



2H 2023

Relatório de cenário de ameaças global

Um relatório semestral da FortiGuard Labs



Resumo executivo

No segundo semestre de 2023, o cenário de segurança cibernética viu uma série de desenvolvimentos significativos que afetaram consideravelmente a superfície de ataque digital. Dentre eles, notável foi o aumento de ataques cibernéticos sofisticados direcionados a entidades de grande escala e infraestrutura essencial.

Se o crescente número de ataques não fosse suficiente para manter a maioria dos CISO acordados à noite, o domínio da segurança cibernética está lutando simultaneamente com o desafio contínuo de atrair e reter profissionais qualificados. A crescente demanda por especialistas qualificados em segurança cibernética, juntamente com a necessidade de as organizações oferecerem oportunidades atraentes de desenvolvimento de carreira e ambientes de trabalho, continua a destacar a importância do capital humano no combate às ameaças cibernéticas.

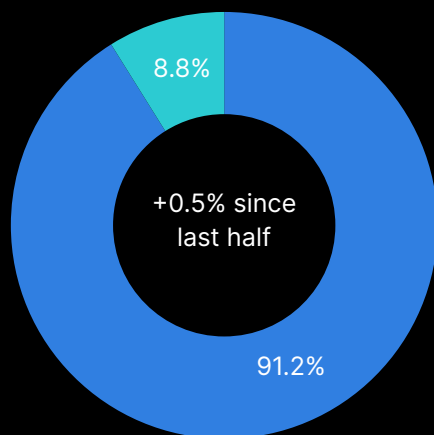
A necessidade de entender onde estão suas lacunas na superfície de ataque em detecção, mitigação e resposta é mais vital do que nunca e a coisa mais impactante que podemos fazer é esclarecer como o cenário de ameaças tem mudado e como as organizações precisam construir sistemas de rede seguros que possam se adaptar rapidamente às demandas de negócios em constante mudança e ao cenário de ameaças em evolução. É por isso que publicamos este relatório. Nosso objetivo é ajudá-lo a navegar por essas mudanças e entender onde concentrar seu tempo e energia, usando seus recursos da maneira mais impactante.

As descobertas neste relatório representam a inteligência coletiva do FortiGuard Labs, extraída de uma vasta gama de sensores de rede que coletam eventos de ameaças todos os dias observados em ambientes de produção ao vivo em todo o mundo de mais de 600K ambientes e mais de 10M de sensores que capturam todos os detalhes sobre ameaças que atingem nossa tecnologia de detecção. Examinamos todos esses dados para encontrar e extrair percepções importantes que esperamos que ajudem a guiá-lo pelos desafios cibernéticos de 2024.



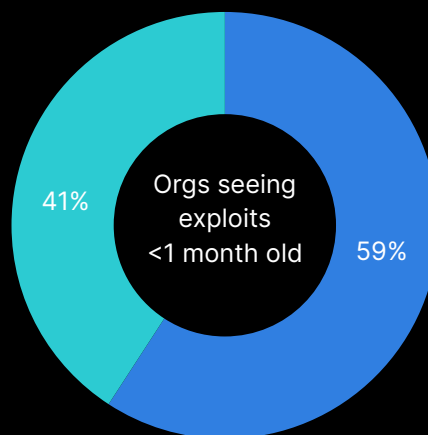
2H 2023 Active Threat Landscape at a Glance

Into the Red Zone



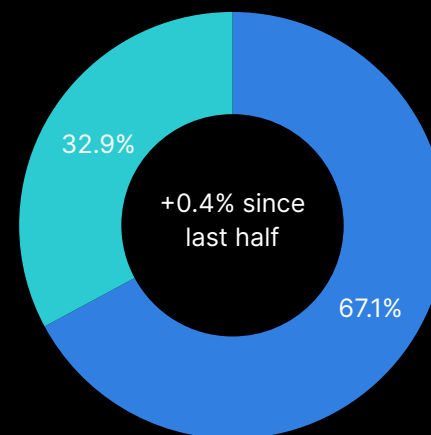
The percent of all endpoint vulnerabilities targeted by attacks remained steady, around 9%.

Exploit Dispersion



Attacks can spread quickly. 41% of organizations detected activity for exploits less than one month old.

ATT&CK Sightings



Sandbox and network detection and response (NDR) sensors observed activity for over two-thirds of MITRE ATT&CK techniques.

APT Groups

38/143

FortiRecon intelligence indicates 38 of the 143 advanced persistent threat (APT) groups listed by MITRE were active during this time.

Ransomware

40%+

More than 40% of ransomware and wipers targeted the industrial sector, indicating that cybercriminals are focused on OT and the supply chain.

Time-to-Exploitation

43%

On average, for new exploits identified, attacks occurred in 4.76 days after discovery. That's 43% faster than the prior period.

Uma visão das tendências de exploração, malware e botnets

O FortiGuard Labs monitora uma vasta gama de sensores implantados globalmente que coletam trilhões de eventos de ameaças em todo o mundo todos os dias. Esse ponto de vista exclusivo nos dá uma visão detalhada e abrangente do cenário de ameaças cibernéticas, incluindo como as tendências de exploração, malware e botnet mudam ao longo do tempo.

Explorações	Malware	Botnet
11.030 detecções de exploração exclus vas, +10% na última metade	39.896 variantes únicas detectadas, -11% em relação à última metade	319 botnets exclusivos detectados, -3% em relação à última metade
63 detecções de exploração por organização, +17% na última metade	5.962 famílias ativas diferentes, -16% em relação à última metade	4,3 botnets ativas por sensor, +/-0% em relação à última metade
73% das empresas observaram ataques graves, +4% em relação à última metade	16 famílias se espalharam para mais de 10% das organizações, -11% em relação à última metade	85 dias de infecção em média, +2% na última metade

Esses dados, descritos no gráfico acima, mostram que a criação e prevalência de explorações estão aumentando. Os cibercriminosos estão visando o número cada vez maior de novas vulnerabilidades resultantes do crescimento exponencial no número e na variedade de dispositivos conectados e uma explosão em novos aplicativos e serviços on-line. É natural que os ataques que buscam explorar essas vulnerabilidades também aumentem. Esse aumento no volume de explorações por organização está, sem dúvida, contribuindo para a prevalência de equipes de segurança sobrecarregadas.

Curiosamente, após aumentar no primeiro semestre de 2023, o volume de amostras de malware detectadas por nossos sensores diminuiu no segundo semestre do ano. Infelizmente, para os defensores, isso não significa que o malware esteja caindo desfavoravelmente entre invasores inteligentes. A desaceleração observada é provável porque certos tipos de malware, especialmente ransomware, estão adotando uma abordagem mais direcionada, levando a um aumento no incidente de custo por ransomware. Isso também explica por que o tráfego de bots permaneceu estável durante esse mesmo tempo.

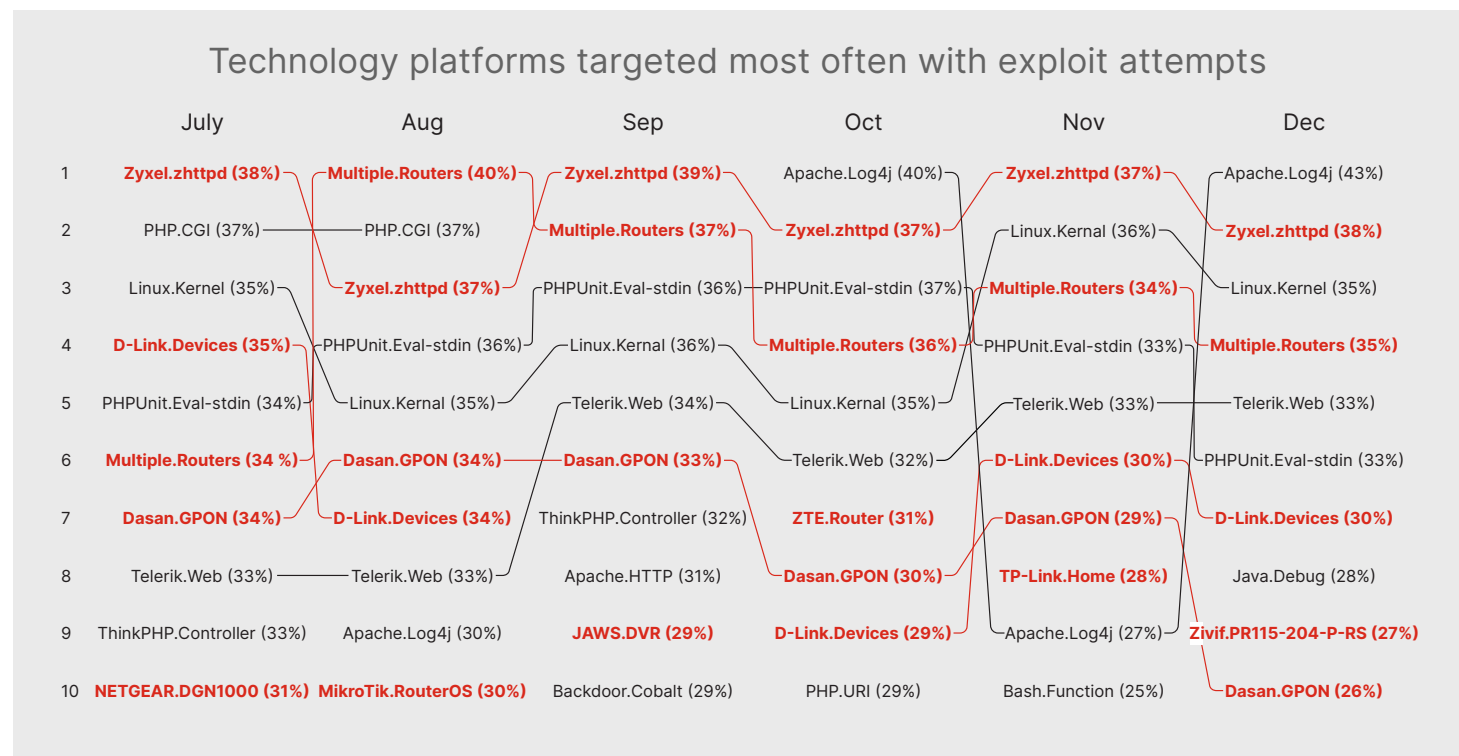
As explorações da IoT estão aumentando

A atividade de exploração capturada pelos sensores do Sistema de prevenção de intrusão (IPS) FortiGuard em execução em nossos FortiGate Next-Generation Firewalls fornece visibilidade incomparável de como os agentes de ameaças encontram vulnerabilidades, exploram seus alvos e constroem infraestrutura maliciosa. Esses sensores são frequentemente o primeiro ponto de contato com um invasor que sonda exposições. Vamos começar com uma visão das tecnologias que os invasores estão sondando de forma mais agressiva. Não é de surpreender que os dispositivos de Internet das Coisas (IoT), mostrados em vermelho no gráfico correspondente, sejam alvos populares, em grande parte porque muitas vezes estão protegidos ou desprotegidos.



Embora tenhamos destacado alertas de surtos para dispositivos IoT aqui, nossa equipe do FortiGuard Labs teve seus radares preenchidos com todos os tipos de explorações de vulnerabilidade adicionais no 2H de 2023. Aqui está uma rápida recapitulação de alguns deles:

- Vulnerability⁵
- Vulnerabilidade de execução de código IBM Aspera Faspex⁶
- Attack⁷
- Attack⁸
- Vulnerability⁹
- Vulnerability¹⁰

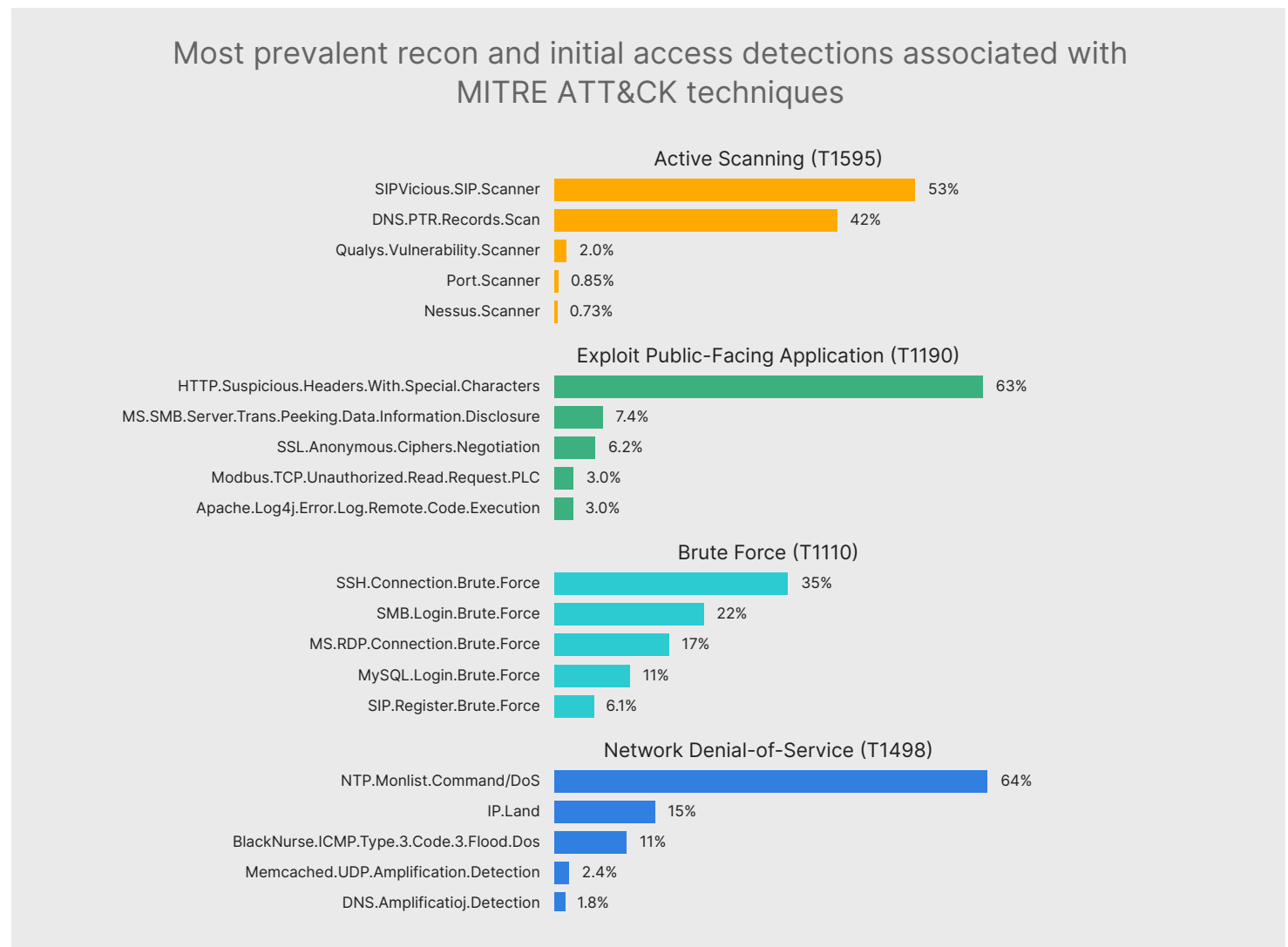


As vulnerabilidades que afetam roteadores, câmeras e outros dispositivos IoT foram o foco de vários alertas de surto publicados pelo FortiGuard Labs ao longo de 2023.¹

O equipamento da Zyxel Networks foi um alvo favorito para explorações ao longo do segundo semestre do ano, com o FortiGuard Labs emitindo um alerta de surto sobre os firewalls da empresa.² Talvez cheirando sangue na água, os invasores redescobriram e exploraram uma vulnerabilidade da Zyxel Networks relacionada a um roteador de fim de vida útil, que foi inicialmente publicado em 2017.³

Falando em antigas vulnerabilidades que atraem nova atenção, as explorações direcionadas às câmeras web Zivif (CVE-2017-17107) ficaram na lista das 10 principais em dezembro de 2023. Essas explorações parecem estar relacionadas a ataques Zerobot em andamento que alertamos os profissionais de segurança no final de 2022.⁴ Este cenário mostra que vulnerabilidades antigas sempre podem ser novas (e melhores) por agentes de ameaças empreendedores.

