RELATÓRIO DE AMEAÇAS CIBERNÉTICAS

Junho de 2024

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

CONTÉM:

Mudanças rápidas e significativas no cenário de APT

LockBit agita o ecossistema de ransomware

Expansão da caixa de ferramentas dos atacantes

Apresentado por

Trellix ADVANCED RESEARCH CENTER

Uma ferramenta de evasão de EDR acabou de ser utilizada com êxito para desativar capacidades de detecção e resposta em uma outra organização do seu setor.

A corrida da cibersegurança para superar os atacantes e impedi-los de utilizar ferramentas de segurança legítimas para fins ilícitos está se tornando mais complicada.

Como CISO, você precisa se mover com agilidade, rapidez, confiança e controle. O seu CEO e o conselho diretor estão esperando para saber mais sobre as suas ferramentas de alerta e registro. Você encarrega a sua equipe de identificar brechas e tem um plano para resolvê-las.

A corrida da cibersegurança é um triatlo. Você compete em operações de segurança, tecnologia e inteligência. A corrida já começou e sua modalidade é endurance.

> Conforme os mecanismos de defesa se tornam mais sofisticados, o mesmo ocorre com as ferramentas e táticas ofensivas empregadas por estados-nações e criminosos cibernéticos.

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 principalmente entre 1º de outubro de 2023 e 31 de março de 2024.

1. Mudanças rápidas e significativas no cenário de APT
2. LockBit agita o ecossistema de ransomware
3. Surgimento dos eliminadores de EDR
4. Fraudes com o tema da eleição presidencial dos EUA
5. Inteligência artificial generativa e o submundo do crime cibernético

PREÂMBULO

A inteligência operacional sobre ameaças e a capacidade de agregar contexto sobre ameaças globais ao seu ambiente nunca foi tão importante para a função do CISO.

Sendo encarregados de fazer mais com menos, os CISOs e suas equipes de operações de segurança precisam de inteligência para antever ameaças, identificar e preparar-se para as ameaças predominantes que visam a sua organização, alinhar programas e orçamentos contra as ameaças e perpetradores mais prováveis e, finalmente, mudar a postura de reativa para proativa.

Como um "cliente zero" da Trellix, eu nunca vi um potencial maior de que a inteligência determine a movimentação e a estratégia dos encarregados pela resposta às ameaças.

Pegue este conteúdo, assimile-o e coloque-o em prática no seu planejamento estratégico, racionalização orçamentária, educação do conselho diretor e suporte operacional. Espero que estes insights sejam educativos, informativos e benéficos e que eles sirvam como um ponto de partida para melhor orientar e influenciar a maneira como você planeja, se prepara e persiste contra APTs.

Harold Rivas
CISO da TRELLIX

SUMÁRIO

PREFÁCIO

Com este relatório e todos os nossos relatórios, objetivamos oferecer estrutura em torno de inteligência e contexto do que estamos observando.

O cenário

Os últimos seis meses foram inéditos - um estado de crise múltipla persiste e tem acelerado as atividades de perpetradores de ameaças e criminosos cibernéticos no mundo todo. Estamos vendo mudanças radicais de comportamento, inclusive:

- O ecossistema de ransomware comporta-se de forma atípica após ações policiais,
- Grupos autônomos estão vendendo para quadrilhas de ransomware suas participações em métodos de ataque alternativos e testes de penetração,
- A guerra em Israel desencadeou hacktivismo e ataques diretos patrocinados por países,
- Os perpetradores de ameaças estão procurando se sofisticar com acesso a ferramentas de inteligência artificial generativa baratas ou gratuitas que os permitem se tornar especialistas da noite para o dia e
- As ferramentas de término e evasão de EDR tornaram-se mais importantes para os perpetradores de ameaças.

Um jogo de gato e rato

Com uma implementação maior de soluções de detecção e resposta (EDR) para endpoints, estamos vendo o jogo de gato e rato da cibersegurança tornar-se mais complexo. O aumento na quantidade de perpetradores de ameaças que utilizam ferramentas criminosas para desmantelar a EDR chamou nossa atenção, constituindo uma mudança de rumo abrupta em relação ao uso de ferramentas tradicionais baseadas em malware.

Como defensores, precisamos mudar de rumo também. A EDR provou ser eficaz na detecção de malware, de ransomware e de atividades de grupos de APT, mas se a EDR estiver fora do ar, o que as organizações e seus CISOs farão? Você precisa de registros em logs, de alertas e de inteligência operacional sobre ameaças para não ficar alheio a comportamentos incomuns no seu sistema. Há uma camada nova nesse jogo.

Nós trabalhamos com afinco para compartilhar inteligência sobre ameaças com a comunidade - um valor fundamental nosso para nos mantermos à frente dos adversários - e rastrear campanhas e grupos de ameaças em grande escala.

O cenário está mudando mais do que nunca. Nosso objetivo é apoiar nossos clientes e o setor como um todo com a inteligência necessária para afiar as defesas, criar contramedidas e identificar brechas.

Nesse jogo de gato e rato, temos que jogar para vencer.

John Fokker
CHEFE DE INTELIGÊNCIA SOBRE AMEAÇAS DA TRELLIX

SUMÁRIO

INTRODUÇÃO: RELATÓRIO DE AMEAÇAS CIBERNÉTICAS: JUNHO DE 2024

Eventos geopolíticos que afetam o domínio cibernético

Pesquisas do Trellix Advanced Research Center sobre atividades entre 1º de outubro de 2023 e 31 de março de 2024 revelaram uma mudança em atividades de ameaça, com um aumento notável em operações de ameaças cibernéticas com motivação geopolítica. Observou-se que grandes eventos regionais e globais – como exercícios militares, reuniões políticas ou econômicas, convenções políticas e eleições – impulsionaram atividades de ameaças cibernéticas.

Os analistas da Trellix estimam, com um grau moderado de confiança, que os perpetradores de ameaças concentraram-se nesses eventos para coletar inteligência relevante sobre suas contrapartes, sondar redes proativamente para obter informações que proporcionem conscientização situacional ou posicionar-se estrategicamente em redes de TI para ataques futuros.

- **Presidentes Biden e Xi encontram-se em San Francisco:** em novembro de 2023, dados de detecção de telemetria da Trellix indicaram um surto de atividade maliciosa de grupos de APT ligados à China poucos dias antes do encontro entre o presidente Biden dos EUA e o Presidente Xi da China em San Francisco como parte da reunião de cooperação econômica Ásia-Pacífico (APEC). A quantidade de atividades de ameaça diminuiu consideravelmente após o encontro Biden-Xi e no decorrer da reunião da APEC.

  Com o encerramento da reunião da APEC, o nível de atividade de ameaças caiu ao ponto mais baixo do mês de novembro de 2023. Esse padrão de atividade de ameaças de grupos de perpetradores de ameaças associados à China provavelmente sugere que grupos de perpetradores de ameaças patrocinados pelo estado chinês foram fortemente influenciados por eventos geopolíticos, como a APEC. Isso também pode indicar que grupos de APT chineses podem ter cessado deliberadamente suas atividades de hacking durante um grande evento político, possivelmente para preservar sua imagem pública e reputação internacional.
- **Guerra Israel-Hamas:** ameaças de grupos de perpetradores de ameaças APT ligados ao Irã também foram impulsionadas por desdobramentos políticos em torno da guerra Israel-Hamas. Nos Estados Unidos, dados de telemetria global da Trellix mostram surtos periódicos de atividade maliciosa de grupos de perpetradores de ameaças APT ligados ao Irã nos últimos seis meses (com exceção dos meses de novembro e dezembro de 2023). Nossa telemetria global mostra, especificamente, uma redução em atividade de ameaças de grupos de APT ligados ao Irã visando organizações dos EUA durante os períodos de troca de reféns com Israel e acordos de cessar-fogo em novembro e dezembro de 2023, quando os EUA pressionaram por um cessar-fogo humanitário na Faixa de Gaza, sendo que o Irã apoia abertamente o Hamas. Além disso, a telemetria global da Trellix indica que grupos de perpetradores de ameaças APT ligados ao Irã empregaram uma variedade de TTPs, inclusive phishing, malware para roubo de informações, backdoors, downloaders, webshells maliciosos e vulnerabilidades frequentemente exploradas para visar organizações de Israel durante o período do relatório.

SUMÁRIO

- **Exercícios militares:** além disso, exercícios militares internacionais para aumentar a prontidão para o combate podem desencadear um aumento em atividades maliciosas. Mais recentemente, em março de 2024, dados de telemetria global da Trellix mostram surtos repetidos em atividades de ameaças na Coreia do Sul durante exercícios militares conjuntos em grande escala entre EUA e Coreia do Sul, conhecidos como Freedom Shield, de 4 a 14 de março de 2024. Esses exercícios militares foram concebidos em resposta ao "teatro de operações coreano" e para se contrapor à ameaça nuclear em evolução na Coreia do Norte. Especificamente, as detecções de ameaças na Coreia do Sul excederam mais de 150.000 em número nos dias 7 e 13 de março de 2024, ou seja, aproximadamente sete vezes mais que as 20.000 detecções diárias no país.
- **Guerra Rússia-Ucrânia:** a guerra cinética continuada na região foi acompanhada de iniciativas cibernéticas grandes e pequenas. Destacam-se perpetradores ligados à Rússia, observados aproveitando malware de eliminação novo e mais avançado para eliminar milhares de servidores virtuais e PCs ao atacar a operadora de telecomunicações ucraniana Kyivstar. O ataque à Kyivstar é um dos ataques cibernéticos mais perturbadores e de mais alto impacto na Ucrânia desde que a Rússia invadiu o país em 2022.

Resumo dos destaques

Embora este relatório sirva como um repositório para pesquisas de várias áreas de nossos negócios, temas fundamentais persistem:

1. **Mudanças rápidas e significativas no cenário de APT**
    a. **Escalada do Sandworm, ligado à Rússia:** conforme as tensões geopolíticas aumentam, o mesmo acontece com a atividade de APT em todo o ecossistema. Enquanto as ameaças APT crescem em geral, o grupo Sandworm, ligado à Rússia, foi detectado 40% mais vezes no período observado deste relatório.
    b. **A China continua um terreno fértil:** grupo de ameaças ligados à China continuam sendo os maiores originadores de atividades de APT. A Trellix observou mais de 21 milhões de detecções de atividades de ameaças de grupos de perpetradores de ameaças alinhados com a China. Mais de 23% das detecções de atividades maliciosas foram direcionadas contra setores governamentais do mundo todo.
    c. **Picos de atividade do Volt Typhoon:** como grupo de APT patrocinado pelo estado chinês relativamente novo, o Volt Typhoon destaca-se por seu padrão comportamental e suas práticas de direcionamento peculiares. Desde meados de janeiro de 2024, a telemetria da Trellix detectou mais de 7.100 atividades maliciosas associadas ao Volt Typhoon, com picos periódicos durante o período de janeiro a março de 2024.

SUMÁRIO

2. **LockBit agita o ecossistema de ransomware**
    a. **Impostores afetam reputação de quadrilha:** após uma operação policial global de grandes proporções (Operation Cronos), a Trellix observou impostores fazendo-se passar pelo LockBit, enquanto o grupo tentava desesperadamente preservar sua reputação e restaurar sua operação lucrativa.
    b. **EUA continuam sendo os mais visados:** os Estados Unidos continuaram sendo o país mais visado por grupos de ransomware, seguidos por Turquia, Hong Kong, Índia e Brasil.
    c. **Transportes e logística mais atingidos:** o setor de transportes e logística foi o mais ameaçado por perpetradores de ransomware no quarto trimestre de 2023 e no primeiro trimestre de 2024. O setor gerou 53% e 45% das detecções globais de ransomware, respectivamente, sendo seguido pelo setor financeiro.
    d. **Ação policial resulta em condenação:** antes de finalizar este relatório, autoridades policiais globais revelaram a verdadeira identidade do líder da quadrilha LockBit. Ações adicionais contra criminosos de ransomware ocorreram em 1º de maio. O afiliado do REvil que atacou a Kaseya e muitas outras organizações foi sentenciado a 13 anos de prisão e à devolução de US$ 16 milhões.
3. **Surgimento dos eliminadores de EDR**
    a. **A quadrilha de ransomware D0nut aparece:** o surgimento da quadrilha de ransomware D0nut foi particularmente interessante pelo uso inovador de uma ferramenta eliminadora de EDR, demonstrando uma tática avançada para contornar a detecção em endpoint e aumentar a eficácia de seus ataques.
    b. **Ferramenta de evasão de EDR do Spyboy utilizada para visar setor de telecomunicações:** uma ferramenta eliminadora de EDR chamada "Terminator", criada pelo desenvolvedor Spyboy, foi utilizada em uma nova campanha em janeiro de 2024. Essa ferramenta é utilizada para contornar soluções de EDR e 80% dos ataques detectados foram direcionados contra o setor de telecomunicações.
4. **Fraudes com o tema da eleição presidencial dos EUA**
    a. **O phishing continua dando frutos:** enquanto o mundo espera pelo resultado da eleição presidencial dos EUA em novembro, fraudes foram observadas utilizando imagens sobre a eleição com o objetivo de obter doações.

SUMÁRIO

5. **Inteligência artificial generativa e o submundo do crime cibernético**
    a. **Ferramentas gratuitas baseadas em inteligência artificial:** a Trellix observou uma ferramenta ChatGPT 4.0 Jabber gratuita no submundo do crime cibernético que permite ao desenvolvedor viabilizar a adoção de inteligência artificial generativa por perpetradores de ameaças em suas operações, bem como criar uma base de conhecimentos de inteligência artificial generativa para aprender com outros criminosos cibernéticos ou até mesmo roubar suas ideias e ferramentas.
    b. **Cresce a adoção do malware para roubo de informações:** dois InfoStealers (malware para roubo de informações) com recursos baseados em inteligência artificial generativa foram observados em uso por criminosos cibernéticos. O MetaStealer e o LummaStealer são equipados com inteligência artificial generativa para evadir detecção e para detectar bots entre a lista de logs, respectivamente. Capacidades de inteligência artificial generativa tornam essas táticas criminosas mais difíceis de localizar e de bloquear.

Metodologia: como coletamos e analisamos dados

Os especialistas do Trellix Advanced Research Center 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.

SUMÁRIO

ANÁLISES, INSIGHTS E DADOS DO RELATÓRIO

Estados-nações e ameaças persistentes avançadas (APT)

De outubro de 2023 a março de 2024, a Trellix observou um aumento de 17% em detecções baseadas em APT, em comparação com os seis meses anteriores. Isso é marcante porque nosso último relatório identificou um aumento impressionante de 50% nessas detecções. O ecossistema de APT está fundamentalmente diferente de um ano atrás – mais agressivo, astuto e ativo.

