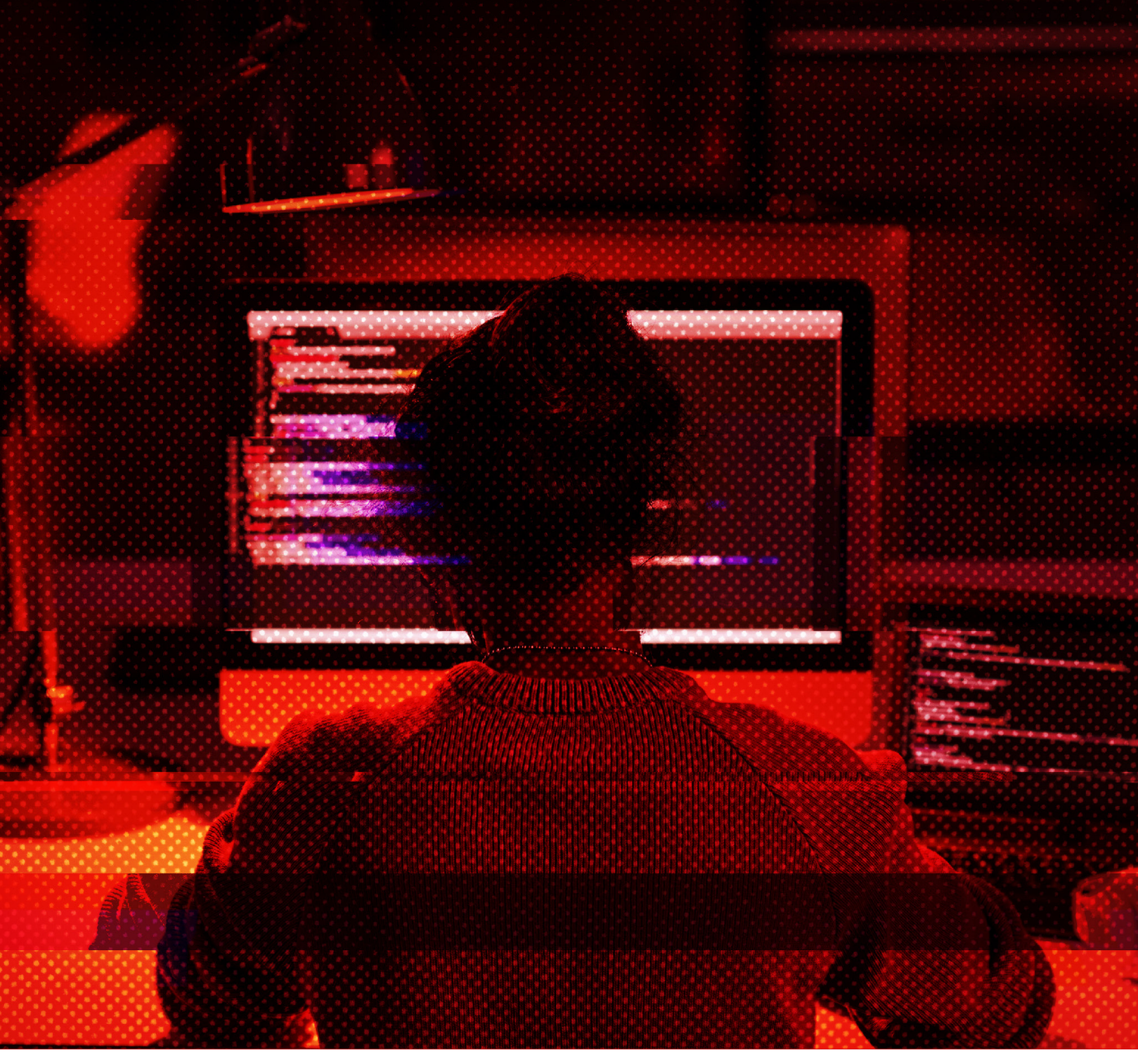
Trend Research

TREND MICRO

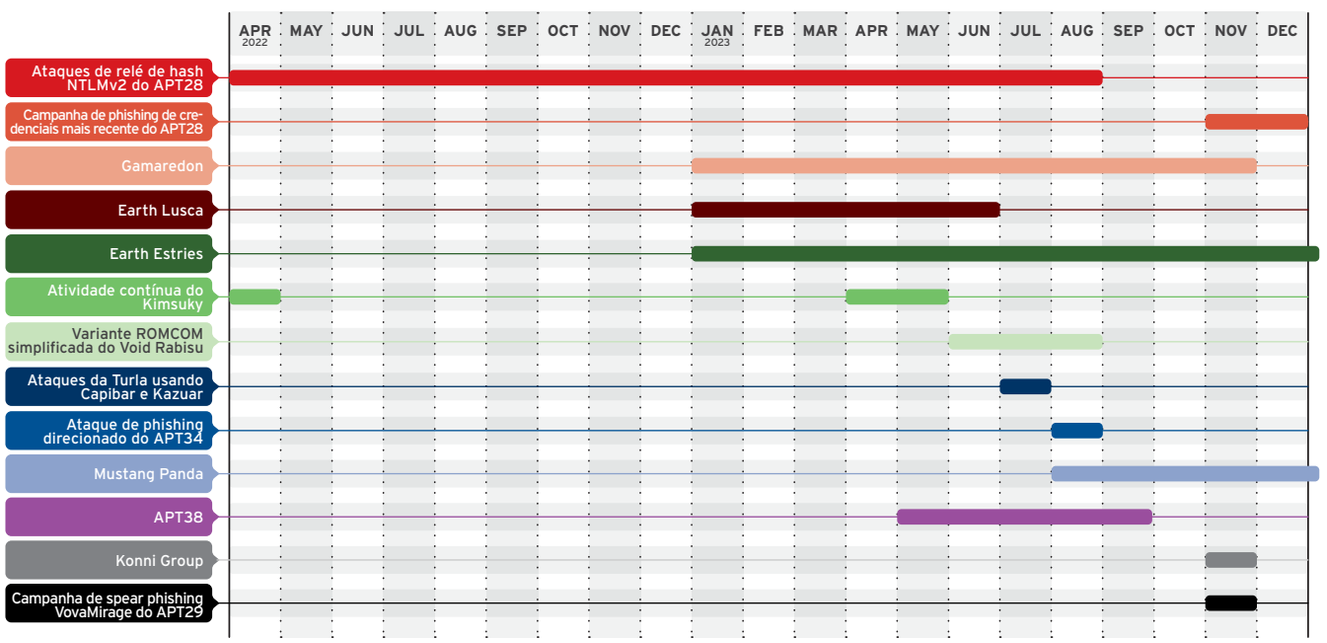
CALIBRATING EXPANSION

RELATÓRIO ANUAL DE CIBERSEGURANÇA 2023




03 CAMPANHAS APT
07 AMEAÇAS DE RANSOMWARE
13 AMEAÇAS À CLOUD E EMPRESAS
16 MITRE ATT&CK DETECCÇÕES
20 CENÁRIO DE AMEAÇAS

CAMPANHAS APT



Ataques de relé de hash NTLMv2 do APT28

Abril de 2022 - Agosto de 2023

Alvos:

- Organizações envolvidas em uma ampla gama de campos, mas principalmente em assuntos estrangeiros, energia, defesa e transporte

Possivelmente uma tentativa de forçar sua entrada nas redes-alvo

Explorou a CVE-2023-23397 que foi corrigida em março de 2023, momento em que o APT28 usou métodos mais elaborados que envolviam scripts hospedados no Mockbin enviados para os alvos

Campanha de phishing de credenciais mais recente do APT28

Novembro - Dezembro de 2023

Alvos:

- Várias organizações governamentais na Europa

Apresenta semelhanças com a campanha anterior de relé de hash em indicadores técnicos, como o compartilhamento do mesmo nome de computador usado para enviar e-mails de spear-phishing e criar arquivos LNK

Gamaredon

Janeiro - Novembro de 2023

Alvos:
- Organizações governamentais na Ucrânia

O Gamaredon continua suas atividades com ataques usando Injeção Remota de Modelo e arquivos executáveis autoextraíveis

A linha do tempo de aumento de atividade da amostra investigada sugere que a campanha foi lançada para intensificar as atividades de espionagem

Earth Estries

Janeiro de 2023 – presente

Alvos:
- Organizações governamentais e indústrias de tecnologia nas Filipinas, Taiwan, Malásia, África do Sul, Alemanha e EUA

Eles utilizam múltiplos backdoors e ferramentas de hacking, além de ataques de degradação do PowerShell para evitar detecção

Eles usam serviços públicos como Github, Gmail, AnonFiles e File.io para aprimorar e transferir comandos e dados roubados

Earth Estries é conhecido por implantar campanhas de ciberespionagem

Earth Lusca

Janeiro - Junho de 2023

Alvos:
- Departamentos governamentais envolvidos em assuntos estrangeiros, tecnologia e telecomunicações em países do Sudeste Asiático, Ásia Central e Bálcãs, com ataques dispersos em países da América Latina e da África.

O payload descriptografado é um backdoor direcionado ao Linux, uma nova variante chamada SprySOCKS

Visa os servidores de acesso público de suas vítimas

Atividade contínua do Kimsuky

Abril de 2022, e Abril a Maio de 2023

Alvos:
- Indivíduos que trabalham em áreas relacionadas à República Popular Democrática da Coreia
- Possivelmente organizações relacionadas a militares, diplomacia, unificação e grupos de apoio à língua coreana, com base no histórico de campanhas anteriores do Kimsuky.

Entregue como um arquivo de e-mail

Provavelmente direcionado para coletar informações sobre eventos geopolíticos, estratégias diplomáticas e atividades que impactam os interesses do alvo

Também pode ser lançado para coletar informações relacionadas a armamentos e para ataques relacionados a criptomoedas

Variante simplificada do ROMCOM do Void Rabisu

Junho - Agosto de 2023

Alvos:
- Pessoal militar e líderes políticos na Europa

Explorou a vulnerabilidade de dia zero CVE-2023-36884 na época

Principalmente conhecido por atividades de ciberespionagem direcionadas a governos e militares com motivações financeiras

Ataque de phishing direcionado do APT34

Agosto de 2023

Alvos:
- Possivelmente organizações dentro do Reino da Arábia

O documento malicioso no esquema de phishing deixou cair um novo malware projetado para espionagem, capaz de identificar a máquina, ler e enviar arquivos da máquina e baixar outro arquivo ou malware

O APT34 é conhecido por suas atividades de ciberespionagem direcionadas a agências governamentais, organizações envolvidas em infraestrutura crítica e telecomunicações no Oriente Médio

Ataques da Turla usando Capibar e Kazuar

Julho de 2023

Alvos:
- Organizações diplomáticas e militares na Ucrânia

Nesta campanha de phishing, o malware Capibar foi usado para coleta de inteligência, enquanto o malware Kazuar foi usado para roubo de credenciais

A Turla está ativa desde 2014 e é conhecida por suas atividades de ciberespionagem

Mustang Panda

Agosto de 2023 – presente

Alvos:
- Organizações governamentais nas Filipinas e outras organizações relacionadas

Utilizou componentes de software legítimo comumente usados no Sudeste Asiático para carregamento lateral de DLLs

Possivelmente lançado com propósitos de coleta de informações

Amostras contêm strings que sugerem a possibilidade de atacar funcionários do governo de Myanmar

APT38

Maio - Setembro de 2023

- Alvos:
  - Organizações relacionadas a criptomoedas, firmas de investimento e bancos
- Detectado em uma amostra usada pelo BlueNoroff, associado ao APT38. A amostra foi posteriormente relatada pela SentinelOne como usada nas fases posteriores do SwiftLoader e indicada em uma conexão entre KandyKorn e SwiftLoader
- Provavelmente motivado financeiramente e lançado para adquirir moeda estrangeira para financiar armamentos e espionagem

Grupo Konni

Novembro de 2023

- Alvos:
  - Empresas dentro da República da Coreia
- Associado ao OSMIUM, Opal Sleet, SectorA07, TA406 e Kimsuky
- De acordo com nossa análise, o arquivo zip malicioso da campanha contém um arquivo LNK, que, quando executado, solta HTML e VBScript para buscar payloads adicionais, possivelmente apontando para APT37
- Possivelmente lançado como um meio adicional de adquirir moeda estrangeira

Campanha de spear phishing VovaMirage do APT29

Novembro de 2023

- Alvos:
  - Embaixadas e entidades diplomáticas em países europeus, especialmente Azerbaijão, Grécia, Romênia e Itália
- Explorou a vulnerabilidade do WinRAR CVE-2023-38831 em uma campanha de spear phishing
- Provavelmente lançada para reunir informações sobre atividades estratégicas envolvendo os respectivos alvos dos países

O que Observar

As seguintes táticas foram observadas em 2023 e podem ser vistas no próximo ano à medida que as atividades de ransomware se tornam mais sofisticadas.

Há um aumento contínuo no uso de criptografia remota

- Observado em Akira, BlackCat, BlackMatter, LockBit e Royal.
- Os atacantes mapeiam ativamente unidades para criptografar no endpoint afetado em vez de fazer movimentação lateral. Isso pode representar um avanço tático para reduzir sua pegada em ataques e evitar detecção.

Os grupos de ransomware também estão maximizando a conveniência da criptografia intermitente

- Observado em NoEscape, Ransomware Play, BlackBasta, Agenda e BlackCat.
- Os atacantes criptografam fragmentos de dados em vez de criptografar todos os dados de uma vez; esse processo acelera a criptografia enquanto ainda torna os dados afetados inúteis para a vítima e também torna o processo de descriptografia mais complicado.

