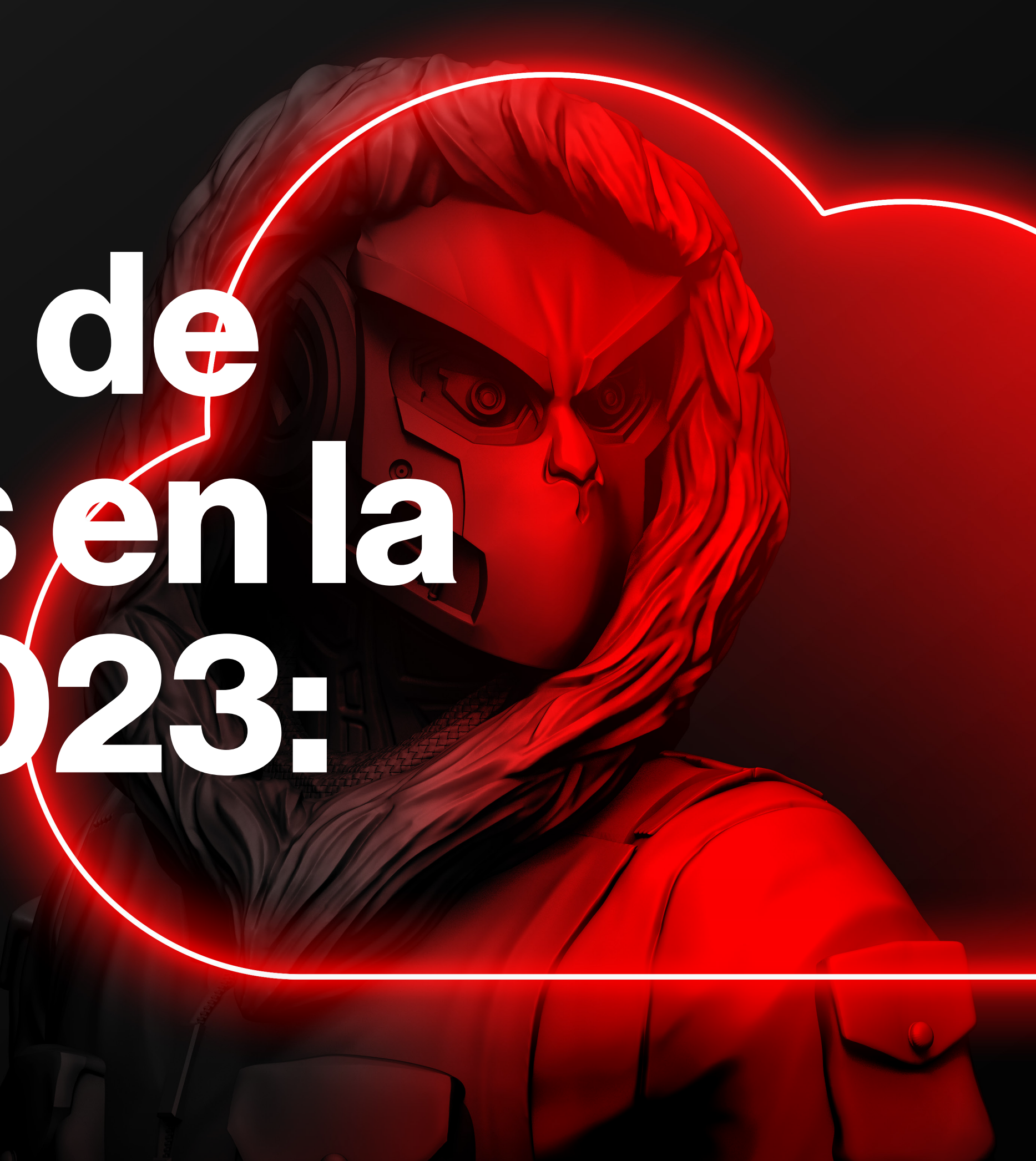
CROWDSTRIKE



Informe de Riesgos en la Nube 2023:

Informate Sobre los Adversarios y las TTPs que Apuntan a la Nube

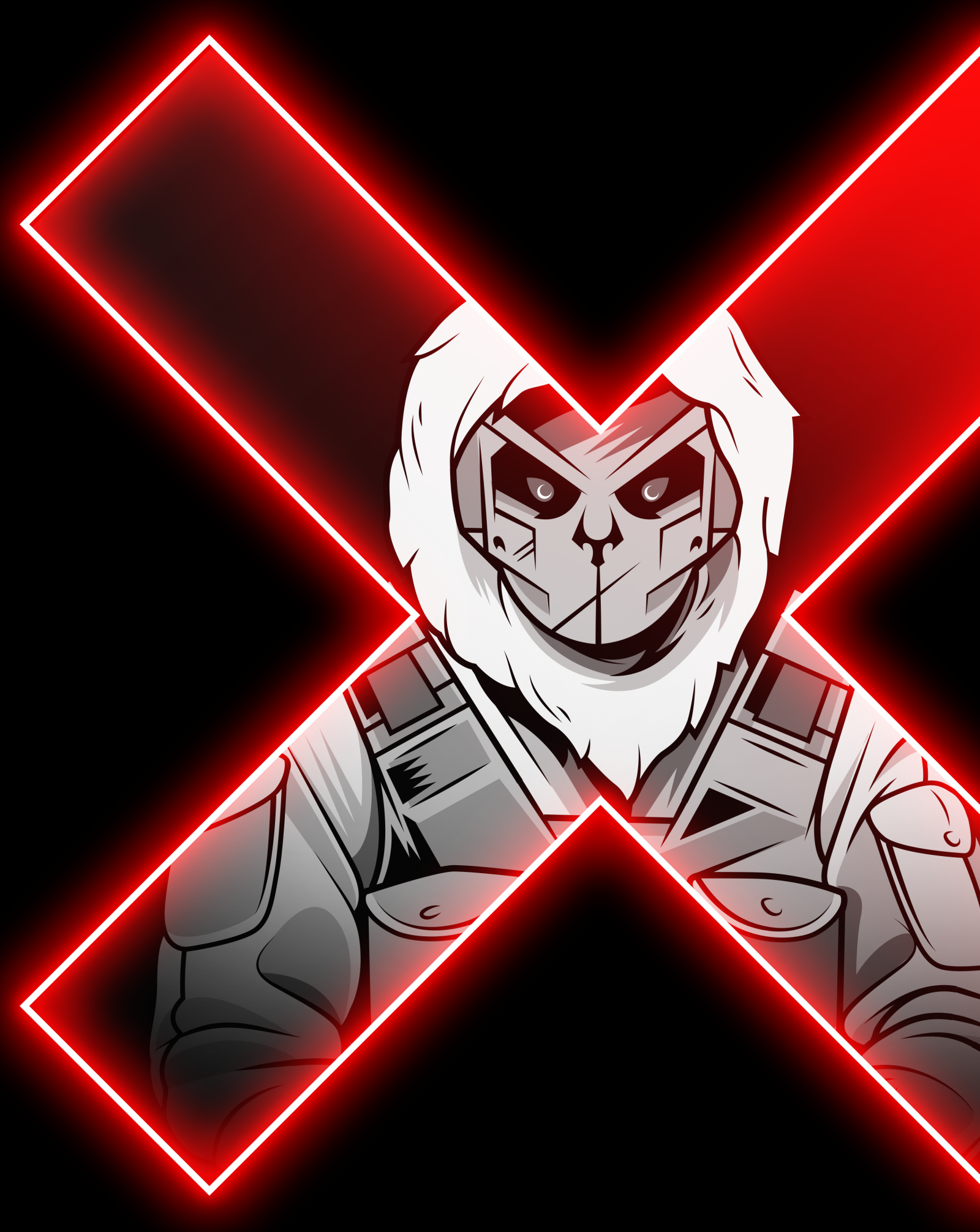
95%
Aumento en la Explotación de la Nube

3X
Aumento de Casos que Involucran a Actores de Amenazas Conscientes de la Nube

Los Adversarios Están Perfeccionando las TTPs de la Nube

Varios grupos de adversarios, incluyendo **Cozy Bear** (Russia-Nexus), **Scattered Spider** (Crimen electrónico), **Labyrinth Chollima** (DPRK-nexus) y **Cosmic Wolf** (Turkey-Nexus) se están haciendo más sofisticados y decididos a apuntar a la nube.

