

# Relatório de Riscos em Nuvem 2023:

Conheça os adversários e as táticas mirando na nuvem

**95%**

de aumento nas explorações em nuvem

**3X**

em aumento nos casos envolvendo atores de ameaças conscientes da nuvem

## Os adversários estão aprimorando as técnicas, táticas e procedimentos (TTPs) em nuvem

Vários grupos adversários, incluindo **COZY BEAR** (Rússia-nexus), **SCATTERED SPIDER** (e-crime), **LABYRINTH CHOLLIMA** (DPRK-nexus) e **COSMIC WOLF** (Turquia-nexus) estão ficando mais sofisticados e determinados a atacar a nuvem.

### COZY BEAR



- País de origem: Federação Russa
- Táticas: usa ferramentas maliciosas para modificar serviços em nuvem

Saiba mais sobre esse adversário prolífico e como ele afeta o cenário global da nuvem.



### SCATTERED SPIDER



- País de origem: Desconhecido
- Táticas: implementa ransomware a partir de um ambiente de teste em nuvem

Conheça esse adversário do e-crime e como ele tem como alvo os ambientes de nuvem.



### LABYRINTH CHOLLIMA



- País de origem: Coreia do Norte
- Táticas: usa recursos da nuvem para entregar documentos com macros maliciosas

Descubra como esse adversário perigoso está causando danos em todo o cenário da nuvem.



### COSMIC WOLF



- País de origem: Turquia
- Táticas: Tem como alvo os dados da vítima armazenados em ambientes de nuvem

Saiba como esse adversário de intrusão direcionada opera na nuvem.



## A identidade é o principal ponto de acesso à nuvem

Os atores de ameaças estão buscando novas maneiras de utilizar as identidades na nuvem

**43%**

Os adversários estão ficando mais dependentes de obter acesso válida, que foram usadas para obter acesso inicial em **43%** das invasões de nuvem observadas.\*

**67%**

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

**47%**

**Quase metade (47%)** das configurações incorretas críticas na nuvem estavam relacionadas à falta de higiene de identidade e de autorizações.\*

## Erro humano gera riscos na nuvem

As configurações incorretas da nuvem são lacunas, erros ou vulnerabilidades que expõem um ambiente de nuvem a riscos. Isso pode ocorrer quando as configurações de segurança são mal escolhidas ou nem estão implementadas. Ambientes multinuvem podem ser complexos e pode ser difícil saber se permissões excessivas de conta são concedidas, o acesso público impróprio é configurado ou outros erros são cometidos.

**28%**

dos workloads são executados como root ou permitem a escalabilidade para root\*

**24%**

dos workloads têm capacidades semelhantes ao root\*



**60%**

dos workloads não têm proteções de segurança devidamente configuradas\*

**26%**

dos workloads têm o token de conta do Kubernetes Service montado automaticamente\*

Saiba mais sobre as ameaças ao seu ambiente de nuvem.



Saiba mais: <https://www.crowdstrike.com.br/>  
 Nos siga: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)  
 Comece uma avaliação gratuita hoje: <https://www.crowdstrike.com/free-trial-guide/>

#### 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: Protection that powers you.

© 2023 CrowdStrike, Inc. Todos os direitos reservados.

\*Fonte: dados de segurança em nuvem observados durante um período de avaliação de 24 horas