CROWDSTRIKE

Cloud Risk Report 2023:

Descubre quiénes atacan la nube y qué tácticas emplean

95 %
Incremento de ataques a la nube

3X
Se triplican los casos de ciberataques relacionados con la nube

Los ciberdelincuentes perfeccionan las TTP para la nube

Algunos grupos de ciberdelincuentes, **COZY BEAR** (ligado a Rusia), **SCATTERED SPIDER** (de origen desconocido), **LABYRINTH CHOLLIMA** (ligado a la RPDC) y **COSMIC WOLF** (ligado a Turquía), son cada vez más sofisticados y priorizan sus ataques a la nube.

COZY BEAR

- **País de origen:** Federación de Rusia
- **Tácticas:** uso de herramientas maliciosas para modificar los servicios en la nube

Infórmate sobre este prolífico grupo de ciberdelincuentes y descubre su impacto en el panorama de la nube a nivel mundial.

Más información

SCATTERED SPIDER

- **País de origen:** desconocido
- **Tácticas:** despliega ransomware desde un entorno de ensayo en la nube

Conoce a este ciberdelincuente y descubre cómo ataca los entornos en la nube.

Más información

LABYRINTH CHOLLIMA

- **País de origen:** Corea del Norte
- **Tácticas:** empleo de recursos en la nube para distribuir documentos con macros maliciosas

Descubre cómo este peligroso grupo de ciberdelincuentes está causando daños en todo el panorama de la nube.

Más información

COSMIC WOLF

- **País de origen:** Turquía
- **Tácticas:** su objetivo son datos de las víctimas almacenados en entornos en la nube

Descubre cómo actúa este ciberdelincuente en sus intrusiones selectivas en la nube.

Más información

La identidad es un punto de acceso clave a la nube.

Los ciberdelincuentes buscan nuevas formas de sacar partido de las identidades en la nube.

43 %
Los atacantes utilizan cada vez más cuentas válidas para conseguir acceso inicial. Su uso representa el **43 %** de las intrusiones en la nube observadas.*

67 %
En el **67 %** de los incidentes de seguridad en la nube CrowdStrike descubrió roles de administración de identidades y acceso que tenían privilegios superiores a los que se necesitaban. Esto indica que un atacante puede haber alterado el rol para comprometer el entorno y moverse lateralmente.*

47 %
Casi la mitad (47 %) de los errores graves de configuración de la nube se debieron a una higiene insuficiente de las identidades y los derechos.*

Los errores humanos aumentan el riesgo en la nube

Los errores de configuración de la nube son lagunas, fallos o vulnerabilidades que exponen a riesgos un entorno en la nube. Esto ocurre cuando los ajustes de seguridad no se eligen bien o simplemente no se implementan. Los entornos multinube pueden ser complejos y es posible que no sea fácil determinar si se han concedido demasiados permisos para las cuentas o un acceso público inadecuado, o si se ha cometido cualquier otro error.

60 %
de las cargas de trabajo carecen de medidas de seguridad configuradas correctamente*

28 %
de las cargas de trabajo se ejecutan como root o permiten que se eleven los privilegios a nivel root*

26 %
de las cargas de trabajo tienen tokens de cuenta de servicio de Kubernetes que se montan automáticamente*

24 %
de las cargas de trabajo tienen privilegios de nivel root*

Infórmate sobre las amenazas contra tu entorno en la nube.

Descarga ya el informe
Cloud Risk Report 2023 de CrowdStrike

Más información: https://www.crowdstrike.com/
Síguenos: Blog | Twitter | LinkedIn | Facebook | Instagram
Empieza una prueba gratuita hoy mismo: https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa para la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los ciberdelincuentes y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: la protección para triunfar.

*Fuente: Datos de seguridad de la nube observados a lo largo de un período de evaluación de 24 horas