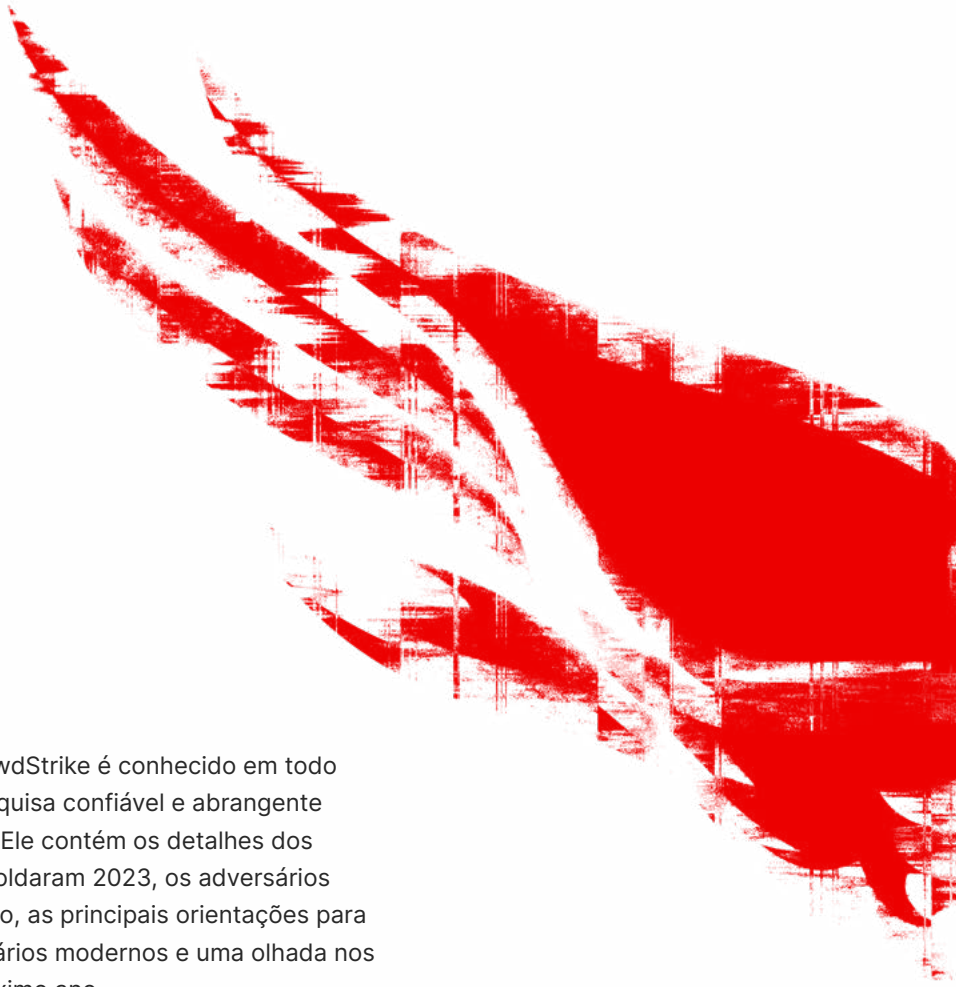
2024

RELATÓRIO GLOBAL DE AMEAÇAS

RESUMO EXECUTIVO

CROWDSTRIKE



O Relatório Global de Ameaças da CrowdStrike é conhecido em todo o setor de cibersegurança por sua pesquisa confiável e abrangente sobre o cenário moderno de ameaças. Ele contém os detalhes dos principais eventos e tendências que moldaram 2023, os adversários que impulsionaram as atividades do ano, as principais orientações para organizações que lutam contra adversários modernos e uma olhada nos eventos que estamos prevendo no próximo ano.

Para derrotar os adversários de hoje, você deve primeiro saber o que está enfrentando. A cibersegurança está mudando constantemente à medida que as inovações tecnológicas revolucionam os setores e os adversários mudam suas técnicas para se tornarem mais rápidos, sigilosos e eficazes. O Relatório Global de Ameaças 2024 da CrowdStrike faz uma retrospectiva de 2023 para que as organizações possam se preparar para o próximo ano. Aprender os detalhes de eventos passados pode ajudar a entender melhor o que os adversários buscam, quem são seus alvos e como trabalham.

Em 2023, o CrowdStrike Falcon® Intelligence e o CrowdStrike® Falcon OverWatch® se fundiram para se tornar o CrowdStrike Counter Adversary Operations (CAO), que combina o poder da inteligência de ameaças com a velocidade de equipes de investigação dedicadas e trilhões de eventos de telemetria da plataforma CrowdStrike Falcon® nativa da IA. O Relatório Global de Ameaças deste ano foi desenvolvido com base nas observações em primeira mão dessa equipe de elite.

Este resumo é uma visão geral das principais descobertas do relatório, que detalham informações importantes sobre o que as equipes de segurança precisam saber — e fazer — em um cenário de ameaças cada vez mais complexo.

