado da superfície de ataque que os líderes de segurança podem usar para priorizar seus esforços de correção.

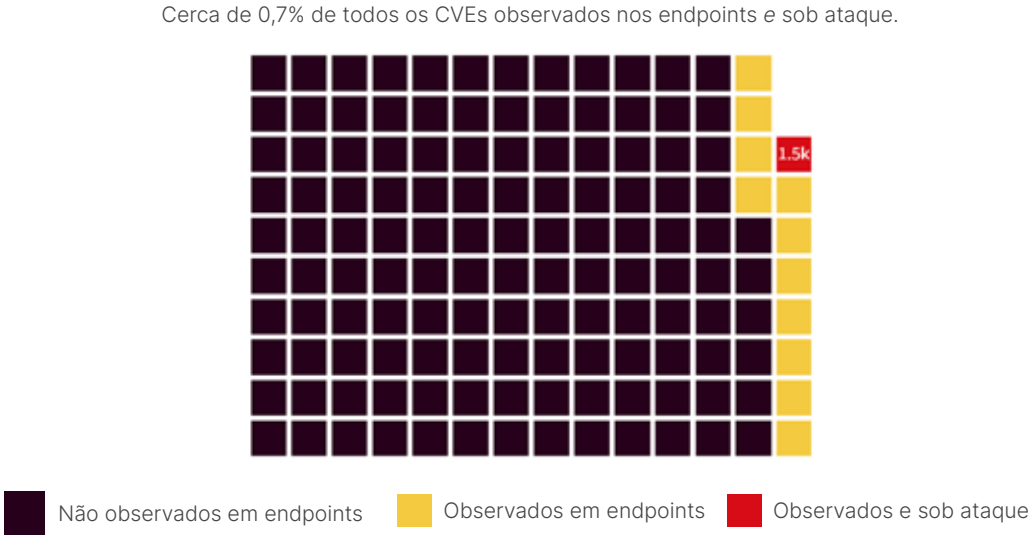


Figura 2: Todos os CVEs por presença nos endpoints e entre os ataques

No segundo semestre de 2022, a área de risco ficou em torno de 9%, o que significa que cerca de 1.500 CVEs, dos mais de 16.500 que observamos, estavam sob ataque. Mas para o primeiro semestre de 2023, essa proporção de CVEs sob ataque caiu para 8,3%. Curiosamente, aproximadamente o mesmo número de CVEs apareceu nos ataques, enquanto a parcela de CVEs observada nos endpoints cresceu. Embora isso não indique necessariamente que as organizações estão ganhando terreno na luta contra novas vulnerabilidades, pelo menos a porcentagem de vulnerabilidades sob ataque parece ser um pouco menor do que no passado.

Também sabemos que a parcela de vulnerabilidades sob ataque pode variar amplamente de acordo com a plataforma, chegando a 11%, conforme mostrado abaixo. Outra distinção notável entre as plataformas é a participação de todos os CVEs que apareceram nos endpoints, mostrados em amarelo. Considere a Microsoft e a Adobe, onde mais da metade das vulnerabilidades relacionadas foram observadas, em comparação com 12% para plataformas Apple ou 20% para Linux. Vale a pena notar que esses gráficos normalizam todas as plataformas. Por exemplo, um quadrado para Adobe representa um número absoluto diferente de vulnerabilidades do Linux.

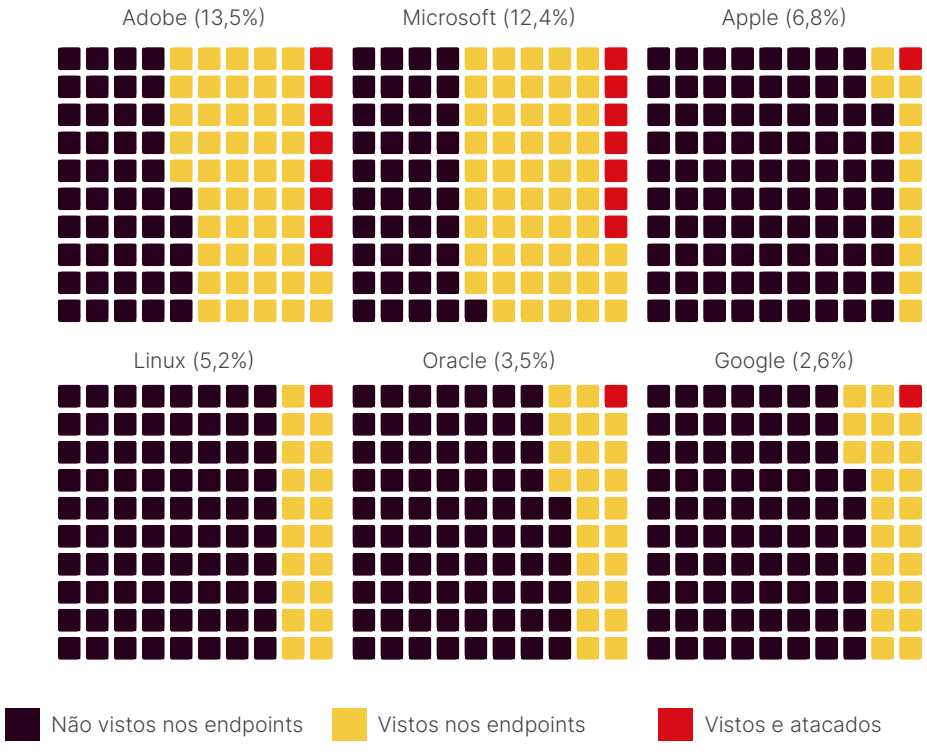


Figura 3: CVEs para várias plataformas por presença nos endpoints e entre os ataques

