RESUMO EXECUTIVO

CROWDSTRIKE

RELATÓRIO GLOBAL DE AMEAÇAS 2025

O ano do adversário empreendedor

Todos os anos, o Relatório Global de Ameaças da CrowdStrike oferece à indústria da cibersegurança uma análise completa do cenário de ameaças do ano anterior, bem como do comportamento e das estratégias dos adversários que moldaram esse cenário. Nas páginas do relatório, apresentamos as tendências e os eventos que definiram o ano de 2024, os métodos que os adversários estão usando e as medidas que as organizações devem adotar para se proteger das novas ameaças.

Ao longo de 2024, os adversários adotaram uma empresarial, refinando e escalando suas estratégias bem-sucedidas e simultaneamente explorando novas tecnologias para impulsionar sua velocidade e eficiência. Os adversários modernos são determinados e profissionais. Eles aprendem e se adaptam rapidamente às transformações das defesas e se mantêm extremamente focados em suas metas.

Para detê-los, precisamos conhecê-los. Aprender os comportamentos, as motivações e as técnicas dos adversários pode construir um entendimento mais sólido da atividade deles e, consequentemente, uma defesa mais forte.

O Relatório Global de Ameaças 2025 da CrowdStrike faz uma retrospectiva de 2024, para que os leitores tenham acesso a uma visão mais completa das ameaças que enfrentam. Este relatório consiste em observações da equipe de elite de Operações contra Adversários da CrowdStrike, que combina o poder da inteligência de ameaças, a agilidade das equipes dedicadas de investigação de ameaças e trilhões de eventos de telemetria da plataforma CrowdStrike Falcon® nativa em IA.

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

PARA OBTER MAIS INFORMAÇÕES SOBRE QUALQUER UM DOS ADVERSÁRIOS MENCIONADOS NESTE RESUMO EXECUTIVO E SOBRE AQUELES QUE ATACAM SEU SETOR OU SUA REGIÃO, CONFIRA O CROWDSTRIKE ADVERSARY UNIVERSE.

Visão geral do cenário de ameaças

Os adversários continuam acelerando: o tempo médio para comprometimento pelo e-crime (isto é, o tempo que um adversário leva para se mover do primeiro host comprometido para outro dentro da organização alvo) caiu para **48 minutos** em 2024, e o menor tempo para comprometimento registrado foi de **51 segundos**.

Os métodos de acesso estão evoluindo: os adversários estão adotando phishing por voz (vishing), phishing de retorno de chamada e engenharia social aplicada a suporte técnico para entrar nas redes alvos. Eles também aproveitam credenciais comprometidas: os anúncios de brokers de acesso, que vendem credenciais válidas roubadas, cresceram **50% ao ano**. **Mais da metade (52%) das vulnerabilidades** observadas pela CrowdStrike em 2024 estavam relacionadas a acesso inicial.

O sigilo continua sendo prioridade: as ameaças modernas são dominadas por técnicas de intrusão interativa, nas quais os adversários usam ações com acesso interativo para alcançar seus objetivos. Em 2024, **79% das detecções estavam livres de malware**, e a CrowdStrike observou um **aumento de 35% ao ano** nas campanhas de intrusão interativa.

A IA generativa é uma estratégia dos adversários: em 2024, os adversários usaram cada vez mais a IA generativa para aprimorar sua engenharia social, acelerar operações de desinformação e facilitar atividades maliciosas na rede.

Cresce o empreendimento cibernético na China: a atividade no nexo chinês cresceu **150% em todos os setores**, com um aumento impressionante de **200% a 300%** nos setores mais atacados, como serviços financeiros, mídia, fabricação e indústrias/engenharia.

Os ambientes na nuvem estão sitiados: a nuvem continua sendo um importante alvo devido ao seu vasto volume de dados, escalabilidade e erros de configuração exploráveis. Em 2024, a CrowdStrike identificou um **aumento de 26%** em intrusões na nuvem classificadas como novas e não atribuídas, o que indica que mais adversários estão mirando os serviços na nuvem.