No cenário de ameaças cibernéticas em evolução rápida, grupos de ameaças persistentes avançadas (APT) continuam constituindo um desafio sofisticado e significativo para a cibersegurança global.

Nós objetivamos analisar completamente as atividades associadas às ameaças persistentes avançadas (APT) detectadas do quarto trimestre de 2023 ao primeiro trimestre de 2024. Essa análise concentra-se nas origens dessas ameaças, seus principais alvos e as ferramentas utilizadas em suas operações. Nós comparamos essas descobertas com dados da primeira metade de 2023 (segundo e terceiro trimestres) utilizando duas métricas principais: variação percentual e variação de contribuição proporcional.

- Variação percentual: essa métrica nos ajuda a ver se a atividade de um grupo de APT específico, o direcionamento contra certos países ou o uso de determinadas ferramentas aumentou, diminuiu ou permaneceu o mesmo com o tempo. Compreender isso nos ajuda a rastrear mudanças nos comportamentos desses perpetradores de ameaças e a forma como o cenário de ameaças cibernéticas como um todo está evoluindo.
- Variação de contribuição proporcional: essa métrica agrega contexto, não só mostrando a mudança bruta de atividade, mas a forma como essa mudança se apresenta em relação a todo o ambiente de ameaças à cibersegurança. Por exemplo, mesmo que as detecções de um determinado perpetrador tenham aumentado significativamente, isso ainda pode representar apenas uma pequena parte do total de ameaças cibernéticas, caso o ambiente de ameaças como um todo tenha se tornado mais agitado. Por outro lado, caso as detecções tenham diminuído, mas o restante do ambiente de ameaças tenha sofrido uma desaceleração ainda maior, o perpetrador em questão pode estar se tornando relativamente mais importante.

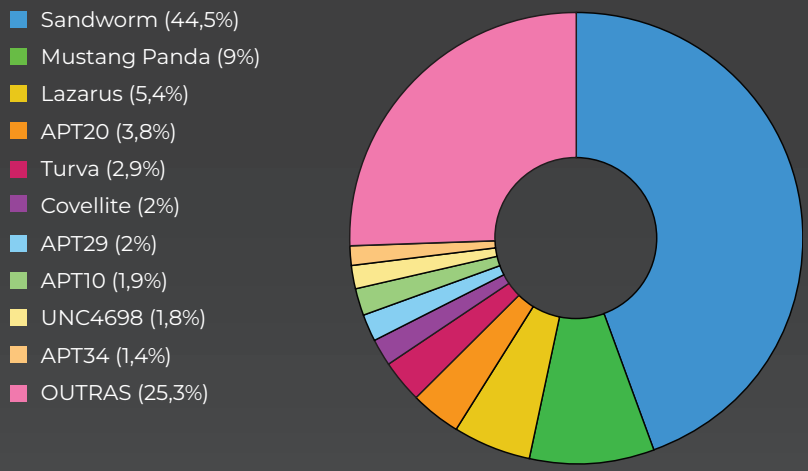
Ao empregar essas métricas, buscamos proporcionar uma compreensão mais sutil das mudanças nas atividades de APT, o que nos permite obter insights sobre seus objetivos estratégicos, metodologias preferidas e os desafios de cibersegurança que elas representam. As seções seguintes aprofundam-se nessas descobertas, esclarecendo o mundo intrincado das APTs e o trabalho contínuo necessário para proteção contra suas ameaças sofisticadas.

SUMÁRIO

Estados-nações e grupos de APT ativos

Além disso, no período de outubro de 2023 a março de 2024 houve flutuações significativas nas atividades de vários grupos de APT. Essas flutuações não somente confirmam a natureza dinâmica das ameaças cibernéticas, como também ressaltam mudanças no foco operacional e nas técnicas empregadas por esses perpetradores sofisticados.

10 PRINCIPAIS APTs COM BASE EM DETECÇÕES ENTRE O ÚLTIMO TRIMESTRE DE 2023 E O PRIMEIRO TRIMESTRE DE 2024



MUDANÇAS NAS ATIVIDADES DE OUTROS GRUPOS DE AMEAÇAS CIBERNÉTICAS: VARIAÇÃO E CONTRIBUIÇÃO PROPORCIONAL

Ameaças persistentes avançadas	Variação percentual	Variação de contribuição proporcional
Sandworm	1669,43%	40,34%
Mustang Panda	-2,19%	-6,14%
Lazarus	66,87%	0,07%
APT28	18,67%	-1,49%
Turla	2,95%	-1,74%
Covellite	85,30%	0,23%
APT29	123,98%	0,53%
APT10	80,46%	0,17%
UNC4698	368,75%	1,14%
APT34	96,73%	0,23%
Outras	-28,99%	-33,33%

SUMÁRIO

- **Uma mudança de tática:** o Sandworm, notório por suas operações cibernéticas perturbadoras, teve um aumento impressionante de 1669% em detecções e uma variação de contribuição proporcional de 40%. Esse aumento monumental sugere uma escalada sem precedentes nas atividades cibernéticas desse grupo ligado à Rússia.
- **Expansão agressiva de operações:** APT29, um grupo com uma história de ampla espionagem cibernética, apresentou um surto de atividade significativo, com detecções aumentando em 124%. De forma semelhante, APT34 e Covellite também apresentaram aumentos consideráveis em detecções, de 97% e 85% respectivamente, indicando um ritmo operacional acelerado ou o início de novas campanhas.
- **Homeostase:** por outro lado, grupos como Mustang Panda, Turla e APT28 tiveram mudanças mínimas em seus níveis de atividade, com o Mustang Panda apresentando uma pequena diminuição de -2% e o Turla um aumento modesto de 3% em detecções.
- **Surgem novos perpetradores:** digno de nota é o surgimento de UNC4698, que teve um aumento de 363% em detecções, o que sugere a ascensão de um novo participante potencialmente significativo no cenário de APT.

O QUE SABEMOS SOBRE O UNC4698?

Não se sabe muito sobre esse grupo, mas pesquisadores conseguiram reconhecer seu comportamento como atividade de grupo e não sabem ainda como atribuí-lo.

Dito isso, o que se sabe do UNC4698 é que seu foco é espionagem industrial, coletando dados operacionais confidenciais que possam ser utilizados para apoiar objetivos econômicos e de segurança nacional do estado patrocinador, e presume-se que ele está ligado à China devido à natureza e ao foco regional dos ataques.

Seus alvos habituais são organizações do setor de petróleo e gás da Ásia.

O grupo também é conhecido por empregar um malware específico chamado “SNOWYDRIVE”.

O UNC4698 emprega uma variedade de táticas, técnicas e procedimentos (TTPs) centrados no uso de malware entregue por meio de unidades flash USB. Eis alguns dos principais TTPs associados a esse perpetrador de ameaças:

- **Acesso inicial por meio de dispositivos USB infectados:** o principal método de infecção envolve unidades USB contendo software malicioso desenvolvido para criar uma porta dos fundos no sistema do host.

SUMÁRIO

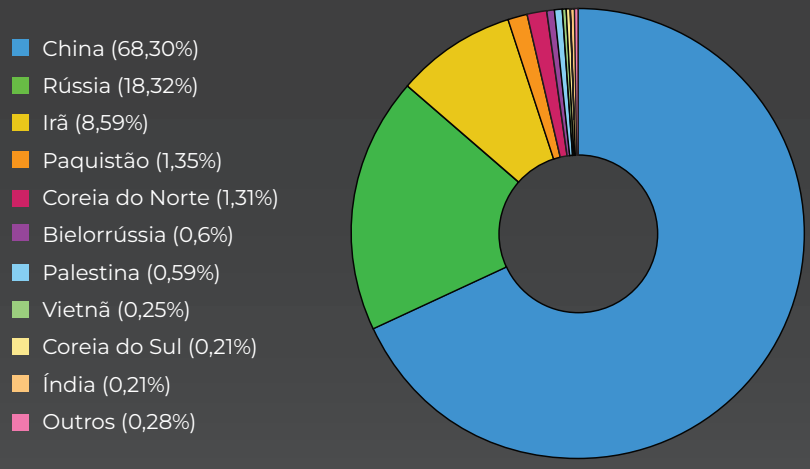
O QUE SABEMOS SOBRE O UNC4698? *(continuação)*

- **Execução através de arquivos maliciosos:** o malware costuma incluir um dropper que grava DLLs e executáveis maliciosos em disco. Esses arquivos costumam passar por software legítimo para evitar detecção e são executados para estabelecer controle adicional.
- **Persistência e modificação do Registro:** o UNC4698 assegura persistência nos sistemas infectados modificando o Registro do Windows. Isso permite que o malware seja iniciado automaticamente sempre que o sistema é inicializado.
- **Comunicações de comando e controle:** o malware estabelece um método para comunicação remota, possibilitando que os atacantes enviem comandos e controlem remotamente os sistemas comprometidos.
- **Movimentação lateral por meio de mídias removíveis:** o malware pode copiar a si próprio para outros dispositivos USB conectados à máquina infectada, o que ajuda a disseminar a infecção para outros sistemas.

Grupos menos conhecidos ou não identificados tiveram um aumento de 62% em detecção, indicando uma gama de ameaças diversificada e crescente que vai além das entidades de APT bem documentadas. Esse aumento de 8% em sua contribuição proporcional no total de detecções destaca a evolução e a diversificação constantes das ameaças cibernéticas.

Grupos de APT e seus países de origem

10 PRINCIPAIS PAÍSES ASSOCIADOS A APTS COM BASE EM DETECÇÕES CORRELACIONADAS A CAMPANHAS ENTRE O ÚLTIMO TRIMESTRE DE 2023 E O PRIMEIRO TRIMESTRE DE 2024



SUMÁRIO

Ao observar os países de origem, a telemetria da Trellix de outubro de 2023 a março de 2024 também indica mudanças notáveis no cenário das atividades cibernéticas patrocinadas por países.

Grupos de ameaças ligados à China continuam sendo os maiores originadores de atividades de APT

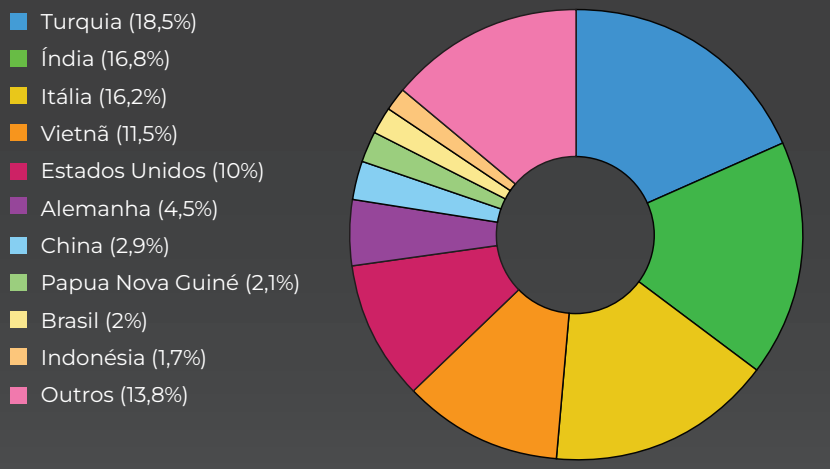
- **Escalada considerável em operações:** motivações geopolíticas e capacidades de cibersegurança estão evoluindo em diversas nações. Nossa telemetria observou o seguinte:
  a. Grupos de ameaças ligados à Rússia apresentaram um aumento significativo em detecções de APT, de até 31%, e sua contribuição proporcional aumentou em 4%. Isso indica uma escalada considerável em operações cibernéticas, possivelmente refletindo objetivos estratégicos mais amplos ou respostas à dinâmica global da cibersegurança.
  b. Grupos de ameaças ligados ao Irã também aceleraram de forma marcante suas atividades cibernéticas, com um aumento de 8%em detecções e uma alta de 3,89% na contribuição proporcional. Isso ressalta uma expansão significativa nas operações cibernéticas do Irã, alinhada com seus objetivos geopolíticos e seu envolvimento na guerra Israel-Hamas.
- **Diversificação mais ampla:** a China continua sendo origem do maior número de atividades de APT, com um leve aumento de 1% em detecções. Porém, sua contribuição proporcional para o total de detecções apresentou uma leve queda de -1%, o que pode sugerir uma diversificação mais ampla em origens de APT durante esse período. Em fevereiro deste ano também houve relatos de um empenho considerável por parte do grupo de APT Volt Typhoon, ligado à China, visando infraestrutura crítica dos EUA. Leia mais sobre isso na seção seguinte.
- **Mudança de estratégia:** por outro lado, grupos ligados à Coreia do Norte, ao Vietnã e à Índia apresentaram reduções dramáticas em suas atividades de APT, com quedas em detecções de -82% na Coreia do Norte, -80% no Vietnã e -82% na Índia. Particularmente notável é a queda significativa na contribuição proporcional da Coreia do norte (-6%), possivelmente indicando uma mudança de foco, estratégia ou capacidades.
- **Mais países emergindo:** grupos ligados ao Paquistão e à Bielorrússia tiveram aumentos consideráveis em suas atividades de APT, com aumentos de 55% e impressionantes 2019%, respectivamente, em detecções. Esses aumentos, particularmente a alta exponencial associada à Bielorrússia, corroboram a ascensão de elementos novos ou antes não reconhecidos na arena de APT.

  A categoria "Outros" mostra um aumento de 121% em detecções, indicando que as atividades de APT não estão limitadas aos países mais frequentemente citados. Essa diversidade ressalta a natureza global das ameaças cibernéticas e a necessidade de uma postura de cibersegurança mais ampla e adaptável.

Acompanharemos de perto esses novos padrões nos próximos meses.

SUMÁRIO

PAÍSES E REGIÕES VISADOS COM DETECÇÕES ASSOCIADAS DE APT



Países e regiões visados

Esta seção aborda os países e regiões nos quais a Trellix detectou atividades relacionadas a APT por grupos de APT entre o quarto trimestre de 2023 e o primeiro trimestre de 2024, revelando mudanças significativas em foco e estratégia entre esses perpetradores cibernéticos sofisticados.

> Os dados confirmam a natureza global das ameaças cibernéticas e os níveis variados de atenção que as diversas nações recebem dos grupos de APT.

