RELATÓRIO DE AMEAÇAS CIBERNÉTICAS

Junho de 2023

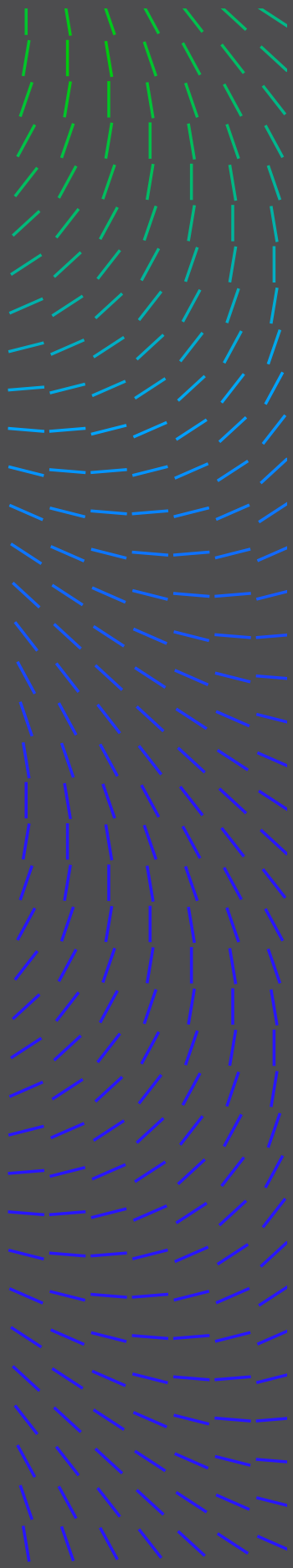
Insights obtidos de uma rede global de especialistas, sensores, telemetria e inteligência

Apresentado por

Trellix ADVANCED RESEARCH CENTER

RELATÓRIO DE AMEAÇAS CIBERNÉTICAS

Este relatório, de autoria do Advanced Research Center da Trellix, (1) destaca insights, inteligência e orientações obtidos de múltiplas fontes de dados críticos sobre ameaças à segurança cibernética e (2) desenvolve interpretações razoáveis e racionais de especialistas desses dados para informar e viabilizar as melhores práticas de defesa cibernética. Esta edição concentra-se em dados e insights capturados entre 1º de janeiro de 2023 e 31 de março de 2023.



As ameaças cibernéticas continuam evoluindo e multiplicando-se. Em velocidade e em escala.

Embora equipes de operações de segurança estejam a postos para defender informações, ativos e operações, nenhuma delas tem uma visão completa e detalhada do cenário de ameaças.

Por que? Obter perspectiva requer um horizonte amplo. Múltiplas fontes. Fluxos de dados. Inteligência bruta. Volumes imensos de telemetria.

Insights reais exigem uma visão estratégica sobre muitas organizações e setores. E regiões. E superfícies de ataque.

Bem-vindo à edição de junho de 2023 do Relatório de ameaças cibernéticas.

COMPREENSÃO DOS RISCOS, AMEAÇAS E VULNERABILIDADES VISADOS – E CAÇADOS ATIVAMENTE – POR ATACANTES

Eu passo bastante tempo falando com membros de conselhos diretores, CEOs, CISOs, CIOs, CTOs e outros líderes responsáveis pela defesa cibernética de nações, órgãos governamentais e organizações privadas de vários setores.

Nós abordamos uma ampla variedade de tópicos – de inteligência, inovação e pesquisa global às práticas de defesa cibernética mais recentes de suas equipes de operações de segurança. Nós falamos sobre seus desafios, recentemente documentados pela Trellix em nossa perspectiva de liderança Mind of the CISO – por exemplo, excesso de fontes diferentes de informação (35%), requisitos regulatórios variáveis (35%), superfícies de ataque crescentes (34%), escassez de funcionários qualificados (34%) e falta de adoção e uso por outras partes da empresa (31%).[1]

Quase todas essas interações tratam, direta ou implicitamente, da natureza do ambiente de ameaças. Quais tipos de ataques estão ocorrendo? Quais são os grupos de ransomware mais impactantes? Quais vulnerabilidades são visadas? Quais países parecem ser os mais ativos? Quais tendências de ameaças estamos rastreando na segurança de e-mail e de rede?

> "Para um membro de diretoria, CEO, CISO, CIO, CTO ou membro de equipe de operações de segurança, esse conhecimento – compartilhado neste relatório e pela ampla biblioteca de orientações, informações e perspectivas da Trellix – é, frequentemente, fundamental para a sua missão."

Na Trellix temos muito a compartilhar porque estamos todos os dias na linha de frente. Temos acesso a um reservatório imenso de inteligência sobre segurança, insights e dados obtidos de mais de um bilhão de sensores no mundo todo. Para um membro de diretoria, CEO, CISO, CIO, CTO ou membro de equipe de operações de segurança, esse conhecimento – compartilhado neste relatório e pela ampla biblioteca de orientações, informações e perspectivas da Trellix – é, frequentemente, fundamental para a sua missão.

Meu colega John Fokker, que lidera o trabalho de inteligência sobre ameaças dentro da equipe de elite do Advanced Research Center da Trellix, compilou este excelente relatório. Use estes insights para dar foco à sua equipe, aprimorar seus processos e implantar as tecnologias de XDR certas. Mantenha-nos informados sobre onde deve ser o foco das edições futuras para ajudar a manter a sua organização segura, protegida e próspera.

Joseph (Yossi) Tal
VICE-PRESIDENTE SÊNIOR E CHEFE DO
TRELLIX ADVANCED RESEARCH CENTER

EM APOIO AOS HERÓIS DAS LINHAS DE FRENTE DA SEGURANÇA CIBERNÉTICA

Eu trabalho com heróis. Não me refiro à minha equipe, embora eles tenham demonstrado ter superpoderes no decorrer de suas várias carreiras nos setores público e privado.

Estou me referindo a você. Estou falando de pessoas e equipes do mundo todo que contam com as capacidades avançadas de pesquisa da Trellix – nossos sistemas, insights e inteligência – para proteger suas organizações contra ataques cibernéticos. CISOs, CTOs e CIOs, sim, bem como nossos colegas em agências como Europol, FBI e NSA, a Cybersecurity and Infrastructure Security Agency (CISA), o Cyber Security Centre (ACSC) da Austrália e o National Cyber Security Centre (NCSC-UK) do Reino Unido. Igualmente – e talvez até mais – importante, estou falando de cada membro da sua equipe de operações de segurança.

"Como você bem sabe pelo dia a dia do seu trabalho, a segurança cibernética está evoluindo com uma rapidez notável. Avanços tecnológicos e uma migração forte rumo à XDR."

O que você acha que pode virar o jogo para a sua missão de operações de segurança? Segundo relatório da Trellix que meu colega Yossi mencionou anteriormente, líderes de segurança cibernética do mundo todo compartilharam seus pontos de vista sobre isso. Eles incluíram melhor visibilidade (44%), priorização mais forte do que importa (42%), colaboração mais ampla para lidar com ataques multivetoriais (40%) e precisão aprimorada (37%).[2]

Cada um desses fatores depende fundamentalmente de dados, informações e insights precisos – como o conteúdo deste relatório.

Como você bem sabe pelo dia a dia do seu trabalho, a segurança cibernética está evoluindo com uma rapidez notável. Avanços tecnológicos e uma migração forte rumo à XDR. Mudanças em regulamentos, de leis a responsabilidade civil. Mudanças no ambiente de ameaças. Há uma revolução em curso, uma transformação na forma como as equipes de operações de segurança podem se manter "um passo à frente" da próxima geração de ataques cibernéticos. A vitória sempre começa com insights, com uma compreensão de nosso estado atual.

Estamos juntos nisso. Você pode contar com a Trellix. Este relatório é para você.

John Fokker
CHEFE DE INTELIGÊNCIA SOBRE AMEAÇAS
E ENGENHEIRO-CHEFE DO
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, "Relatório de 2023: The Mind of the CISO", 2023.
[2] Trellix, "Relatório de 2023: The Mind of the CISO", 2023.

INTRODUÇÃO

Contexto estratégico: um mundo instável

Interpretar os dados deste relatório requer uma compreensão do "panorama geral" em escala global. Porque ameaças cibernéticas a organizações do mundo todo não ocorrem em um vácuo técnico. Entre os vários elementos que contribuem para o risco cibernético estão guerras e outros motivos de força maior, mudanças em grande escala de ciclos econômicos e novas vulnerabilidades que podem surgir sempre que uma equipe introduz mudanças em fatores como modelos de negócios, parcerias importantes, processos fundamentais, adoção de tecnologias e conformidade regulatória. Uma amostra dos fatores que influenciam nossos dados de ameaças no primeiro trimestre de 2023 inclui:

A invasão da Ucrânia pela Rússia e a guerra assimétrica contra o Ocidente: a atividade cibernética para fins de espionagem, guerra e desinformação a serviço de ambições políticas, econômicas e territoriais de grandes países continua aumentando. Hackers utilizam ataques cibernéticos cada vez mais sofisticados contra empresas, governos e infraestruturas do Ocidente.