COZY BEAR

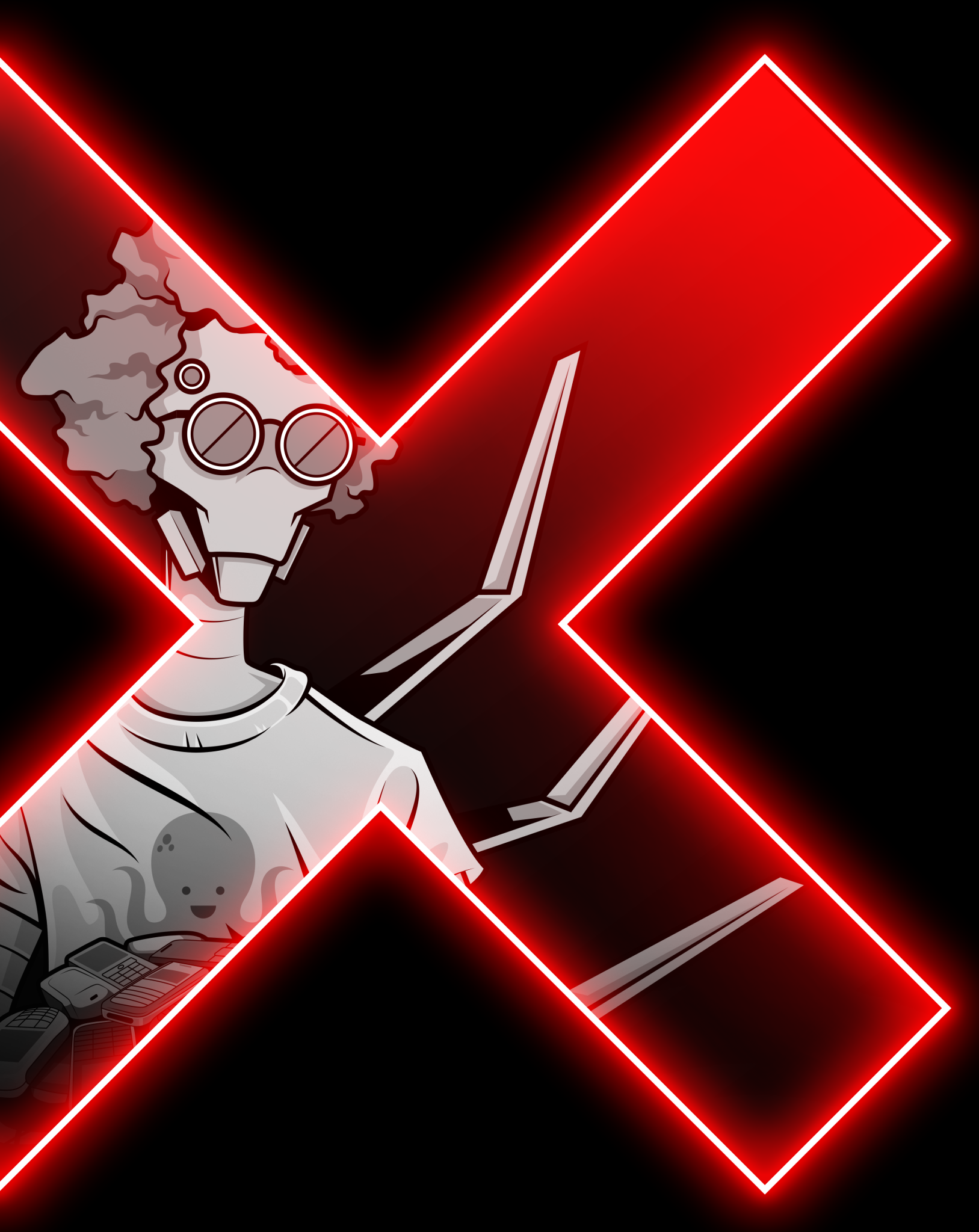


- **País de origen:** Federación Rusa
- **TTPs:** Utiliza herramientas maliciosas para modificar los servicios en la nube

Obtén más información sobre este prolífico adversario y cómo afectan el panorama global de la nube.

