Presented by

Trellix ADVANCED RESEARCH CENTER

THE CYBERTHREAT REPORT

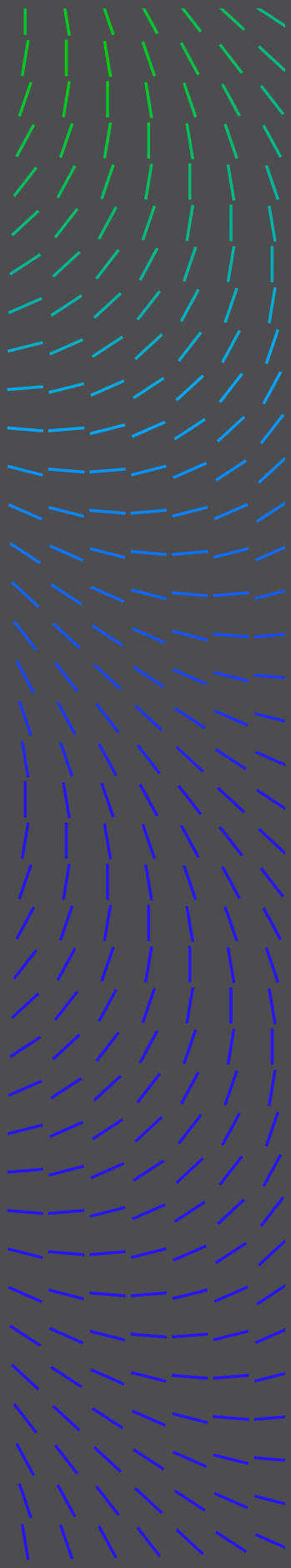
October 2025 Executive Summary

Between April and September 2025, the global cyber threat landscape experienced an intense escalation, marked by rising activity, shifting motivations, and an evolving cast of adversaries. This period saw APTs increasingly used as an extension of state power, new players emerged in ransomware, a notable increase in AI adoption by criminals, and attacks exploiting vulnerabilities in the software supply chain.

This executive brief offers key takeaways and a high-level summary of the findings detailed in the CyberThreat Report. It takes you through the latest geopolitical and cyber threat activity, detailing the tactics, techniques, and procedures currently favored by malicious actors worldwide. For industry threat breakdowns, exploitation trends, and specific APT attacks, dive into the complete CyberThreat Report.

METHODOLOGY

Trellix® and experts from our Advanced Research Center (ARC) compile the statistics, trends, and insights that comprise this report from a wide range of global sources, both open and captive. The aggregated data is fed into our Insights and ATLAS platforms. Leveraging AI, machine learning, automation, and human acuity, the team cycles through an intensive, integrated, and iterative set of processes – normalizing the data, analyzing the information, and developing insights meaningful to cybersecurity leaders and SecOps teams on the front lines of cybersecurity worldwide.



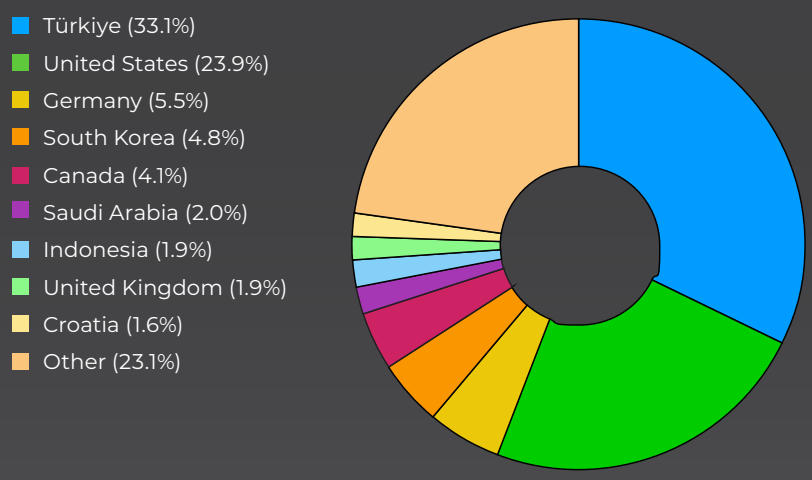
A LOOK INTO THE EVOLVING APT LANDSCAPE

Analysis of Advanced Persistent Threat (APT) activity shows 540,974 detections across 1,221 campaigns, as adversaries refine their tradecraft, focusing on strategic targets and maximizing evasion.

Key findings:

- **Geographic concentration:** Over half of global detections (57%) were concentrated in Türkiye (33.1%) and the United States (23.9%), highlighting the regions' geopolitical interests and economic significance.
- **Critical infrastructure focus:** APT groups strategically prioritize telecommunications (70.8%), as a high-value sector for persistent access.
- **Evasion via trusted tools:** Attackers are living-off-the-land by leveraging trusted, legitimate administration tools like Cmd (48.7%) and PowerShell (47.3%) to evade detection.
- **Global actor dominance:** The landscape is led by sophisticated, nation-state groups, primarily North Korean-affiliated Lazarus (17.8%), with Chinese and Russian-affiliated groups maintaining a consistent operational tempo.
- **DRPK's "malware-less" infiltration:** North Korea's new infiltration technique embeds operatives directly within organizations as legitimately hired IT workers.