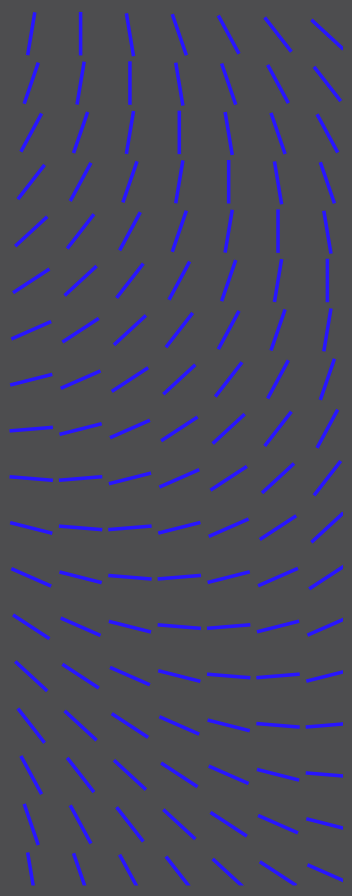
O controle consolidado de Xi Jinping sobre a China e suas aspirações geopolíticas: os objetivos nacionalistas, a política externa assertiva e as práticas de espionagem corporativa da China continuam a causar riscos cibernéticos enquanto grupos de ameaças persistentes avançadas (APTs) ligados à China dominam o cenário global.

Economias em desenvolvimento e expansão rápida de infraestruturas: quando muitas regiões em desenvolvimento expandem suas tecnologias e infraestruturas para acompanhar seu crescimento econômico, a segurança cibernética não costuma ser uma prioridade – o que resulta em muitas vulnerabilidades cibernéticas em infraestruturas críticas.

Inflação global e seus impactos políticos e econômicos: este trimestre incluiu volatilidade de mercado, crises financeiras e políticas e pressões sobre prioridades de gastos e orçamentos de segurança cibernética.

Continuação de perturbações em cadeias de fornecimento após a COVID: novos caminhos para mercados de várias regiões exigiram mudanças em parceiros, redes de transportes, compartilhamento de informações e – por extensão – no risco cibernético. Como as ameaças cibernéticas estão afetando as cadeias de fornecimento diariamente, a necessidade de capacidades de confiança zero continua forte em vários setores.

O mito do ambiente de segurança superior da Apple: este persiste, apesar do fato de que os ambientes macOS não podem mais ser considerados seguros, visto que perpetradores de ameaças começam a utilizar malware baseado em Golang em grande escala e a expandir vetores de ataque para abranger vários sistemas operacionais.



O advento da inteligência artificial no mundo todo, prometendo revolucionar tudo: a defesa cibernética é auxiliada e prejudicada por avanços em autoaprendizagem, processamento de linguagem natural e outros avanços. Conforme as ameaças cibernéticas globais evoluem e ocorrem em escala mais rapidamente que as equipes humanas podem gerenciar, as soluções de inteligência artificial tornam-se vitais para a defesa cibernética das empresas.

Segurança cibernética: os desafios do CISO e a revolução das operações de segurança

Quais são os desafios mais críticos para profissionais de segurança cibernética e equipes de operações de segurança? Absorver a inteligência sobre ameaças obtida – com rapidez e em escala – e enviar imediatamente insights decisivos para as equipes de caça a ameaças e forças-tarefa das organizações.

O objetivo da Trellix? Simplificar essa jornada.

Como? Oferecendo o nível de automação necessário para obter as respostas de que as organizações precisam para se concentrar em capacidades de caça a ameaças e operações de segurança incorporadas em nossos produtos de XDR, proteção de hosts, rede e e-mail, utilizando nossa inteligência superior contra ameaças.

O ambiente de ameaças do primeiro trimestre deste ano também foi influenciado por fatores internos, muitos dos quais refletem desafios constantes enfrentados pelos líderes de segurança cibernética e pelas equipes de linha de frente.

Tecnologia ultrapassada: muitas organizações continuam a contar com tecnologias tradicionais, como SOAR e SIEM. Com efeito, 96% dos CISOs afirmam que precisam de soluções melhores para proteger suas organizações contra ameaças cibernéticas.[3]

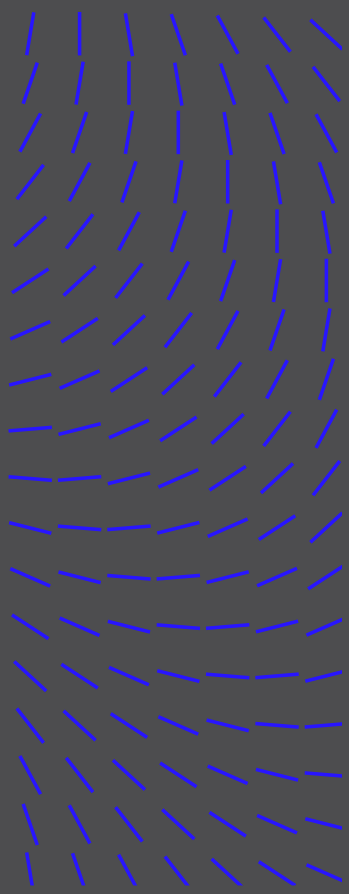
Um mar de ferramentas de segurança: as equipes de operações de segurança são sobrecarregadas por um excesso de alertas e pela falta do que precisam para priorizar seu tempo. As organizações empregam, em média, uma mistura confusa de 25 ferramentas e soluções de segurança.[4]

Fadiga de alertas: sob uma enxurrada de alertas, as equipes de operações de segurança enfrentam dificuldades com priorização de alertas, falsos positivos e alertas perdidos. Segundo o IDC, 35% ignoram alertas – talvez, em parte, porque 45% são falsos positivos.[5]

Recursos insuficientes: com recursos e qualificações limitados para as operações de segurança, é difícil combater ameaças efetivamente. Qual é o tempo médio de permanência de um analista de SOC? Aproximadamente dois anos.[6]

Metodologia: como coletamos e analisamos dados

Os especialistas de nível internacional do Advanced Research Center da Trellix coletam as estatísticas, tendências e insights que compõem este relatório de uma ampla variedade de fontes globais, tanto reservadas quanto abertas. Os dados agregados são fornecidos a nossas plataformas Insights e ATLAS. Por meio do uso de autoaprendizagem, automação e perspicácia humana, a equipe percorre um conjunto intensivo, integrado e iterativo de processos – normalizando os dados, analisando as informações e desenvolvendo insights significativos para líderes de segurança cibernética e equipes de operações de segurança nas linhas de frente da segurança cibernética no mundo todo. Para uma descrição mais detalhada de nossa metodologia, leia o final deste relatório.



Aplicação: como usar estas informações

É imperativo que toda equipe líder do setor compreenda, reconheça e, sempre que possível, mitigue os efeitos do prejulgamento – a propensão natural, internalizada ou invisível de aceitar, rejeitar ou manipular fatos e seus significados. O mesmo preceito aplica-se aos consumidores do conteúdo.

Diferente de um experimento ou teste matemático altamente estruturado e com bases comparativas, este relatório é, por sua própria natureza, uma amostra de conveniência – um tipo de estudo não probabilístico frequentemente utilizado em testes médicos, psicológicos e sociológicos que fazem uso de dados disponíveis e acessíveis.

Em suma, nossas descobertas baseiam-se no que podemos observar e certamente não incluem evidências de ameaças, ataques ou táticas que evadiram detecção, geração de relatórios e captura de dados.

Na falta de informações "completas" ou de visibilidade "perfeita", este é o tipo de estudo mais adequado para o objetivo deste relatório: identificar fontes conhecidas de dados críticos sobre ameaças à segurança cibernética e desenvolver interpretações racionais, especializadas e éticas desses dados que informem e viabilizem as melhores práticas de defesa cibernética.

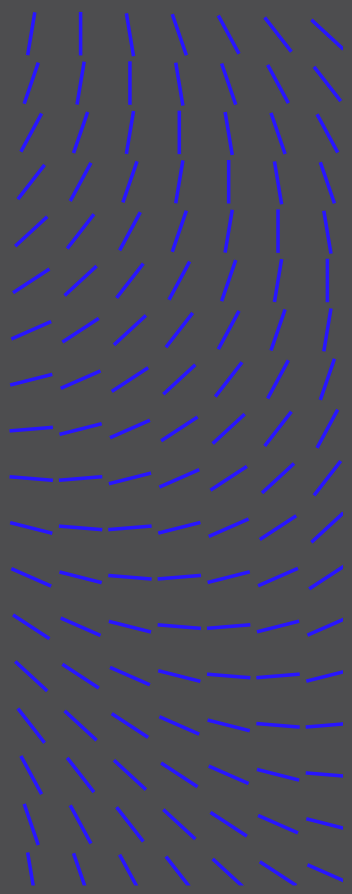
Um aspecto fundamental dessa ética investigativa é o seguinte:

Um momento no tempo: ninguém tem acesso a todos os logs de todos os sistemas conectados à Internet, nem todos os incidentes de segurança são relatados e nem todas as vítimas são extorquidas e incluídas nos sites de vazamentos. Contudo, rastrear o que podemos resulta em uma compreensão melhor das várias ameaças, enquanto reduz pontos cegos analíticos e investigativos.

Falsos positivos e falsos negativos: entre as características técnicas de alto desempenho dos sistemas especiais de rastreamento e telemetria para coleta de dados da Trellix estão mecanismos, filtros e táticas que ajudam a combater ou remover resultados falsos positivos e negativos. Essas características ajudam a elevar o nível da análise e a qualidade de nossas descobertas.

