2023 Global Threat Report
Understanding the current Threat Landscape

Philip Scheidl
Sales Engineer

CROWDSTRIKE

2023 GLOBAL THREAT REPORT

Agenda

- Threat landscape
- 2022 themes
- 5 steps to be prepared

CROWDSTRIKE

CROWDSTRIKE

2023 GLOBAL THREAT REPORT

Threat Landscape

- Breakout time – Every second counts
- Access broker boom
- Adversaries move beyond malware
- Interactive intrusions

CROWDSTRIKE

eCRIME BREAKOUT TIME

84'

Every Second Counts

Minimize cost and damage

To contain the threat, protectors must respond within the breakout time

Adversaries are getting faster

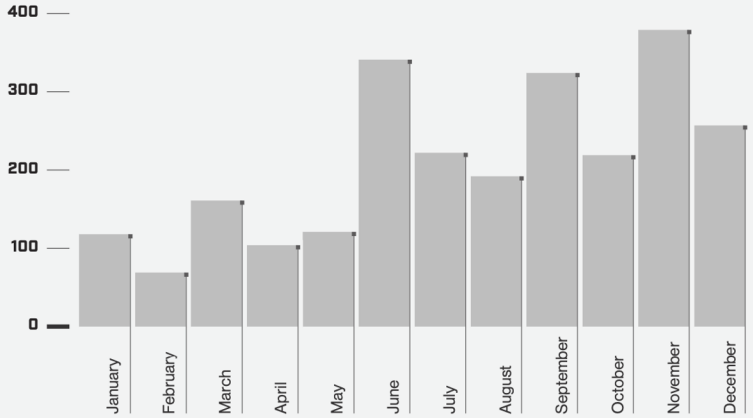
Breakout time declined from 98 minutes in 2021 to 84 minutes in 2022

Beat the 1-10-60 rule

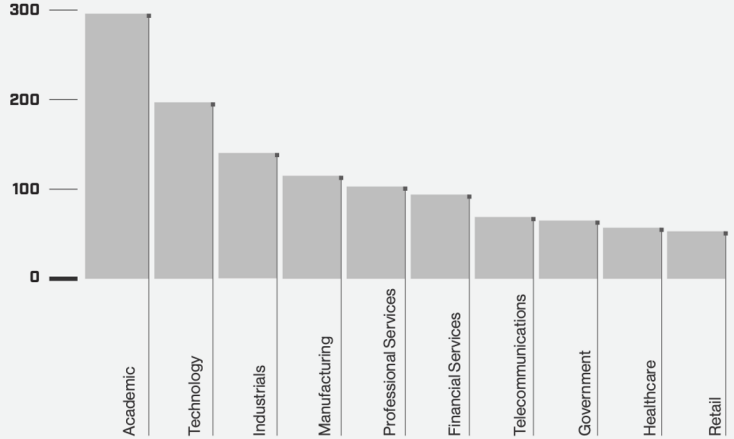
Detect in one minute, investigate in 10 and respond in 60

CROWDSTRIKE

ACCESS BROKER ADVERTISEMENTS BY MONTH, 2022



TOP 10 SECTORS ADVERTISED BY ACCESS BROKERS, 2022



Access Broker Boom

Acceleration of demand

Popularity of services increasing with more than 2,500 advertisements – a 112% increase from 2021

Buy a la carte or in bulk

Several brokers will sell in bulk as others will use a “one-access, one-auction” technique.

Access methods remain consistent

Abuse of compromised credentials obtained by information stealers or purchased in log shops on the dark web

> “80% of all breaches use compromised identities and 50% of organizations have experienced an Active Directory (AD) attack in the last two years.”

CROWDSTRIKE

Adversaries Continued to Move Beyond Malware to Gain Initial Access and Persistence

There was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This was partly related to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another contributing factor was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits.