O Trellix Advanced Research Center avalia com um grau moderado de confiança que os fatores seguintes afetaram a atividade detectada em determinados países e regiões

A Turquia tem apresentado um surto inédito em detecções relacionadas a APTs

Objetivos operacionais:
As detecções de ameaças contra a Turquia aumentaram impressionantes 1458%, o que se traduz em um aumento de 16% em sua contribuição proporcional no total de detecções. Esse aumento marcante indica uma mudança significativa no foco das ameaças cibernéticas em relação à Turquia, possivelmente refletindo tensões geopolíticas mais amplas ou objetivos operacionais específicos dos grupos de APT.

- **Importância estratégica:** Índia e Itália também tiveram aumentos consideráveis de 614% e 308%, respectivamente. A proeminência cada vez maior desses países na lista de alvos pode indicar sua importância estratégica crescente no domínio cibernético, seja por fatores econômicos, políticos ou tecnológicos.

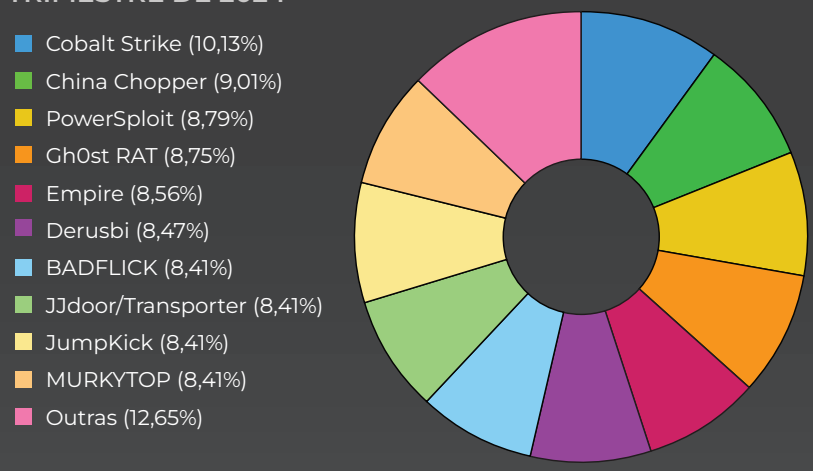
SUMÁRIO

- **Cenário em expansão:** é interessante observar que Vietnã e Estados Unidos, apesar de ainda gerarem detecções de APT significativas, apresentaram tendências diferentes. As detecções no Vietnã aumentaram 9%, mas sua contribuição proporcional diminuiu -9%, indicando uma ampliação do leque de alvos. Os Estados Unidos tiveram um aumento moderado de 15% em detecções, mas contabilizaram uma queda de -7% em sua contribuição proporcional, o que sugere uma diversificação nas estratégias de direcionamento dos grupos de APT.
- **Desdobramentos geopolíticos:** Alemanha, China, Papua Nova Guiné e Brasil tiveram aumentos em detecções, com Alemanha e China apresentando mudanças significativas em contribuição proporcional. Essa diversificação em termos de alvos reflete os ajustes estratégicos e oportunistas feitos pelos grupos de APT em resposta a posturas de cibersegurança e desdobramentos políticos globais.
- **Incremento da segurança nacional:** por outro lado, a Indonésia teve uma queda notável de -48% em detecções, aliada a uma diminuição de -4% em sua contribuição proporcional. Essa redução pode sugerir uma queda temporária de priorização ou um incremento bem-sucedido de medidas de cibersegurança nacional.
- **Consolidação do foco:** a categoria "Outros", que representa uma coletividade de vários outros países nos quais a Trellix detectou atividades relacionadas a APT, teve uma queda de -23% em detecções e um declínio de -21% em contribuição proporcional. Essa redução ressalta uma possível consolidação de foco por parte dos grupos de APT em alvos específicos de alto nível de interesse durante esse período.

Vemos possibilidades de que o cenário continue mudando rapidamente em decorrência de tendências geopolíticas.

Ferramentas maliciosas

10 PRINCIPAIS FERRAMENTAS MALICIOSAS DETECTADAS ENTRE O ÚLTIMO TRIMESTRE DE 2023 E O PRIMEIRO TRIMESTRE DE 2024



SUMÁRIO

A análise de ferramentas maliciosas utilizadas em campanhas de APT do quarto trimestre de 2023 ao primeiro trimestre de 2024 revela tendências notáveis nas preferências e táticas operacionais dos perpetradores de ameaças cibernéticas. As variações nas taxas de detecção e em suas contribuições proporcionais fornecem insights sobre o cenário de ameaças cibernéticas em evolução e sobre a dinâmica do uso de ferramentas entre esses grupos sofisticados.

As seguintes tendências foram observadas:

- **Ferramentas ofensivas tornando-se mais fortes:** o Cobalt Strike continua sendo uma ferramenta preferida de muitos grupos de ameaças, apesar de uma redução de 17% em detecções. A diminuição relativamente pequena em sua variação de contribuição proporcional (-1%) sugere que ele mantém sua popularidade e eficácia em operações cibernéticas, ressaltando o desafio da defesa contra ferramentas ofensivas versáteis e amplamente utilizadas.
- **Dependência de ataques à base de Web shells, PowerShell e acesso remoto:** China Chopper, PowerSploit e Gh0st RAT também apresentaram diminuições significativas em detecções, de 23%, 24% e 24%, respectivamente. Apesar dessas quedas, suas poucas mudanças em variação de contribuição proporcional indicam que continuam sendo parte integrante do kit de ferramentas dos perpetradores de ameaças. Essas ferramentas, conhecidas por suas capacidades em ataques de Web shell, explorações de PowerShell e acesso remoto, destacam que as operações cibernéticas continuam dependendo de ferramentas versáteis e comprovadas.
- **Ferramentas menos detectáveis:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick e MURKYTOP apresentaram tendências de queda semelhantes nas detecções, todas excedendo 25% de redução. Esse declínio uniforme pode refletir uma mudança mais ampla nas ferramentas preferidas por grupos de ameaças ou uma adaptação a contramedidas e técnicas de detecção, incentivando uma migração para ferramentas mais novas e menos detectáveis.
- **Inovação constante:** a categoria de "Outras" ferramentas maliciosas teve um aumento significativo em detecções, 30%, e um aumento marcante em sua variação de contribuição proporcional, 6%. Esse aumento ressalta a constante inovação e adaptação entre os perpetradores de ameaças enquanto estes exploram novas ferramentas e técnicas para evadir detecções e atingir seus objetivos.

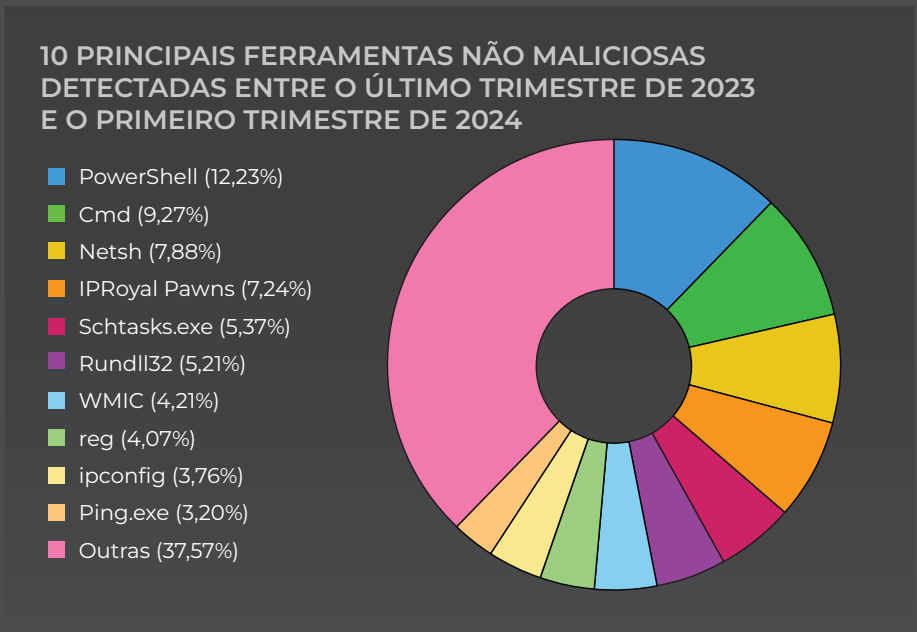
A evolução das preferências quanto ao uso de ferramentas maliciosas sinaliza a natureza adaptável dos perpetradores de ameaças em resposta a desdobramentos de cibersegurança.

> Conforme os mecanismos de defesa se tornam mais sofisticados, o mesmo ocorre com as ferramentas e táticas ofensivas dos grupos de APT.

A migração para um conjunto mais amplo de ferramentas, conforme indicado pelo aumento em "Outras" detecções, destaca a necessidade contínua de pesquisas, inteligência sobre ameaças e estratégias de defesa adaptáveis para mitigar o risco representado por essas ameaças cibernéticas em evolução.

SUMÁRIO

Ferramentas não maliciosas



> Essa prática, conhecida como aproveitamento da funcionalidade existente, complica o trabalho de detecção e confirma a sofisticação desses perpetradores de ameaças.

O uso de ferramentas não maliciosas em operações cibernéticas por grupos de APT do quarto trimestre de 2023 ao primeiro trimestre de 2024 ressalta um aspecto importante das ameaças cibernéticas modernas: o aproveitamento de ferramentas de sistema legítimas para fins maliciosos. Essa prática, conhecida como aproveitamento da funcionalidade existente, complica o trabalho de detecção e confirma a sofisticação desses perpetradores de ameaças. As estatísticas revelam variações significativas no uso dessas ferramentas, refletindo sua importância estratégica em operações cibernéticas

- **Versatilidade:** o PowerShell apresentou um aumento dramático de 105% em detecções e uma variação de contribuição proporcional de 1%. Esse surto ressalta sua versatilidade e seu poder na automação de uma ampla gama de atividades maliciosas, do reconhecimento à entrega de cargas virais.
- **Foco na manipulação de rede:** Netsh e IPRoyal Pawns tiveram ambos aumentos significativos em detecções, 99% e 102%, respectivamente. Essas ferramentas são frequentemente utilizadas para configuração de rede e tráfego de proxy, indicando um foco estratégico em manipulação de rede e técnicas de evasão.
- **Automação em escala:** Schtasks.exe apresentou a mais alta variação percentual entre as ferramentas listadas, 138%. Isso reflete a dependência crescente de tarefas agendadas para persistência e execução de cargas virais maliciosas sem intervenção direta do usuário.

SUMÁRIO

- **Mudanças táticas:** por outro lado, Rundll32 e WMIC apresentaram aumentos em seu uso, mas tiveram quedas na variação de contribuição proporcional, indicando uma mudança nas preferências táticas dos grupos de APT, apesar dessas ferramentas continuarem úteis.
- **Diversificação de ferramentas:** Cmd, o bom e velho interpretador de linha de comando de sistemas Windows, também teve um aumento considerável de uso, com detecções aumentando 65%. Apesar de seu uso crescente, sua variação de contribuição proporcional caiu -2,5%, sugerindo uma diversificação mais ampla no uso de ferramentas entre os grupos de APT.

  A categoria "Outros", que representa uma variedade de ferramentas menos frequentemente utilizadas ou mais especializadas, teve um aumento de 42% em detecções. Contudo, ela apresentou uma queda significativa na variação de contribuição proporcional (-21%), destacando a expansão do arsenal de ferramentas à disposição dos perpetradores de ameaças cibernéticas.

A evolução do cenário de utilização de ferramentas não maliciosas por grupos de APT ilustra a complexidade da detecção e defesa contra ameaças cibernéticas sofisticadas. A seleção e aplicação estratégicas dessas ferramentas revela uma compreensão profunda dos ambientes visados e o empenho para não serem detectados.

> **DICA DE CISO:** as defesas de cibersegurança precisam, portanto, avançar além da detecção de malware tradicional e incluir análise comportamental e detecção de anomalias para se contrapôr ao uso indevido de ferramentas legítimas em operações cibernéticas.

Dados coletados através de nossos sensores globais Trellix ATLAS, juntamente com insights estratégicos de relatórios aprovados pelo setor, fornecidos pelo Trellix Advanced Research Center, permitem aos nossos clientes identificar perpetradores de ameaças que estejam visando seus respectivos setores e utilizar nossa análise comportamental para detectar comportamentos anômalos em seus ambientes.

SUMÁRIO

Conclusão

A análise de atividades de ameaças persistentes avançadas (APT) do quarto trimestre de 2023 ao primeiro trimestre de 2024 esclareceu a dinâmica e a natureza cada vez mais complexa do cenário de ameaças cibernéticas. Nosso exame das estatísticas relacionadas às origens dos grupos de APT, aos países visados e ao uso de ferramentas maliciosas e não maliciosas revela várias tendências importantes que confirmam a evolução das estratégias dos perpetradores de ameaças cibernéticas.

Os grupos de APT continuam a demonstrar um alto nível de

1. Adaptabilidade e sofisticação
2. Aproveitamento de uma combinação de ferramentas maliciosas
3. Exploração de utilitários de sistema legítimos para realizar espionagem, perturbar operações e roubar informações confidenciais.

As variações significativas observadas na escolha dos alvos e nas táticas operacionais desses grupos refletem não apenas seus objetivos estratégicos, mas também sua resposta a medidas defensivas e desdobramentos globais de cibersegurança.

As mudanças dramáticas nas práticas de direcionamento de ameaças, com determinados países sofrendo aumentos consideráveis em atividades relacionadas a APTs, ressaltam as motivações geopolíticas que impulsionam essas operações cibernéticas. Da mesma forma, as mudanças no uso de ferramentas, inclusive o aumento marcante em táticas de aproveitamento de funcionalidades existentes, enfatizam o desafio constante que é detectar e combater ameaças de APT em um cenário no qual atividades legítimas e maliciosas estão cada vez mais entrelaçadas.

Além disso, a diversificação de origens de APT e a ampliação de suas estratégias de direcionamento indicam uma proliferação global de capacidades cibernéticas e a necessidade de uma abordagem de cibersegurança unificada e colaborativa.

> Está claro que nenhuma nação ou organização está imune ao alcance desses perpetradores de ameaças organizados.

SUMÁRIO

Volt Typhoon: ameaças de APT de estados-nações com foco na China

Grupos de perpetradores de ameaças ligados a estados-países continuaram representando uma grave ameaça a organizações comerciais e do setor público no mundo todo durante o último trimestre de 2023 e o primeiro trimestre de 2024. Esses adversários, frequentemente bem equipados e hábeis no uso de ameaças cibernéticas sofisticadas, visam redes incansavelmente ao longo de períodos de tempo prolongados utilizando habilidades e recursos superiores, em comparação com suas contrapartes hacktivistas ou cibercriminosas.