O que está claro é que as organizações continuam lutando para fechar vulnerabilidades com a mesma rapidez com que são liberadas, e os cibercriminosos são rápidos em explorar essa realidade. Portanto, é vital ter uma estratégia sólida ao priorizar quais vulnerabilidades corrigir. Embora cada plataforma deva ser considerada durante esse processo de priorização, isso apenas antecipa superficialmente quais vulnerabilidades abertas provavelmente serão alvo de invasores em um futuro próximo.

A boa notícia é que os defensores já têm algo mais poderoso à disposição, o Sistema de Pontuação de Previsão de Exploração (Exploit Prediction Scoring System, EPSS), abordado na próxima seção.[7]

Da previsão da exploração ao surto

Desde a sua criação, a Fortinet tem sido um dos principais contribuintes para os dados de atividade de exploração em apoio ao EPSS. O EPSS aproveita várias fontes de dados para prever as chances de uma vulnerabilidade ser explorada no contexto real. Ele é liderado por um grupo de interesse especial na FIRST.org, do qual a Fortinet é uma empresa membro.

As equipes de gerenciamento de vulnerabilidades usam o EPSS para ajudar a priorizar seus esforços de correção. Mas o EPSS também pode apoiar os esforços de inteligência para rastrear a progressão das vulnerabilidades desde a divulgação inicial até o surto de uma exploração no contexto real. É esse caso de uso que queremos explorar aqui. Se os dados do EPSS forem incorporados ao seu processo de threat intelligence, eles poderão ser usados de forma eficaz como um sistema de alerta precoce.

Vejamos um exemplo. Em 31 de maio, uma vulnerabilidade de injeção de SQL foi anunciada na aplicação da Web MOVEit Transfer, que poderia permitir que um invasor não autenticado alterasse ou excluísse elementos no mecanismo de banco de dados usado.[8] A comunidade de cibersegurança rapidamente reconheceu essa vulnerabilidade como algo a se observar, e a FortiGuard Labs lançou um Sinal de Ameaça para disseminar a conscientização e uma assinatura IPS para monitorar a atividade de exploração.[9]

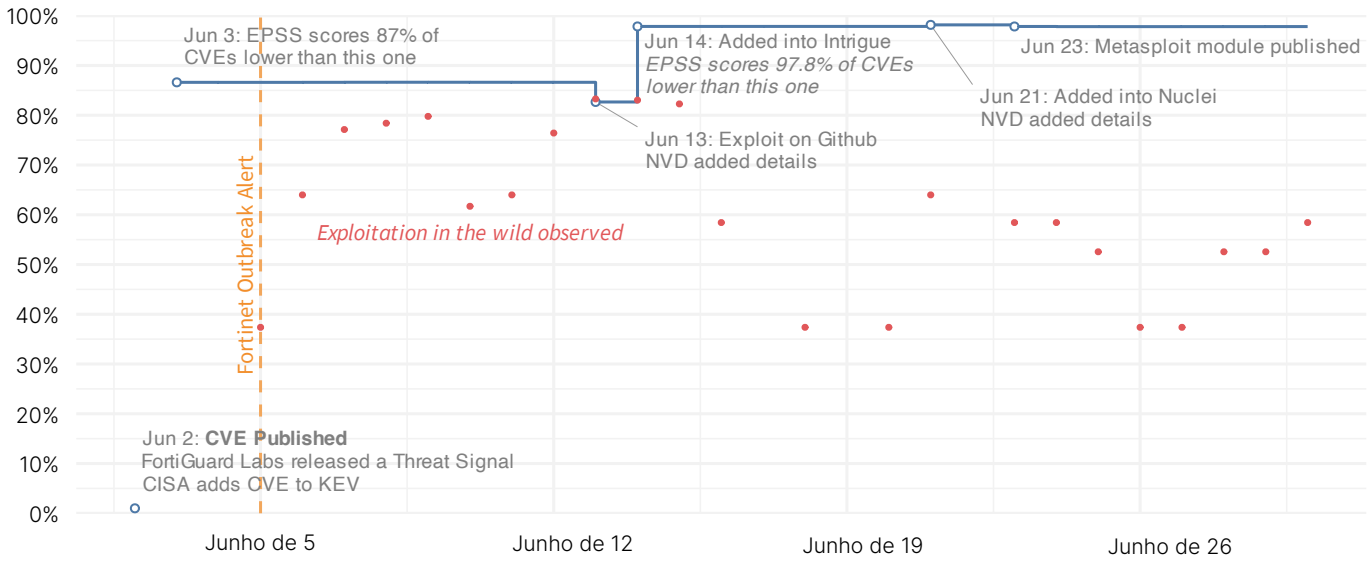


Figura 4: Evolução do EPSS e exploração para a vulnerabilidade MOVEit

Uma vez que a CVE foi publicada, o EPSS foi capaz de prever uma chance muito alta de exploração nos próximos 30 dias. Alerta de spoiler: não demorou muito. Nossos sensores registraram tentativas de invasores de explorar a vulnerabilidade MOVEit em 5 de junho, apenas cinco dias após a vulnerabilidade ter sido identificada pela primeira vez, e lançamos uma assinatura no mesmo dia. Nesse caso, os EPSS forneceram validação independente do que nossos analistas anteciparam e nos ajudaram a ficar à frente dessa ameaça emergente durante seu rápido período de aceleração.

