Threat Intelligence

Overview and Recent Observations

WINNISEC
May 2025

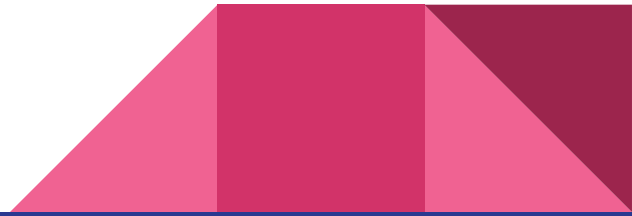
Overview

What is threat intelligence and why do I care?

M-Trends 2025

Google Threat Horizons Report H1 2025

Google Threat Intel Zero-Day Exploitation Analysis Report



Threat Intelligence?

Threat intelligence is understanding of an adversary - their motivations, objectives, tactics, techniques, and procedures (TTPs)

Threat intelligence teams ***acquire and analyze information*** to confirm relevance, accuracy, etc.

This information is distilled and transformed into ***threat intelligence products:***

- ***Strategic***: High-level analysis on observed trends relevant to the org
  - E.g., Emerging threat information, geopolitical impacts, risk assessments against specific groups or incidents
- ***Operational***: Behavioural analysis of threat actors based on observed activities
  - E.g., Threat actor profiles defining TTPs, motivations, and defining attributes
- ***Tactical***: Low-level details from observed threat actor activity
  - E.g., Network and host-based indicators of compromise

These products are consumed by teams within the organization in order to ***enhance defences***

M-Trends Overview and AI Analysis

M-Trends is Mandiant's annual report, covering trends and observations from incident response efforts over the previous year

M-Trends 2025: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Here are the top three takeaways from the M-Trends 2025 report:

- Attackers are using infostealer malware to enable intrusions using stolen credentials.
- Attackers are targeting unsecured data repositories due to a lack of basic security.
- Attackers are exploiting gaps and risks introduced as organizations migrate to the cloud.

You can find the full report here: M-Trends 2025 Report

Note: QR codes generated with CyberChef, so GCHQ is probably watching you right now - legal disclaimer: please laugh at this joke

M-Trends Artisan, Human-Collected Highlights

Cloud Initial Infection Vectors, 2024

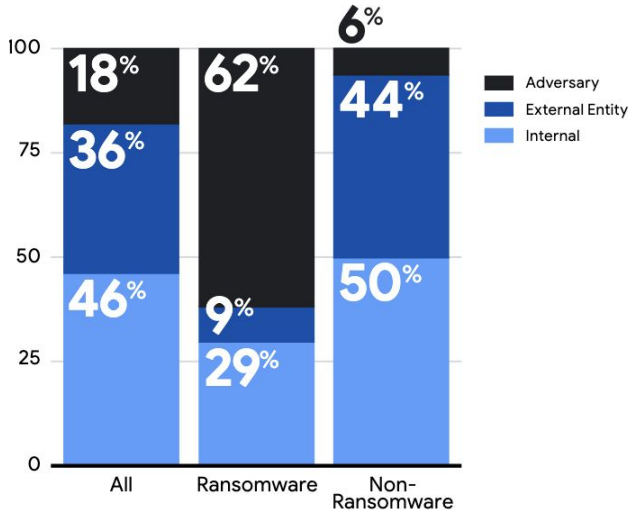
AMERICAS

Exploit
28%

Stolen Credentials
18%

Email Phishing
16%

Americas Detection by Source, 2024



Threat Horizons Overview and AI Analysis

Google releases H1 and H2 ‘Threat Horizon’ reports to provide strategic insights into threat actor activities and observations

H1 2025 Threat Horizons Report: https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf

Here are the top three insights from the Google Cloud Threat Horizons Report:

- Threat actors are shifting their focus to target overprivileged service accounts to move laterally within an organization's systems, instead of solely focusing on stealing user login information and exploiting misconfigurations to gain initial entry.
- Compromised user identities in hybrid environments can lead to persistent access and lateral movement between on-premises and cloud environments, subsequently resulting in multifaceted extortion.
- Threat actors are actively exploiting vulnerabilities and weak credentials to access sensitive information in cloud databases.

