CROWDSTRIKE

Apresentado por:

CALLISTER
SOLUÇÕES EM TI

RESUMO EXECUTIVO

RELATÓRIO DE INVESTIGAÇÃO DE AMEAÇAS DE 2026

Introdução

Em 2025, os adversários priorizaram a evasão. Em vez de forçar a entrada pela porta da frente, eles minaram sistematicamente a confiança das organizações ao visar parceiros da cadeia de suprimento, ecossistemas de desenvolvedores upstream, softwares legítimos e funcionários para obter acesso inicial e avançar sem serem detectados.

O Relatório de Investigação de Ameaças 2026 da CrowdStrike ilustra a próxima evolução do abuso de confiança. Os adversários entendem as lacunas entre controles de segurança fragmentados e exploram cada vez mais áreas nas quais os defensores muitas vezes não têm visibilidade completa: credenciais válidas, fluxos de autenticação na nuvem, aplicações SaaS, dispositivos de borda e sistemas não gerenciados. Eles estão explorando a confiança em todo o ecossistema de desenvolvedores, avançando para pipelines de CI/CD, registros de containers, registros de pacotes e extensões de ambientes de desenvolvimento integrado.

Os adversários modernos também estão usando IA para acelerar phishing, reconhecimento e operações técnicas, além de visar os sistemas de IA que agora estão integrados em toda a empresa. A IA de ponta está reduzindo a janela entre a descoberta e a exploração de vulnerabilidades. Ela ajuda os adversários a identificar vulnerabilidades, gerar exploits de PoC e mapear caminhos de ataque com mais velocidade e em maior escala.

As organizações que entendem essas ameaças em evolução estão mais preparadas para detê-las. O Relatório de Investigação de Ameaças 2026 da CrowdStrike fornece as informações de que elas precisam. Em suas páginas, a equipe do CrowdStrike Counter Adversary Operations, composta pela CrowdStrike Intelligence e pelo CrowdStrike OverWatch, detalha as principais observações e tendências que definem o cenário de ameaças.

Principais Conclusões



Os alertas de detecção acionados por agentes de IA ocorreram a uma taxa **2,5 vezes** maior que a dos alertas acionados por humanos.



De janeiro a junho de 2026, **88%** das explorações observadas pela CrowdStrike de vulnerabilidades com uma PoC pública **ocorreram até 48 horas** após a divulgação da PoC. Os adversários ligados à China agem ainda mais rápido; em um caso, em apenas **24 horas**.



Uma campanha de LLMJacking **gerou quase 200.000 solicitações de API** em dois minutos, causando impactos financeiros e operacionais em larga escala.



O ALTERED SPIDER comprometeu mais de **300 dependências de software** em um único dia durante suas campanhas de maio de 2026.



As intrusões por vishing no primeiro semestre de 2026 **aumentaram 2 vezes** em comparação com o segundo semestre de 2025.



Os atores do e-crime CORDIAL SPIDER e SNARKY SPIDER **usaram vishing para exfiltrar dados de aplicações SaaS** e comprometer contas de logon único (SSO). Em um dos casos, o SNARKY SPIDER passou do comprometimento da conta ao roubo de dados em menos de cinco minutos.



As tentativas mensais de phishing de código de dispositivo **aumentaram 15 vezes** no primeiro semestre de 2026.



As atividades de e-crime voltadas para a nuvem **aumentaram 171%**, à medida que os adversários realizaram roubo de credenciais, mineração de criptomoedas, abuso de LLMs e roubo de ativos financeiros digitais.

CONVENÇÕES DE NOMENCLATURA DE ADVERSÁRIOS



BEAR
RÚSSIA



BISON
BIELORRÚSSIA



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



SAIGA
CAZAQUISTÃO



SPHINX
EGITO



SPIDER
E-CRIME



TIGER
ÍNDIA



WOLF
TURQUIA

O relatório deste ano amplia o escopo das análises para além das intrusões puramente interativas, passando a incluir ataques automatizados, uma mudança que oferece uma visão mais precisa e abrangente da evolução do comportamento dos adversários e do cenário moderno de ameaças.

Os dados da CrowdStrike revelam um aumento de aproximadamente 4% na atividade geral de intrusões, um forte contraste com o aumento de 27% em relação ao ano anterior observado no relatório do ano passado. Essa estabilização é esperada e não indica uma redução da intenção dos adversários nem dos riscos operacionais. Os adversários estão investindo mais tempo e recursos no desenvolvimento de campanhas complexas, com pontos de acesso inicial cada vez mais inovadores, em vez das campanhas oportunistas de força bruta e alto volume dos anos anteriores.