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
SAIGA	CAZAQUISTÃO
SPHINX	EGITO
SPIDER	eCRIME
TIGER	ÍNDIA
WOLF	TURQUIA

Intrusões interativas por região

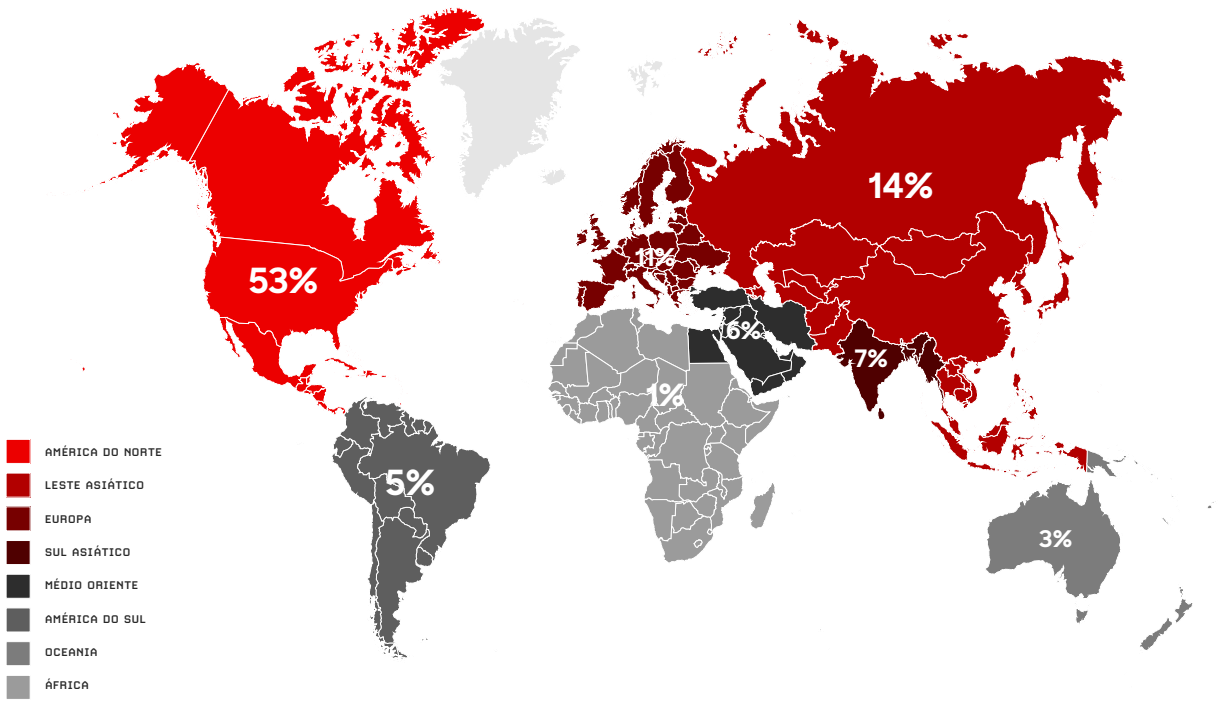

Figura 1. Intrusões interativas por região; janeiro a dezembro de 2024

Os 10 setores mais atacados por intrusões interativas

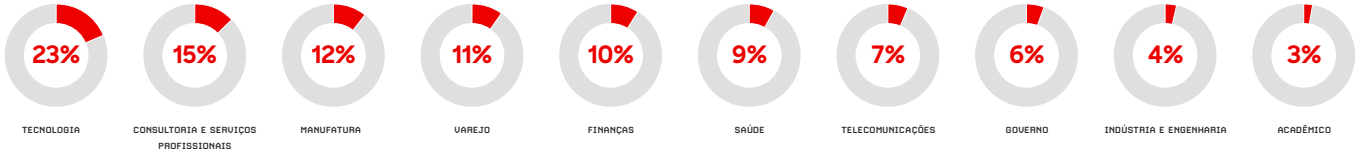

Figura 2. Os 10 setores mais atacados por intrusões interativas; janeiro a dezembro de 2024

Essas estatísticas destacam o alcance global das operações adversárias e a necessidade de estratégias de segurança entre domínios que levem com conta o comprometimento de identidades, movimento lateral e vetores de ataque baseados na nuvem.

A mudança em direção a técnicas de ataque livres de malware tem sido uma tendência determinante nos últimos cinco anos. Em 2024, as atividades livres de malware foram responsáveis por 79% das detecções, um aumento significativo em relação ao índice de 40% registrado em 2019.