ADVERSARY TACTICS — Malware-Free

71%	**2022**
62%	2021
51%	2020
40%	2019
39%	2018

50%

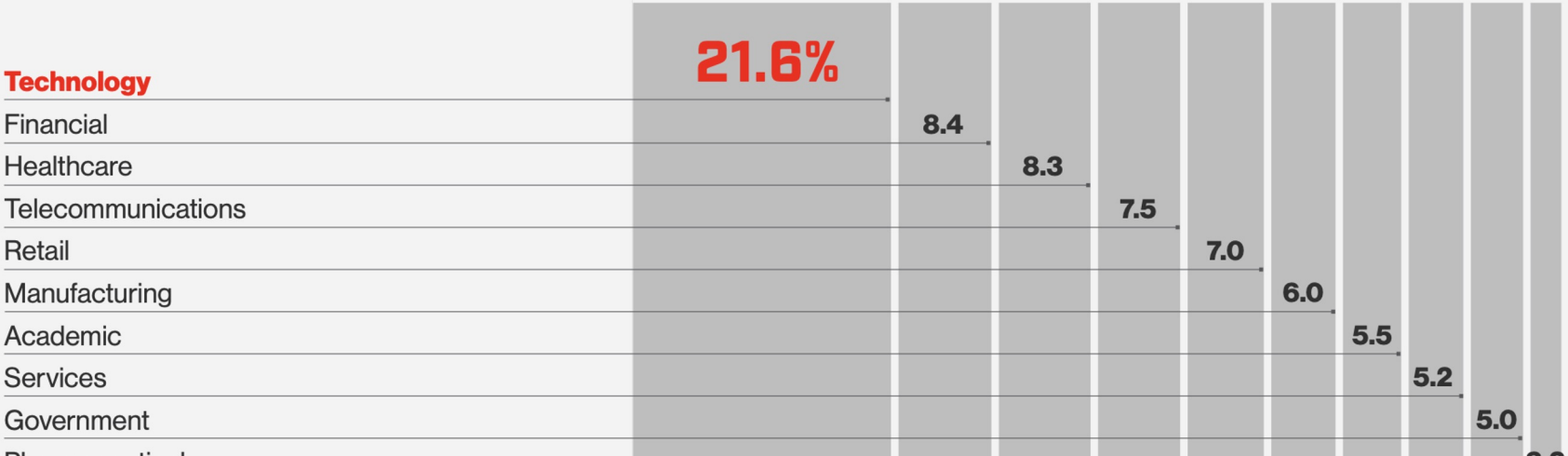
increase in interactive intrusion campaigns

Interactive Intrusions Gained Speed and Momentum

Compared to 2021, CrowdStrike observed a 50% increase in the number of interactive intrusion campaigns with accelerating activity into the fourth quarter.

In addition, the technology sector was the most frequently targeted vertical in which Falcon OverWatch uncovered interactive intrusion activity in 2022. This reflects an increase compared with the relative frequency of intrusions in the top 10 industry verticals from the prior 12 months.

TOP 10 VERTICALS BY INTRUSION FREQUENCY



CROWDSTRIKE

2023 GLOBAL THREAT REPORT

2022 Themes

- eCrime actors gained notoriety for high-profile attacks
- The continued rise of cloud exploitation
- Discovery, rediscovery and circumvention:
  The 2022 vulnerability intelligence landscape
- High-effort, limited return:
  Russian cyber operations are supporting the War in Ukraine
- Dominating the espionage landscape:
  China-nexus adversaries significantly increased 2022 operational scale

CROWDSTRIKE

eCrime Actors Gained Notoriety for High-Profile attacks

Rise in "double-extortion" model

20% increase in the number of adversaries conducting data theft and extortion without deploying ransomware