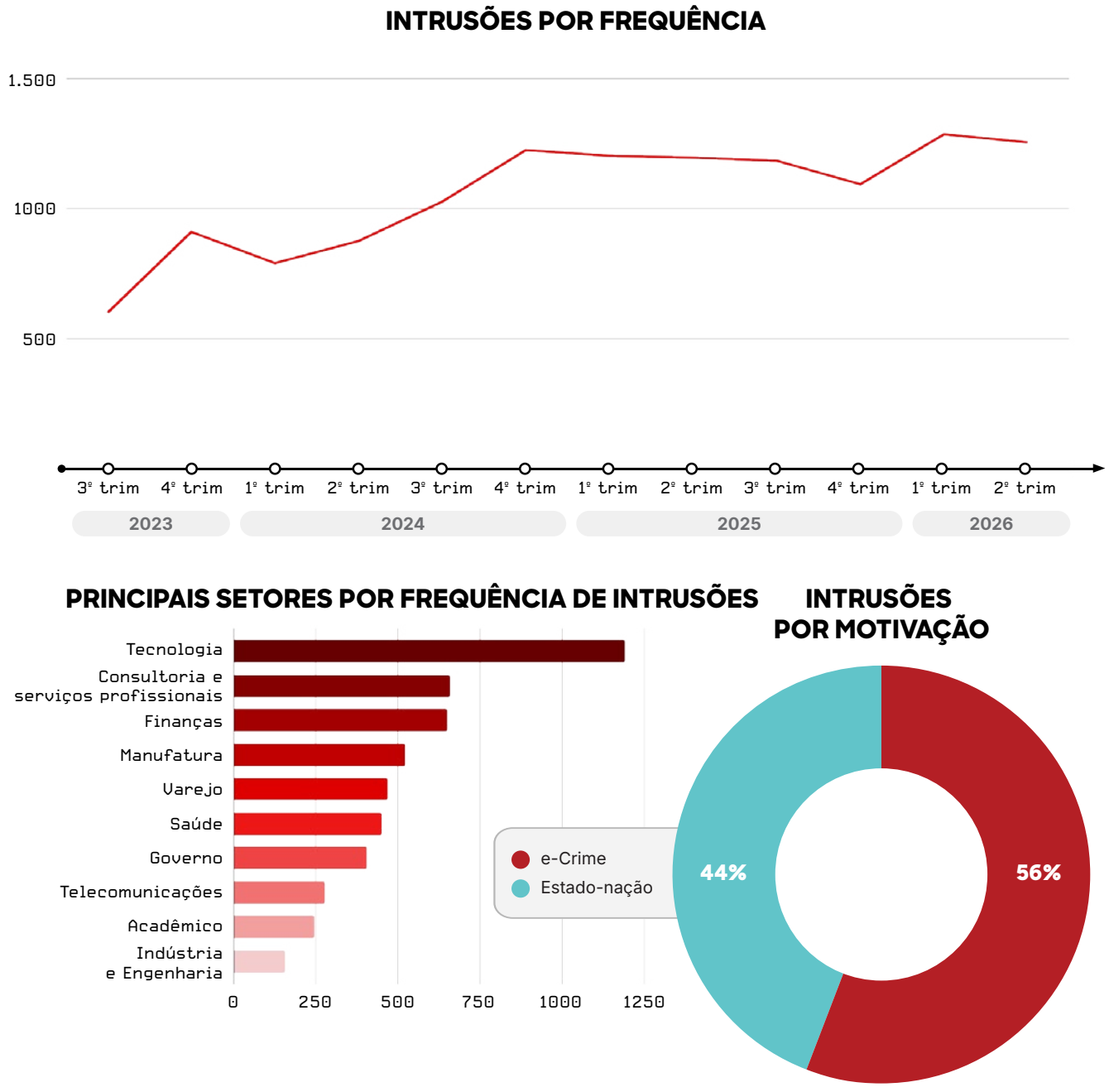


Figura 1. Detalhamento das intrusões, de 1º de julho de 2025 a 30 de junho de 2026

O setor mais atacado

O setor de tecnologia continua sendo o mais visado pelo nono ano consecutivo, com um aumento de 5% na atividade de intrusões em relação ao ano anterior. Essa distinção reflete o alto valor dos dados e da infraestrutura crítica que esse setor representa.

Os cinco setores mais visados mudam significativamente quando analisados por tipo de adversário. Os atores de ameaças de Estados-nação priorizam os setores de tecnologia e serviços financeiros, além de entidades governamentais. Os adversários de e-crime se concentram nos setores de tecnologia, consultoria e serviços profissionais, além de entidades de manufatura.

As classificações dos setores permaneceram praticamente estáveis em relação ao ano anterior. As duas exceções mais notáveis foram os setores de serviços financeiros e acadêmico, que registraram os maiores aumentos entre todos os setores, de 11% e 17%, respectivamente. Isso indica que os adversários estão visando cada vez mais instituições nas quais convergem ativos financeiros e dados confidenciais de pesquisa.

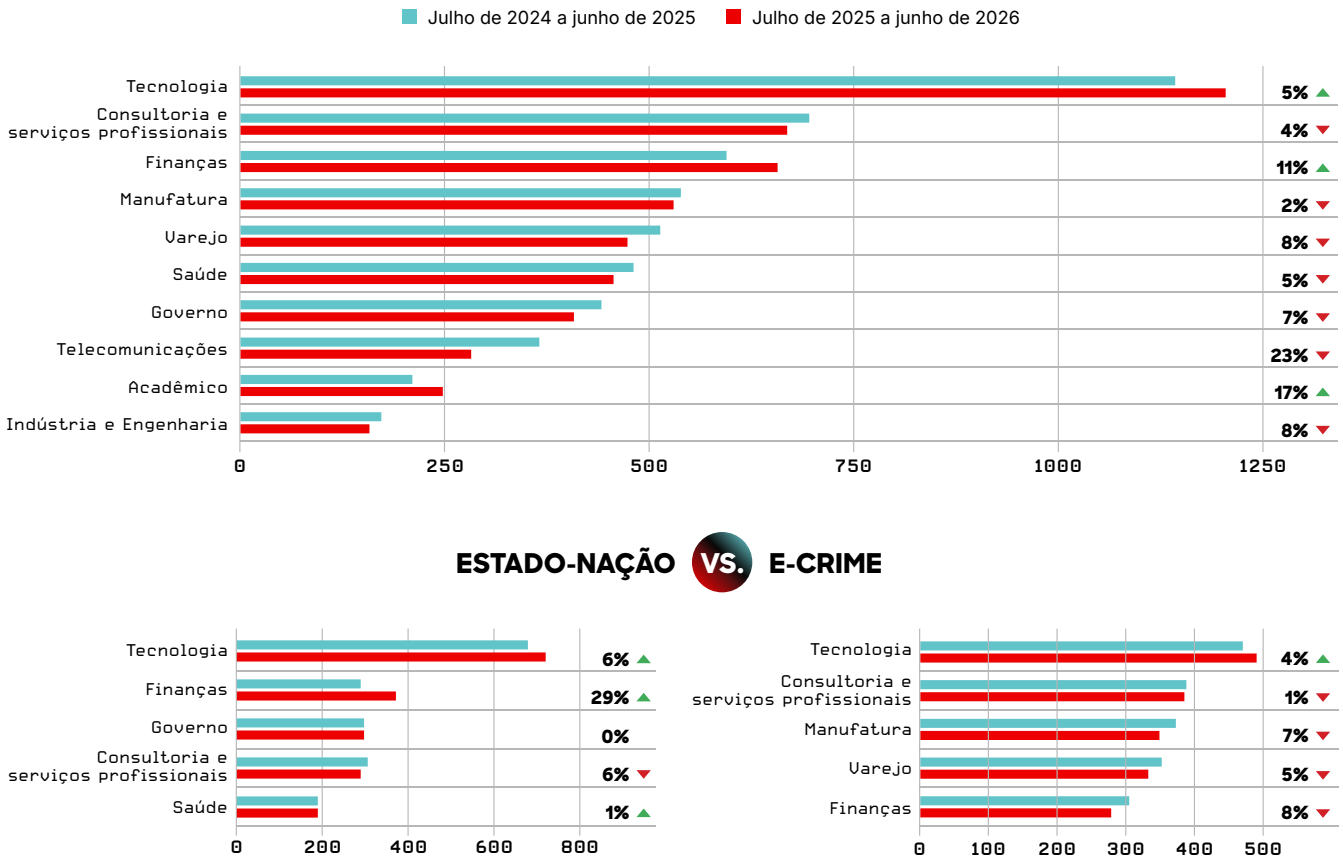


Figura 2. Setores visados por frequência de intrusões, julho de 2024 a junho de 2025 vs. julho de 2025 a junho de 2026