Detecções, e não infecções: quando falamos em telemetria, referimo-nos a detecções, e não a infecções. Uma detecção é registrada quando um arquivo, URL, endereço IP ou outro indicador é detectado por um de nossos produtos e relatado para nós.

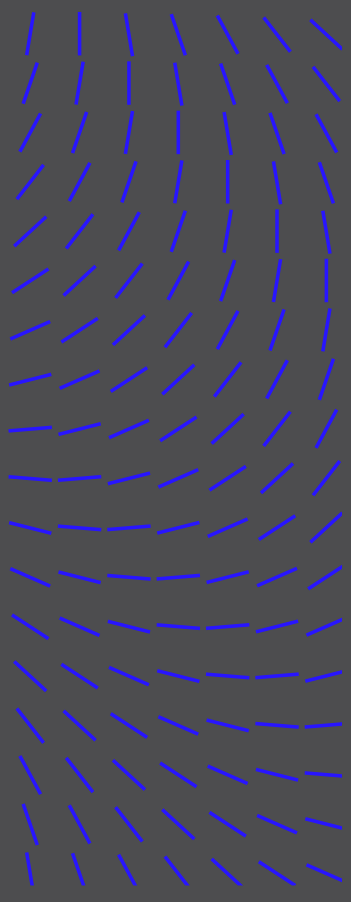
Captura de dados não uniforme: alguns conjuntos de dados exigem uma interpretação cuidadosa. Dados de telecomunicações, por exemplo, incluem telemetria de clientes provedores de serviços de Internet que atuam em vários outros setores e indústrias.



Atribuição a países: da mesma forma, determinar a responsabilidade de países por várias ameaças e ataques cibernéticos pode ser muito difícil, considerando-se a prática comum entre criminosos cibernéticos e hackers patrocinados por países de se fazerem passar uns pelos outros ou de disfarçar atividades maliciosas como se originassem de uma fonte confiável.

O caminho à frente: orientação e recursos

O que as informações contidas neste relatório significam para os heróis da segurança cibernética nas linhas de frente? Insights e dados de segurança cibernética só são úteis quando transformados em ações – resultando em redução de riscos, melhora na tomada de decisões ou aumento da eficiência ou da economia das atividades das operações de segurança. Para orientação e recursos adicionais, visite www.trellix.com.



[3] Trellix, "Relatório de 2023: The Mind of the CISO," 2023
[4] Trellix, "Relatório de 2023: The Mind of the CISO," 2023
[5] IDC, The Voice of the Analysts, 2021
[6] Ponemon Institute, 2020

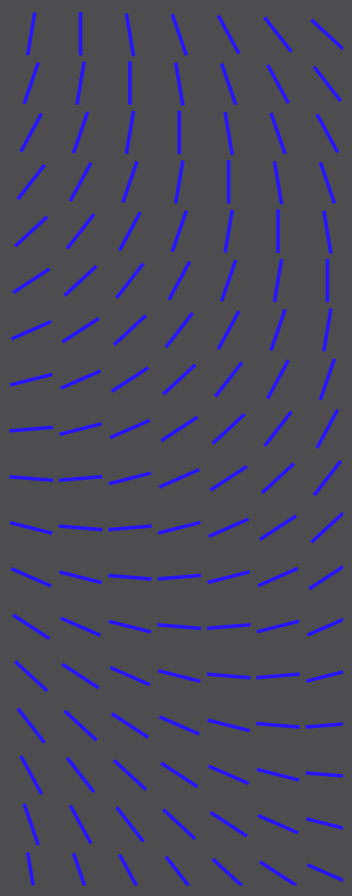
RESUMO DOS DESTAQUES DO 1° TRIMESTRE DE 2023

O cenário do ransomware

- **A onda do ransomware:** O ransomware continua na liderança como principal tipo de ataque cibernético em todo o mundo. Golpes de engenharia social para enganar e induzir pessoas a divulgar informações confidenciais ou pessoais, como é o caso do phishing, continuam mais frequentes do que nunca, mesmo estando mais sofisticados.
- **Cuba e Play dominam:** embora tenhamos observado uma queda nas atividades de criminosos cibernéticos relacionadas a ransomware no início do ano, as famílias de ransomware predominantes no primeiro trimestre foram Cuba (9%) e Play (7%).
- **O LockBit perdura:** apesar de uma redução de atividade durante dois trimestres seguidos, o LockBit continua sendo o ransomware mais agressivo ao pressionar suas vítimas a fazer pagamentos de resgate.
- **Magecart Group possivelmente em alta?** Relatos públicos indicam que as atividades desse grupo de roubo de cartões de crédito e fraudes de comércio eletrônico aumentaram incrivelmente no primeiro trimestre de 2023. Essa ameaça opera no mesmo nível de atividade que outras APTs ligadas a governos de países, possivelmente indicando um ressurgimento do Magecart Group mundialmente.

Evolução das táticas de ransomware

- **Objetivos monetários:** não é surpreendente que as motivações do ransomware continuem sendo financeiras; os setores de seguros (20%) e de serviços financeiros (17%) registraram o maior número de detecções de ataques em potencial.
- **Empresas médias mais afetadas:** avaliações de nossos dados de sites de vazamentos revelam que as vítimas desses ataques são, principalmente, empresas de médio porte, com apenas 51 a 200 funcionários (32%) e US$ 10 milhões a US$ 50 milhões em receitas (38%).
- **Estados Unidos como alvo principal:** os EUA (15%) foram o país mais afetado por grupos de ransomware. Foram também o país com o mais alto percentual de vítimas corporativas (48%) que decidiram "comprar seus dados de volta" dos atacantes – um percentual seis vezes maior que o país seguinte da lista, o Reino Unido.
- **Cobalt Strike como arma preferida:** a telemetria da Trellix identifica essa ferramenta como grande favorita dos perpetradores de ransomware (28% dos incidentes). Ela parece estar crescendo em uso e popularidade entre esses grupos, apesar das tentativas do fornecedor Fortra de dificultar seu uso por perpetradores de ameaças, no final do quarto trimestre de 2022.



Alertas vermelhos estrangeiros

- **Maiores perpetradores:** durante os últimos seis meses, perpetradores de APT vinculados à China, inclusive o Mustang Panda e o UNC4191, foram os mais ativos nos ataques a outros países no primeiro trimestre. Perpetradores de ameaças ligados à China dominaram a cena global, sendo responsáveis por 79,3% de todas as atividades de países, seguidos por perpetradores ligados à Coreia do Norte, Rússia e Irã.
- **Grupo de APT mais ativo:** o Mustang Panda continuou sendo, pelo terceiro trimestre consecutivo, o grupo de APT mais ativo mundialmente (72%) – demonstrando o trabalho cibernético contínuo e crescente da China para fins de espionagem e sabotagem.

Inteligência sobre vulnerabilidades

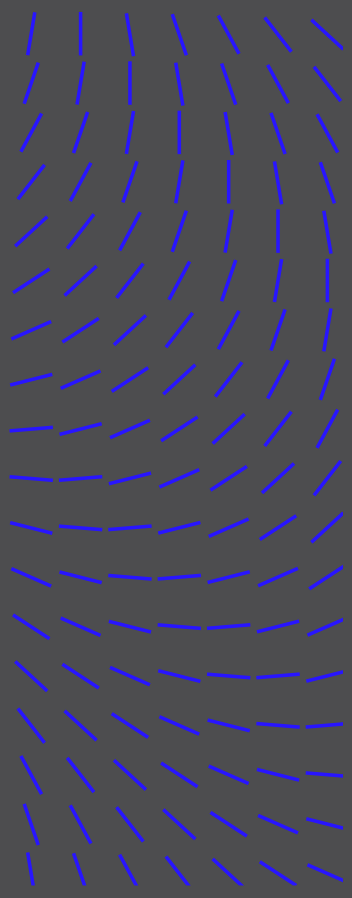
- **Vulnerabilidades conhecidas não resolvidas:** a maioria das vulnerabilidades mais críticas deste trimestre consistiram em vulnerabilidades conhecidas e ainda não resolvidas.
- **Notícias de ontem:** no caso de uma vulnerabilidade da Apple divulgada em fevereiro deste ano, a origem do bug remonta à exploração FORCEDENTRY, utilizada pelo NSO Group como parte de seu spyware Pegasus e divulgada em 2021.

Segurança de e-mail

- **Novas rotas de ataque:** embora a Microsoft tenha começado a bloquear anexos com macros na plataforma Office, os perpetradores de ameaças logo começaram a adotar novos meios para que infecções continuem visando dispositivos com Windows – como envenenamento de SEO, OneNote e anexos no formato Zip.
- **Marcas não confiáveis:** além de e-mails de phishing genéricos, malfeitores estão cada vez mais utilizando nomes de marcas e serviços legítimos, como PayPal, Google, DWeb e IPFS, para enganar as vítimas e roubar suas credenciais on-line.