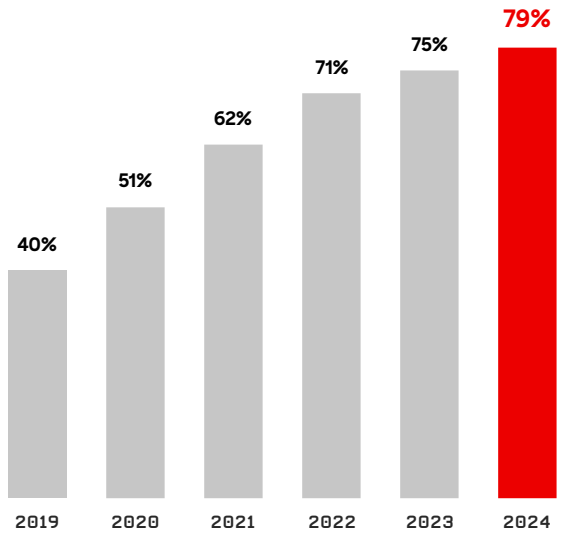

Figura 3. Percentual de detecções de ataques livres de malware; 2019 a 2024

Principais temas dos adversários

A ENGENHARIA SOCIAL ENQUANTO NEGÓCIO

Em 2024, as técnicas de acesso inicial mudaram, e os adversários passaram a atacar pontos fracos humanos, usando credenciais comprometidas e engenharia social para obter acesso e se movimentar lateralmente dentro das organizações. A CrowdStrike observou um aumento nas campanhas de engenharia social por telefone e na manipulação relacionada a suporte técnico, o que sinaliza uma evolução nas táticas de e-crime.

- As operações de vishing cresceram 442% entre o primeiro e o segundo semestres de 2024.
- Sofisticados grupos de e-crime, como CURLY SPIDER, CHATTY SPIDER e PLUMP SPIDER usaram essas táticas para roubar credenciais, estabelecer sessões remotas e evitar a detecção.
- Ao longo do ano de 2024, a CrowdStrike rastreou pelo menos seis campanhas similares, mas distintas, na qual atores de ameaças que se passavam por técnicos de TI telefonavam para os alvos e tentavam persuadi-los a estabelecer sessões de suporte remoto.

ESTUDO DE CASO

CURLY SPIDER

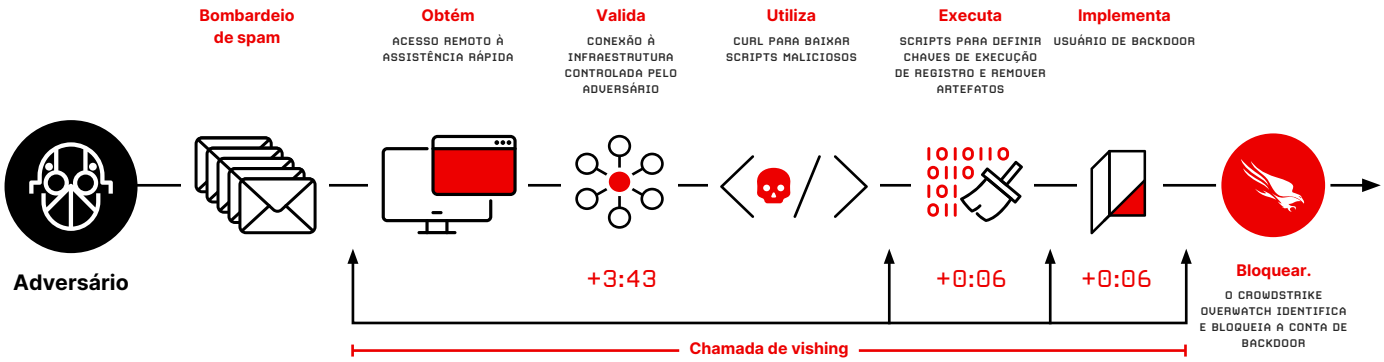

Figura 4. Linha do tempo mostrando o CrowdStrike OverWatch ultrapassando a velocidade do CURLY SPIDER para interromper um ataque de engenharia social em menos de quatro minutos

Em 2024, o CURLY SPIDER surgiu como um dos adversários mais rápidos e mais adaptáveis no e-crime. Neste caso, os invasores tentavam atingir seus objetivos sem precisar invadir outro dispositivo. Toda a cadeia de ataque — da interação inicial com o usuário e engenharia social e até a introdução de uma conta backdoor e o estabelecimento de persistência — levou menos de quatro minutos.