O exemplo do MOVEit gera uma série de perguntas interessantes. Quanto tempo normalmente leva para uma vulnerabilidade passar da versão inicial para a exploração no contexto real? As CVEs com um EPSS alto são exploradas mais rapidamente do que aqueles com pontuações mais baixas? Em caso afirmativo, podemos prever o tempo médio de exploração de qualquer vulnerabilidade usando o EPSS?

Vamos ver se podemos responder a essas perguntas. Para fazer isso, analisamos seis anos de dados abrangendo mais de 11.000 vulnerabilidades publicadas para as quais nossos sensores detectaram exploração. Para cada CVE, determinamos o tempo desde a publicação até a primeira observação da exploração e a pontuação EPSS correspondente. A análise resultante é capturada no gráfico abaixo:

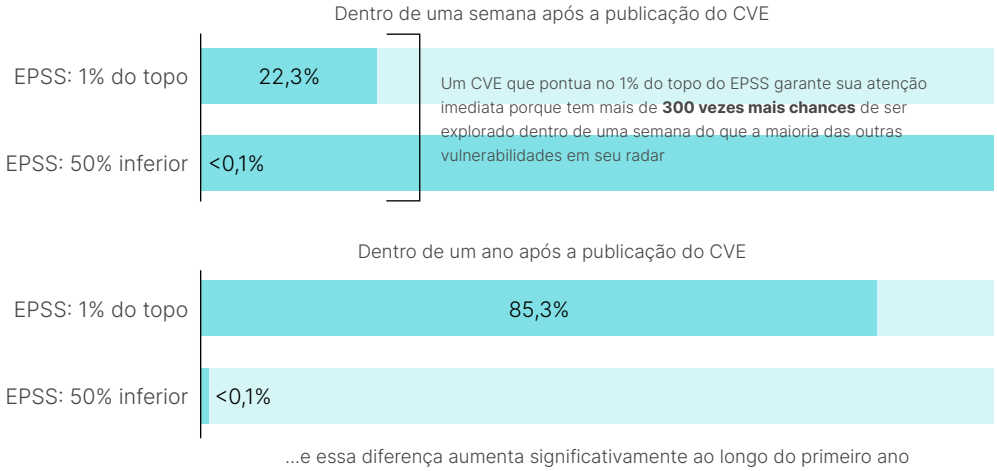


Figura 5: Taxa de exploração de vulnerabilidades com diferentes pontuações de EPSS

Resumindo, aprendemos que o EPSS é importante ao prever quais vulnerabilidades podem ser exploradas e com que rapidez essa exploração ocorrerá. Dentro de sete dias após a publicação, 22% das vulnerabilidades com as pontuações mais altas de EPSS (1% do topo) tiveram atividade de exploração, em comparação com apenas 0,07% daqueles na metade inferior das pontuações de EPSS. Após um ano inteiro, 85% das CVEs de EPSS de mais alto escalão registraram exploração, enquanto a metade inferior permaneceu amplamente ignorada pelos invasores.

Isso significa que um CVE que pontua no 1% do topo do EPSS merece sua atenção imediata porque tem mais de 300 vezes mais chances de ser explorado dentro de uma semana do que a maioria das outras vulnerabilidades em seu radar. Se você ainda não estiver fazendo isso, obtenha essas pontuações de EPSS diariamente e priorize seus esforços de correção de acordo.[10]

Mapa de calor global ATT&CK

Após aproximadamente seis meses de processamento contínuo de dados, aproveitando nossa rede global de mais de 10 milhões de sensores, compilamos uma lista dos hashes mais comumente observados no contexto real. Nossos sensores de última geração empregam técnicas de aprendizado de máquina (ML) para transformar dados brutos em um conjunto de dados enriquecido que examina o tráfego de rede em busca de ameaças potenciais. Em seguida, usamos nosso portfólio de produtos e soluções Fortinet para analisar cargas úteis maliciosas detectadas, observando e identificando comportamentos sutis indicativos de sua intenção subjacente. Os insights gerados por esse processo são cruciais para os defensores da cibersegurança em todo o mundo, permitindo engajamentos da equipe vermelha com foco em laser e atividades eficazes de investigação de ameaças.

A MITRE nos oferece um melhor entendimento das operações dos atores de ameaças. Fácil de seguir e acionável, o ATT&CK permite que os defensores categorizem os comportamentos dos agentes mal-intencionados de uma maneira sistemática e reproduzível, ajudando as equipes de segurança a identificar melhor os possíveis ataques e avaliar com precisão o risco organizacional.