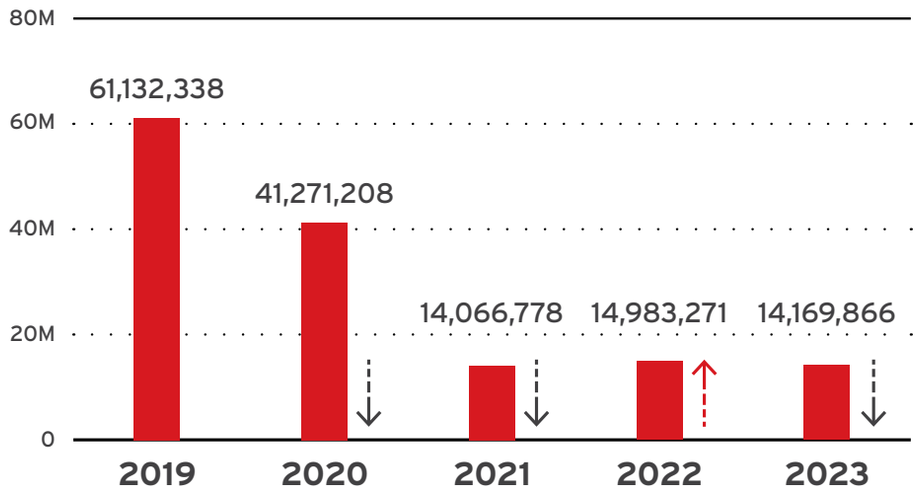
Bypass de Detecção e Resposta de Endpoint (EDR) usando máquinas virtuais (VM) não monitoradas

- Observado em Akira e BlackCat.
- Os atacantes contornam o EDR criando VMs não monitoradas para navegar, mapear e criptografar arquivos nos sistemas de hipervisor Windows Hyper-V e VMs anexadas.

Ataques de múltiplos ransomwares

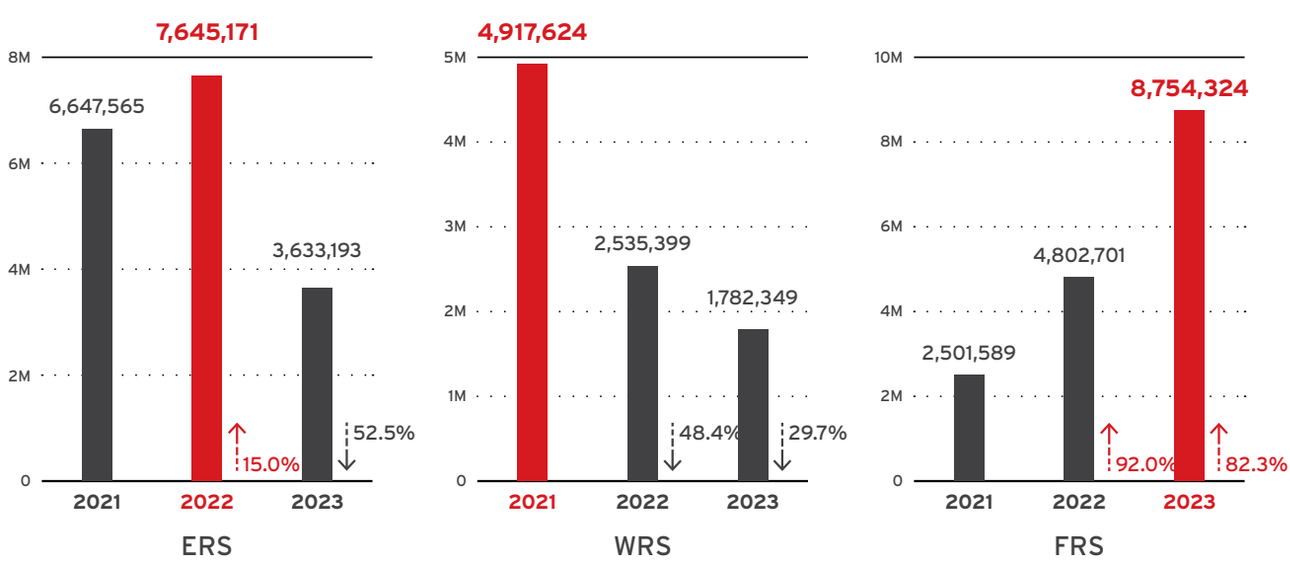
- O atacante inicial vende seu acesso a outros grupos de ransomware para lançar múltiplos ataques com uma combinação de malware, roubo de dados e ferramentas de apagamento para maximizar a manipulação e pressão contra as vítimas.

Detecções Totais de Ransomware

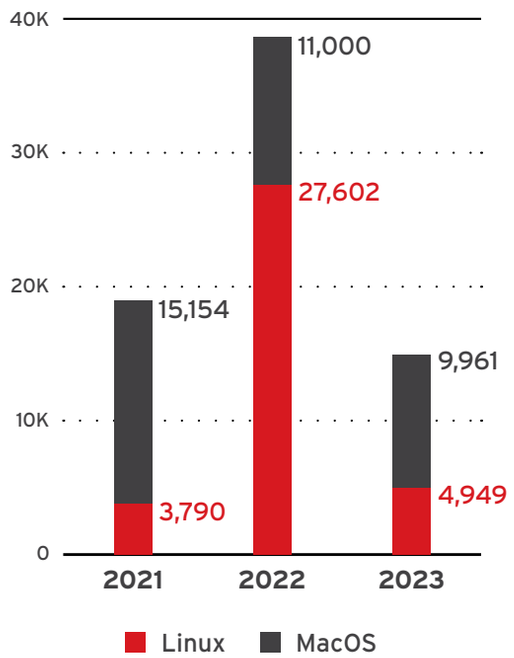


Houve uma tendência geral de queda nas detecções de ransomware, com as detecções de 2021 a 2023 apresentando uma média inferior a metade das detecções registradas em 2020; no entanto, isso não deve ser interpretado como um sinal para os centros de operações de segurança e tomadores de decisão baixarem a guarda. Historicamente, os ataques de ransomware eram lançados em "grande quantidade", como campanhas de spam com links maliciosos, mas ataques que se concentram em quantidade podem ser mais facilmente bloqueados, como mostram nossos dados de ERS e WRS de ransomware na figura seguinte. Esses números mostram uma tendência geral de queda consistente com as detecções totais de ransomware.

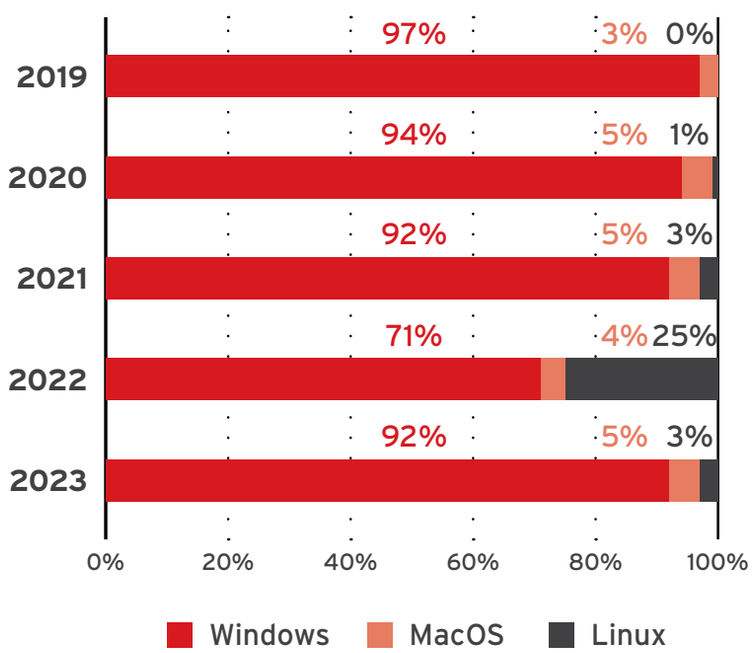
Houve uma tendência geral de queda nas detecções de ransomware, com as detecções de 2021 a 2023 apresentando uma média inferior a metade das detecções registradas em 2020; no entanto, isso não deve ser interpretado como um sinal para os centros de operações de segurança e tomadores de decisão baixarem a guarda. Historicamente, os ataques de ransomware eram lançados em "grande quantidade", como campanhas de spam com links maliciosos, mas ataques que se concentram em quantidade podem ser mais facilmente bloqueados, como mostram nossos dados de ERS e WRS de ransomware na figura seguinte. Esses números mostram uma tendência geral de queda consistente com as detecções totais de ransomware..



Sistemas Operacionais Afetados por Ransomware



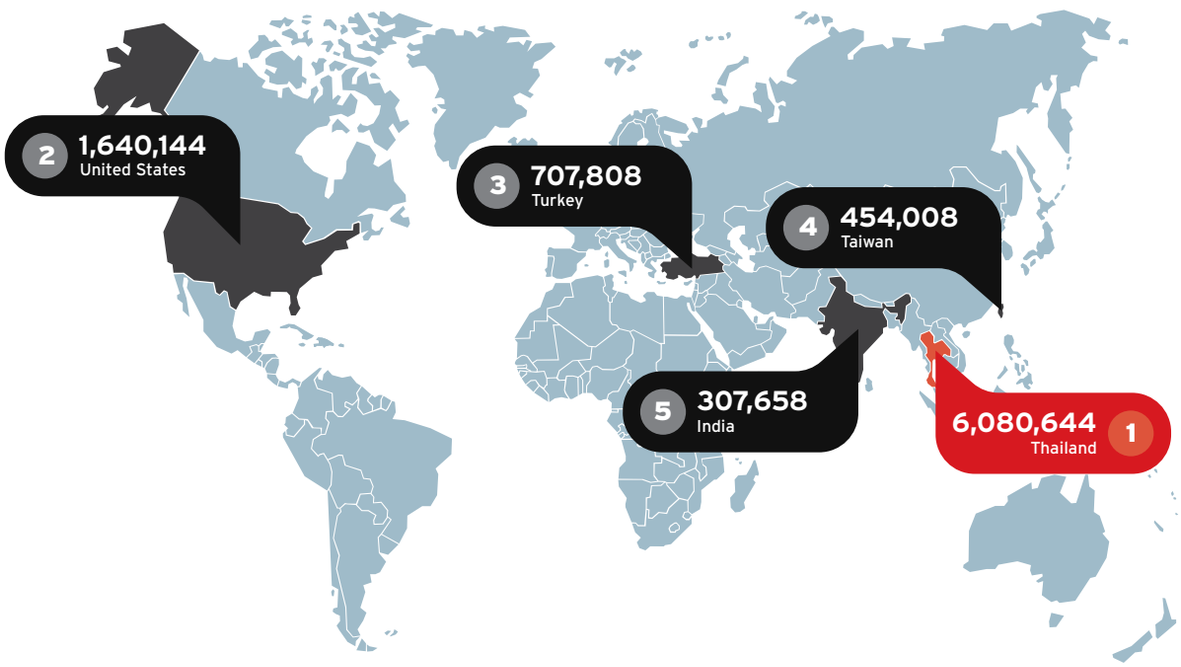
Com base em dados do nosso relatório do meio do ano, as detecções de ataques de ransomware direcionados ao Linux continuam a superar as detecções de ataques ao MacOS no primeiro semestre de 2023. Isso é consistente com os dados reunidos em 2022, que foi um ano excepcional para detecções de malware baseados em Linux, representando 25% da nossa telemetria; anteriormente, ataques direcionados ao Linux representavam apenas de dois a três por cento da proporção de sistemas operacionais. Deve-se notar que o Windows continua a representar a maioria das nossas detecções de ransomware, com a única diminuição significativa em 2022.

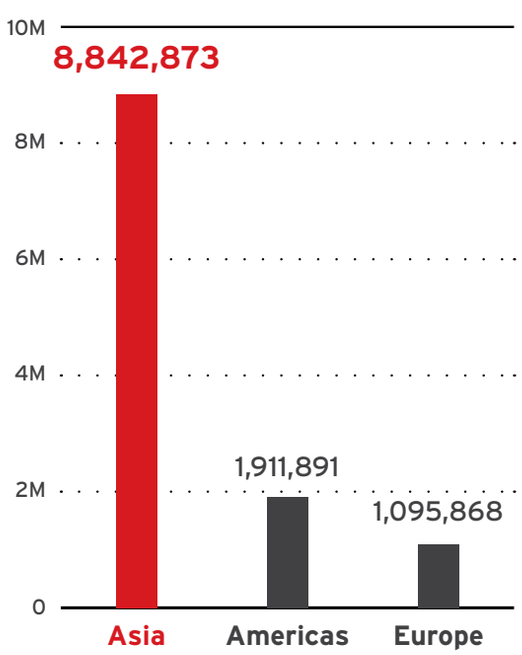


No entanto, ao concluirmos nossos dados para 2023, os ataques de ransomware no MacOS ficaram mais altos, com 9.961 detecções, enquanto as detecções no Linux foram finalizadas em 4.949. Isso pode sugerir que os ataques direcionados ao Linux estão se estabilizando após o influxo de novas variantes do Linux em 2022 até o início de 2023, mas também pode ser influenciado pela diminuição geral na atividade de ransomware.