Más información

SCATTERED SPIDER

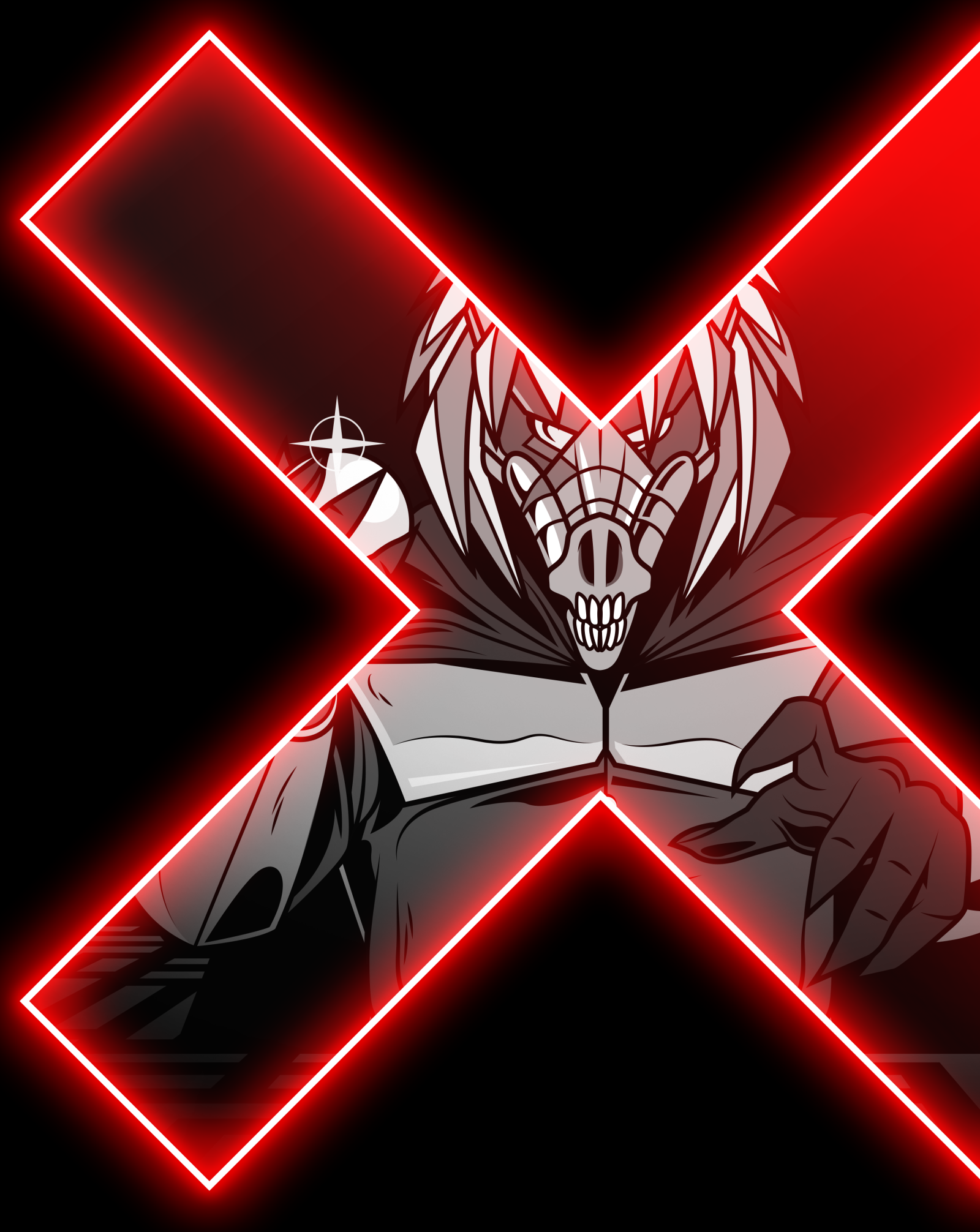


- **País de origen:** Desconocido
- **TTPs:** Despliega ransomware desde un entorno de almacenamiento en la nube

Conoce a este adversario de Crimen electrónico y cómo se dirige a los entornos de la nube.