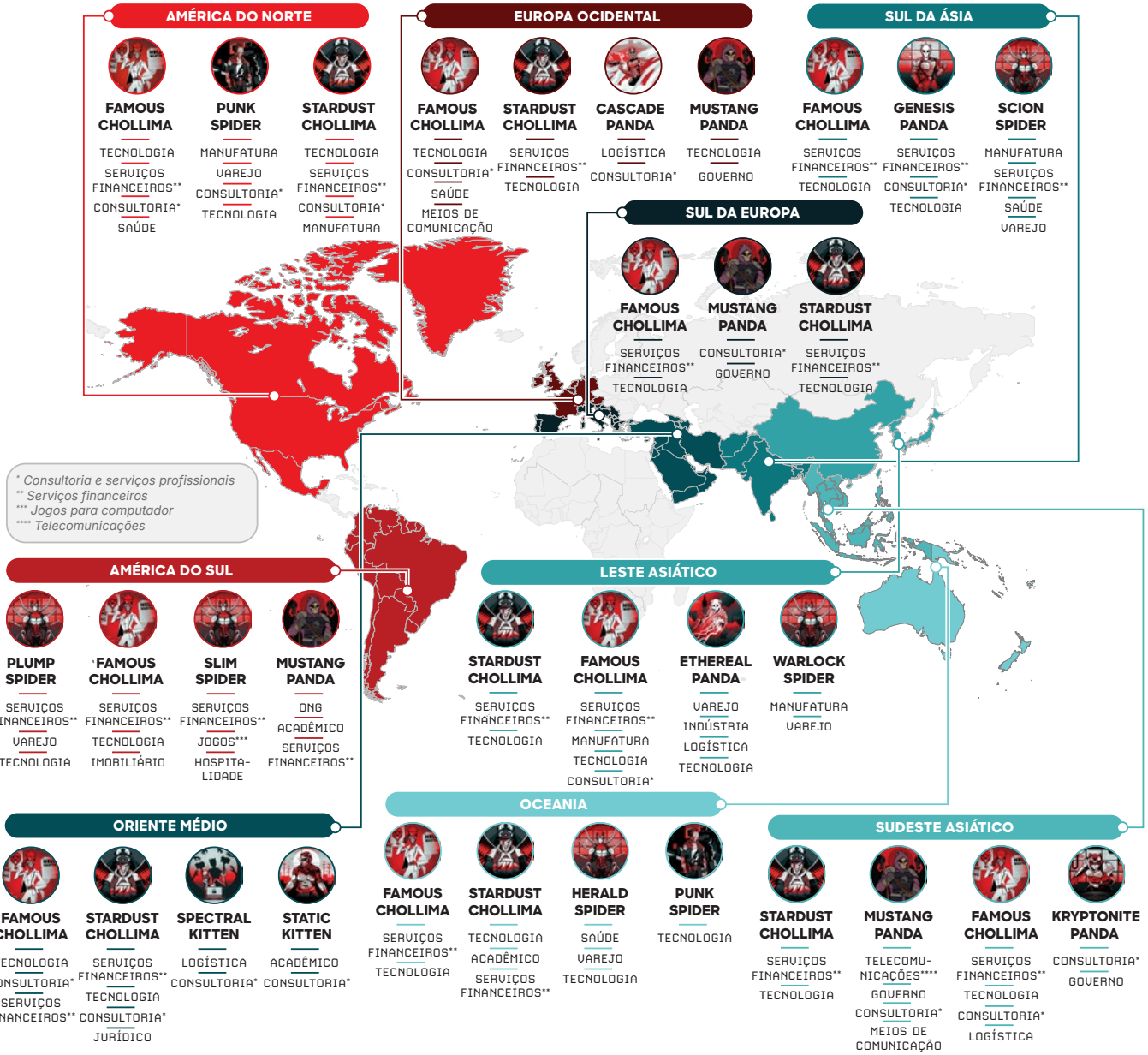


Figura 3. Interrupções de adversários em todo o mundo, 1º de julho de 2025 a 30 de junho de 2026

Observações das linhas de frente

Transformação mais rápida de vulnerabilidades em armas e descoberta de vulnerabilidades assistida por IA

A CrowdStrike Intelligence registrou um aumento de 42% na exploração de vulnerabilidades de dia zero entre 2024 e 2025, refletindo a capacidade cada vez maior dos adversários de descobrir e transformar vulnerabilidades em armas antes que os defensores pudessem corrigi-las.

Agora, a janela entre a divulgação e a exploração de uma vulnerabilidade está diminuindo: de janeiro a junho de 2026, 88% das explorações observadas pela CrowdStrike de vulnerabilidades com uma prova de conceito (PoC, na sigla em inglês) pública ocorreram até 48 horas após a divulgação da PoC. É praticamente certo que os prazos de exploração continuarão diminuindo no curto, médio e longo prazo.

Considere o estudo de caso abaixo, em que a vulnerabilidade React2Shell foi transformada em arma poucas horas após sua exposição:

> O React2Shell (CVE-2025-55182) é uma vulnerabilidade crítica de desserialização insegura que permite a execução remota de código (RCE) não autenticada em React Server Components e aplicações Next.js. A rápida exploração dessa falha ilustra claramente a redução da janela entre a divulgação e a exploração de uma vulnerabilidade.