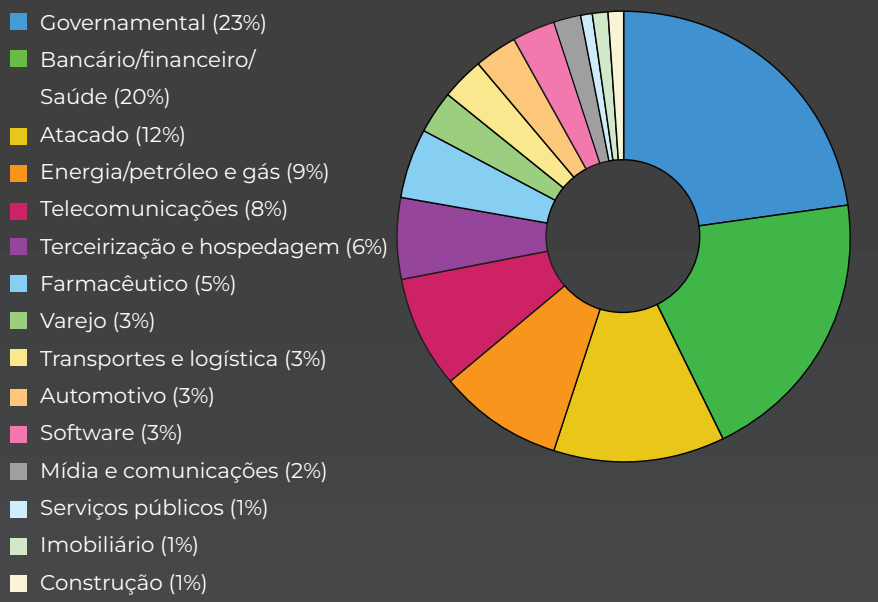
23%

Mais de 23% das detecções de atividades maliciosas foram direcionadas contra setores governamentais do mundo todo

Mais de 21 milhões de detecções de atividades de ameaças de grupos perpetradores de ameaças alinhados com a China

Com base em detecções de telemetria da Trellix, grupos de perpetradores de ameaças com patrocínio estatal ligados à China especificamente têm representado uma ameaça crescente ao setor governamental no mundo todo. Nossos dados mostram mais de 21 milhões de detecções de atividades de ameaças de grupos de ameaças alinhados com a China entre outubro de 2023 e março de 2024.

DETECÇÕES GLOBAIS DE GRUPOS DE APT AFILIADOS À CHINA



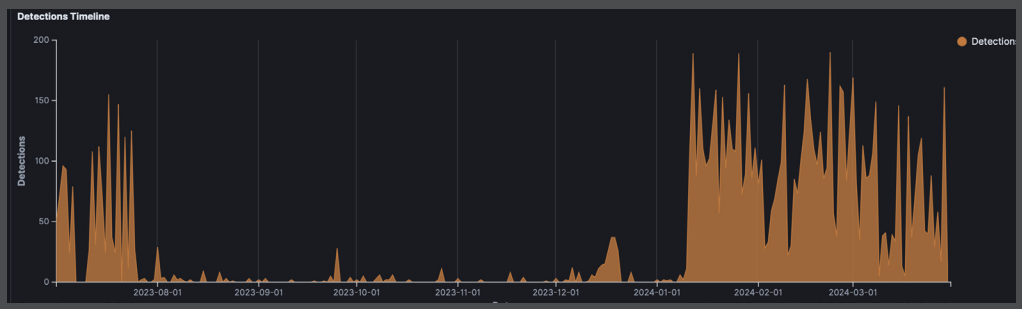
(Fonte: ATLAS)

Visão geral

Como grupo de APT com patrocínio estatal chinês relativamente novo, o Volt Typhoon destaca-se por seu padrão de comportamento peculiar e seus perfis de direcionamento, os quais divergem da coleta de inteligência e espionagem cibernética convencionais de outros grupos de APT associados à China. Relatos anteriores de fontes abertas sugerem que esse grupo de APT chinês pré-posicionou-se em redes de TI de controle industrial para viabilizar movimentações laterais com o objetivo de perturbar ativos e funções de tecnologia operacional (OT) na eventualidade de uma guerra ou crise geopolítica. Dados de telemetria da Trellix mostram que, desde a retomada de suas operações em janeiro de 2024, o Volt Typhoon visou repetidamente o setor governamental global, inclusive nos Estados Unidos, empregando técnicas de aproveitamento de funcionalidades existentes.

Cronologia operacional

Dados de telemetria global da Trellix mostram que o Volt Typhoon foi detectado pela primeira vez em meados de 2021, mas permaneceu em hibernação, com pouca ou nenhuma atividade, de agosto de 2023 a janeiro de 2024. Esse período de inação pode ter sido resultado de uma culminação de investigações de ameaças nos meses seguintes ao primeiro relatório de fornecedor sobre o Volt Typhoon, publicado em maio de 2023, que despertou a atenção global. Também pode ser devido a uma possível mudança da infraestrutura de ataque do Volt Typhoon durante esse período, como consequência de exposição pública, de modo que poucas atividades de ameaça foram detectadas.



Cronologia das detecções do Volt Typhoon de julho de 2023 a março de 2024 (fonte: Trellix ATLAS)

O Volt Typhoon retomou suas operações em meados de janeiro de 2024, com base nos dados de telemetria da Trellix. Desde meados de janeiro de 2024, a telemetria da Trellix detectou mais de 7.100 atividades maliciosas associadas ao Volt Typhoon, com picos periódicos durante o período de janeiro a março de 2024.

Detalhes das detecções do Volt Typhoon de janeiro a março de 2024

SUMÁRIO

Táticas, técnicas e procedimentos (TTPs)

Nossos dados de detecção sugerem que desde o retorno das operações em meados de janeiro de 2024, o Volt Typhoon aproveitou consistentemente várias ferramentas e funcionalidade nativas do Windows para executar comandos para fins maliciosos. Essas ferramentas, conhecidas como "living-off-the-land" (LOTL) — ou seja, ferramentas de uso duplo que consistem em funções e software legítimos disponíveis no sistema — tornaram-se cada vez mais populares entre grupos de perpetradores de ameaças com patrocínio estatal baseados na China, inclusive o Volt Typhoon. Netsh.exe é uma dessas ferramentas que podem ser utilizadas para vários fins maliciosos, como desativar configurações de firewall ou configurar um túnel de proxy para permitir acesso remoto a um host infectado. Ldifde é uma outra ferramenta aproveitada pelos perpetradores de ameaças do Volt Typhoon para coleta de informações.

Após obter acesso a um controlador de domínio, os atacantes podem utilizar o Ldifde.exe para exportar dados confidenciais ou efetuar mudanças autorizadas no diretório. De maneira semelhante, os perpetradores de ameaças do Volt Typhoon também utilizam a ferramenta Ntdsutil para fins maliciosos. Ntdsutil é uma ferramenta legítima que permite aos administradores realizar manutenção de bancos de dados; porém, ela também pode ser utilizada para criar uma descarga do Active Directory para fins de garimpo de credenciais e vazamento de dados confidenciais.

O grupo perpetrador de ameaças Volt Typhoon continuou utilizando ferramentas de código aberto, como FRP, Impacket e Mimikatz, em suas operações de ameaça. A telemetria da Trellix também detectou o Volt Typhoon utilizando os seguintes comandos e ferramentas LOTL entre fevereiro e março de 2023:

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- ping
- PowerShell
- PsExec

SUMÁRIO

As principais ferramentas MITRE ATT&CK aproveitadas pelo Volt Typhoon observadas em nossa telemetria foram as seguintes:

- Acesso inicial – T1190: Exploração de aplicativos voltados ao público
- Execução – T1106: API nativa
- Persistência – T1546: Execução disparada por evento
- Ampliação de privilégios - T1546: Execução disparada por evento
- Evasão de defesas – T1070.001: Limpeza dos logs de eventos do Windows
- Evasão de defesas – T1070: Exclusão de arquivos
- Evasão de defesas – T1027: Ocultação de arquivos ou informações
- Acesso por credenciais – T1003.003: NTDS
- Acesso por credenciais – T1003: Descarga de credenciais do SO
- Acesso por credenciais – T1110: Força bruta
- Acesso por credenciais – T1555: Credenciais de armazenamento de senhas
- Descoberta – T1069.002: Grupos de domínios
- Descoberta – T1069.001: Grupos locais
- Descoberta – T1083: Descoberta de arquivos e diretórios
- Descoberta – T1057: Descoberta de processos
- Descoberta – T1010: Descoberta de janela de aplicativo
- Coleta – T1560: Dados arquivados coletados
- Coleta – T1560.001: Compactação por utilitário
- Comando e controle – T1090.002: Proxy externo
- Comando e controle – T1105: Transferência de ferramenta de ingresso
- Comando e controle – T1132: Codificação de dados

Evolução do cenário de ransomware

No quarto trimestre de 2023, o cenário de ameaças cibernéticas presenciou uma escalada em ataques de ransomware, com as novas famílias do ano tendo um impacto cada vez mais significativo.

- **Ferramentas eliminadoras de EDR:** entre estas, o surgimento da quadrilha de ransomware D0nut foi particularmente interessante pelo uso inovador de uma ferramenta eliminadora de EDR, demonstrando uma tática avançada para contornar a detecção em endpoint e aumentar a eficácia de seus ataques. Saiba mais sobre isso na seção seguinte.
- **Exploração de vulnerabilidades:** esse período também viu uma continuação da tendência de exploração de vulnerabilidades críticas para viabilizar a distribuição de ransomware. Destaca-se a CVE-2023-4966, referida como Citrix Bleed e explorada por afiliados do LockBit 3.0, o que ressalta a vulnerabilidade contínua da infraestrutura crítica a ataques cibernéticos sofisticados. Além disso, a exploração do CVE-2023-22518 no Confluence Data Center e Confluence Server confirma o foco dos atacantes em infiltrar plataformas empresariais amplamente utilizadas para distribuir ransomware.

SUMÁRIO

A campanha de ransomware Cactus, que visou instalações do Qlik Sense explorando vulnerabilidades recém-descobertas, demonstrou ainda mais a agilidade dos atacantes na adaptação a cenários de segurança e exploração de vulnerabilidades emergentes. Isso fez do quarto trimestre de 2023 um trimestre agitado para os grupos de ransomware.

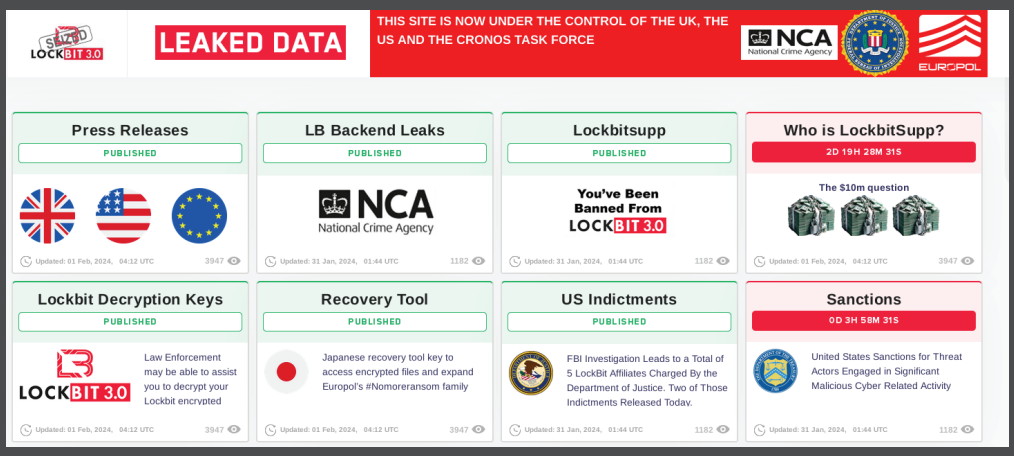
Contudo, o status quo estava prestes a mudar no primeiro trimestre de 2024 devido a uma ação policial marcante.

Operation Cronos: ação policial para interromper o LockBit

Em 19 de fevereiro de 2024 teve início uma ação policial internacional chamada Operation Cronos. Ela derrubou meticulosamente a notória quadrilha LockBit, dando ao grupo criminoso de longa data uma amostra de seu próprio remédio. As autoridades policiais não só apresentaram os já conhecidos avisos de derrubada, mas eventualmente conseguiram controle total sobre o site de vazamentos do grupo criminoso e exibiram alguns vazamentos de sua própria autoria ao expor o grupo criminoso para o mundo. Vários indiciamentos foram feitos e os afiliados ativos receberam uma mensagem amistosa de boas-vindas ao efetuarem login no backend do LockBit, deixando perfeitamente claro que suas identidades foram descobertas.

Essas ações objetivavam não só interromper as operações do LockBit, mas também atingir a reputação e quebrar a confiança na quadrilha.

Quando da finalização deste relatório, a Operation Cronos provocou mais uma surpresa. As autoridades policiais globais foram mais longe ao revelar a verdadeira identidade do líder do grupo LockBit. Essa não foi a única vitória das autoridades policiais. Em 1° de maio, o afiliado REvil, que atacou a Kaseya e muitas outras organizações, foi condenado a 13 anos de prisão e teve de pagar US$ 16 milhões em danos. Leia mais informações sobre como o Trellix Advanced Research Center ajudou no caso REvil aqui.



Ano passado, nosso relatório de fevereiro identificou o LockBit como o mais agressivo em pedidos de resgate. Esses criminosos cibernéticos utilizam uma variedade de técnicas para executar suas campanhas, inclusive a exploração de vulnerabilidades encontradas desde 2018. No decorrer de 2023, o LockBit continuou consistentemente sendo o grupo de ransomware predominante, com o maior número de vítimas postadas em seu site. Eles atacaram principalmente organizações norte-americanas e europeias de diversos setores, entre os quais o mais afetado foi o de serviços e bens industriais. Em 2023, o LockBit continuou evoluindo e introduzindo novas ferramentas e métodos em seu programa de ransomware. Entre os eventos dignos de nota, podemos citar o LockBit trabalhando no desenvolvimento do encriptador LockBit Green com base no código vazado do ransomware Conti, bem como as variantes do LockBit que visam o macOS. Além disso, testemunhamos a oferta do LockBit RaaS em 2023 como um novo lar para afiliados e outros programas de RaaS, como ALPHV e NoEscape, cujas operações foram derrubadas.

Após sofrer ações perturbadoras, vimos o LockBit tentar desesperadamente preservar sua reputação e restaurar sua operação lucrativa. Isso era de se esperar, considerando-se a publicidade das atividades criminosas do LockBit, mas no submundo do crime cibernético, é mais fácil restaurar um servidor do que recuperar anos de confiança. Ainda não se sabe quanta informação as autoridades policiais obtiveram contra a operação, o pessoal e os afiliados do LockBit.