Más información

LABYRINTH CHOLLIMA

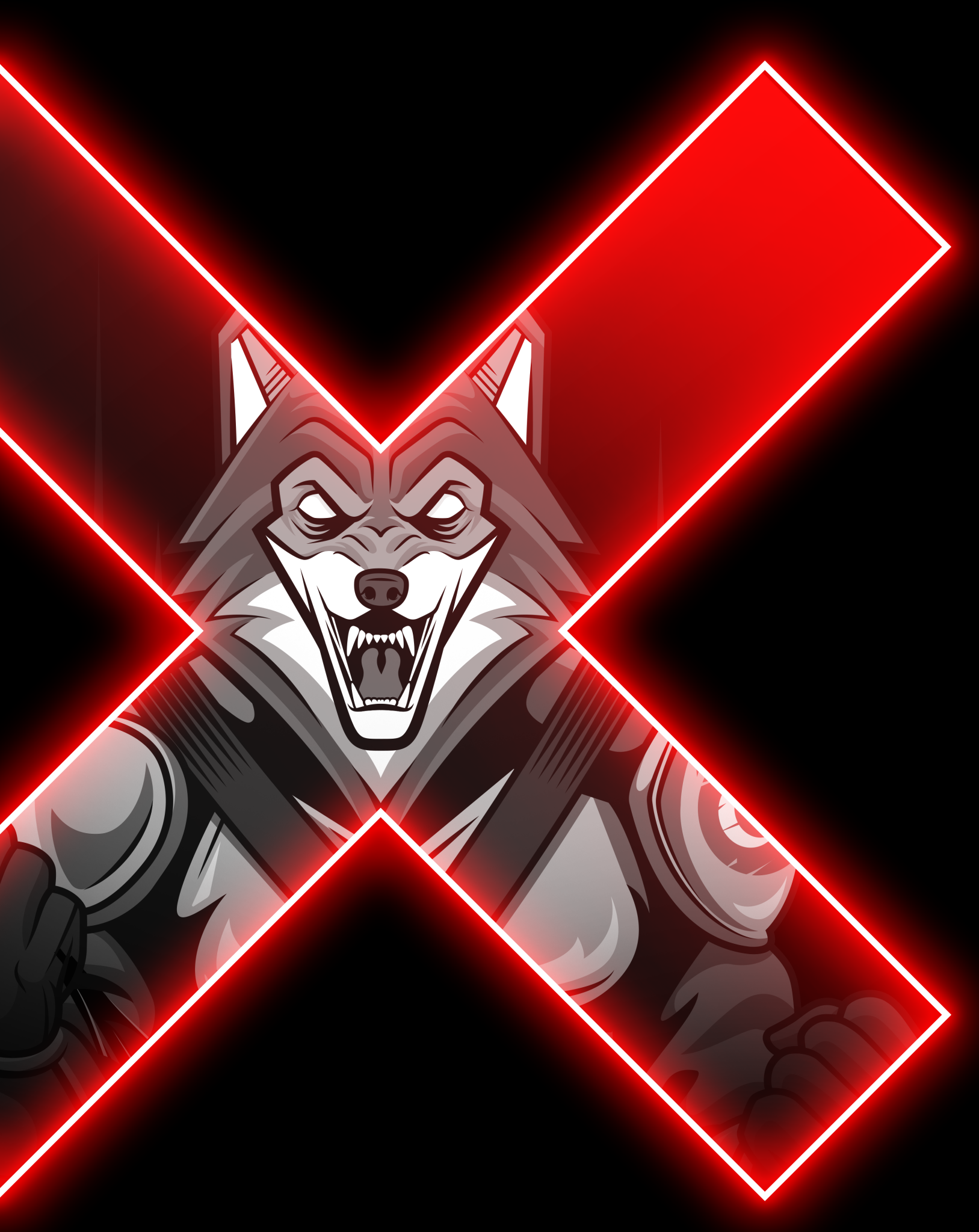


- **País de origen:** Corea del Norte
- **TTPs:** Usa recursos en la nube para entregar documentos con macros maliciosas

Descubre cómo este peligroso adversario está causando daño a través del entorno de la nube.

Más información

COSMIC WOLF



- **País de origen:** Turquía
- **TTPs:** Se dirige a los datos de víctimas almacenados en entornos de la nube