Acesso indevido à nuvem

- **Uma mudança de tática:** ataques a infraestruturas de nuvem continuam em alta, conforme mais e mais empresas migram de infraestruturas locais para opções mais econômicas e expansíveis da Amazon, Microsoft, Google e outras.
- **Contas válidas:** embora ataques mais sofisticados com autenticação por múltiplos fatores, proxies e execução de API estejam em alta, a técnica de ataque predominante continua sendo o uso de contas válidas, com o dobro da frequência do segundo vetor de ataque mais utilizado. Isso enfatiza que o risco do acesso ilegítimo é real, enquanto criminosos cibernéticos acessam e vendem logins de contas e sites legítimos para fins de infiltração e realização de ataques.



ANÁLISES, INSIGHTS E DADOS DO RELATÓRIO

Incidentes de segurança

Os incidentes de segurança discutidos nesta seção baseiam-se em relatos públicos. No primeiro trimestre de 2023, binários do Windows, ferramentas de terceiros, malware personalizado e ferramentas de teste de penetração continuaram a afetar operações enquanto perpetradores de ameaças exploravam rotas de menor resistência. PowerShell e o shell de comandos do Windows continuaram sendo aproveitados para disseminar tarefas ligadas a persistência, distribuição e extração.

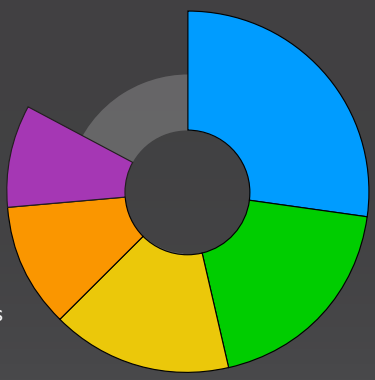
PRINCIPAIS BINÁRIOS DE WINDOWS UTILIZADOS EM EVENTOS NO 1° TRIMESTRE DE 2023

1. PowerShell
2. CMD do Windows
3. Tarefa agendada
4. RunDLL32
5. WMIC

Agendamento de tarefas, inserção de arquivos DLL maliciosos e execução de comandos por meio da instrumentação de gerenciamento do Windows ficaram entre os cinco primeiros colocados. Binários desprotegidos e não monitorados, executados por scripts ou manualmente via teclado, continuaram a ser utilizados por perpetradores de ameaças por já estarem à sua disposição.

Em muitos casos, ferramentas de terceiros, freeware e ferramentas de teste de penetração participam do ciclo de vida de um ataque ajudando perpetradores de ameaças a configurar persistência, executar scripts, descobrir e coletar informações visadas e ampliar privilégios para acessar ativos ou dados que, de outra forma, estão inacessíveis para contas restritas. Além disso, quando utilizados para ampliação de privilégios, um atacante pode executar processos de instalação com privilégios elevados e acessar áreas, ativos ou dados que, de outra forma, não estão acessíveis para contas restritas.

PRINCIPAIS FERRAMENTAS DE TERCEIROS UTILIZADAS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

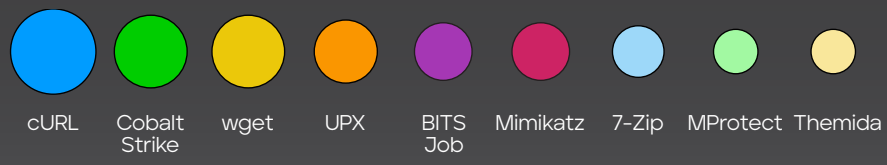


CATEGORIAS DE FERRAMENTAS

- Transferência de arquivos
- Acondicionadores de software
- Ferramentas de exploração de postagens
- Ferramentas de acesso remoto
- Utilitários de compactação

FERRAMENTAS DE TERCEIROS UTILIZADAS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

FERRAMENTAS ESPECÍFICAS



As ferramentas de terceiros mais nocivas, como Cobalt Strike, Mimikatz e Sharphound são utilizadas, tanto legitimamente quanto por perpetradores de ameaças, para coletar senhas, estabelecer beacons e ampliar privilégios. Assim que compromete um ambiente, o atacante pode utilizar ferramentas de transferência de arquivos, como cURL para acessar cargas remotas, ou Rclone para vazar dados para armazenamento em nuvem.

No primeiro trimestre de 2023, Magecart Group, APT29 e APT41 foram os três grupos de ameaças e APTs mais ativos a visar usuários por geolocalização e setores como métodos para coletar valores monetários, revelar segredos de estado ou inibir o uso de infraestruturas. Ficamos surpresos ao saber que o Magecart Group ficou no topo da lista, pois ele raramente opera na escala das outras grandes APTs ligadas a governos de países. Estaremos monitorando as atividades do grupo nos meses à frente para verificar se os dados do período atual indicam um ressurgimento do grupo no cenário global.

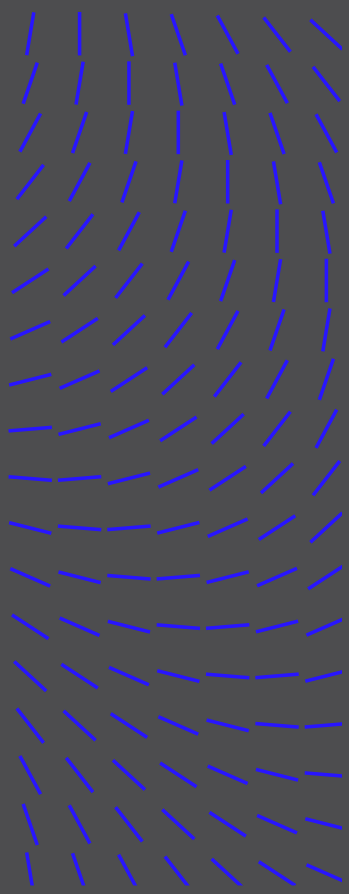
PRINCIPAIS PERPETRADORES DE AMEAÇAS ATIVOS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

1.	Magecart Group	5%
2.	APT29	4%
3.	APT41	4%
4.	Blind Eagle	4%
5.	Gamaredon Group	4%
6.	Lazarus	4%
7.	Mustang Panda	4%
8.	Sandworm Team	4%

Técnicas menos sofisticadas de disseminação indiscriminada, desenvolvidas para enganar qualquer um que venha a clicar em um link ou a fazer um download, afligiram vários setores nas últimas campanhas globais. Os ataques direcionados evoluíram em sofisticação, aumentando sua persistência contra os setores de manufatura, finanças e saúde. Embora os dois setores restantes, de telecomunicações e de energia, pareçam ter sido visados com menos frequência em eventos globais, ambos são igualmente importantes e organizações desses setores podem não ter relatado violações ou podem não estar cientes de incidentes.

PRINCIPAIS SETORES VISADOS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

1.	Manufatura	8%
2.	Finanças	7%
3.	Saúde	6%
4.	Telecomunicações	5%
5.	Energia	5%



Os eventos relatados analisados e selecionados por nossa equipe de pesquisa contêm muitas informações, correlações ou atribuições de um determinado perpetrador de ameaças, grupo de ameaças ou APT mais sofisticada. As ferramentas, técnicas e procedimentos, juntamente com as famílias de malware, incluem malware dos tipos loader e downloader, RATs, malware para roubo de informações e ransomware. Nos eventos analisados e disponibilizados via Insights no primeiro trimestre de 2023, determinamos que a Ucrânia foi visada mais frequentemente, seguida de perto pelos EUA.

As famílias de ransomware Royal Ransom, Trigona e Maui foram os pesos-pesados do primeiro trimestre de 2023. A Trellix publicou recentemente uma análise detalhada do Royal Ransom e de sua interação com executáveis de Windows e de Linux. Embora as estatísticas representadas tenham surgido especificamente de nossa plataforma Insights, muitos eventos adicionais ocorreram na infraestrutura conectada globalmente – inclusive eventos conhecidos, sejam relatados ou mantidos privados, e eventos que ainda precisam ser identificados e remediados.

PRINCIPAIS PAÍSES VISADOS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

7% 

Nos eventos públicos disponíveis para análise, determinamos que a Ucrânia foi o país mais visado por perpetradores de ameaças, seguida de perto pelos Estados Unidos.

1.	Ucrânia	7%
2.	Estados Unidos	7%
3.	Alemanha	4%
4.	Coreia do Sul	3%
5.	Índia	3%

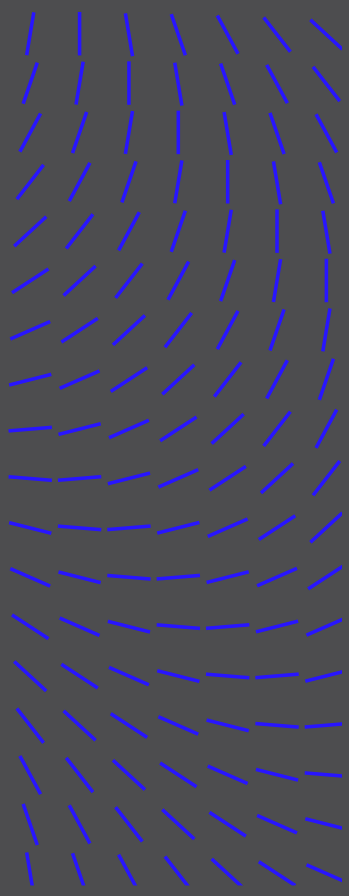
PRINCIPAIS EXEMPLARES DE RANSOMWARE UTILIZADOS NO 1° TRIMESTRE DE 2023 SEGUNDO RELATOS PÚBLICOS

1.	Royal Ransom	7%
2.	Trigona	4%
3.	Maui	4%
4.	Magniber	3%
5.	LockBit	3%

Ransomware

As estatísticas exibidas abaixo são das campanhas, e não propriamente das detecções. Nossa telemetria global revelou indicadores de comprometimento (IoCs) pertencentes a várias campanhas de diversos grupos de ransomware.

