Technical white paper

HPE Threat Labs 2026

In the Wild Threat Report

Contents

3 Executive summary

4 2025 key findings

6 Emerging threats and notable trends

10 Additional findings

11 Conclusion and recommendations

12 Methodology

13 Glossary of terms

Section 1

Executive summary

Cybercrime Inc.: Inside the enterprise-grade operations powering 2025's global threats

In this report, HPE Threat Labs reviewed **1186** active threat campaigns globally from January 1 through December 31, 2025. These campaigns demonstrated the ongoing exploitation of both new and known vulnerabilities, employing a wide range of tactics and targeting multiple sectors. Even more alarming than the volume of these campaigns was the professionalism behind the attacks. Threat actors ran their operations like Fortune 500 enterprises, complete with hierarchical chains of command, specialized teams, rapid coordination, and a nuanced understanding of ubiquitous workforce applications and documents. Virtually no sector was spared.

Globally, government agencies were the hardest hit, but financial and technology firms were close behind. The defense, manufacturing, telecommunications, healthcare, and education sectors also faced a significant volume of attacks.

Government agencies

274 campaigns

Financial

211

Technology

179

Defense

98

Manufacturing

75

Telecommunications

63

Healthcare

63

Education

61

Nation-state-linked espionage groups and organized cybercrime threat actors deployed an advanced arsenal of malicious infrastructure with **147,087** malicious domains, 57,956 malware files, and **549** exploited vulnerabilities. In addition, these actors replicated their techniques with business-like efficiency. One data-stealing operation even coordinated an automated **assembly line** through the Telegram messaging application to exfiltrate data in real time. Others utilized generative AI to produce synthetic voices and deepfake videos for targeted video-phishing (vishing) and executive impersonation fraud, while an extortion gang did market research on virtual private network (VPN) flaws to tailor their break-ins. These tactics allowed threat actors to strike more targets more expeditiously, with a focus on sectors tied to national infrastructure, critical data, and economic stability. Essentially, these methods allowed them to pursue financial gain by strategically **following the money**.

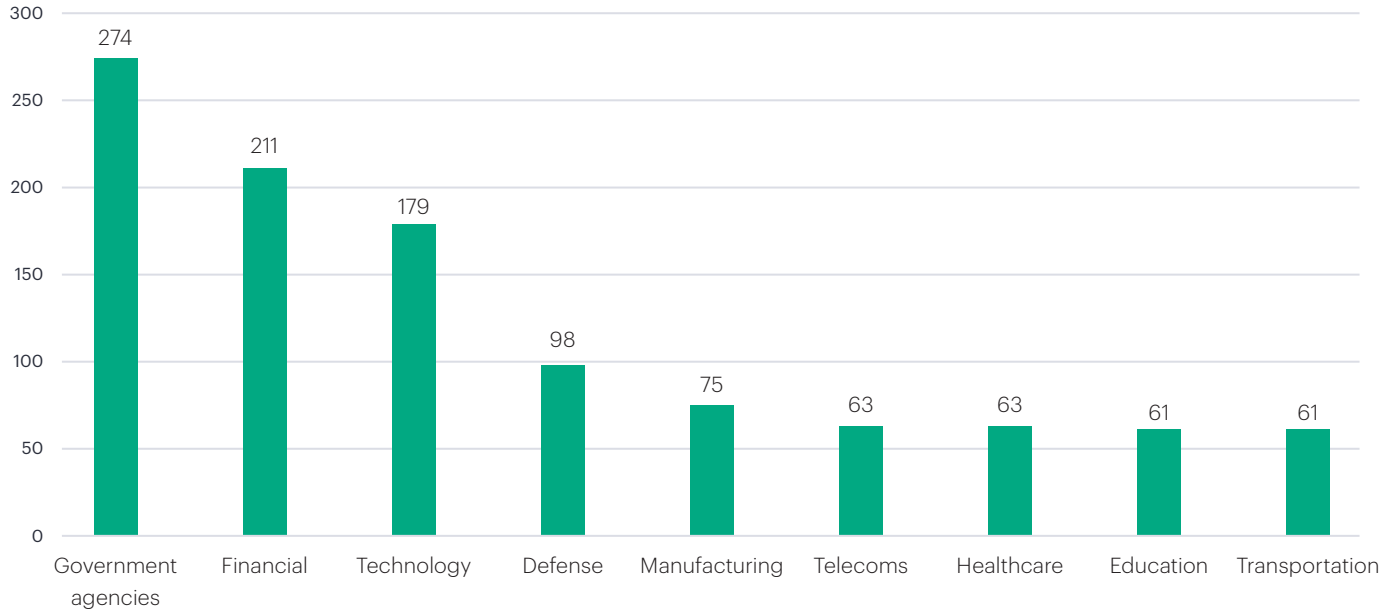
The bottom line is that the global threat landscape in 2025 was defined by a sophisticated, fast-moving adversary ecosystem. Defending against it demands matching the attackers' agility, efficacy, and strategy with an organization's own. This HPE Threat Labs report is a call to action for enterprises to adopt integrated—not bolt-on—AI-native networking security defenses, underscoring the need for comprehensive detection and mitigation practices alongside proactive, pervasive cyber hygiene and education.