A vulnerabilidade foi divulgada de forma privada aos administradores do React e do Next.js e divulgada publicamente, juntamente com as correções, em 3 de dezembro de 2025. Em até 24 horas, vários exploits de PoC funcionais já circulavam abertamente, e diversos atores de ameaças de e-crime, de Estados-nação e desconhecidos já usavam o React2Shell in the wild. Nos primeiros quatro dias após a divulgação pública, o CrowdStrike OverWatch respondeu a mais de 800 alertas de investigação relacionados a possíveis explorações do React2Shell em mais de 80 vítimas diferentes.

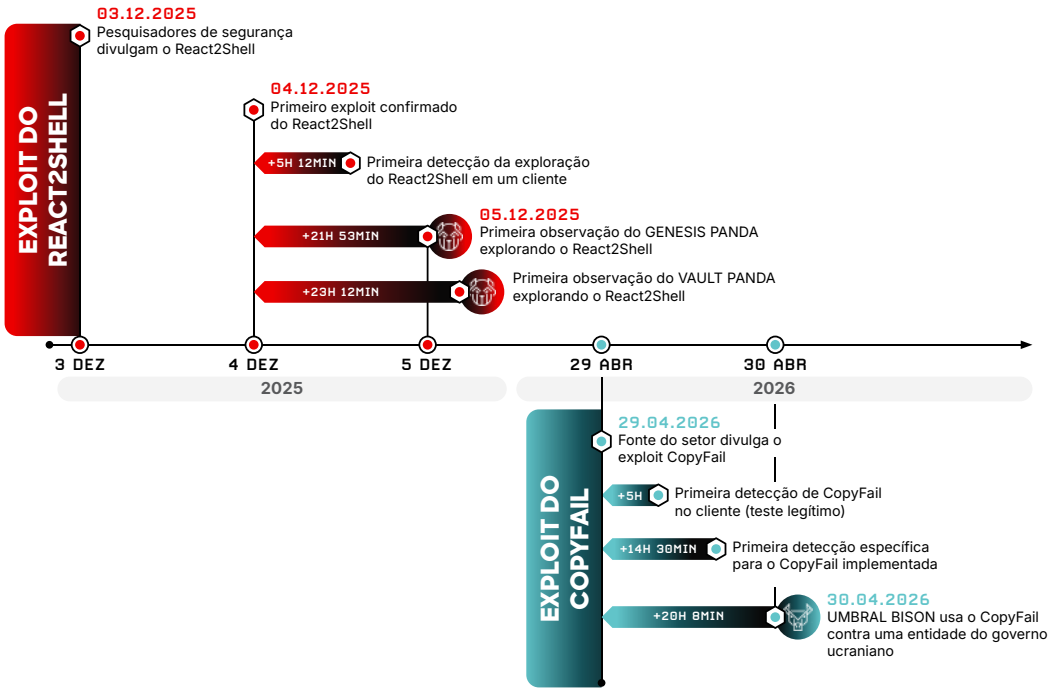


Figura 4. Linhas do tempo da elevação de privilégios local do UMBRAL BISON e da RCE do GENESIS PANDA, incluindo a cobertura do CrowdStrike OverWatch e as detecções do sensor

Ataques à cadeia de suprimento de software: defesa em um cenário de ameaças entre domínios

No Relatório Global de Ameaças 2026 da CrowdStrike, a CrowdStrike identificou uma mudança nas técnicas de acesso inicial em direção a métodos desenvolvidos para evitar os controles de segurança tradicionais. No primeiro semestre de 2026, essa tendência se consolidou, com ataques à cadeia de suprimento de software usando cada vez mais pacotes de software malicioso carregados em registros públicos de software.

Como esses registros de software são usados por desenvolvedores e organizações de todos os setores e regiões geográficas, a escala da exposição é significativa. Um único pacote de software malicioso pode alcançar milhões de usuários por semana. Embora os adversários tenham visado diversos registros públicos de software, os pacotes npm maliciosos dominaram as atividades, representando 87% de todos os pacotes maliciosos identificados durante o período de seis meses.

O ecossistema npm é um alvo atraente devido à prática estabelecida de projetos terem árvores de dependências profundas, compostas por muitos pacotes pequenos, à capacidade dos pacotes de executar scripts automaticamente após a instalação e à popularidade geral do JavaScript para o desenvolvimento de software full-stack. Milhões de usuários dependem de pacotes distribuídos pelo registro npm.

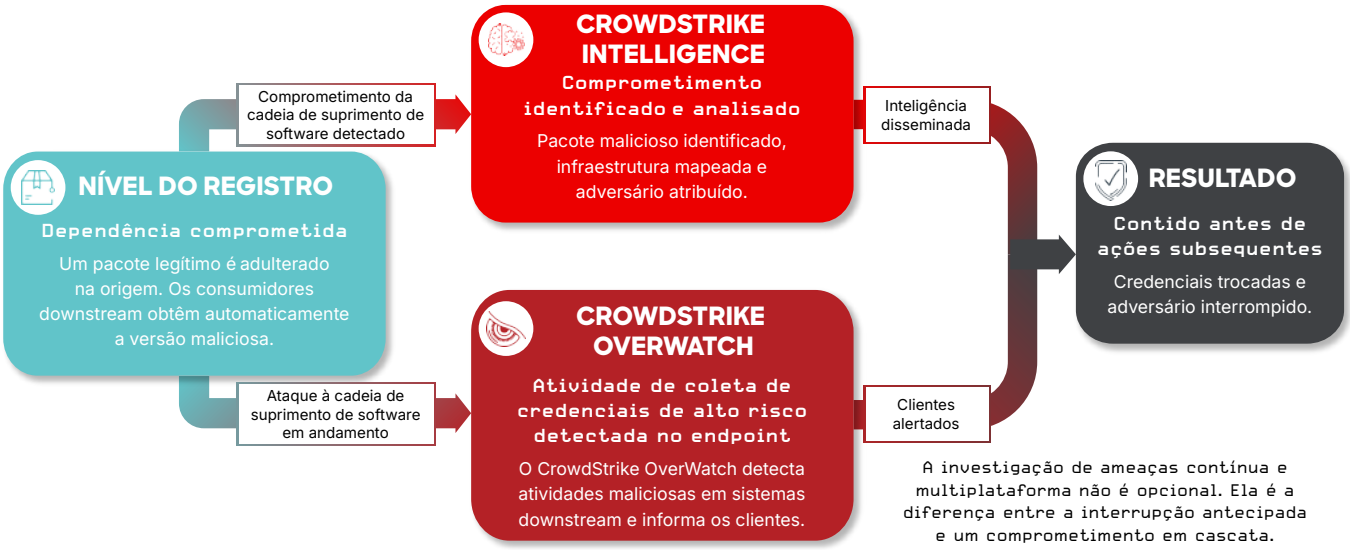


Figura 5. Resposta do CrowdStrike Counter Adversary Operations ao comprometimento da cadeia de suprimento de software

