CROWDSTRIKE

Principales técnicas de ataque a la nube

Y cómo defenderse de ellas

La nube es una superficie de ataque que está siempre creciendo y desarrollándose. Defender este ambiente contra ataques cada vez más frecuentes a la nube requiere un profundo conocimiento de las actividades de los actores de amenazas. Aquí están las tres principales tendencias de ataque en la nube, según lo observado por CrowdStrike, y cómo defenderse de ellos.

Los actores de amenazas están apuntando cada vez más a la nube

Los entornos de nube siguen creciendo:

41,4% de los líderes de nube dicen que están aumentando el uso de servicios y productos basados en la nube[1]

33,4% están planeando migrar de softwares corporativos tradicionales a herramientas basadas en la nube[1]

32,8% están migrando workloads situados on-premises a la nube[1]

Y los actores de amenazas lo han percibido.

En 2022, CrowdStrike observó:

95% de aumento en casos de explotación en la nube

3x el número de casos involucrando actores conscientes de la nube

71% de los ataques fue sin malware

¿Por qué apuntar a entornos en la nube?

Los entornos multinube son complejos y, por lo tanto, más difíciles de proteger

Los rápidos procesos de entrega de software hacen que las aplicaciones nativas para la nube sean susceptibles a vulnerabilidades y configuraciones erróneas

Los entornos de nubes desfavorables y clandestinos carecen de controles de seguridad y supervisión

Los productos de puntos de seguridad que quedan aislados dejan puntos ciegos en que los adversarios pueden pasar desapercibidos

Los actores de amenazas son conocedores de la nube y refinan sus tácticas para abusar de los servicios en la nube y explotar las vulnerabilidades de la nube. Estas son las tres técnicas principales de ataque a la nube observadas por el equipo de Inteligencia sobre Amenazas de CrowdStrike durante el último año mientras rastreaba a más de 200 actores de amenazas.

Movimiento lateral a través de la infraestructura de TI

Los actores de amenazas aprovechan cada vez más los endpoints tradicionales para migrar a la infraestructura de la nube, y viceversa: la infraestructura de la nube está siendo utilizada como puerta de entrada para acceder a los endpoints. Las organizaciones rara vez tienen la visibilidad que necesitan para detener esta actividad, ya que han adquirido múltiples soluciones específicas para abordar el entorno on-premise y, más recientemente, los entornos en la nube.

Para detener el movimiento lateral, las organizaciones necesitan visibilidad completa en toda la infraestructura de TI, tanto a nivel local como en la nube.

Errores de configuración en la nube que conducen a brechas

CrowdStrike investiga consistentemente brechas en la nube que podrían haber sido detectadas antes o prevenidas si los parámetros de seguridad en la nube hubieran sido correctamente configurados. Los errores de configuración no solo aumentan el riesgo de una brecha, sino que son más frecuentes y problemáticos a medida que las organizaciones expanden su infraestructura en la nube.

N.º 1 vulnerabilidad en entornos de nube

60% de los contenedores que CrowdStrike observó carecían de protecciones de seguridad correctamente configuradas

36% de los entornos en la nube tenían configuraciones predeterminadas inseguras del proveedor de servicios en la nube

Identidades en la nube como el nuevo perímetro

Como nuevo perímetro, las identidades se han convertido en las llaves del reino. Los actores de amenazas se centran menos en desactivar las tecnologías antivirus y de firewall y más en modificar los procesos de autenticación y atacar identidades. La adopción continua de aplicaciones y servicios basados en la nube aumenta el número de identidades al que un adversario puede apuntar y utilizar para su beneficio.

Cuentas de usuario legítimas fueron usadas para conseguir acceso inicial en **43%** de las intrusiones en la nube

47% de los errores de configuración críticos en la nube **están relacionados con una higiene deficiente de identidad y asignación de permisos**

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.**

CrowdStrike para seguridad en la nube

A medida que los entornos en la nube continúan creciendo, también lo harán los ataques contra ellos. Es imposible capturar cada vulnerabilidad, configuración errónea y error de usuario en la nube,—qué decir de comprender todas las tácticas, herramientas y procedimientos en evolución de los actores de amenazas. Las organizaciones no pueden hacerlo solas, necesitan un socio que sea profundo conocedor de la nube y del comportamiento de los actores de amenazas.

Como la proveedora N.º 1 en el mundo en detección y respuesta de endpoints basada en agentes, CrowdStrike ha emprendido un abordaje visionario para diseñar una seguridad en la nube que sea escalable y efectiva y pueda ser implementada y gestionada de manera fácil en una única plataforma. CrowdStrike Falcon® Cloud Security fue construida de cero para entregar protección tanto basada en agentes como sin agentes. Las organizaciones pueden simplemente activarla y ampliar la protección a partir de sus endpoints hasta la nube, cubriendo toda la infraestructura de TI con una protección unificada. Falcon Cloud Security reúne la gestión de la postura de seguridad en la nube, la protección del workload de la nube y una gestión de derechos de identidad en la nube como una oferta de plataforma de protección de aplicación nativa para la nube (CNAPP) completamente integrada.

Descarga el white paper: Guía del Insider para Defender la Nube. Más información

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.

Impulsado 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, caceria 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 valor inmediato.

CrowdStrike: Detenemos las brechas.

Síganos:

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

CROWDSTRIKE