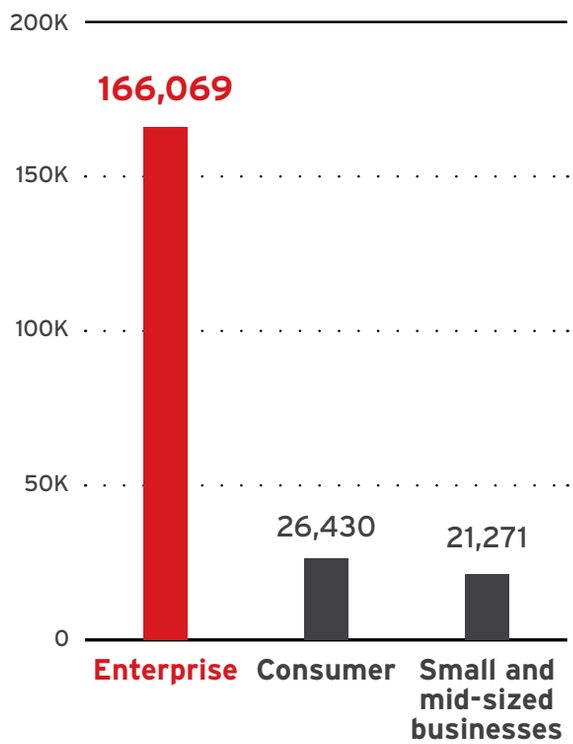
Principais Países e Regiões por Ataques de Ransomware Detectados

A Tailândia representou 68% das detecções de ransomware na Ásia.





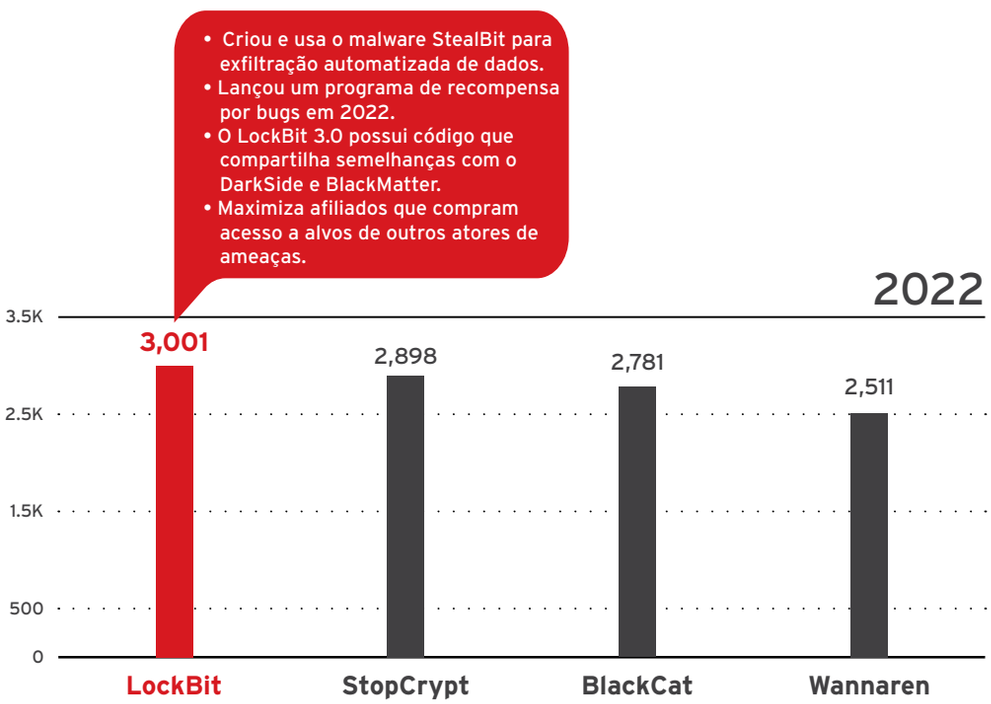
Principais Indústrias e Segmentos por Ataques de Ransomware Detectados

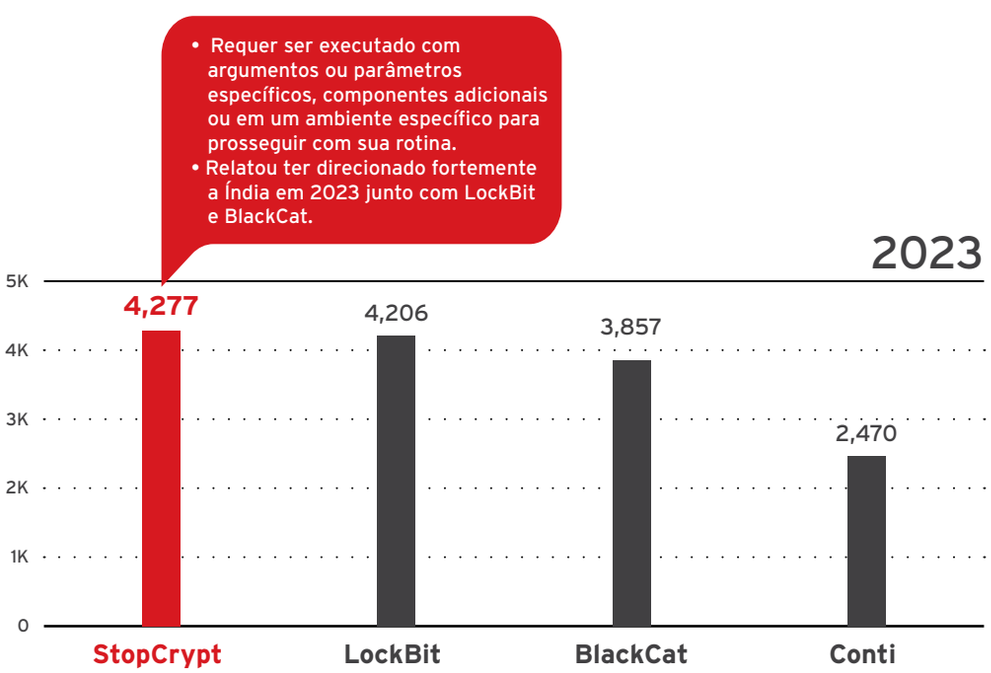


As classificações da indústria e os segmentos baseados em contagens únicas de detecção no endpoint mostram que as empresas são os principais alvos, com um interesse significativo no setor bancário em 2023.

As principais famílias de ransomware

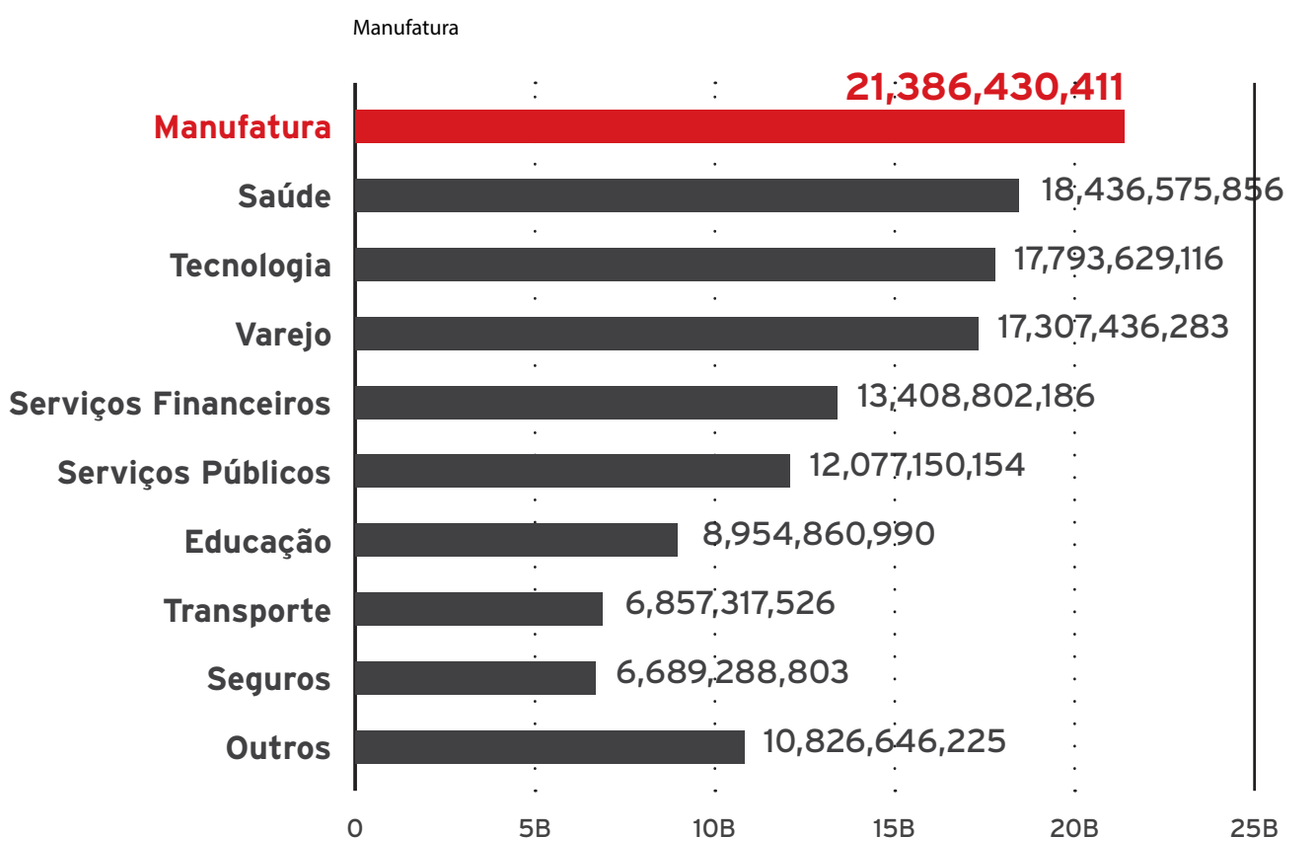
StopCrypt e LockBit mantêm os primeiros lugares como as famílias de ransomware mais prolíficas de 2023, como aconteceu no ano anterior, mas a primeira superou a segunda por uma pequena margem este ano. Observação: esses dados não incluem famílias de ransomware legadas.





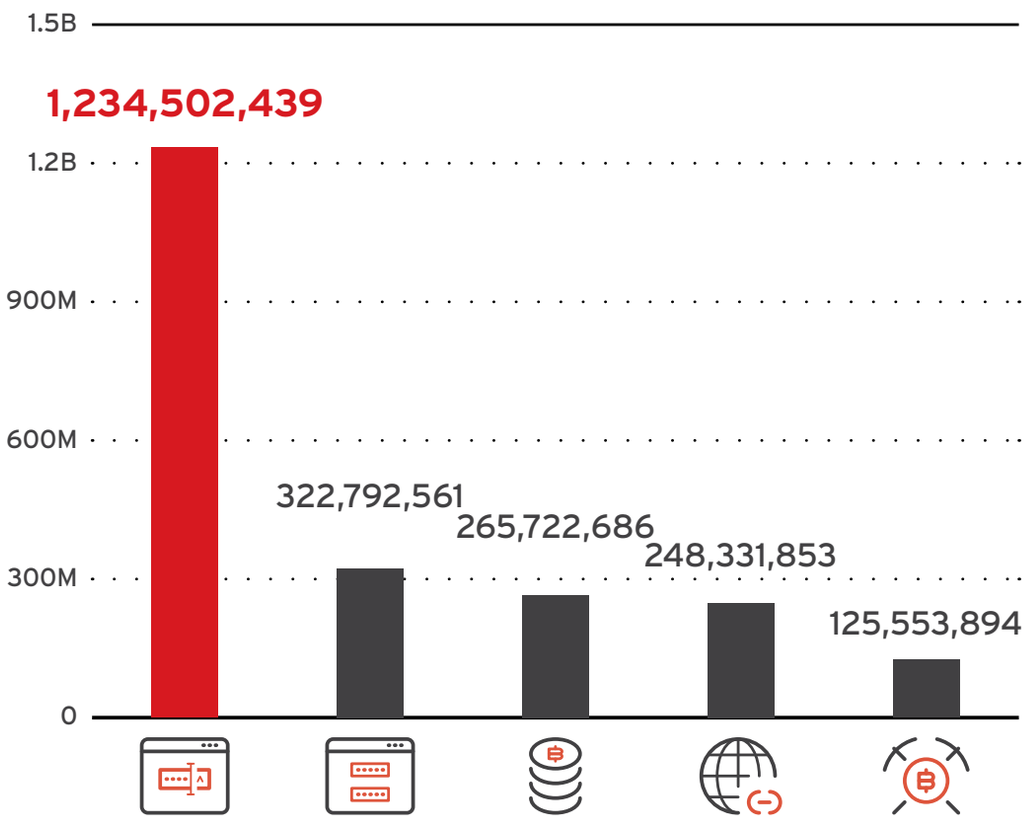
Eventos de Risco

Principais Indústrias por Eventos de Risco (ASRM)



Principais Eventos de Segurança de Rede Doméstica

Com o trabalho híbrido agora estabelecido como parte das operações comerciais, analisamos nossa telemetria de Segurança de Rede Doméstica para ver quais eventos específicos os cibercriminosos favorecem particularmente para usar e quais dispositivos eles visam para maximizar a superfície de ataque maior criada por espaços de trabalho remotos e domésticos.