Estamos encerrando essa revisão de exploração com outro gráfico demonstrando o amplo escopo de atividade detectado por nossos sensores IPS. Aqui está uma visão das cinco principais detecções de exploração associadas a quatro técnicas principais MITRE ATT&CK ¹ de varredura ativa, aplicativos de exploração voltados para o público, força bruta e DoS de rede.



Os appliances de segurança de rede fornecem inteligência no lado esquerdo da estrutura MITRE ATT&CK , o que nos ajuda a entender mais sobre as ameaças que os agentes maliciosos estão usando para tentar entrar nas organizações. Idealmente, ao aplicar a estrutura ATT&CK em toda a sua empresa, recomendamos agrupar fontes ATT&CK e criar um mapa de calor consolidado para uso em caça a ameaças, equipe roxa, emulação adversária e engenharia de detecção.

Rastreamento do movimento entre famílias de malware

Depois que os agentes de ameaças encontram uma vulnerabilidade explorável, seu próximo passo é geralmente implantar malware. As amostras coletadas por nossas várias soluções antimalware oferecem informações sobre ferramentas populares do adversário para estabelecer uma base, aumentar os privilégios, manter a presença e mover-se lateralmente dentro dos ambientes-alvo para alcançar seus objetivos.

A figura na próxima página mede a proporção de organizações em cada região que detectaram variantes das famílias de malware mais comuns durante o segundo semestre do ano. O malware que ganha uma posição em uma região do mundo, como a família JS/Agente, ganha tração semelhante na maioria das outras geografias.



Top malware families based on regional prevalence

	Africa	Asia	Europe	Latin America	Middle East	North America	Oceania
JS/Agent	40.9%	34.2%	34.0%	37.4%	30.9%	30.0%	35.9%
JS/Phishing	17.6%	15.9%	19.2%	19.8%	12.7%	12.0%	18.5%
MSIL/Kryptik	17.4%	22.6%	19.8%	16.6%	16.9%	4.8%	7.5%
HTML/Phish	16.5%	19.9%	18.6%	15.2%	13.9%	7.9%	12.0%
JS/ScrInject	20.1%	13.1%	11.9%	18.6%	33.4%	10.3%	18.7%
JS/Cryxos	12.8%	28.6%	13.6%	14.7%	12.1%	13.3%	18.7%
MSIL/GenKryptik	14.6%	20.8%	17.9%	16.1%	15.4%	4.3%	7.2%
PDF/Phishing	14.1%	12.8%	14.9%	12.9%	11.2%	8.9%	14.1%
MSIL/GenericKDS	11.8%	19.1%	15.2%	13.6%	12.7%	3.7%	6.1%
HTML/Phishing	12.5%	13.1%	12.0%	9.6%	9.2%	5.6%	7.3%
MSIL/Agent	11.6%	16.1%	14.6%	11.4%	12.1%	3.5%	5.6%
Msoffice/CVE_2018_0798	9.8%	15.0%	15.1%	9.4%	10.2%	3.4%	4.7%
JS/Redirector	13.7%	7.7%	9.6%	8.0%	7.8%	7.5%	10.7%
MSIL/Stealer	9.5%	14.6%	11.8%	10.3%	10.3%	2.8%	4.5%
NSIS/Injector	8.5%	13.4%	13.1%	7.1%	10.1%	2.4%	5.3%
Msoffice/CVE_2017_11882	8.4%	12.1%	11.0%	17.6%	9.5%	2.5%	3.4%
HTML/infObfus	11.8%	5.9%	6.3%	4.2%	10.1%	10.5%	15.7%
BAT/Agent	5.5%	9.1%	6.3%	9.0%	6.7%	3.7%	4.3%
W32/Injector	8.6%	11/9%	8.9%	6.8%	9.0%	2.2%	3.0%
MSEXcel/CVE_2017_11882	8.2%	12/3%	8.6%	5.0%	7.4%	2.3%	3.3%

Caso você queira verificar novamente suas verificações antivírus em busca das variantes mais comuns de JS/Agente, veja as três principais a serem procuradas, além de uma variante final que subiu rapidamente na popularidade no 2H de 2023:

- JS/Agent.CY!.tr¹²
- JS/Agent.F022!.tr¹³
- JS/Agent.PIV!.tr¹⁴
- JS/Agent.NDS!.tr¹⁵

No entanto, duas famílias de malware contornaram a tendência de uniformidade regional: JS/ScrInject e JS/Cryxos. Para o primeiro, a variante responsável é JS/ScrInject.B!.tr.¹⁶ Este Cavalo de Troia de acesso remoto (RAT) está circulando desde 2011 e tem um ciclo de atividade semanal muito regular.¹⁷ O outro é JS/Cryxos e, em particular, o JS/Cryxos.⁵⁴⁷⁸!.tr variante.¹⁸ Este Cavalo de Troia, conhecido por ter uma variedade de recursos clandestinos, parece estar impulsionando a maioria das detecções em toda a Ásia.

Fora das famílias genéricas mais prevalentes descritas acima, quatro campanhas adicionais de malware chamaram nossa atenção no segundo semestre de 2023: AndroxGh0st, ransomware Apache ActiveMQ, RATs Lazarus e Agent Tesla. Cobriremos o AndroxGh0st extensivamente na seção de botnets, então vamos resumir os outros três aqui.

Apache ActiveMQ

O Apache ActiveMQ é um corretor de mensagens de código aberto popular. Uma vulnerabilidade foi divulgada (CVE-2023-46604) no outono de 2023 que permitiu que um invasor remoto com acesso à rede a um corretor executasse comandos de shell arbitrários manipulando tipos de classe serializados no protocolo OpenWire.¹⁹ Em novembro surgiram relatórios de que os invasores estavam aproveitando essa falha na forma do ransomware HelloKitty.²⁰ O FortiGuard Labs lançou um alerta de surto detalhando como os agentes de ameaças estavam explorando essa falha executando campanhas de ransomware direcionadas a servidores que executam versões desatualizadas e vulneráveis do Apache ActiveMQ.²¹

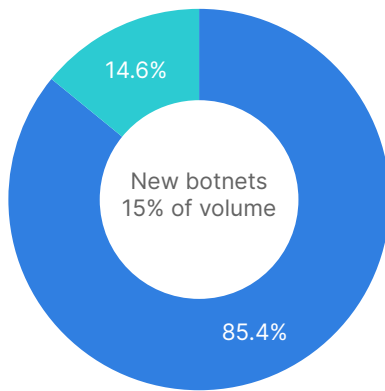
RATs Lazarus

O Grupo Lazarus é um grupo APT patrocinado pelo governo norte-coreano. Nesta nova campanha, Lazarus foi observado empregando malware RAT baseado em DLang na natureza. O acesso inicial de Lazarus começa com a exploração bem-sucedida do CVE-2021-44228, a infame vulnerabilidade Log4j descoberta em 2021.²²

Agente Tesla

O FortiGuard Labs capturou uma campanha de phishing que espalha uma nova variante do Agent Tesla.²³ Essa conhecida família de malware usa um RAT baseado em .Net e furtor de dados para obter acesso inicial explorando as vulnerabilidades do Microsoft Office CVE-2017-11882 e CVE-2018-0802.²⁴ , ²⁵ O módulo central do Agent Tesla pode coletar informações confidenciais do dispositivo da vítima, como credenciais salvas, informações de keylogging e capturas de tela do dispositivo.

Into the Red Zone



Old versus new bots

Novos bots no bloco: AndroxGh0st, Prometei e DarkGate

Uma vez infectados com malware, os sistemas muitas vezes tentam se comunicar com hosts remotos para baixar cargas úteis adicionais, estabelecer canais de comando e controle (C2) e abrir backdoors no ambiente. Isso torna a análise do tráfego de botnets uma parte importante do monitoramento de todo o escopo da atividade maliciosa.

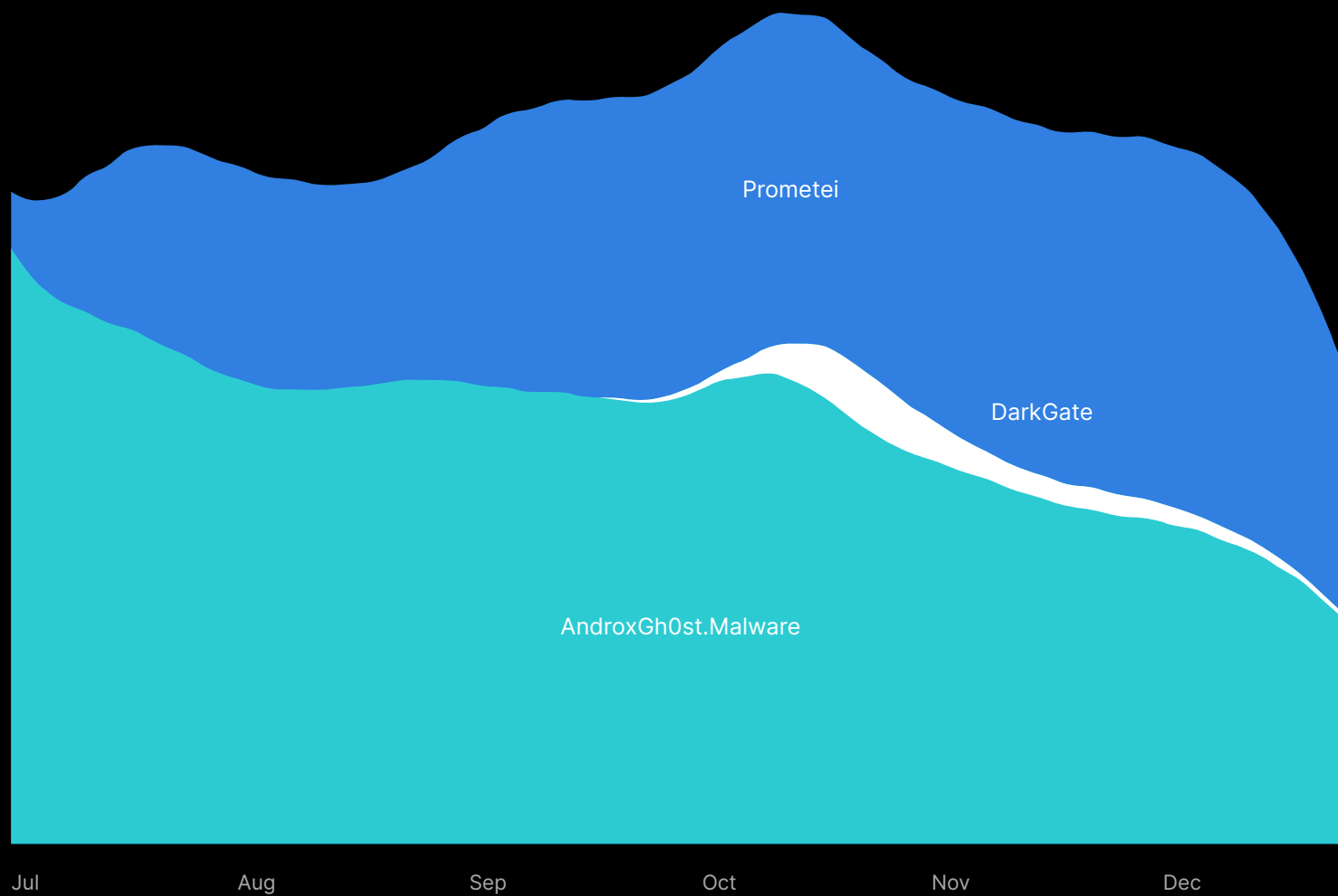
Um gráfico das botnets mais ativas é inevitavelmente preenchido com muitas das mesmas que vimos há anos, incluindo Gh0st, Mirai e ZeroAccess. Isso demonstra duas coisas:

- Os botnets são resilientes. Eles são criados para persistir e, apesar das derrubadas coordenadas das autoridades policiais, podem ser difíceis de matar.
- A remediação de botnets é um processo lento. Grande parte do tráfego de botnets que detectamos vem de sistemas infectados que tentam se comunicar com botnets que não estão mais ativos.

Dito isso, novas botnets surgem ocasionalmente que justificam a atenção. No segundo semestre de 2023, três novos botnets levaram holofotes: AndroxGh0st, Prometei e DarkGate.



Volume of traffic associated with new botnets emerging in 2H 2023



AndroxGh0st

A botnet AndroxGh0st está relacionada ao malware baseado em Python do mesmo nome. Ele tem como alvo principalmente arquivos do ambiente do usuário (.env), que muitas vezes contêm credenciais para uma variedade de aplicativos de alto nível. O AndroxGh0st inclui várias funções maliciosas para abusar de protocolos simples de transferência de e-mail (SMTP). Ele também verifica e explora credenciais e APIs expostas e implanta web shells para manter o acesso persistente aos sistemas.

Continuamos a observar a atividade generalizada do malware AndroxGh0st na natureza, explorando várias vulnerabilidades. Ele tem como alvo especificamente as vulnerabilidades PHPUnit (CVE-2017-9841), Laravel Framework (CVE-2018-15133) e Apache Web Server (CVE-2021-41773) para espalhar e realizar ataques de coleta de informações nas redes de destino.^{26, 27, 28} A Fortinet foi creditada por expor telemetria no AndroxGh0st, mostrando mais de 40.000 dispositivos infectados pela botnet.²⁹

Prometei

O Prometei é um malware que pode controlar remotamente máquinas infectadas. É capaz de se espalhar lateralmente pelas redes, roubar credenciais de senha, executar comandos arbitrários e baixar e executar componentes maliciosos adicionais. A Prometei também pode realizar mineração de criptomoedas e tem recursos de atualização automática.

