May 26 – June 1, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- IT management software company ConnectWise confirmed that a sophisticated nation-state cyberattack had compromised its environment, affecting a limited number of customers using its ScreenConnect remote access tool. The company launched a forensic investigation, patched the vulnerability, and implemented enhanced monitoring measures. While no further malicious activity has been detected, ConnectWise has communicated with all affected customers and is coordinating with law enforcement.
- German sportswear giant Adidas has disclosed that customer data was accessed in a cyberattack. According to the firm's statement, the attack targeted a third-party customer service provider, and the data includes contact information of customers who have previously contacted the customer service helpdesk of Adidas.
- Victoria's Secret, the global lingerie retailer, has taken down its website following a security event that indicated a potential ransomware attack. In response to media inquiries, the company said it was following its security response protocols and has engaged experts to restore services securely. So far, no ransomware gang has claimed responsibility.
- US based software developer MathWorks, which develops MATLAB, has disclosed that it had suffered a ransomware attack. The incident has affected the company’s IT systems, as well as some customer-facing applications and internal staff services.
- LexisNexis Risk Solutions reported a data breach that exposed personal information of more than 364,000 individuals. The breach, discovered on April 1st, involved data held on GitHub, a third-party platform used by LexisNexis for software development. Although systems were not compromised, the exposed data included names, contact information, social security numbers, driver’s license numbers, and dates of birth.
- Crypto platform Cork Protocol suffered a significant security breach, resulting in the theft of over $12 million worth of cryptocurrency. The attacker exploited a vulnerability in the platform's smart contract logic. In response, Cork Protocol has paused all contracts and trading activities while investigating the incident.
- Russian internet provider ASVT experienced a major distributed denial-of-service (DDoS) attack, resulting in prolonged internet outages for tens of thousands of residents in Moscow and surrounding areas. The attack disrupted ASVT’s mobile app, website, and customer accounts, affecting services such as remote work, card payments, and internet-based intercom systems. The attack was attributed to the IT Army of Ukraine, a pro-Kyiv hacker collective, though the group has not claimed responsibility.

VULNERABILITIES AND PATCHES

- Google's has released patches to two high-severity security vulnerabilities. CVE-2025-5063, a use-after-free flaw in Compositing, and CVE-2025-5280, an out-of-bounds write in the V8 JavaScript engine—alongside several medium-risk issues affecting APIs like Background Fetch and FileSystemAccess. While no active exploits have been reported, Google has restricted technical details to prevent attacks before widespread patching.

- Sucuri's monthly roundup highlighted several critical vulnerabilities in popular WordPress plugins, including a privilege escalation flaw in OttoKit and an unauthenticated SQL injection in Popup and Slider Builder by Depicter, both affecting over 100,000 installations. Other notable issues involved cross-site scripting (XSS) vulnerabilities in plugins like Newsletter and SureForms, emphasizing the ongoing need for prompt updates and robust security measures to protect WordPress sites from automated attacks.

- Wordfence's weekly vulnerability report included 160 vulnerabilities across 108 WordPress plugins and 44 themes. These issues encompassed various security flaws, including cross-site scripting (XSS), SQL injection, and privilege escalation vulnerabilities. Wordfence emphasized the importance of promptly updating affected plugins and themes to mitigate potential risks.

THREAT INTELLIGENCE REPORTS

- Check Point Research comments on the international law enforcement operation involving Europol, the FBI, and Microsoft, which disrupted the infrastructure of the Lumma Infostealer. The takedown of the prominent malware-as-a-service platform led to the seizure of approximately 2,500 domains and the wiping of Lumma's main server through an exploited vulnerability in Dell's iDRAC. Despite this, Lumma's developers quickly claimed to have restored operations, with Russian-hosted command-and-control servers remaining active and stolen data logs continuing to surface online. The operation also aimed to undermine trust within the cybercriminal community. While the technical impact was significant, the long-term effectiveness of the takedown may hinge on the reputational damage inflicted on Lumma's brand.

- Threat Intelligence researchers have uncovered a cyber-espionage campaign by China-affiliated group APT41, which used a malware called TOUGHPROGRESS delivered via spear-phishing. The attackers disguised malicious payloads as images and leveraged Google Calendar for command-and-control, targeting sectors such as government, media, and automotive.

- Cybersecurity researchers identified a new Linux-based botnet named PumaBot, which targets IoT devices by brute-forcing SSH credentials. Unlike typical botnets, it uses a C2 server to select targets and installs a backdoor to steal credentials. The botnet notably targets surveillance and traffic camera systems, as indicated by its search for the "Pumatronix" string during attacks – a traffic camera system manufacturer.