Section 2

2025 key findings

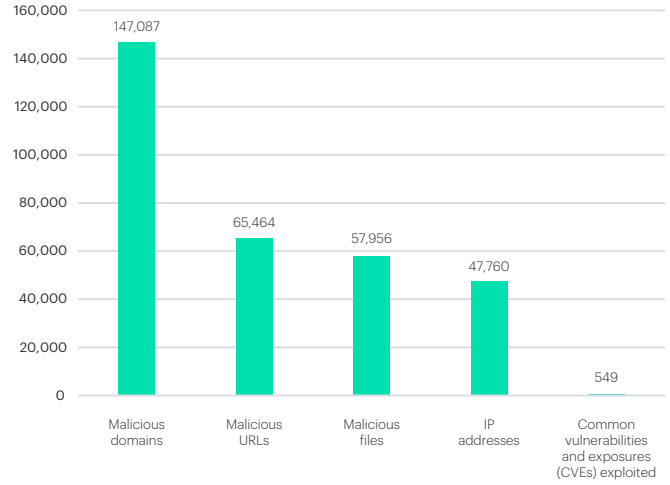
— Between January 1 and December 31, 2025, government organizations worldwide faced the highest number of threat campaigns, with 274 attacks targeting various federal, state, and municipal bodies. The finance and technology sectors followed closely with 211 and 179 campaigns, respectively, reflecting attackers' interest in high-value data for financial gain. The defense sector experienced 98 campaigns, while the manufacturing and telecommunications sectors recorded 75 and 61 campaigns, respectively, primarily driven by targeted espionage and data theft operations.

Top sectors targeted by threat campaigns in 2025

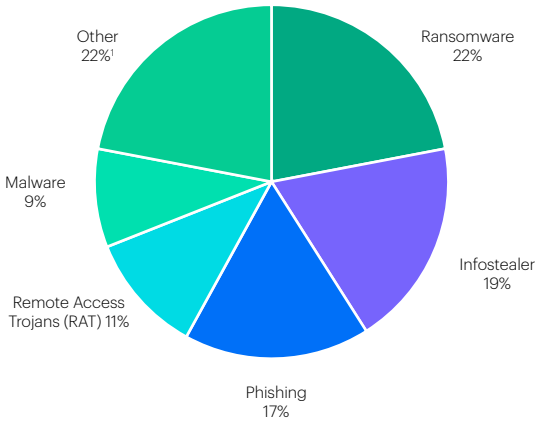


— From the 1186 threat campaigns reported, HPE Threat Labs characterized a vast array of attacker tools and infrastructure, underlining both the large scale and diversity of these campaigns.