É bastante comum ver uma queda em atividades de crime cibernético no início do ano, especialmente em janeiro. Essa tendência pode explicar a queda notável nas atividades do Hive e do Cuba. Além disso, a interrupção de atividades do Hive por parte do FBI e da Europol no final de janeiro pode ter interferido significativamente em suas operações. O LockBit continua sendo uma família importante no espaço do ransomware – sendo particularmente agressivo e aparentemente bem-sucedido em pressionar suas vítimas a pagar resgate.



PRINCIPAIS EXEMPLARES DE RANSOMWARE UTILIZADOS EM EVENTOS NO 1° TRIMESTRE DE 2023

8%

Cuba foi o grupo de ransomware mais ativo, seguido por Play e LockBit.

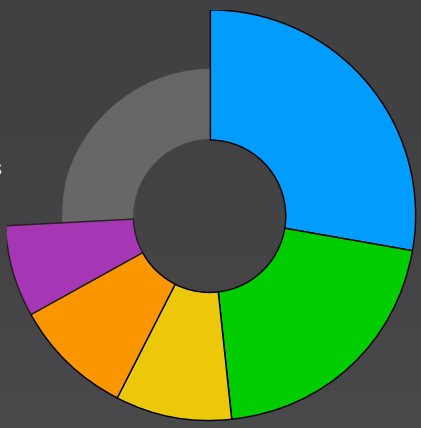
- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

FERRAMENTAS DE RANSOMWARE UTILIZADAS NO 1° TRIMESTRE DE 2023

28%

O CobaltStrike foi utilizado em quase um terço de todos os incidentes de ransomware do trimestre, crescendo em uso apesar de atualizações recentes para dificultar o abuso do mesmo por parte de perpetradores de ameaças.

- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC



PAÍSES MAIS AFETADOS POR GRUPOS DE RANSOMWARE NO 1° TRIMESTRE DE 2023

15%

Os Estados Unidos continuam sendo o país mais afetado por atividades de ransomware, seguido de perto pela Turquia nesse trimestre.

1.	Estados Unidos	15%
2.	Turquia	14%
3.	Portugal	10%
4.	Índia	9%
5.	Canadá	9%

SETORES MAIS AFETADOS POR GRUPOS DE RANSOMWARE NO 1° TRIMESTRE DE 2023

1.	Seguros	20%
2.	Serviços financeiros	17%
3.	Farmacêutico	7%
4.	Telecomunicações	4%
5.	Terceirização e hospedagem	4%

Os grupos de ransomware extorquem suas vítimas publicando informações destas em sites referidos como "sites de vazamento" e utilizando essa exposição para reativar negociações com as vítimas ou quando o pagamento do resgate é recusado. Nossos especialistas na Trellix utilizam o RansomLook, uma ferramenta de código aberto, pra coletar dados de postagens e, em seguida, normalizar e enriquecer os resultados para oferecer uma análise anonimizada de vitimologia.

É importante observar que nem todas as vítimas de ransomware são expostas nos respectivos sites de vazamentos. Muitas vítimas pagam o resgate e não são divulgadas. As métricas abaixo são uma indicação de vítimas extorquidas por grupos de ransomware ou que sofreram retaliação, não devendo ser confundidas com o número total de vítimas.

GRUPOS DE RANSOMWARE QUE MAIS FIZERAM VÍTIMAS NO 1° TRIMESTRE DE 2023, SEGUNDO SITES DE VAZAMENTOS

1.	LockBit	30%
2.	Hive	22%
3.	Clop	12%
4.	Royal Ransom	7%
5.	ALPHV	5%

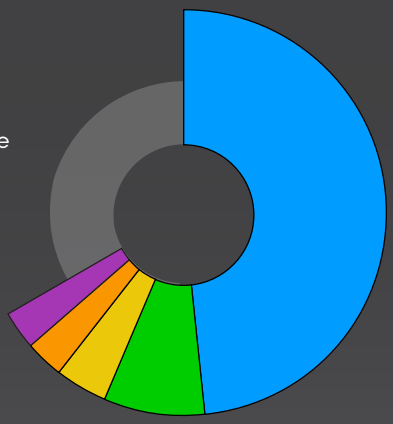
SETORES MAIS AFETADOS POR GRUPOS DE RANSOMWARE NO 1° TRIMESTRE DE 2023, SEGUNDO SITES DE VAZAMENTOS

1.	Serviços e bens industriais	25%
2.	Varejo	14%
3.	Tecnologia	11%
4.	Saúde	8%
5.	Serviços financeiros	6%

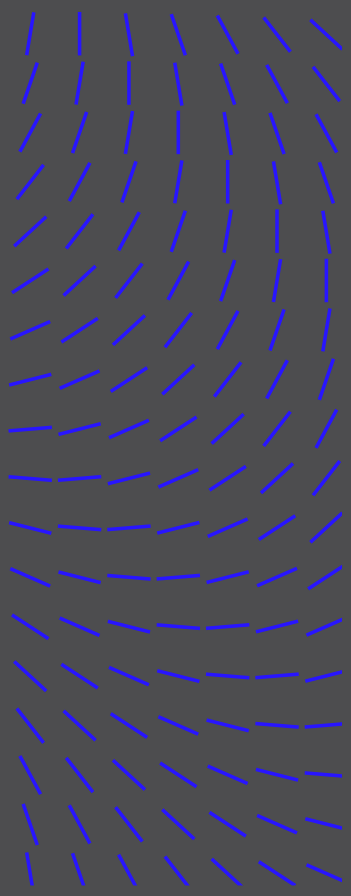
PRINCIPAIS PAÍSES DE EMPRESAS LISTADAS EM SITES DE VAZAMENTOS DE RANSOMWARE NO 1° TRIMESTRE DE 2023

48%

das empresas vitimadas listadas em sites de vazamentos de grupos de ransomware estão sediadas nos Estados Unidos



- Estados Unidos
- Reino Unido
- Alemanha
- Canadá
- Índia



TAMANHO DAS EMPRESAS LISTADAS EM SITES DE VAZAMENTOS DE RANSOMWARE NO 1° TRIMESTRE DE 2023

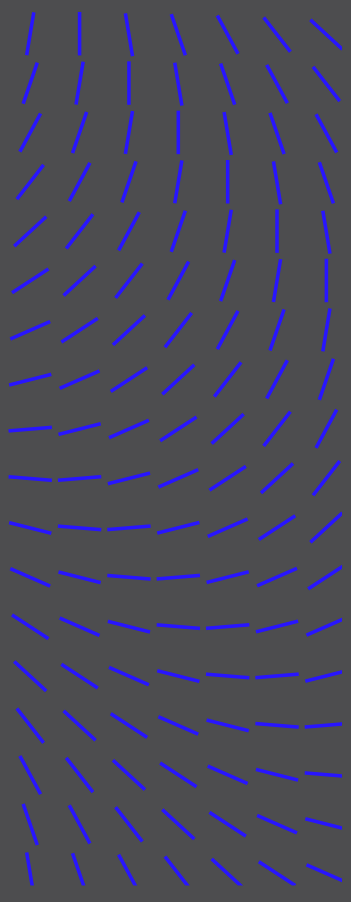
NÚMERO DE FUNCIONÁRIOS		RECEITA ANUAL	
1. 51 a 200	32%	1. US$ 10 mi a US$ 50 mi	38%
2. 1.001 a 5.000	22%	2. US$ 1 bi a US$ 10 bi	23%
3. 11 a 50	15%	3. US$ 1 mi a US$ 10 mi	21%
4. 201 a 500	15%	4. US$ 100 mi a US$ 250 mi	11%
5. 501 a 1.000	15%	5. US$ 500 mi a US$ 1 bi	7%

Atividades de governos

Insights sobre atividades de governos de países são coletados de várias fontes para criar uma imagem melhor do cenário de ameaças e ajudar a reduzir o viés da observação. Primeiramente, apresentamos as estatísticas extraídas da correlação entre grupos ligados a estados-nações, IoCs e a telemetria dos clientes da Trellix. Em seguida, oferecemos insights de vários relatórios publicados pelo setor de segurança, os quais são selecionados, triados e analisados pelo grupo Threat Intelligence.

Conforme observado acima, essas estatísticas são das campanhas, e não propriamente das detecções. Devido a várias agregações de logs, ao uso de estruturas de simulação de ameaças por nossos clientes e a correlações de alto nível com a base de conhecimentos de inteligência sobre ameaças, os dados são filtrados manualmente para satisfazer nossos objetivos de análise.

Continuamos vendo perpetradores de ameaças ligados à China dominando o cenário global, particularmente com o Mustang Panda por trás de uma maioria significativa das detecções no primeiro trimestre de 2023. Como eles dependem muito de carregamento lateral (sideloading) e de outras técnicas para se esconder, é possível que grupos de APT ligados à China façam rotatividade de suas ferramentas de malware com menos frequência que outros perpetradores de ameaças. Nessa hipótese, essa prática pode levar a um "viés de projeção" ou uma estimativa inflada das detecções de hashes ligados à China.