> Essa incerteza gera um risco enorme para qualquer criminoso cibernético disposto a se relacionar com o LockBit e sua (antiga) equipe.

Após as ações policiais ficou muito claro que, entre os criminosos, é cada um por si. O Trellix Advanced Research Center observou outros perpetradores utilizando a versão LockBit Black vazada para se fazerem passar pela marca bem conhecida e obter seus próprios ganhos financeiros.

Impostores ou não, as vítimas que eles atingiram são reais e todos esses eventos dos dois últimos trimestres poderiam ser inspiração paro o roteiro de um filme.

Uma visão global do ransomware

Durante nossa pesquisa sobre atividade de ransomware no primeiro trimestre de 2024, investigamos múltiplas fontes: sites de vazamento, telemetria e relatos públicos. Seguem algumas palavras sobre cada uma dessas categorias.

- **Sites de vazamento:** tais sites são criados para apresentar provas de vítimas extorquidas que não pagaram o resgate exigido e permitem acompanhar a atividade da quadrilha criminosa. Também é importante observar que os sites de vazamento não refletem, necessariamente, a realidade do cenário. Como esses sites são operados por criminosos, nem todas as declarações são verídicas ou corretas. Além disso, se as quadrilhas honram sua palavra, as vítimas que pagam o resgate não são listadas, o que nos dá uma imagem incompleta. Os dados utilizados neste relatório referem-se a tendências gerais de sites de vazamento e não representam uma imagem significativa.

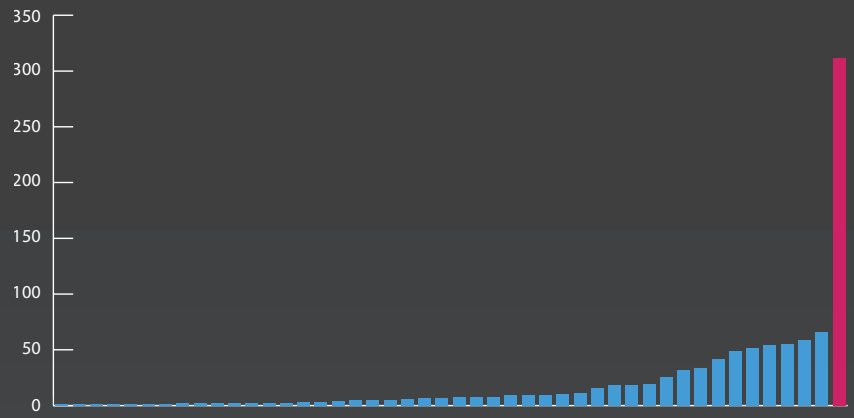
SUMÁRIO

- **Telemetria:** a telemetria é derivada do ecossistema de sensores da Trellix e as detecções indicam quando um arquivo, URL, endereço IP ou outro indicador é identificado por um de nossos produtos e relatado para nós. Isso não significa que toda detecção indica uma infecção, pois os clientes testam a detecção de determinados arquivos para ajustar melhor suas regras internas e isso também aparece nos logs agregados. Mesmo assim, esses dados continuam sendo úteis quando se observa o cenário como um todo, pois as tendências continuam evidentes.
- **Relatos públicos:** relatos de fornecedores e indivíduos foram processados por nosso Advanced Research Center para analisar características e identificar tendências. Cada relatório é inerentemente tendencioso e um exemplo disso pode ser visto na presença geográfica dominante de um determinado fornecedor em comparação com os demais. Essa diferença pode fazer com que uma entidade relate uma coisa enquanto outra entidade relata outra coisa diferente. Considerando a variedade de inclinações dos relatórios incluídos, não aplicamos um filtro específico.

Grupos de ransomware ativos

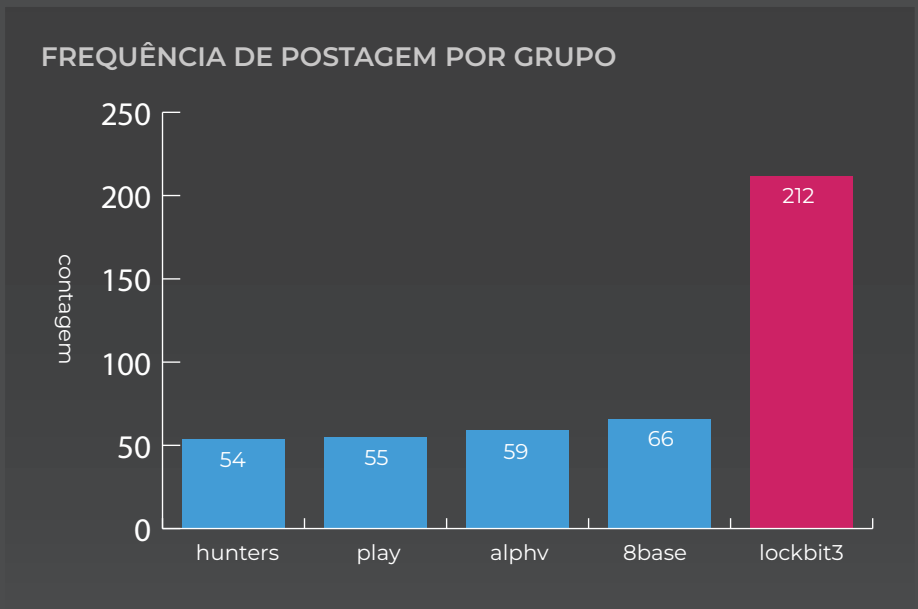
Quando observamos postagens de sites de vazamento agregadas desde o primeiro trimestre de 2024, muitas apresentam sinais de atividade. Ocasionalmente, vemos sites de vazamento postarem anúncios genéricos, mas a maioria é "prova" de extorsão ou vazamentos de dados de vítimas. Eles também postam frequentemente várias vezes a mesma vítima, o que pode inflar os números, pois uma mesma vítima é contada mais de uma vez nos dados.

FREQUÊNCIA DE POSTAGEM POR GRUPO



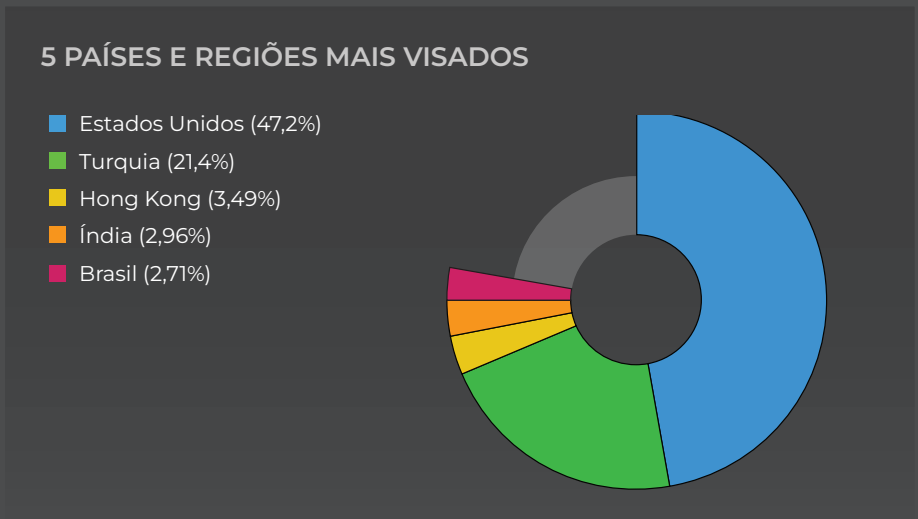
SUMÁRIO

Ao examinar a frequência dos cinco sites de vazamento mais ativos das quadrilhas de ransomware, os gráficos mostram um predomínio de atividades do LockBit. A atividade das quadrilhas excetuando o LockBit é de mais de 50 postagens por trimestre, em média, significando que o tempo médio entre a postagem de duas vítimas é inferior a dois dias. Conforme afirmado acima, esses números refletem vítimas não pagantes, ou seja, o número real de vítimas provavelmente é maior, embora não haja um método para definir quantas são.



Países e regiões visados

Com base na atividade contínua das quadrilhas de ransomware, podemos ver as detecções de ransomware na telemetria da Trellix. Os Estados Unidos geram a maioria das detecções, seguidos por Turquia, Hong Kong, Índia e Brasil.

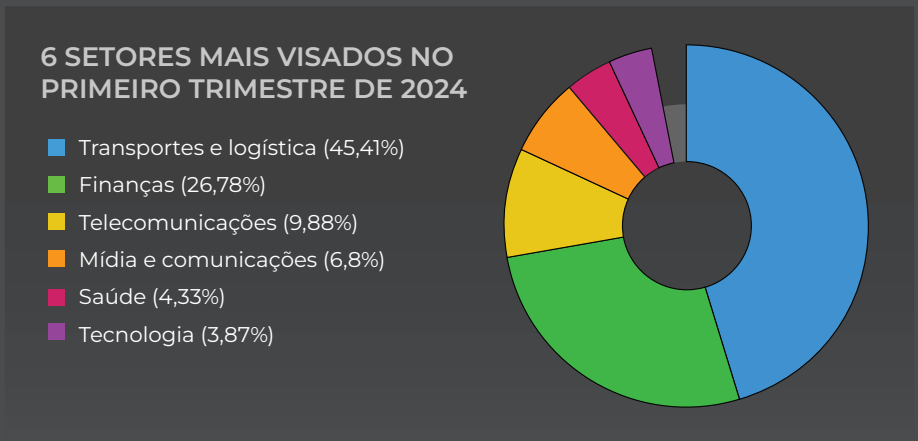


Considerando-se que o ransomware é uma ameaça para todos os setores em praticamente qualquer região geográfica, a métrica de detecção faz sentido em relação à população de clientes.

No trimestre anterior, a telemetria é semelhante, descontando-se o aumento em detecções na Índia e na China. Não temos indicações de que há uma campanha específica contra essas regiões e suspeitamos que testes de malware foram realizados, causando uma quantidade maior de detecções nas regiões referidas.

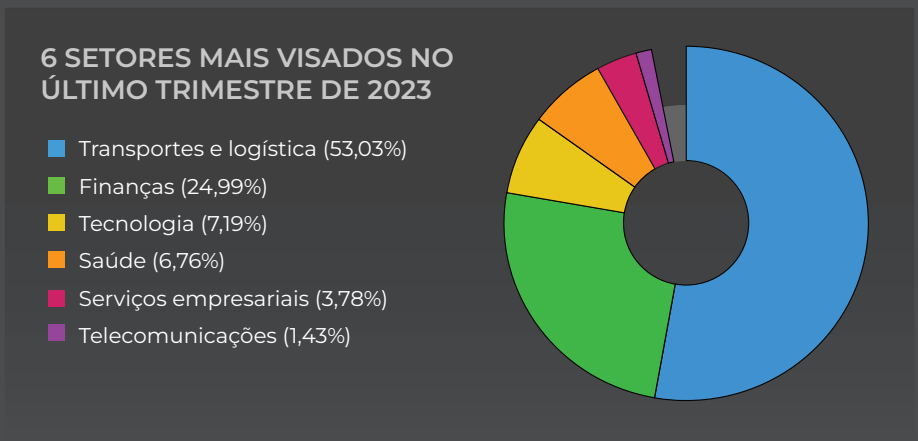
Setores visados

A agregação da telemetria global por setor mostra que metade das detecções vem do setor de transportes e logística e apenas um pouco mais que a quarta parte vem de serviços financeiros. Esses dois setores perfazem mais de 72% de todas as detecções, o que faz sentido: a disponibilidade desses serviços é de suma importância. Quando uma empresa de transportes não consegue entregar mercadorias devido a um ataque de ransomware, seu processo operacional não pode continuar, causando um imenso prejuízo financeiro. De forma semelhante, o setor financeiro baseia-se em confiança, enquanto o vazamento de dados confidenciais e/ou paralisação de uma empresa devido a um ataque de ransomware afeta empresas do setor financeiro em sua essência.



No último trimestre de 2023, os setores mais visados foram um pouco diferentes, embora sem diferenças nos dois principais setores. Esses dois foram responsáveis por uma parcela ainda maior, com um total combinado de 78% de todas as detecções no período em questão. Os setores de tecnologia e saúde caíram no primeiro trimestre de 2024 em comparação com o trimestre anterior, mas a diferença em si não pode ser atribuída a um ou mais eventos específicos.

SUMÁRIO



Ferramentas e técnicas

A última das três fontes mencionadas consiste em relatórios públicos. Com base nos relatórios coletados, é possível depreender técnicas MITRE, ferramentas associadas e linhas de comando.

> **DICA DE CISO:** estas podem ser utilizadas pelo "blue team" da organização do ponto de vista da detecção: ao se concentrar nas técnicas e ferramentas mais utilizadas, vários tipos de ataques de diversos perpetradores podem ser mitigados, a começar pelos mais eficazes. Além disso, exercícios de "red team" e "purple team" podem se concentrar nessas técnicas para determinar quais medidas de detecção estão em vigor.

A tabela abaixo mostra as técnicas mais frequentes, listadas em ordem descendente.

Técnicas MITRE ATT&CK	Campanhas exclusivas
Dados criptografados para maior impacto	31
Descoberta de arquivos e diretórios	23
PowerShell	23
Transferência de ferramenta de ingresso	21
Descoberta de informações do sistema	21
Arquivos ou informações ocultadas	19
Modificação do Registro	18
Windows Command Shell	17
Decodificação/decifração de arquivos ou informações	16
Interrupção de serviços	16

Levando em consideração o objetivo do ransomware, não surpreende que técnicas de descoberta de arquivos e diretórios e de criptografia de dados estejam no topo da lista. Ao comparar essas técnicas com as técnicas predominantes do quarto trimestre de 2023, nota-se que a maioria das principais técnicas da lista são semelhantes, embora sua colocação específica possa diferir.

SUMÁRIO

Técnicas MITRE ATT&CK	Campanhas exclusivas
Dados criptografados para maior impacto	45
PowerShell	29
Arquivos ou informações ocultadas	25
Descoberta de arquivos e diretórios	24
Windows Command Shell	24
Inibição da recuperação do sistema	23
Exploração de aplicativos voltados ao público	21
Transferência de ferramenta de ingresso	21
Descoberta de processos	21
Interrupção de serviços	21

Tal como na seção acima sobre APTs, os atacantes continuam aproveitando ferramentas legítimas para a prática de crimes. As ferramentas utilizadas influenciam as técnicas observadas, pois toda ferramenta é um meio para um fim, o qual é uma técnica neste caso. Por exemplo, o PowerShell e o Windows Command Shell são frequentemente utilizados para executar comandos adicionais no sistema, como a remoção de cópias ocultas, sendo esse o principal fator que contribui para a técnica "Inibição da recuperação do sistema". Essa também é a razão de serem as ferramentas mais utilizadas, conforme mostrado na imagem abaixo.