Observe que este relatório representa apenas “uma fatia do bolo”. Diferentes soluções de segurança têm suas próprias capacidades e funções exclusivas quando se trata de detectar técnicas específicas. Esta análise se baseia em dados das soluções de sandboxing FortiSandbox e de detecção e resposta a ameaças de endpoints FortiEDR.

Vamos examinar os dados primeiro. Essas técnicas podem ser melhor interpretadas como capacidade de ataque.

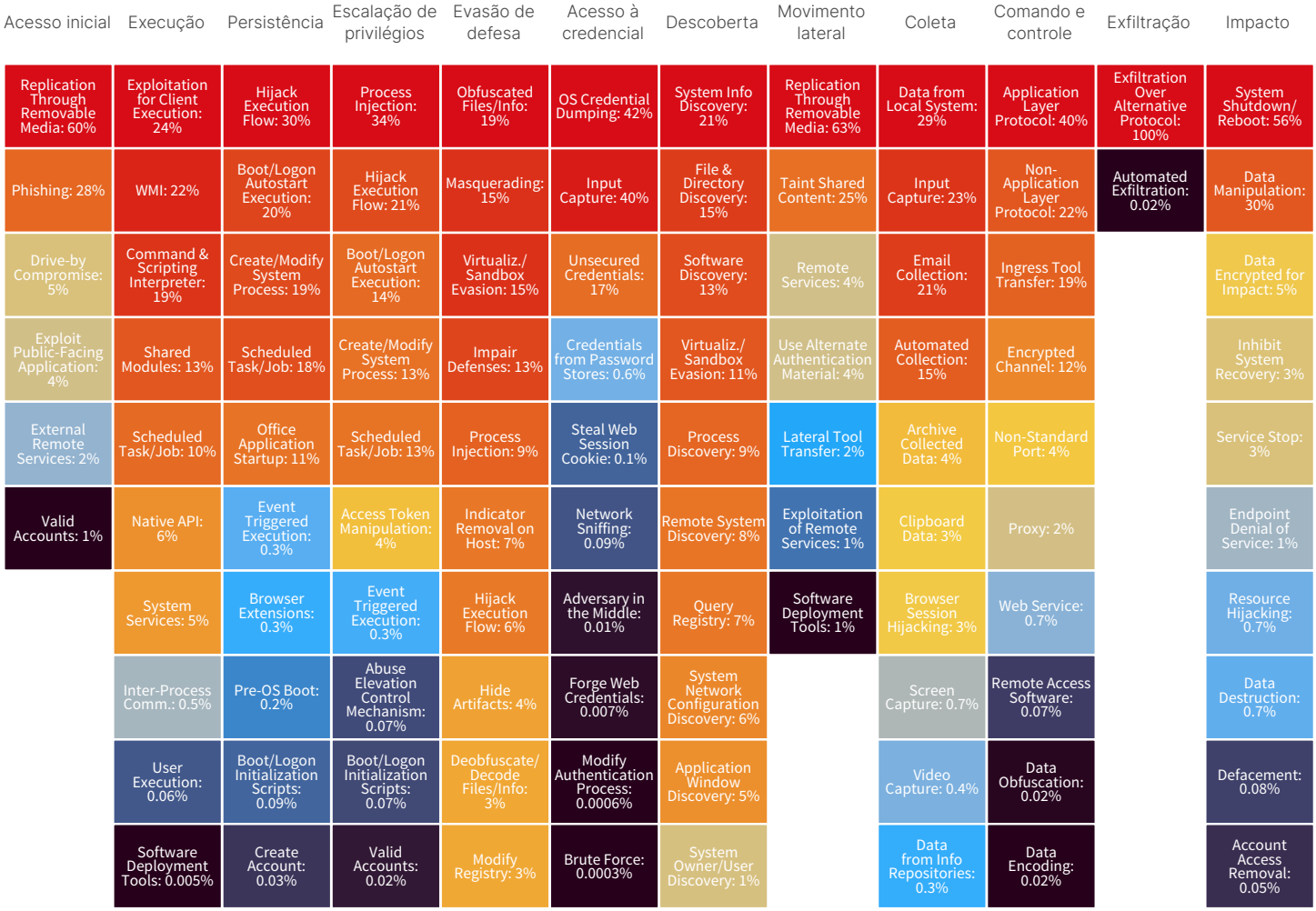


Figura 6: Técnicas ATT&CK em dados de nuvem por tática

Como você pode ver, as detecções obtidas a partir de dados fornecem visibilidade completa em toda a estrutura ATT&CK. As colunas acima destacam as 10 técnicas mais detectadas para cada tática. As subtécnicas listadas em cada coluna de categoria foram agrupadas em sua técnica pai por causa do visual. Vamos explorar como essas técnicas foram implantadas nos últimos seis meses e discutir maneiras de combatê-las.