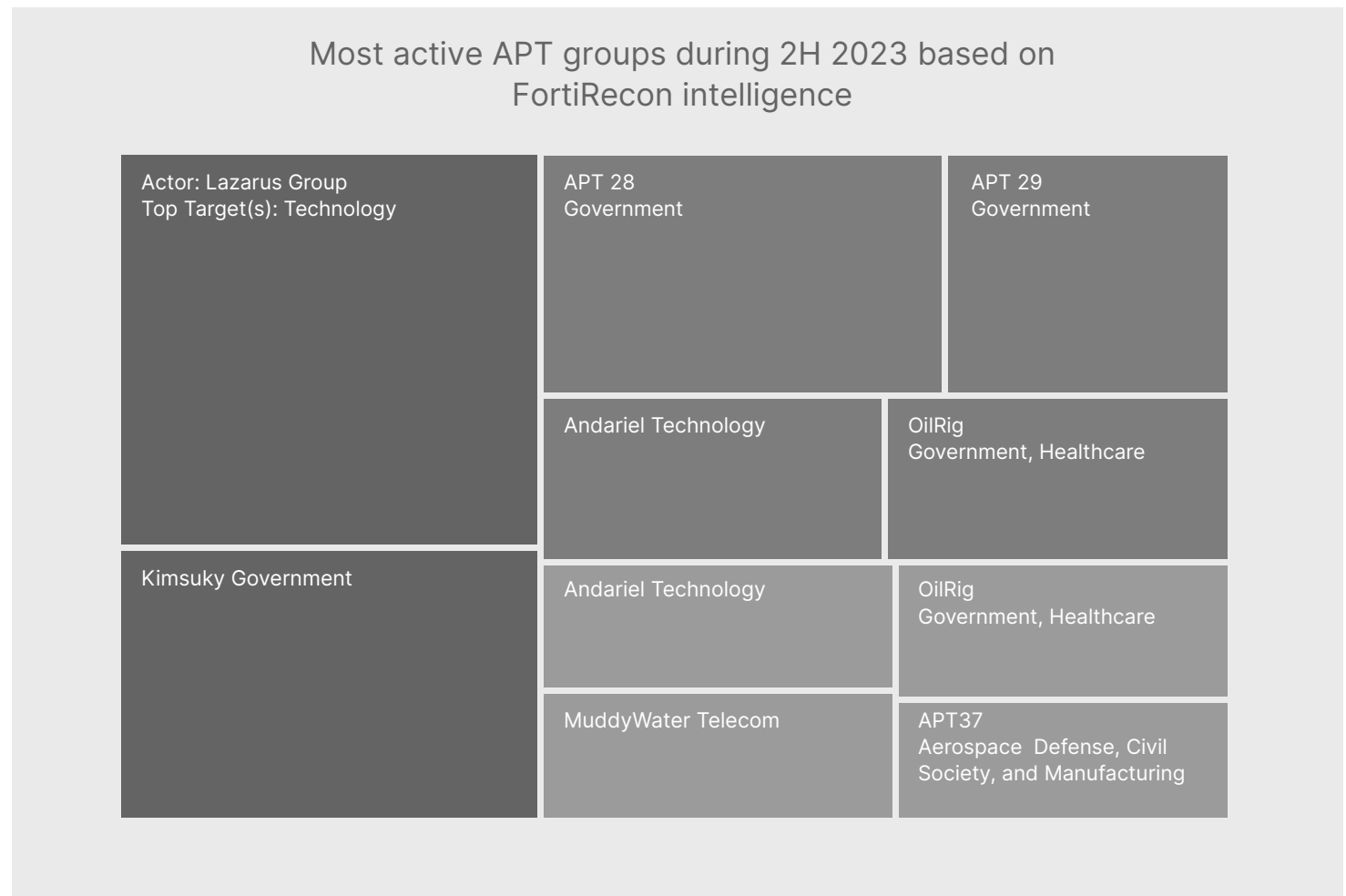
Essa cepa de malware foi recentemente reinventada e criamos novas assinaturas de IPS para ajudar na detecção.³⁰ Esse retrabalho funcionou bem, pois a botnet Prometei foi posteriormente catapultada para o sexto lugar em nossa lista para o volume total de tráfego em nossos sensores no 2H de 2023.

DarkGate

Embora seja um terço distante do AndroxGh0st e do Prometei, a botnet DarkGate justifica menção. O malware DarkGate, que tem uma variedade de recursos, desde acesso remoto até criptomineração e roubo de informações, foi relatado pela primeira vez em 2017. Desde então, seus criadores o usaram apenas para campanhas específicas. Mas em meados de 2023, o suposto autor se ofereceu para vendê-lo, e o malware logo começou a fazer rodadas mais amplas.³¹ Vimos a botnet DarkGate emergir após a derrubada do Qakbot como um possível sucessor.³² Ainda não se sabe se a DarkGate tem um futuro como uma ferramenta líder para cibercriminosos.

APTs mais ativos

No primeiro semestre do ano, observamos atividade significativa entre os grupos de APT, e esse volume se manteve estável durante o restante de 2023. Os grupos de APT continuam a ser altamente adaptáveis às mudanças no cenário digital e são cada vez mais furtivos à medida que planejam e executam ataques cuidadosamente. A imagem abaixo oferece uma visão dos grupos de APT mais ativos durante o segundo semestre do ano.



As descobertas mais recentes dos pesquisadores indicam uma mudança definitiva nas táticas do grupo norte-coreano de APT, Lazarus. No ano passado e meio, eles divulgaram três RATs diferentes construídas usando tecnologias incomuns durante o desenvolvimento, como QtFramework, PowerBasic e DLang. Isso indica que o Lazarus Group é uma organização madura e capaz, geralmente usando explorações de N-Day e técnicas conhecidas para violar empresas no setor de tecnologia, como trocas de blockchain e empresas de desenvolvimento de software. Os ataques do grupo têm sido bastante lucrativos, superando US\$ 100 milhões apenas em roubos de criptomoedas.

Outro grupo que esteve ativo nos últimos meses de 2023 foi o APT 28, usando vulnerabilidades N-Day no Outlook e no Winrar para roubar credenciais do New Technology Lan Manager (NTLM), concentrando-se em violar organizações governamentais, bem como empresas nos setores de ensino superior, manufatura e aeroespacial. O grupo visou organizações no Leste Europeu, com várias campanhas destinadas a interromper as operações e roubar informações dessas empresas. Esse mesmo grupo também usou dias zero anteriormente não divulgados este ano para realizar espionagem cibernética e roubar dados. O APT 28 também deixou de usar backdoors e comprometer dispositivos periféricos na rede e agora está usando serviços legítimos, como Google Drive e Microsoft OneDrive, para exfiltrar dados confidenciais.

Penetrando na zona vermelha

Priorizar vulnerabilidades para remediação é mais importante do que nunca, uma vez que a taxa de descoberta e divulgação continua a acelerar. Até a publicação deste relatório, há mais de 222.000 vulnerabilidades na lista de Vulnerabilidades e Exposições Comuns (Common Vulnerabilities and Exposures, CVE).³³ Vimos um novo recorde em 2023, com um total de 30.000 novas vulnerabilidades publicadas, um salto de 17% em relação ao ano anterior.

Em 2022, introduzimos o conceito de “zona vermelha”, que ajuda os leitores a entender melhor a probabilidade (ou improvável) de os agentes de ameaças explorarem uma vulnerabilidade específica.³⁴ Isso permite que as equipes de segurança se concentrem nas vulnerabilidades que apresentam maior risco, priorizando os esforços de remediação.

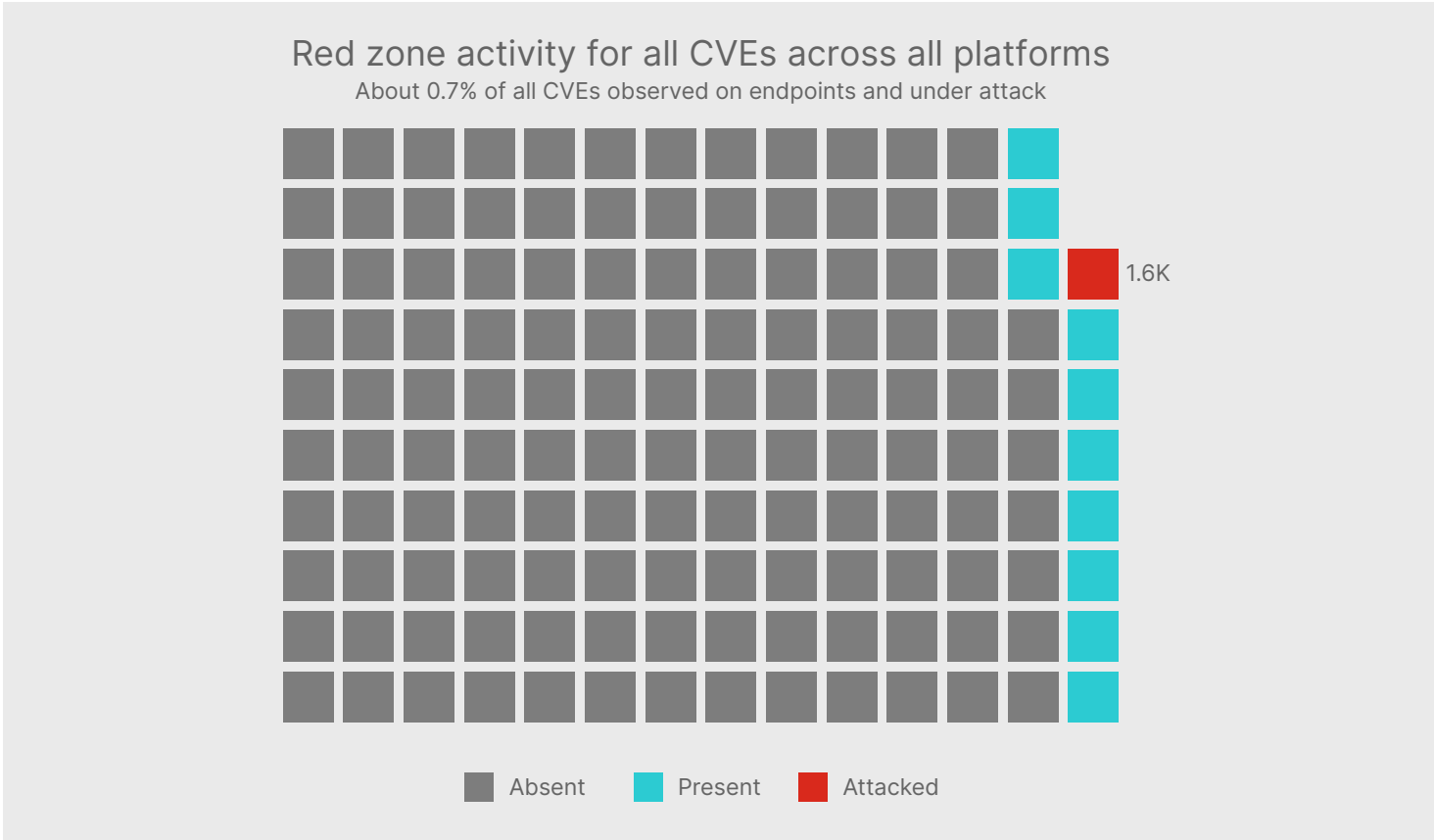
Felizmente, nossos dados mostram que um pequeno subconjunto (12,5%) de todos os CVEs históricos estão presentes e não corrigidos em endpoints em ambientes ao vivo. Isso é representado na proporção de quadrados azul versus cinza no gráfico adjacente.

Além disso, apenas uma fração (< 1%) de todas as vulnerabilidades foi explorada no segundo 2H de 2023. Essa proporção permaneceu notavelmente estável ao longo do tempo, o que é uma boa notícia para as equipes de segurança.

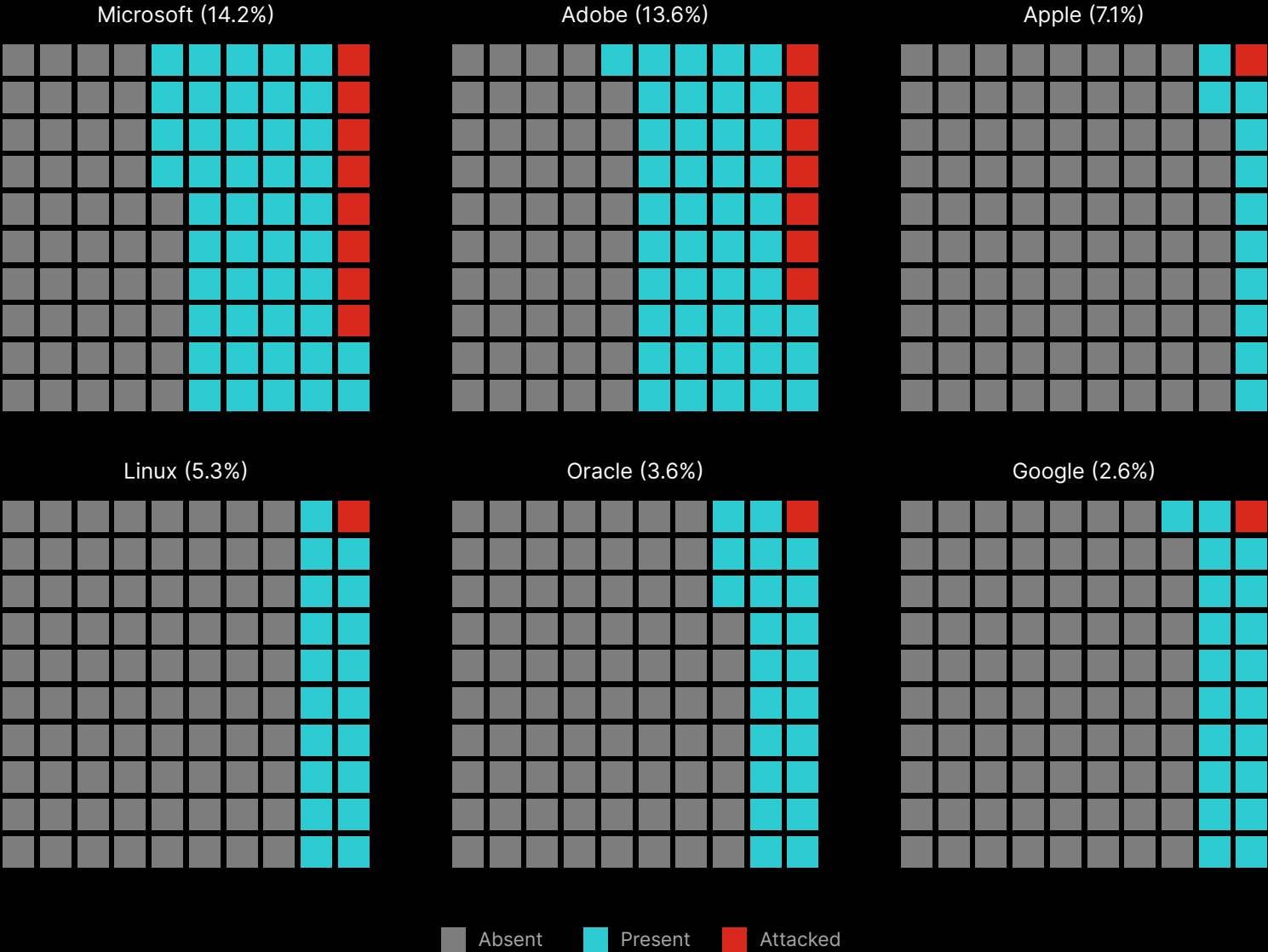
30K

novas vulnerabilidades em todos os setores foram publicadas em 2023, marcando um aumento de 17% em relação ao ano anterior.