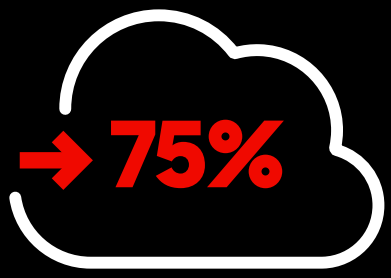
CONVENÇÕES DE NOMENCLATURA

Adversário	Estado-nação ou Categoria
BEAR	RÚSSIA
BUFFALO	VIETNÃ
CHOLLIMA	RPDC (COREIA DO NORTE)
CRANE	ROK (REPÚBLICA DA COREIA)
HAWK	SÍRIA
JACKAL	HACKTIVISTAS
KITTEN	IRÃ
LEOPARD	PAQUISTÃO
LYNX	GEÓRGIA
OCELOT	COLÔMBIA
PANDA	REPÚBLICA POPULAR DA CHINA
SPHINX	EGITO
SPIDER	ECRIME
TIGER	ÍNDIA
WOLF	TURQUIA

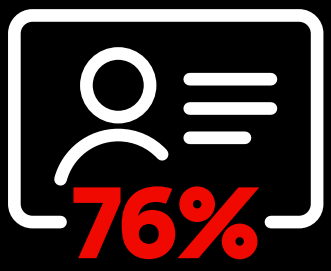
Visão geral do cenário de ameaças

34 novos adversários rastreados pela CrowdStrike, elevando o total para **232**

Casos com conhecimento de nuvem aumentaram **110% em relação ao ano anterior**



As intrusões no ambiente de nuvem aumentaram **75% em relação ao ano anterior**



Aumento anual de 76% nas vítimas citadas em website de vazamento de dados para e-crime

84% das intrusões com conhecimento de nuvem atribuídas pelo adversário priorizavam e-crime

VISÃO GERAL DO CENÁRIO DE AMEAÇAS

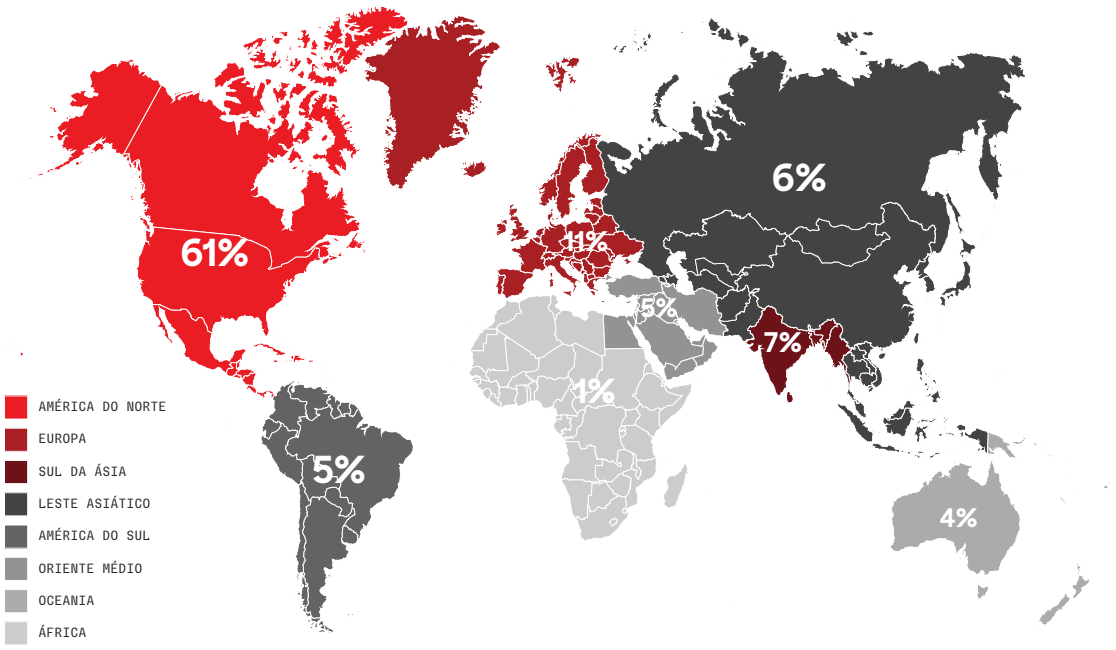
- **Os adversários estão ganhando velocidade:** o tempo médio de comprometimento do e-crime em 2023 foi de 62 minutos, e o tempo de comprometimento mais rápido registrado foi de 2 minutos e 7 segundos. Em um ataque típico observado pela CrowdStrike, mais de 88% do tempo de ataque foi dedicado a obter acesso inicial — e os adversários estão trabalhando para reduzir isso. Depois de conseguir acesso, foram necessários apenas 31 segundos para que um ator de ameaças lançasse uma ferramenta de descoberta inicial.

- **As intrusões interativas estão aumentando rapidamente:** as atividades com acesso interativo aumentaram 60% em 2023 em comparação com 2022. No segundo semestre de 2023, o aumento passou para 73% em comparação com o mesmo período do ano anterior. Três quartos dos ataques para obter acesso inicial estavam livres de malware, contra 71% em 2022, ressaltando a mudança dos adversários para técnicas mais rápidas e eficazes.