Aprende cómo opera este adversario de intrusión selectiva en la nube.

Más información

La Identidad es un Punto Clave de Acceso a la Nube

Los actores de amenazas buscan nuevas formas de aprovechar las identidades en la nube

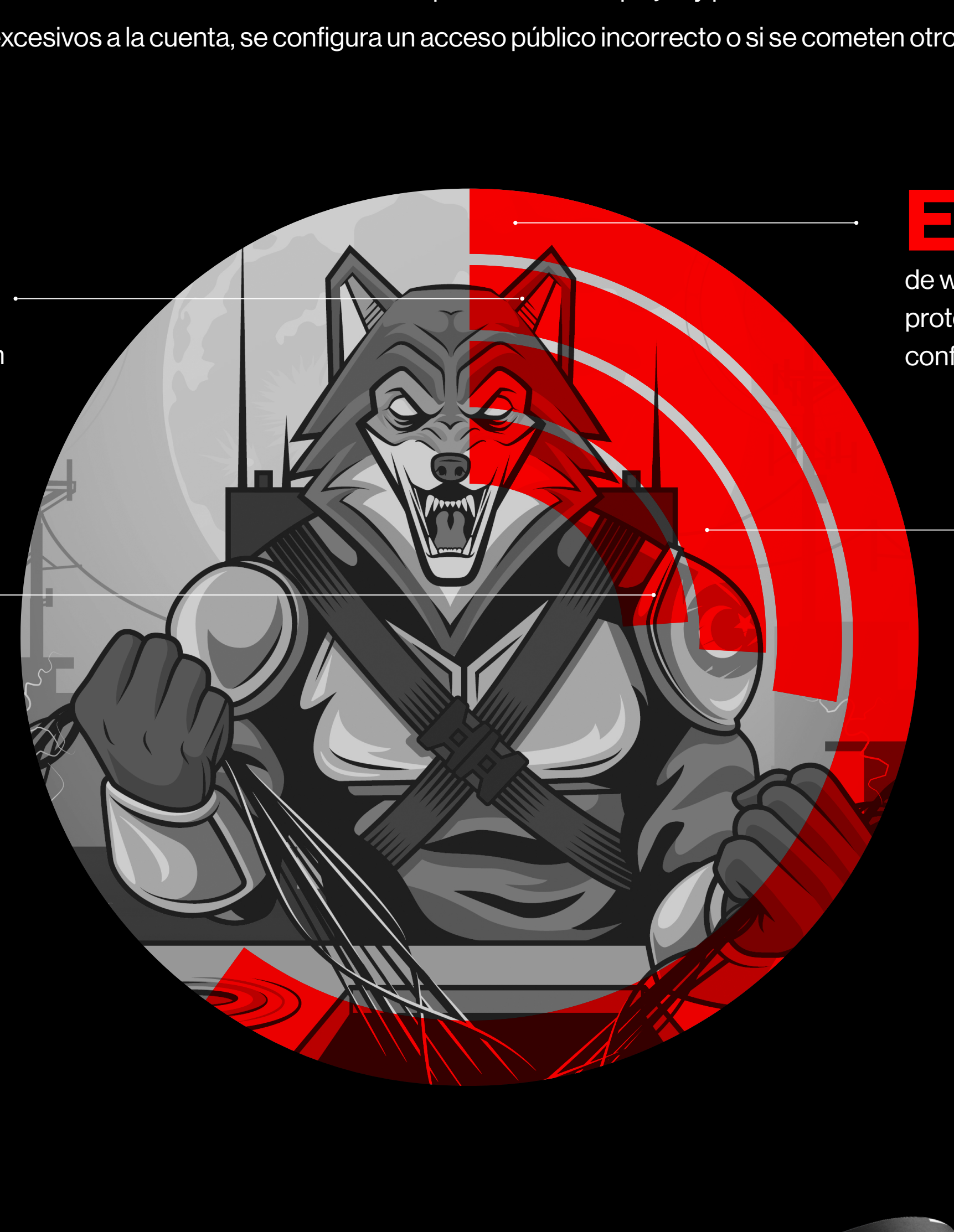
43%
Los adversarios son cada vez más dependientes de cuentas válidas, que se utilizaron para obtener acceso inicial en el **43%** de las intrusiones observadas en la nube.*