Observed malicious artifacts by category

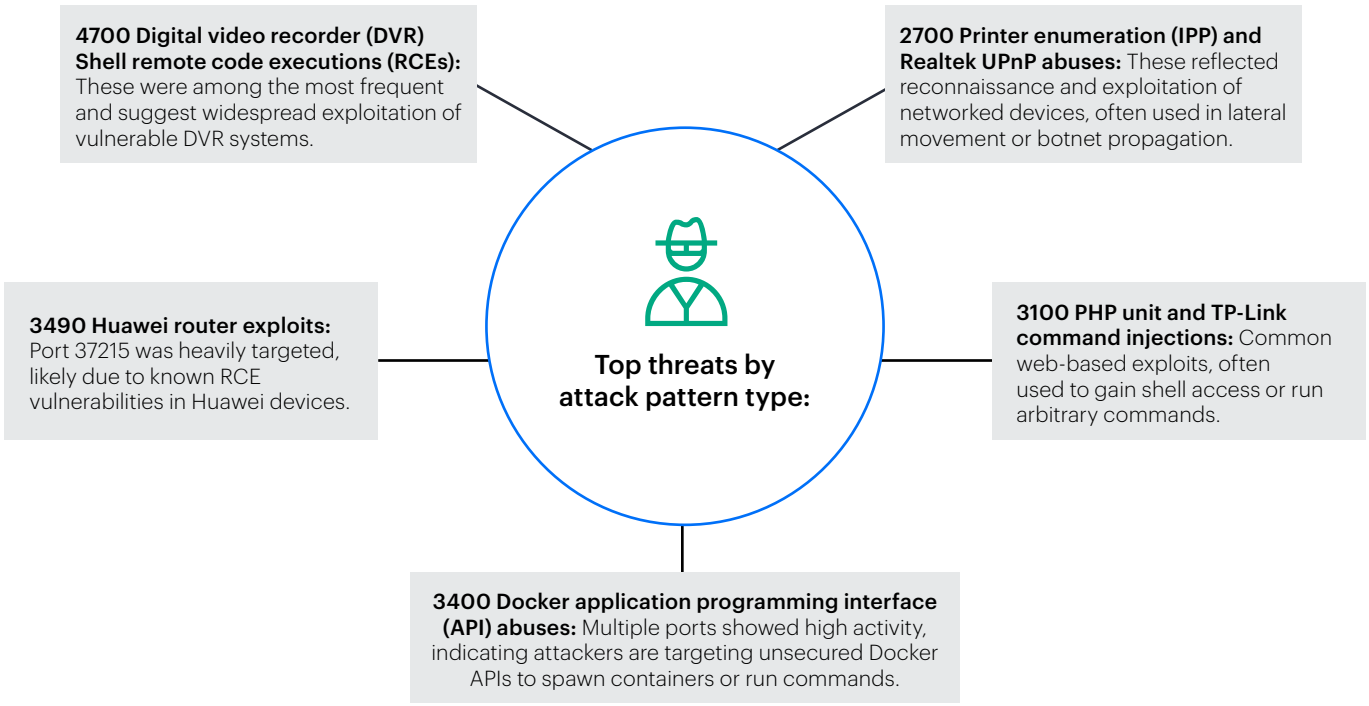


Distribution of campaign types



[1] The **other** category includes campaigns that couldn't be clearly attributed to a specific sector, often due to generic or ambiguous descriptions.

— Throughout 2025, HPE Threat Labs deception network infrastructure recorded 44.5 million connection attempts originating from 372,800 unique source IPs, illustrating the scale and diversity of internet-facing threats. Remarkably, among these, 36,600 requests matched known attack signatures, originating from only 8,200 distinct source IPs targeting just five destination IPs. These findings highlight the concentration of malicious traffic on vulnerable services and the persistent probing behavior of threat actors across various regions.



— Among the 549 CVEs observed in 2025, the top five stood out not just for their volume, but because each was published by the National Institute of Standards and Technology (NIST) several years ago. This development serves as a powerful reminder that while often time-consuming, patching vulnerabilities is critical and ultimately worthwhile.

