CROWDSTRIKE

# 2022 Global Threat Report

## EXECUTIVE SUMMARY

# A Year of Adaptability and Perseverance

**CrowdStrike's annual report provides crucial insights for staying ahead of and ultimately defeating today's threats.**

The annual CrowdStrike Global Threat Report is one of the industry's most trusted and comprehensive analyses of today's threat landscape and evolving adversary tradecraft. In this 2022 edition, we explore the most significant cybersecurity events and trends of 2021 and the adversaries behind this activity.

In an industry where it is crucially important to stay ahead, you may wonder why we focus on the past. And therein lies the power of CrowdStrike's annual Global Threat Report: Understanding the significance of recent events gives visibility into the shifting dynamics of adversary tactics, which is critical for staying ahead of and ultimately defeating today's threats.

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

# Threat Landscape Overview

- **Breakout time:** Our analysis 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 — at just 1 hour 38 minutes on average for hands-on-keyboard eCrime intrusion activity during 2021.
- **Malware:** Of all detections indexed by the CrowdStrike Security Cloud in the fourth quarter of 2021, nearly two-thirds (62%) were malware-free. Instead of using malware, attackers are increasingly leveraging legitimate credentials and built-in tools — an approach known as "living off the land" (LOTL) — in a deliberate effort to evade detection by legacy antivirus products.
- **Distribution of attacks:** Financially motivated eCrime activity continues to dominate the interactive intrusion attempts tracked by OverWatch. Intrusions attributed to eCrime in 2021 accounted for nearly half (49%) of the observed activity, while targeted intrusions accounted for 18%. Almost one-third (32%) of attacks remain unattributed.

# Key Findings

## Ransomware and the Ever-adaptable Adversary

The growth and impact of big game hunting (BGH) in 2021 was a palpable force felt across all sectors and in nearly every region of the world.

- CrowdStrike Intelligence observed an 82% increase in ransomware-related data leaks in 2021. This point, coupled with other data leaks, highlights how valuable victim data is to adversaries.
- Increased scrutiny and intervention from government and law enforcement agencies, as well as an uptick in media attention, drove fluctuations and variability within the CrowdStrike eCrime Index (ECX).
- New tactics, techniques and procedures (TTPs) used in data theft attacks in 2021, such as the development of advanced exfiltration tools, aided adversaries in extorting their victims.

## Iran and the New Face of Disruptive Operations

Since late 2020, multiple Iran-nexus adversaries and activity clusters have adopted the use of various techniques to target multiple organizations within the U.S., Israel and other countries within the greater Middle East and North Africa (MENA) region.

- In 2021, these cybercriminals masqueraded as hacktivists to conduct “lock-and-leak” attacks, which use ransomware to encrypt target networks and subsequently leak victim information via actor-controlled personas or entities.
- High-profile lock-and-leak operations, as well as more traditional ransomware methods, provide Iran with an effective capability to disruptively target its rivals in the region and abroad in the coming year.

## China Emerges as Leader in Vulnerability Exploitation

China-nexus actors deployed exploits for new vulnerabilities at a significantly elevated rate in 2021.

- CrowdStrike Intelligence confirmed a sixfold increase in exploitation of published vulnerabilities from 2020 to 2021 and linked 10 named adversaries or activity clusters to these attacks.
- 2021 highlighted a shift in China-nexus actors' preferred exploitation method from attacks that required user interaction to exploitation of vulnerabilities in internet-facing devices or services.
- Throughout 2021, Chinese actors focused significant attention on a series of vulnerabilities in Microsoft Exchange — now collectively known as ProxyLogon and ProxyShell — and used them to launch intrusions against numerous organizations worldwide.

## Log4Shell Sets the Internet on Fire

Due to the number of potentially affected endpoints, Log4Shell received more attention than any other vulnerability in 2021.

- First reported in November 2021, Log4Shell exploits Apache's Log4j2, a ubiquitous logging library used by many web applications.
- Opportunistic eCrime actors aggressively engaged in widespread Log4Shell exploitation commonly affiliated with commodity botnet malware, while other actors adopted Log4Shell as an access vector to enable ransomware operations.
- Many state-operated actors are likely to integrate Log4Shell exploits into their toolchain, since this logging library provides a method through which actors can gain access to target environments via vulnerable entry point systems or move laterally by exploiting internal servers on already compromised networks.

## Increasing Threats to Cloud Environments

CrowdStrike Intelligence observed an increase in exploitation of cloud-based services in 2021.

- Common cloud attack vectors used by eCrime and targeted intrusion adversaries include: cloud vulnerability exploitation; credential theft; cloud service provider abuse; use of cloud services for malware hosting and C2; and the exploitation of misconfigured image containers.
- Popular file sharing and collaboration tools are increasingly abused by malicious actors in the course of computer network operation. This trend is likely to continue as more businesses seek hybrid work environments.
- Russian adversaries are increasingly looking to the cloud to target new victims. FANCY BEAR has targeted numerous cloud-based email providers for credential harvesting, while COZY BEAR repeatedly demonstrated a high level of post-exploitation proficiency within cloud environments.

# Recommendations

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

## 01 Protect All Workloads

In the modern threat landscape, organizations must secure all critical areas of enterprise risk: endpoints and cloud workloads, identity and data.

## 02 Know Your Adversary

To protect your organization, you must understand the adversaries that may target your industry or geolocation and strengthen your defenses against the tools and tactics these actors employ.

## 03 Be Ready When Every Second Counts

Security teams of all sizes must enhance speed and agility to stop stealthy breaches before consequences turn devastating.

## 04 Stop Modern Attacks

Protect against identity-based attacks using a combination of artificial intelligence, behavioral analytics and a flexible policy engine to enforce risk-based conditional access.

## 05 Adopt Zero Trust

Because today's global economy requires data to be accessible from anywhere at any time, it is critical to adopt a Zero Trust model.

## 06 Monitor the Criminal Underground

In addition to monitoring your own environment, security teams must be vigilant and monitor activity within the criminal underground to uncover advance warnings of active threats.

## 07 Eliminate Misconfigurations

Security and IT teams must work together to address the most common causes of cloud intrusions: human errors such as omissions introduced during common administrative activities.

## 08 Invest in Elite Threat Hunting

As adversaries advance their tradecraft to bypass legacy security solutions, organizations must employ a combination of autonomous tools and expert threat hunters to see and stop the most sophisticated threats.

## 09 Build a Cybersecurity Culture

While technology is clearly critical in the fight to detect and stop intrusions, organizations must develop user awareness programs to combat the continued threat of phishing and related social engineering techniques.

# Download the full report

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

# 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:
**www.crowdstrike.com**

Follow us:
Blog | Twitter | LinkedIn | Facebook | Instagram

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