Claro, a zona vermelha para muitas plataformas de software proeminentes é substancialmente maior. Por exemplo, a superfície de ataque da Microsoft é 20 vezes maior do que a média geral (14%) e o dobro da Apple (7%) e Linux (5%). Na prática, quanto maior a zona vermelha, mais esforço e correção automatizada são necessários para remediação oportuna de vulnerabilidades de alto risco com explorações ativas.

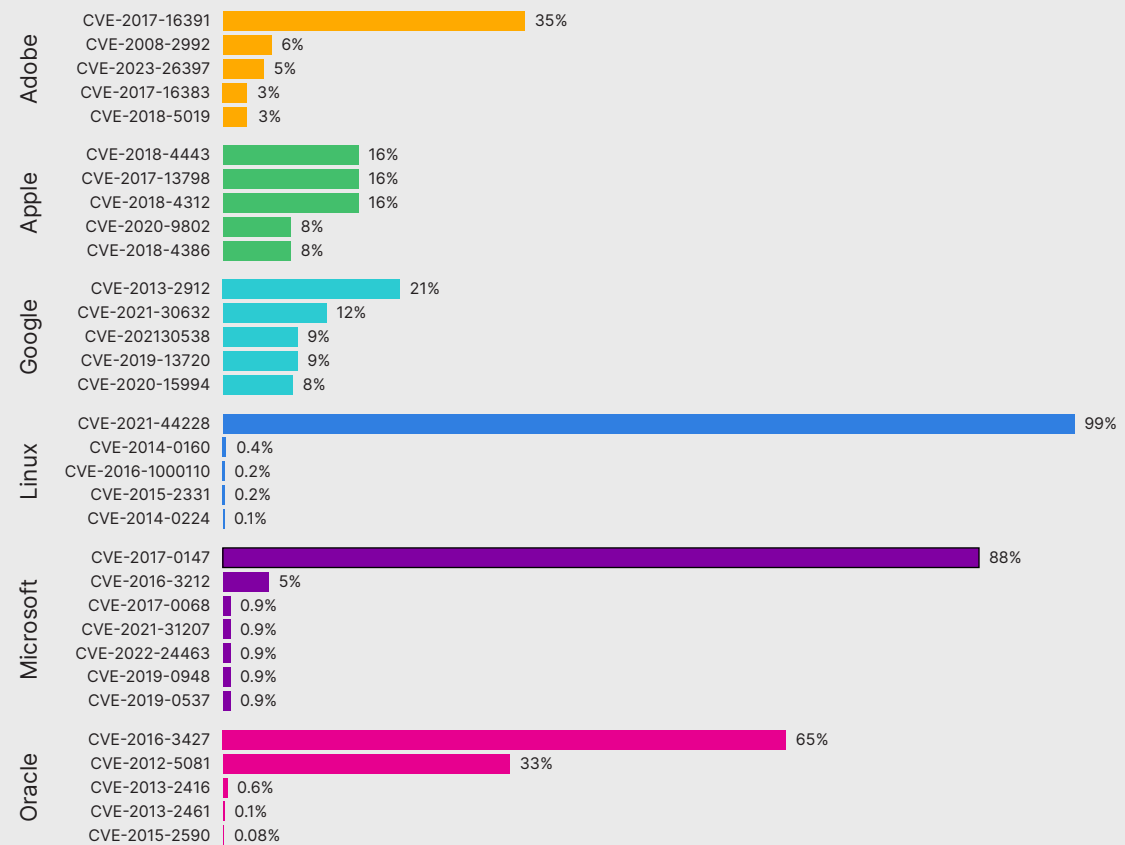


Red zone activity for CVEs affecting prominent platforms



Aqui está uma visão das cinco principais vulnerabilidades que compõem a zona vermelha de cada plataforma com base na prevalência de tentativas de exploração detectadas:

CVEs with the highest exploit activity for each prominent software platform



A participação da atividade da zona vermelha nas vulnerabilidades difere drasticamente entre as plataformas. Um total de 99% da zona vermelha do Linux é dominado por explorações direcionadas ao CVE-2021-44228.³⁵ Compare isso com a Apple, onde as três principais vulnerabilidades respondem por aproximadamente 16% da atividade de exploração.

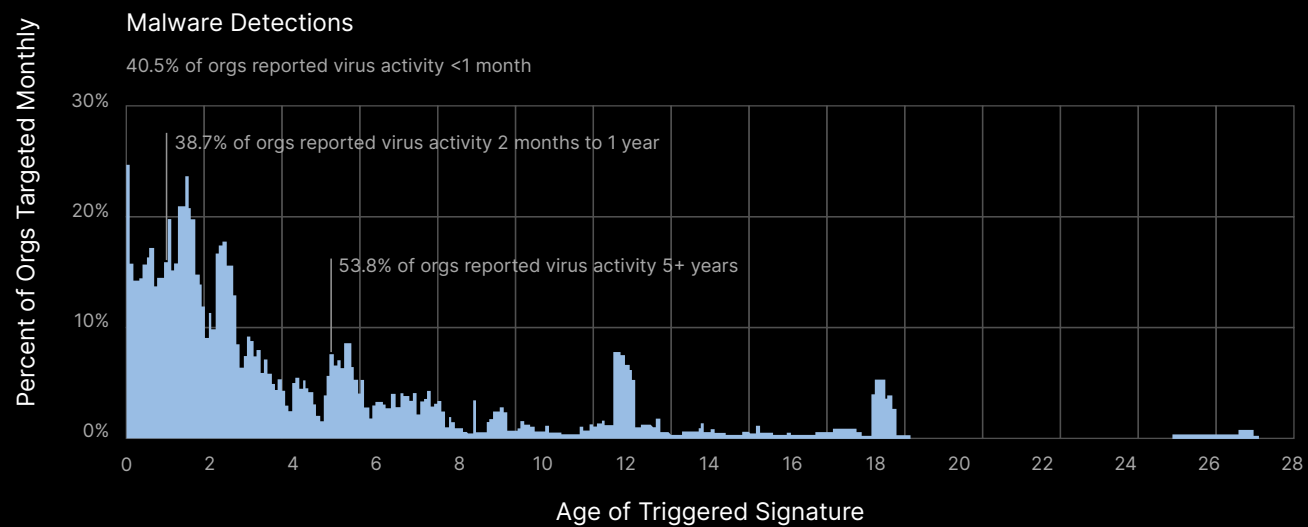
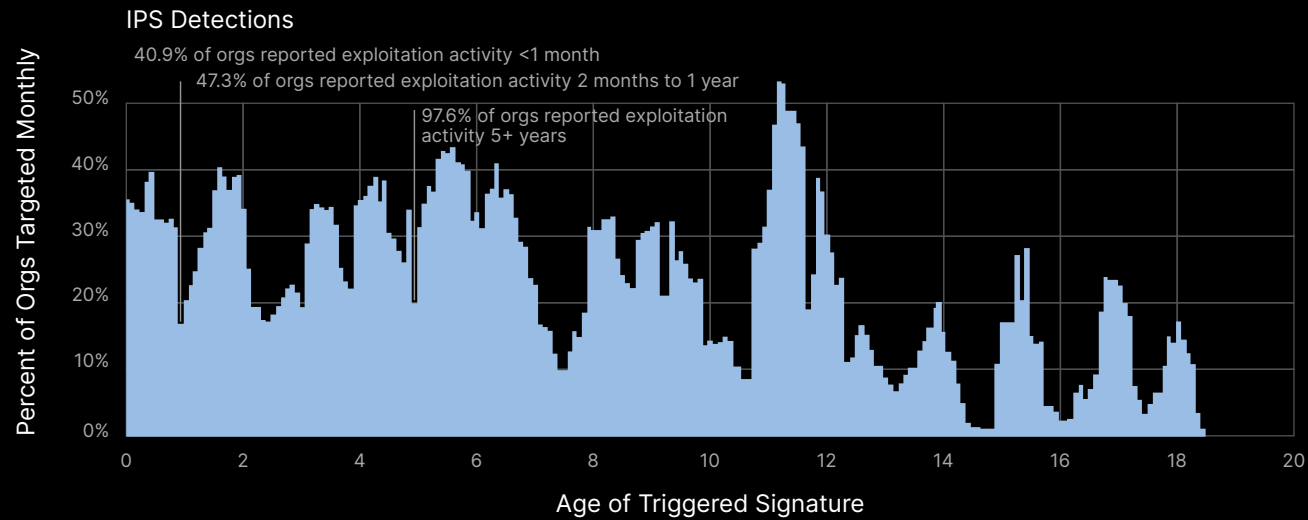
A maioria dessas vulnerabilidades da zona vermelha não é nova. Apenas dois foram publicados em 2023, e apenas um deles surgiu no segundo semestre do ano (CVE-2023-44487).³⁶ O restante abrange a última década. E lembre-se de que as vulnerabilidades “antigas” de exploração não estão desacelerando — a principal vulnerabilidade para metade das plataformas listadas foi descoberta pelo menos cinco anos antes.

Da previsão de exploração ao surto

Como discutimos anteriormente, quando se trata de vulnerabilidades, o que é antigo ainda é novo aos olhos de muitos invasores. Para entender a prevalência dessa tendência, identificamos todas as explorações de vulnerabilidade e amostras de malware que ocorreram no 2H de 2023, juntamente com a proporção de organizações que registram detecções. Em seguida, mapeamos essas assinaturas de acordo com quando elas foram criadas e adicionadas aos dispositivos Fortinet. Os gráficos na próxima página medem a vida útil ativa das ameaças de exploração e malware.



Age and prevalence of exploits and malware detected in 2H 2023

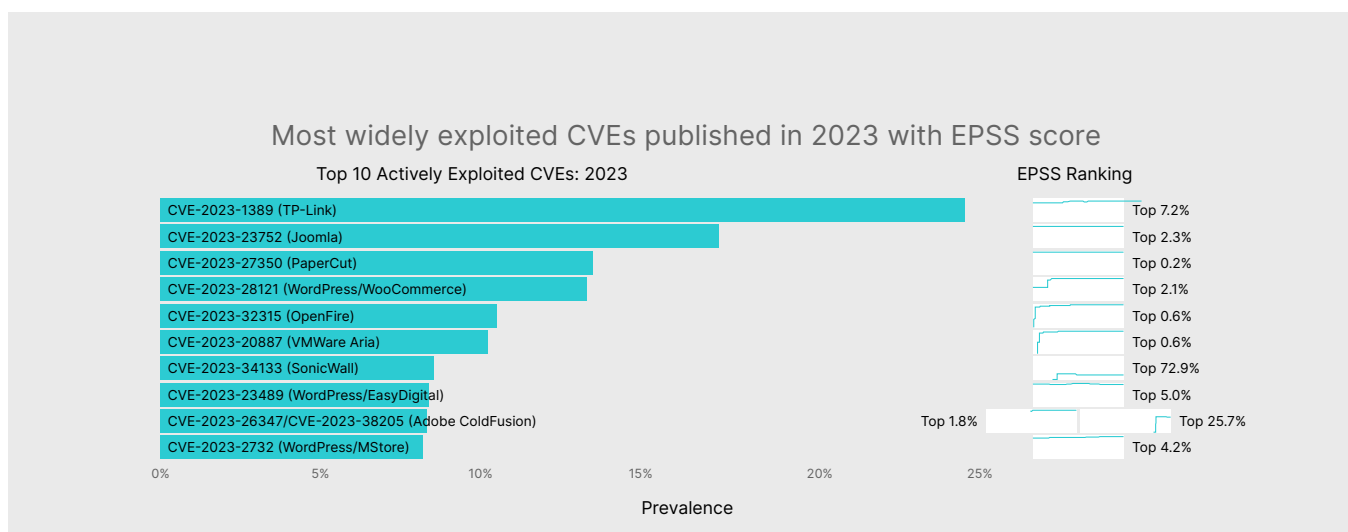


Continuamos a observar agentes de ameaças explorando vulnerabilidades com mais de 15 anos. Quase todas as organizações (98%) detectaram explorações que existem há pelo menos cinco anos. No entanto, há muito espaço para novas ameaças entrarem em cena: 41% das organizações também detectaram explorações de assinaturas com menos de um mês de idade. Mas quando se trata de malware, pouco mais da metade das organizações detectou variantes que existem há cinco anos ou mais, muito menos do que vemos para explorações.

Essa análise produz algumas percepções críticas sobre o cenário de ameaças cibernéticas. Explorações e malware têm velocidades e escopos muito semelhantes relacionados à sua disseminação, mas a longevidade de cada um difere. As variantes de malware morrem mais rapidamente à medida que o novo código substitui o antigo. As explorações mostram uma vida útil muito mais ativa porque as vulnerabilidades que os cibercriminosos visam podem permanecer sem correção por anos.

Praticamente falando, isso reforça a importância de permanecer vigilante sobre a higiene da segurança, pois os invasores provavelmente não pararão de explorar vulnerabilidades mais antigas. Também é um ótimo lembrete para que os profissionais de segurança ajam rapidamente por meio de um programa consistente de correção e atualização quando surgem novas vulnerabilidades que provavelmente serão exploradas.

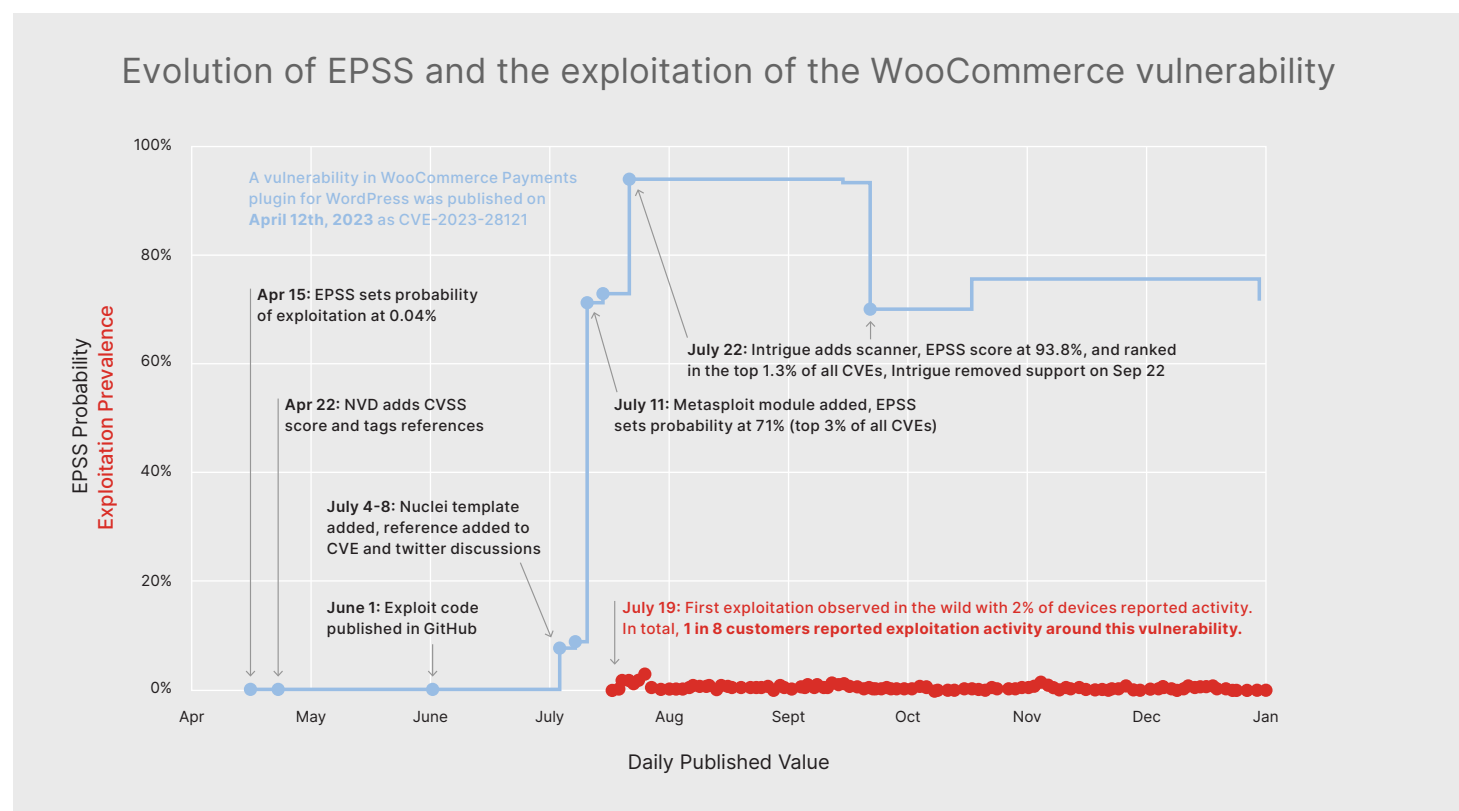
Como você pode rastrear vulnerabilidades emergentes que são mais propensas a serem atacadas? O Sistema de pontuação de previsão de exploração (Exploit Prediction Scoring System, EPSS) existe para esse propósito exato.³⁷ A Fortinet é um dos principais contribuintes para os dados de exploração que impulsionam o EPSS. O gráfico abaixo mostra as vulnerabilidades lançadas em 2023 que foram mais visadas pela atividade de exploração no último semestre do ano.



