CROWDSTRIKE

NO HAY DÓNDE ESCONDERSE

Informe sobre Threat Hunting de Falcon OverWatch de 2022

Todos los años, Falcon OverWatch™, el equipo proactivo de Threat Hunting 24/7 de CrowdStrike, publica su análisis técnico con sus conclusiones, en el que describe las técnicas de ataque más novedosas y destacables, así como las nuevas tendencias de intrusión que el equipo descubrió durante los 12 meses anteriores, en este caso desde el 1 de julio de 2021 hasta el 30 de junio de 2022. Este último año en particular, OverWatch observó sorprendentes variaciones en cómo diseñan y despliegan los ciberdelincuentes sus ataques.

Se intensifican las intrusiones, aumenta la complejidad

2022

71 %
de las amenazas detectadas por OverWatch no utilizaban malware

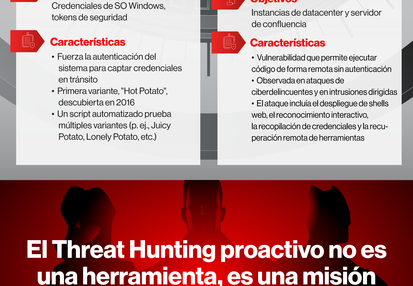
50 %
de aumento interanual en intrusiones hands-on-keyboard

1 h 24 min
de tiempo medio de propagación

Las motivaciones de los agresores dictan la estrategia de ataque

5 sectores principales por tipo de intrusión

Ciberdelincuencia vs Intrusiones dirigidas



Ciberdelincuencia = Ataques con motivaciones económicas
Intrusiones dirigidas = Ataques vinculados a Estados

Técnicas novedosas y destacables

IceApple

Fines
Elusión de las defensas, acceso con credenciales, filtración

Objetivos
Servidores IIS

Características
- Sofisticado marco basado en .NET para actuar después del ataque
- Los exploits cargan deliberadamente ensamblados .NET
- Huella forense reducida, residente en memoria

fscan

Fines
Descubrimiento

Objetivos
Host interno, mapa del entorno

Características
- Herramienta de ataque habitual a finales de 2021 y principios de 2022
- Análisis de vulnerabilidades reformulado para el registro avanzado de huellas digitales
- Vulneración mediante modificación de clave pública, comandos SSH

Sweet Potato

Fines
Escalada de privilegios

Objetivos
Credenciales de SO Windows, tokens de seguridad

Características
- Fuerza la autenticación del sistema para captar credenciales en tránsito
- Primera variante, "Hot Potato", descubierta en 2016
- Un script automatizado prueba múltiples variantes (p. ej., Juicy Potato, Lonely Potato, etc.)

Vulnerabilidad de día cero en servidor web

Fines
Persistencia (mediante shell web), reconocimiento interactivo, recopilación de credenciales, filtración

Objetivos
Instancias de datacenter y servidor de confluencia

Características
- Vulnerabilidad que permite ejecutar código de forma remota sin autenticación
- Observada en ataques de ciberdelincuentes y en intrusiones dirigidas
- El ataque incluía el despliegue de shells web, el reconocimiento interactivo, la recopilación de credenciales y la recuperación remota de herramientas

El Threat Hunting proactivo no es una herramienta, es una misión

Conoce sus técnicas. Conoce a tu adversario.
Busca sin tregua.

Informe sobre Threat Hunting de Falcon OverWatch de 2022

Descargar el informe completo

Más información: https://www.crowdstrike.com/services/

Síguenos:

CROWDSTRIKE

We Stop Breaches