Assim que o CURLY SPIDER obtém o acesso inicial, a janela de oportunidade é limitada; o acesso só dura enquanto a vítima estiver na chamada. Para estender o controle, o objetivo imediato do adversário é estabelecer acesso persistente antes que a sessão termine.

Com o acesso remoto garantido, o CURLY SPIDER se move rapidamente — geralmente enquanto ainda está em contato ativo com a vítima — para implementar payloads e estabelecer persistência. A maior parte do tempo de intrusão é gasta garantindo a conectividade e solucionando problemas de acesso para alcançar scripts maliciosos hospedados na nuvem.

A IA generativa e o adversário empreendedor

Apesar da relativa novidade da IA generativa, a CrowdStrike tem identificado vários casos em que ela está sendo usada pelos adversários. A facilidade da IA generativa e suas poderosas funcionalidades fazem dela uma ferramenta atrativa. Ela permite que os atores de ameaças criem atrativos e-mails de phishing, conduzam campanhas fraudulentas e desenvolvam scripts maliciosos, uma tendência que deve continuar em 2025.

- Grandes modelos de linguagem (LLMs) e modelos de IA generativa que criam imagens fotorrealistas são capazes de gerar conteúdo convincente em escala, com conhecimento mínimo. Essas tecnologias podem impulsionar iniciativas de engenharia social ou operações de informações.
- A CrowdStrike respondeu à atividade do FAMOUS CHOLLIMA em **304 incidentes ao longo do ano**, com **40% dos casos representado operações de ameaças internas**. Em alguns casos, o adversário usou IA generativa para criar perfis falsos do LinkedIn.
- O NITRO SPIDER usou sites gerados por IA em campanhas de malvertising, filtrando vítimas por meio de anúncios maliciosos e redirecionando-as para páginas falsas criadas por IA.

Empreendimento cibernético em crescimento na China

Em 2024, as capacidades de ciberespionagem da China alcançaram um crítico ponto de inflexão, marcado por ataques cada vez mais ousados, táticas mais sigilosas e capacidade operacional expandida. Esses avanços refletem as prioridades da inteligência estratégica chinesa, que incluem influência regional, aquisição de tecnologia e supressão de supostas ameaças à estabilidade do regime.

- Ao longo de 2024, os adversários no nexo chinês continuaram operando em todos os setores e regiões do mundo, mantendo o escopo de suas operações e ampliando a escala delas.
- A CrowdStrike identificou sete novos adversários no nexo chinês em 2024, o que enfatiza uma mudança em direção a intrusões mais direcionadas e específicas. Cinco desses grupos têm níveis diferenciados de especialização e sofisticação.
- LIMINAL PANDA, LOCKSMITH PANDA e OPERATOR PANDA são adversários altamente capacitados, com competências e ferramentas incomparáveis para o ataque a redes de telecomunicações; o VAULT PANDA se concentra no setor de serviços financeiros em todo o mundo; e o ENVOY PANDA é um adversário que, embora apresentasse baixa capacidade no passado, tem aperfeiçoado acentuadamente sua postura de segurança de operações (OPSEC).

Os atores conscientes da nuvem continuam inovando

Adversários focados na nuvem exploram erros de configuração, credenciais roubadas e ferramentas de gerenciamento da nuvem, com o intuito de se infiltrar em sistemas, se movimentar lateralmente e manter o acesso persistente para a prática de atividades maliciosas, como roubo de dados e implantação de ransomware. Os atores do nexo chinês e norte-coreano vêm expandindo seus ataques a plataformas na nuvem. Grupos de e-crime estão adotando táticas avançadas, como abuso de relações de confiança e ameaças internas, para comprometer os recursos na nuvem.