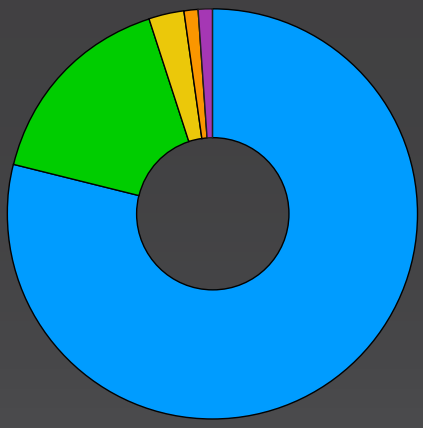


PAÍSES DOS PERPETRADORES DE AMEAÇAS MAIS COMUNS POR TRÁS DE ATIVIDADES DE ESTADOS-NAÇÕES NO 1° TRIMESTRE DE 2023

79%

A China foi responsável por grande maioria das atividades relacionadas a estados-nações no 1° trimestre de 2023.

- China
- Coreia do Norte
- Rússia
- Irã
- Paquistão



GRUPOS DE PERPETRADORES DE AMEAÇAS PREDOMINANTES NO 1° TRIMESTRE DE 2023

1.	Mustang Panda	72%
2.	Lazarus	17%
3.	UNC4191	1%
4.	Common Raven	1%
5.	APT34	1%

TÉCNICAS MITRE ATT&CK MAIS COMUNS EM ATIVIDADES DE ESTADOS-NAÇÕES NO 1° TRIMESTRE DE 2023

1.	Carregamento lateral de LDLL	14%
2.	Decodificação/decifração de arquivos para obtenção de informações	11%
3.	Transferência de ferramenta de ingresso	10%
4.	Dados do sistema local	10%
5.	Descoberta de arquivos e diretórios	10%

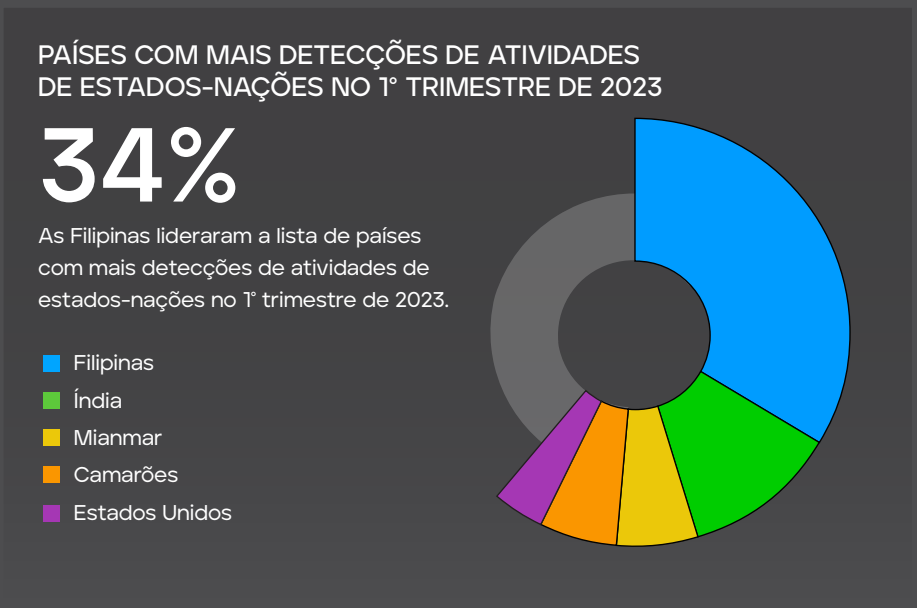
FERRAMENTAS MALICIOSAS PREDOMINANTES EM ATIVIDADES DE ESTADOS-NAÇÕES NO 1° TRIMESTRE DE 2023

38%

O PlugX foi responsável por 38% das atividades maliciosas de estados-nações no 1° trimestre de 2023.

1.	PlugX	38%
2.	Cobalt Strike	35%
3.	Raspberry Robin	14%
4.	BLUEHAZE/DARKDEW MISTCLOAK	3%
5.	Mimikatz	3%

A Índia é um dos países líderes na Ásia e nas regiões vizinhas com programas cibernéticos competentes. Alguns grupos, predominantemente perpetradores de ameaças ligados à China, demonstraram grande interesse nos desenvolvimentos tecnológicos, militares e políticos da Índia. Uma quantidade notável de detecções na Índia pode ser atribuída ao Mustang Panda.



Inteligência sobre vulnerabilidades

Especialistas em engenharia reversa e análise de vulnerabilidades do Trellix Advanced Research Center continuam monitorando as mais recentes vulnerabilidades para oferecer aos clientes orientações sobre como os perpetradores de ameaças estão aproveitando essas vulnerabilidades e como mitigar a probabilidade e o impacto desses ataques.

Uma de nossas descobertas mais críticas, mas não surpreendente, no primeiro trimestre de 2023 é que muitas das vulnerabilidades mais críticas deste período consistiram em desvios de patches de CVEs mais antigas, bugs de cadeia de fornecimento resultantes da utilização de bibliotecas desatualizadas ou vulnerabilidades há muito corrigidas que persistiram muito além de seus esperados cinco minutos de fama.

Considere a CVE-2022-47966, por exemplo, uma vulnerabilidade crítica (9,8) nos produtos ManageEngine da Zoho que circulou janeiro passado. O ManageEngine é utilizado por milhares de empresas do mundo todo e, portanto, não ficamos surpresos quando a exploração desse vuln foi detectada na Internet. O que nos impressionou foi a causa raiz: a utilização do Apache Santuario 1.4.1 – uma versão tão velha que quase chega à maioridade – que continha um problema conhecido que permitia injeção de XML. A Zoho corrigiu a vulnerabilidade em toda a sua linha de produtos

em outubro e, então, quase três meses depois, no primeiro trimestre, a CISA fez uma recomendação, advertindo sobre a exploração aberta dessa vulnerabilidade e instando os fornecedores a corrigi-la.

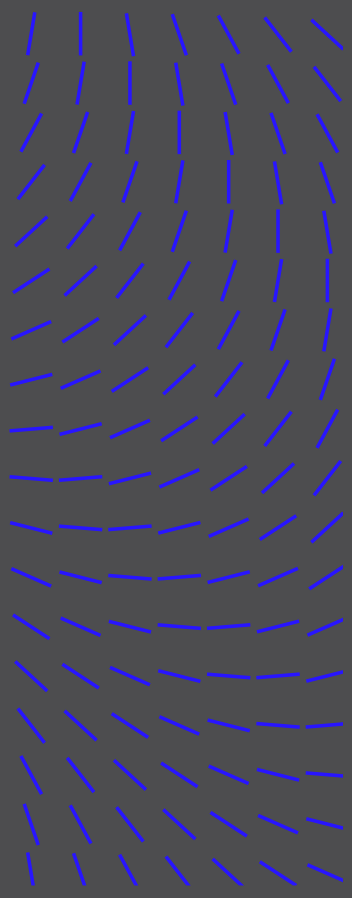
Um outro exemplo é a CVE-2022-44877, uma vulnerabilidade crítica no Control Web Panel (CWP). Embora não relacionada diretamente, essa vulnerabilidade tem muitas das mesmas características de nosso exemplo anterior: é mais uma RCE 9,8 que teve ampla exploração ativa em janeiro, apesar de ter sido corrigida em outubro. A causa raiz também não foi propriamente digna de uma palestra na Black Hat: injeção de comando utilizando expansão de variável de shell padrão em um parâmetro de URL.

Um terceiro exemplo é a CVE-2021-21974, uma vulnerabilidade no serviço OpenSLP do VMware ESXi, resolvida em fevereiro de 2021, quase exatamente dois anos antes de seu súbito ressurgimento devido a uma exploração na Internet. Quando citamos essa vulnerabilidade em nosso relatório de bugs de fevereiro, observamos que aproximadamente 48.000 servidores acessíveis pela Internet ainda executavam versões vulneráveis do ESXi, segundo a Shodan. Hoje esse número ainda é superior a 38.000 – uma mudança de menos de 22%.

Data	Número de servidores ESXi vulneráveis, segundo a Shodan
Final de fevereiro de 2023	48.471
Final de abril de 2023	38.047

Encontramos alguns exemplos por nossa própria conta ao pesquisar dispositivos da Apple no início do ano: CVE-2023-23530 e CVE-2023-23531. Essas duas vulnerabilidades diferem dos exemplos anteriores porque seu impacto limita-se à elevação local de privilégios, e não RCE. Porém, isso não é razão para subestimar sua importância, visto que uma vulnerabilidade bastante parecida foi aproveitada pela exploração FORCEDENTRY, a qual foi utilizada pelo NSO Group para distribuir seu spyware Pegasus em 2021. De fato, as duas CVEs que revelamos utilizam o mesmo primitivo que serviu como base para a exploração FORCEDENTRY: uma classe inócua chamada NSPredicate. Infelizmente, a abordagem da Apple para mitigação da FORCEDENTRY envolveu o uso de uma ampla lista de negação para restringir as formas pelas quais a NSPredicate estava sendo aproveitada – uma mitigação que não resolveu o problema subjacente e nos permitiu contorná-la.