Nome da ferramenta de linha de comando	Campanhas exclusivas
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

SUMÁRIO

O uso de VSSAdmin, BCDEdit e wevtutil são sinais de que o ransomware está assegurando que o sistema da vítima não volte a um estado normal, como o anterior ao ataque. A utilização de reg mostra as mudanças no Registro, as quais podem ser feitas por uma variedade de motivos. O malware frequentemente usa o Registro para fins de persistência, mas o ransomware não é afeito a persistência, visto que não há razão que a justifique, uma vez criptografados os dados. Em vez disso, ele pode alterar outras configurações para permitir determinadas ações que normalmente não seriam possíveis. Rundll32 é frequentemente utilizado para carregar e executar uma DLL, mas isso também é frequentemente alvo de injeção de processos.

Tal como no trimestre anterior ao mencionado acima, o PowerShell e o prompt de comandos encimam a lista por exatamente o mesmo motivo. VSSAdmin e BCDEdit estão presentes também, embora o Windows Event Log Utility (wevtutil) não esteja presente na lista das principais ferramentas. Dadas as poucas ocorrências de todas as ferramentas mencionadas, com a frequência maior sendo de 13 em qualquer dos trimestres, não é surpresa que nem todas as campanhas utilizem as mesmas ferramentas. Um pequeno desvio pode levar à exclusão de tais ferramentas.

Nome da ferramenta de linha de comando	Campanhas exclusivas
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

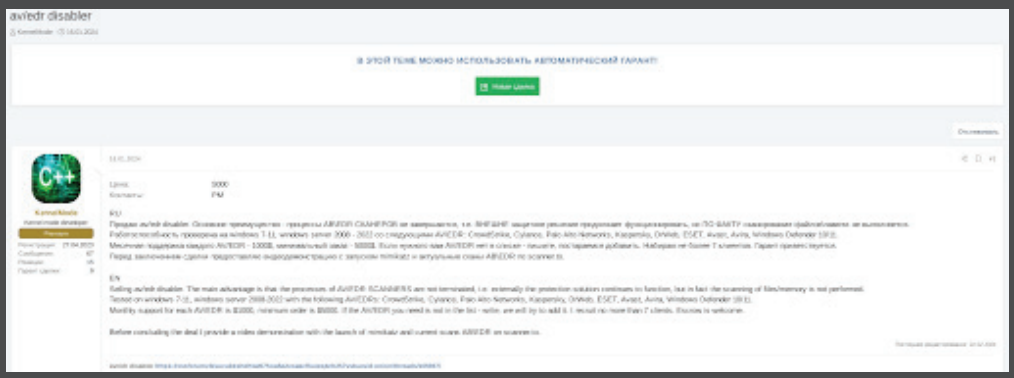
A ameaça do ransomware persiste.

SUMÁRIO

O surgimento de ferramentas de eliminação e evasão de EDR

A adoção global de soluções de EDR por muitas organizações provou melhorar a detecção, a compreensão e a resposta aos ataques mais sofisticados. Os perpetradores de ameaças de hoje em dia costumam contar com binários já existentes (LOLBins) e métodos de ataque mais complexos, mas a presença de tecnologia de EDR tornou mais difícil para os atacantes não serem detectados.

Contudo, a segurança continua sendo um jogo de gato e rato e os atacantes estão tentando encontrar maneiras de evadir ou desativar soluções de EDR. Essa movimentação deu lugar a toda uma onda de eliminadores de EDR e ferramentas/técnicas de evasão, algumas das quais estão sendo oferecidas em fóruns clandestinos de criminosos cibernéticos. Vimos anteriormente, por exemplo, que a quadrilha de ransomware D0nut ganhou destaque graças a seu próprio eliminador de EDR.



Anúncio de desativador de EDR no fórum clandestino XSS

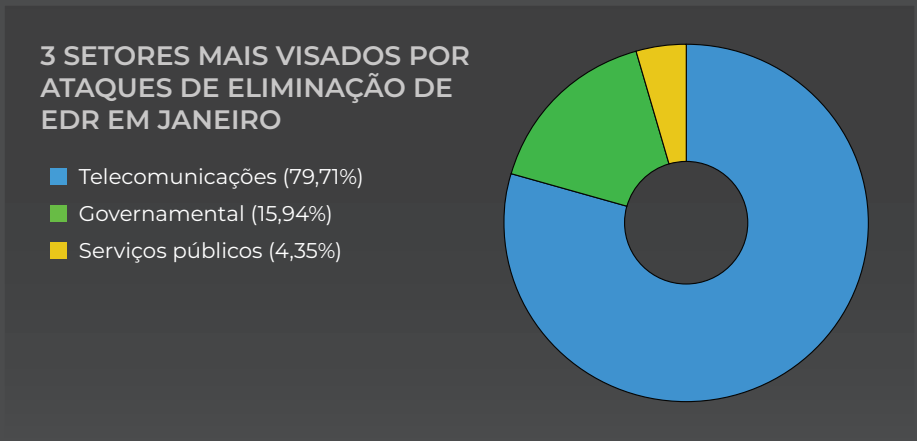
Campanha de janeiro utilizando a ferramenta EDR Terminator do Spyboy

Uma técnica comum consiste em explorar drivers vulneráveis para conseguir execução de código privilegiado, sendo referida como ataque Bring Your Own Vulnerable Driver (BYOVD, algo como “traga o seu próprio driver vulnerável”).

Um exemplo desse método é a ferramenta eliminadora de EDR “Terminator” que foi oferecida por um perpetrador de ameaças chamado Spyboy. A ferramenta Terminator aproveita um driver de Windows legítimo, porém vulnerável pertencente à ferramenta antimalware Zemana para executar código arbitrário de dentro do kernel do Windows, provavelmente explorando a CVE-2021-31728. O Terminator apareceu on-line em meados de 2023 e a Trellix publicou em sua base de conhecimentos um artigo detalhado com uma cobertura do produto que pode ser encontrado aqui.

Entre 11 e 17 de janeiro de 2024, o Trellix Advanced Research Center observou um conjunto incomum de detecções do Terminator de Spyboy na telemetria da Trellix – uma nova campanha. Essa campanha do Terminator apresentou um pico de três dias durante o período de seis dias em questão e foi detectada múltiplas vezes em uma mesma organização governamental, uma empresa nacional de serviços públicos e uma empresa de comunicações via satélite. Dados os alvos específicos, a Trellix avalia com um alto grau de confiança que o ataque esteve relacionado ao conflito russo-ucraniano.

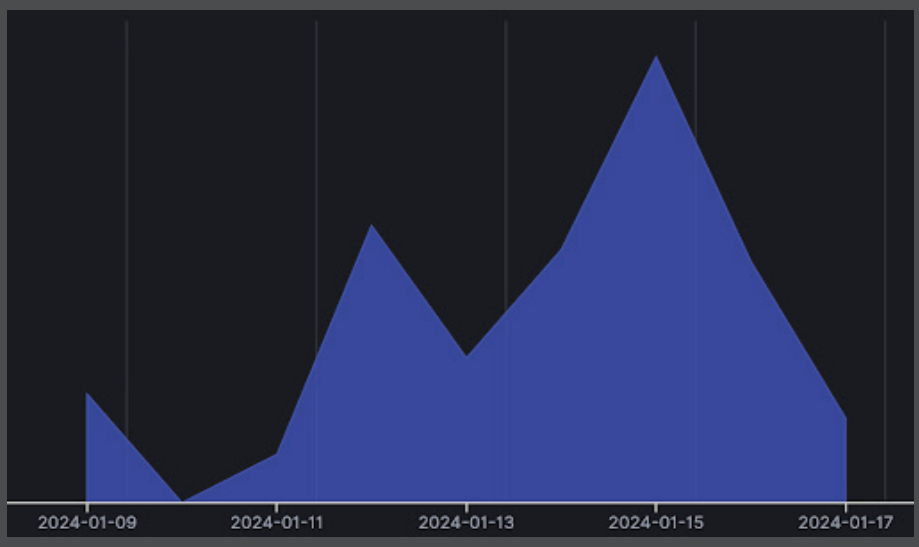
SUMÁRIO



Detecções do Trellix ATLAS da campanha EDR Terminator visando a Ucrânia em janeiro

Mais eliminadores de EDR observados

Anteriormente em 2023, uma ferramenta com finalidade semelhante foi descrita pela Sophos – AuKill. Ela também utilizava um driver vulnerável trazido por ela própria (BYOVD). Os drivers utilizados nos casos do EDR Terminator e do AuKill são diferentes, mas ambos são drivers benignos. Por outro lado, algumas campanhas de 2022 que utilizaram ferramentas semelhantes carregaram drivers maliciosos personalizados.



SUMÁRIO

O abuso de drivers benignos para esses fins dificulta a detecção de tais ataques e coincide com o uso supracitado de LOLBin. Embora binários e drivers sejam tecnicamente diferentes, a intenção e a motivação são semelhantes, se não idênticas. O HermeticWiper de 2022 também vem à mente no que se refere ao uso de drivers benignos. Nesse caso, o driver foi utilizado para eliminar uma máquina em vez de desativar o antivírus. Uma sobreposição adicional com o uso do EDR Terminator mencionado anteriormente e com a atribuição do HermeticWiper é a utilização por um perpetrador pró-Rússia.

Também vimos um exemplo da rede de distribuição de conteúdo Discord sendo utilizada para distribuição de malware em um de nossos clientes da América Latina. Nossa equipe observou que o Discord continua a ser utilizado dessa forma em ataques de malware.

> **DICA DE CISO:** é absolutamente essencial que todo SOC monitore atentamente sua EDR. Alertas e registros em logs precisam ser configurados de maneira que o SOC seja notificado imediatamente caso ferramentas de EDR sejam desativadas, para que providências adequadas possam ser tomadas. A desativação de ferramentas de EDR pode ser um indício de adulteração e uma reação rápida é fundamental para limitar o acesso do atacante à sua rede. Também é da maior importância utilizar uma estratégia de defesa em profundidade, possibilitando que outras ferramentas, como a sua plataforma de detecção e resposta de rede (NDR), detectem possíveis incidentes, pois agir rapidamente é fundamental para limitar o acesso que o atacante obtém à sua rede.

SUMÁRIO

O e-mail continua sendo um terreno fértil para os atacantes

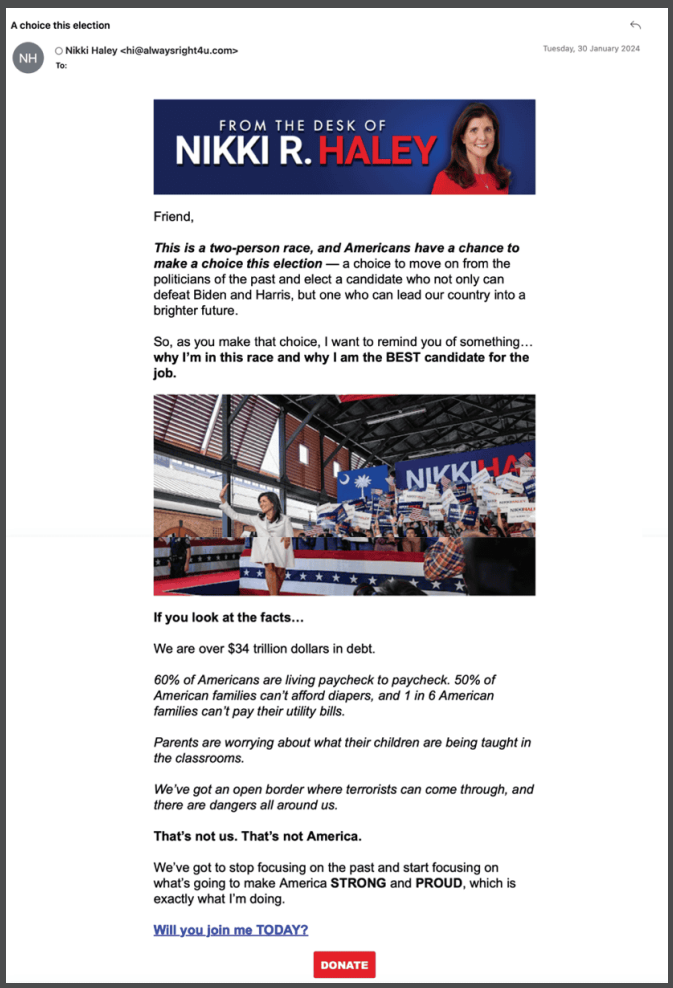
A Trellix processa dois bilhões de amostras de e-mail e 93 milhões de anexos de e-mail por dia. Assim se obtém uma imensa quantidade de dados e uma oportunidade de observar novas técnicas aproveitadas por atacantes que visam vítimas por e-mail.

Fraudes de doação eleitoral

Fraudes de phishing de doações eleitorais exploram a boa vontade das pessoas e seu apoio a candidatos políticos aproveitando-se de seus sentimentos patrióticos e utilizando nomes de candidatos políticos famosos. No primeiro trimestre de 2024, nossos pesquisadores descobriram criminosos cibernéticos aproveitando-se de serviços de marketing legítimos para criar páginas de doações convincentes, adornadas com imagens de candidatos junto com bandeiras americanas, instando os destinatários a doar dinheiro.

Essas fraudes utilizam URLs de serviços de marketing autênticos para enganar os destinatários, levando-os a crer que os e-mails são legítimos. No entanto, os e-mails são enviados para capitalizar a generosidade das pessoas. Links dentro dos e-mails direcionam os usuários a páginas de doação, nas quais eles são instados a fornecer dados financeiros ou enviar contribuições para as contas ou endereços de carteira dos remetentes.

Nossos pesquisadores de e-mail observaram os seguintes e-mails maliciosos aproveitando-se de doações eleitorais.