- **A nuvem é um campo de batalha em constante evolução:** à medida que as organizações transferem suas operações para a nuvem, os adversários continuam desenvolvendo sua expertise em nuvem. As intrusões na nuvem aumentaram 75% em 2023, e os casos com conhecimento de nuvem aumentaram em 110%.

- **Extorsão por roubo de dados ajuda na monetização:** a CrowdStrike observou um aumento de 76% no número de vítimas citadas em website de vazamento de dados dedicados a Big Game Hunting (BGH), demonstrando o status de BGH como a ameaça eletrônica mais significativa para organizações que abrangem regiões e setores.

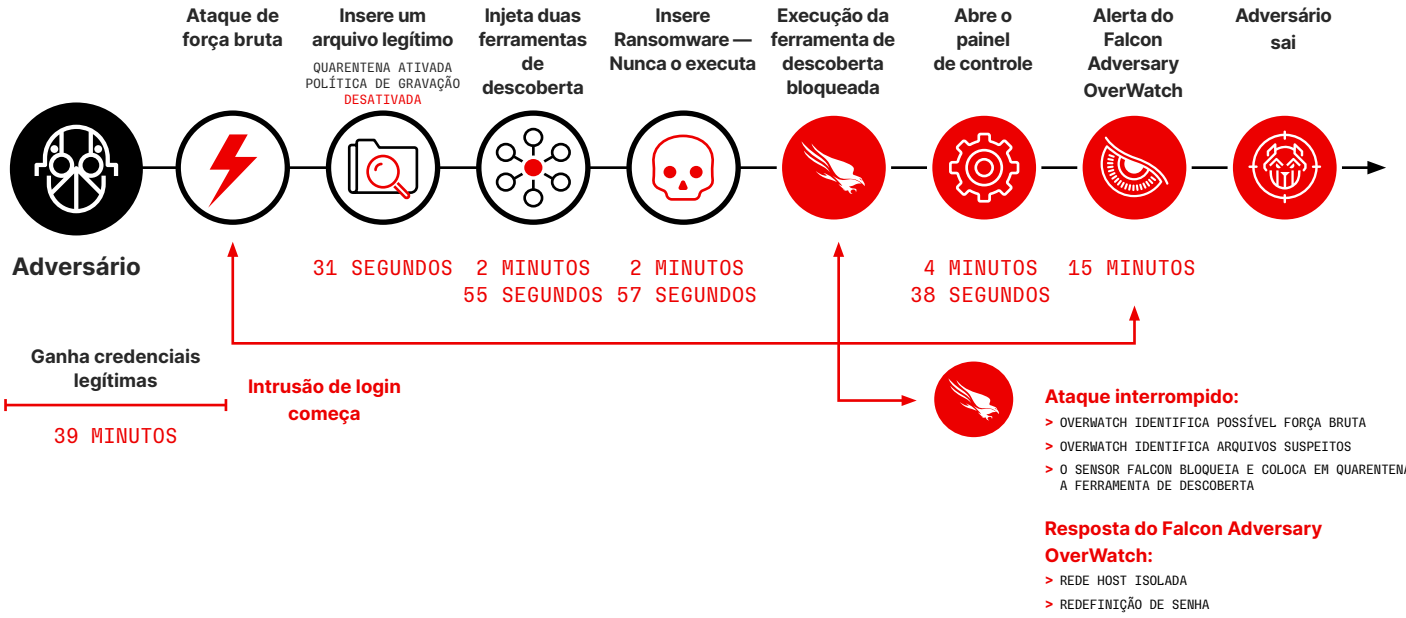
Intrusões interativas por região



Intrusões interativas por setor

ANATOMIA DE UM E-CRIME

INTRUSÃO INTERATIVA



Em um ataque (mostrado na figura acima), a equipe de segurança teve a configuração de política "quarentena na gravação" desativada, permitindo que quatro arquivos fossem gravados em disco. O adversário executou uma ferramenta legítima para obter informações do sistema para reconhecimento e, depois, inseriu mais três arquivos, incluindo um ransomware, no sistema. Eles tentaram executar uma ferramenta de descoberta e reconhecimento de rede para mapear as opções de movimento lateral, que foi imediatamente bloqueada e colocada em quarentena pelo sensor Falcon. Isso fez com que o adversário abrisse o painel de controle para entender qual ferramenta de segurança estava em uso. Quando identificaram a plataforma Falcon, nunca tentaram executar a segunda ferramenta de descoberta ou o ransomware (que teria sido evitado e colocado em quarentena) e passaram para outra vítima. Em minutos, o time de threat hunters CAO da CrowdStrike notificou o cliente, desligou a máquina e redefiniu a senha do usuário.

Quando ocorre um comprometimento inicial, são necessários apenas alguns segundos para que os adversários insiram ferramentas e/ou malware no ambiente da vítima durante uma intrusão interativa. No entanto, o ditado "tempo é dinheiro" vale para os adversários. Mais de 88% do tempo de ataque foi dedicado a invadir e obter acesso inicial. Ao reduzir ou eliminar esse tempo, os adversários liberam recursos para realizar mais ataques.