Na fase de Acesso Inicial, a técnica mais prevalente observada é a replicação via mídia removível.[11] Embora não seja o ponto de entrada número um em redes corporativas, a maioria das cargas úteis maliciosas que analisamos pode se espalhar por esse método. Essa técnica teve um aumento no uso quando foi adquirida pela Raspberry Robin, que abordamos em nosso relatório anterior.[12] Desde então, a Microsoft descobriu vários outros usos desse worm, com o Raspberry Robin se tornando uma das maiores plataformas de distribuição de malware. Do ponto de vista do FortiGuard Labs, esse worm se espalhou amplamente, principalmente por causa de sua tática simples de mascarar um arquivo .LNK como uma pasta, que a maioria das pessoas provavelmente abrirá. Esta família de malware foi nomeada pela Agência de Cibersegurança e Infraestruturas (Cybersecurity and Infrastructure Security Agency, CISA) dos EUA como um dos droppers mais ativos existentes, sendo usada para distribuir malware IcedID, TrueBot e Bumblebee.[13]

Na fase de Execução, notamos um aumento na Exploração para Execução do Usuário.[14] Essa tendência implica que os ataques são cada vez menos dependentes de os usuários acionarem inadvertidamente uma carga útil ou habilitarem macros. Um exemplo é uma vulnerabilidade específica explorada no Microsoft Word, como a vulnerabilidade Follina cada vez mais prevalente detalhada em vários de nossos posts recentes no blog.[15] Também observamos essa tendência nas ameaças interrompidas pelo FortiEDR. Muitos agora dependem menos da interação do usuário para conseguir a execução do código. Uma maneira de proteger sua organização dessa técnica é reduzir sua superfície de ataque corrigindo vulnerabilidades regularmente.

Para a fase de Persistência, continuamos a ver altas instâncias de Side-loading de DLL (sob o Fluxo de Execução de Sequestro).[16] A 3CX empregou essa técnica para alcançar a Evasão de Defesa e a Persistência, que analisamos neste post recente.[17] Essa técnica é particularmente problemática porque permite que os invasores evitem medidas de proteção, como application control e outras limitações na execução de software. Para proteger a rede da sua organização contra essa técnica, certifique-se de que o software não seja vulnerável ao Side-loading de DLL em primeiro lugar, pois não há muito que você possa fazer para evitar a execução de código não intencional. Embora as cargas úteis maliciosas dentro da rede sejam sinalizadas eventualmente, isso só ocorrerá depois que elas forem carregadas na memória.

As três principais técnicas de Evasão de Defesa não são uma grande surpresa: Arquivos e Informações Ofuscados, Mascaramento e Virtualização/Evasão de Sandbox.[18, 19, 20] Mesmo peças únicas de malware demonstram várias formas de ofuscação, desde chamadas de API até strings na memória. Dada a ampla implementação de soluções de sandbox no local e como ofertas de Software como Serviço (SaaS), dominar essas técnicas tornou-se essencial para qualquer agente mal-intencionado.

OS Credential Dumping and Input Capture lideram o pacote em Credential Access.[21, 22] Desde o seu lançamento, observamos vários agentes mal-intencionados aproveitando o Mimikatz para funcionalidades relacionadas. Além disso, sua integração em várias estruturas pós-exploração, como Cobalt Strike, Metasploit e Sliver (e sua capacidade de ser carregada reflexivamente via PowerShell) o tornam uma ferramenta útil, mesmo entre ataques sem arquivo.

As fases de Descoberta e Movimento Lateral exibem uma relação simbiótica; o aumento da descoberta de ativos leva ao aumento do movimento lateral em ambientes comprometidos. Uma das estratégias de defesa mais eficazes contra isso é garantir visibilidade e controle adequados sobre o tráfego de rede, pois uma ampla variedade de técnicas ocorre durante essas fases e pode ser detectada com controles apropriados.

Da Coleção ao Impacto, pouco mudou. Os invasores usam as mesmas técnicas para coletar e agregar dados confidenciais e, em seguida, exfiltrar em um protocolo diferente do canal de comando e controle. Cerca de 22% dos ataques usam uma camada não relacionada a aplicações, como UDP ou ICMP, para se comunicar com seus servidores C2. Embora seja uma escolha incomum devido à maior complexidade de estabelecer e manter uma conexão e à falta de correção de erros, essa técnica pode passar despercebida porque esses protocolos não são monitorados de perto.

Insights técnicos da telemetria de endpoint

Analisar nossos dados do FortiEDR nos dá outra perspectiva em relação aos ataques e às técnicas iniciais de acesso que os cibercriminosos usam. Na maioria dos casos, as organizações que usam recursos de EDR também usam alguma forma de sandbox, por isso é seguro dizer que as ameaças que são interrompidas por uma ferramenta de EDR são provavelmente aquelas que teriam conseguido contornar a tecnologia de sandboxing "tradicional" (um excelente exemplo da necessidade de defesa em profundidade). Entender como essas ameaças operam pode dar aos defensores uma inteligência mais focada em suas atividades de investigação de ameaças.

Figura 7: Principais técnicas ATT&CK detectadas pelo FortiEDR por mês

Acima estão as cinco técnicas mais ativas por mês. Algumas das mesmas técnicas vistas e interrompidas pela tecnologia de sandboxing são usadas em outros eventos, uma vez que a execução é alcançada dentro de uma máquina em uma organização. As técnicas mais ativas que observamos durante o 1º semestre de 2023 incluem:

- Injeção de processo
- Captura de entrada
- Despejo de credenciais do sistema operacional
- Aplicações de exploração voltadas ao público
- Exploração para evasão de defesa

A injeção de processo é a líder em todos os meses.[23] Com uma dúzia de possíveis tipos de injeção de processo que já foram categorizados, essa técnica é, sem dúvida, usada e abusada pelos invasores para evasão de defesa e escalonamento de privilégios.

