Presented by

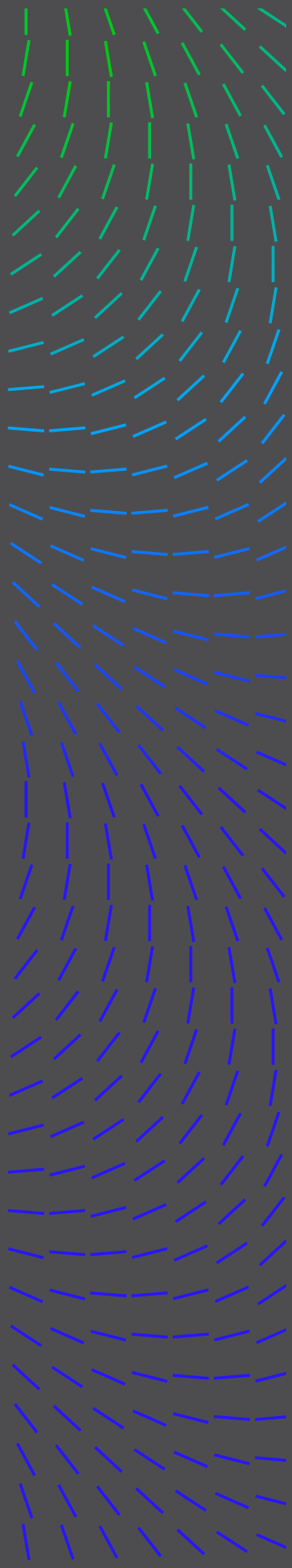
Trellix ADVANCED RESEARCH CENTER

# THE CYBERTHREAT REPORT

April 2026
Executive Brief

The past six months have seen a sharp escalation in the cyber threat landscape, defined by the convergence of nation-state tradecraft and criminal efficiency. This period was marked by the rapid adoption of AI to scale attacks, the exploitation of trusted administrative tools, and the growing sophistication of supply chain attacks.

This executive brief offers key takeaways and a high-level summary of the findings in the CyberThreat Report. It takes you through the adaptive tactics and shifting motivations currently driving global adversaries. For industry threat breakdowns, technical 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.

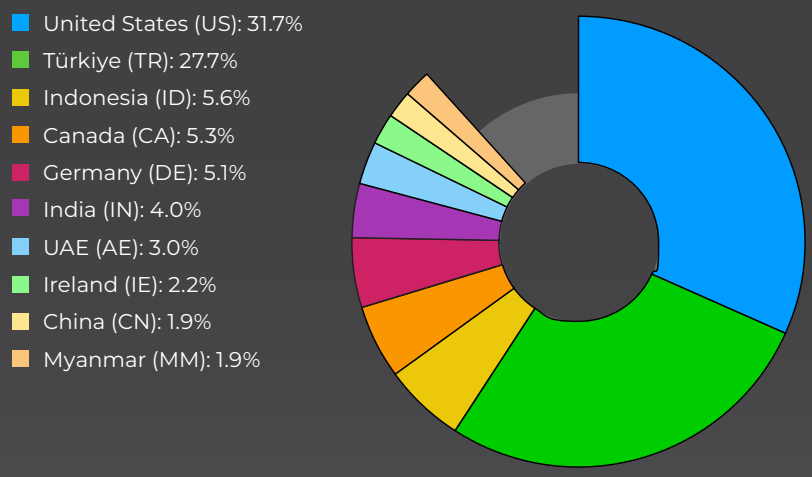
## A LOOK INTO THE EVOLVING APT LANDSCAPE

Analysis of advanced persistent threat (APT) activity shows nearly 565K detections, as adversaries refine their tradecraft, focusing on strategic targets and maximizing evasion.

