

# 2026 GLOBAL THREAT REPORT

An in-depth analysis of the adversaries, tradecraft, and trends that defined 2025

- 24 newly named adversaries
- 281+ adversaries actively tracked by CrowdStrike



## The Race Against Time: Adversary Speed Accelerates



**27 seconds** was the fastest eCrime breakout time on record



**29 minutes** was the average eCrime breakout time, a **65% increase** in speed year-over-year



**4 minutes** was the time it took for CHATTY SPIDER to attempt to exfiltrate sensitive data after gaining access

## Adversaries Exploit the Gaps: Edge Device and Cross-Domain Attacks Escalate



**40% of vulnerabilities** exploited by China-nexus adversaries targeted edge devices that lack comprehensive monitoring

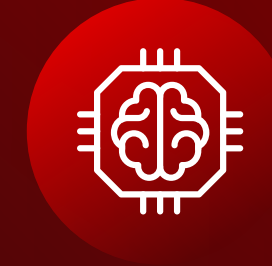


**266% increase** in cloud-conscious intrusions by state-nexus threat actors



**42% increase** in zero-day vulnerabilities exploited prior to public disclosure

## The Dual Threat of AI: The Adversary's Advantage and Enterprise's New Attack Surface



**89% increase** in attacks by AI-enabled adversaries



**90+ organizations** had their own legitimate AI tools exploited by threat actors to generate malicious commands and steal sensitive data

## Nation-State Threat Acceleration: Strategic Targeting and Financial Theft



**85% increase** in China-nexus activity against logistics organizations, with a **38% increase** across all sectors



**130% increase** in North Korea-nexus incidents, including the largest single financial theft (1.46B USD) ever reported<sup>1</sup>

## Adversaries Are Blending In: Malware-Free Tradecraft Dominates



**82% of detections** in 2025 were malware-free, up from **51%** in 2020

1. <https://www.ic3.gov/psa/2025/psa250226>