ATIVIDADE LIVRE DE MALWARE

»

75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

Principais temas

Ataques baseados em identidade e engenharia social

Adversários de várias regiões e com diferentes motivações continuam usando técnicas de phishing para fazer spoofing de usuários legítimos e atacar contas válidas, juntamente com outros dados de autenticação e identificação, para conduzir seus ataques.

- Além de roubar as credenciais da conta, o CrowdStrike CAO observou adversários atacando chaves e segredos de API, cookies e tokens de sessão, senhas únicas e tíquetes Kerberos ao longo de 2023.
- Esses ataques são comuns entre adversários transnacionais e atores do e-crime. Para estados nacionais, a FANCY BEAR realizou campanhas regulares de coleta de credenciais ao longo de 2023. Em campanhas de phishing com credenciais, ela desenvolveu um kit de ferramentas personalizado para capturar credenciais de usuários do Yahoo! Mail e ukr.net. A COZY BEAR realizou campanhas de phishing com credenciais usando mensagens do Microsoft Teams para solicitar tokens de autenticação multifatorial (MFA) para contas do Microsoft 365.
- Técnicas baseadas em identidade também são fundamentais para a estratégia da SCATTERED SPIDER: ao longo de 2023, esse adversário realizou ataques sofisticados de engenharia social para acessar as contas das vítimas.

Os adversários continuam desenvolvendo conhecimento da nuvem

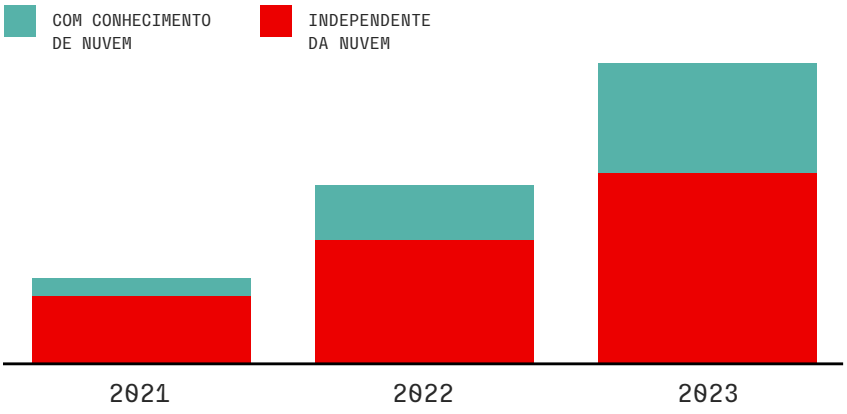
Conforme previsto, a nuvem continuou a ser um campo de batalha em evolução para as atividades dos adversários em 2023. O CrowdStrike CAO observou um aumento de 110% nos casos envolvendo a nuvem (em que os adversários sabiam da violação de um ambiente de nuvem e usaram esse acesso para abusar do serviço em nuvem) e um aumento de 60% nos casos independentes de nuvem. Os atores de ameaças envolvidos em casos independentes da nuvem não sabiam que haviam comprometido um ambiente em nuvem ou não aproveitaram as funcionalidades específicas da nuvem.

- O SCATTERED SPIDER gerou predominantemente os aumentos em atividades com conhecimento da nuvem ao longo de 2023, representando 29% do total de casos. O adversário demonstrou uma estratégia comercial progressiva e sofisticada em ambientes de nuvem direcionados para manter a persistência, obter credenciais, fazer movimentos laterais e exfiltrar dados.

- Os adversários de e-crime foram especialmente ativos no ataque a ambientes de nuvem: 84% das intrusões com conhecimento de nuvem atribuídas a adversários foram conduzidas por prováveis atores do e-crime.

- A preferência dos adversários por técnicas baseadas em identidade é evidente em seus ataques com foco na nuvem. Eles geralmente usam credenciais válidas para obter acesso inicial a ambientes em nuvem e ganhar persistência no nível da identidade para, depois, aumentar os privilégios ao conseguir acesso a identidades adicionais.

INCIDENTES NA NUVEM



▲ 110% CASOS COM CONHECIMENTO DA NUVEM — OS ATORES ESTÃO CIENTES DE QUE OBTIVERAM ACESSO EM UM AMBIENTE DE NUVEM DE PROPRIEDADE DA VÍTIMA E USAM ESSE ACESSO PARA ABUSAR DO SERVIÇO DA VÍTIMA

▲ 60% CASOS INDEPENDENTES DE NUVEM — OS ATORES TAMBÉM NÃO SABIAM QUE TINHAM COMPROMETIDO UM AMBIENTE DE NUVEM OU NÃO APROVEITARAM OS RECURSOS DA NUVEM

↑75%
INTRUSÕES NA NUVEM

Exploração de relacionamento com terceiros

Os atores de intrusão direcionada tentaram consistentemente explorar relacionamentos confiáveis para obter acesso inicial às organizações ao longo de 2023. Esse tipo de ataque aproveita as relações entre fabricante e cliente para implementar ferramentas mal-intencionadas usando duas técnicas principais: uma que envolve comprometer a cadeia de suprimentos de software usando software confiável para distribuir ferramentas mal-intencionadas, e outra que envolve aproveitar o acesso aos fabricantes que prestam serviços de TI.

