CROWDSTRIKE

As principais técnicas de ataque em nuvem

e como se defender delas

A nuvem é uma superfície de ataque em constante crescimento e evolução. Proteger este ambiente contra o aumento dos ataques em nuvem requer um conhecimento profundo das atividades dos atores de ameaças. Trazemos aqui as três principais tendências de ataques em nuvem observadas pela CrowdStrike e como se defender contra elas.

Cada vez mais, os ciber criminosos têm a nuvem na mira

Os ambientes de nuvem seguem crescendo:

41,4% dos líderes de nuvem afirmam que estão aumentando o seu uso de serviços e produtos baseados em nuvem[1]

33,4% estão planejando migrar de um software corporativo legado para ferramentas baseadas em nuvem[1]

32,8% estão migrando workloads locais para a nuvem[1]

E os atores de ameaças já perceberam.

Em 2022, a CrowdStrike observou:

95% de aumento nos casos de exploração da nuvem

3x mais casos envolvendo atores de ameaças focados na nuvem

71% dos ataques foram livres de malware

Por que atacar ambientes de nuvem?

Ambientes multinuvem são complexos e, portanto, mais difíceis de proteger

Processos rápidos de entrega de software deixam as aplicações nativas em nuvem suscetíveis a vulnerabilidades e configurações incorretas

Ambientes rogue (clandestinos) e de shadow cloud não têm os controles e supervisão de segurança

Produtos de segurança isolados deixam pontos cegos que os criminosos podem aproveitar para passar despercebidos

Os atores de ameaças entendem de nuvem e continuam a refinar suas táticas para explorar as vulnerabilidades e abusar dos serviços em nuvem. Aqui estão as três principais técnicas de ataque em nuvem observadas pela equipe CrowdStrike Intelligence em 2022 ao rastrear mais de 200 atores de ameaças.

Movimento lateral pela infraestrutura de TI

Os atores de ameaças estão cada vez mais aproveitando os endpoints tradicionais para passar para a infraestrutura em nuvem — e vice-versa: a infraestrutura em nuvem está sendo usada como um gateway para acessar os endpoints. As organizações raramente têm a visibilidade necessária para interromper esta atividade, já que adquirem várias soluções pontuais diferentes para lidar com o ambiente local e, mais recentemente, para lidar também com ambientes de nuvem.

Para interromper o movimento lateral, as organizações precisam ter visibilidade total de toda a infraestrutura de TI, tanto local quanto em nuvem.

Configurações incorretas da nuvem levam a ataques

A CrowdStrike investiga constantemente violações em nuvem que poderiam ter sido detectadas anteriormente ou evitadas se a segurança tivesse sido configurada corretamente. Erros de configuração não apenas aumentam o risco de ataque, mas também se tornam mais prevalentes e problemáticos à medida que as organizações expandem sua infraestrutura de nuvem.

Nº 1 vulnerabilidade em ambientes de nuvem

60% dos containers observados pela CrowdStrike não têm proteções de segurança devidamente configuradas

36% dos ambientes de nuvem tinham uma configuração padrão insegura do provedor de serviços de nuvem

Identidades na nuvem sendo o novo perímetro

Como o novo perímetro, as identidades se tornaram as chaves do reino. Os atores de ameaças estão focando menos na desativação de tecnologias antivírus e de firewall e mais na modificação de processos de autenticação e no ataque a identidades. A adoção contínua de aplicações e serviços baseados em nuvem aumenta o número de identidades que um adversário pode atacar e usar a seu favor.

Contas de usuários legítimos foram usadas para obter acesso inicial em **43%** das intrusões na nuvem

47% das configurações incorretas mais críticas na nuvem **estavam relacionadas à falta de higiene de identidade e de autorizações**

Em **67%** dos incidentes de segurança na nuvem, **a CrowdStrike encontrou perfis de gerenciamento de identidade e acesso com privilégios elevados além do necessário — indicando que um adversário pode ter subvertido esse perfil para comprometer o ambiente e se mover lateralmente**

CrowdStrike para Cloud Security

À medida que os ambientes de nuvem continuam a crescer, também aumentarão os ataques contra eles. É impossível detectar cada erro de usuário, configuração incorreta e vulnerabilidade na nuvem — e muito menos compreender todas as táticas, ferramentas e procedimentos em constante evolução usados pelos atores de ameaças. As organizações não conseguem fazer isso sozinhas, elas precisam de um parceiro que conheça profundamente o comportamento dos atores de ameaças e a nuvem.

Como o provedor nº 1 de detecção e resposta de endpoint baseada em agente do mundo, a CrowdStrike adotou uma abordagem visionária para projetar uma segurança em nuvem escalável e eficaz que pode ser implementada e gerenciada facilmente em uma única plataforma. A CrowdStrike Falcon® Cloud Security foi construída desde o início para oferecer proteção sem agente e baseada em agente. As organizações podem simplesmente ativá-la e estender a proteção de seus endpoints para sua nuvem, cobrindo toda a sua infraestrutura de TI com uma proteção contínua e unificada. Falcon Cloud Security reúne gerenciamento de postura de segurança, proteção de workload e gerenciamento de direitos de identidade em nuvem em uma solução CNAPP totalmente integrada.

Baixe o white paper: Guia do especialista para proteção na nuvem. Saiba mais →

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.

Nos siga:

CROWDSTRIKE

[1] https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023