98%

das organizações detectaram
explorações que existem há
pelo menos cinco anos.

Vamos dar uma olhada mais de perto em como o EPSS é preciso na identificação de vulnerabilidades que provavelmente serão exploradas. O gráfico abaixo destaca a pontuação EPSS para a vulnerabilidade que afeta o plug-in WooCommerce Payments para WordPress (CVE-2023-28121).³⁸ Esta CVE foi publicada em 12 de abril de 2023 e inicialmente avaliada pelo EPSS como tendo uma baixa probabilidade de exploração. Essa avaliação foi revisada drasticamente após o lançamento de um modelo de núcleo e módulo Metasploit no início de julho. Dadas essas mudanças, a vulnerabilidade subiu para os 3% principais das pontuações do EPSS com uma chance de exploração de 71% em nos próximos 30 dias.



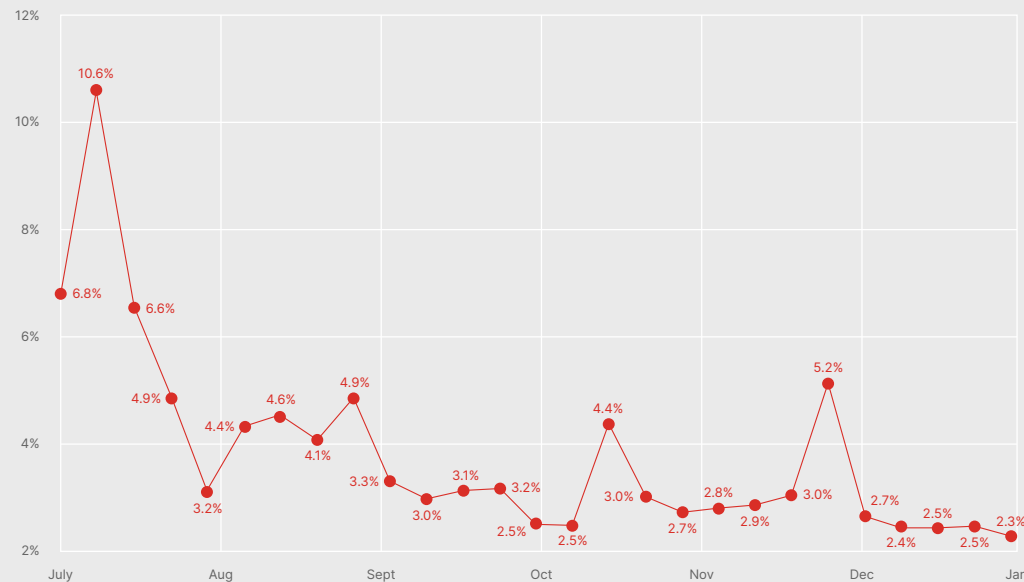
Logo após essa revisão do EPSS, nossa equipe observou os primeiros sinais de exploração na natureza em 19 de julho. Nesse caso, o EPSS forneceu um sistema de alerta precoce eficaz antes do surto de ataques, dando aos defensores uma vantagem valiosa na remediação.

Com o tempo de exploração diminuindo significativamente em 43% para apenas 4,76 dias, a pressão sobre os recursos de defesa cibernética já estendidos se intensificou. A capacidade de analisar rapidamente uma lista priorizada de vulnerabilidades, gerenciando efetivamente essas “bombas-relógio de marcação”, agora é mais crítica do que nunca. Integrar essa priorização ao seu processo de gerenciamento de correções equipa você com uma estratégia clara e sensível ao tempo para mitigação de riscos, aprimorando sua postura de segurança cibernética em um cenário de ameaças em rápida evolução.

Os ataques de ransomware têm como alvo cada vez mais os setores críticos

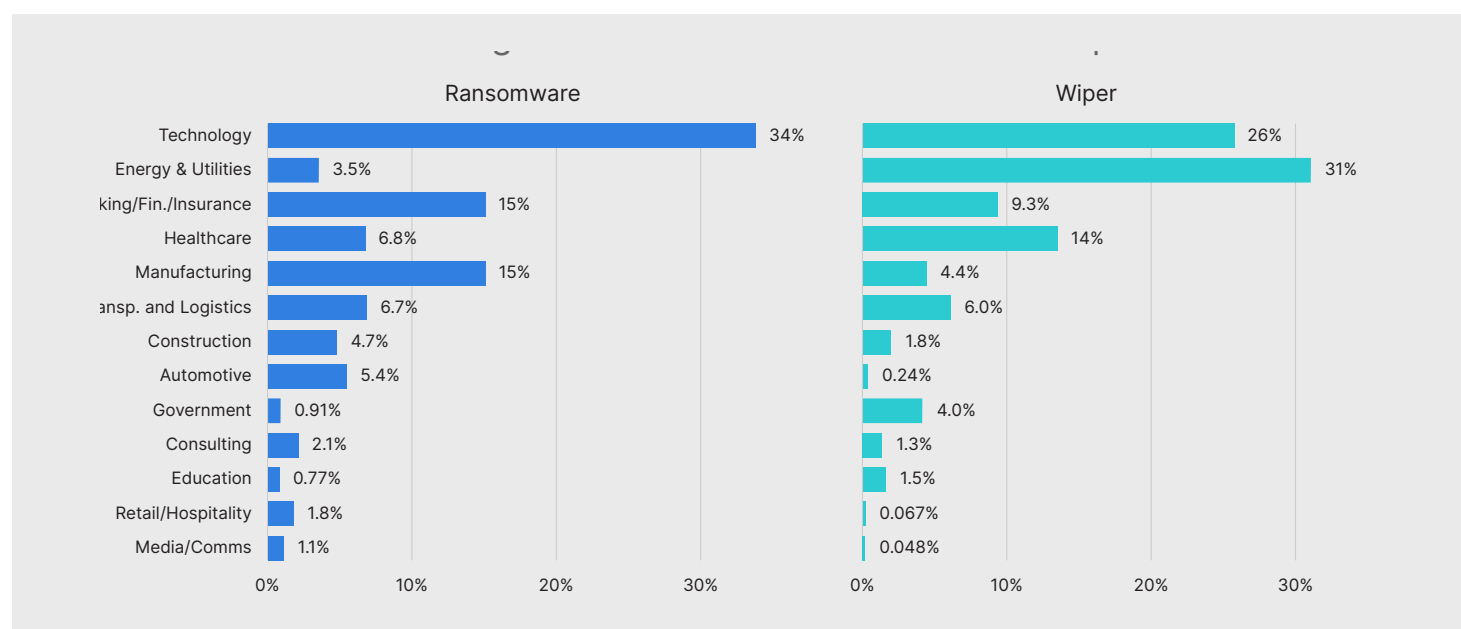
O ransomware continua a manter as equipes de segurança à noite. De acordo com uma pesquisa recente da Fortinet, mais de 80% dos líderes estão “muito” ou “extremamente” preocupados com ransomware.³⁹ Em nossos sensores, as detecções de ransomware aumentaram 13 vezes mais no primeiro semestre de 2023. Isso foi seguido por uma queda de 70% durante o último semestre do ano, durante o qual também vimos menos organizações detectando variantes de ransomware.

Weekly prevalence of ransomware detections over 2H 2023



Muitos desses altos e baixos podem ser rastreados até a dinâmica das gangues de ransomware. Alguns seguem uma estratégia de alto volume e baixa margem, o que resulta em um número maior de variantes e vítimas de ransomware. Outras gangues focam em menos organizações que podem pagar resgates maiores usando ataques altamente direcionados.

Em nosso relatório de previsões de ameaças de 2024, prevemos que os adversários que procuram pagamentos maiores chamariam sua atenção para setores críticos, como saúde, serviços públicos, fabricação e finanças. Como previsto, no 2H de 2023, testemunhamos uma mudança da estratégia tradicional de “spray and pray”, com cibercriminosos adotando uma abordagem mais direcionada combinada com o aumento das demandas de resgate.⁴⁰



O gráfico acima fornece um detalhamento do setor de todas as amostras de ransomware e limpador coletadas por nossos sensores no final de 2023. A presença significativa de setores como energia, saúde, fabricação, transporte e logística e automotivo oferece algumas evidências de nossa previsão tomando forma. No total, os setores industriais experimentaram 44% de todas as detecções de ransomware e limpador para o 2H de 2023. Essa tendência é preocupante por muitos motivos, especialmente porque violações críticas do setor podem ter um impacto considerável e adverso na sociedade.

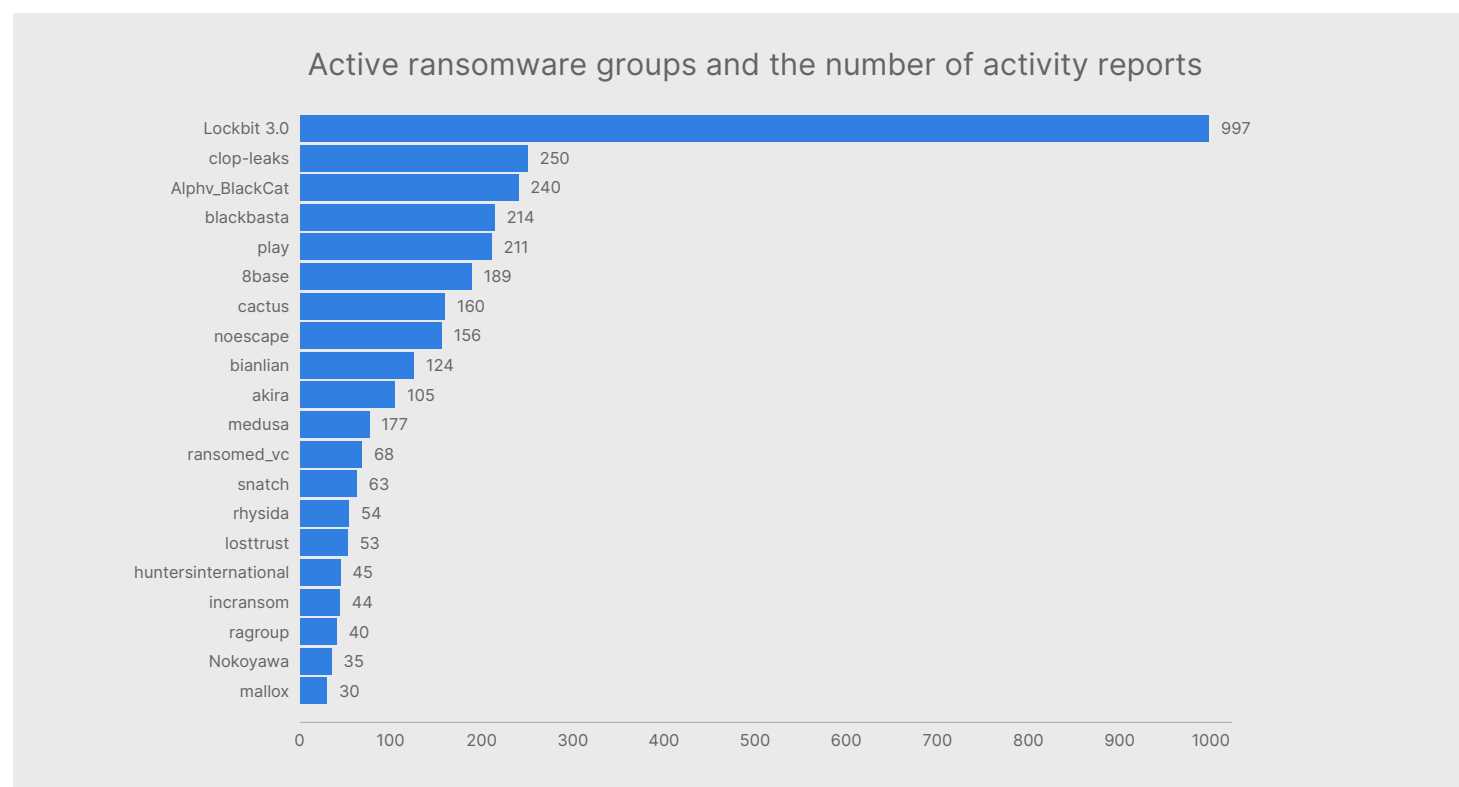
44%

das organizações industriais sofreram quase metade de todas as detecções de ransomware e limpadores no segundo semestre de 2023.

Grupos de ransomware

No último semestre do ano, os agentes de ameaças anunciaram 23 novas cepas de malware, oito cepas de malware para dispositivos móveis, 15 ofertas de malware como serviço (MaaS) e seis novos programas de ransomware como serviço (RaaS).

Um exemplo notável de um novo grupo de ransomware que surgiu no final de 2023 é o Ransomed.VC, que inicialmente serviu como um fórum, mas foi posteriormente transformado em um site de vazamento de dados focado em ransomware. As ações do grupo Ransomed.VC servem como um testemunho das táticas dinâmicas empregadas pelos grupos de ransomware atuais. Seu envolvimento em assuntos geopolíticos, alianças com outros grupos, participação em violações de dados e promoção de serviços DDoS rapidamente os estabeleceram como um grande participante no domínio em constante mudança do crime cibernético.