- O abuso de contas válidas tem se tornado a principal tática de acesso inicial, respondendo por **35% dos incidentes na nuvem** no primeiro semestre de 2024. Cada vez mais, os invasores estão usando táticas sigilosas e tentando acessar credenciais para atacar contas válidas.
- Em 2023, o adversário SCATTERED SPIDER foi responsável por **30% de todas as intrusões na nuvem**. Esse número caiu para **13% em 2024**, em parte por que muitos atores de ameaças oportunistas e de estados-nação estão atacando o painel de controle na nuvem.
- Em **75% dos casos observados**, atores conscientes da nuvem removeram indicadores dos arquivos de log, na tentativa de escapar da detecção.

O empreendimento da exploração de vulnerabilidade

Os adversários cada vez mais miram dispositivos de rede expostos na internet, explorando seus pontos fracos de segurança inerentes para obter acesso inicial onde a visibilidade de detecção e resposta de endpoint (EDR) é limitada. Eles realizam execução remota de código (RCE) com técnicas como encadeamento de exploits ou abuso de funcionalidades legítimas de produtos, e muitas vezes redirecionam vulnerabilidades conhecidas para comprometer repetidamente os mesmos dispositivos. Os adversários continuam atacando dispositivos no fim da vida útil, já que sistemas desatualizados com vulnerabilidades não corrigidas servem como uma base de apoio para os ambientes alvos.

- Os atores de ameaças estão atacando vulnerabilidades dentro do sistema operacional (SO) patenteado dos dispositivos de rede. Essas vulnerabilidades são alvos atraentes porque possibilitam que os invasores usem uma falha para atacar múltiplos produtos que executam o mesmo SO.
- Em encadeamento de múltiplas vulnerabilidades traz mais vantagens aos invasores. Em primeiro lugar, o encadeamento permite que eles realizem RCE não autenticada, combinando vários exploits em um só ataque. Em segundo lugar, o encadeamento de exploits enfraquece o processo de correção baseado na pontuação de gravidade, que é adotado em muitas empresas.
- Para descobrir novas vulnerabilidades ou abusar de funcionalidades legítimas do produto, os adversários provavelmente usarão blogs de tecnologia e operacionalizarão exploits de provas de conceito (POCs) públicas numa velocidade maior do que nos anos anteriores.

Previsão de que a exploração de SaaS continue

Ao longo de 2024, a Inteligência CrowdStrike observou que vários adversários de e-crime e de intrusão direcionada usam o acesso a aplicações de software como um serviço (SaaS) baseadas na nuvem para obter dados e, assim, facilitar movimento lateral, extorsão e ataques via terceiros. Muitas vezes, os atores de ameaças acessavam essas aplicações comprometendo identidades de logon único (SSO). À medida que a adoção da nuvem cresce, a previsão é de que os adversários refinem suas estratégias em 2025, o que torna a exploração do SaaS uma ameaça crítica e dinâmica.

- No primeiro semestre de 2024, atores de ameaças conscientes da nuvem atacaram o Microsoft 365 com frequência. O **SharePoint foi acessado em 22% das intrusões, e o Outlook em 17% delas**.
- O SCATTERED SPIDER aproveitou contas de SSO comprometidas para acessar diversas aplicações SaaS integradas, incluindo ferramentas de bate-papo, gerenciamento de relacionamento com o cliente, gerenciamento de credenciais, armazenamento de documentos, produtividade e segurança.
- Em muitas intrusões, os adversários buscavam as seguintes informações das aplicações SaaS: 1) credencias de contas e documentação de infraestrutura de rede para realizar movimento lateral e 2) dados de seguro cibernético e receita para fins de extorsão.

Conclusão

No início de 2025, o cenário de cibersegurança continua mudando rapidamente e apresentando desafios consideráveis para organizações em todos os setores e regiões geográficas. A resiliência, inovação e capacidade de adaptação dos adversários ressaltam a necessidade crítica de um abrangente entendimento das ameaças atuais, em todos os aspectos do cenário.

A engenharia social se proliferou ao longo de 2024, e os adversários passaram a explorar novos métodos de acesso inicial para burlar as defesas de segurança. A IA generativa transformou-se em uma importante ferramenta adversária, especialmente em campanhas de engenharia social e campanhas de operações de inteligência (IO) de ritmo acelerado. A CrowdStrike prevê que, em 2025, os adversários empregarão IA generativa em suas operações.

