cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- SimonMed Imaging, one of the largest diagnostic imaging companies in the US, has been breached by Medusa ransomware group, resulting in the theft of over 212 GB of sensitive data from its servers. The group demanded a $1 million ransom in Bitcoin and exposed private information of more than 132,000 individuals, including patients and employees.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.MedusaLocker.ta.; Ransomware.Wins.MedusaLocker.*; Trojan.WIN32.Medusalocker.*)*

- US-based publishing giant Lee Enterprises has been a victim of cyber-attack that disrupted its print services, as well as impacted the availability of its online publications. The nature and the extent of the attack are yet to be disclosed.

- The University of Notre Dame Australia has experienced a cyber-attack that resulted in the theft of 62.2 GB of data, including student medical documents, employee and student contact details, and confidential documents. The Fog ransomware group has claimed responsibility for this attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.FOG.)*

- The Sault Ste. Marie Tribe of Chippewa Indians has experienced a ransomware attack that resulted in the shutdown of critical services, including casinos, health centers, and various businesses. The attack has led to the cancellation of medical appointments, suspension of gaming operations, and disruption of administrative functions, affecting over 44,000 tribal members.

- US-based demolition and environmental services company Empire Group was hit by a ransomware attack that resulted in the exfiltration of sensitive data, with sample screenshots published on the attackers' dark web portal. The Lynx ransomware group has claimed responsibility for the attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (
  Ransomware.Win.Lynx.; Ransomware.Wins.Lynx.B)*

- Unimicron Technology, a Taiwan-based printed circuit board manufacturer, was breached by an unknown ransomware group at the end of January 2025. The incident led to disruptions in their operations, affecting production schedules.

- Papua New Guinea's Internal Revenue Commission has been a victim of a cyber-attack that compromised sensitive data belonging to millions of individuals and businesses. The attack also led to disruptions in critical systems, affecting both online services and internal operations.

VULNERABILITIES AND PATCHES

- Microsoft's February 2025 Patch Tuesday addresses 67 different vulnerabilities, including three listed as critical RCE risks. Two proprietary vulnerabilities, a heap-based buffer overflow in the Windows Ancillary Function Driver (AFD) and an elevation of privilege (EoP) flaw in the Windows Storage service, have been observed being exploited in the wild. Furthermore, a zero-day NTLMv2 hash disclosure vulnerability, security feature bypass in Microsoft Surface devices, and a critical RCE vulnerabilities in Windows LDAP server and DHCP client are also being addressed.

- Newly discovered authentication bypass vulnerability CVE-2025-0108 in Palo Alto's next-generation firewalls is now under active exploitation. The vulnerability exists due to discrepancies in how Nginx and Apache handle URL requests, which could compromise system integrity and confidentiality. This vulnerability does not grant full Remote Code Execution (RCE), yet it poses risks to data integrity and confidentiality within PAN-OS.

  Check Point IPS provides protection against this threat *(Palo Alto Networks PAN-OS Authentication Bypass (CVE-2025-0108))*

- Adobe has released patches addressing CVE-2025-24434, a critical improper authorization vulnerability affecting Adobe Commerce and Magento Open Source versions 2.4.8-beta1 and earlier. This flaw allows unauthenticated attackers to escalate privileges, potentially leading to unauthorized access and remote code execution without user interaction. Affected users are advised to apply the isolated patches provided by Adobe promptly.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released January 2025's Most Wanted Malware report, highlighting the dominant position of FakeUpdates malware. Recently, FakeUpdates has been used as an infection vector by RansomHub ransomware group. Among top mobile malware threats, Anubis remains at the top, followed by AhMyth and Necro.

- Check Point Research has detected a Valentine's Day-themed phishing campaign targeting users through emotionally manipulative messages. The research identified a substantial rise in registration of malicious domains prior to the holiday and malicious emails posing as love-related offers.

- Google Threat Intelligence Group (GTIG) addresses the escalation of financially motivated cybercrime, revealing its impact on national security. It describes how state-linked entities tap into cybercrime capabilities for their goals, exemplified in the case of Russian military intelligence leveraging tools from cybercrime communities.

- Researchers analyzed a campaign targeting multiple Russian companies, identifying the use of Merlin and Loki malware by the newly named "Mythic Likho" group. The attackers use the Mythic framework with custom agents to steal confidential information from victims, employing a flexible infection chain and malicious emails disguised as legitimate communications.