No último ano, dois adversários foram responsáveis pelos ataques mais significativos à cadeia de suprimento de software: STARDUST CHOLLIMA, um adversário ligado à RPDC com foco contínuo em serviços financeiros e criptomoedas, e ALTERED SPIDER, um adversário de e-crime motivado financeiramente que conduz uma ampla operação de ataques à cadeia de suprimento de software em rápida evolução. Juntas, suas campanhas representam alguns dos comprometimentos mais impactantes da cadeia de suprimento de software em 2026 e ilustram todo o espectro de sofisticação dos adversários que visam essa superfície de ataque.

Vishing dispara como vetor de acesso inicial baseado em identidade

O uso de vishing como vetor de acesso inicial continua aumentando. Entre 2024 e 2025, o CrowdStrike OverWatch detectou um aumento de 134% nas intrusões por vishing. Somente no primeiro semestre de 2026, o número de intrusões em que o vishing foi o provável vetor de acesso inicial já foi duas vezes maior do que no segundo semestre de 2025.

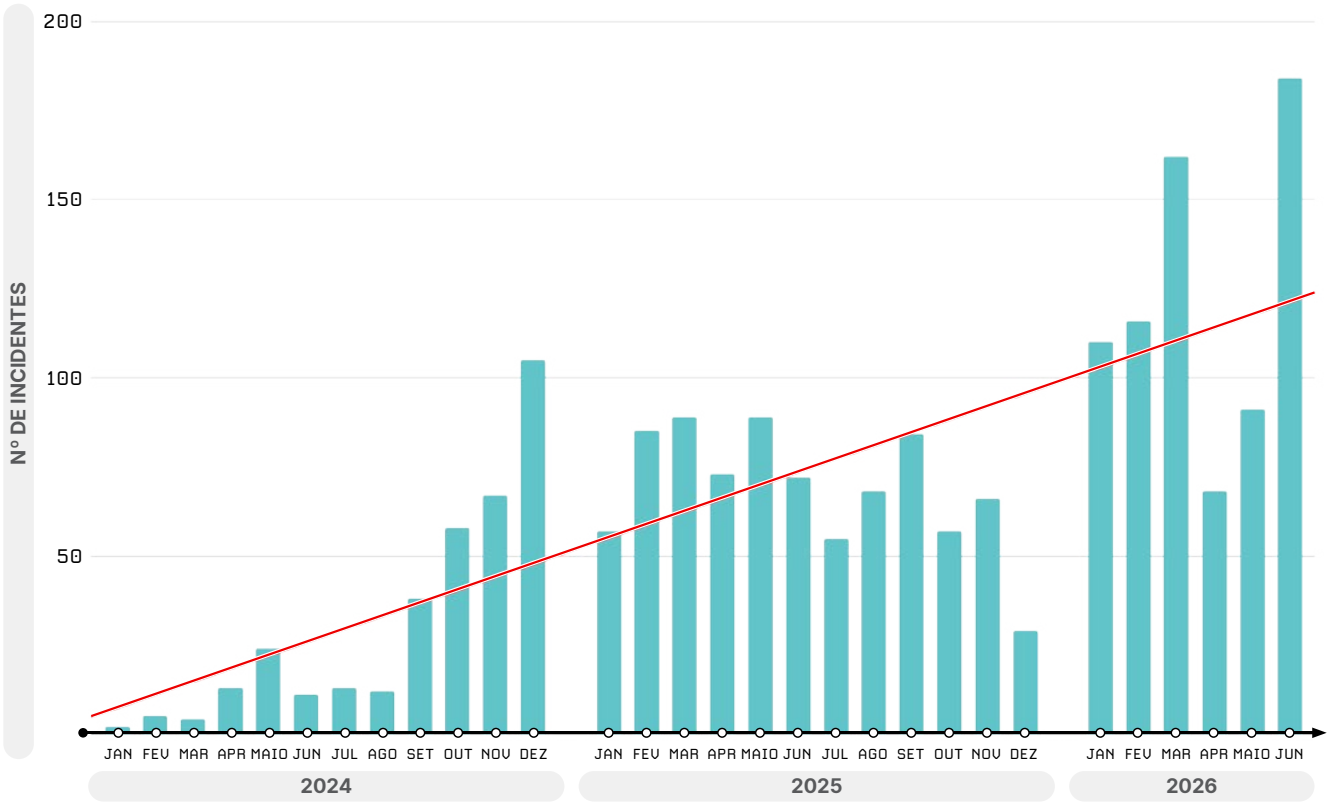


Figura 6. Intrusões detectadas pelo CrowdStrike OverWatch nas quais o vishing foi o provável vetor de acesso inicial por mês, de janeiro de 2024 a junho de 2026

O vishing se tornou uma técnica importante de e-crime por vários motivos:

- **Contorna os controles de segurança tradicionais:** ao convencer usuários a inserir credenciais em páginas de adversário no meio (AiTM) ou ativar sessões de desktop remoto, os adversários obtêm acesso sem executar código malicioso em hosts monitorados.
- **Explora o fator humano mais do que outras técnicas de engenharia social:** a interação direta entre pessoas oferece uma forma mais convincente de aplicar engenharia social aos usuários do que, por exemplo, e-mails de phishing.
- **Deixa poucos elementos para os defensores analisarem após a exploração:** em comparação com técnicas como phishing por SMS e phishing por e-mail, o vishing deixa relativamente poucos artefatos forenses para as equipes de resposta a incidentes, tornando as investigações pós-incidente mais desafiadoras.

Adversários voltados para a nuvem e direcionamento financeiro

A rápida adoção da infraestrutura de nuvem transformou o cenário da cibersegurança ao criar novas superfícies de ataque e desafiar os paradigmas tradicionais de segurança, que dependiam fortemente de perímetros de rede e controles de endpoint.