You can find the full report at: Threat Horizons Report H1 2025

Threat Horizons Artisan, Human-Collected Highlights

Figure 1: Cloud Risk Alerts Detected H2 2024

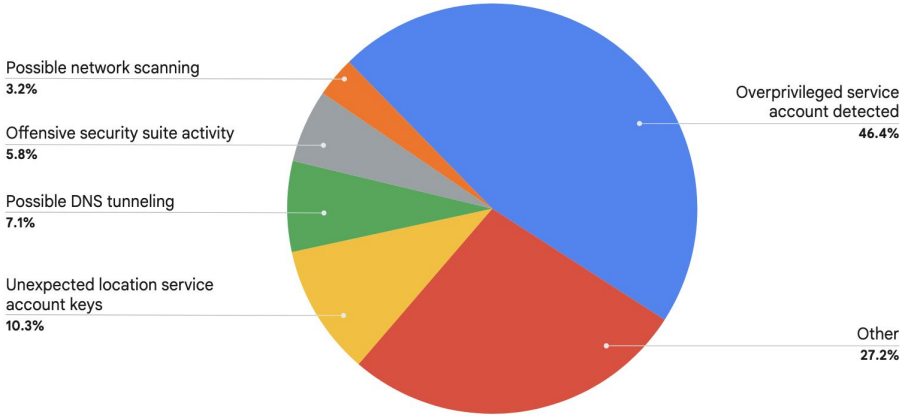
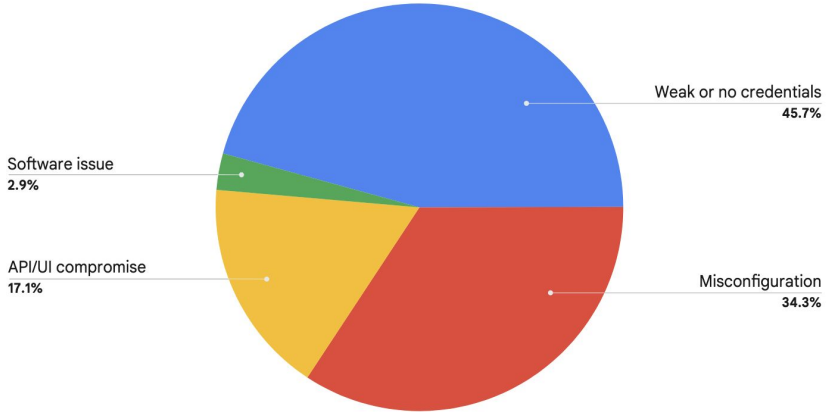


Figure 3: Initial Access Vectors of Concern H2 2024



Zero-Day Overview and AI Analysis

Google's Threat Intelligence Group released a report analyzing 0-day exploitation throughout 2024.

Hello 0-Days My Old Friend: https://services.google.com/fh/files/misc/2024-zero-day-exploitation-analysis-en.pdf

Here are the top three insights from the 2024 Zero-Day Exploitation Analysis:

- GTIG tracked 75 zero-day vulnerabilities exploited in the wild in 2024. The average trendline indicates that the rate of zero-day exploitation continues to grow at a slow but steady pace.
- GTIG observed an increase in adversary exploitation of enterprise-specific technologies throughout 2024. In 2023, 37% of zero-day vulnerabilities targeted enterprise products, which jumped to 44% in 2024.
- Actors conducting cyber espionage operations accounted for over 50% of the vulnerabilities we could attribute in 2024. People's Republic of China (PRC)-backed groups exploited five zero-days, and customers of CSVs exploited eight, continuing their collective leading role in zero-day exploitation.