A segunda e terceira técnicas mais usadas em todos os meses é acesso à credencial: captura de entrada. Usando essas técnicas, os possíveis agentes mal-intencionados tentam interceptar a entrada do usuário para adquirir credenciais ou acumular dados procurando credenciais na memória. Durante a interação regular do sistema, os usuários normalmente compartilham suas credenciais em vários pontos de extremidade, como portais de autenticação ou janelas de prompt do sistema. Os mecanismos implantados para capturar essa entrada muitas vezes podem ser indistinguíveis para o usuário, como por meio do Credential API Hooking.

Para terminar, temos Exploração para Evasão de Defesa e Acesso Inicial como as técnicas finais mais usadas, com quase o mesmo número de gatilhos no contexto real. Os invasores estão ansiosos para explorar vulnerabilidades no software para obter um ponto de vantagem no sistema, para que possam realizar ainda mais suas ações nefastas. Com o número de CVEs crescendo exponencialmente nos últimos dois anos (estamos a caminho de atingir 30.000 CVEs este ano, um aumento de 50% em relação aos 20.000 CVEs relatados em 2021), não é como se houvesse uma escassez de vulnerabilidades para os invasores adicionarem às suas respectivas caixas de ferramentas. Juntamente com o advento dos Modelos de Linguagem Grande (Large Language Models, LLMs) usados para processar rapidamente grandes conjuntos de dados para identificar rapidamente ameaças recebidas e vulnerabilidades existentes, esse é um alvo fácil a ser explorado, então esperamos que elas continuem a ser a arma de escolha dos cibercriminosos.

Protegendo sua empresa contra ameaças em evolução

Os cibercriminosos nunca perderão uma oportunidade de lucrar, e o aumento do crime cibernético organizado, como grupos RaaS nos últimos anos, tornou ainda mais fácil conseguir um pagamento rápido. Os agentes mal-intencionados encontrarão constantemente novas vulnerabilidades para explorar e técnicas de ataque mais sofisticadas para se infiltrar nas redes. No entanto, a boa notícia é que a maioria das táticas usadas pelos agentes mal-intencionados nos últimos meses são familiares para nós, o que significa que os defensores nunca tiveram tantas oportunidades para impedir ataques antes que eles aconteçam.

À medida que os invasores continuam a evoluir suas próprias operações, no entanto, é crucial avaliar e aprimorar as estratégias de defesa cibernética dentro de sua organização para ficar à frente de ameaças potenciais. Desde o uso e compartilhamento de threat intelligence até a implementação das tecnologias certas, aqui estão várias etapas que você pode seguir hoje para proteger as redes e os dados da sua empresa.

Compartilhar e utilizar threat intelligence

Para combater a sofisticação e o volume cada vez maiores de ameaças cibernéticas, a prática de compartilhar e utilizar threat intelligence surgiu como um componente vital de qualquer estratégia de defesa organizacional. A Fortinet está empenhada em fazer a sua parte para permitir avanços no compartilhamento de threat intelligence.

A Fortinet é membro fundador da Cyber Threat Alliance (CTA), uma organização criada em 2014 para permitir o compartilhamento de threat intelligence entre fornecedores concorrentes de cibersegurança.[24] Avançando rapidamente até hoje, essa organização tornou-se vital para combater o crime cibernético de forma eficaz em escala global. No entanto, estabelecer confiança e confidencialidade, garantir a padronização dos dados e gerenciar um alto volume de informações são apenas alguns obstáculos que complicam o compartilhamento eficaz de informações. O CTA enfrentou com sucesso esses desafios, unindo equipes de elite de Threat Intelligence Cibernética (CTI) em todo o mundo e aprimorando significativamente a perspectiva global sobre ameaças cibernéticas.

Compreender os fluxos de ataque para identificar padrões e indicadores de compromisso

Os ataques cibernéticos estão se tornando mais sofisticados, frequentes e prejudiciais, portanto é crucial que as empresas aprimorem seu conhecimento sobre seus invasores. Compreender o fluxo de ataque, desde os pontos de entrada iniciais até as atividades pós-exploração, é essencial para o desenvolvimento de estratégias eficazes de cibersegurança.

O fluxo de ataque refere-se à sequência de etapas que um invasor segue para se infiltrar em um sistema alvo e atingir seus objetivos. Ela engloba vários estágios, incluindo reconhecimento, acesso inicial, escalonamento de privilégios, movimento lateral, exfiltração de dados e persistência. As organizações podem identificar melhor as vulnerabilidades, implementar medidas de segurança apropriadas e responder de forma eficaz às ameaças cibernéticas, entendendo cada estágio.

Compreender o fluxo de ataque é crucial por vários motivos. Primeiro, permite que as organizações entendam visualmente as etapas de um ataque e seus relacionamentos e resultados. Ao estudar as táticas, técnicas e procedimentos (Tactics, Techniques, and Procedures, TTPs) dos invasores em cada estágio, as equipes de segurança podem identificar padrões e indicadores de compromisso (indicatores of compromise, IOCs), permitindo que identifiquem um ataque em andamento e tomem medidas oportunas.