Top 5 CVEs exploited in deception network data

01 **CVE-2017-17215**—Huawei HG532 Remote Code Execution

02 **CVE-2014-8361**—Realtek SDK UPnP SOAP Command Injection

03 **CVE-2023-1389**—TP-Link Archer AX21 Command Injection

04 **CVE-2017-9841**—PHPUnit Remote Code Execution

05 **CVE-2023-26801**—LB-Link Routers Command Injection

— Geolocation telemetry from HPE Threat Labs revealed that the United States, Seychelles, and China led in the volume of attacker/scanner IPs. The presence of Seychelles, a small African nation, alongside major countries can be attributed to its bulletproof service providers. Continue reading to understand how these providers contribute to Seychelles' prominence in this area.

Top threat actor countries by source IP count

1	2	3	4	5	6
United States	Seychelles	China	Germany	United Kingdom	Russia

Section 3

Emerging threats and notable trends

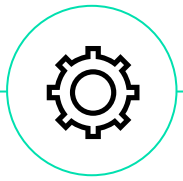
1. Organized cybercrime is rapidly evolving and escalating

Insight: Cybercrime cartels in 2025 **operated with an increasingly sophisticated level of organization, mirroring Fortune 500 companies in structure and efficiency while demonstrating a keen understanding of modern workplace applications and documents**. They prioritized strategic planning and encompassed **specialized teams and dedicated researchers**.

Case in point: The **PXA Stealer** malware came with **built-in Telegram integration**, enabling criminals to coordinate and share stolen data in real time. AI-powered deepfake and vishing attacks are on the rise, as threat actors increasingly target the financial sector through generative artificial intelligence (AI) tools that reduce the effort to craft believable social engineering. Furthermore, the top 2025 CVEs reported in the wild are each linked to Microsoft SharePoint, indicating a deep understanding of commonly used workforce applications. Meanwhile, the group behind **Akira ransomware** conducted extensive research on **VPN vulnerabilities** to plan their intrusions.

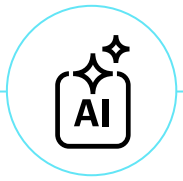
Such well-run operations reflect professional and systematic operations, dispelling the conventional assumption that threat actors primarily operate as lone wolves or with a sparse understanding of ubiquitous modern workforce tools.

What happened: HPE Threat Labs observed that multiple large cybercriminal rings function like businesses, leveraging emerging generative AI tools and exploiting vulnerabilities with extreme precision.



Business operations of crime:

One striking example was how data-stealing malware dubbed **PXA Stealer** was integrated with Telegram. Once PXA infected a victim's machine, it automatically **sent stolen passwords and files to a private Telegram channel**. This process acted like an industrial assembly line. As soon as the data was taken, the attackers could quickly package it for sale or ransom. The process was slick, seamless, and fast, mirroring how a company dashboard would track and process sales in real time.



AI-powered deepfakes and vishing:

Adversaries leveraged generative AI to produce synthetic voices and deepfake videos for executive impersonation fraud. With generative AI accelerating scale and accuracy, threat actors can clone a voice from short audio samples and carry out persuasive, live interactions that bypass simple **knowledge-based** checks. The impact is twofold: Higher success rates for business email compromise (BEC) and fraud, as well as increased difficulty for human operators to detect deception.

Targeted research and development (R&D) by hackers:

The **Akira ransomware group** exemplified a professional approach to R&D. Before attacking, their members **researched VPN weaknesses** in target organizations' infrastructure. By understanding which VPN systems a company was using, the group tailored its attack tools, which is analogous to a company conducting market research before launching a product. This preparation paid off with more successful breaches and rapid deployments of ransomware once inside.

Scale and efficiency:

Top cybercrime groups launched **1186 distinct campaigns between January 1 and December 31, 2025**. They often **moved faster and with better coordination than their victims' incident response teams**. Attackers also recycled techniques across victims, learning from each attack, much like a business refining its operations.

Why it matters:

Threat actors are more sophisticated and organized than ever before. Today's big hacking crews have C-suite (founders and leaders), **department leads** (i.e., experts in malware, finance), as well as **negotiation support** (for ransom payments). This **professionalization of cybercrime** means attacks are more predictable in execution, yet harder to disrupt, because taking down one part of the criminal operation is like trying to shutter a single branch of a franchise. As threat actors automate their operations, defenders must match this speed with AI-native protection, detection, and response capabilities that can consistently identify and neutralize threats faster than human operators alone.

