CROWDSTRIKE

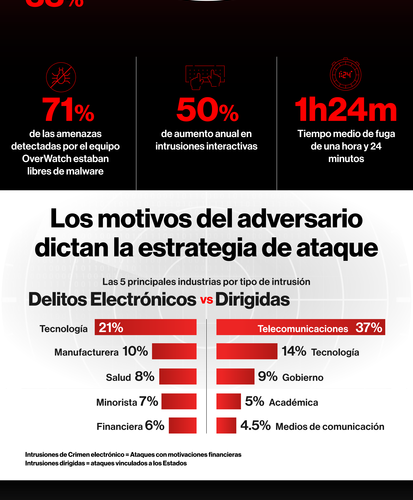
# NO HAY DONDE ESCONDERSE

**Informe de Investigación de Amenazas de Falcon OverWatch de 2022.**

Cada año, Falcon OverWatch™, el equipo proactivo de investigación de amenazas 24x7 de CrowdStrike, publica sus hallazgos y análisis técnicos que detallan las novedosas y destacadas estrategias de los adversarios y las tendencias de intrusión emergentes que el equipo encontró en los 12 meses anteriores, en esta edición, del 1 de julio de 2021 hasta el 30 de junio, 2022. En particular, el año pasado, OverWatch observó cambios sorprendentes en la forma en que los atacantes diseñan e implementan sus ataques.

## Las intrusiones se intensifican, la complejidad aumenta

### 2022




**71%**
de las amenazas detectadas por el equipo OverWatch estaban libres de malware

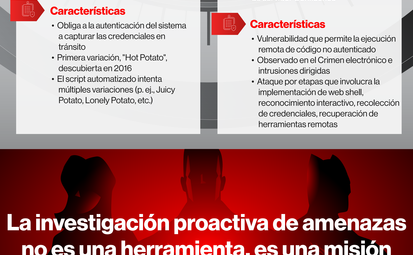
**50%**
de aumento anual en intrusiones interactivas

**1h24m**
Tiempo medio de fuga de una hora y 24 minutos

## Los motivos del adversario dictan la estrategia de ataque

Las 5 principales industrias por tipo de intrusión

### Delitos Electrónicos vs Dirigidas




**Intrusiones de Crimen electrónico = Ataques con motivaciones financieras**
**Intrusiones dirigidas = ataques vinculados a los Estados**

## Estrategia novedosa y notable

### IceApple

**Objetivos**
Evasión de defensa, acceso a credenciales, exfiltración

**Blancos**
Servidores IIS

**Características**
- Framework de post-explotación sofisticado basado en .NET
- Explota assemblies .NET cargados reflexivamente
- Huella forense reducida, residiendo en la memoria

### fscan

**Objetivos**
Descubrimiento

**Blancos**
Host interno, mapeo del entorno

**Características**
- Herramienta adversaria muy utilizada a fines de 2021/principios de 2022
- Escáner de vulnerabilidades avanzado adaptado para huellas dactilares
- Explotación a través de modificación de clave pública, comandos SSH

### Sweet Potato

**Objetivos**
Aumento de privilegios

**Blancos**
Credenciales del sistema operativo Windows, Tokens de seguridad

**Características**
- Obliga a la autenticación del sistema a capturar las credenciales en tránsito
- Primera variación, "Hot Potato", descubierta en 2016
- El script automatizado intenta múltiples variaciones (p. ej., Juicy Potato, Lonely Potato, etc.)

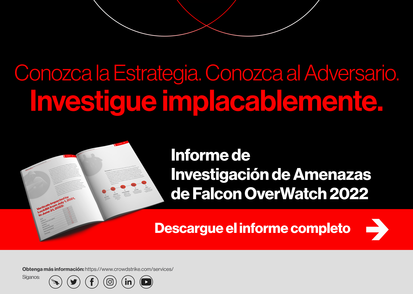
### Servidor Web Zero-Day

**Objetivos**
Persistencia (a través de Web Shell), Reconocimiento interactivo, Recolección de credenciales, Exfiltración

**Blancos**
Instancias de centro de datos y de servidor Confluence

**Características**
- Vulnerabilidad que permite la ejecución remota de código no autenticado
- Observado en el Crimen electrónico e intrusiones dirigidas
- Ataque por etapas que involucra la implementación de web shell, reconocimiento interactivo, recolección de credenciales, recuperación de herramientas remotas

## La investigación proactiva de amenazas no es una herramienta, es una misión




## Conozca la Estrategia. Conozca al Adversario. Investigue implacablemente.

**Informe de Investigación de Amenazas de Falcon OverWatch 2022**

**Descargue el informe completo**

**Obtenga más información:** https://www.crowdstrike.com/services/

Síganos



CROWDSTRIKE

Detenemos las brechas