TOP 10 AFFECTED COUNTRIES:



CISO TIPS:

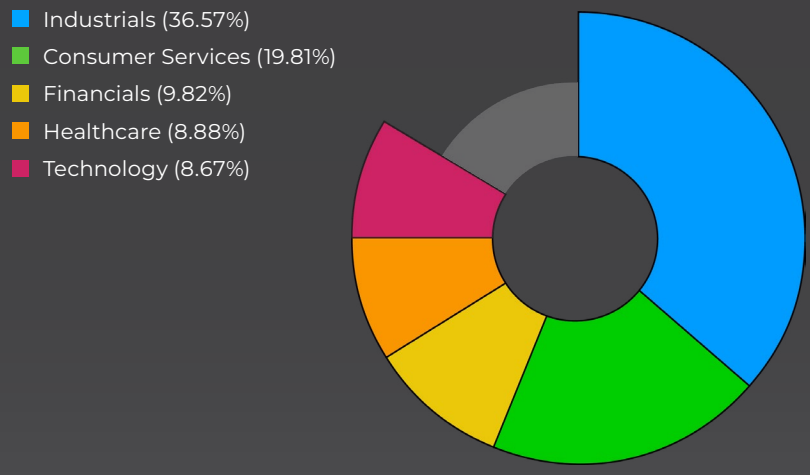
- Treat APT defense as a strategic imperative. Embed resilience by design, strengthen cross-sector collaboration, and conduct regular threat simulations.
- Emphasize behavioral and contextual detection over simple signature-based alerts.

RANSOMWARE'S NEW DOMINANCE AND EMERGING THREATS

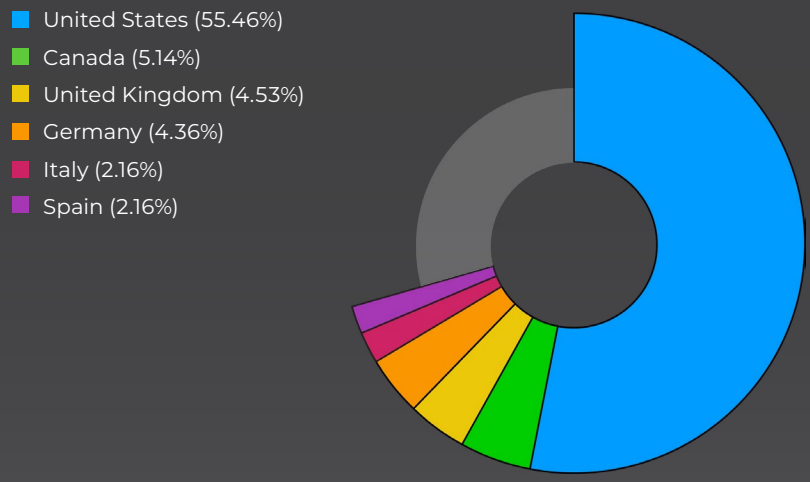
During the past six months, Trellix ARC observed 3,280 ransomware victim posts, revealing fundamental changes in threat actor behavior, targeting patterns, and operational strategies.

In April 2025, RansomHub collapsed due to intergang conflict and coordinated law enforcement efforts. However, its affiliates fueled the rise of new groups such as Qilin and Dragon Force. The resilience of the affiliate economy demonstrates that defenders should use takedowns as windows of opportunity to harden controls.

TOP 5 MOST TARGETED SECTORS (APRIL - SEPTEMBER, 2025)



TOP 6 MOST TARGETED COUNTRIES (APRIL - SEPTEMBER, 2025)



CISO TIPS:

- Prioritize detection of intrusion patterns over actor-specific signatures, monitor living-off-the-land tooling (PowerShell, PsExec, net), and prepare for rapid actor turnover and rebranding.
- Implement PowerShell logging, constrained language mode, and application allowlisting.

CYBERCRIMINALS' USE OF AI-POWERED MALWARE

During Q2-Q3 2025, Trellix ARC has observed a notable surge in the adoption and interest of AI-driven tools among cybercriminals. This trend marks a significant increase compared to earlier quarters of 2024/2025, where threat actors primarily used AI applications for phishing campaigns and assistance in script/code generation.

