THE CYBERTHREAT REPORT

Executive Summary

April 2025

Presented by

Trellix ADVANCED RESEARCH CENTER

THE CYBERTHREAT REPORT

The CyberThreat Report: April 2025, is the latest research from the Trellix Advanced Research Center. Our team of dedicated researchers and intelligence analysts poured over Trellix telemetry, industry reports, and more to craft a report filled with operational threat intelligence intended to accelerate cyber resilience.

Our report investigates the geopolitical events impacting the cyber domain; the overarching landscape for Advanced Persistent Threat (APT) and criminal actors; the activity of China-aligned groups; the use of AI by InfoStealers, password sprays, and phishing by cybercriminals; and concludes with an analysis of industry reports. The CyberThreat Report: April 2025 provides readers with insight into the regions and industries at risk, the evolving tools, tactics, and procedures of malicious actors, and offers recommendations for CISOs and security operations teams tasked with protecting their organizations from the mounting threats ahead.

> *"...our team has pieced together an ever-sharpening picture of how threats form, flourish, and–most importantly–how they can be stopped."*
>
> John Fokker, Head of Threat Intelligence

EXECUTIVE SUMMARY

The last six months have realized further escalation of the cyber domain–driven by dramatic shifts in geopolitics, the economy, and technological advancements. Key themes include:

- **Increased intensification of threats linked to China:** China-affiliated threat actors continued to evolve and refine their tactics to remain effective in their operations while minimizing the risk of attribution. There was a notable reliance on exploiting zero-day vulnerabilities and known vulnerabilities in commonly used network edge devices versus traditional methods like spear-phishing and social engineering. Further, the use of Operational Relay Box (ORB) networks in attacks grew considerably. The most active APT groups were China's APT40 and Mustang Panda, with the two groups generating 46% of all detected APT activity. China-aligned APT41 showed a 113% increase in activity in Q1 2025 relative to the previous quarter.
- **Heightened cyberactivity originating from Russia:** As the Russia-Ukraine conflict entered late 2024 and early 2025, the intensity of the war escalated. One of the most striking developments during this period was both sides' intensified use of hybrid warfare tactics. Cyberattacks, disinformation campaigns, and economic warfare became central to the conflict. Trellix telemetry data identified a notable increase in threat activity linked to Russia-aligned cyber actors, particularly the Sandworm team, also known as APT44, during the final quarter of 2024. Additionally, Russia-aligned APT29, also known as Midnight Blizzard, was the third most active APT group, directing the bulk of its activities toward transportation and shipping (55%) and telecommunications (40%).

- **Spike in activity targeting the United States:** This may be the most active moment in history when it comes to cyber attacks targeting the United States. Trellix telemetry shows there was a 136% increase in APT detections targeting the US in Q1 2025 alone. When looking at APT activity directed at the US, 47% of detections were attributed to China and 35% to Russia-aligned groups, and 64% of detections targeted the telecom sector. Further the US remains the primary target of ransomware activity and was the reported victim in 58% of ransomware posts, up from 42% in our last report, and was the country with the most ransomware detections at 39%.

- **Focus on telecom and technology sectors:** While analysis of industry reports shows that government institutions far outpaced other sectors as a target of malicious activity, Trellix observed APT detections targeting the telecommunications sector increased 92% in Q1 when compared to the previous quarter. The telecommunications sector had the most APT related detections, receiving 47% of all detected activity, followed by transportation and shipping. The actor behind the highest number of APT detections, China-aligned APT40, directed 66% of its activity toward the sector. The technology sector saw an increase in APT related detections as well, generating 119% more detections in Q1 2025 when compared to Q4 2024.

- **Expanding use of complex attack chains:** We've observed increases in tool sophistication, greater emphasis on evasion, an evolution of post-exploitation frameworks, and more complex attack chains. This spans the use of novel and sophisticated combinations of TTPs, malicious scripts, legitimate tool abuse, and persistence mechanisms. Additionally, various threat actors actively leveraged vulnerabilities, particularly vulnerabilities in products from popular security vendors.

RECOMMENDATIONS

In many ways, cybersecurity is a bedrock of real business resilience. A line of defense can be undone by a vulnerability left unpatched or the mistaken opening of a phishing email. Organizations must prioritize layered defenses and incident response, along with a culture of security.

- **Defense in breadth:** Security controls should be deployed throughout your organization's IT infrastructure, software, and applications, to ensure layers of visibility and protection

- **Platform approach:** By leveraging a security platform approach with a combination of robust solutions like EDR, NDR, XDR, augmented with a service like MDR, organizations are better able to respond to multi-vector threats

- **Threat intelligence:** Stay informed about emerging threats, TTPs, and threat actors through implementing operational threat intelligence on top of your security controls

- **Security awareness training:** Educate employees about phishing, social engineering, and other attack vectors

- **Vulnerability management:** Identify and address vulnerabilities in systems \ and applications

- **Incident response planning:** Identify and address vulnerabilities in systems and application

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. 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.

ABOUT THE TRELLIX ADVANCED RESEARCH CENTER

The Trellix Advanced Research Center is at the forefront of research into the emerging methods, trends, and tools used by cyber threat actors across the global cyber threat landscape. Our elite team of researchers serve as the premier partner of CISOs, senior security leaders, and their security operations teams worldwide. The Trellix Advanced Research Center provides operational and strategic threat intelligence through cutting-edge content to security analysts, powers our industry leading AI powered XDR platform, and offers intelligence products and services to customers globally. More at https://www.trellix.com/en-us/advanced-research-center.html.

ABOUT TRELLIX

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's comprehensive, open and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security. More at https://trellix.com.