CROWDSTRIKE

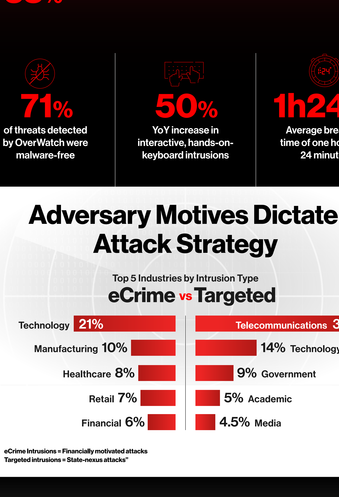
NOWHERE TO HIDE

2022 Falcon OverWatch Threat Hunting Report

Every year, CrowdStrike's proactive 24/7 threat hunting team, Falcon OverWatch™, publishes its findings and technical analysis detailing the novel and prominent adversary tradecraft and emerging intrusion trends the team unearthed during the preceding 12-month period from July 1, 2021 through June 30, 2022. This past year in particular, OverWatch observed striking shifts in how attackers design and deploy their attacks.

Intrusions Intensify, Complexity Escalates

2022



71%
of threats detected by OverWatch were malware-free

50%
YoY increase in interactive, hands-on-keyboard intrusions

1h24m
Average breakout time of one hour and 24 minutes

Adversary Motives Dictate Attack Strategy

Top 5 Industries by Intrusion Type

eCrime vs Targeted

eCrime		Targeted	
Technology	21%	Telecommunications	37%
Manufacturing	10%	Technology	14%
Healthcare	8%	Government	9%
Retail	7%	Academic	5%
Financial	6%	Media	4.5%

eCrime Intrusions = Financially motivated attacks
Targeted intrusions = State-nexus attacks*

Novel and Notable Tradecraft

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

Objectives
Discovery

Targets
Internal Host, Environment Mapping

Characteristics
- Trending adversary tool in late/early 2021/2022
- Vulnerability scanner repurposed for advanced fingerprinting
- Exploitation via public key modification, SSH commands

Sweet Potato

Objectives
Privilege Escalation

Targets
Windows OS Credentials, Security Tokens

Characteristics
- Forces system authentication to capture credentials in transit
- First variation, "Hot Potato," discovered in 2016
- Automated script attempts multiple variations (e.g., Juicy Potato, Lonely Potato, etc.)

Web Server Zero-Day

Objectives
Persistence (via Web Shell), Interactive Reconnaissance, Credential Harvesting, Exfiltration

Targets
Confluence Server and Data Center Instances

Characteristics
- Vulnerability enabling unauthenticated remote code execution
- Observed in eCrime and targeted intrusions
- Staged attack involved web shell deployment, interactive recon, credential harvesting, remote tooling retrieval

Proactive Threat Hunting Isn't a Tool, It's a Mission

Know the Tradecraft. Know the Adversary. Hunt Relentlessly.

2022 Falcon OverWatch Threat Hunting Report

Download the full report

Learn more: https://www.crowdstrike.com/services/
Follow us:

CROWDSTRIKE

We Stop Breaches