- Os adversários que buscam relacionamentos com terceiros são motivados pelo possível retorno do investimento: uma organização comprometida pode levar a centenas ou milhares de alvos subsequentes.

- Em 2023, o maior alvo dos adversários da China-nexus eram relacionamentos com terceiros para implementar implantes mal-intencionados e ganhar acesso inicial. O JACKPOT PANDA e o CASCADE PANDA exploraram consistentemente relacionamentos confiáveis por meio de comprometimentos na cadeia de suprimento e ataques de atores paralelos ou intermediários.

- A Coreia do Norte também demonstrou um interesse crescente em explorar relacionamentos confiáveis em 2023: a LABYRINTH CHOLLIMA, em particular, abusou de uma relação confiável entre um fabricante de tecnologia e um cliente em três casos no ano passado.

Cenário de vulnerabilidades: exploração “Under the Radar”

Os adversários se adaptaram à visibilidade aprimorada dos sensores tradicionais de detecção e resposta de endpoint (EDR) alterando suas táticas de exploração para acesso inicial e movimento lateral. Agora, eles têm como alvo a periferia da rede, em que a visibilidade do defensor é reduzida pela possibilidade de os endpoints não terem sensores EDR ou não poderem sustentar a implantação de sensores.

- Os dispositivos de rede não gerenciados, principalmente os dispositivos de gateway de borda, continuaram sendo o vetor de acesso inicial mais observado para exploração rotineira em 2023.

- Os atores de ameaças estão desenvolvendo exploits para produtos em fim de vida útil que não podem ser corrigidos e geralmente não permitem a implantação de sensores modernos. Servidores de sistema operacional incompatíveis e dispositivos de gateway legados oferecem acesso fácil, até mesmo a famílias de malware mais antigas, o que causa infecções persistentes.

Conflito Israel-Hamas 2023: operações cibernéticas Foco na interrupção e na influência

O CrowdStrike CAO acompanhou as operações cibernéticas contínuas de intrusão direcionada e atores hacktivistas desde o início do conflito Israel-Hamas de 2023. As atividades e as alegações dos dois tipos de atores de ameaças se concentram principalmente em atacar a tecnologia operacional ou outros sistemas importantes — que possam influenciar psicologicamente as populações-alvo — e implementar limpadores destrutivos contra entidades israelenses ou vinculadas a Israel.

- O CrowdStrike CAO rastreia vários adversários associados ao grupo militante do Hamas; no entanto, a atividade atribuída a esses adversários não pareceu apresentar conexão com o conflito Israel-Hamas até o momento. Provavelmente, isso se deve à indisponibilidade de recursos ou à degradação da infraestrutura de distribuição de eletricidade e internet na zona de conflito.
- O RENEGADE JACKAL foi o adversário mais ativo do Hamas-nexus ao longo de 2023. Os prováveis adversários EXTREME JACKAL e RENEGADE JACKAL, avaliados pelo CrowdStrike CAO, em Gaza, demonstram apoio aos interesses estratégicos do Hamas.
- É quase certo que a atividade hacktivista continuará em ritmo acelerado com as flutuações nos desenvolvimentos geopolíticos relacionados. Essa avaliação é feita com alta confiança com base nos padrões de atividade exibidos até o momento.

PERSPECTIVA PARA 2024

À medida que as organizações planejam possíveis ameaças em 2024, dois fatores potenciais de disrupção emergem como principais: IA generativa e eleições governamentais globais em 2024.

Uso de IA generativa no cenário de ameaças

A IA generativa democratizou massivamente a computação para melhorar as operações dos adversários. Ela também pode reduzir a barreira de entrada ao cenário de ameaças para atores de ameaças menos sofisticados.

As duas principais áreas de oportunidades de IA generativa dentro do cenário de ameaças são:

