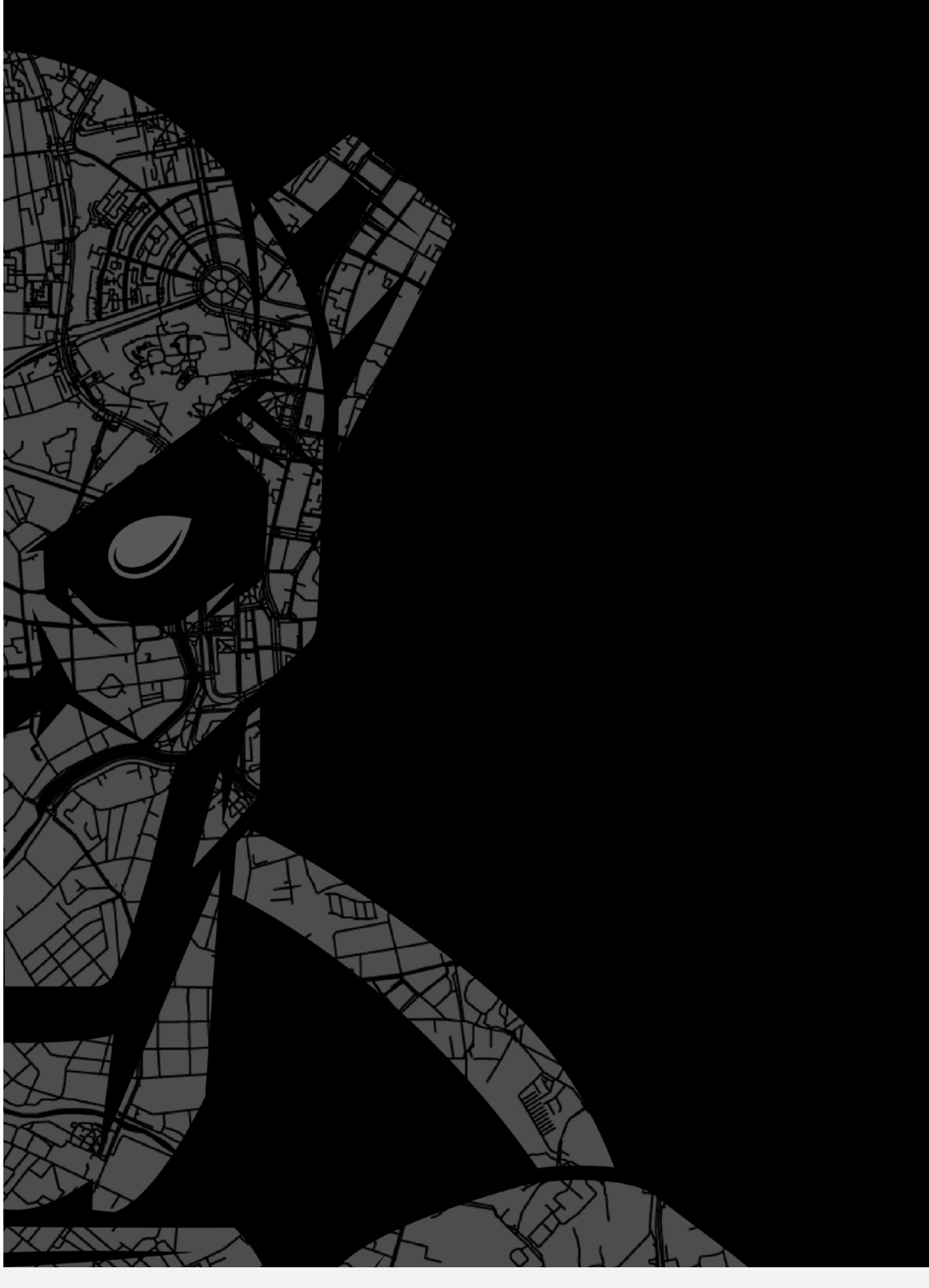


2023 GLOBAL THREAT REPORT

Relentless Adversaries Increase Speed and Sophistication in 2022:
What You Need to Know

The CrowdStrike 2023 Global Threat Report,
one of the industry's most trusted and comprehensive analyses of today's cybersecurity threat landscape and evolving adversary tradecraft, explores the most significant trends of 2022 and the adversaries behind them.