No Relatório de Investigação de Ameaças 2026 da CrowdStrike, estudos de caso ilustram como cibercriminosos e atores de ameaças de Estados-nação desenvolveram técnicas avançadas para abusar de serviços legítimos de nuvem, desde a exploração de fluxos de autenticação OAuth 2.0 e o sequestro de recursos computacionais em escala até a implementação de ferramentas customizadas desenvolvidas para ambientes nativos da nuvem.

Tendências de operações de phishing com OAuth 2.0 em 2026

Desde pelo menos fevereiro de 2025, a CrowdStrike observa adversários ligados a Estados abusando de fluxos OAuth 2.0 para realizar phishing e obter acesso a contas do Entra ID. Isso ocorreu principalmente na forma do fluxo de concessão de autorização de dispositivo OAuth 2.0, também conhecido como fluxo de código de dispositivo, no qual os atores de ameaças fornecem à vítima um código de dispositivo válido para fazer login na conta.

Nesses casos, o ator de ameaças pode coletar tokens de sessão para acessar a conta. Atores de ameaças ligados a Estados, incluindo o adversário COZY BEAR, ligado à Rússia, usaram vários métodos para fornecer esses códigos de dispositivo, incluindo páginas HTML, redirecionamentos por meio de uma aplicação maliciosa do Entra ID e comunicações por e-mail.

Em meados de abril de 2026, o CrowdStrike OverWatch e o CrowdStrike Falcon Complete identificaram o COZY BEAR visando um think tank sediado no Reino Unido por meio de uma combinação de WhatsApp e phishing de código de autorização OAuth 2.0, executada contra um alvo geopolítico de alto valor. Essa intrusão representa as operações avançadas e direcionadas com OAuth 2.0 que o COZY BEAR aperfeiçoou no último ano e reflete as técnicas mais amplas que os atores do e-crime agora estão adotando em escala.



Figura 7. Linha do tempo de intrusão de phishing do COZY BEAR

Sequestro de recursos de nuvem e roubo de credenciais para obter ganhos financeiros

Os cibercriminosos estão visando cada vez mais ambientes de nuvem para acessar ativos financeiros digitais e sequestrar recursos computacionais. Nos últimos 12 meses, as atividades de e-crime voltadas para a nuvem aumentaram 171%.

Operações não autorizadas de mineração de criptomoedas podem aumentar rapidamente os custos de computação em nuvem, principalmente quando os adversários usam ferramentas automatizadas para provisionar recursos em várias regiões em questão de minutos.

A recuperação nem sempre é simples. Os atores de ameaças costumam empregar técnicas como desativar o encerramento de instâncias por meio de modificações na API para impedir que as organizações recuperem os recursos sequestrados. Eles também estabelecem persistência por meio de mecanismos nativos da nuvem, como usuários de identidade da nuvem com backdoors, modificações em políticas de confiança entre contas e caminhos de execução atípicos, como as configurações de ciclo de vida de serviços gerenciados de machine learning (ML).

Ator de ameaças de e-crime realiza sequestro de recursos de nuvem por meio de implementação com vários vetores

Em 8 de janeiro de 2026, o CrowdStrike OverWatch detectou um ator de ameaças de e-crime sequestrando recursos de nuvem de uma empresa de tecnologia dos EUA para realizar uma operação de mineração de criptomoedas, um claro exemplo do direcionamento à nuvem com motivação financeira que, segundo as observações da CrowdStrike, vem aumentando no último ano. Depois de obter acesso inicial, o ator de ameaças de e-crime agiu de forma rápida e metódica, usando três vetores de ataque paralelos para maximizar o alcance da operação e, ao mesmo tempo, estabelecendo persistência entre contas para garantir que o sequestro não fosse facilmente interrompido.

Ganho financeiro: sequestro de recursos na nuvem e roubo de dados

FLUXO DO ATAQUE:

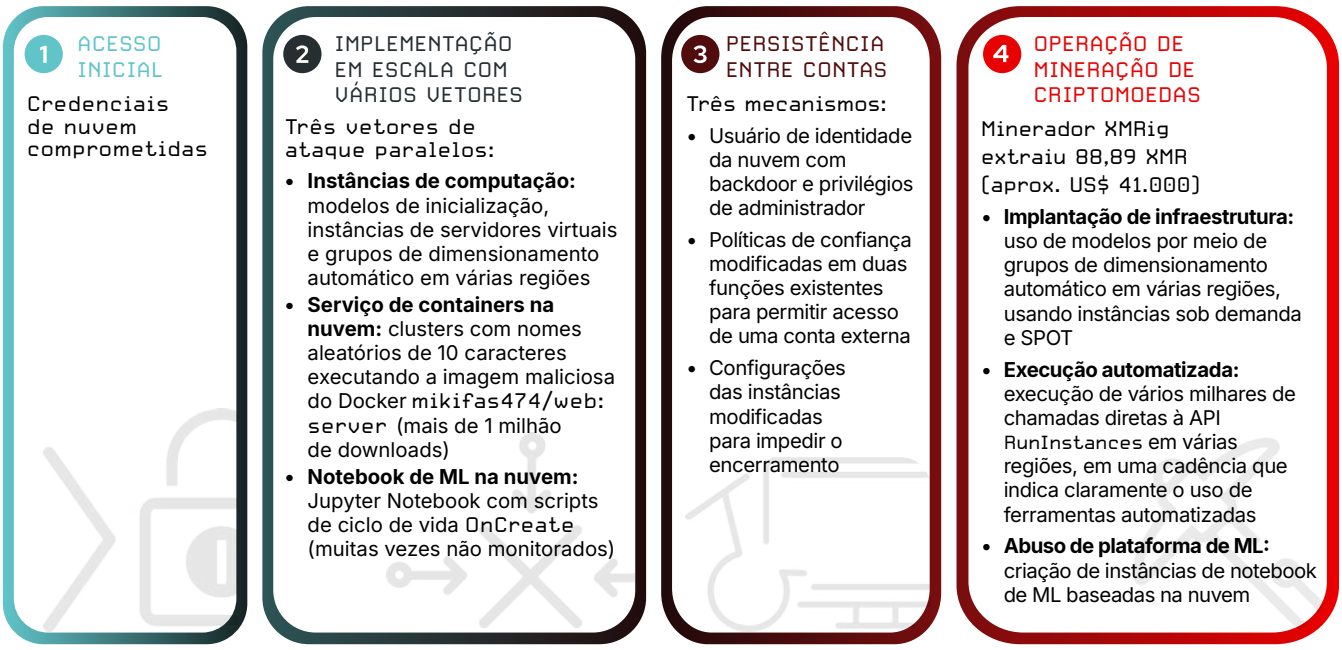


Figura 8. Fluxo de implantação do sequestro de recursos de nuvem

OVERCAST PANDA: operações de acesso próximo e a ameaça ao endpoint além da defesa de rede