Key findings:

- **U.S. & Türkiye are most targeted:** The concentration (59.4%) of global APT detections in just two countries (United States 31.7%, Türkiye 27.7%) suggests coordinated, strategic targeting aligned with geopolitical interests.
- **Preference toward critical infrastructure:** The APT detections demonstrate clear sectoral preferences, with the telecom and transportation and shipping sectors bearing the highest threat burden.
- **APT group dominance:** The top three threat actors—Gamaredon Group (9.6%), Mustang Panda (9.4%), and Lazarus (7.9%)—are responsible for over a quarter of all recorded detections, totaling 26.6% of the overall volume.
- **Living-off-the-land usage:** APT groups demonstrate continuous use of living-off-the-land techniques, with Cmd (48.9%) and PowerShell (49.6%) leading tool usage.

### TOP 10 AFFECTED COUNTRIES:




### CISO TIPS:

- Develop a mature security posture that transitions from legacy signature-based alerting to behavioral and contextual detection methodologies..
- Require comprehensive activity baselining, rigorous least-privilege protocols, and the logical segmentation of administrative domains.

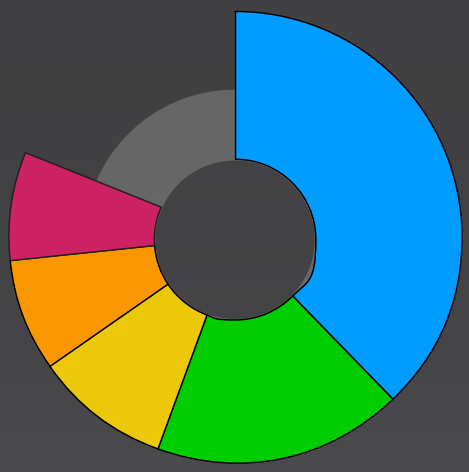
## RANSOMWARE LANDSCAPE PIVOT: STRUCTURAL VOLATILITY AND THE RISE OF AI-ASSISTED EXTORTION

Over the past six months, Trellix ARC observed 4,801 victim posts and a steady average of 800 monthly posts from legitimate ransomware operators, revealing a structurally elevated ransomware threat environment.

Additionally, ransomware group activity went through a reset. Once dominant groups, including RansomHub, LockBit3, BlackBasta, and Cactus, disappeared. This is most likely due to law enforcement pressure and internal turmoil. However, a wave of new groups, including Sinobi, Nightspire, and LockBit5, filled the gap—illustrating the resilience and adaptability of the cybercriminal underground.

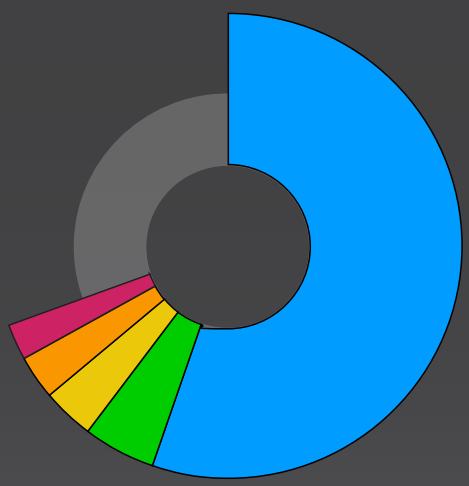
### TOP 5 MOST TARGETED SECTORS (OCTOBER 2025–MARCH 2026)

- Industrials: 37.9%
- Consumer services: 17.8%
- Technology: 9.7%
- Healthcare: 8.1%
- Financials: 7.7%



### TOP 5 MOST TARGETED COUNTRIES (OCTOBER 2025–MARCH 2026)

- United States: 55.4%
- Canada: 5%
- United Kingdom: 3.5%
- Germany: 3.3%
- France: 2.4%



### CISO TIPS:

- Implement zero-trust controls and establish an approved RMM tool inventory to block unauthorized endpoint remote access software, and require MFA for all remote access sessions.
- Implement VPN appliance patches immediately, especially for SonicWall, Fortinent, and Cisco GlobalProtect.
- Establish shadow copy, maintain offline, immutable backups, and test restoration procedures quarterly.

