CROWDSTRIKE

2023 GLOBAL THREAT REPORT

FROM RELENTLESS ADVERSARIES TO RESILIENT BUSINESSES

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The annual CrowdStrike Global Threat Report is among the cybersecurity industry's most trusted and comprehensive research on the modern threat landscape and evolving adversary tradecraft. In its pages, we explore the most significant security events and trends of the previous year, as well as the adversaries driving this activity.

CrowdStrike's 2023 Global Threat Report delves into the recent past of adversary activity so you can better prepare for future attacks. By studying the details of these events, you gain visibility into the shifting dynamics of adversary tactics: what they're after, who they're targeting and how they operate.

This year's report was developed based on the firsthand observations of our elite CrowdStrike® Intelligence and CrowdStrike® Falcon OverWatch™ teams, combined with insights from the vast telemetry of the CrowdStrike Security Cloud. It provides crucial information on what security teams need to know — and do — in an increasingly ominous threat landscape.

THREAT LANDSCAPE OVERVIEW

ADVERSARY TACTICS

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

Malware-Free

- **Breakout time decreased:** The Falcon OverWatch Team calculates the average breakout time — the period it takes for an adversary to move laterally from a compromised host to another within the victim environment — was 84 minutes for eCrime intrusion activity during 2022.
- **Access broker services grew more popular:** More than 2,500 advertisements for access broker services, which provide or sell illicitly acquired access to organizations, were identified in 2022. This marks a 112% increase from 2021. An especially popular tactic involved the abuse of compromised credentials acquired via information stealers or purchased on the criminal underground.
- **Malware-free attacks spiked:** Malware-free activity accounted for 71% of all detections in 2022, up from 62% in 2021. This underscores a continued shift away from the use of malware and a greater reliance on credential abuse and vulnerability exploitation among adversaries.
- **Hands-on-keyboard activity increased:** The number of interactive intrusions increased 50% in 2022 with accelerating activity into the fourth quarter.

KEY FINDINGS

eCrime Actors Gained Notoriety for High-Profile Attacks

Adversaries are operating with relentless determination, launching more sophisticated and more frequent attacks across a broad range of targets.

- Throughout 2022, CrowdStrike Intelligence observed two newly named adversaries — SLIPPY SPIDER and SCATTERED SPIDER — pushing operational limits by targeting high-profile victims and impacting associated employees, customers and partners.
- In their 2022 activity, SLIPPY SPIDER attracted significant attention for high-profile data theft and extortion incidents targeting technology companies. SCATTERED SPIDER leveraged social engineering to overcome multifactor authentication (MFA). Both of these adversaries have successfully used a range of techniques including MFA fatigue, vishing and SIM swapping.
- CrowdStrike Intelligence observed a 20% increase in the number of adversaries conducting data theft and extortion campaigns, without deploying ransomware, in 2022.

The Rise of Cloud Exploitation

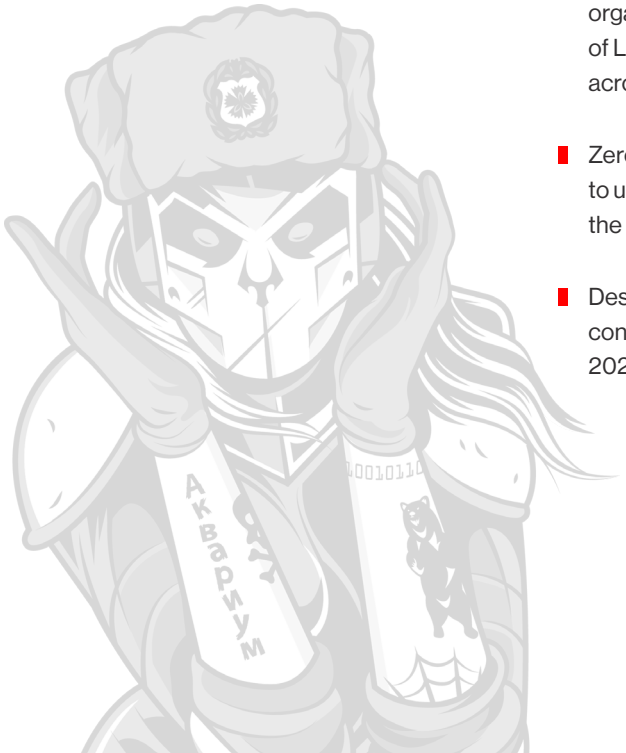
Adversaries are increasingly setting their sights on cloud targets and using more advanced operations for initial access, post-breach lateral movement, privilege escalation, defense evasion and data collection.

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.

- Adversaries ramped up cloud-focused activity over the course of 2022. Observed cloud exploitation cases grew by 95%, and cases involving cloud-conscious threat actors nearly tripled from 2021. This pattern signifies a larger trend of adversaries adopting the knowledge and tradecraft they need to target cloud environments.
- CrowdStrike Intelligence saw adversaries 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 target identities.
- While the goals of adversary operations remain similar to their intrusion ambitions outside the cloud, the short-lived nature of some cloud environments means they may need a more tenacious approach to succeed. It's expected cloud-conscious targeting will continue into 2023.

Discovery, Rediscovery and Circumvention: The Re-Weaponization of Vulnerabilities

Adversaries increasingly re-exploited vulnerabilities and focused on previously established attack vectors and components. There are two ways this can unfold. Actors can modify or reapply the same exploit to target other similarly vulnerable products; alternatively, they can identify a potential target and focus on these known vulnerable components, as well as circumvent patching by exploring other exploit vectors.