O adversário OVERCAST PANDA, ligado à China, representa uma das ameaças persistentes e mais sofisticadas em termos operacionais enfrentadas por organizações com funcionários que viajam para a China. Ao contrário da maioria dos atores de ameaças cibernéticas que operam à distância, o OVERCAST PANDA emprega uma abordagem diferente: proximidade física com o dispositivo-alvo. Isso permite que o adversário contorne completamente os controles de segurança convencionais baseados em rede, tornando as defesas de perímetro, a detecção de endpoint e o treinamento de conscientização dos usuários ineficazes contra o vetor de comprometimento inicial.

Entre março e maio de 2026, o CrowdStrike OverWatch identificou e interrompeu uma série de intrusões de acesso próximo nas quais o OVERCAST PANDA implantou seu backdoor proprietário FlowCloud em dispositivos por meio de acesso físico direto enquanto essas pessoas estavam na China. Em cada caso, o time de threat hunters identificou atividades anômalas de endpoint compatíveis com a cadeia de execução característica do FlowCloud, possibilitando a notificação imediata do cliente e a rápida contenção antes que o adversário atingisse seus objetivos de coleta.

O padrão de direcionamento documentado nas operações de acesso próximo do OVERCAST PANDA em 2026 não é oportunista, mas é abrangente. É muito provável que cada intrusão reflita uma seleção deliberada de pessoas cujas funções profissionais proporcionam acesso a informações diretamente relevantes para as prioridades da inteligência estatal chinesa. Qualquer pessoa que viaje pela China é um alvo em potencial se tiver acesso a essas informações.

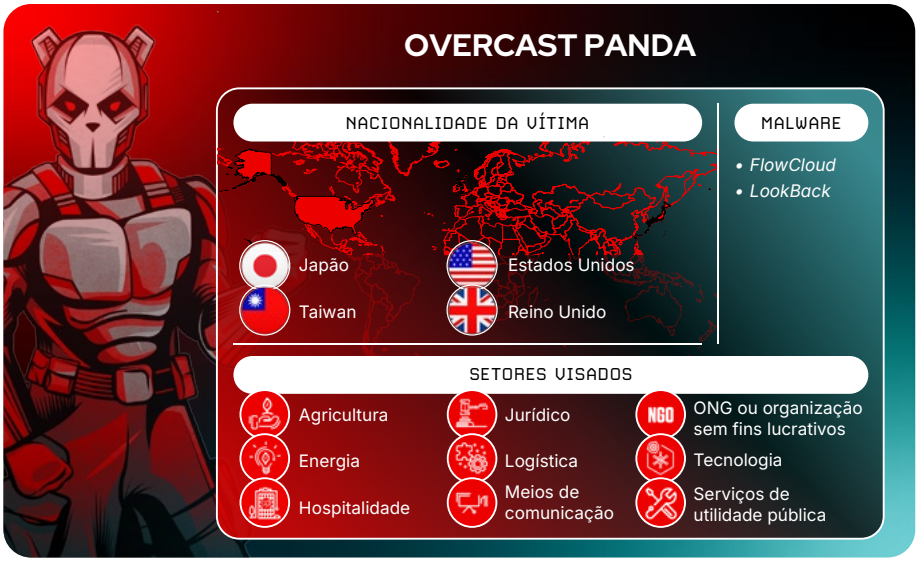


Figura 9. Resumo do escopo de alvos do OVERCAST PANDA e dos malwares atribuídos



Figura 10. Resumo das táticas, técnicas e procedimentos (TTPs) do OVERCAST PANDA em campanhas de acesso próximo

Conclusão

O último ano marcou um capítulo decisivo na evolução da investigação de ameaças. Da aceleração da exploração de vulnerabilidades aos ataques à cadeia de suprimento de software que se disseminam rapidamente, o time de threat hunters enfrenta uma necessidade sem precedentes de velocidade e precisão. Seja motivados por ganho financeiro, espionagem ou acesso de longo prazo, os adversários evasivos exploram relações de confiança e vão além das superfícies de ataque tradicionais para evitar a detecção.

O time de threat hunters do CrowdStrike OverWatch revelou como os adversários não operam mais em silos. Eles executam ataques entre domínios envolvendo ferramentas de IA e ambientes de identidade, endpoint e nuvem, usando tanto estratégias com acesso interativo quanto ataques automatizados que desafiam as ferramentas de segurança tradicionais. Os defensores estão se preparando para enfrentar o desafio com detecção mais rápida, contexto aprofundado e defesa coordenada baseada em inteligência.

Este relatório reforça por que a investigação proativa e orientada por inteligência é essencial. As equipes de segurança precisam integrar a telemetria de toda a empresa, operacionalizar a inteligência de ameaças e aproveitar a automação para ampliar a capacidade humana. É exatamente isso que o CrowdStrike OverWatch faz, usando IA para ajudar o time de threat hunters a identificar e priorizar continuamente os dados mais estreitamente relacionados às atividades de adversários e garantindo que a experiência humana seja sempre o fator determinante final.

Recomendações

1 IA segura para reduzir riscos emergentes nos negócios e operacionais

A IA está cada vez mais integrada a ambientes empresariais, de desenvolvimento e de nuvem, tornando-se um alvo de alto valor para os adversários. Os atores de ameaças estão abusando do acesso corporativo a LLMs, explorando software de servidor relacionado à IA, visando ambientes de desenvolvimento centrados em IA e usando IA para acelerar phishing, reconhecimento e exploração de vulnerabilidades. As organizações devem proteger os sistemas de IA como infraestrutura crítica. Isso começa pelo inventário de aplicações de IA, endpoints de modelos, chaves de API, contas de serviço, ferramentas de desenvolvimento de IA e recursos de nuvem/GPU. As equipes de segurança devem impor acesso com privilégios mínimos a modelos e APIs, proteger credenciais de IA, monitorar o uso anormal de LLMs e picos de custos, considerar a segmentação da infraestrutura de LLM das redes internas quando apropriado, avaliar as dependências de IA quanto aos riscos à cadeia de suprimento e reforçar a segurança dos ambientes de desenvolvimento de IA. Elas também devem incorporar ameaças voltadas para IA e viabilizadas por IA aos planos de resposta a incidentes e fluxos de trabalho de investigação de ameaças.