É tentador apontar para tendências como essas e concluir que os fornecedores não levam a segurança a sério ou lamentar a reciclagem de explorações antigas por parte de perpetradores de ameaças e pesquisadores, mas esse não é o caminho certo. Os pesquisadores de vulnerabilidades trabalham com análise de variantes porque um pesquisador eficiente emula as prioridades dos verdadeiros perpetradores de ameaças e descobrir uma maneira de contornar uma mitigação ou encontrar uma CVE antiga em um produto raramente corrigido produz, consistentemente, um melhor retorno de investimento do que reinventar a roda. Para organizações que reconhecem



devidamente essa tendência, a conclusão deve ser esta: embora tecnologias avançadas de detecção de ameaças sejam insubstituíveis no cenário de ameaças moderno, muitas vitórias podem ser obtidas com base nos fundamentos, como corrigir processos e aprovar cadeias de fornecimento.

Segurança de e-mail

As estatísticas de segurança de e-mail baseiam-se em telemetria gerada em vários appliances de segurança de e-mail distribuídos em redes de clientes do mundo todo.

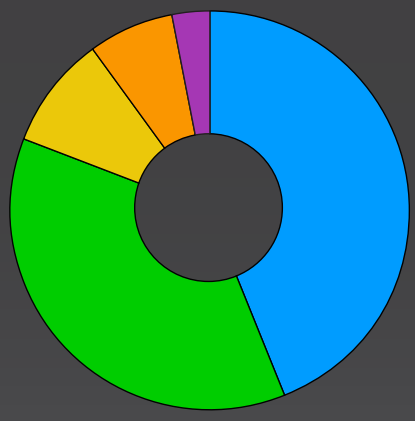
Ataques de phishing que aproveitam marcas legítimas para fraudar usuários e roubar suas credenciais estão em alta, com DWeb, IPFS e Google Translate utilizados intensivamente em ataques de e-mail. Atacantes também se aproveitaram de serviços de e-mail gratuito e outros similares, como os dois aplicativos PayPal Invoicing e Google Forms, para montar ataques de vishing e evitar detecções. Visadas de maneira semelhante durante esse período foram marcas novas, como Scribd, LesMills e cartões de presente do Google Play.

Além disso, em termos do malware específico utilizado nesses ataques, Formbook e Agent Tesla tiveram ambos aumentos notáveis no primeiro trimestre de 2023, em comparação com o final do ano passado. Um fato que pode ter contribuído para isso é que ambos os exemplares de malware são mais fáceis de adquirir e distribuir, em comparação com Remcos, Emotet e Qakbot.

TÁTICAS DE MALWARE DE E-MAIL PREDOMINANTES NO 1° TRIMESTRE DE 2023

44%

O Formbook representou quase a metade do malware de e-mail no 1° trimestre, seguido de perto pelo Agent Tesla.



PAÍSES MAIS VISADOS POR PHISHING DE E-MAIL NO 1° TRIMESTRE DE 2023

30%

Estados Unidos e Coreia foram as principais vítimas de tentativas de phishing de e-mail no 1° trimestre, recebendo quase dois terços de todas as tentativas de phishing globais.

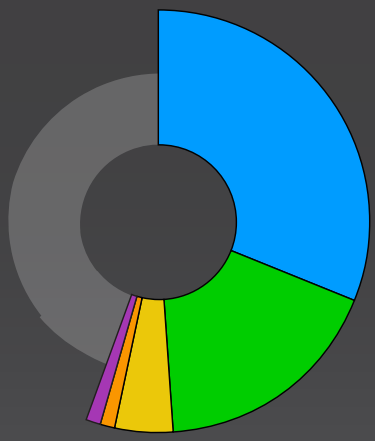
1.	Estados Unidos	30%
2.	Coreia do Sul	29%
3.	Taiwan	10%
4.	Brasil	8%
5.	Japão	7%

PRODUTOS E MARCAS MAIS VISADOS POR PHISHING DE E-MAIL NO 1° TRIMESTRE DE 2023

38%

Embora centenas de marcas tenham sido visadas, os produtos da Microsoft foram maioria por ampla margem no 1° trimestre de 2023.

- Microsoft
- Google Captcha
- Outlook
- GCash
- USPS



SETORES MAIS AFETADOS POR E-MAILS MALICIOSOS NO 1° TRIMESTRE DE 2023

1.	Governamental	11%
2.	Serviços financeiros	8%
3.	Manufatura	6%
4.	Tecnologia	6%
5.	Entretenimento	5%

PROVEDORES DE HOSPEDAGEM DE WEB ALTAMENTE APROVEITADOS NO 1° TRIMESTRE DE 2023

1.	IPFS	41%
2.	Google Translate	33%
3.	Dweb	16%
4.	AmazonAWS Appforest	3%
5.	Firebase OWA	3%

TÉCNICAS DE EVASÃO MAIS UTILIZADAS EM ATAQUES DE PHISHING NO 1° TRIMESTRE DE 2023

79%

A evasão baseada em Redirect 302 foi a técnica de evasão mais utilizada por ataques de phishing no 1° trimestre de 2023.

46%

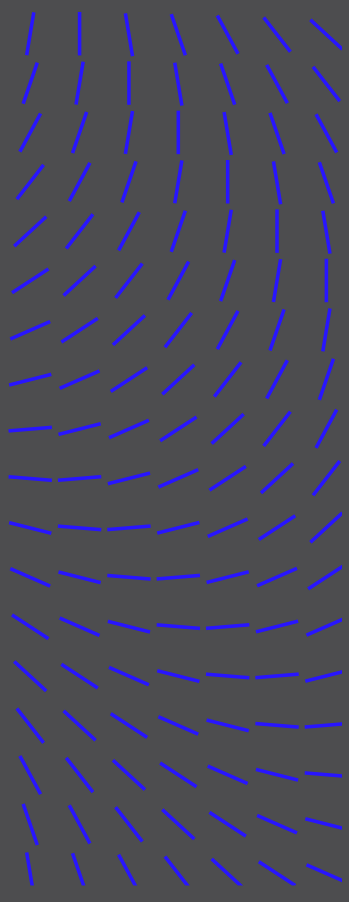
Os ataques baseados em Captcha aumentaram significativamente no 1° trimestre, em comparação com o 4° trimestre de 2022.

Segurança de rede

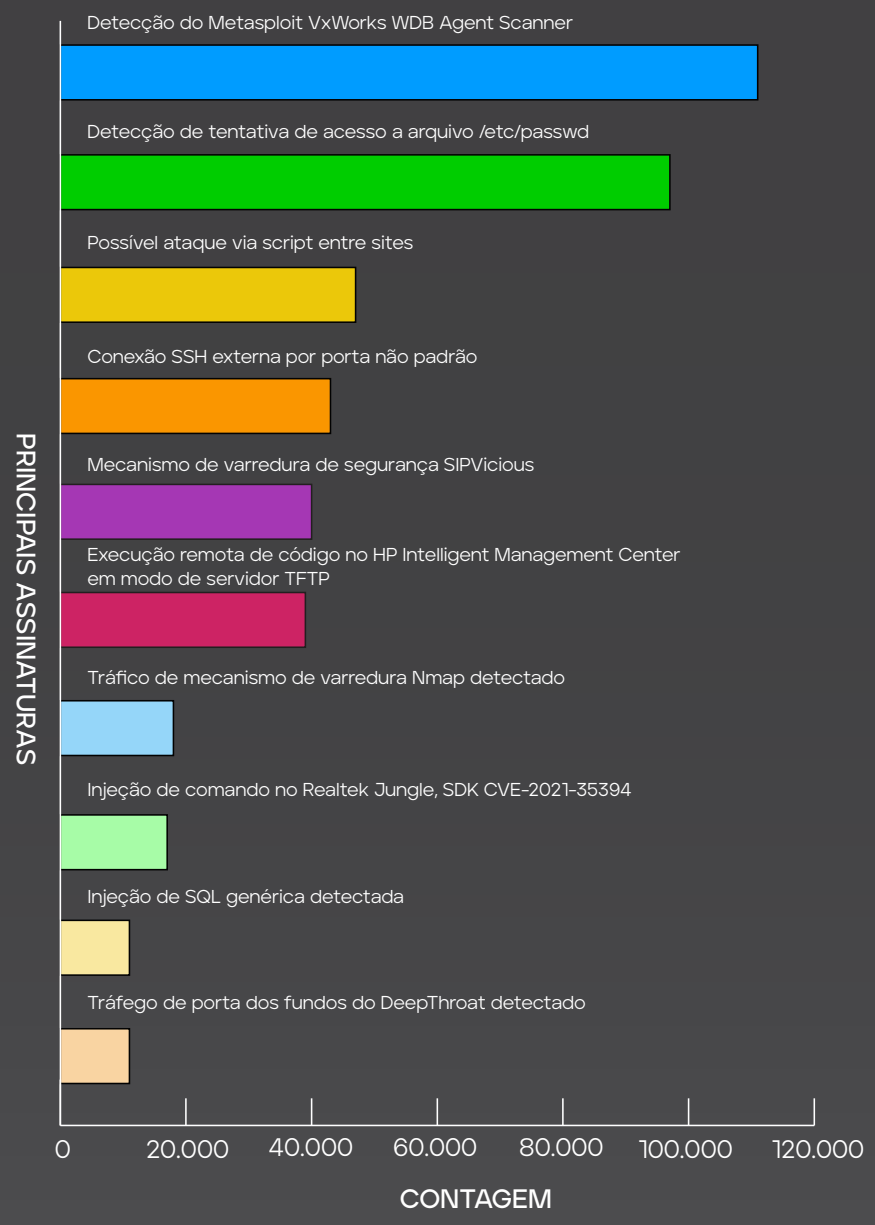
No decorrer da detecção e bloqueio de ataques baseados em rede que ameaçam nossos clientes, a equipe de pesquisa de rede do Trellix Advanced Research Center inspeciona áreas diferentes da cadeia de destruição – sejam de reconhecimento, comprometimento inicial, comunicações de comando e controle e TTPs de movimentação lateral.