Login por Força Bruta

- Pode ser RDP via porta 3389, FTP via porta 21 ou SSH via porta 22 para tentar repetidamente fazer login em hosts-alvo usando um dicionário de nomes de usuário e senhas comuns

Login por Senha Padrão TELNET -6

- Detecta quando um usuário dentro da rede usa a senha padrão para fazer login

Atividade de Mineração de Bitcoin/Litecoin/Dogecoin Diversos -1

- Relacionado à divulgação de informações e possivelmente à atividade de mineração de Bitcoin/Litecoin/Dogecoin

HTTP WEB Conteúdo-Length Inválido -2

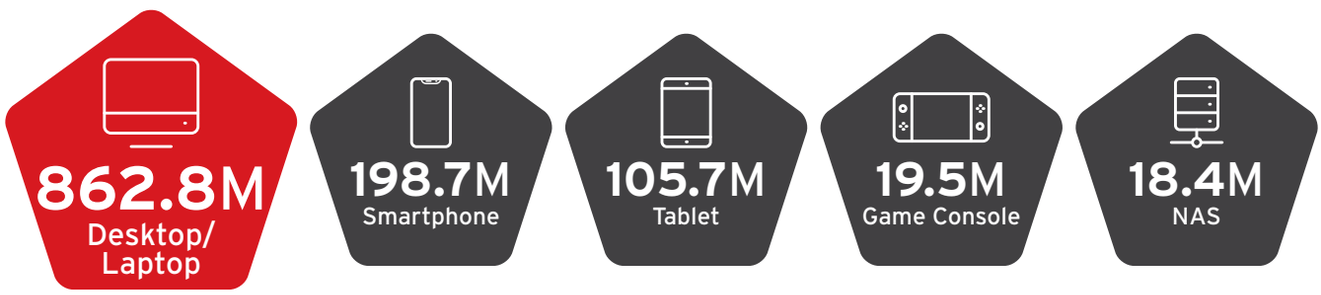
- Causado por um erro no processamento de pacotes HTTP contendo valores negativos no cabeçalho Content-Length que resultam em uma sobrecarga de buffer

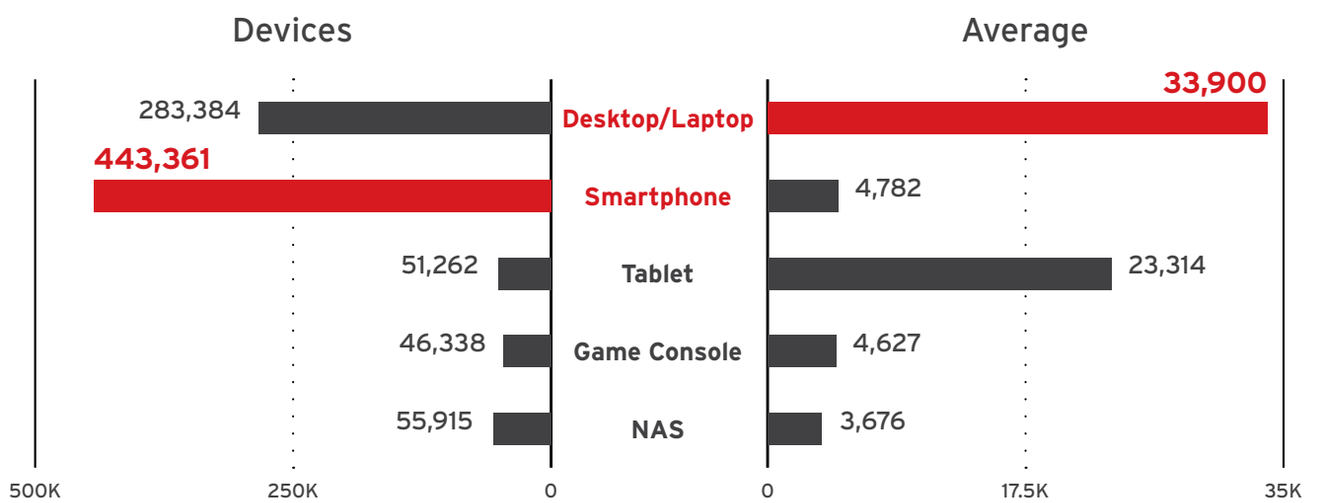
Atividade de Mineração de Cryptocurrency Monero -1

- Possível atividade de mineração de criptomoeda Monero (XMR)

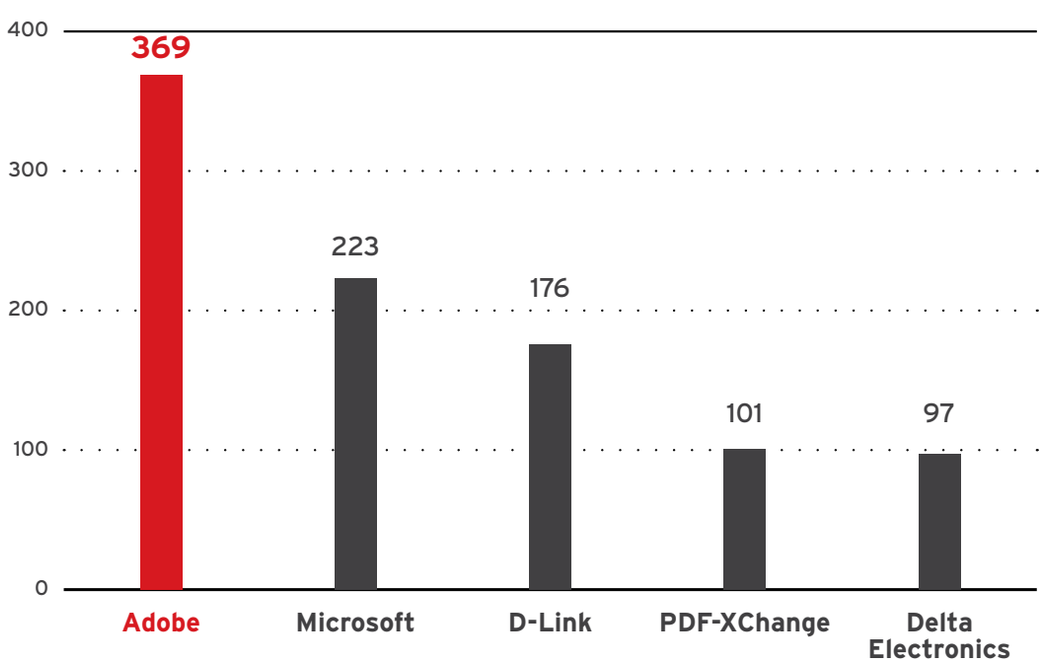
Principais Tipos de Dispositivos Afetados pela Segurança de Rede Doméstica

Desktops e laptops registraram o maior número de detecções de ataques de entrada com base em nossos dados de telemetria de Segurança de Rede Doméstica.



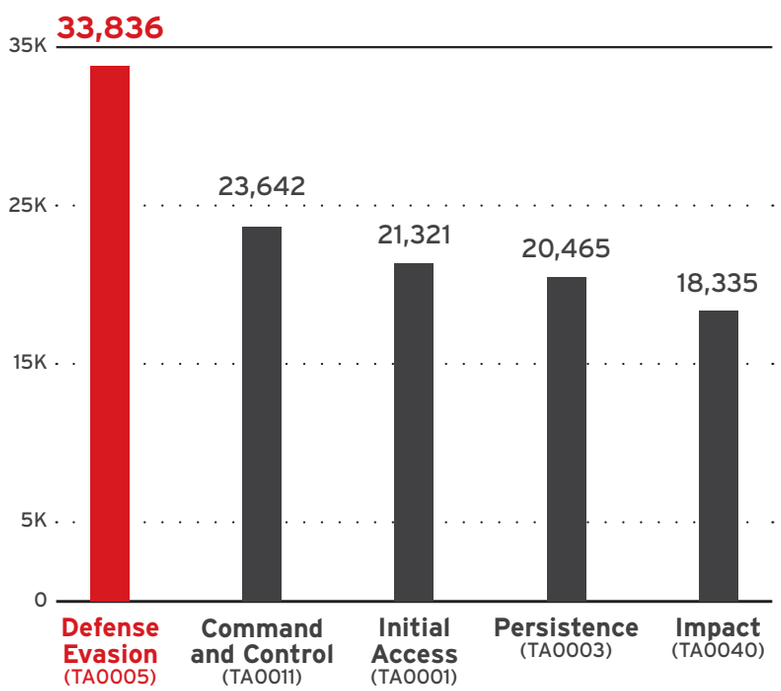


Vulnerabolidade por fabricante

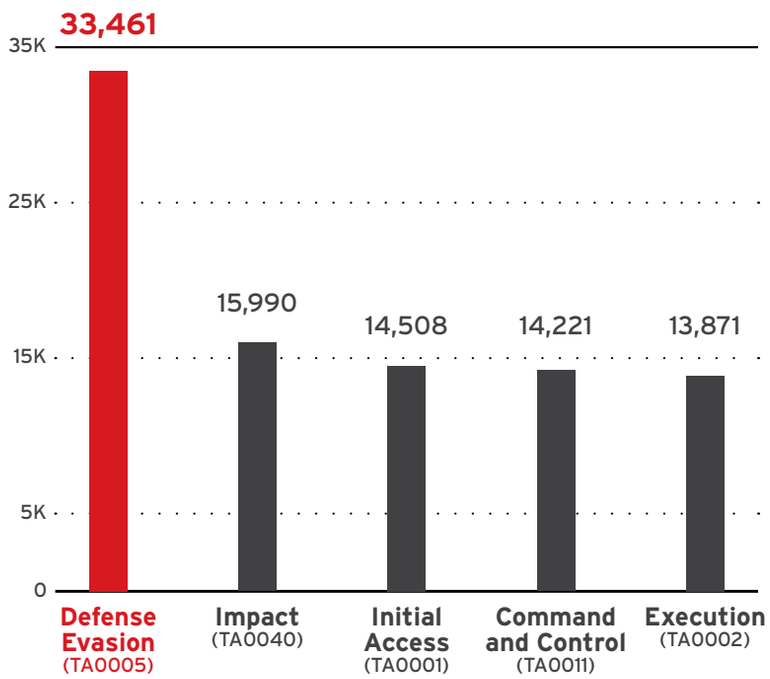


Principais 5 Táticas Detectadas (Geral)

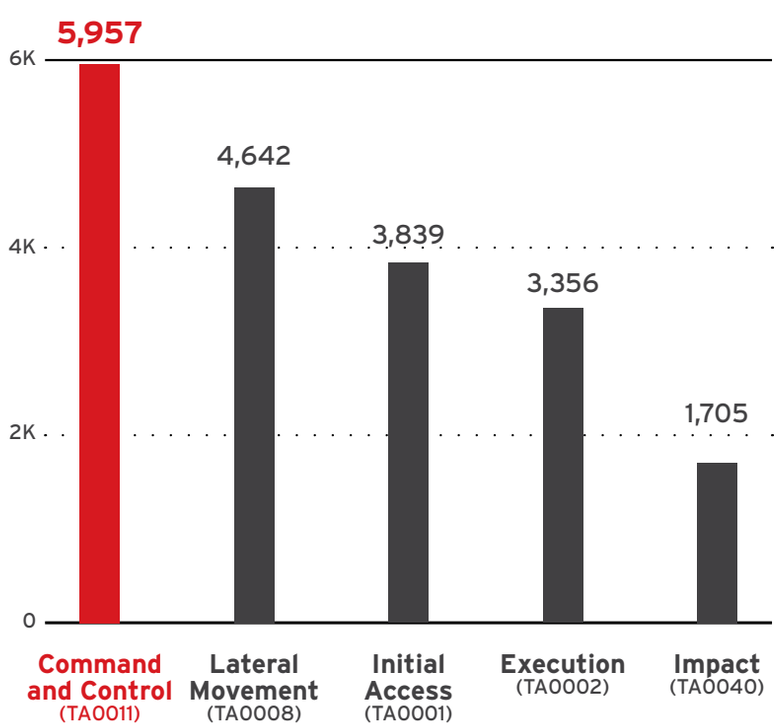
Evitar ferramentas de segurança, comunicação e controle de sistemas comprometidos, e obter uma posição de entrada nos sistemas e redes das vítimas são as TTPs mais utilizadas (globalmente, em endpoints, redes e e-mails)