- **Automating Ransomware Negotiations:** Ransomware groups are incorporating AI chatbots for victim negotiation and using AI call bots to replace human callers.
- **Emergence of AI-Generated Ransomware:** XenWare, which claims to be fully AI-generated ransomware, appeared in April 2025 with aggressive multithreading for rapid, concurrent encryption.
- **Introducing AI-Powered Infostealers:** LameHug, the first publicly reported AI-powered infostealer, leverages LLMs for dynamic command generation, marking a paradigm shift in malware development.
- **Enhancing Email Attack Capabilities:** AI-enhanced SMTP warming tools now support over 40 conversation topics in 10+ languages, vastly improving phishing and deception success.

COMPLEX ATTACK CHAINS AND EXPLOITATION OF VULNERABILITIES

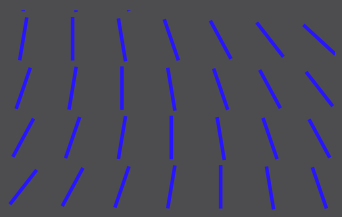
Taking a look at the analysis of the vulnerability landscape reveals a sustained high level of malicious activity targeting known software weaknesses in major vendors.

Key takeaways from the vulnerability environment include:

- **AI Collapses Patch Window:** AI systems can generate working exploits for a published CVE in as little as 10-15 minutes, collapsing the traditional time buffer defenders relied on.
- **Attacks on Key Vendors:** Microsoft was affected by 15 campaigns exploiting vulnerabilities in its Windows, SharePoint, and Office products. Cisco and Fortinet were also heavily targeted.
- **Software Supply Chain Attacks:** Threat actors actively exploited vulnerabilities in enterprise applications and open-source software, targeting foundational weaknesses in the software supply chain.

CISO TIPS:

- Update incident response playbooks to address AI-powered ransomware scenarios.
- Train security teams to recognize the unique characteristics of AI-generated attack vectors, such as XenWare ransomware.
- Implement automated security postures capable of responding to AI-generated exploits.
- Establish robust governance frameworks for securing AI-powered development lifecycles against sophisticated attack chains.



CISO TIPS:

- Shift from traditional patching approaches to threat-intelligence-driven vulnerability management.
- Implement threat intelligence-driven "vulnerability contextualization" frameworks that transform raw CVE data into actionable risk intelligence.

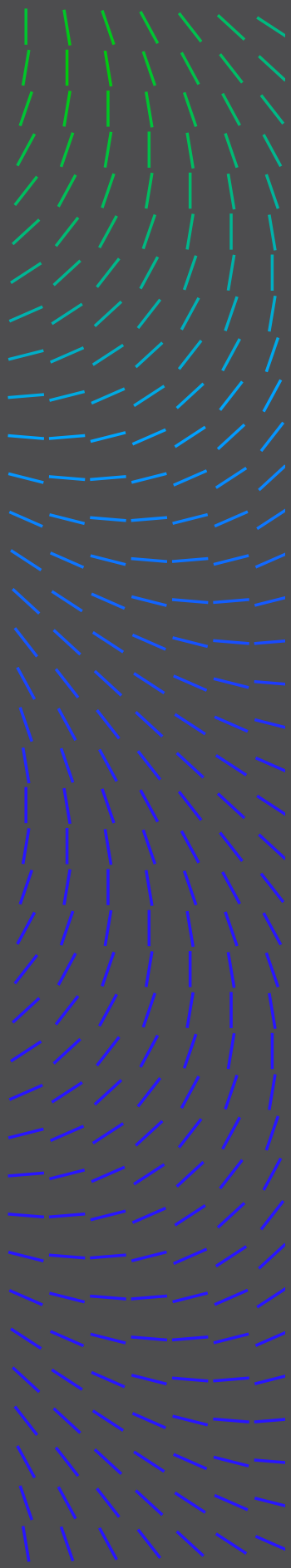
CONCLUSION

Sophisticated APT campaigns and the rise of AI-driven ransomware define the Q2-Q3 2025 landscape, demanding a critical response. Organizations must stop relying on patching time buffers and traditional code review to adopt an urgent, strategic shift toward a proactive, threat-intelligence-driven security posture.

Building resilience requires focusing on five core pillars:

- **Threat intelligence:** Maintaining visibility into emerging threats, techniques, and actors.
- **Defense in depth:** Building layered defenses to mitigate the risk of compromise.
- **Security awareness:** Empowering employees to recognize and resist phishing and social engineering.
- **Vulnerability management:** Continuously identifying and addressing weaknesses before attackers exploit them.
- **Incident response preparedness:** Developing and exercising robust plans to minimize operational impact.

By embracing this adaptive security posture, organizations can shift from a reactive stance to one of readiness, turning intelligence into action and uncertainty into resilience. For a deeper analysis of the findings, access the complete CyberThreat Report.



This document and the information continued herein describes computer security research for educational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy I Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

Trellix is a trademark or registered trademark of Musarubra US LLC or its affiliates in the US and other countries. Other names and brands may be claimed as the property of others.

Trellix

Copyright © 2025 Musarubra US LLC