O grupo hacktivista GhostSec também anunciou um novo ransomware chamado GhostLocker na dark web. Este anúncio significa a expansão do grupo no domínio de fornecer serviços de ransomware, destacando a natureza em constante evolução do cenário de ameaças e o surgimento de novas ferramentas dentro da comunidade de crimes cibernéticos. Os membros do GhostSec usam principalmente o Telegram e o X para compartilhar suas listas de alvos e resultados de ataques, o que demonstra como o monitoramento da dark web pode servir como um sistema de alerta precoce para novas iniciativas de crime cibernético.

Quanto ao fórum de crime cibernético em russo conhecido como XSS, um agente de ameaças que usa o pseudônimo “malwareguy” promoveu ativamente uma ferramenta de criação projetada para o ransomware do Caos versão 4.0. A presença dessas ofertas em fóruns subterrâneos é outro exemplo das ameaças em andamento e em evolução apresentadas pelos cibercriminosos, bem como a necessidade de monitorar a dark web para discussões que podem nos dar informações sobre possíveis vetores de ataque futuros. Esperamos que essa tendência se intensifique à medida que nos aprofundamos em 2024.

Mapa de calor global da ATT&CK

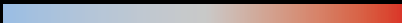
O MITRE ATT&CK é um repositório amplamente usado de táticas, técnicas e procedimentos (TTPs) do adversário.⁴¹ Ele oferece uma linguagem comum desenvolvida a partir de observações do mundo real que são usadas por organizações e equipes de segurança cibernética para construir modelos de ameaças e defesas informadas sobre ameaças. Muitas soluções Fortinet oferecem visibilidade dos ATT&CK, e apresentamos dois deles nesta seção.

A primeira fonte de descoberta de técnicas ATT&CK é por meio de nossas soluções de sandboxing. Milhões de sensores em todo o mundo coletam arquivos suspeitos que são enviados por meio de uma variedade de mecanismos antivírus, análise comportamental, análise estática e dinâmica, IA e ML e inteligência para identificar comportamentos sutis indicativos de sua ameaça subjacente. Os TTPs identificados por meio desse método são melhor interpretados como recursos possuídos por malware na natureza durante o segundo 2H de 2023.

A imagem na página a seguir mostra as técnicas mais prevalentes em cada tática. As percentagens correspondem à proporção de organizações que observaram malware com recursos correspondentes a cada TTP.

Top ATT&CK techniques observed via sandbox solutions

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media: 48%	Exploitation for Client Execution: 27%	Hijack Execution Flow: 33%	Process Injection: 34%	Obfuscated Files/Info: 20%	Input Capture: 43%	System info Discovery: 21%	Replication Through Removable Media: 60%	Data from Local System: 25%	Application Layer Protocol: 44%	Exfiltration Over Alternative Protocol: 96%	System Shutdown/ Reboot: 69%
Phishing: 31%	WMI: 22%	Boot/Logon Autostart Execution: 30%	Hijack Execution Flow: 22%	Masquerading: 15%	OS Credential Dumping: 37%	File and Directory Discovery: 15%	Taint Shared Content: 28%	Input Capture: 25%	Ingress Tool Transfer: 20%	Automated Exfiltration: 3%	Data Encrypted for Impact: 15%
Valid Accounts: 9%	Command and Scripting Interpreter: 19%	Create/Modify System Process: 15%	Boot/Logon Autostart Execution: 20%	Virtualiz./ Sandbox Evasion: 15%	Unsecured Credentials: 15%	Virtualiz./ Sandbox Evasion: 11%	Use Alternate Authentication Material: 4%	Email Collection: 17%	Non-Application Layer Protocol: 18%	Exfiltration Over C2 Channel: 0.4%	Inhibit System Recovery: 5%
Drive-by Compromise: 8%	Shared Modules: 14%	Scheduled Task/Job: 14%	Create/Modify System Process: 10%	Impair Defenses: 11%	Steal Web Session Cookie: 3%	Process Discovery: 11%	Software Deployment Tools: 3%	Automated Collection: 13%	Encrypted Channel: 11%		Service Stop: 4%
Exploit Public-Facing Application: 3%	Scheduled Task/Job: 8%	Office Application Startup: 5%	Scheduled Task/Job: 9%	Process Injection: 10%	Credentials from Password Stores: 0.8%	Software Discovery: 11%	Remote Services: 3%	Browser Session Hijacking: 6%	Non-Standard Port: 6%		Data Destruction: 3%
	Native API: 5%	Event Triggered Execution: 1.0%	Access Token Manipulation: 4%	Hijack Execution Flow: 7%	Network Sniffing: 0.2%	Query Registry: 8%	Exploitation of Remote Services: 0.7%	Clipboard Data: 6%	Proxy: 0.8%		Resource Hijacking: 1%
	System Services: 3%	Browser Extensions: 0.6%	Event Triggered Execution: 1.0%	Modify Registry: 5%	Forge Web Credentials: 0.004%	Remote System Discovery: 8%	Lateral Tool Transfer: 0.7%	Archive Collected Data: 3%	Web Service: 0.5%		Endpoint Denial of Service: 1%
	Inter-Process Comm.: 0.8%	Valid Accounts: 0.3%	Abuse Elevation Control Mechanism: 0.3%	Hide Artifacts: 5%		Application Window Discovery: 6%		Video Capture: 2%	Data Encoding: 0.07%		Data Manipulation: 0.6%
	User Execution: 0.2%	Pre-OS Boot: 0.3%	Valid Accounts: 0.2%	Indicator Removal on Host: 3%		System Network Configuration Discovery: 6%		Screen Capture: 2%	Remote Access Software: 0.05%		Defacement: 0.4%
	Software Deployment Tools: 0.06%	Boot/Logon Initialization Scripts: 0.2%	Boot/Logon Initialization Scripts: 0.1%	Deobfuscate/ Decode Files/Info: 3%		Network Service Discovery: 1%		Data from Info Repositories: 0.5%	Data Obfuscation: 0.04%		Firmware Corruption: 0.2%

Falling  Rising

Compartilhamos esse mesmo gráfico em nosso Relatório do cenário de ameaças do primeiro 1H de 2023 e queríamos destacar as mudanças no período atual.⁴² Nós colocamos o sombreado em camadas no topo para representar se a classificação de cada técnica permaneceu consistente (cinza), aumentada (vermelha) ou reduzida (azul). Curiosamente, o gráfico revela consistência notável entre os TTPs. Observamos que algumas das técnicas que deslizam pelos gráficos estão relacionadas à manipulação, adulteração ou ofuscação de informações.

Como o gráfico mostra, a maioria das táticas tinha técnicas que mostravam aumento da atividade, com a maior mudança vindo de “Impacto” com “Destruição de dados” aumentando drasticamente. Outra técnica que merece atenção é “Contas válidas”, subindo de sexta posição na lista para a terceira posição. Isso se refere aos adversários que usam credenciais comprometidas, muitas vezes compradas na dark web, para ignorar controles de acesso, criar acesso persistente a sistemas remotos e serviços disponíveis externamente, escalar privilégios e escapar da detecção.

Também vemos algumas oscilações entre as posições em “Acesso a credenciais”, mas nada que constitua uma mudança marítima. As técnicas restantes que escalam os gráficos são “Modificar registro” para evitar a detecção, o que é esperado devido ao aumento de seu pré-requisito típico, “Contas válidas”, e o uso de “Ferramentas de implantação de software” para se mover lateralmente. Em algumas campanhas de alto nível, vimos os invasores usarem software de segurança presente nos ambientes das vítimas para seu próprio benefício.

A segunda fonte de observações de TTP vem por meio dos sensores de nuvem FortiNDR (detecção e resposta de rede). Como essas soluções operam em diferentes camadas da pilha, você esperaria que a visibilidade das TTPs fosse diferente.

Top ATT&CK techniques observed via FortiNDR

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application: 44%	Command and Scripting Interpreter: 98%	Valid Accounts: 65%	Valid Accounts: 68%	Valid Accounts: 83%	Forced Authentication: 49%	Network Service Discovery: 44%	Remote Services: 54%	Adversary in the Middle: 100%	Application Layer Protocol: 52%	Exfiltration Over C2 Channel: 51%	Resource Hijacking: 100%
System Network Configuration Discovery: 0.2%	WMI: 1%	Scheduled Task/Job: 13%	Scheduled Task/Job: 13%	Indicator Removal on Host: 11%	OS Credential Dumping: 31%	Account Discovery: 27%	Lateral Tool Transfer: 46%		Proxy: 30%	Exfiltration Over Alternative Protocol: 44%	
System Network Configuration Discovery: 0.2%	System Network Configuration Discovery: 0.2%	Boot/Logon Autostart Execution: 12%	Boot/Logon Autostart Execution: 12%	Obfuscated Files/Info: 3%	Steal/Forge Kerberos Tickets: 11%	File and Directory Discovery: 14%			Ingress Tool Transfer: 10%	Exfiltration Over Web Service: 5%	
System Network Configuration Discovery: 0.2%	Exploitation for Client Execution: 0.08%	Create/Modify System Process: 6%	Create/Modify System Process: 6%	Subvert Trust Controls: 3%	Brute Force: 4%	Permission Groups Discovery: 8%			Remote Access Software: 7%		
System Network Configuration Discovery: 0.2%	User Execution: 0.07%	External Remote Services: 4%		Execution Guardrails: 0.3%	Adversary in the Middle: 4%	Network Share Discovery: 5%			Non-Application Layer Protocol: 0.8%		
	System Services: 0.001%	Server Software Component: 0.4%		Deobfuscate /Decode Files/Info: 0.03%		System Network Connections Discovery: 0.7%			Non-Standard Port: 0.4%		
				Rogue Domain Controller: 0.03%		System Info Discovery: 0.6%			Encrypted Channel: 0.007%		
						System Owner/User Discovery: 0.4%			Web Service: 0.005%		
						Remote System Discovery: 0.3%					
						System Network Configuration Discovery: 0.2%					

As diferenças entre os TTPs observados pelos sandboxes e a tecnologia NDR não significam que um seja melhor ou pior do que o outro. Qualquer fonte que relate as técnicas “principais” da ATT&CK depende inerentemente da lente pela qual está sendo vista. O fato de “verem” ameaças de forma diferente é um argumento convincente para o motivo pelo qual as equipes de segurança precisam de várias camadas de detecção para obter uma compreensão abrangente do risco de sua organização.

Aqui estão alguns destaques adicionais a serem considerados específicos para as observações de TTP fornecidas pelo FortiNDR Cloud:

- **TécnicasC2:** Detectamos várias técnicas na fase C2 da estrutura MITRE ATT&CK , incluindo, entre outras, solicitações de DNS do Cobalt Strike, tunelamento de DNS e consultas de DNS longo. Os invasores estão cada vez mais usando serviços legítimos para C2 e, em alguns casos, já estamos começando a ver o blockchain usado para comunicações, pois isso é resistente à derrubada. O Glupteba foi o grupo que vimos mais recentemente usando essa técnica.
- **Detecções de malware:** RATs como Lokibot e IcedID Banking Trojan continuam a apresentar tendências na atividade de detecção. Loki é uma ferramenta de acesso remoto de código aberto com recursos como transferência de arquivos por HTTP ou SFTP, inicialização de um navegador local, captura de tela, execução de um keylogger e muito mais. O Loki é frequentemente usado como uma ferramenta pós-exploração para atividade de equipe vermelha ou atividade maliciosa. O FortiGuard ATR considera o Loki de alta gravidade devido ao seu uso comum para movimento lateral após um comprometimento de um único host. O Cavalo de Troia bancário IcedID se conecta às sessões de navegador dos usuários e pode fazer capturas de tela para roubar credenciais para instituições financeiras. O IcedID também é usado para facilitar ofertas de acesso como serviço em que o acesso a redes comprometidas é vendido para agentes maliciosos adicionais. O FortiGuard ATR considera o IcedID de alta gravidade devido ao nível de acesso que concede a agentes maliciosos ao ambiente e às informações.
- **Evasão de defesa:** Observe que a técnica de “Contas válidas” listada na fase de “Evasão de defesa” da estrutura MITRE ATT&CK ainda é relevante para possíveis atividades de ameaças às quais as organizações podem querer prestar atenção. Como relatamos de outras fontes, como FSA e Recon, essa técnica parece ser abusada por agentes de ameaças, principalmente alimentada por corretores de acesso inicial na dark web.

- **Execução:** Detectamos arquivos conhecidos de execução portátil (PE) maliciosos vistos na rede. Um arquivo PE é um formato de arquivo especializado projetado para armazenar código executável, código de objeto, bibliotecas de link dinâmico (DLLs) e recursos semelhantes para uso em sistemas operacionais Windows. Quando um arquivo PE se torna malicioso, isso significa que um código prejudicial ou malicioso foi incorporado a ele, potencialmente comprometendo a segurança e a integridade de qualquer sistema onde o arquivo é executado.
- **Descoberta:** Várias enumerações suspeitas do Active Directory (AD) e LDAP (listas de usuários, grupos e confianças de domínio) foram detectadas pelo FortiNDR Cloud. Os agentes de ameaças podem usar LDAP e DCE/RPC para enumerar todos os grupos, administradores, usuários, computadores, controladores de domínio e confianças de domínio dentro de um domínio. Depois de comprometer uma rede, os adversários podem consultar o AD para obter uma melhor compreensão do layout e dos ativos de uma organização.

Lançando luz na atividade da Dark Web

Embora grande parte da nossa telemetria nos mostre quais ações os invasores tomaram no passado, a inteligência da darknet pode nos ajudar a prever o que os adversários podem fazer em seguida. Pela primeira vez em nossos relatórios de cenário de ameaças, estamos compartilhando percepções que coletamos de fóruns da dark web, mercados, canais de telegrama e outras fontes durante o segundo semestre de 2023 que nos dão uma ideia das ameaças emergentes com base na conversa que ocorre entre os agentes de ameaças. Usando essa inteligência, os profissionais de segurança podem se proteger com mais eficácia contra técnicas e táticas de ataque novas e emergentes.