Principais Táticas, Técnicas e Procedimentos (TTPs) em Endpoints



Principais Táticas, Técnicas e Procedimentos (TTPs) em Rede

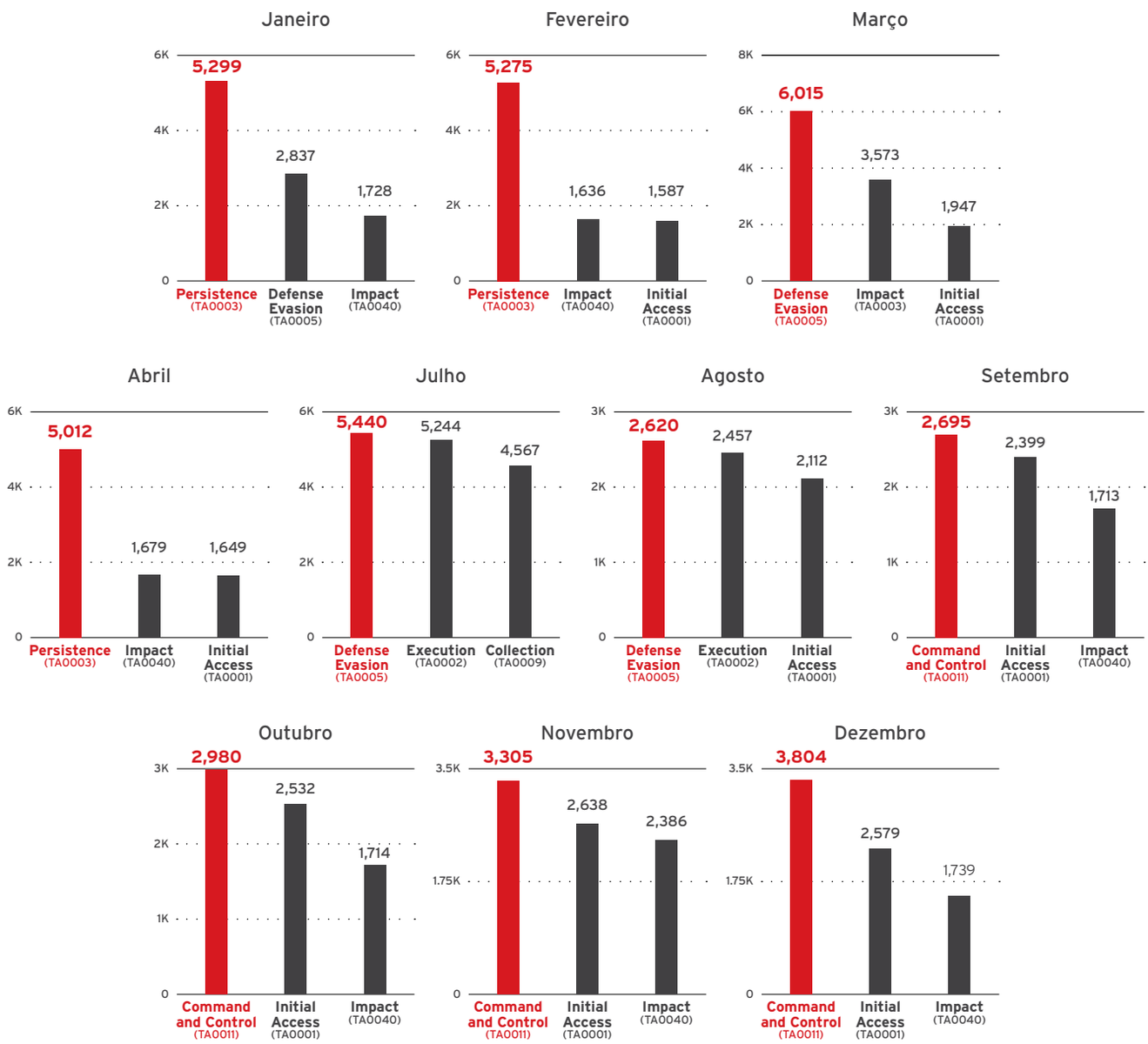


Tendência Geral dos TTPs por Deteções

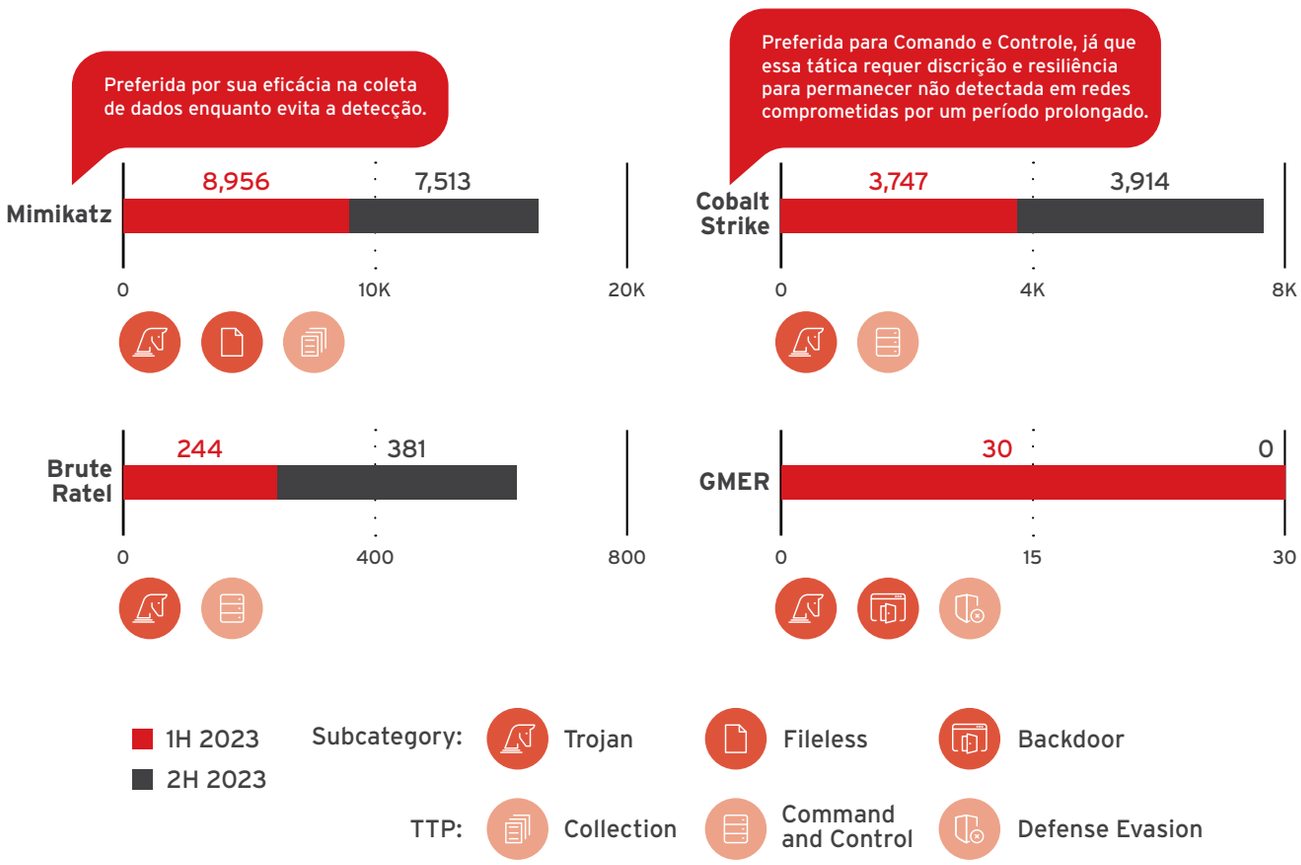
O Controle e Comando mostrou um aumento gradual de setembro a dezembro, enquanto a Evasão de Defesa atingiu o pico em março e julho antes de declinar nas detecções dos clientes nos meses subsequentes. A Execução entrou para as três principais TTPs detectadas em julho e agosto, enquanto o Impacto não mostrou uma tendência clara, apesar de um pico em novembro.

A Persistência só entrou para as três principais no primeiro trimestre do ano, mas estava em uma tendência descendente antes de cair abaixo das três principais. Apesar das flutuações, o Acesso Inicial mantém um número moderado de detecções, já que é o objetivo principal dos atores de ameaças obter uma posição de entrada nos sistemas e redes das vítimas alvo.

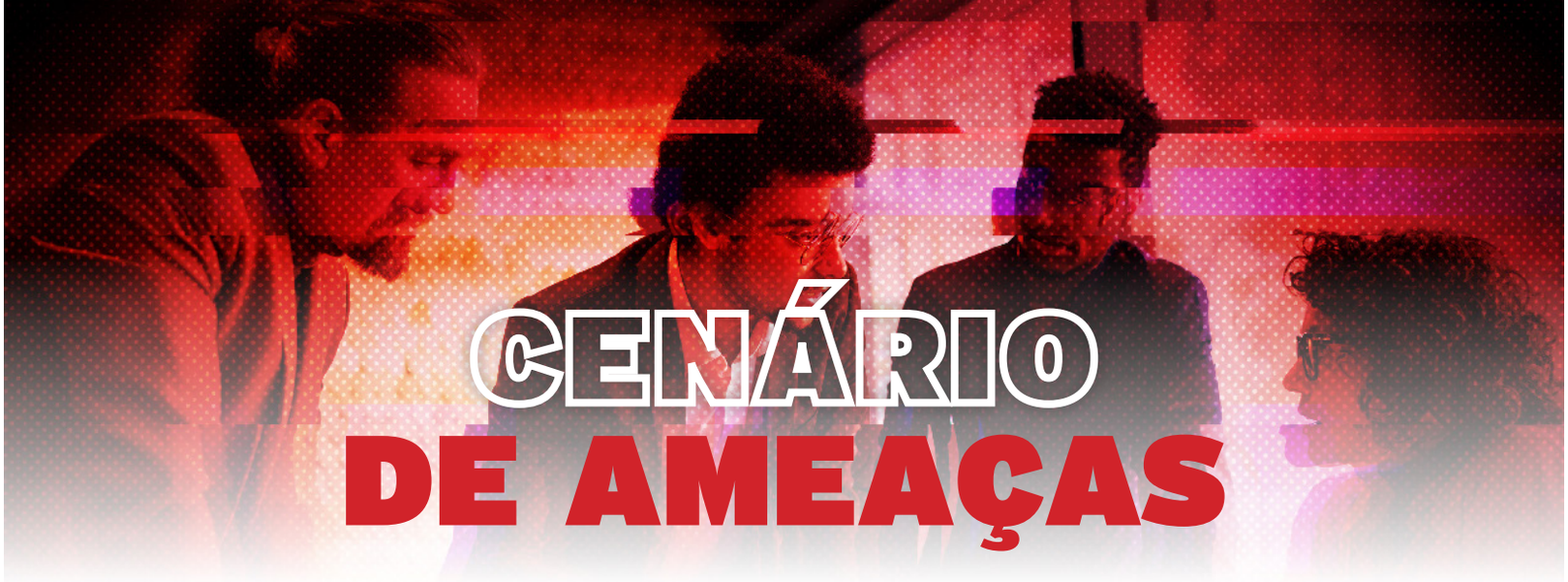
É importante notar que as detecções mensais não mostram dados para maio e junho devido a um erro do sistema ocorrido durante esse período.



Táticas Living-Off-The-Land



Não há uma tendência clara nas detecções, embora Mimikatz e Cobalt Strike continuem sendo as ferramentas legítimas preferidas para abuso e auxílio em atividades criminosas. Pode-se assumir que os atores de ameaças preferem usar ferramentas conhecidas em vez de explorar novas, um comportamento lógico que é comumente observado, já que garante maior probabilidade de sucesso com menos esforço.

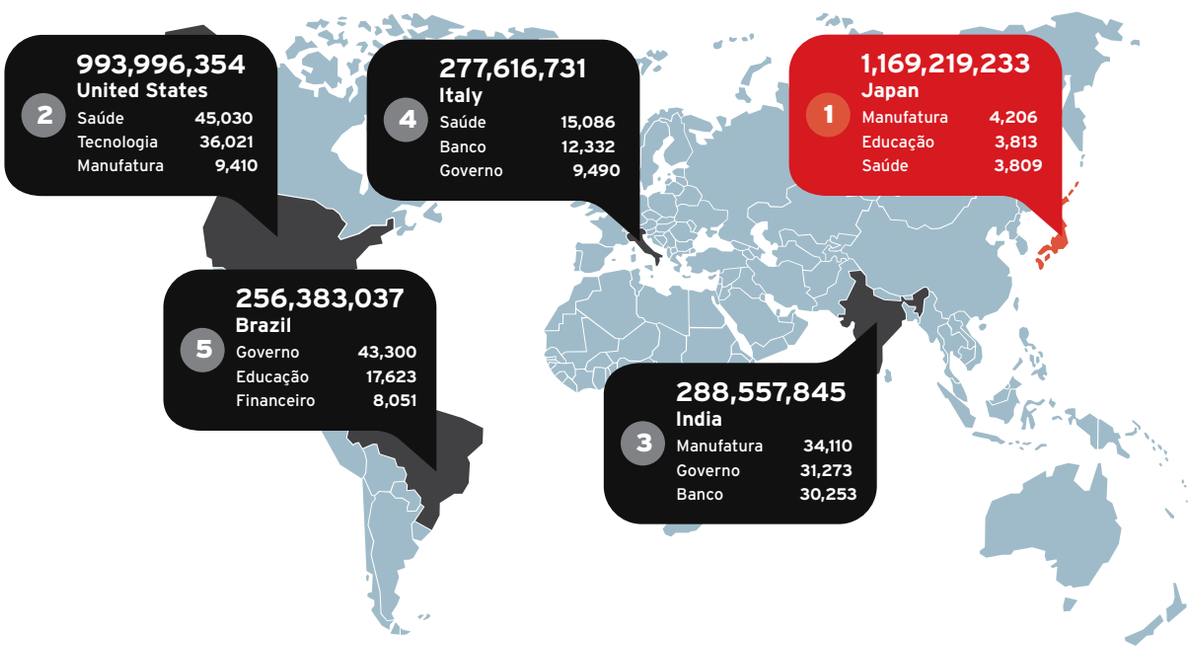


CENÁRIO DE AMEAÇAS

Detecção de Malware

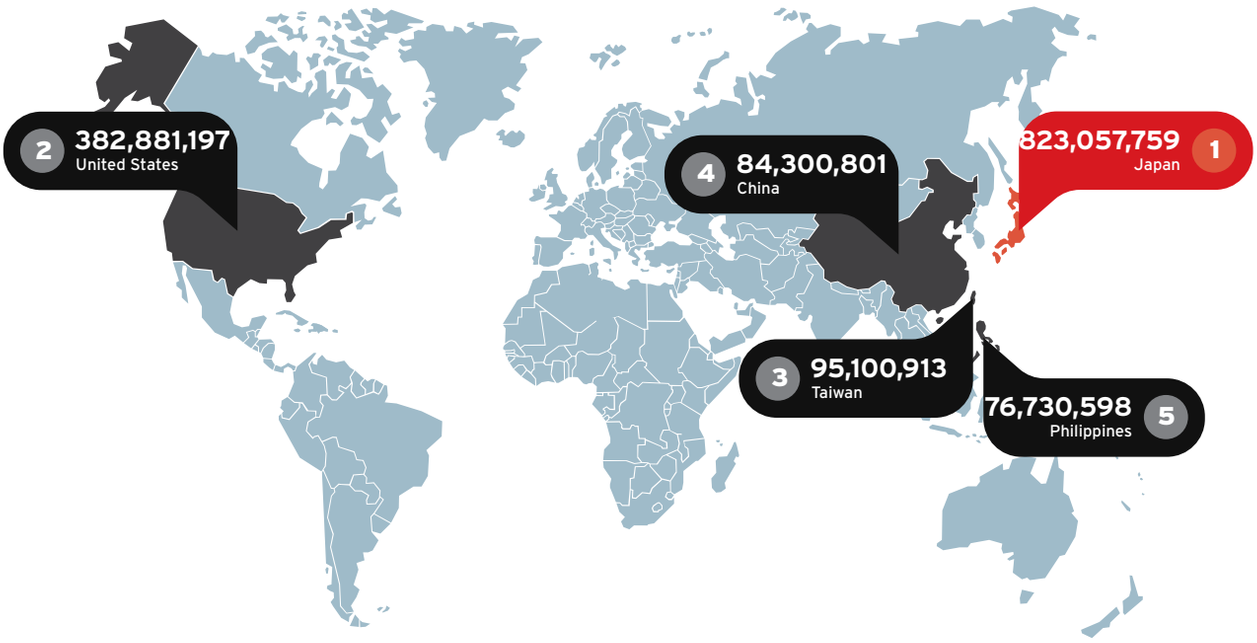
Países com Maior Número de Detecções de Malware

e as principais indústrias visadas em cada um



Observe que as contagens de dados da indústria estão limitadas aos clientes que optaram por fornecer detalhes relacionados aos setores comerciais aos quais pertencem. As contagens totais de detecção de malware incluem clientes que não forneceram nenhuma informação sobre suas indústrias.