TENDÊNCIAS DE CALLBACK DE MALWARE MAIS NOTÁVEIS NO 1° TRIMESTRE DE 2023

A atividade do ransomware STOP caiu	94%
O ransomware LockBit distribuído pelo Amadey aumentou	25%
A atividade do malware para Android aumentou	12,5%
A atividade do Ursnif aumentou	10%
A atividade do Smoke Loader aumentou	7X
A atividade do Amadey aumentou	4X
A atividade do Cobalt Strike aumentou	3X
A atividade do Emotet aumentou	2X



ATAQUES MAIS IMPACTANTES CONTRA SERVIÇOS VOLTADOS PARA A INTERNET NO 1° TRIMESTRE DE 2023



Incidentes de nuvem

Os ataques de infraestrutura de nuvem contra serviços desenvolvidos e fornecidos pela Amazon, Microsoft, Google e outros continuam a aumentar. A tabela abaixo descreve os dados de telemetria de ataques baseados em nuvem por cliente e por provedor de nuvem.

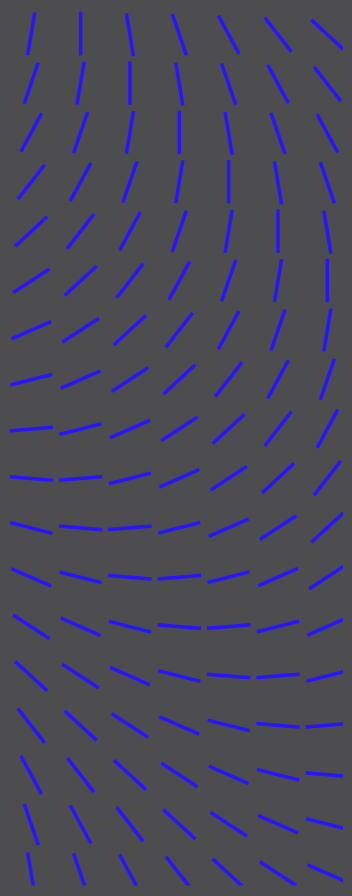
DETECÇÕES POR TÉCNICAS MITRE ATT&CK NO 1° TRIMESTRE DE 2023

	AWS	Microsoft Azure	GCP
Contas válidas	3.437	4.312	997
Modificação da infraestrutura de computação na nuvem	4.268	0	17
Porta fora do padrão	115	0	17
Autenticação por múltiplos fatores	190	1.534	22
Descoberta de serviços de rede	141	93	0
Força bruta	25	1.869	22
Proxy	299	2.744	135
Descoberta de contas	264	68	787
Regra de encaminhamento de e-mail	25	0	22
Execução por API	1.143	0	252

METODOLOGIA

Coleta: os especialistas experientes e de nível internacional da Trellix e do Advanced Research Center coletam as estatísticas, tendências e insights que compõem este relatório de uma ampla variedade de fontes globais.

- **Fontes reservadas:** em alguns casos, a telemetria é gerada pelas soluções de segurança da Trellix sobre redes de segurança cibernética de clientes e estruturas de defesa distribuídas mundo afora, em redes de setores tanto públicos quanto privados, inclusive os que fornecem serviços de dados, infraestrutura e tecnologia. Esses sistemas, que se contam aos milhões, geram dados de um bilhão de sensores.
- **Fontes abertas:** em outros casos, a Trellix aproveita uma combinação de ferramentas patenteadas, próprias e de código-aberto para garimpar sites, logs e repositórios de dados na Internet, bem como na Dark Web, como os "sites de vazamentos" nos quais elementos maliciosos publicam informações sobre ou pertencentes às suas vítimas de ransomware.



Normalização: os dados agregados são fornecidos a nossas plataformas Insights e ATLAS. Por meio do uso de autoaprendizagem, automação e perspicácia humana, a equipe percorre um conjunto intensivo, integrado e iterativo de processos – normalizando os dados, enriquecendo resultados, removendo informações pessoais e identificando correlações entre métodos de ataque, agentes, setores, regiões, estratégias e resultados.

Análise: em seguida, a Trellix analisa esse amplo reservatório de informações, com referência a (1) sua extensiva base de inteligência sobre ameaças, (2) relatórios de fontes altamente reputadas e certificadas do setor de segurança cibernética e (3) experiência e insights de analistas de segurança cibernética, investigadores, especialistas em engenharia reversa, pesquisadores forenses e especialistas em vulnerabilidades da Trellix.

Interpretação: finalmente, a equipe da Trellix extrai, examina e valida insights significativos que podem ajudar equipes de operações de segurança e líderes de segurança cibernética a (1) compreender as tendências mais recentes do ambiente de ameaças cibernéticas e (2) a utilizar essa perspectiva para melhorar sua capacidade de antever, prevenir e defender suas organizações contra ataques cibernéticos no futuro.

RECURSOS

Arquivos dos relatórios de ameaças

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

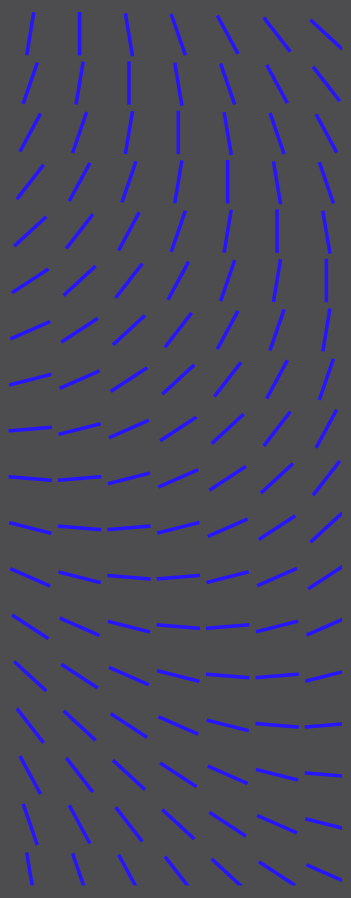
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

Visualize os arquivos dos relatórios de ameaças cibernéticas

Trellix Advance Research Center

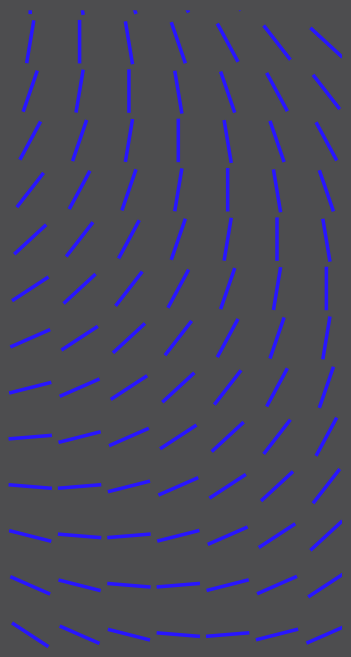


SOBRE O TRELLIX ADVANCED RESEARCH CENTER

Como proposta mais abrangente do setor de segurança cibernética, o Trellix Advanced Research Center está na vanguarda dos agentes, tendências e métodos emergentes de todo o cenário de ameaças global, atuando como principal parceiro de equipes de operações de segurança do mundo todo. O Trellix Advanced Research Center oferece inteligência e conteúdo de ponta para analistas de segurança enquanto alimenta nossa plataforma de XDR. Além disso, o grupo Threat Intelligence do Advanced Research Center da Trellix oferece produtos e serviços de inteligência para clientes em todo o mundo.

SOBRE A TRELLIX

A Trellix é uma empresa global que está redefinindo o futuro da segurança cibernética e do trabalho abnegado. A plataforma aberta e nativa de detecção e resposta estendida (eXtended Detection and Response, XDR) ajuda as organizações confrontadas pelas ameaças mais avançadas da atualidade a ter confiança na proteção e na resiliência de suas operações. A Trellix, juntamente com um amplo ecossistema de parceiros, acelerou a inovação tecnológica através de autoaprendizagem e automação para capacitar mais de 40.000 clientes corporativos e governamentais com uma segurança viva.



Visite Trellix.com para saber mais.

Trellix

Sobre a Trellix

A Trellix é uma empresa global que está redefinindo o futuro da segurança cibernética. A plataforma aberta e nativa de detecção e resposta estendida (Extended Detection and Response, XDR) ajuda as organizações confrontadas pelas ameaças mais avançadas da atualidade a ter confiança na proteção e na resiliência de suas operações. Os especialistas de segurança da Trellix, juntamente com um amplo ecossistema de parceiros, aceleram a inovação tecnológica através de autoaprendizagem e automação para capacitar mais de 40.000 clientes corporativos e governamentais.

072022-05