Os adversários que praticam e-crime direcionado continuam sendo uma ameaça persistente a setores específicos. Durante 2024, eles demonstraram determinação em seus ataques, e muitas vezes o menor grau de sofisticação era compensado por um profundo conhecimento dos setores e das regiões geográficas das vítimas, bem como das tecnologias associadas.

Os adversários de intrusão direcionada estavam ativos e inovadores em 2024, e adaptaram suas táticas para alcançar metas estratégias e geopolíticas e escapar das defesas aprimoradas. Existe a previsão de que os adversários do nexo russo continuem sua agressiva busca pela vitória na Ucrânia, concentrando-se em operações de coleta de inteligência voltadas à Ucrânia e a membros da OTAN. Os adversários do nexo chinês provavelmente se beneficiarão dos investimentos de longo prazo da China em programas cibernéticos, o que é perceptível no aumento das práticas de OPSEC, na manutenção do alto ritmo operacional e na prolífica atividade de intrusões globais.

O cenário de exploração de vulnerabilidade permanece sendo uma preocupação crítica. A previsão é de que os atores de ameaças continuem atacando agressivamente os dispositivos da periferia da rede, especialmente dispositivos de rede. As aplicações SaaS também estão na mira. Depois de identificar que os adversários de e-crime e intrusão direcionada utilizam o acesso a aplicações SaaS baseadas na nuvem para obter dados e explorar movimento lateral, extorsão e ataques via terceiros, a CrowdStrike prevê que a exploração de SaaS será uma ameaça que deve ser observada em 2025.

Durante o ano de 2024, o adversário empreendedor expandiu a maturidade e a sofisticação de suas operações em diferentes setores e regiões geográficas. À medida que essas ameaças evoluem em 2025, a equipe de Operações contra adversários da CrowdStrike continua comprometida a identificar, rastrear e barrar os atores de ameaças, quando e onde for possível.

Recomendações

1 Proteger todo o ecossistema de identidades

Os adversários cada vez mais atacam identidades usando o roubo de credenciais e engenharia social e contornando a autenticação multifatorial (MFA), enquanto dissimuladamente se movem lateralmente entre ambientes locais, na nuvem e SaaS, por meio de relações confiáveis. Isso possibilita que eles se passem por usuários legítimos, elevem o acesso e escapem da detecção.

As organizações precisam adotar soluções de autenticação multifatorial (MFA) resistentes a phishing, como chaves de segurança de hardware, para evitar o acesso não autorizado. Políticas fortes de identidade e acesso são essenciais e devem abranger acesso just-in-time, revisões regulares da conta e controles de acesso condicional. As ferramentas de detecção de ameaças devem monitorar o comportamento em endpoints e em ambientes locais, na nuvem e SaaS, a fim de detectar elevação de privilégios, acesso não autorizado ou criação de conta backdoor. A integração dessas ferramentas a plataformas de detecção e resposta estendidas (XDR) assegura uma visibilidade ampla e uma defesa unificada contra os adversários.

Além disso, as organizações devem ensinar os usuários a reconhecer tentativas de vishing e phishing, mantendo sempre um monitoramento proativo para detectar e responder a ameaças baseadas em identidade.

2 Eliminar lacunas de visibilidade entre domínios

O crescente uso de técnicas com acesso interativo e de ferramentas legítimas pelos adversários dificulta a detecção e a resposta aos ataques. Diferentemente do malware tradicional, esses métodos permitem que os invasores burlem as medidas de segurança tradicionais executando comandos e utilizando software legítimo para mimetizar operações normais.

Para combater isso, as organizações precisam modernizar suas estratégias de detecção e resposta. Soluções de detecção e resposta estendidas (XDR) e de gerenciamento e correlação de eventos de segurança (SIEM) de última geração oferecem uma visibilidade unificada de endpoints, redes, ambientes na nuvem e sistemas de identidade, para que os analistas correlacionem comportamentos suspeitos e visualizem o caminho completo do ataque.

A investigação de ameaças e a inteligência de ameaças, se proativas, aprimoram ainda mais a detecção, pois identificam possíveis padrões de ataque e trazem insights sobre táticas, técnicas e procedimentos dos adversários. Com inteligência em tempo real, as organizações podem se manter informadas sobre novas ameaças, prever ataques e priorizar esforços críticos de segurança.