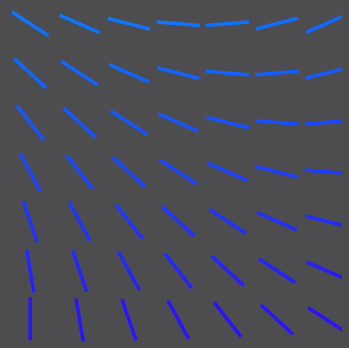
## CYBERCRIMINALS' USE OF AI-POWERED MALWARE

During Q4 2025–Q1 2026, Trellix ARC observed that threat actors no longer use AI as a productivity tool to write better phishing emails or cleaner exploit code; it is now embedded in the execution layer of attacks themselves. This trend marks a significant transition to vibeware malware, where AI-generated malware is operating at an industrial scale.

- **The vibeware doctrine of mass production:** Threat actors like APT36 have begun using AI to mass-produce diverse mediocre implants in niche programming languages (e.g., Nim, Zig, Crystal) to overwhelm detection engines through sheer volume and variety.
- **Emergence of AI-integrated malware families:** New malware, PromptFlux and PromptSteal, call LLM APIs at runtime to dynamically generate unique malicious behavior, breaking the traditional assumption that malicious code must be pre-encoded in a binary.
- **Collapse of technical barriers for low-skilled actors:** Commercial AI enables unskilled actors to achieve nation-state-level operational scale. One instance includes a single actor compromising 600 devices globally via automated AI reconnaissance.
- **Commoditization of deepfake-driven fraud:** Deepfake and voice synthesis tools transitioned into mass-market commodities, with underground services offering high-quality video for as little as $100 to bypass financial know your customer (KYC) controls and multifactor authentication (MFA).

### CISO TIPS:

- Develop specific detection logic for anomalous AI API traffic patterns and adapt to a threat environment where the attackers' tools possess inherent intelligence.
- Train security teams to recognize the unique characteristics of AI-generated attack vectors.



## SUPPLY CHAIN ATTACKS

Between October 2025 and March 2026, Trellix ARC witnessed a grim maturation of supply chain warfare, from simple typosquatting to threat actors integrating immutable blockchains into their C2 infrastructure to evade traditional security scanners.

- **Takedown-resistant C2 infrastructure:** Threat actors have integrated immutable blockchains such as Solana and ICP to host C2 channels. These sophisticated tactics, including phantom dependencies and invisible Unicode, allow malicious traffic to blend with legitimate Web3 activity.
- **Cascading security tool compromises:** A single Trivy scanner breach enabled TeamPCP to propagate attacks across the ecosystem. By using tag poisoning on trusted tools, attackers gained elevated access to secrets and built environments for KICS and LiteLLM.
- **High-impact maintainer account takeovers:** The Axios compromise demonstrated the massive blast radius of a single maintainer account takeover, impacting a library with 100 million weekly downloads. These attacks bypass source code auditing by using hidden dependencies to deploy remote access trojans.

### CISO TIPS:

- Require hardware security keys for all accounts that can publish packages or push to production repositories.
- Pin CI/CD actions to immutable commit references rather than mutable version tags.
- Implement monitoring for unexpected dependency changes in lockfiles, particularly the addition of unfamiliar transitive dependencies or shifts from pinned to floating-version references.

## CONCLUSION

The convergence of nation-state tradecraft and AI-driven efficiency defines the current landscape. As adversaries adopt vibeware and exploit immutable blockchains to scale attacks, traditional defenses must evolve.

For defenders, this environment demands resilience over reaction. Effective security programs must look beyond isolated indicators and instead focus on behavior, context, and operational coordination across intelligence, security operations, and incident response.

By embracing intelligence-led cyber resilience, 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.