You can find the full report at: 2024 Zero-Day Exploitation Analysis

Zero-Day Highlights

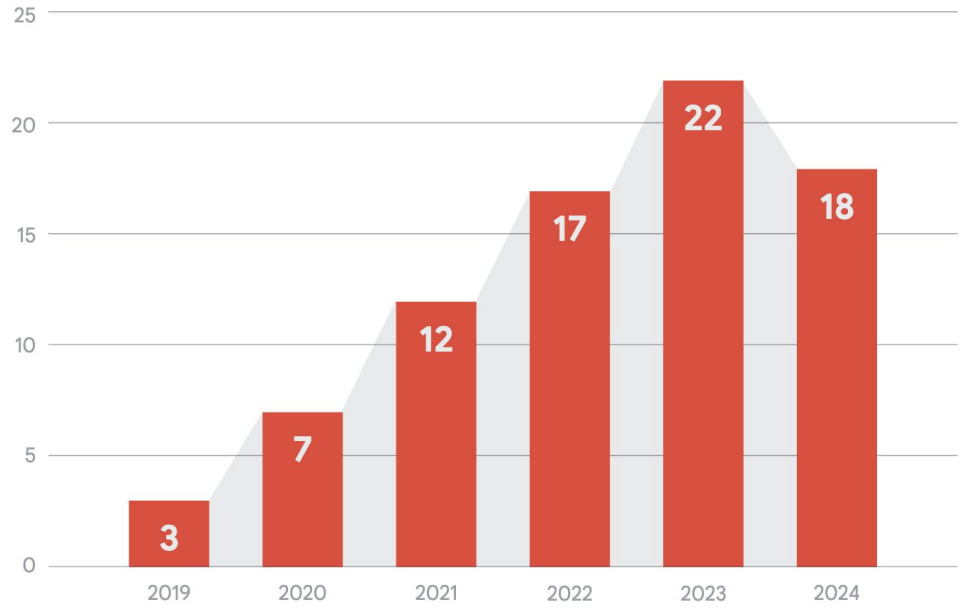
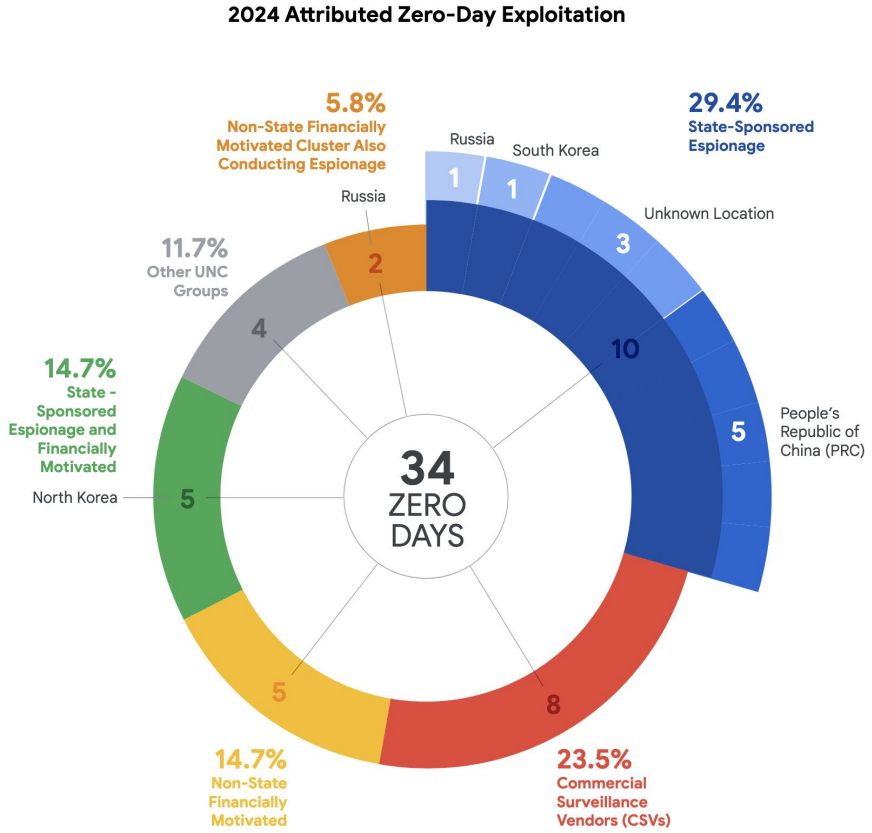


Figure 3: Number of unique enterprise vendors targeted



Outro

Thanks for attending!

Next month's event is June 27th @ 17:45

Want to speak at a future event? Have a question?

talk@winnisec.life

Skullspace Discord *#events*

DC204 *#events*