Veja algumas das descobertas mais prevalentes

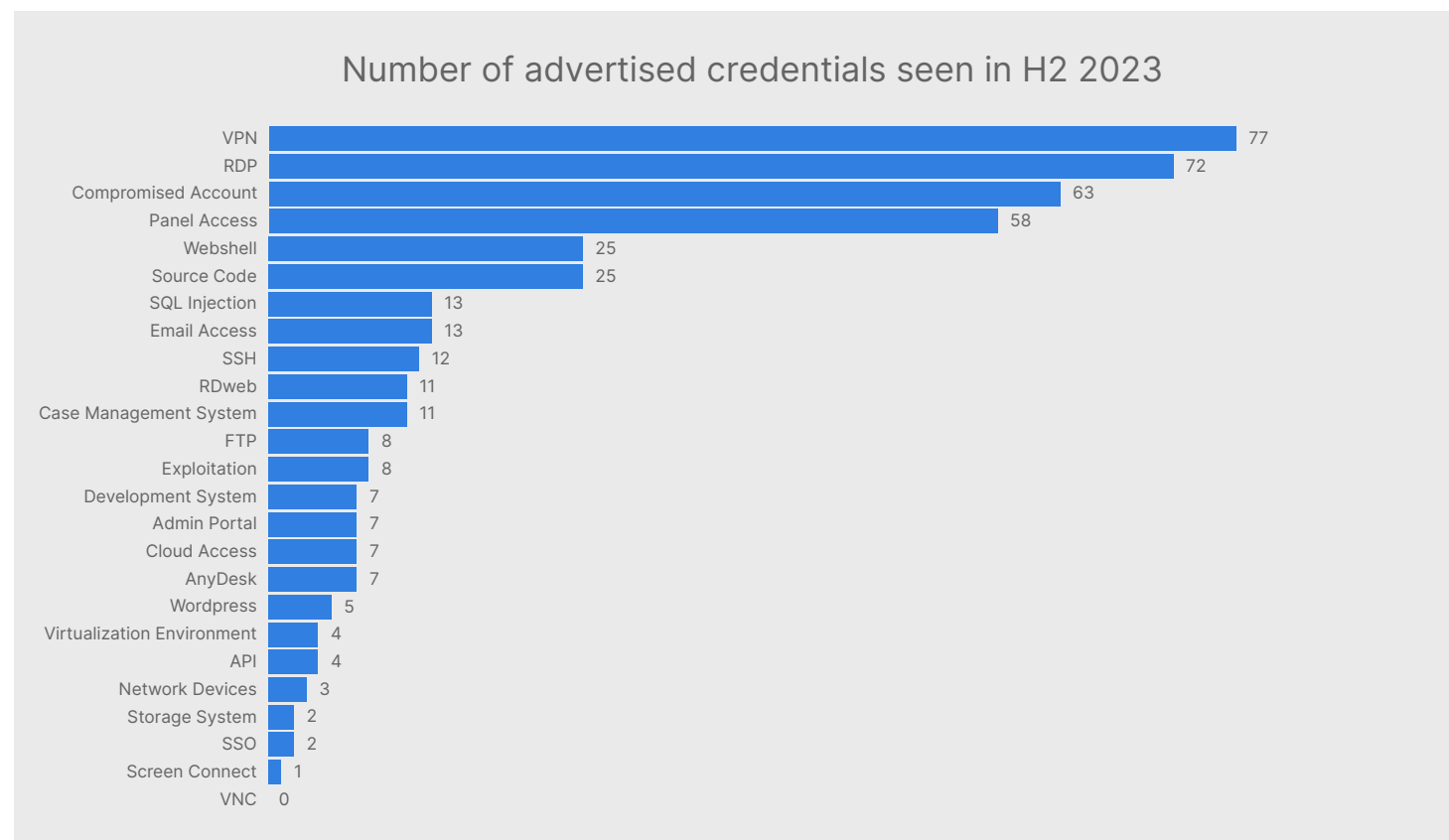
- Os agentes de ameaças discutiram com mais frequência o direcionamento a organizações dentro do setor de serviços financeiros, seguido pelos setores de serviços de negócios e educação.
- Os agentes de ameaças mais ativos publicamente em toda a dark web foram Valerka, Punktir, CoreLab, XXXX e qwer.
- Mais de 3.000 violações de dados foram compartilhadas em fóruns proeminentes da dark web.
- Dessas violações de dados, os agentes de ameaças frequentemente anunciaram acesso às organizações por meio de VPN, RDP e contas comprometidas.
- 221 vulnerabilidades foram ativamente discutidas na dark web, enquanto 237 vulnerabilidades foram discutidas nos canais do Telegram.
- Vinte e dois dias zero significativos foram anunciados, afetando Microsoft Windows, Microsoft Server, Google Chrome, Microsoft Outlook, Adobe Commerce e BIG-IP.
- Mais de 850.000 cartões de pagamento foram anunciados para venda, sendo a maioria credenciais VISA ou Mastercard.



Tipos de acesso anunciados em fóruns dark web

No segundo semestre de 2023, observamos que os agentes de ameaças que operam na dark web geralmente anunciam acesso a organizações via VPN, seguido por RDP e contas comprometidas:

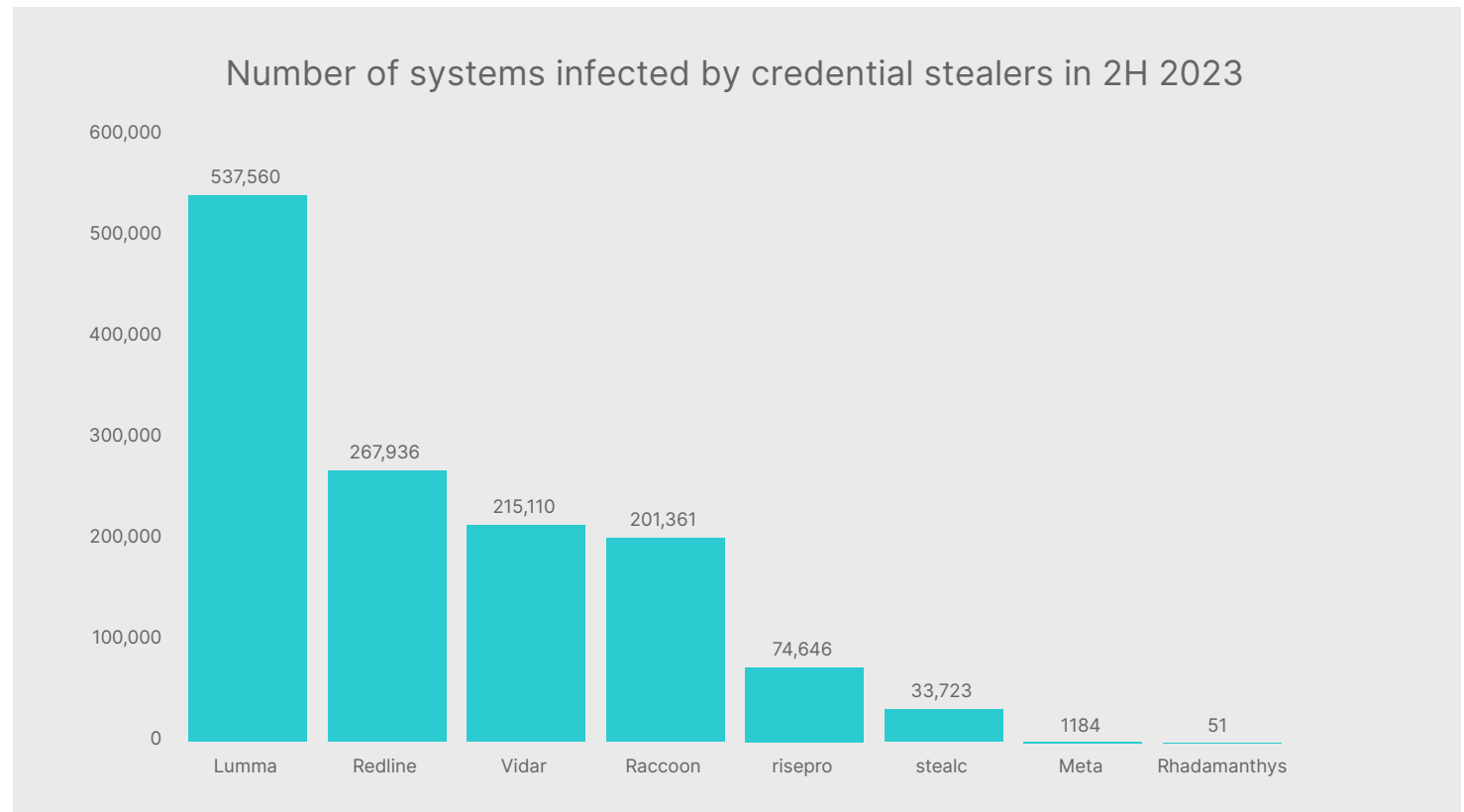
O preço anunciado para credenciais de acesso em fóruns darknet é dinâmico e depende principalmente da organização alvo específica. Vários fatores contribuem para essa estrutura de preços, como a avaliação do setor-alvo, sua escala, o tamanho da força de trabalho e as receitas anuais. Além disso, a suscetibilidade da organização desempenha um papel fundamental na determinação de preços oferecidos pelos agentes de ameaças. O nível de vulnerabilidade exibido pela organização é outro fator crucial que afeta os preços.



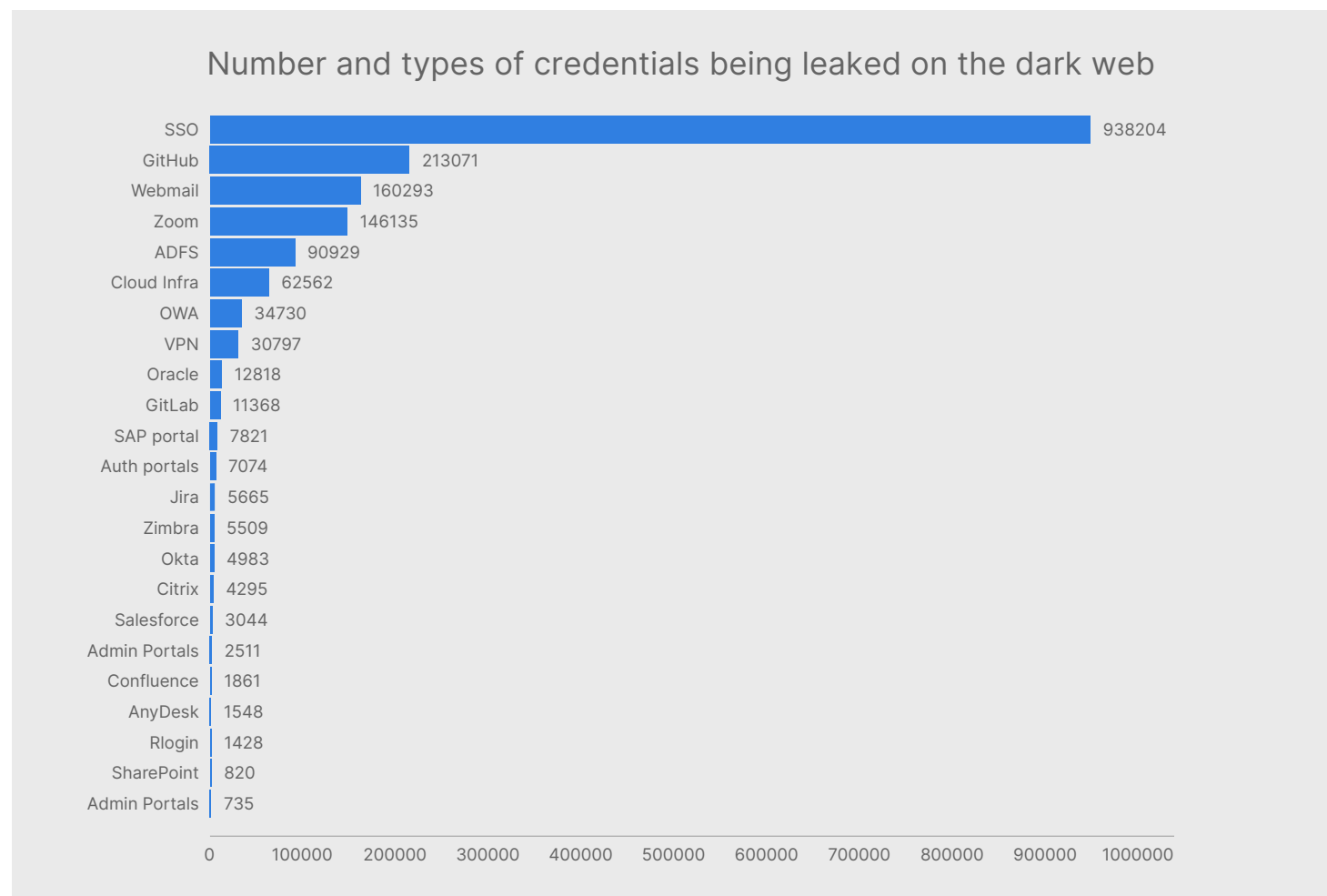
Roubadores de credenciais

Os ladrões de credenciais são um tipo de malware projetado para roubar credenciais de conta de usuário que, se adquiridas, podem ajudar um invasor a obter acesso a sistemas e redes seguros para coletar informações confidenciais ou críticas. Os dados do sistema do usuário final infectado também são frequentemente listados para venda em mercados de darknet de roubo de credenciais.

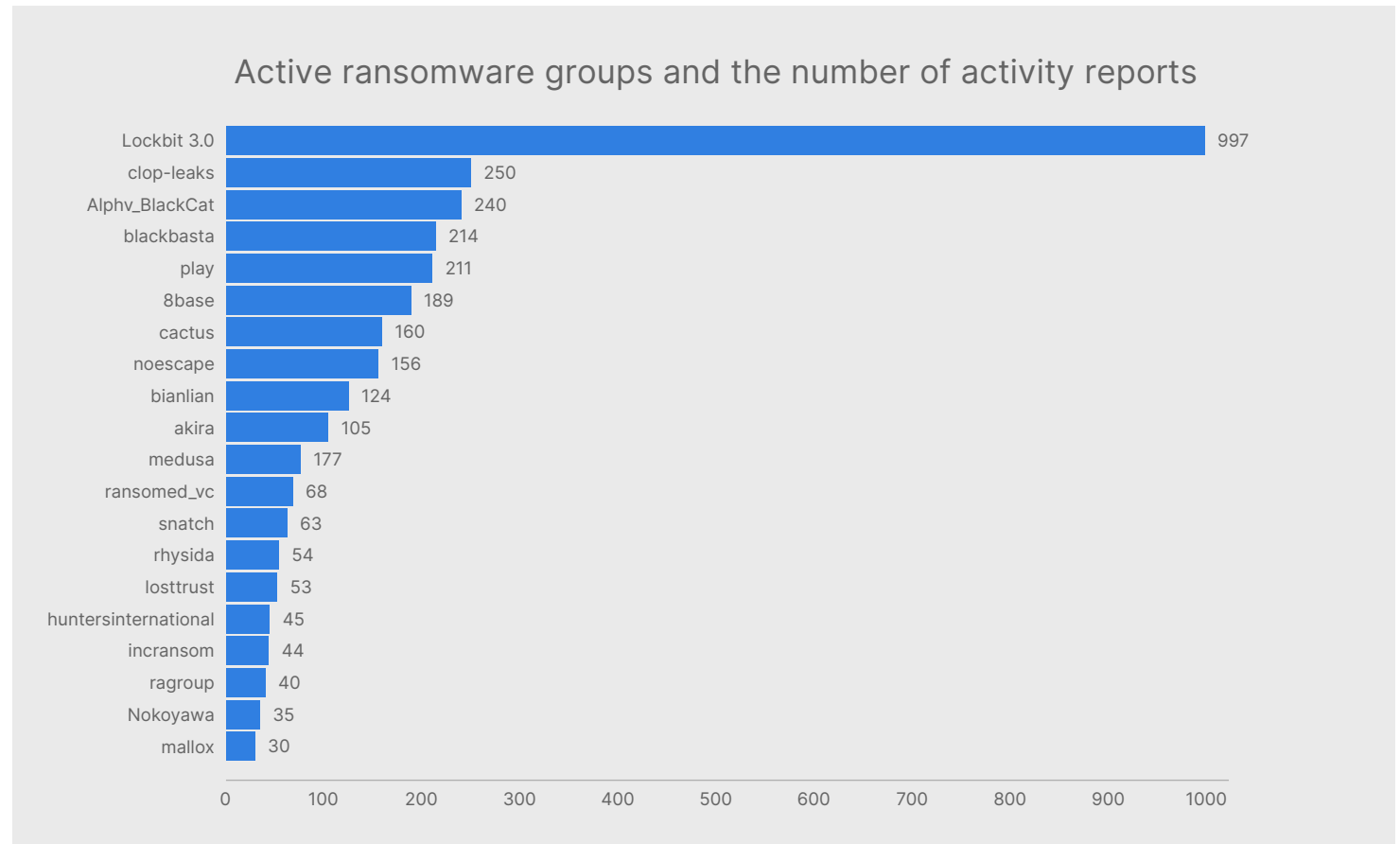
No 2H de 2023, observamos mais de 1.331.571 sistemas infectados por roubadores de credenciais, incluindo Lumma, Redline, Vidar, Raccoon, Risepro, stealc, Meta e Rhadamanthys. Esses logs de roubadores estão disponíveis a preços baixos, permitindo que um grande número de agentes de ameaças os adquira facilmente.