Compreender o fluxo de ataques também ajuda as organizações a alocar recursos de forma mais eficaz. Ao se concentrar nos estágios mais vulneráveis de um ataque, como acesso inicial ou escalonamento de privilégios, as empresas podem priorizar medidas de segurança e investimentos para maximizar sua postura de cibersegurança.

Por fim, entender um fluxo de ataques permite que as organizações aprimorem suas capacidades de resposta a incidentes. Ao mapear os vários estágios e atividades potenciais de um ataque, as equipes de segurança podem desenvolver cartilhas e planos de resposta adaptados a cada estágio, garantindo uma resposta rápida e eficaz durante um ataque cibernético.

As vantagens de entender completamente os fluxos de ataque são o motivo pelo qual a Fortinet participou como patrocinadora de pesquisa nos projetos de MITRE Engenuity's Center for Threat-Informed Defense (CTID) ATTACK Flow.[25] Acreditamos que tais avanços na threat intelligence, nos quais podemos identificar e responder a ameaças com base em seu perfil, mudarão a economia de um ataque para inclinar a escala em favor dos defensores.

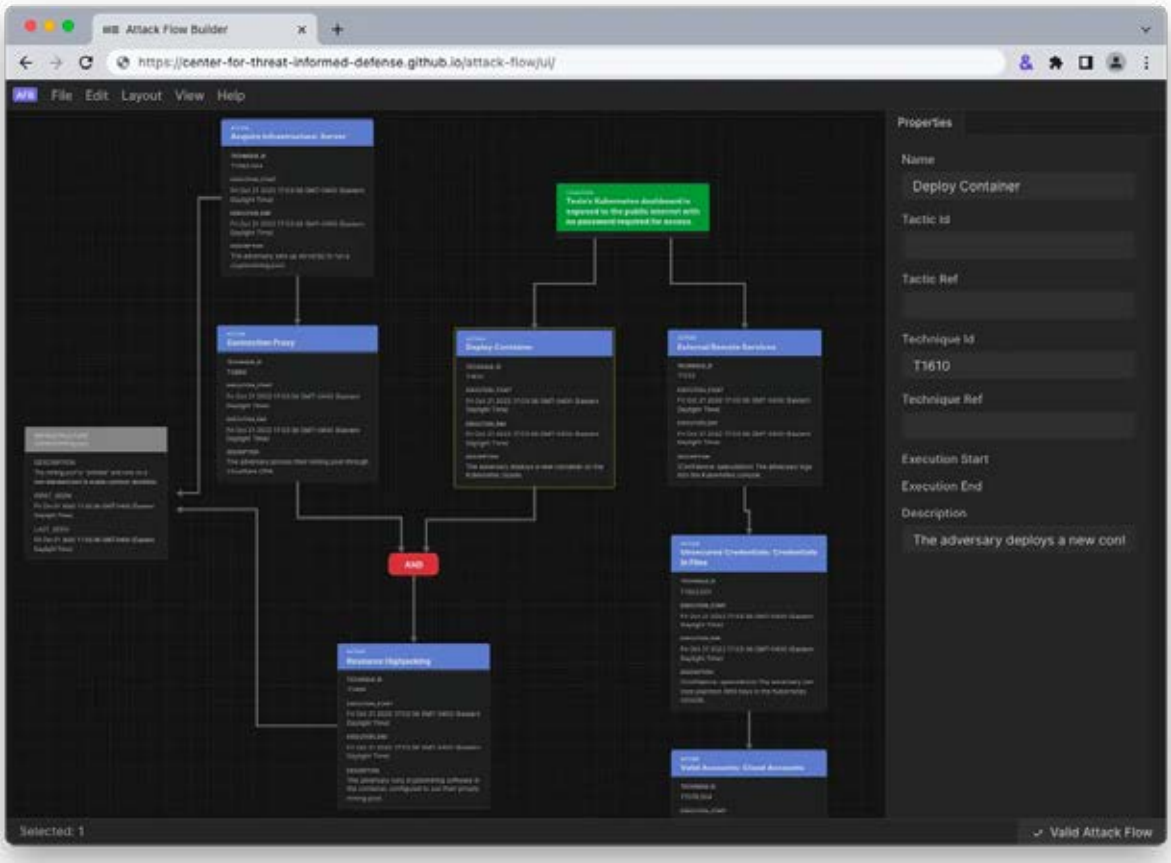


Figura 8: Construtor de fluxo MITRE ATT&CK - exemplo de fluxo

Também estamos começando a incorporar padrões em nossos relatórios, como o trabalho de driver da Wintapix, publicado por dois de nossos pesquisadores.[26]

Fortaleça suas tecnologias e processos

Agora é o melhor momento para implementar novas tecnologias de segurança ou reavaliar sua pilha atual. Independentemente das ferramentas escolhidas, você deve garantir que elas possam aproveitar a inteligência artificial (IA), o aprendizado de máquina (ML), o aprendizado profundo (DL) e a análise avançada. Esses recursos se tornaram essenciais para processar o enorme volume de dados que as organizações geram para identificar tráfego arriscado ou anômalo que pode indicar uma ameaça ou outro risco.