Países com Maior Acesso a URLs Maliciosas



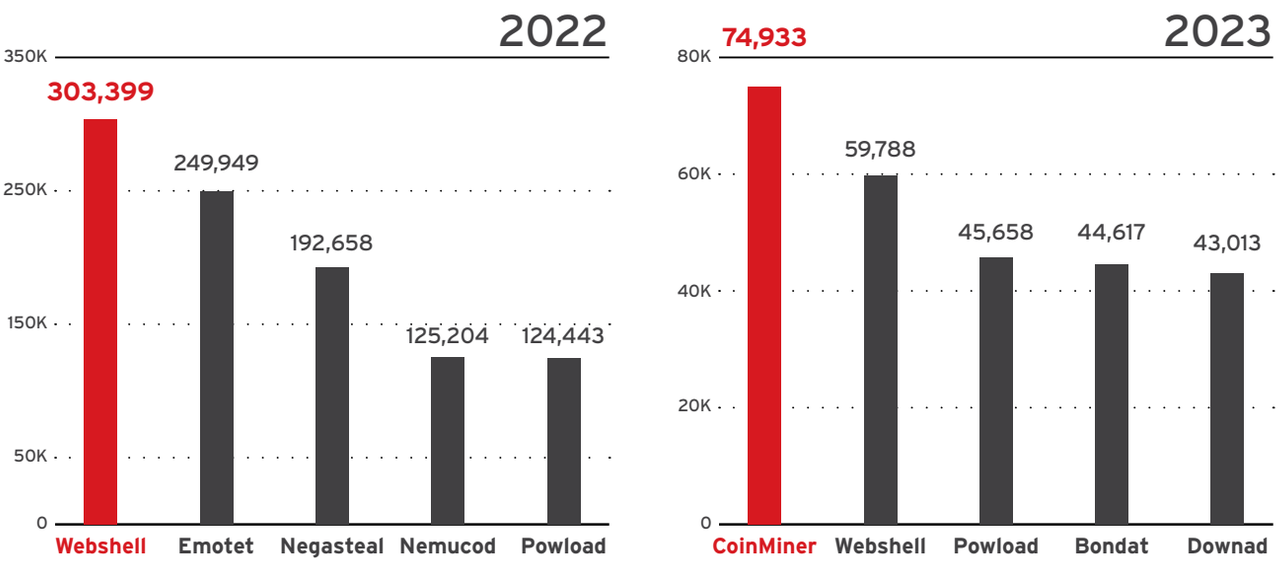
Principais Indústrias Afetadas por Campanhas de Malware

Com base na média agregada dos dados da nossa Rede de Proteção Inteligente (SPN), as campanhas de malware direcionaram principalmente organizações governamentais, com 302.555 detecções.

Principais Famílias de Malware

Um malware de mineração de criptomoedas superou nomes prolíficos em 2023.

Os dados pessoais continuam sendo a mercadoria mais valiosa nas comunidades criminosas underground; carteiras de criptomoedas e dados relacionados a criptos são os dados mais acionáveis que podem ser roubados por atores maliciosos, equivalente a dinheiro que pode ser gasto imediatamente sem rastreabilidade.



O malware de mineração de criptomoedas CoinMiner assume a liderança sobre o famoso Webshell

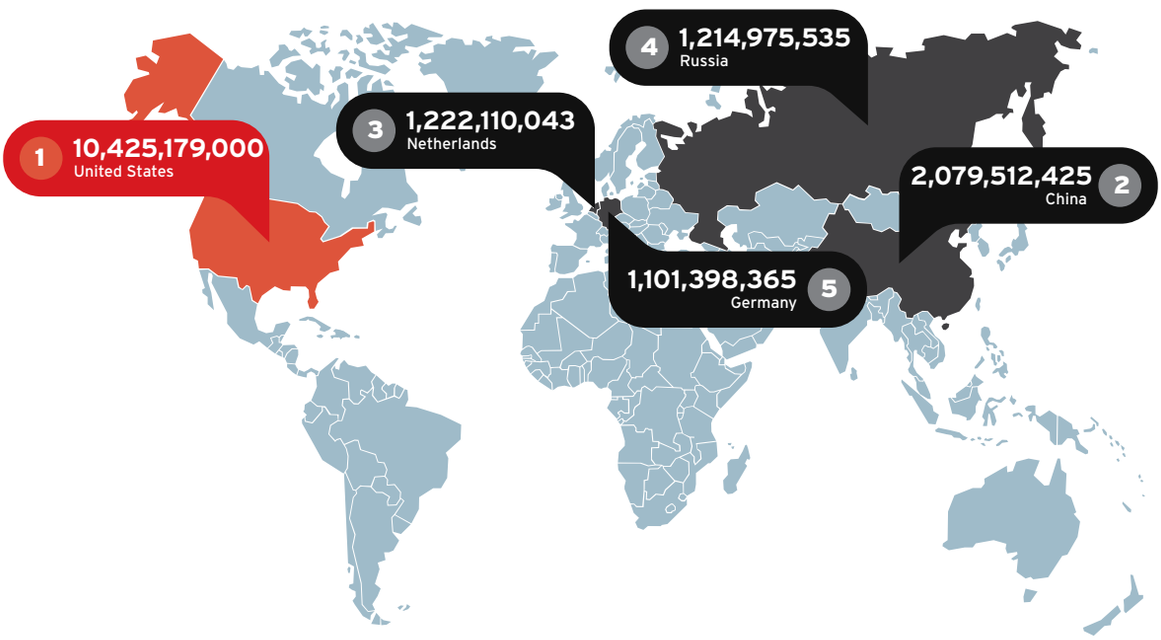
- Último exploit relatado: Vulnerabilidades do Oracle WebLogic Server (CVE-2020-14882)
- Relatado como tendo sido implantado por pacotes maliciosos do Python Package Index visando o Linux
- Utiliza os recursos de processamento central (CPU) e/ou gráficos (GPU) do sistema da vítima para minerar criptomoedas
- Durante a infecção, podem ser observados:
  - Utilização elevada da CPU com powershell.exe ou schtasks.exe
  - Detecção de aplicativo Monero.Cryptocurrency.Miner na rede
  - Origem da execução pode ser identificada durante a instalação do serviço
  - Scripts WMI powershell no servidor DC

Apesar de ter sido superado, o Webshell permanece como uma escolha para atores de ameaças

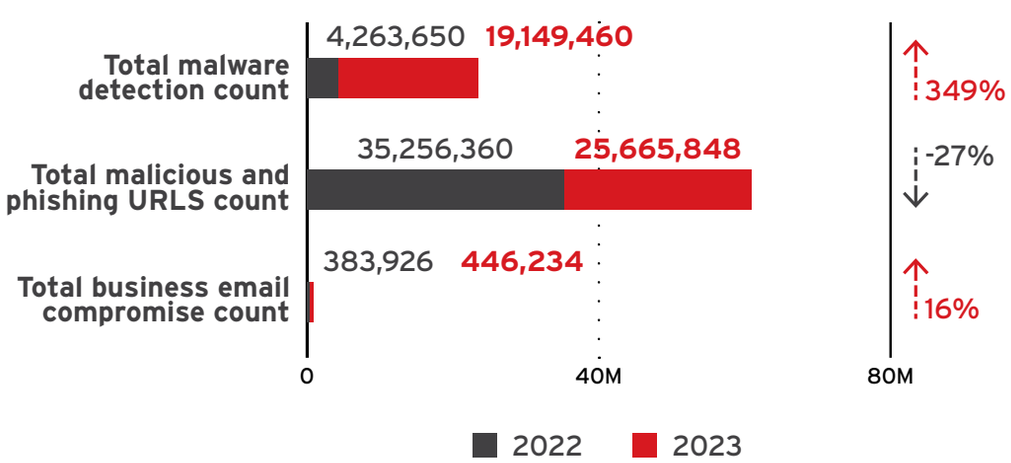
- Explora vulnerabilidades em servidores web expostos à internet

Ameaças por E-mail

Principais Países por Deteção

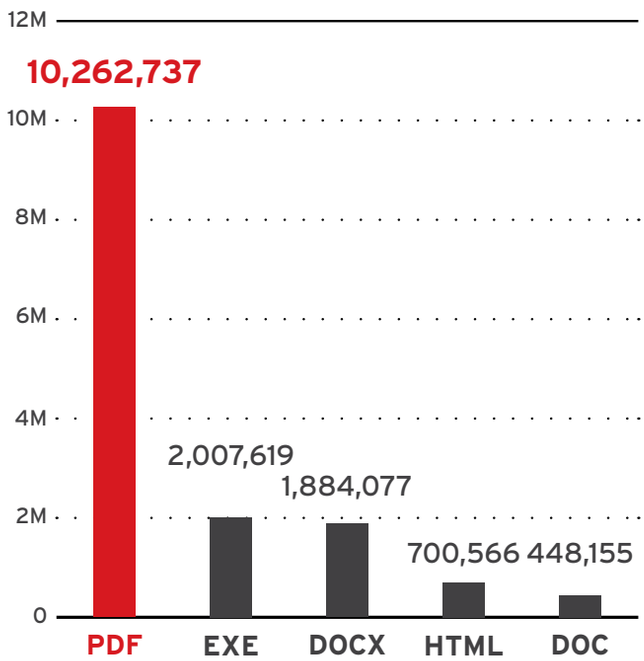


Ameaças de E-mail de Alto Risco

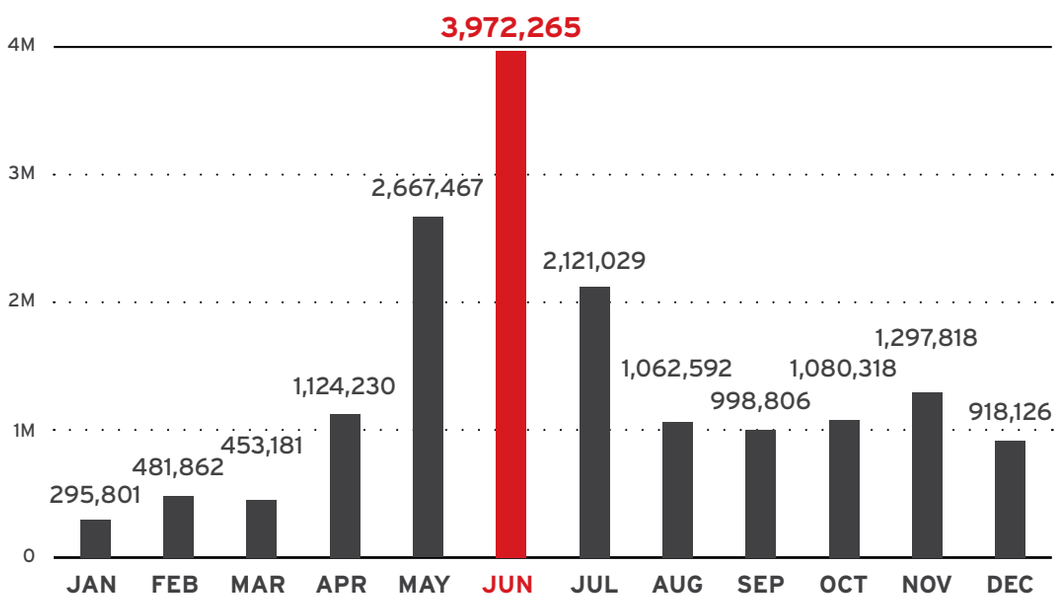


Embora haja uma diminuição nas detecções de URLs maliciosas e de phishing de 2022 para 2023, o aumento no número de detecções de malware e BEC sugere uma mudança no cenário de ameaças, onde os atacantes estão usando maneiras mais sofisticadas de evitar a detecção. Neste caso, em vez de focar em URLs maliciosas e de phishing para vitimar aleatoriamente os usuários, os esquemas de BEC sugerem operações mais direcionadas, enquanto uma análise mais detalhada de nossa contagem de detecção de malware inclui links de phishing incorporados nos anexos. Isso é consistente com os padrões observados em nossos dados da SPN sobre ameaças bloqueadas de 2021 a 2023, onde as detecções que dependem da atribuição de URLs (WRS) e e-mails (ERS) mostram uma diminuição, enquanto as detecções de endpoint que identificam diretamente arquivos maliciosos aumentaram consistentemente.

