CROWDSTRIKE

NOWHERE TO HIDE

You don't have a malware problem, you have an adversary problem.

It is critical that security teams know how threat actors operate to be best positioned to stop them.

The CrowdStrike 2023 Threat Hunting Report, developed by CrowdStrike's Counter Adversary Operations team, exposes the latest adversary tradecraft and provides knowledge and insights to help stop breaches.

Jaw-Dropping New Insights

IDENTITY THREATS HAVE BECOME MAINSTREAM

Adversaries are doubling down on identity-based intrusions, with the theft and abuse of compromised identities becoming even more impactful.

62%
of interactive intrusions involved compromised identities

583%
increase in Kerberoasting, a growing identity-based attack technique

ECRIME IS SURGING AS ADVERSARIES BECOME FASTER

Adversaries are breaking in and out of environments faster than ever.

79 MINUTES
was the average eCrime breakout time observed

7 MINUTES
was the fastest eCrime breakout time observed

ADVERSARIES ARE GETTING SMARTER IN THE CLOUD

Threat actors are becoming cloud experts, exploiting common misconfigurations and abusing built-in cloud management tooling.

160%
increase in credential theft via cloud instance metadata APIs

CROSS-PLATFORM PROFICIENCY TAKES CENTER STAGE

Proficiency across operating systems is a hallmark of interactive intrusions in 2023.

3X INCREASE
in adversaries replacing pluggable authentication modules (PAMs) with malicious modules in Linux

FINANCIAL, TECHNOLOGY AND SERVICE
sectors were most impacted

Discover the adversaries targeting you

CROWDSTRIKE IS ACTIVELY TRACKING THESE ADVERSARIES, ALONG WITH OVER 200 OTHERS. LEARN MORE ABOUT THEM IN THE 2023 THREAT HUNTING REPORT.

LABYRINTH CHOLLIMA
Led the charge in multiple operating system attacks

VICE SPIDER
Responsible for 27% of all Kerberoasting attacks

INDRIK SPIDER
Shifted from opportunistic eCrime to tailored attacks

Know them. **Find** them. **Stop** them.

- Gain unparalleled insights from our expert threat hunters as they discuss standout intrusions and techniques.
- Equip yourself with real-world experiences to fortify your security strategy and outmaneuver fast-moving threats.
- Stay ahead of adversaries by understanding both global and regional trends.

GET THE REPORT

CROWDSTRIKE