Também analisamos os tipos e números de credenciais que estão sendo vazadas na dark web:



O gráfico abaixo representa os grupos de ransomware que estiveram ativos no 2H de 2023, juntamente com a respectiva contagem de vítimas:



Tendências das ramificações

A equipe de detecção e resposta gerenciadas (MDR) do FortiGuard gerencia instâncias de detecção e resposta de endpoints (EDR) em nome de clientes em todo o mundo. Suas responsabilidades diárias dão à equipe um instantâneo significativo das atividades do adversário em verticais de negócios e regiões geopolíticas. Da mesma forma, nossa equipe de resposta a intrusão (Intrusion response, IR) oferece serviços proativos e reativos para apoiar nossa base global de clientes. A exposição a clientes que combatem ativamente um incidente de segurança fornece informações valiosas sobre intrusões iniciadas por grupos APT e agentes de ameaças financeiramente motivados.

As seguintes percepções vêm de casos do mundo real observados pelas equipes de MDR e IR do FortiGuard no segundo semestre de 2023. Essas descobertas fornecem recomendações práticas para responder a recursos consistentes e emergentes do cenário de ameaças. Eles também nos dão uma compreensão mais sólida de como as ações dos clientes moldam as tendências de ameaças.

Respostas mal definidas resultam em erros não forçados

Algumas organizações não têm planos ou procedimentos de RI adequados em vigor, resultando em reações bruscas quando ocorre uma violação. As investigações e ações de remediação geralmente são deixadas incompletas. Remediações de escopo ruim resultaram em organizações inadvertidamente “encarregando o urso”, com adversários respondendo implantando rapidamente ransomware para causar danos significativos e totalmente desnecessários. Esse problema também ocorre quando as organizações aplicam tecnologias fora do caso de uso pretendido, por exemplo, profissionais que empregam soluções antivírus legadas baseadas em assinatura na tentativa de erradicar um adversário que persiste por meio de cargas úteis na memória.

As organizações devem garantir que tenham planos e procedimentos de RI precisos e acionáveis. As equipes podem melhorar significativamente sua postura de segurança empregando com eficiência sua tecnologia existente por meio de procedimentos robustos.

O não patch continua a contribuir para intrusões

Em 86% dos casos que investigamos, em que o acesso não autorizado ocorreu por meio da exploração de uma vulnerabilidade, a vulnerabilidade já era conhecida na época e um patch estava prontamente disponível. Onde as organizações não respondem à inteligência de ameaças direta e direcionada, é provável que seja devido a um problema de recursos. No entanto, os líderes devem reavaliar seus investimentos em segurança, dado o quanto a correção regular é vital para proteger contra violações.



Backups conectados à produção são alvos atraentes do invasor

Os membros da nossa equipe de RI trabalharam com algumas vítimas de ransomware que investiram em soluções de backup que se autenticam em seu principal ambiente corporativo e permanecem conectadas 24 horas por dia, sete dias por semana. Nesses casos, os agentes de ameaças envolvidos puderam acessar, manipular e criptografar as soluções de backup durante as intrusões, tornando-as inúteis. Os agentes de ameaças geralmente pesquisam ativamente backups para inibir a recuperação do sistema. As organizações devem garantir que seus backups sejam adequadamente separados da rede.

Os processos de exclusão automatizados podem dificultar as investigações

Em muitas ocasiões, nossa equipe de RI trabalhou com organizações que haviam configurado suas ferramentas antivírus para excluir automaticamente arquivos maliciosos após a detecção, em vez de colocá-los em quarentena. Essa regra de exclusão automática impede a atribuição adequada da atividade observada, o que pode retardar uma investigação. Isso também pode afetar as equipes de segurança que podem não ser capazes de realizar a triagem corretamente após a remoção desses artefatos. Recomendamos que as organizações passem para uma configuração que coloque amostras em quarentena e armazene uma cópia (ou pelo menos colete hashes de arquivo) para que as equipes de IR possam usar métodos de recuperação alternativos, se necessário.

Os servidores ESXi são vacas de caixa para operadoras de ransomware

Os servidores ESXi estão sendo cada vez mais alvo durante ataques de ransomware. (O ESXi é um hipervisor bare-metal que pode particionar um servidor em várias máquinas virtuais.) Os servidores ESXi oferecem aos adversários um grande bônus por seu dinheiro, dado o impacto significativo que eles podem ter na capacidade de uma organização de conduzir negócios quando comprometidos. O lançamento de criadores como o ransomware Babuk e HelloKitty, que podem ser usados para direcionar servidores ESXi, tornou mais fácil do que nunca para adversários com motivação financeira direcionar esses dispositivos.

As contas válidas continuam a fornecer caminhos rápidos por meio de cadeias de destruição

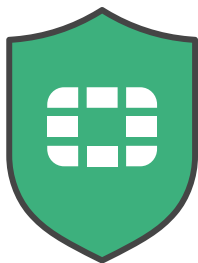
Os invasores continuam a usar contas válidas indevidamente para se mover lateralmente em ambientes comprometidos. Os agentes de ameaças usam essas contas válidas em combinação com técnicas LoLbins para escapar das defesas das organizações. Como resultado, as organizações precisam monitorar o uso suspeito de contas válidas em seu ambiente.

Os adversários estão cada vez mais usando os serviços do Microsoft Windows para executar RATs

Houve um pequeno aumento na prevalência de serviços do Microsoft Windows sendo usados como o principal método de execução para RATs no ambiente de uma vítima. A execução do serviço pode ser usada para escalonamento de privilégios e pode abstrair a execução em cadeias de processos RAT, obscurecendo atividades maliciosas e aumentando as complexidades para equipes de segurança encarregadas de fazer a triagem de um incidente. Isso muitas vezes resulta em uma investigação incompleta por equipes que não têm os recursos para apoiar a análise aprofundada necessária para vincular a atividade de serviço anômala a contas comprometidas e pontos de entrada. A execução do serviço é simples de implementar e, dada a natureza pesada do serviço de versões mais recentes do Microsoft Windows, os adversários provavelmente veem isso como outra oportunidade de escapar da detecção.

Os agentes de ameaças usam regularmente ferramentas de administração de código aberto

Agentes de ameaças e grupos APT continuam a usar ferramentas de administração de código aberto conhecidas para comprometer vítimas desavisadas. O uso dessas ferramentas é consistentemente alto para muitos estágios de uma intrusão, desde a descoberta até o movimento lateral. As ferramentas de código aberto são normalmente leves e muitas vezes podem voar sob o radar em organizações que não entendem a ameaça que representam. A questão de identificar o uso suspeito dessas ferramentas se torna mais complexa pelo uso legítimo de software de código aberto pelos administradores do sistema. As organizações devem procurar caracterizar o uso legítimo dessas ferramentas e usar técnicas de controle de aplicativos para bloquear o uso anômalo.



Para ser notificado quando detectamos uma ameaça nova ou emergente, [inscreva-se](#) aqui para receber alertas de surtos do FortiGuard Labs. Você também pode baixar o Relatório anual de alertas de surtos de 2023 [aqui](#).

Conclusão

Esperamos que esta edição do relatório do cenário de ameaças da Fortinet forneça informações valiosas para ajudá-lo a priorizar e implementar medidas de segurança apropriadas em sua organização. Em resumo, aqui estão as três principais tendências que observamos durante o segundo semestre de 2023 que mais se destacaram para nós. Lembre-se disso e ajuste sua estratégia de gerenciamento de riscos de acordo.

A zona vermelha permanece estável. O cenário de ameaças normalmente é definido por mudanças constantes, e é por isso que é incomum encontrar algo estático. A proporção de vulnerabilidades observadas com explorações conhecidas pairou em torno de 8% desde que começamos a medi-las há quase dois anos. As vulnerabilidades em si mudam, é claro, mas o esforço geral necessário para resolvê-las aparentemente não muda. Aproveite essa previsibilidade para alocar recursos para minimizar a zona vermelha da sua organização.

Mantenha vulnerabilidades “antigas” em seu radar. Novas explorações e malware podem se espalhar de longe e rapidamente, portanto, se sua organização tende a estar entre os primeiros alvos, pode ser apenas uma questão de horas ou dias antes que os ataques ocorram. No entanto, também vimos que muitas vulnerabilidades, mesmo aquelas que existem há anos, muitas vezes permanecem no radar dos agentes de ameaças como alvos ativos. Infelizmente, isso significa que você não pode estar tão focado na proteção contra novas vulnerabilidades e ataques que negligencia as antigas. As equipes de segurança bem-sucedidas precisam se proteger contra todo o ciclo de vida da exploração, e isso começa com um programa proativo de correção e atualização.

Os setores críticos são os principais alvos de ransomware. Os agentes por trás das campanhas de ransomware sempre foram sedutores. Seja fazendo ajustes rápidos nas demandas de resgate com base na dinâmica do mercado de criptomoedas ou criando grandes empresas criminosas para minimizar custos e maximizar a escala, elas têm uma tendência para fazer as coisas acontecerem. É isso que torna a mudança contínua para direcionar setores críticos ainda mais preocupante. Esses ambientes pesados de OT são particularmente suscetíveis a interrupções dispendiosas, o que aumenta muito a pressão para pagar altos resgates para restaurar a produtividade.

Embora cada um de nós tenha um papel vital a desempenhar na luta contra nossos adversários coletivos, nenhuma organização pode interromper com uma única mão os agentes de ameaças. A inteligência compartilhada é uma parte crucial de como garantimos respostas oportunas e precisas quando os invasores atacam. Quanto mais colaboramos nos setores público e privado, mais eficazes podemos ser para interromper o crime cibernético.

Notas de rodapé

- 1 FortiGuard Outbreak Alerts, FortiGuard Labs, acessado em 18 de fevereiro de 2024.
- 2 Vulnerabilidades do Zyxel Multiple Firewall, FortiGuard Outbreak Alerts, 6 de junho de 2023.
- 3 Ataque de injeção de comando do roteador Zyxel, FortiGuard Outbreak Alerts, 9 de agosto de 2023.
- 4 Zerobot Attack, FortiGuard Outbreak Alerts, 27 de dezembro de 2022.
- 5 VMware Aria Operations for Networks Command Injection Vulnerability, FortiGuard Outbreak Alerts, 22 de junho de 2023.
- 6 IBM Aspera Faspex Code Execution Vulnerability, FortiGuard Outbreak Alerts, 1o de março de 2023.
- 7 Cisco IOS XE Web UI Attack, FortiGuard Outbreak Alerts, 20 de outubro de 2023.
- 8 Citrix Bleed Attack, FortiGuard Outbreak Alerts, 2 de novembro de 2023.
- 9 Apache RocketMQ Remote Command Execution Vulnerability, FortiGuard Outbreak Alerts, 5 de julho de 2023.
- 10 Vulnerabilidade de injeção SQL de transferência MOVEit Progress, FortiGuard Outbreak Alerts, 5 de junho de 2023.
- 11 MITRE ATT&CK, acessado em 18 de fevereiro de 2024.
- 12 JS/Agent.CY!tr, FortiGuard Labs Encyclopedia, 9 de junho de 2022.
- 13 JS/Agent.F022!tr, FortiGuard Labs Encyclopedia, 10 de julho de 2023.
- 14 JS/Agent.PIV!tr, FortiGuard Labs Encyclopedia, 1.o de novembro de 2021.
- 15 JS/Agent.NDS!tr, FortiGuard Labs Encyclopedia, 7 de novembro de 2023.
- 16 JS/ScrInject.B!tr, FortiGuard Labs Encyclopedia, 30 de agosto de 2011.
- 17 Ibid.
- 18 JS/Cryxos.5478!tr, FortiGuard Labs Encyclopedia, 30 de março de 2021.
- 19 CVE-2023-46604, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 20 Lucian Constantin, HelloKitty Ransomware Deployed Via Critical Apache Active MQ Flaw, CSO Online, 2 de novembro de 2023.
- 21 Apache ActiveMQ Ransomware Attack, FortiGuard Outbreak Alerts, 6 de novembro de 2023.
- 22 Lazarus RAT Attack, FortiGuard Outbreak Alerts, 12 de dezembro de 2023.
- 23 Agent Tesla Malware Attack, FortiGuard Outbreak Alerts, 7 de setembro de 2023.
- 24 CVE-2017-11882, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 25 CVE-2018-0802, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 26 CVE-2017-9841, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 27 CVE-2018-15133, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 28 CVE-2021-41773, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 29 Cedric Pernet, AndroXgh0st Malware Botnet Steals AWS, Microsoft Credentials and More, TechRepublic, 18 de janeiro de 2024.
- 30 Ravie Lakshmanan, New Version of Prometei Botnet Infects Over 10,000 Systems Worldwide, The Hacker News, 10 de março de 2023.



- 31 O economista subterrâneo: Volume 3, Edição 12, ZeroFox, 27 de junho de 2023.
- 32 Kevin Poireault, DarkGate and PikaBot Activity Surge in the Wake of QakBot Takedown, Infosecurity Magazine, 21 de novembro de 2023.
- 33 Índice comum de vulnerabilidades e exposições, MITRE , acessado em 18 de fevereiro de 2024.
- 34 Douglas Jose Pereira dos Santos, 2H 2022 Relatório do cenário global de ameaças: Principais insights para diretores de segurança da informação, Fortinet, 3 de março de 2023.
- 35 CVE-2021-44228, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 36 CVE-2023-44487, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 37 Exploit Prediction Scoring System, Forum of Incident Response and Security Teams, acessado em 18 de fevereiro de 2024.
- 38 CVE-2023-28121, NIST National Vulnerability Database, acessado em 18 de fevereiro de 2024.
- 39 O Relatório global de ransomware de 2023, Fortinet, 20 de abril de 2023.
- 40 O Ransomware Extortion Skyrockets em 2023, Reaching \$449.1M and Counting, The Hacker News, 12 de julho de 2023.
- 41 MITRE ATT&CK, acessado em 18 de fevereiro de 2024.
- 42 Relatório do cenário de ameaças do FortiGuard Labs 1H 2023, Fortinet, 7 de agosto de 2023.



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Copyright © 2024 Fortinet, Inc. All rights reserved. May 29, 2024 8:07 pm 2564222-0-0-EN