CROWDSTRIKE

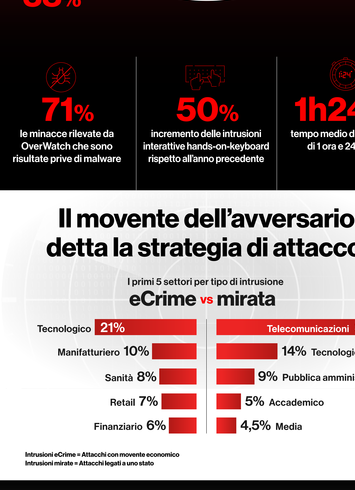
NESSUN POSTO DOVE NASCONDERSI

Report sul threat hunting di Falcon OverWatch 2022

Ogni anno, il team proattivo di threat hunting 24/7 di CrowdStrike, Falcon OverWatch™, pubblica i risultati e l'analisi tecnica che illustrano le nuove e prevalenti abilità operative degli avversari e le tendenze emergenti in materia di intrusioni che il team ha scoperto durante il precedente periodo di 12 mesi, dal 1° luglio 2021 al 30 giugno 2022. Nell'ultimo anno, in particolare, OverWatch ha osservato cambiamenti sorprendenti nel modo in cui gli attaccanti progettano e distribuiscono i loro attacchi.

Intensificazione delle intrusioni, escalation della complessità Avversario

2022



71%
le minacce rilevate da OverWatch che sono risultate prive di malware

50%
incremento delle intrusioni interattive hands-on-keyboard rispetto all'anno precedente

1h24m
tempo medio di diffusione di 1 ora e 24 minuti

Il movente dell'avversario detta la strategia di attacco

I primi 5 settori per tipo di intrusione

eCrime vs **mirata**

Intrusioni eCrime = Attacchi con movente economico
Intrusioni mirate = Attacchi legati a uno stato

Abilità operativa nuova e rilevante

IceApple

Objectives
Defense Evasion, Credential Access, Exfiltration

Targets
IIS Servers

Characteristics
- Sophisticated .NET-based post-exploitation framework
- Exploits reflectively loaded .NET assemblies
- Low forensic footprint, residing in-memory

fscan

Obiettivi
Rilevazione

Target
Host interno, mappatura dell'ambiente

Caratteristiche
- Strumento avversario di tendenza alla fine/inizio del 2021/2022
- Scanner di vulnerabilità riutilizzato per identificazione avanzata
- Sfruttamento tramite modifica della chiave pubblica e comandi SSH

Sweet Potato

Obiettivi
Privilege escalation

Target
Credenziali del sistema operativo Windows, token di sicurezza

Caratteristiche
- Forza l'autenticazione del sistema per acquisire le credenziali in transito
- Prima variante, "Hot Potato", rilevata nel 2016
- Lo script automatico tenta più varianti (ad es. Juicy Potato, Lonely Potato ecc.)

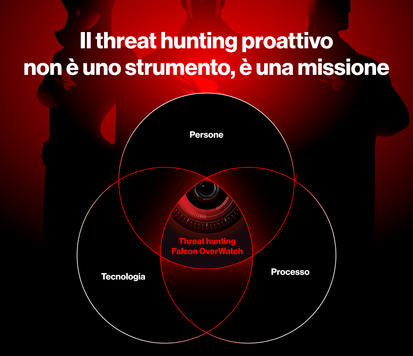
Web Server Zero-Day

Obiettivi
Persistenza (tramite web shell), ricognizione interattiva, raccolta di credenziali, esfiltrazione

Target
Server di confluenza e istanze di data center

Caratteristiche
- Vulnerabilità che consente l'esecuzione di codice remoto non autenticato
- Osservato in eCrime e intrusioni mirate
- L'attacco in più fasi prevedeva distribuzione di web shell, ricognizione interattiva, raccolta di credenziali e recupero di strumenti remoti

Il threat hunting proattivo non è uno strumento, è una missione



Conosci la sua abilità operativa. Conosci l'avversario. **Caccia senza tregua.**

Report sul threat hunting di Falcon OverWatch 2022

Scarica il report completo

Ulteriori informazioni: https://www.crowdstrike.com/services/
Seguici

CROWDSTRIKE

We Stop Breaches