MEET YOUR ADVERSARIES

eCRIME | STATE-SPONSORED | HACKTIVISTS

33 newly named adversaries introduced in 2022

200+ tracked adversaries

WHERE THEY'RE ACTIVE

- Technology
- Financial Services
- Healthcare
- Telecommunications
- Manufacturing
- Academia
- Government

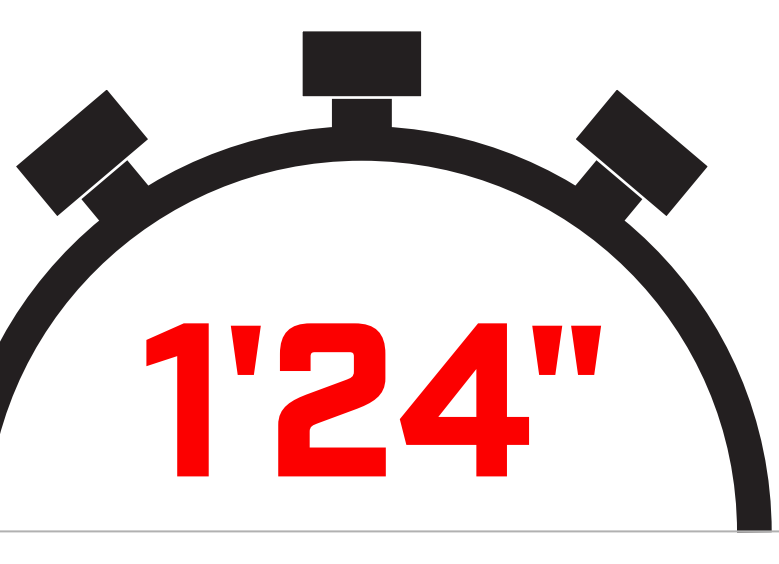
HOW THEY OPERATE

The threat landscape continued to evolve in 2022, with adversary operations making it increasingly difficult for organizations to protect themselves.

98' → **84'**

BREAKOUT TIME REMAINS UNDER 2 HOURS

eCrime adversaries need an average of 1 hour and 24 minutes to move laterally – a decrease of 14 minutes from 2021.



71% OF ATTACKS WERE MALWARE-FREE

Adversaries continue to move beyond malware and employ "hands-on-keyboard" techniques, a trend partly related to their prolific abuse of valid credentials to enable access and persistence, as well as their ability to quickly operationalize vulnerability exploits.

50% JUMP IN INTERACTIVE INTRUSION CAMPAIGNS

CrowdStrike observed a significant increase in interactive intrusions, with activity ramping up into the fourth quarter of 2022.

ACCESS BROKER ADS ACCELERATED WITH A 112% INCREASE

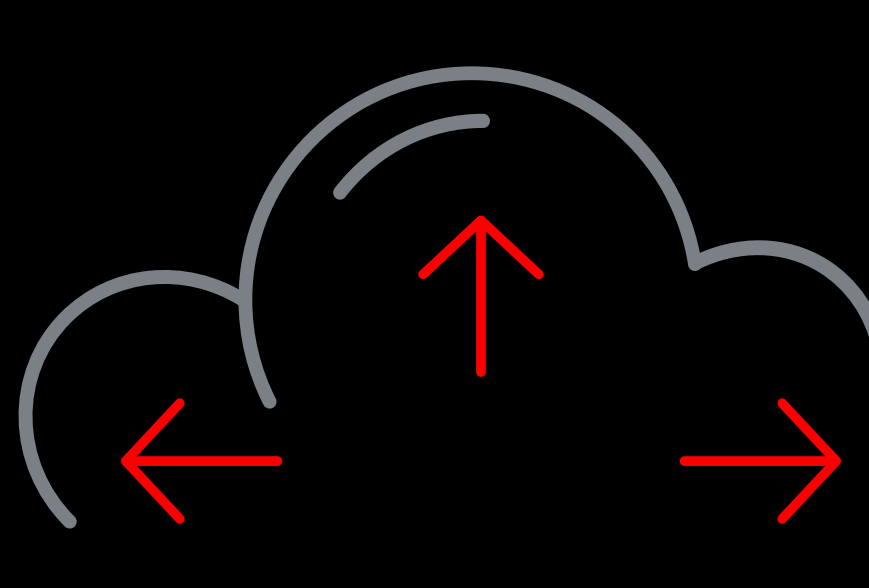
The popularity of access broker services increased in 2022 with more than 2,500 advertisements for access identified, a sharp increase compared to 2021 – underscoring the growing demand for access broker services.