3 Proteger a nuvem como infraestrutura central

Adversários focados na nuvem estão explorando erros de configuração, credenciais roubadas e ferramentas de gerenciamento da nuvem, com o intuito de se infiltrar em sistemas, se movimentar lateralmente e manter o acesso persistente para a prática de atividades maliciosas, como roubo de dados e implantação de ransomware.

Plataformas de proteção de aplicações nativas em nuvem (CNAPPs) com capacidades de detecção e resposta na nuvem (CDR) são essenciais para conter essas ameaças.

Essas soluções oferecem aos operadores uma visão unificada de sua postura de segurança na nuvem e os ajudam a rapidamente detectar, priorizar e remediar erros de configuração, vulnerabilidades e ameaças adversárias. Além disso, a adoção de rígidos controles de acesso, como acesso baseado em função e políticas condicionais, limita a exposição de sistemas críticos e garante o monitoramento contínuo de anomalias, incluindo logins de locais inesperados.

Auditorias regulares também são fundamentais para a manutenção da segurança. Ferramentas automatizadas podem revelar configurações de armazenamento excessivamente permissivas, APIs expostas e vulnerabilidades não corrigidas. Revisões frequentes dos ambientes na nuvem asseguram a correção imediata de permissões não utilizadas e configurações desatualizadas.

4 Priorizar vulnerabilidades com uma abordagem focada no adversário

Cada vez mais, os adversários estão explorando vulnerabilidades divulgadas publicamente, usando encadeamento de exploits e combinando múltiplas vulnerabilidades para obter acesso rápido, escalar privilégios e burlar defesas. Esses ataques em múltiplos estágios muitas vezes contam com recursos disponíveis publicamente, como exploits de POCs e blogs técnicos, o que permite que os adversários elaborem payloads eficazes e difíceis de detectar.

Para conter essas ameaças, as organizações devem priorizar a correção ou a atualização frequentes de sistemas críticos, especialmente serviços de internet que são frequentemente atacados, como servidores da web e gateways de VPN. O monitoramento de sinais sutis de encadeamento de exploits, como falhas inesperadas ou tentativas de elevação de privilégios, pode ajudar a detectar ataques antes que eles avancem.

Ferramentas como o CrowdStrike Falcon® Exposure Management, criadas com priorização de IA nativa, possibilitam que as equipes reduzam o ruído e se concentrem nas vulnerabilidades mais relevantes, especificamente naquelas que afetam sistemas críticos e de alto risco. Ao adotar abordagens de segurança proativas, descobrir exposições na superfície de ataque e aproveitar a automação, as organizações podem mitigar ameaças sofisticadas e limitar as oportunidades dos adversários.

5 Conhecer o adversário e se preparar

Quando se sabe que um ciberataque se desenrola em minutos — ou até mesmo segundos —, estar preparado pode ser a diferença entre a contenção e a catástrofe. Com uma abordagem orientada por inteligência, as equipes de segurança conseguem ir além da defesa reativa e compreender qual adversário está atacando, como ele opera e quais são seus objetivos. Com inteligência de ameaças, perfil do adversário e análise da estratégia, as equipes de segurança podem priorizar recursos, adaptar defesas e investigar ativamente ameaças as antes que elas progridam. A inteligência de ameaças da CrowdStrike não apenas detecta ameaças conhecidas — ela também prevê estratégias novas e em desenvolvimento e assegura que os defensores estejam sempre um passo à frente. Ao integrar perfeitamente inteligência em fluxos de trabalho de segurança, as organizações podem acelerar tempos de resposta, barrar adversários e converter inteligência em ação.

Embora a tecnologia seja essencial para detectar e interromper intrusões, o usuário final continua sendo um elo crítico na cadeia para impedir ataques. As organizações devem implementar programas de conscientização do usuário 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.

Baixe o relatório completo

O Relatório Global de Ameaças 2025 da CrowdStrike apresenta uma análise abrangente dos eventos e tendências mais significativos das atividades de ciberameaças em 2024. 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: https://www.crowdstrike.com/pt-br/

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

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