SLIPPY SPIDER

Targeted technology giants with data theft and extortion

SCATTERED SPIDER

Used social engineering to overcome multi-factor authentication

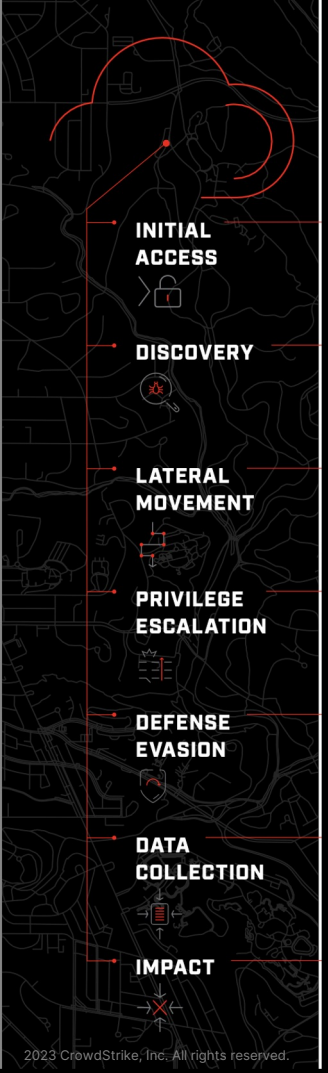
CROWDSTRIKE INTELLIGENCE BEGAN TRACKING

33

NEW ADVERSARIES, RAISING THE TOTAL NUMBER OF ACTORS TRACKED TO

200+

CROWDSTRIKE



The Continued Rise Of Cloud Exploitation

Increasing exploitation

Observed cloud exploitation cases grew by 95%; cases involving cloud-conscious actors nearly tripled from 2021

Cloud-conscious TTPs

Expanding TTP repertoire includes cloud account discovery, public facing apps for initial access, use of higher-privileged accounts for escalation

Suspected PANDA becoming cloud-conscious

Adversaries growing more confident leveraging traditional endpoints to pivot to cloud – and vice-versa

"CrowdStrike Intelligence saw actors shift away from the deactivation of antivirus and firewall technologies, as well as from log-tampering efforts. Instead, they were observed seeking ways to modify authentication processes and attack identities."

"Stopping cloud breaches requires the combination of agentless capabilities that protect against misconfigurations and control plane attacks with agent-based runtime security that protects cloud workloads."

CROWDSTRIKE

DISCOVERY, REDISCOVERY AND CIRCUMVENTION

The 2022 Vulnerability Intelligence Landscape

Vulnerability discovery and rediscovery

Adversaries modify – or even reapply – the same exploit to target similarly vulnerable products.

Circumvention of earlier patches

Zero-day and N-day vulnerabilities observed in 2022 demonstrated adversaries' ability to leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components

Microsoft's crisis of trust

MSFT has issued more than 1200 patches in 2022, including 28 zero days

> "Patch management is not set and forget - adversary sophistication requires prioritization of critical patches and defense in depth that can immediately identify adversary activity."

CROWDSTRIKE

High Effort, Limited Return

Russian Cyber Operations Supporting The War In Ukraine

Attacks against core sectors such as energy, telecommunications, transportation and media have not been as extensive as predicted, likely indicating the Kremlin expected a swift and decisive victory over Ukraine and planned to use these functioning resources to keep Ukraine running under a new regime.

"Stopping breaches requires an understanding of the adversary, including their motivations, techniques and how they're going to target your organization."

CROWDSTRIKE

DOMINATING THE ESPIONAGE LANDSCAPE

China-nexus adversaries significantly increased 2022 operational scale

Exploits to gain initial access

China-Nexus Adversaries continued shifting toward exploitation of web-facing services

Increase in use of zero-day exploits

Enterprise software continued to be a high-priority target. Additional zero-day exploits include weaponized MSFT Office documents.

Target Taiwan

Adversaries growing more confident leveraging traditional endpoints to pivot to cloud – and vice-versa

Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-nexus adversaries used zero-day exploits to compromise entities in the aerospace, legal and academic sectors.

"China-nexus adversaries were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks."

CROWDSTRIKE

5 Steps To Be Prepared

1. Gain visibility into your security gaps
2. Prioritize identity protection
3. Prioritize cloud protection
4. Know your adversary
5. Practice makes perfect


Questions?