CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The FBI and CISA issued a joint statement detailing a major Chinese cyber-espionage campaign targeting U.S. telecommunications infrastructure, led by the APT group Salt Typhoon. This operation compromised networks to steal call records, intercept communications involving government and political figures, and access data linked to U.S. legal requests. This statement follows confirmation of breaches affecting multiple telecom companies, including AT&T, Verizon, and Lumen Technologies, in October 2024. T-Mobile has also confirmed being a victim of this campaign, stating that Salt Typhoon infiltrated its network using vulnerabilities like those in Cisco routers to spy on senior government and national security officials. However, T-Mobile reported no significant harm to its systems or compromise of customer data.

- Hungary's Defense Procurement Agency (VBÜ) has confirmed a cyberattack by the INC Ransomware group. The group claims to have accessed and encrypted the VBÜ's data, including documents on military procurements, and are demanding a $5 million ransom. The Ministry of National Defense stated that VBÜ does not store sensitive military data and is currently investigating the breach.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat

- The City of Sheboygan, Wisconsin updated that it has recently experienced unauthorized access to its network by a ransomware attack. In response, the city has secured its systems and is conducting a thorough forensic investigation with cybersecurity experts to assess the incident's scope. Currently, there is no evidence that sensitive personal information has been compromised, however, the city has been dealing with technology outages since late October.

- American Associated Pharmacies (AAP), managing over 2,000 U.S. pharmacies, was reportedly targeted by the Embargo ransomware group, which claims to have stolen 1.469 TB of data and encrypted files. Embargo claims AAP paid $1.3 million for decryption and now faces another $1.3 million demand to prevent data exposure. While AAP has not confirmed the attack, it reset user passwords and advised credential updates.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Embargo, Ransomware.Wins.Embargo)

- A Distributed Denial of Service (DDoS) attack disrupted credit card readers across Israeli gas stations and supermarkets, causing widespread payment processing issues. Credit Guard, the company responsible for the readers' cybersecurity, identified the attack and restored services after approximately one hour. The attack is linked to the hacktivist group Anonymous for Justice.

VULNERABILITIES AND PATCHES

- Microsoft published their Patch Tuesday update, fixing 89 vulnerabilities, including four zero-days. Two of the zero-day vulnerabilities CVE-2024-43451 (NTLM Hash Disclosure Spoofing Vulnerability) and CVE-2024-49039 (Windows Task Scheduler Elevation of Privilege Vulnerability) are actively exploited in the wild.

- Palo Alto Networks has identified a critical zero-day vulnerability (PAN-SA-2024-0015) in the management interfaces of its Next-Generation Firewalls (NGFW). This flaw, which allows unauthenticated remote code execution, is currently being exploited in attacks targeting internet-exposed management interfaces. The company advised multiple security measures while patches are being developed, including restriction of access to these interfaces by permitting connections only from trusted internal IP addresses.

- WordFence identified a critical authentication bypass vulnerability in the Really Simple Security plugin. This flaw allows unauthenticated attackers to gain administrative access to WordPress sites when the plugin's two-factor authentication feature is enabled. The plugin has pushed forced updates to patch the vulnerabilities, but unmaintained websites might still be vulnerable.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released October 2024's Most Wanted Malware, highlighting a significant rise in infostealer malware during October, with AgentTesla and Lumma Stealer dominating the list of prevalent threats. These malwares are often spread through phishing emails and malicious websites, targeting sensitive data such as login credentials and financial information. The report also mentions the new version of Necro mobile malware that has emerged as a significant threat, ranking 2nd among mobile malwares.

- Check Point Research revealed the latest activity during 2024 of a Hamas-linked APT group dubbed WIRTE. The group continued its espionage activity against Middle Eastern countries and has expanded its activity beyond espionage to conduct disruptive attacks against Israel. The report connects the custom malware used by the group and SameCoin, a wiper malware targeting Israeli entities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (APT.Wins.Wirte.ta.A/B/C/D/E/F; ransom.win.honey, infostealer.win.blackguard.d)

- Check Point Research reports on WezRAT, a custom modular RAT tool used by Iranian threat group Emennet Pasargad, following the advisory published by the FBI, the US Department of Treasury, and the Israeli National Cybersecurity Directorate. The group has been targeting Israel, France, Sweden and the United States lately. In recent campaigns, WezRAT was modified to include additional infostealer capabilities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Behavioral.Win.FakeChrome.B, Trojan.Wins.FakeUpdater.A)