A choice this election

NH Nikki Haley <hi@alwaysright4u.com>
To:

Tuesday, 30 January 2024

FROM THE DESK OF NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

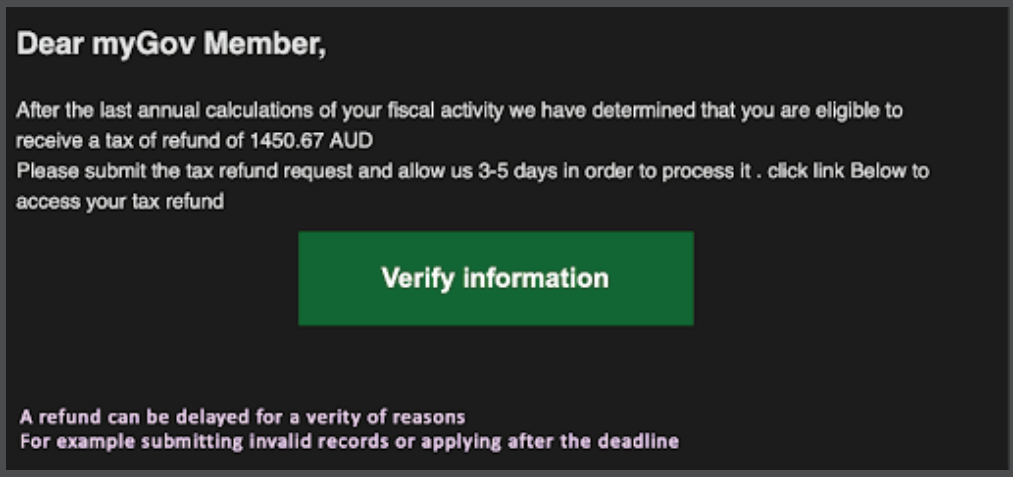
Phishing fiscal

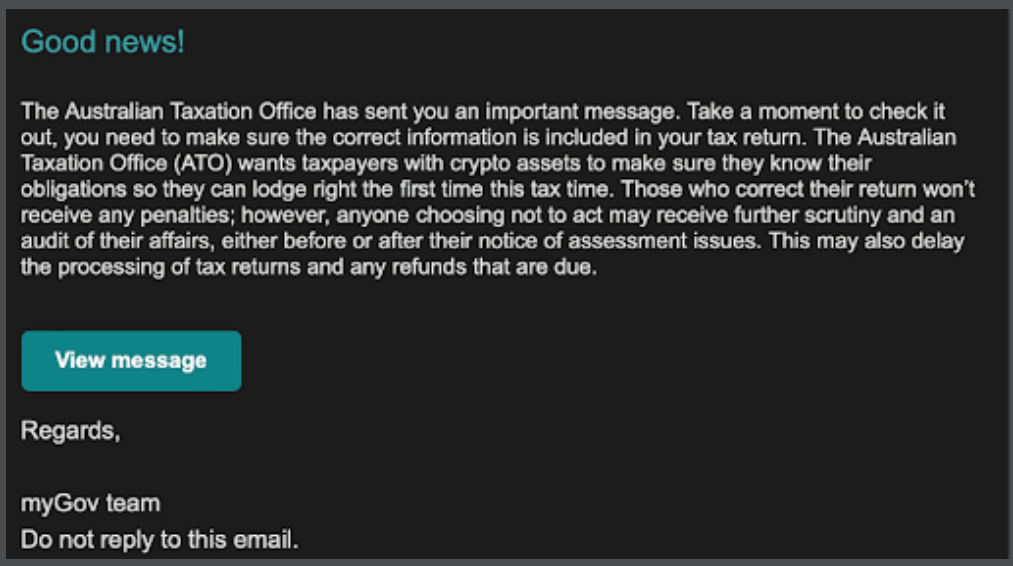
No contexto de impostos, os ataques de phishing são particularmente preocupantes. Fraudadores fazem-se passar por órgãos governamentais, autoridades fiscais ou serviços idôneos de preenchimento de declarações de imposto de renda para induzir as pessoas a fornecer informações pessoais. Eles podem alegar que você deve impostos atrasados, tem declarações não enviadas ou restituições a receber. Seu objetivo final é obter sua documentação, dados de suas contas bancárias ou outros dados valiosos. O e-mail contém links que parecem levar a sites de serviços fiscais ou governamentais oficiais, mas na verdade redirecionam você a sites fraudulentos criados para roubar dados.

A Trellix também observou um surto em e-mails desse tipo alegando vir da autoridade fiscal australiana no primeiro trimestre de 2024, detectando-os com sucesso.

SUMÁRIO

Veja a seguir uma amostra da campanha, onde se pode ver claramente que os atacantes tentam gerar um senso de urgência para que o usuário clique no link relacionado a uma restituição de imposto.





A corrida armamentista da inteligência artificial generativa: descobertas do submundo do crime cibernético

Inteligência artificial e autoaprendizagem não são mais acessíveis apenas para organizações com fundos ilimitados. ChatGPT e similares podem ser utilizados por qualquer um, inclusive por criminosos. Assim, a inteligência artificial tornou-se uma corrida armamentista entre elementos idôneos e malfeitores. A inteligência artificial é poderosa e deve ser utilizada com responsabilidade para se alcançar objetivos empresariais, mas é imperativo que as organizações não permitam que os atacantes se aproveitem. Precisamos utilizar capacidades novas para superar os criminosos cibernéticos conforme suas táticas são aprimoradas e suas armas se tornam mais poderosas.

SUMÁRIO

DICA DE CISO: o papel do CISO tornou-se ainda mais essencial, pois é a ele que se recorre para navegar por esse cenário em evolução. Com os ataques cibernéticos em alta, a crescente pressão da inteligência artificial e o aumento de responsabilidades, não é surpresa que 90% dos CISOs sintam-se sob uma pressão cada vez maior. Acompanhar o ritmo da inteligência artificial e da inteligência artificial generativa é fundamental e quase todos os CISOs concordam que suas organizações poderiam fazer mais. Leia mais sobre isso no último relatório da Trellix, A mente do CISO: decodificando o impacto da inteligência artificial generativa.

Os perpetradores de ameaças são atraídos pela inteligência artificial generativa por conta de suas capacidades aceleradas e acessibilidade econômica. Mais significativo é que ela agrega conhecimento: malfeitores podem elaborar e-mails de spear phishing em qualquer idioma com informações de login, logotipos e gramática perfeita. Eles podem localizar, criar e testar explorações dez vezes mais rapidamente, sem qualificações de elite.

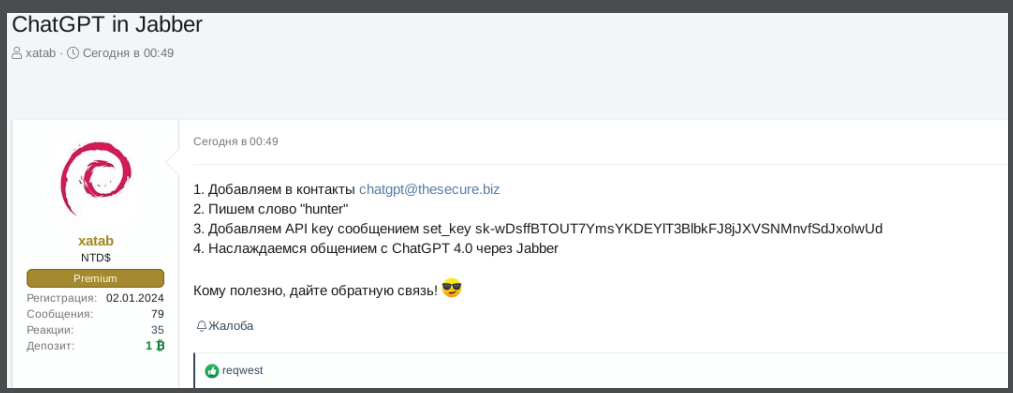
A equipe de nosso Advanced Research Center vasculha regularmente o submundo do crime cibernético para acompanhar as tendências. A inteligência artificial generativa está ganhando impulso com os criminosos cibernéticos e estes estão compartilhando seus sucessos e vendendo suas ferramentas. Desde nosso último relatório, temos observado o seguinte a partir do início de 2024.

Projeto "ChatGPT in Jabber" possivelmente utilizado por um grupo de APT de criminosos russos

Em janeiro, observamos o destacado perpetrador de ameaças **xatab** de um fórum clandestino XSS procurando um desenvolvedor para criar um "ChatGPT 4.0 in Jabber", juntamente com uma API e instruções sobre como utilizá-lo.

Além do uso criminoso de integrações com LLM, também é possível que a intenção/motivação de **xatab** com o projeto "ChatGPT in Jabber" seja interceptar e coletar correspondência de perpetradores de ameaças, espionar suas atividades para obter inteligência e conhecimento sobre os interesses dos criminosos cibernéticos e sobre os principais tópicos e áreas de suas atividades ilícitas auxiliadas pela inteligência artificial generativa.

Nós observamos o seguinte -



xatab compartilhou no fórum XSS instruções e a chave de API do "ChatGPT in Jabber"