What enterprises can do:

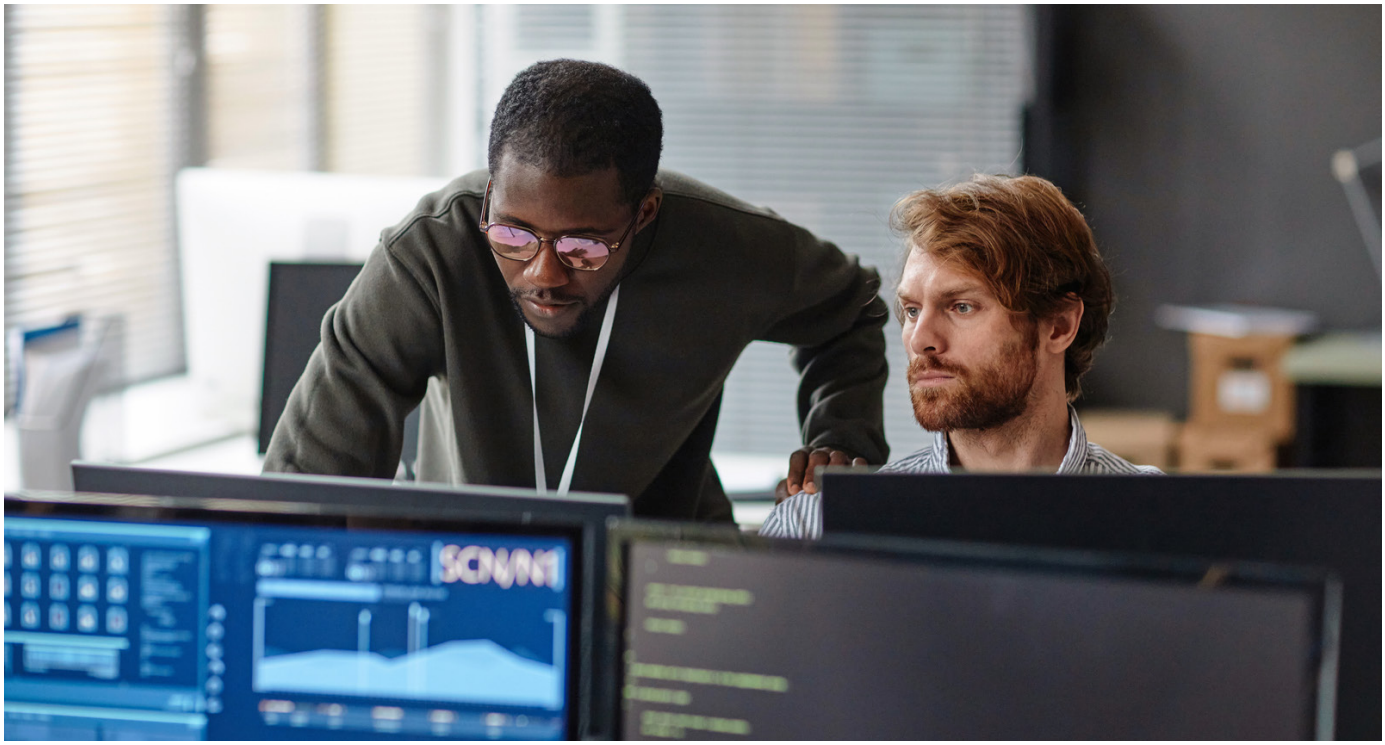
In practice, these developments call for equally organized countermeasures, including intelligence-sharing consortia, faster decision cycles, and proactive threat hunting that works in concert with network-wide AI-native mitigation tools. Mitigation for vishing and deepfake attacks requires strict verification processes for voice/phone requests, as well as awareness training that features synthetic media scenarios. Enterprises must treat these criminal enterprises as formidable competitors and invest in integrated AI-native network security tools and workflows that can counter automation with more sophisticated automation.