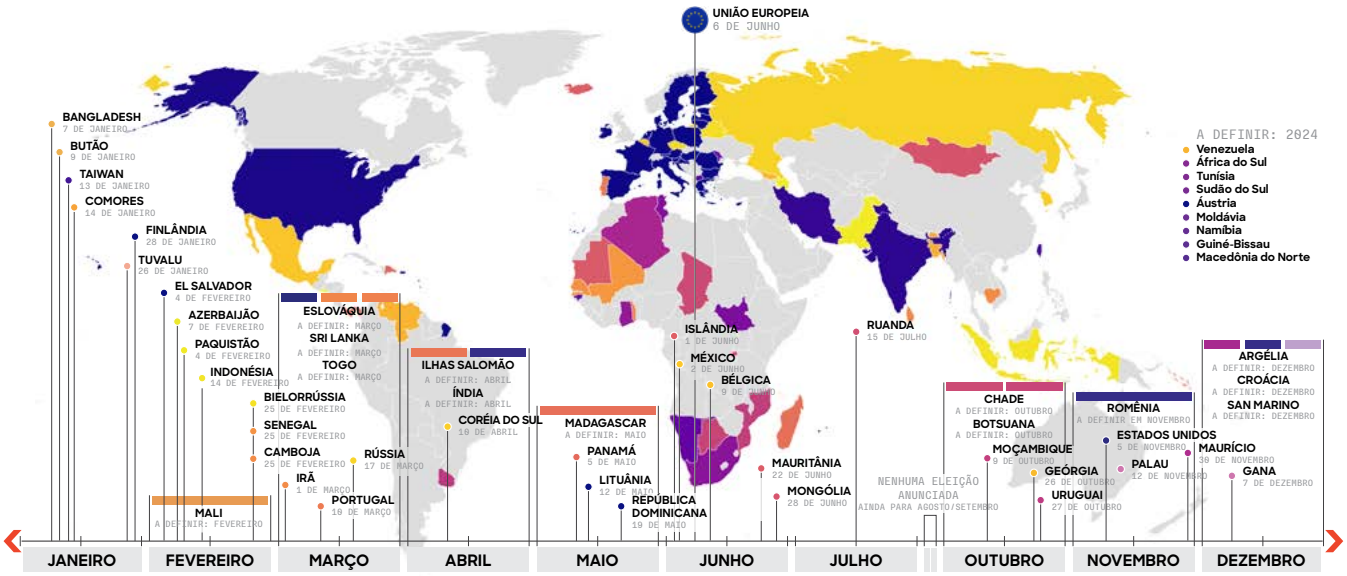
- Desenvolver e/ou executar operações de rede de computadores (CNO) mal-intencionadas, incluindo desenvolvimento de ferramentas e recursos, como scripts ou códigos, que podem ser funcionalmente mal-intencionados se usados corretamente
- Apoiar a eficiência e a eficácia das campanhas de engenharia social e operações de informação (IO)

O CrowdStrike CAO avalia que a IA generativa provavelmente será usada para ciberatividades em 2024, à medida que continua ganhando popularidade. A equipe acompanhará como os agentes de ameaças usam essa tecnologia e como esse uso difere dos aplicativos convencionais ao longo de 2024.

Eleições de 2024

Indivíduos de 55 países representando mais de 42% da população global participarão das eleições presidenciais, parlamentares e/ou gerais. Isso inclui sete dos 10 países mais populosos do mundo. As eleições em âmbito nacional também ocorrerão em países ou grupos envolvidos ou próximos a grandes conflitos geopolíticos.

Historicamente, as atividades mal-intencionadas mais comuns direcionadas às eleições envolveram IOs, provavelmente conduzidas por entidades vinculadas a estados contra cidadãos de países que têm interesse geopolítico específico no ator da ameaça, e um hacktivismo simples e de curta duração (incluindo ataques de negação de serviço distribuído (DDoS) e desfigurações de websites) contra entidades governamentais estaduais e locais. É altamente provável que essa tendência continue em 2024. Os países de interesse envolvidos nos ciclos eleitorais provavelmente correrão o risco de campanhas de IO significativas e longas das principais potências globais.



CENÁRIO DO E-CRIME

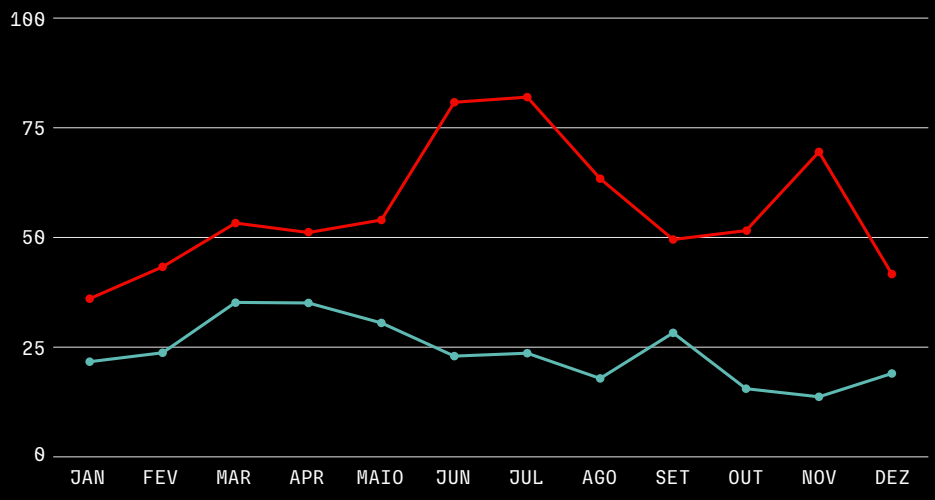
O Índice do e-Crime® da CrowdStrike(ECX) rastreia a atividade — incluindo o número de e-mails de spam observados e o custo médio de compra de acesso a uma rede corporativa — em vários segmentos do ecossistema de e-crime e calcula o número total de vítimas de ransomware observadas.