SUMÁRIO

```
Python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

Em 31 de janeiro de 2024, **xatab** ofereceu US$ 2.000 por seu projeto "ChatGPT in Jabber" no fórum XSS. Com base na recente reclamação feita no XSS pelo participante **germans**, que criou o bot solicitado e que foi a princípio ignorado por **xatab**, parece que **germans** concordou em desenvolver o bot ChatGPT em Jabber por US$ 1.500. O bot foi criado para os servidores de Jabber dos fóruns Exploit (@exploit[.]im) e XSS (@thesecure[.]biz) e **xatab** postou o mesmo em ambos os fóruns Exploit e XSS na darknet, supostamente para testá-lo e obter feedback dos membros dos fóruns. O bot talvez tenha sido baseado no projeto xmppgpt.

xatab tem múltiplas postagens nos fóruns Exploit/XSS nas quais alega ser uma equipe de APT (conhecida em determinados círculos de testadores de penetração experientes) interessada em contratar um intermediador de acessos corporativos de organizações dos EUA/Reino Unido/Canadá/Austrália para uma cooperação frutífera. Ele ofereceu 20% de participação de receita para cada acesso e depositou um BTC nos fóruns Exploit e XSS para comprovar suas intenções e a seriedade de sua oferta.

Ao oferecer o ChatGPT 4.0 gratuito para a comunidade do crime cibernético, **xatab** está atingindo dois objetivos:

1. Atuar como facilitador e viabilizador de quem estiver disposto a ajudar os perpetradores de ameaças a inovar e a adotar inteligência artificial generativa em suas operações
2. Tentar criar uma base de conhecimentos sobre inteligência artificial generativa para aprender com outros criminosos cibernéticos ou mesmo roubar suas ferramentas e ideias inovadoras

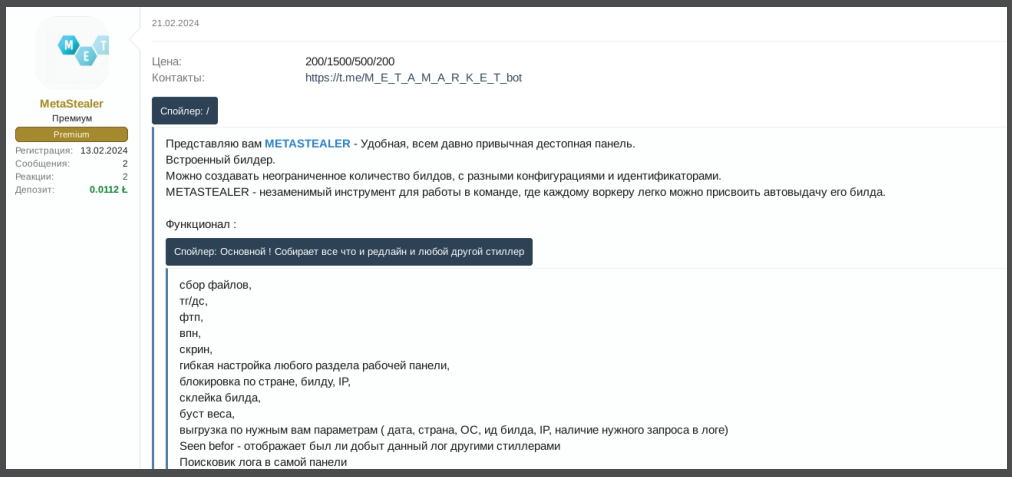
A Trellix testou o projeto "ChatGPT in Jabber" conforme as instruções fornecidas e ele parece funcionar como anunciado pelo perpetrador de ameaças.

Adoção de inteligência artificial generativa em malware para roubo de informações

Em 21 de fevereiro de 2024, nossos pesquisadores observaram um perpetrador de ameaças MetaStealer anunciando uma versão nova e aprimorada do **MetaStealer** no fórum XSS. MetaStealer é um malware de roubo de informações que surgiu pela primeira vez em 2021. Acredita-se que seja uma derivação do notório malware de roubo de informações Redline. Várias versões do **MetaStealer** foram vistas na Internet, mas a versão recente identificada pela Trellix tem um recurso baseado em inteligência artificial generativa para evitar detecções ainda mais.

Na captura de tela abaixo, o texto laranja ao lado de "35)" diz "Geração de assinaturas exclusivas para cada compilação; com o uso de inteligência

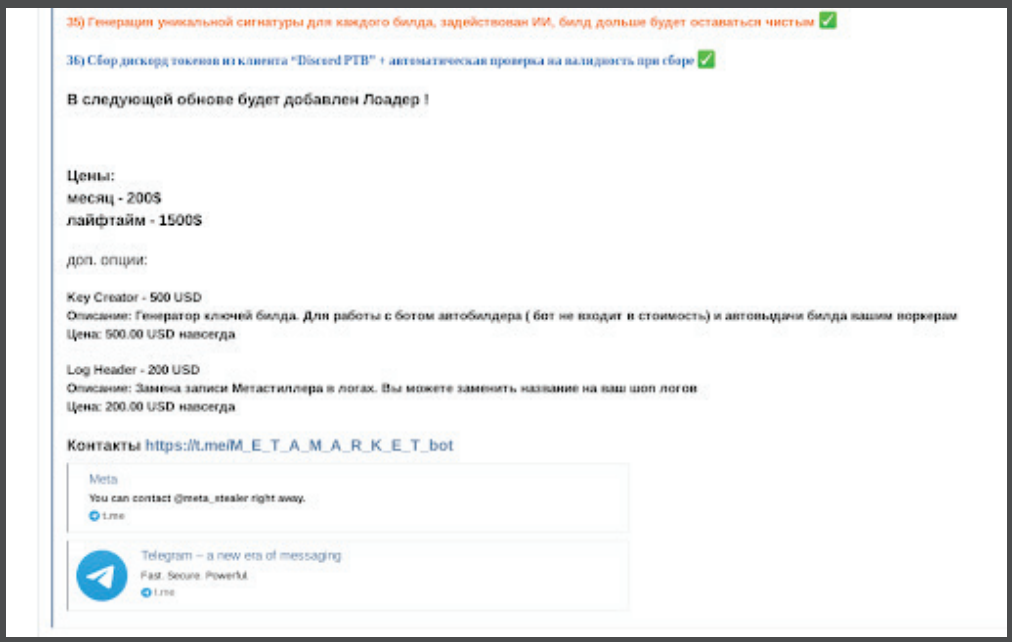
SUMÁRIO



MetaStealer compartilhou no fórum XSS uma versão modificada do MetaStealer

artificial, a compilação permanece limpa (ou não detectada) por mais tempo", sugerindo que os desenvolvedores do MetaStealer incorporaram um novo recurso baseado em inteligência artificial generativa em seu malware de roubo que os permite criar compilações exclusivas do MetaStealer para evadir detecções e permanecer fora da vista de sistemas AV/EDR por um período mais longo do que antes.

Um outro exemplo é um malware de roubo de informações bem estabelecido, chamado LummaStealer. Desde agosto de 2023,

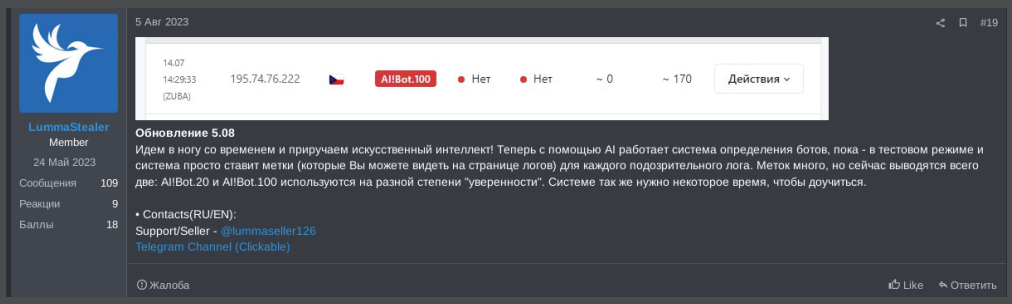


O MetaStealer modificado tinha um recurso incorporado baseado em inteligência artificial generativa para evasão de defesas

observamos a equipe do LummaStealer testando um recurso baseado em inteligência artificial que permite aos seus usuários detectar bots em sua lista de logs. O sistema baseado em inteligência artificial incorporado no LummaStealer é, potencialmente, uma rede neural personalizada treinada para determinar se um usuário suspeito conectado é ou não um bot. O LummaStealer utiliza um rótulo **AI!Bot.<número>** para categorizar o log detectado como um bot, onde

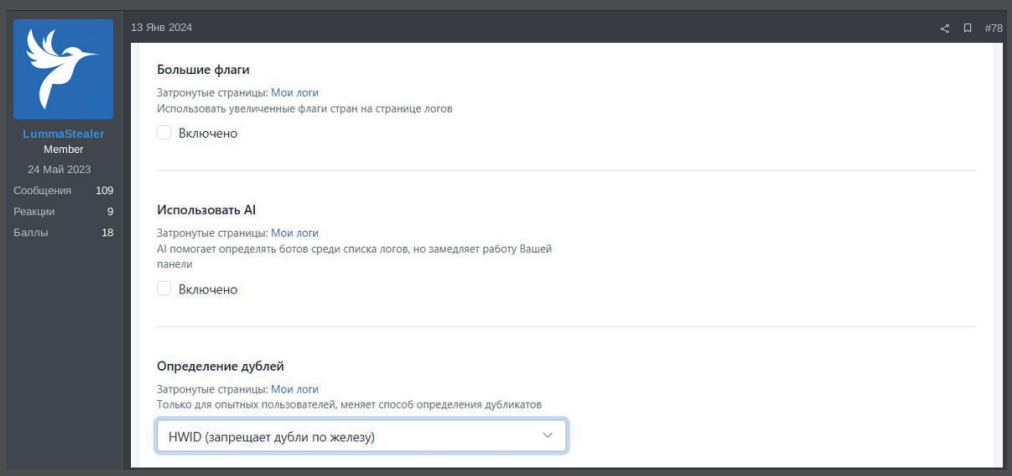
SUMÁRIO

<número> parece estar em uma faixa de 0 a 100, representando o grau de certeza da detecção do bot:



Postagem do LummaStealer no fórum RAMP onde o perpetrador informou que seu malware de roubo de informações possui um recurso baseado em inteligência artificial para detectar bots em sua lista de logs

O **LummaStealer** advertiu a seus usuários que a rede neural ainda estava sendo treinada e que levaria algum tempo para melhorar a precisão da detecção. Além disso, em janeiro de 2024, o **LummaStealer** recomendou que o recurso baseado em inteligência artificial generativa fique desativado por padrão, pois ele retarda o trabalho do painel do LummaStealer.

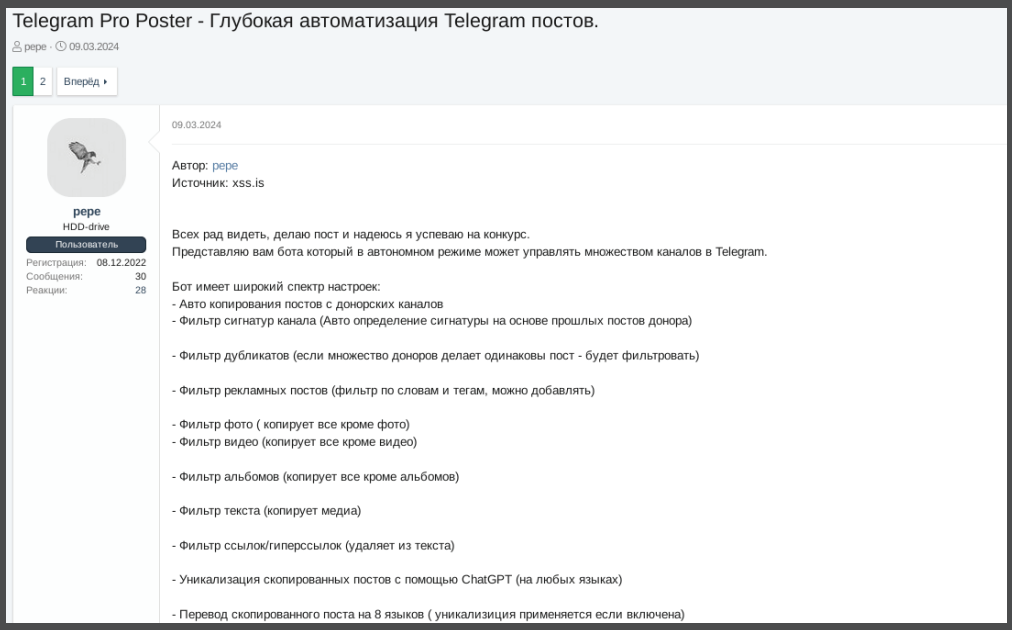


Postagem do LummaStealer no fórum RAMP onde o perpetrador informou que a detecção de bots baseada em inteligência artificial fica desativada por padrão

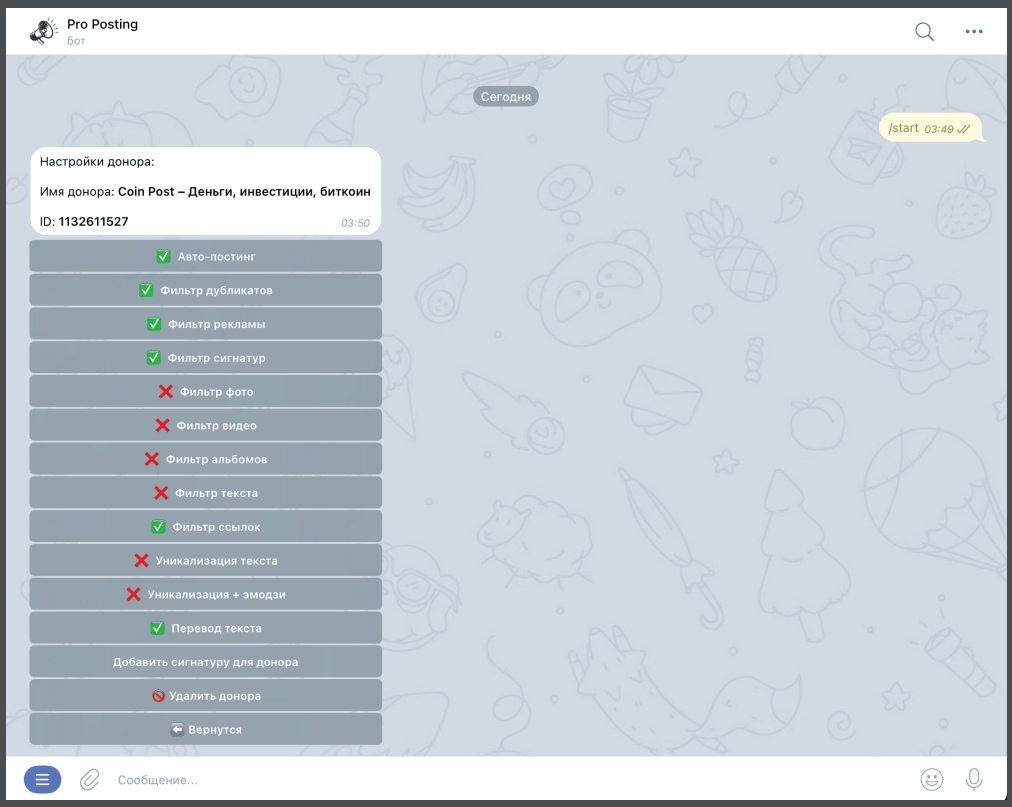
Projeto de bot “Telegram Pro Poster”

No início de março de 2024, a Trellix observou um perpetrador de ameaças chamado pepe postando seu projeto “Telegram Pro Poster” no fórum XSS como parte de uma competição clandestina de ferramentas/software malicioso. Telegram Pro Poster é um bot para “automação profunda de postagens no Telegram”. Esse bot baseado em python permite que os usuários gerenciem vários (uma quantidade ilimitada de) canais do Telegram de maneira autônoma, copiando automaticamente as postagens de canais de Telegram “doadores” para os canais de destino. Entre diversos recursos de filtragem de postagens, esse bot possui dois recursos de inteligência artificial generativa incorporados para traduzir mensagens do Telegram e parafrasear uma determinada postagem utilizando o ChatGPT.

SUMÁRIO



Postagem no fórum XSS sobre o bot baseado em inteligência artificial generativa do Telegram Pro Poster



Recursos de filtragem do Telegram Pro Poster, inclusive recursos de “unique-alisation” (exclusivização) desativados por padrão

A Trellix obteve o código-fonte do Telegram Pro Poster e identificou os seguintes fragmentos de código, responsáveis pela tradução das postagens copiadas dos canais doadores em oito mensagens consecutivas, por meio da API do ChatGPT, antes de enviá-las para os canais de Telegram de destino:

SUMÁRIO

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

O segundo recurso, chamado “unique-alization” (algo como “exclusivização”) fica desativado por padrão, mas quando é ativado, utiliza OPEN_AI_KEY para solicitar ao ChatGPT que parafraseie o texto fornecido em um idioma especificado e, opcionalmente, acrescente um emoji.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

SUMÁRIO

A comunidade de criminosos cibernéticos do XSS já está compartilhando seu feedback positivo sobre o projeto "Telegram Pro Poster", afirmando que é um projeto interessante e que, em mãos competentes, certamente será útil. Um outro perpetrador de ameaças avisou no thread do fórum XSS que esse bot já está sendo adotado na prática por vários canais do Telegram.

POSFÁCIO

A corrida continua

A inteligência operacional sobre ameaças proporciona insights sobre a natureza, a intenção e a temporização de ameaças cibernéticas específicas. Ela é mais detalhada e contextual que a inteligência tática, incluindo informações sobre as táticas, técnicas e procedimentos (TTPs) dos perpetradores de ameaças.

As organizações podem utilizar inteligência operacional para compreender o contexto mais amplo dos ataques cibernéticos, como as motivações por trás deles ou os métodos utilizados, ajudando as equipes de segurança a antever e a se preparar para tipos específicos de ataque.

Em meu trabalho com clientes, eu sei que o objetivo mais importante de todo CISO é limitar o risco para sua organização. A aplicação de inteligência operacional sobre ameaças é uma maneira concreta de limitar esse risco, pois permite que os CISOs e suas equipes de operações de segurança vejam à frente e se posicionem. Ela os capacita a identificar brechas em suas medidas de segurança ao longo de toda a extensão da organização e a pensar como seus oponentes, buscando desnorteá-los.

Nós compartilhamos nossa inteligência sobre ameaças para oferecer a você uma plataforma sólida, baseada em fatos e que sirva de base para algumas das decisões mais importantes que você precisará tomar. Nosso objetivo é ajudar você a melhorar consideravelmente a sua defesa cibernética e vencer os atacantes na próxima etapa da corrida - na forma que você preferir.

Vamos lá!

Ashok Banerjee,
TECNÓLOGO-CHEFE DA TRELLIX

SUMÁRIO

METODOLOGIA

Coleta: a Trellix e os especialistas de nível internacional de nosso Advanced Research Center coletam as estatísticas 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 líderes de segurança cibernética e suas equipes de operações de segurança 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.

Aplicação: como usar estas informações

É imperativo que todo processo e 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.

SUMÁRIO

- 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.

Como compreender a análise deste relatório

Compreender os insights e dados deste relatório requer uma breve revisão das seguintes diretrizes:

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

SUMÁRIO

RECURSOS

Arquivos dos relatórios de ameaças

A mente do CISO

SIGA TRELLIX ARC NO X

Trellix ARC

Visualize os arquivos dos relatórios de ameaças cibernéticas

Trellix Advanced Research Center

SUMÁRIO

SOBRE O TRELLIX ADVANCED RESEARCH CENTER

O Trellix Advanced Research Center está na vanguarda da pesquisa de ferramentas, tendências e métodos emergentes utilizados por perpetradores de ameaças cibernéticas em todo o cenário global de ameaças cibernéticas. Nossa equipe de pesquisadores de elite atua como principal parceira de CISOs, líderes de segurança seniores e suas equipes de operações de segurança no mundo todo. O Trellix Advanced Research Center oferece inteligência operacional e estratégica sobre ameaças por meio de conteúdo de ponta para analistas de segurança, alimenta nossa plataforma XDR com inteligência artificial líder do setor e oferece produtos e serviços de inteligência para clientes do mundo todo. Saiba mais em https://www.trellix.com/pt-br/advanced-research-center.html.

SOBRE A TRELLIX

A Trellix é uma empresa global que está redefinindo o futuro da segurança cibernética e do trabalho com paixão. 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, acelera a inovação tecnológica através de inteligência artificial, automação e análise para capacitar mais de 40.000 clientes corporativos e governamentais com uma segurança viva. Saiba mais em https://trellix.com/pt-br.

SUMÁRIO