Os 5 principais anexos de spam

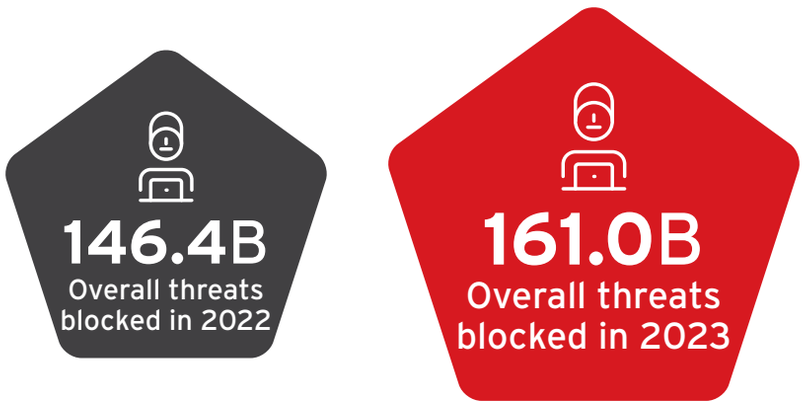


Anexos de spam por mês de 2023

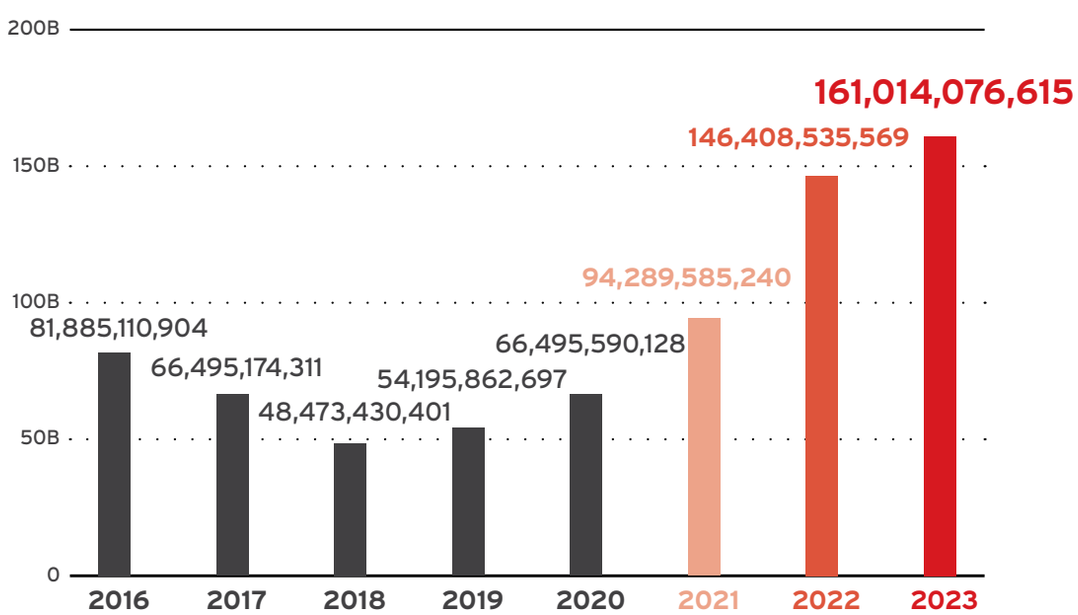


Há uma tendência geral de aumento durante o primeiro semestre do ano, onde as detecções de anexos de spam maliciosos atingiram o pico em junho. Isso é seguido por flutuações no segundo semestre do ano, que eventualmente diminuem até dezembro. Apesar das maneiras mais astutas de atrair vítimas para clicar em links maliciosos, as campanhas de spam continuam sendo uma opção para cibercriminosos.

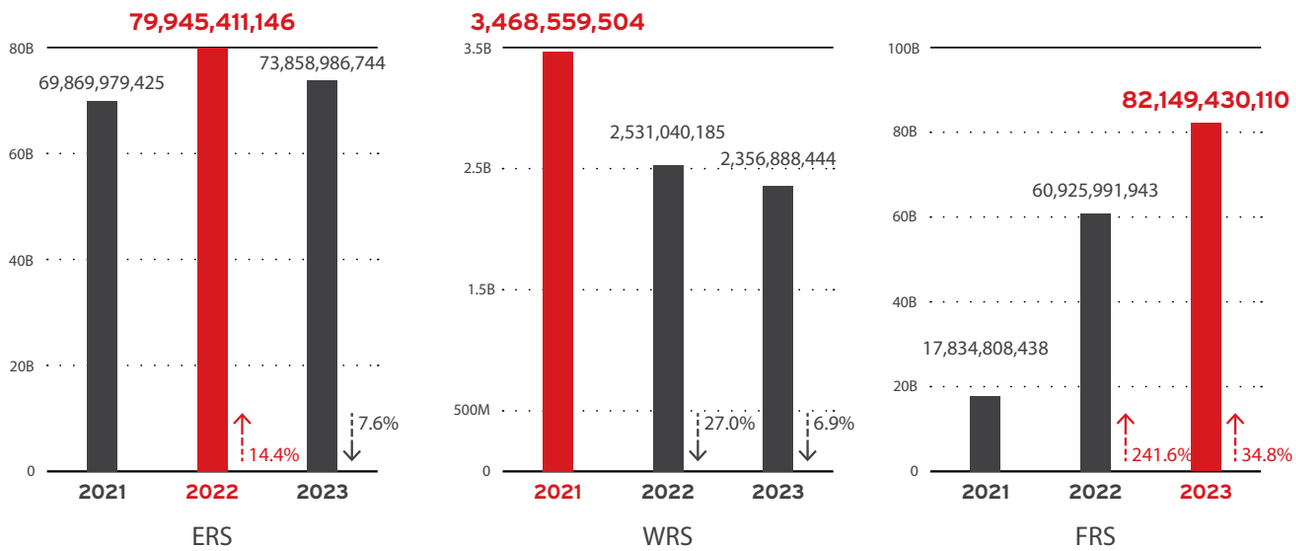
Ameaças Bloqueadas



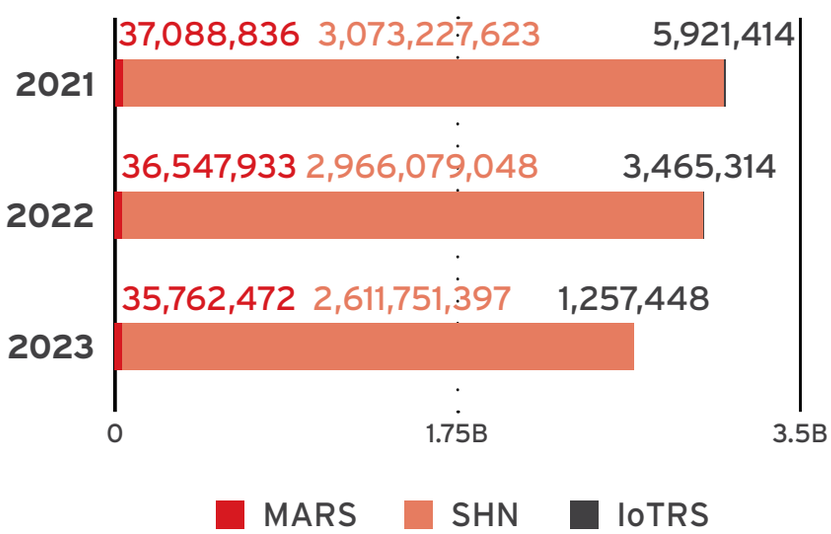
O número total de ameaças bloqueadas com base em nossa SPN alcançou um recorde em 2023, 10% maior do que no ano anterior. Também continua a escalada dramática de ameaças bloqueadas que começou a ser registrada em 2021, o primeiro ano que ultrapassou o pico anterior de 82 bilhões em 2016. Isso coincide com a pandemia, sugerindo fortemente seu papel em impulsionar o aumento..



Apesar do pico geral de ameaças bloqueadas em 2023, há uma tendência fluctuante e de queda nas ameaças bloqueadas sob nosso Serviço de Reputação de E-mail (ERS) e Serviço de Reputação Web (WRS), indicando que as ameaças nessas áreas estão sendo melhor gerenciadas ou são menos frequentes. No entanto, há um aumento contínuo nas ameaças bloqueadas sob nosso Serviço de Reputação de Arquivos (FRS).

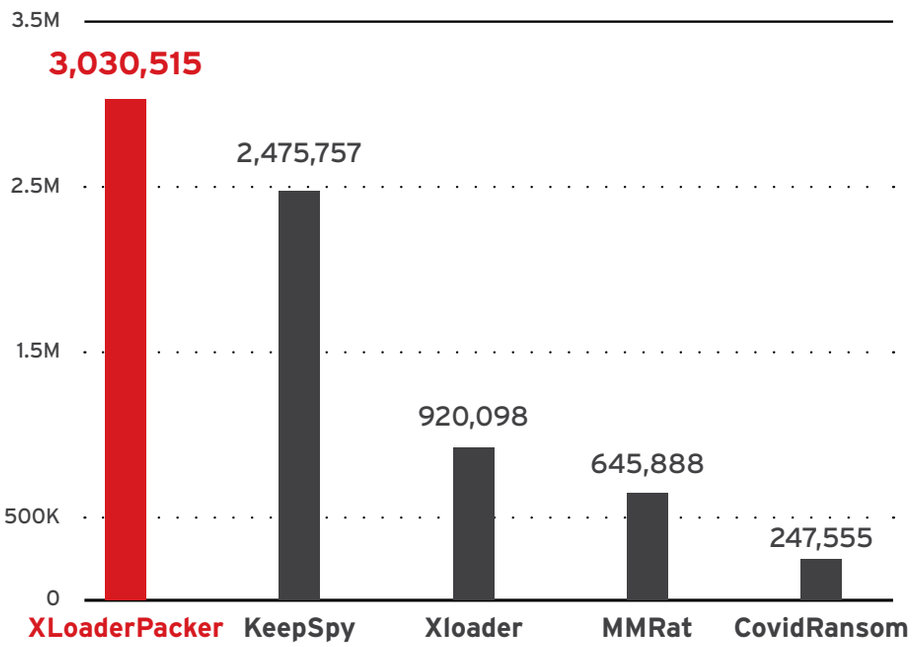


Isso pode ser indicativo da mudança no cenário de ameaças, onde se pode presumir que os atores de ameaças agora optam pela qualidade em vez de quantidade: em vez de lançar ataques em um grupo mais amplo de usuários e depender de vítimas clicando em links maliciosos em sites e e-mails, ataques mais sofisticados são lançados usando especificidade para enganar um campo mais estreito de vítimas de alto perfil. Isso também lhes permite contornar camadas de detecção precoce, como filtros de rede e e-mail. Pode-se especular que isso contribuiu para o aumento contínuo nas detecções de arquivos maliciosos que são detectados nos endpoints.



Também há uma diminuição contínua nas ameaças bloqueadas sob nosso Serviço de Reputação de Aplicativos Móveis (MARS), Rede Doméstica Inteligente (SHN) e Serviço de Reputação da Internet das Coisas (IoTRS), sugerindo que os cibercriminosos estão escolhendo seus alvos cuidadosamente em vez de aleatoriamente. Permanece crucial proteger todas as camadas da superfície de ataque, e os Centros de Operações de Segurança (SOCs) devem compreender que entender as estratégias de direcionamento dos atacantes é importante para uma defesa eficaz.

Familias de Malware para Android

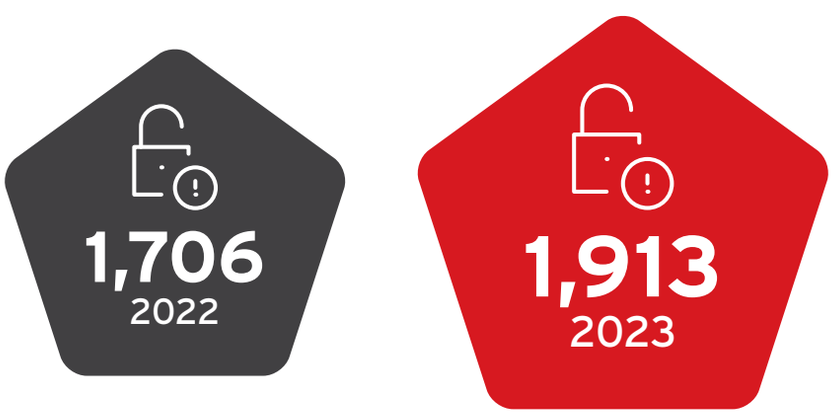


- XLoaderPacker é um spyware que pode ser instalado manualmente por um usuário. Ele se disfarça como um aplicativo Android usando diferentes nomes de aplicativos e, uma vez instalado, pode monitorar chamadas de entrada e saída e bloquear a tela do sistema afetado.
- KeepSpy é carregado lateralmente através de um malware TianySpy entregue via mensagens smishing. Ele também se disfarça como um aplicativo Android usando diferentes nomes de aplicativos e, uma vez instalado, pode coletar credenciais bancárias e configurações de Wi-Fi.

