CROWDSTRIKE

2022 Global Threat Report

Adversary and Tradecraft Highlights

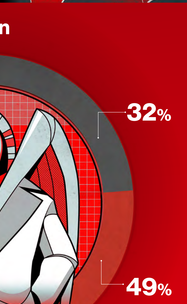
The CrowdStrike 2022 Global Threat Report, one of the industry's most trusted and comprehensive analyses of today's threat landscape and evolving adversary tradecraft, explores the most significant cybersecurity events and trends of 2021 and the adversaries behind them.

Meet the Adversaries

2 New countries added in 2021

21 Newly named adversaries in 2021

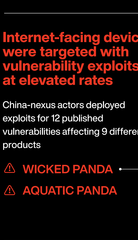
170+ Total tracked actors



Know Their Motivation

How They Operate

Today's eCrime adversaries move with speed and purpose in pursuit of their objectives



Breakout time remains under 2 hours

On average, eCrime adversaries need 1 hour 38 minutes to move laterally

62% attacks were malware-free

Adversaries have moved beyond malware to use "hands-on-keyboard" techniques and "living off the land" tools to attempt to evade detection

45% increase in interactive intrusions

Such attacks allow adversaries to harvest new credentials and try to go undetected

What They're After

The adversaries got smarter and bolder in targeting victims' data and infrastructure.

Ransomware-related data leaks shot up 82% from 2020

Big game hunting campaigns increased ransom demands by 36%

⚠ CARBON SPIDER ⚠ PINCHY SPIDER ⚠ WIZARD SPIDER

Internet-facing devices were targeted with vulnerability exploits at elevated rates

China-nexus actors deployed exploits for 12 published vulnerabilities affecting 9 different products

⚠ WICKED PANDA

⚠ AQUATIC PANDA

Disruptive information operations hid behind criminal activity

Nation-state groups acting as eCrime or hacktivist entities use "lock-and-leak" tactics and distribute stolen data via social media, chat platform to conduct information operations

⚠ PIONEER KITTEN

⚠ NEMESIS KITTEN

⚠ SPECTRAL KITTEN

Cloud environments face increasing threats

eCrime and targeted intrusion-focused adversaries are using remote code execution, credential theft, admin account abuse, command and control, and exploitation of misconfigured containers to advance their attacks.

⚠ COZY BEAR

⚠ FANCY BEAR

To be prepared, you need to:

KNOW YOUR ADVERSARIES
BE READY WHEN EVERY SECOND COUNTS
MONITOR THE CRIMINAL UNDERGROUND

Download the full 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.

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

Follow us:

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

CROWDSTRIKE

We Stop Breaches