Até maio de 2023, o ECX exibiu tendências semelhantes às observadas em 2022. No entanto, a partir de junho de 2023, o ECX cresceu significativamente, com grandes picos entre junho e agosto. Os colaboradores mais impactantes para esses picos incluíram a alta frequência de incidentes de BGH e um aumento repentino nos ataques de DDoS observados.

O ECX subiu novamente em novembro de 2023, refletindo o aumento no número de e-mails de spam e o aumento do preço médio de loaders e stealers.

2023
2022

Valor do índice do e-Crime = **+67%**



O ECX de 2023 acompanhou a maior atividade anual até o momento, representando o crescimento ano a ano do índice. Os e-mails de spam provavelmente diminuíram em 2023, quando os adversários procuraram outros meios de acesso inicial e depois que uma operação multinacional encerrou o QakBot do MALLARD SPIDER.

Embora a demanda média de resgate tenha sido menor em 2023 do que em 2022, isso provavelmente representa uma exceção no conjunto de dados, não uma visão precisa do cenário de ameaças. Os pedidos de resgate se mantiveram consistentemente altos durante esse período, mas a capacidade de rastrear esses valores está se tornando um desafio, pois os atores de ameaças e as vítimas implementam medidas de privacidade mais rígidas em relação às demandas e aos pagamentos dos preços de resgate.

Novas vulnerabilidades com pontuação CVSS3 de 9/10
+6%

Incidentes de BGH envolvendo vazamentos de dados
+76%

Custo médio do Loader
+169%

Custo médio do Crypter
+250%

Custo médio do Stealer
+286%

Demanda média de resgate
-27%

Identificação de e-mails de spam
-15%

Big Game Hunting

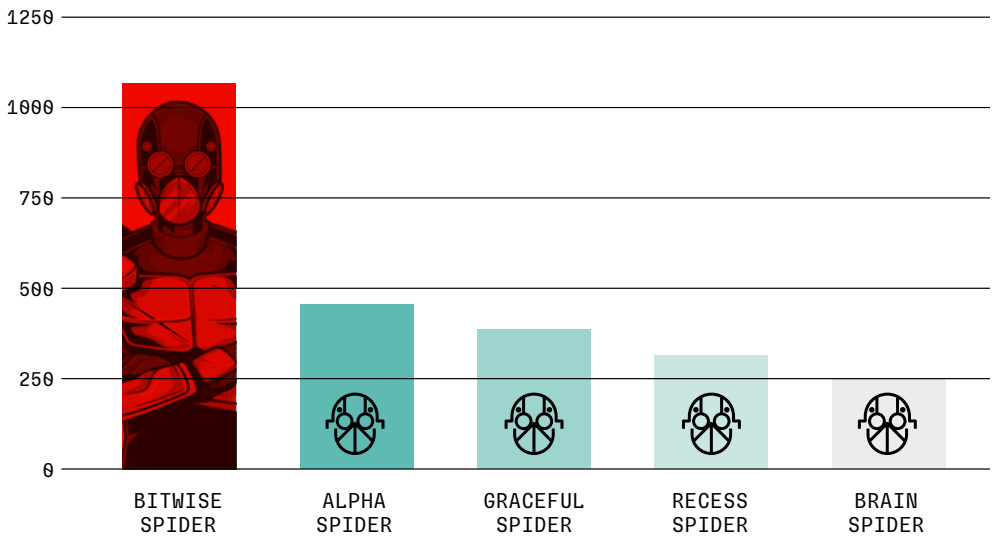
O número de vítimas citadas em websites de vazamento de dados dedicados a BGH aumentou significativamente no ano passado, com 4.615 postagens de vítimas feitas em DLSs em 2023 — um aumento de 76% em relação a 2022. Vários fatores contribuíram para esse crescimento, incluindo os recém-surgidos adversários do BGH, o crescimento das operações de adversários existentes e campanhas selecionadas de alto volume, como várias explorações de dia zero do GRACEFUL SPIDER.

Em conjunto, BITWISE SPIDER, ALPHA SPIDER, GRACEFUL SPIDER, RECESS SPIDER e BRAIN SPIDER respondem por 77% das postagens em todos os DLSs de adversários rastreados. BITWISE SPIDER e ALPHA SPIDER publicaram historicamente várias novas postagens de DLS e se classificaram em primeiro e segundo lugar, respectivamente, com o maior número de postagens DLS em 2022 e 2023.

RECESS SPIDER e BRAIN SPIDER iniciaram suas próprias operações de ransomware em meados de 2022 e janeiro de 2023, respectivamente. Desde então, eles cresceram em destaque para representar o quarto (RECESS SPIDER) e o quinto maiores números (BRAIN SPIDER) de postagens de DLS em 2023.

O GRACEFUL SPIDER, que opera desde 2016 e normalmente realiza campanhas de baixo volume, explorou três vulnerabilidades de dia zero em 2023 para extrair dados de centenas de vítimas em todo o mundo. Esse adversário acabou publicando o terceiro maior número de postagens de DLS naquele ano.