- Architectural weaknesses in technologies from Microsoft create systemic risk for customers. The release of patches and mitigations does not necessarily mean organizations are safe from vulnerability exploits. The notorious and prolonged nature of Log4Shell exploitation was the most prominent example of vulnerability discovery across several products in 2022.
- Zero-day and N-day vulnerabilities observed in 2022 demonstrated adversaries' ability to use specialized knowledge to bypass mitigations from previous patches and target the same vulnerable components.
- Despite early patches and repatching, CrowdStrike Falcon® Intelligence Recon saw continued discussions around Log4Shell on the criminal underground throughout 2022, reflecting a sustained interest in Log4Shell exploitation.

China-Nexus Adversaries Increased Operational Scale, Dominated Espionage Landscape

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

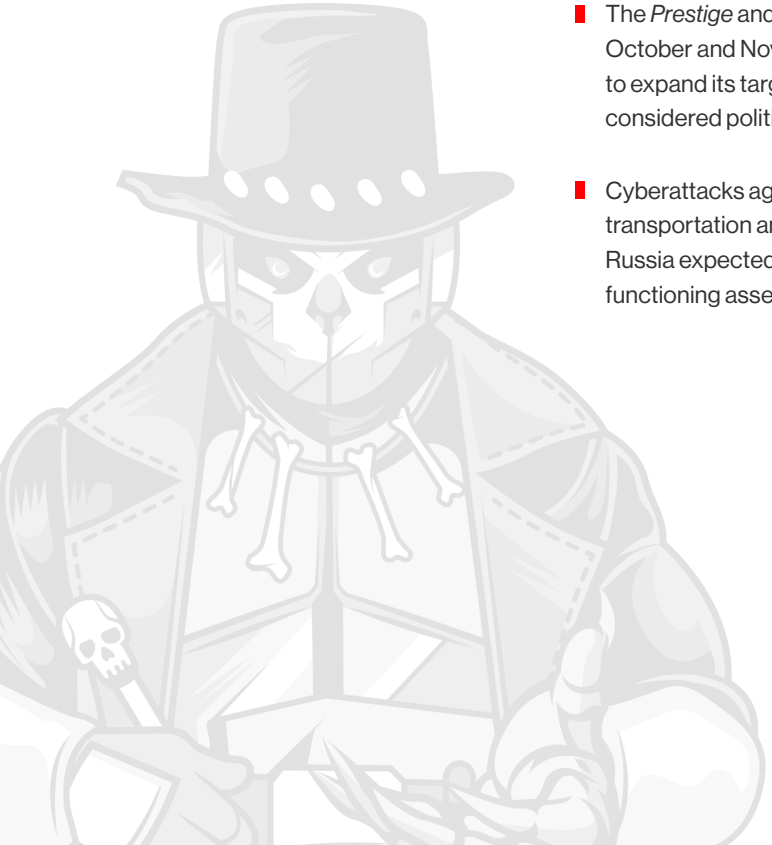
While China-nexus threat actors are often associated with activity targeting APJ regional nation interests and/or advanced Western industrial sectors, their activity greatly expanded in 2022. China-nexus adversaries were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks.

- CrowdStrike Intelligence observed China-nexus actors overwhelmingly target Taiwan-based technology organizations in 2022. This is consistent with the likely economic espionage mission associated with China-nexus actors in support of CCP goals for technological independence and dominance.

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

Russian Cyber Operations in Ukraine: Limited Impact, but Threat Continues

The ground war has so far overshadowed anticipated cyberattacks in the conflict between Russia and Ukraine. Despite bold headlines and political narratives, direct cybersecurity targeting of allied infrastructure and systems by Russia-nexus actors has yet to emerge. However, as the war enters its second year, organizations should take caution and follow best practices discussed in CISA's Shields Up initiative.



- The *Prestige* and *RansomBoggs* wipers, disguised as ransomware, were deployed in October and November 2022. Russia's pivot to fake ransomware suggests an intent to expand its targeting to sectors and regions in which destructive operations are considered politically risky.

- Cyberattacks against core sectors such as energy, telecommunications, transportation and media have not been as extensive as predicted. This likely indicates Russia expected a swift and decisive victory over Ukraine and planned to use these functioning assets to keep the nation running under a new regime.

RECOMMENDATIONS

CrowdStrike offers the following recommendations to help organizations protect their assets and defend against an ever-evolving and expanding adversary ecosystem:

01

Gain Visibility into Your Security Gaps

An organization is only secure if every asset is protected. As adversaries continue to weaponize and target vulnerabilities, security teams should prioritize visibility and enforcing of IT hygiene across the enterprise asset inventory.

02

Prioritize Identity Protection

The increase in malware-free attacks, social engineering and similar attempts to obtain access/credentials has made it clear: A traditional endpoint-only solution is not enough. Find solutions that not only help extend MFA into legacy and unmanaged systems, but also provide immediate detection and real-time prevention of lateral movement, suspicious behavior, misuse of service accounts and more.

03

Prioritize Cloud Protection

Adversaries are aggressively targeting cloud infrastructure and using a broad array of tactics, techniques and procedures — e.g., misconfigurations, credential theft, etc. — to compromise critical business data and applications in the cloud. Stopping cloud breaches requires agentless capabilities to protect against misconfiguration and control-plane and identity-based attacks, as well as runtime security to protect cloud workloads.

04

Know Your Adversary

Invest in threat intelligence that goes beyond supplying indicators of compromise (IOCs). Ensure it also exposes the humans behind the attack, as well as their motivation, capabilities and tools. Security teams can use this knowledge to focus defenses on pivoting to action.

05

Practice Makes Perfect

While technology is critical in the fight to detect and stop intrusions, security teams are the crucial link in the chain to stop breaches. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

DOWNLOAD THE FULL REPORT

The CrowdStrike 2023 Global Threat Report presents deep analysis that highlights the most significant events and trends in cyber threat activity in 2022. Download a free copy of the report at https://www.crowdstrike.com/global-threat-report/.