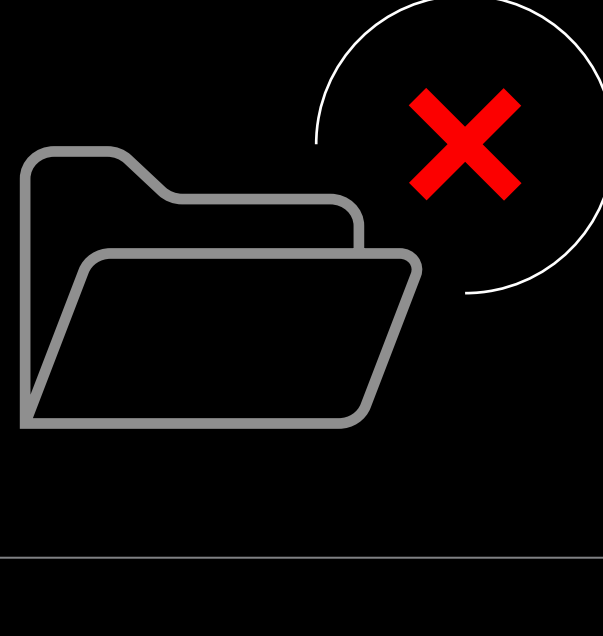
WHAT THEY'RE AFTER

Adversaries were relentless in targeting victims' data and infrastructure in 2022.

CLOUD EXPLOITATION INCIDENTS GREW BY 95%

Over the course of 2022, cases involving cloud-conscious threat actors nearly tripled from 2021, signifying a larger trend of eCrime and nation-state actors adopting knowledge and techniques to target cloud environments.



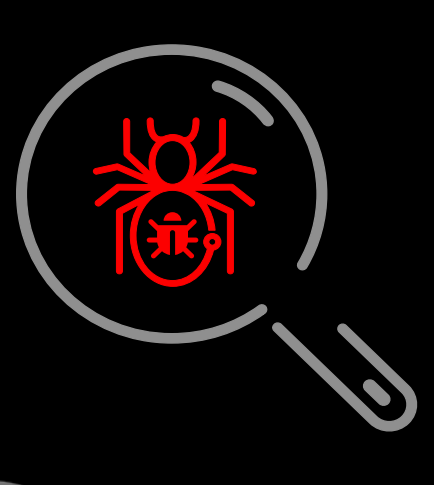


DATA THEFT AND EXTORTION CAMPAIGNS CONTINUED — WITHOUT RANSOMWARE

CrowdStrike Intelligence observed a 20% increase in the number of adversaries conducting data theft and extortion without deploying ransomware. This "double extortion" model is the most common tactic among big game hunting (BGH) adversaries.

VULNERABILITY REUSE PUT EXPOSED COMPONENTS AT RISK

Zero-day and N-day vulnerabilities observed in 2022 demonstrate adversaries' ability to use their specialized knowledge to bypass mitigations from earlier patches and target the same vulnerable components multiple times.



CHINA-NEXUS ADVERSARIES WERE THE MOST ACTIVE TARGETED INTRUSION GROUPS

China-nexus adversaries – and actors using tactics, techniques and procedures (TTPs) consistent with them – were seen in 2022 targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks.

RUSSIA-NEXUS ADVERSARIES CONTINUED MILITARY, PSYCHOLOGICAL AND HACKTIVIST ATTACKS AGAINST UKRAINE

Throughout 2022, unprecedented use of cyber capabilities was observed, aiming to gather intelligence, destroy infrastructure, or sow division and influence public sentiment spilling into Europe.

WHAT'S NEXT?

Everything and anything. To be prepared, you need to:

- > Know your adversaries
- > Prioritize identity and cloud protection
- > Patch vulnerable components
- > Practice how you fight:
  Be ready when every second counts

Download the full report

Understanding their game is the only way to beat them.

About CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches**.

Learn more: **https://www.crowdstrike.com/**

Follow us:

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

CROWDSTRIKE
Protection that powers you