The deployment of AI-native anomaly detection on internal network traffic can help flag unusual behaviors (i.e., a normally home-bound device suddenly trying to access a control system in real time). In practical terms, enterprises should:

(a) Harden authentication through multifactor authentication (MFA), adopt strict password policies, and monitor for credential dumps to make spear-phishing and brute force attacks less effective;

(b) Segment networks so that even if one user or device is breached, an attacker can't freely roam critical systems; and

(c) Closely monitor and filter traffic from unmanaged endpoints (i.e., require authenticated access for all remote connections and scan those sessions for threats).

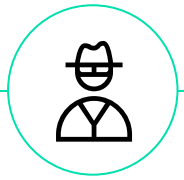


2. State-sponsored threats are zeroing in on critical infrastructure

Insight: State-backed threat actors unleashed consistent **campaigns against government and critical infrastructure globally** in 2025. Government agencies experienced **274 separate cyber campaigns, representing the highest volume of targeting observed in any sector**. These campaigns often blended stealth and ingenuity. For example, **Pakistan-linked APT36** infiltrated Indian critical infrastructure using a **Poseidon** backdoor malware.

Notably, these **sophisticated attacks often succeeded through compromised consumer devices** (i.e., hijacking home-office routers or using personal gadgets as stepping stones). As a result, these attacks fostered **an interconnected threat landscape from household networks up to critical systems**.

What happened: State-sponsored groups focused on critical infrastructure, aiming to disrupt government services and steal sensitive data. Attack vectors included spear-phishing high-value officials, deploying custom malware, and exploiting vulnerabilities in widely used software.



Government attacks:

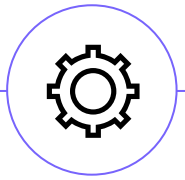
2025 saw threat campaigns targeting federal, state, and local government entities around the world at a higher-than-average level of activity. These threat campaigns ranged from attempts to breach energy grids to intrusions into municipal IT systems.

Tactics and techniques:

Adversaries employed advanced tools such as **backdoor malware (i.e., Poseidon)** and exploited supply chain weaknesses. Many attacks were opportunistic but coordinated, using easily compromised Internet of Things (IoT) devices or home-office systems to bypass hardened perimeters.

Case spotlight:

APT36, a threat group tied to Pakistan, **systematically compromised Indian government systems** using **Poseidon** malware. The group sent seemingly benign documents that, once opened, installed Poseidon to gain persistent remote access. This access allowed them to hop from a bureaucrat's laptop on a home network into critical government servers.



Impact:

These breaches exposed national security data and highlighted how a hack on a **home device can swiftly escalate into a national crisis**.

Why it matters:

This surge in state-sponsored attacks underscores the need for **immediate patching of perimeter systems such as VPN terminators and SharePoint servers, coupled with AI-native anomaly detection and threat hunting to catch and flag sophisticated intrusions**. Critical infrastructure is facing unprecedented pressure, with attacks rising year-over-year since 2015 and exponentially so since 2022. **State-sponsored cyberattacks on energy, transportation, and government systems are now frequent and coordinated**. The growing connectivity of operational and personal devices means an intrusion can originate from almost anywhere, even from a staffer's smart home network. This attack pattern demonstrates why traditional perimeter defenses are insufficient. Organizations need AI-native networking that can detect anomalous behavior and lateral movement in real time, regardless of entry point.

What the public sector can do:

To counter the scale and stealth of state-sponsored campaigns, government agencies must prioritize resilience at both the perimeter and endpoint level. Action steps toward fostering this resilience include hardening remote access infrastructure, enforcing strict patching protocols for widely used platforms such as VPNs and SharePoint, as well as deploying AI-native anomaly detection to identify lateral movement across hybrid environments. Given the increasing use of compromised consumer devices as entry points, agencies should extend security policies to include remote work setups and unmanaged endpoints. Additionally, applying zero trust principles can help contain intrusions before they escalate into systemic disruptions. These measures are essential to protect critical services and national infrastructure from adversaries that now operate with nation-state resources.

3. Why does a small African country have the second-highest threat actor IP count?

Insight: HPE Threat Labs' geolocation telemetry revealed that while the United States, Seychelles, and China lead in volume, attacker infrastructure in 2025 was globally distributed and has a worldwide reach. This distribution includes cloud-hosted environments, compromised consumer devices, and botnet nodes.