67%
En el **67%** de los incidentes de seguridad en la nube, CrowdStrike encontró roles de gestión de identidad y acceso con privilegios elevados más allá de lo requerido—lo que indica que un adversario puede haber subvertido el rol para afectar el entorno y moverse lateralmente.*

47%
Casi la mitad (47%) de los errores de configuración críticos en la nube estaban relacionadas con una deficiente higiene de identidad y asignación de permisos.*

El Error Humano Impulsa el Riesgo en la Nube

Las configuraciones erróneas en la nube son brechas, errores o vulnerabilidades que exponen el entorno de la nube a riesgos. Estos puede ocurrir cuando las configuraciones de seguridad son elegidas deficientemente o no se implementan en absoluto. Los entornos multinube pueden ser complejos y puede ser difícil saber si se otorgan permisos excesivos a la cuenta, se configura un acceso público incorrecto o si se cometen otros errores.



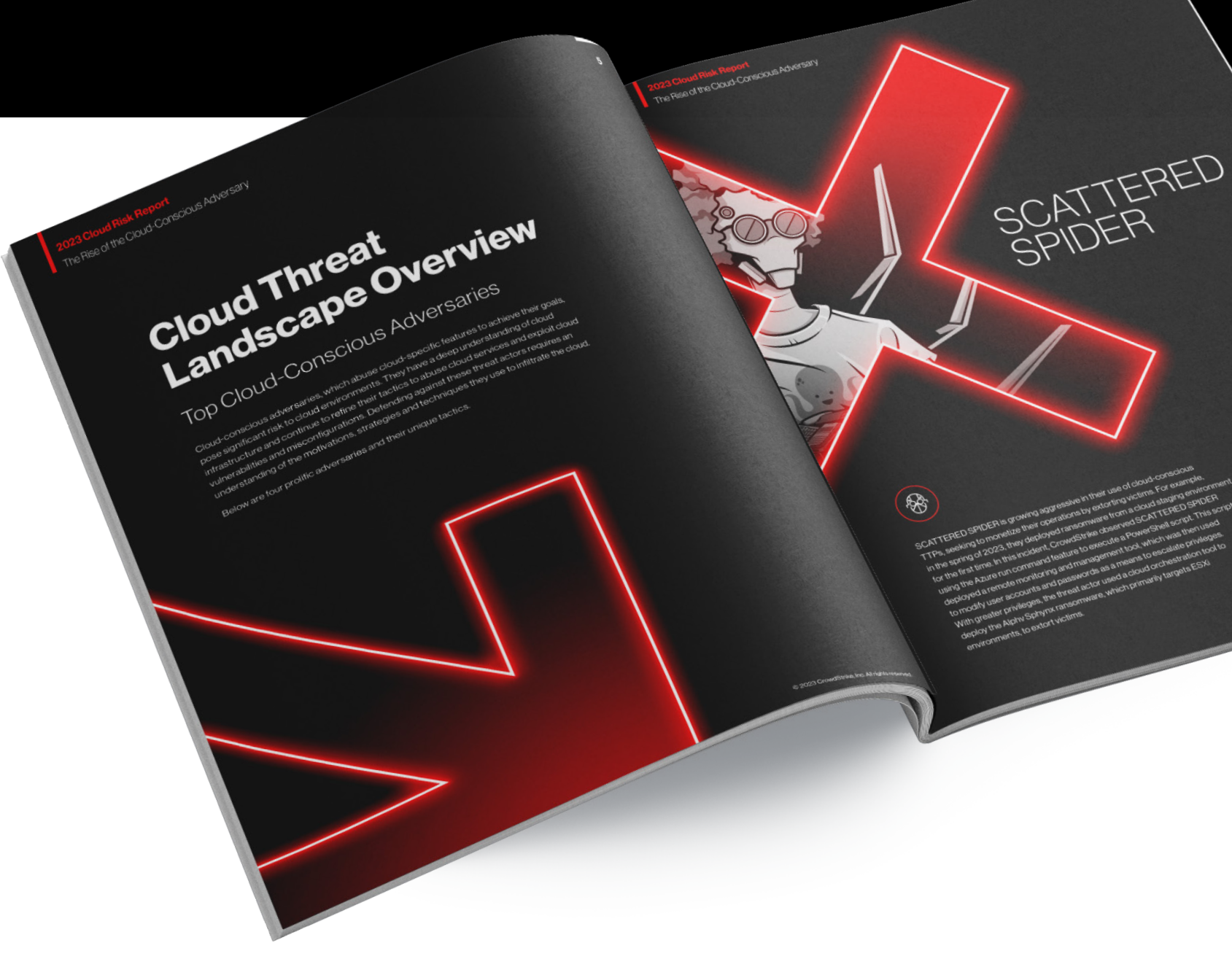
El 28%
de workloads se ejecutan como origen o permiten escalar al origen *

El 24%
de workloads tienen capacidades de origen similares *

El 60%
de workloads carecen de protecciones de seguridad configuradas correctamente *

El 26%
de workloads tienen la Cuenta de Servicio de Token Kubernetes automontada *

Obtén más información sobre las amenazas a tu entorno de la nube.