Vulnerabilidades

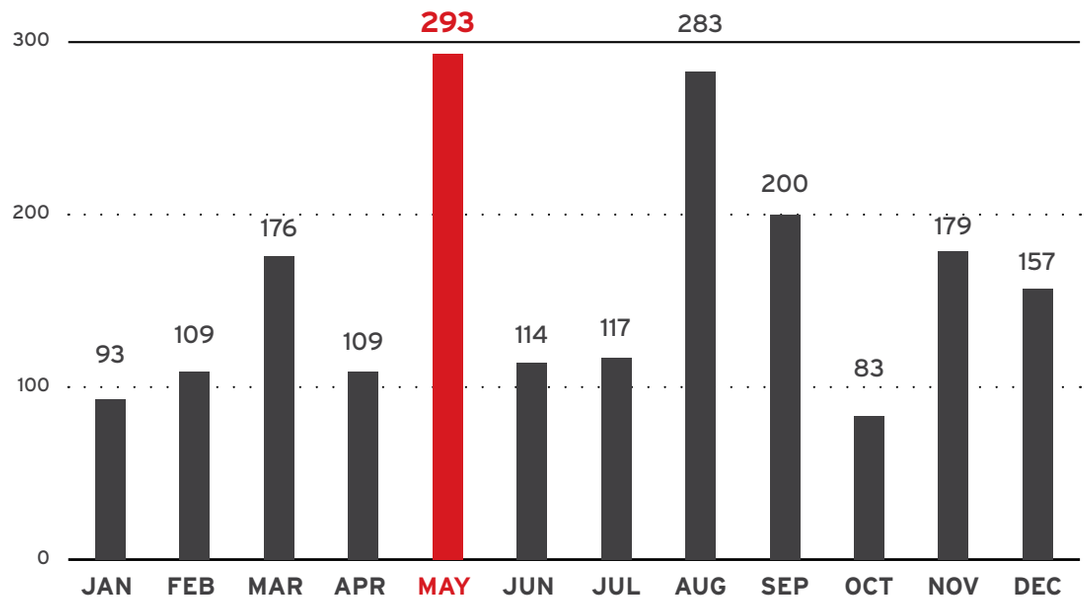
Total de Vulnerabilidades

(Número de avisos de vulnerabilidade publicados pelo Zero-Day Initiative (ZDI))

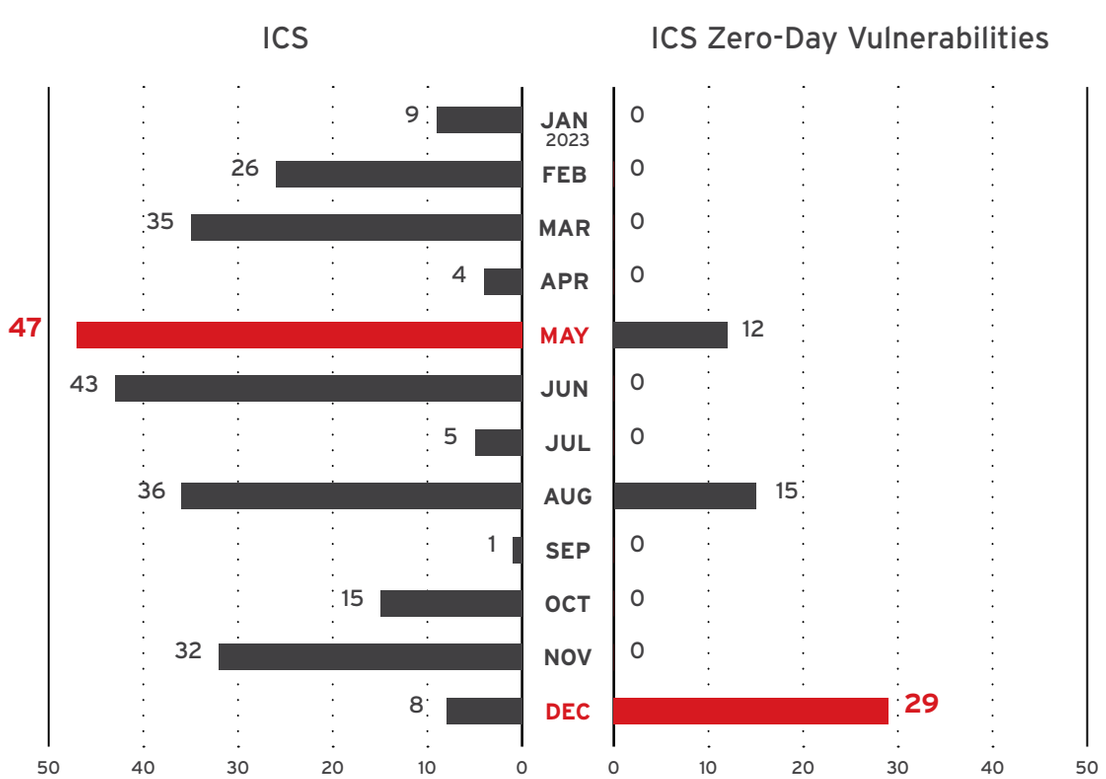


Avisos de Vulnerabilidades Zero-Day (ZDI)

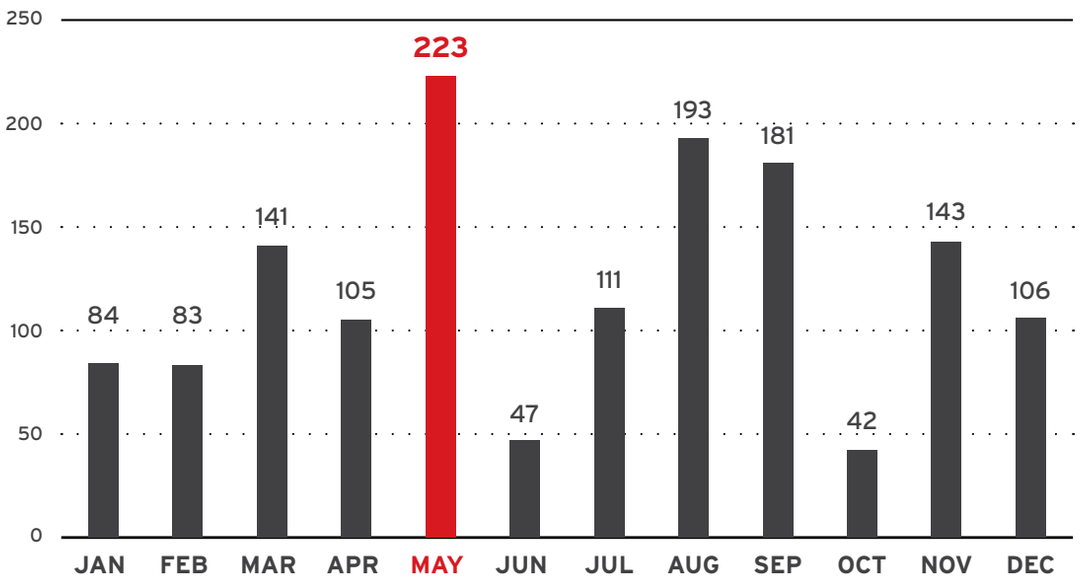
O primeiro trimestre de 2023 começa com avisos de zero-day relativamente baixos, com um aumento significativo até o final do trimestre em março. O segundo trimestre flutua e atinge o pico em maio, enquanto o terceiro trimestre se estabiliza em um nível relativamente alto de atividade. O último trimestre tem o menor número de avisos de zero-day do ano em outubro, volta a subir em novembro, mas mostra uma ligeira queda no último mês, indicando uma possível redução na atividade dos atores de ameaças à medida que o ano terminava.



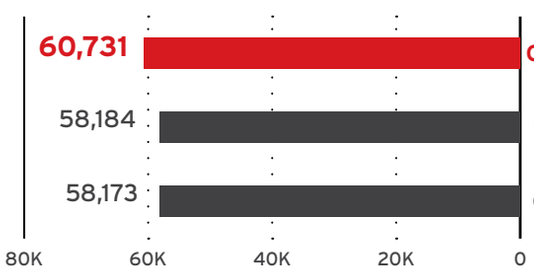
Vulnerabilidades Zero-Day e do Sistema de Controle Industrial (ICS) do ZDI



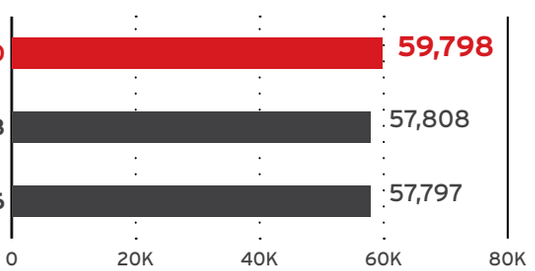
Vulnerabilidades não relacionadas ao Sistema de Controle Industrial (ICS) e Vulnerabilidades N-Day



CVEs mais arriscadas por contagem de clientes



3 CVEs não corrigidas mais arriscadas



CVE-2023-2488 (Vulnerabilidade de Bypass de Segurança do Windows SmartScreen)

- Pontuação base CVSS: 4,4 média

CVE-2023-21823 (Vulnerabilidade de Execução de Código Remoto do Componente Gráfico do Windows)

- Pontuação base CVSS: 7,8 alta

CVE-2023-23376 (Vulnerabilidade de Elevação de Privilégios do Driver de Sistema de Log de Arquivos Comuns do Windows)

- Pontuação base CVSS: 7,8 alta

Eventos de Risco

Dois principais eventos de risco detectados

Os dois principais eventos de risco detectados por meio de nossa gestão de risco da superfície de ataque (ASRM) envolvem aplicativos de nuvem arriscados e o acesso a sites de risco.

82,976,277,500

Acesso a Aplicativos de Nuvem Arriscados

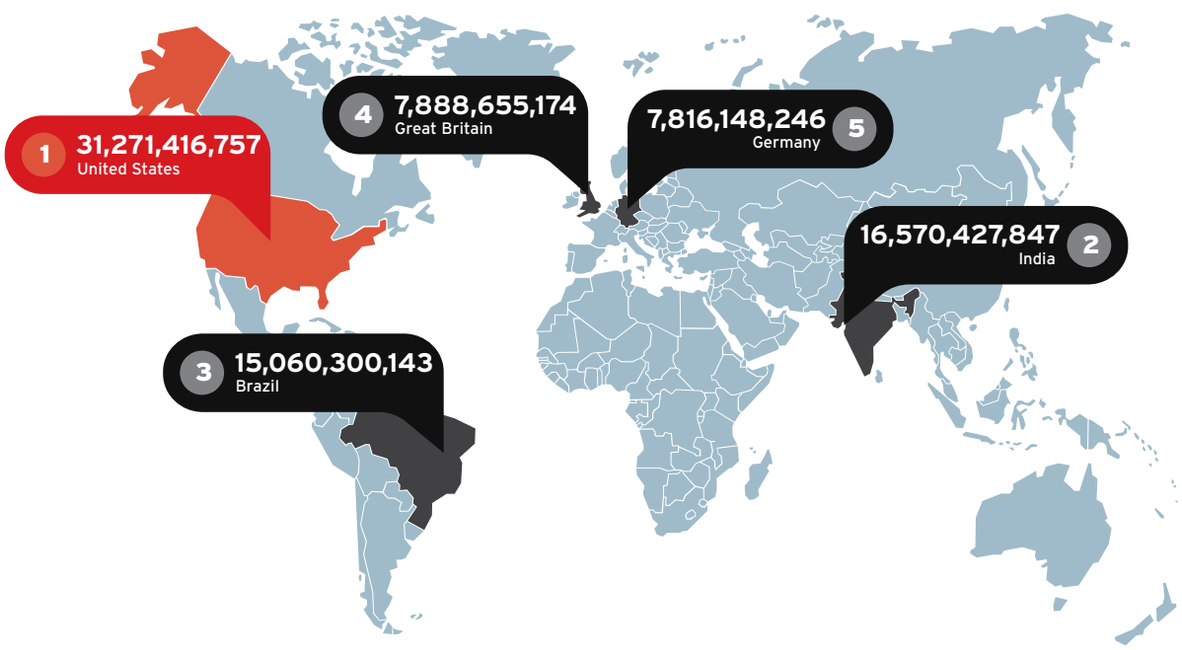
18,819,067,819

Detecção de Acesso a Sites Arriscados

- É recomendada às SOCs uma diligência na monitorização de aplicativos de nuvem acessados por suas redes, especialmente à medida que mais organizações estão integrando ambientes de nuvem em suas operações.
- As equipes de segurança também devem conduzir treinamentos para equipar os usuários finais com o conhecimento necessário para identificar e evitar acessar sites e links arriscados; a negligência humana continua sendo o elo mais fraco na cibersegurança.

Principais Países com Eventos de Risco Detectados

Os Estados Unidos da América registraram a maior quantidade de eventos de risco, com mais de 31,2 bilhões de detecções, quase dobrando o número do país com o segundo maior número de eventos de risco, a Índia, com 16,5 bilhões de detecções.



Recomendações para Reduzir o Risco:

Aplique o patch mais recente ou atualize o seu sistema operacional ou versão do aplicativo.

Aplique regras de prevenção dos produtos da Trend Micro para proteger vulnerabilidades contra exploração.

Otimize configurações fracas no ambiente atual.

Evite acessar o aplicativo relatado como arriscado ou torne o aplicativo um com restrição.

Desative contas com senhas fracas ou redefina-as com senhas fortes. Ative a Política de Bloqueio de Conta no seu Active Directory.

Restrinja o uso da conta de usuário no dispositivo afetado e verifique e resolva as vulnerabilidades do dispositivo de alto risco.

CALIBRATING EXPANSION

RELATÓRIO ANUAL DE CIBERSEGURANÇA 2023

TREND MICRO™

Trend Micro, uma líder global em cibersegurança, ajuda a tornar o mundo seguro para a troca de informações digitais. Impulsionada por décadas de experiência em segurança, pesquisa global de ameaças e inovação contínua, nossa plataforma unificada de cibersegurança protege mais de 500.000 organizações e milhões de indivíduos em nuvens, redes, dispositivos e endpoints.

A plataforma unificada de cibersegurança Trend Vision One™ oferece técnicas avançadas de defesa contra ameaças, detecção e resposta estendidas (XDR) e integração em todo o ecossistema de TI, incluindo AWS, Microsoft e Google, permitindo que as organizações entendam, comuniquem e mitiguem melhor o risco cibernético.

A equipe global de pesquisa de ameaças da Trend Micro oferece inteligência e insights incomparáveis que impulsionam nossa plataforma de cibersegurança e ajudam a proteger organizações em todo o mundo de centenas de milhões de ameaças diariamente.

Contamos com 7.000 funcionários em 65 países, focados exclusivamente em segurança e apaixonados por tornar o mundo um lugar mais seguro e melhor.

A Trend Micro permite que as organizações simplifiquem e protejam seu mundo conectado.

TrendMicro.com