However, Seychelles is particularly noteworthy. Despite being the smallest country in Africa, with a population of just over 120,000, it stands out alongside much larger and more populous countries such as the United States, China, Germany, the United Kingdom, and Russia.

Top countries by source IP count

1	2	3	4	5	6
United States = 3.75	Seychelles = 1.5	China = 1.25	Germany = 1	United Kingdom = 0.75	Russia = 0.5

Why it matters:

This finding underscores the truly borderless nature of cyber threats. A small, neutral country can inadvertently become a hub for cybercrime if conditions such as cheap hosting and weak regulatory oversight are favorable. For defenders, it's a caution against relying solely on geolocation-based blocking or trust. Malicious traffic can originate from data centers anywhere, so security teams must use threat intelligence and behavioral indicators, not just IP location, to identify threats. In the case of Seychelles, the surge in attacker IPs is linked to bulletproof hosting services operating there. These providers exploit jurisdictional loopholes—with servers offshore and enforcement difficulties—and offer criminals a safe haven.

What enterprises can do:

At a minimum, awareness of this phenomenon is crucial for enhancing risk assessments and updating response playbooks. Efforts to crack down on abuse-tolerant hosts through legal action or collaborative takedowns can significantly reduce the attackers' operating space. In the meantime, companies should ensure their security solutions don't presume any location is inherently safe—even traffic coming from what looks like an innocuous island or an atypical country for business could be malicious. Attackers' infrastructure can hide in plain sight, anywhere on the globe. A robust defense strategy means casting a wide net by leveraging global insights to filter out known malicious IPs and continuously analyzing network traffic for suspicious patterns—no matter the source.

Section 4

Additional findings

HPE Threat Labs' deception network data from January 1 to December 31, 2025, revealed attackers' persistent reliance on weak and commonly used passwords and usernames. This trend illustrates the critical need for strong password policies, disabling unused accounts, hardening access to privileged credentials, as well as deploying MFA to mitigate unauthorized access risks.

Telemetry from HPE Threat Labs also revealed a varied malware family landscape. This telemetry points to the fact that obfuscated or emerging malware evading signature-based detection is ubiquitous. The Dynamer, Eldorado, and Variant families remain prevalent, while Emotet continues to feature as a major banking trojan and botnet loader due to its modular, evasive design. The pattern uncovers a systemic failure. Defenders know what malware families are and how to protect against them, yet critical infrastructure remains vulnerable to decade-old strains.

Section 5

Conclusion and recommendations

Cybersecurity is now a battle on all fronts, pitting enterprises and organizations against adversaries ranging from nation-states to highly organized criminal enterprises. No organization can afford complacency. Effective defense is measured not by the sheer number of tools, but by how decisively threats are stopped across an organization's entire network fabric.

HPE Threat Labs recommends these strategies:

Cross-sector, cross-team defense collaboration: Just as attackers have diversified, defenders should break down silos. By sharing threat intelligence between industries (i.e., finance, healthcare, government) and between networks, cybersecurity teams can illuminate patterns and predict attackers' next moves.

Cybersecurity industry-wide threat intelligence sharing: It is clear that no single security vendor has visibility into all cyberattacks. Most organizations deploy networking and security solutions from many different vendors. Therefore, it is imperative that security vendors share threat intelligence in near real-time to accomplish their common mission of defending their customers. HPE is a proud active member of the Cyber Threat Alliance, where security industry heavyweights come together to share threat intelligence.

Strengthen the weakest links: Home devices and third-party tools are increasingly used as entry points, so organizations must extend security beyond their walls. Secure home Wi-Fi kits for employees, strict supply chain audits, and zero trust principles that assume any device could be compromised are now table stakes.

Adaptive security posture: Treat cybersecurity as dynamically as the adversary does. Conduct regular fire drills against ransomware scenarios and invest in AI-native networking platforms such as HPE Aruba Networking Central and HPE Mist, which leverage data-rich, insight-driven machine learning to detect anomalies, predict threats, and automate mitigative responses.