2 Considere identidade e SaaS como superfícies de ataque primárias

As plataformas de identidade e SaaS estão no centro do acesso, dos dados e das operações empresariais, o que as torna alvos prioritários. Os adversários estão usando vishing, abuso de OAuth, phishing de código de dispositivo e tokens de sessão roubados para comprometer contas e acessar rapidamente dados de SaaS. As organizações devem impor autenticação multifator (MFA) resistente a phishing, monitorar logins anômalos e o registro de dispositivos de MFA, aplicar acesso com privilégios mínimos a contas humanas e não humanas e detectar atividades incomuns em SaaS, como acesso em massa a arquivos, agentes de usuário anormais e uso suspeito de tokens.

3 Elimine pontos cegos entre domínios para impedir ataques de alto impacto

As intrusões mais disruptivas da atualidade têm sucesso ao explorar lacunas entre domínios, ferramentas e equipes de segurança, em vez de pontos fracos em um único controle. Os adversários encadeiam atividades em endpoints, ambientes de nuvem, aplicações SaaS, sistemas de identidade, fluxos de trabalho de desenvolvedores e hosts não gerenciados para evitar a detecção. As organizações devem consolidar a telemetria, aplicar correlação entre domínios por meio de fluxos de trabalho de detecção e resposta estendidas (XDR) e SIEM de última geração e automatizar o enriquecimento com inteligência de ameaças para visualizar caminhos de ataque completos e acelerar a resposta.

4 Proteja a cadeia de suprimento de software e os fluxos de trabalho de desenvolvedor

A confiança em atualizações de software, dependências de código aberto e pipelines de desenvolvimento se tornou uma dependência essencial para as empresas e um dos principais alvos dos adversários. Pacotes maliciosos, credenciais roubadas de mantenedores, pipelines de CI/CD comprometidos e ferramentas confiáveis de desenvolvedores estão permitindo que os adversários roubem credenciais e avancem para ambientes de nuvem. As organizações devem reforçar a segurança dos ambientes de desenvolvimento, impor a assinatura de código e a validação de dependências, verificar repositórios e pacotes em busca de anomalias, proteger as identidades dos desenvolvedores e avaliar riscos de terceiros para reduzir a probabilidade de que softwares confiáveis se tornem um veículo para comprometimento.

5 Reduza proativamente a superfície de ataque em toda a empresa

Os adversários estão agindo mais rapidamente do que os ciclos tradicionais de gerenciamento de vulnerabilidades conseguem acompanhar. Eles exploram vulnerabilidades públicas em questão de dias, abusam de configurações incorretas de nuvem e identidade, visam serviços expostos e transformam fluxos de trabalho confiáveis de desenvolvedores e IA em caminhos para obter acesso e roubar credenciais. As organizações devem identificar e priorizar continuamente as exposições com maior probabilidade de criar caminhos de ataque reais, incluindo vulnerabilidades críticas, contas com privilégios excessivos, configurações de nuvem arriscadas, ativos não gerenciados, sistemas expostos à Internet e pontos fracos em ambientes de SaaS, IA e desenvolvimento. Ao reforçar a segurança dos sistemas de forma abrangente, as equipes de segurança podem reduzir a superfície de ataque, limitar o raio de impacto e interromper as intrusões antes que ganhem força.

6 Priorize inteligência de ameaças e investigação proativa

Quando os ataques se desenrolam em minutos ou segundos, a defesa reativa não é mais suficiente. Uma abordagem orientada por inteligência ajuda as organizações a entender quais adversários as estão visando, como eles operam e onde provavelmente atacarão em seguida. Ao aplicar inteligência de ameaças e análise das estratégias dos adversários por meio de investigação proativa, as equipes podem identificar bases de apoio sigilosos, incluindo atividades de AiTM, registros suspeitos de MFA, abuso da nuvem e anomalias na cadeia de suprimento, antes que os ataques se intensifiquem. Agentes de IA especializados podem acelerar ainda mais a análise de inteligência, a investigação, a triagem e a resposta, ajudando os defensores a transformar insights em ações mais cedo no ciclo de vida do ataque.

7 Reforce a resiliência humana contra engenharia social e intrusões rápidas

À medida que os adversários recorrem cada vez mais a phishing, vishing e abuso de confiança para contornar controles técnicos, a tomada de decisões humanas continua sendo essencial para prevenir ataques. As organizações devem reforçar os programas de conscientização com táticas reais dos adversários, incluindo falsificação de identidade de profissionais de TI, phishing AiTM, solicitações suspeitas de MFA e engenharia social destinada a capturar credenciais ou registrar dispositivos não autorizados.

Para as equipes de segurança, a preparação sob pressão é essencial. Exercícios tabletop e operações red/blue team regulares ajudam as organizações a identificar lacunas na detecção, na tomada de decisões e na resposta, garantindo que as equipes possam agir com rapidez e eficácia quando os ataques ocorrerem. A prática contínua fortalece a resiliência organizacional e reduz a probabilidade de que pequenas falhas se transformem em incidentes graves.

Sobre a CrowdStrike

A CrowdStrike (NASDAQ: CRWD), líder global em cibersegurança, 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.

Alimentada 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 remediação automatizadas, investigação de ameaças de elite e observabilidade priorizada de vulnerabilidades.

Desenvolvida especificamente na nuvem com uma arquitetura de agente leve único, a plataforma Falcon oferece implantação rápida e escalável, proteção e desempenho superiores, complexidade reduzida e tempo para retorno do valor imediato.

CrowdStrike: Nós interrompemos as ameaças.

Saiba mais em: www.crowdstrike.com/pt-br

Siga-nos: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Comece uma avaliação gratuita hoje:
https://www.crowdstrike.com/pt-br/products/trials/try-falcon/

© 2026 CrowdStrike, Inc. Todos os direitos reservados.