Principais adversários por DLS Post



O NÚMERO DE VÍTIMAS CITADAS EM WEBSITES DE VAZAMENTO DE DADOS DEDICADOS A BGH AUMENTOU SIGNIFICATIVAMENTE EM 2023, COM 4.615 POSTAGENS DE VÍTIMAS FEITAS EM DLSs – UM AUMENTO DE 76% EM RELAÇÃO A 2022.

RECOMENDAÇÕES

A CrowdStrike oferece as seguintes recomendações para ajudar as organizações a proteger seus ativos e se defender contra um ecossistema adversário em constante evolução:

Torne a proteção de identidade indispensável

Ataques baseados em identidade e de engenharia social moldaram o cenário de ameaças em 2023. Para combater essas ameaças, é essencial implementar a autenticação multifatorial (MFA) e estendê-la a sistemas e protocolos legados, informar equipes sobre engenharia social e implementar tecnologias que possam detectar e correlacionar ameaças em ambientes de identidade, endpoint e nuvem. A visibilidade e a fiscalização entre domínios permitem que as equipes de segurança detectem movimentos laterais, tenham visibilidade total do caminho do ataque e investiguem o uso malicioso de ferramentas legítimas. Lidar com métodos de acesso sofisticados, como troca de SIM, desvio de MFA e roubo de chaves de API, cookies de sessão e tickets Kerberos, exige uma busca contínua por comportamentos maliciosos.

Priorize Plataformas de proteção de aplicações nativas em nuvem (CNAPPs)

As empresas precisam de visibilidade total da nuvem para eliminar configurações incorretas, vulnerabilidades e outras ameaças. As ferramentas de segurança na nuvem não devem existir isoladamente. O CNAPPs é uma plataforma unificada que simplifica o monitoramento, a detecção e a atuação em possíveis ameaças e vulnerabilidades da nuvem. Selecione um CNAPP que inclua proteção pré-tempo de execução, proteção do tempo de execução e tecnologia sem agente para descobrir e mapear aplicações e APIs em execução na produção, mostrando todas as superfícies de ataque, ameaças e riscos comerciais importantes.

Ganhe visibilidade das áreas mais críticas do risco corporativo

À medida que os ambientes corporativos se expandem, as organizações precisam entender as relações entre identidade, nuvem, endpoints e telemetria de proteção de dados para identificar e bloquear ataques modernos. Ao consolidar produtos pontuais em uma plataforma de segurança unificada, as organizações podem obter total visibilidade em uma única exibição e controlar facilmente suas operações, melhorando a capacidade de descobrir, identificar e interromper ataques.

Gere eficiência

Os adversários estão ficando mais rápidos. Você consegue acompanhar? As soluções legadas de gerenciamento e correlação de eventos de segurança (SIEM) costumam ser muito lentas, complexas e caras, e muitas foram projetadas para uma época em que os volumes de dados e a sofisticação dos adversários eram uma fração do que são hoje. As empresas modernas precisam de uma solução SIEM moderna que seja mais rápida, fácil de implementar e mais econômica do que as ferramentas legadas de SIEM. Analise abordagens que unifiquem a detecção, a investigação e a resposta a ameaças em uma única plataforma nativa de IA fornecida por serviços em nuvem.

Crie uma cultura de cibersegurança

O usuário final continua sendo um elo crucial na cadeia para interromper ataques. Os programas de conscientização do usuário devem ser iniciados para combater a ameaça contínua de phishing e técnicas relacionadas de engenharia social. Para equipes de segurança, a prática leva à perfeição. Promova a cultura de executar rotineiramente exercícios tabletop e de Red team/Blue team para identificar lacunas e eliminar pontos fracos em suas práticas e respostas de cibersegurança.

FAÇA O DOWNLOAD DO RELATÓRIO COMPLETO

O Relatório Global de Ameaças 2024 da CrowdStrike apresenta análises detalhadas que destaca os eventos e tendências mais significativos em atividade de ciberameaças em 2023. Baixe uma cópia gratuita do relatório em https://www.crowdstrike.com/global-threat-report/.

Sobre a CrowdStrike

CrowdStrike (Nasdaq: CRWD) é a líder global em cibersegurança que redefiniu a segurança moderna com a plataforma nativa em nuvem mais avançada do mundo para proteger áreas de risco corporativo crítico — endpoints e workloads, identidade e dados na nuvem.

Impulsionada pela CrowdStrike Security Cloud e por IA de alto nível, a plataforma CrowdStrike Falcon® utiliza indicadores de ataque em tempo real, inteligência de ameaças, estratégias adversárias em evolução e telemetria enriquecida de toda a empresa para fornecer detecções hiperprecisas, proteção e correção automatizadas, investigação de ameaças de elite e observabilidade priorizada de vulnerabilidades.

Construída especificamente em nuvem com arquitetura de um único agente leve, a Plataforma Falcon fornece uma implementação rápida e escalável, proteção e desempenho superiores, complexidade reduzida e retorno imediato.

CrowdStrike: Nós interrompemos as ameaças.

Saiba mais em: www.crowdstrike.com

Siga nossas redes: Blog | X | LinkedIn | Facebook | Instagram

Comece um teste gratuito hoje mesmo: www.crowdstrike.com/free-trial-guide