Key takeaways for defenders:

Close the front door: Patch perimeter systems, especially VPNs, SharePoint, and consumer-grade routers, to shut down frequently exploited entry points.

Limit what attackers can see and do: Strengthen authentication and segment networks with zero trust principles to reduce brute-force success and restrict adversary movement.

See more, respond faster: Boost visibility with threat intelligence from HPE Threat Labs, deploy deception networks, and use AI-native detection tools to catch lateral movement and automate responses.

The story of 2025 is not one of isolated incidents, but of a globally connected, technically proficient, AI-enabled, and rapidly evolving adversary ecosystem. Successful defense against this ecosystem demands more than vigilance. Instead, a robust defense necessitates next-generation firewalls, automation, advanced security services, and cloud-based threat prevention to protect against the adversarial techniques and indicators outlined in this report through existing signatures, behavioral detections, and proactive blocking of malicious infrastructure. **That's why HPE embeds this real-time threat intelligence directly into its AI-native networking security portfolio—so defenders can act faster, smarter, and with deeper insights than ever before**.

Section 6

Methodology

HPE Threat Labs used multiple sources to compile the contents of this report. The majority of statistical information is derived from our Juniper Advanced Threat Prevention Cloud subscribed customer telemetry and our private network of honeypots. We use multiple types of honeypots (TCP, SSH, SMB), which are distributed around the world. We sometimes also augment our own data with context and statistics from open-source threat intelligence repositories, as well as third-party industry associations we are a member of.

The data in this report covers the period of time between January 1, 2025, and December 31, 2025.

Section 7

Glossary of terms

AI-native: A system that is built from the ground up with AI at its core

Attack signatures: A unique, recognizable pattern or set of rules identifying a specific cyberattack

Common vulnerabilities and exposures (CVEs): A list of publicly disclosed computer security flaws

Deception network infrastructure: A defense strategy that uses fake, isolated assets placed within a real network to lure attackers, detect breaches early, and gather threat intelligence without impacting production systems

Docker API abuses: A security vulnerability that stems from misconfigured or exposed Docker remote APIs and sockets, which allow attackers to gain unauthorized access and implement commands with root privileges on the host system

DVR shell RCEs: A specific type of security vulnerability that allows attackers to run arbitrary code in the web management interfaces (or shells) of certain DVRs, connecting to them over public or private networks

Hostile domains: A network or domains on the internet that cannot be trusted and are likely being used for malicious activities

Infostealer: A type of malicious software designed to covertly collect sensitive data from an infected device and send it to cybercriminals

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

Malware domains: Website addresses used by cybercriminals to spread malware, conduct phishing, or host scams, often by mimicking legitimate sites through typosquatting or creating nonsensical names through algorithms (DGAs) to trick users into downloading viruses, ransomware, or stealing data

Malware files: Malicious software programs designed to harm devices, steal data, or disrupt systems

Malware IP address: An internet address linked to known malicious online activity, such as hosting viruses, sending spam, commanding botnets, or running phishing sites, and is typically blocked by security systems to prevent threats from reaching your network

Malware URLs: A malicious web address designed to trick users into visiting dangerous sites that can infect devices with viruses, spyware, ransomware, or steal personal data

Patch: A software update designed to fix vulnerabilities, bugs, or weaknesses in computer programs, operating systems, or applications, preventing them from being exploited by cyberattackers to cause data breaches, system failures, or other harm

Phishing: The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers

Command injection: A type of vulnerability exploitation method where the attacker submits specifically crafted input into an existing interface to trigger the vulnerability and compromise the system

Ransomware: Malicious software (malware) that blocks access to your computer files or system, demanding a ransom payment (usually crypto) for their release, often through encryption of your files, displaying a ransom note with payment instructions

Remote Access Trojans (RATs): A type of malware that allows a cybercriminal to secretly gain complete, unauthorized control over an infected device from a remote location

Learn more at

HPE.com/HPE-Threat-Labs

Visit HPE.com

Chat now

a50014950ENW

HEWLETT PACKARD ENTERPRISE

hpe.com