Examinar e ajustar seus processos atuais é uma obrigação se você quiser ficar à frente de seus invasores. Isso inclui redefinir funções e responsabilidades em sua equipe de segurança, criar ou atualizar cartilhas e realizar exercícios de mesa para testar as capacidades de sua equipe ou identificar lacunas de processo que devem ser abordadas.

Muitas organizações hoje também estão recorrendo a fornecedores confiáveis para atuar como uma extensão de seu próprio pessoal de segurança. Nossos Serviços de segurança habilitados por IA do FortiGuard abrangem uma variedade de ferramentas poderosas, como Next-Generation Firewalls (NGFWs); telemetria e análise de rede; EDR; detecção e resposta estendidas (XDR); Digital Risk Protection (DRP); Gerenciamento de Eventos e Informações de Segurança (SIEM); sandboxing em linha; fraude; orquestração, automação e resposta de segurança (SOAR); e muito mais. Essas soluções fornecem à sua organização recursos avançados de detecção e prevenção de ameaças que podem ajudá-lo a detectar e responder rapidamente a incidentes de segurança em toda a superfície de ataque.

Conclusão e perspectiva final

Esperamos que você tenha gostado de ler este relatório tanto quanto gostamos de criá-lo. Entendemos que a cibersegurança às vezes pode parecer extremamente complexa. No entanto, o campo é invariavelmente preenchido por indivíduos inspirados e entusiasmados que trabalham incansavelmente para fornecer à comunidade abordagens inovadoras e simplificadas para melhorar sua postura de segurança. A luta contra o crime cibernético e as ameaças representadas pelos estados-nação é um desafio constante e, como setor, estamos totalmente preparados para enfrentá-lo e combatê-lo.

O fortalecimento de parcerias de compartilhamento de threat intelligence entre os setores público e privado é crucial no combate a essa guerra cibernética. A threat intelligence deve ser imediatamente acionável por meio de cartilhas abrangentes, o que pode ser um desafio sem padrões quando se trata de compartilhamento, ferramentas e relatórios. No entanto, a threat intelligence compartilhada é um componente fundamental de como garantimos respostas sem atrito, oportunas e eficazes. Acreditamos firmemente que os defensores hoje possuem amplo acesso a ferramentas, conhecimento e apoio para começar a alterar a economia de um ataque, todos os quais representam uma poderosa contramedida contra os invasores.

[1] "MITRE ATT&CK Matrix for Enterprise", MITRE, 2015–2023.

[2] Douglas Jose Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs", Fortinet, 3 de março de 2023.

[3] "2H 2022 Global Threat Landscape Report", Fortinet, 3 de março de 2023.

[4] Geri Revay, "The Year of the Wiper", Fortinet, 24 de janeiro de 2023.

[5] Derek Manky, "The Latest Intel on Wipers", Fortinet, 23 de março de 2023.

[6] Douglas Jose Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs", Fortinet, 3 de março de 2023.

[7] "Exploit Prediction Scoring System", FIRST.org, 2015–2023.

[8] James Slaughter, Fred Gutierrez, and Shunichi Imano, "MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-Day", Fortinet, 8 de junho de 2023.

[9] "Threat Signal Report: MOVEit Transfer Critical Vulnerability (CVE-2023-34362)", FortiGuard Labs, 2 de junho de 2023.

[10] "EPSS API", FIRST.org, 2015–2023.

[11] "Replication Through Removable Media", MITRE ATT&CK, 31 de maio de 2017.

[12] "IPS Threat Encyclopedia: Raspberry.Robin.Worm", FortiGuard Labs, 14 de julho de 2022.

[13] "Increased Truebot Activity Infects U.S. and Canada-Based Networks", Cybersecurity and Infrastructure Security Agency, 6 de julho de 2023.

[14] "Exploitation for Client Execution", MITRE ATT&CK, 18 de abril de 2018.

[15] Fortinet Follina Blog Posts, acessado em 27 de julho de 2023.

[16] "Hijack Execution Flow: DLL Side-Loading", MITRE ATT&CK, 13 de março de 2020.

[17] FortiGuard Labs, "3CX Desktop App Compromised (CVE-2023-29059)", Fortinet, 30 de março de 2023.

[18] "Obfuscated Files or Information", MITRE ATT&CK, 31 de maio de 2017.

[19] "Masquerading", MITRE ATT&CK, 31 de maio de 2017.

[20] "Virtualization/Sandbox Evasion", MITRE ATT&CK, 17 de abril de 2019.

[21] "OS Credential Dumping", MITRE ATT&CK, 31 de maio de 2017.

[22] "Input Capture", MITRE ATT&CK, 31 de maio de 2017.

[23] "Process Injection", MITRE ATT&CK, 31 de maio de 2017.

[24] Derek Manky, "Partnering to Disrupt Cybercrime", Fortinet, 14 de fevereiro de 2023.

[25] Douglas Jose Pereira dos Santos, "MITRE Attack Flow Gives CISOs Valuable Context for Better Risk Management", Fortinet, 3 de novembro de 2022.

[26] Geri Revay and Hossein Jazi, "WINTAPIX: A New Kernel Driver Targeting Countries in the Middle East", Fortinet, 22 de maio de 2023.

agosto 17, 2023 4:25 PM

2278529-0-0-PT