Descarga el Informe de Riesgos en la Nube - CrowdStrike 2023

Más información: https://www.crowdstrike.com/es/
Seguinos: Blog | Twitter | LinkedIn | Facebook | Instagram
Comenzá una prueba gratis hoy: https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), es un líder global en ciberseguridad que ha redefinido la seguridad moderna con una de las plataformas nativas para la nube más avanzadas del mundo para proteger áreas críticas de riesgo corporativo — endpoints y workloads de nube, identidad y datos.

Impulsada por CrowdStrike Security Cloud™ y una Inteligencia Artificial de clase mundial, la plataforma CrowdStrike Falcon® aprovecha indicadores de ataque en tiempo real, inteligencia sobre amenazas, el tradecraft cambiante de los adversarios y telemetría enriquecida de toda la empresa para ofrecer detecciones hiper precisas, protección y remediación automatizadas, cacería de amenazas de élite y observabilidad priorizada de vulnerabilidades.

Construida para ese fin en la nube con una arquitectura única y liviana de agente, la plataforma Falcon entrega implantación rápida y escalable, protección y desempeño superiores, complejidad reducida y un tiempo de amortización inmediato.

CrowdStrike: Protección que te empodera.

---

* Fuente: Se observaron datos de seguridad en la nube durante un período de evaluación de 24 horas