TOP ATTACKS AND BREACHES

- MITRE Corporation disclosed a security event that occurred in January 2024. The attack, which is linked to Chinese APT group UNC5221, involved exploitation of two zero-day vulnerabilities in Ivanti VPN products. The attacker conducted session hijacking and lateral movement across MITRE's NERVE network, which is a collaborative network used for research, development, and prototyping.

- Frontier Communications reported a cyberattack involving unauthorized access to its IT systems, which led to operational disruptions. The attack, likely orchestrated by a cybercrime group, compromised personally identifiable information. Efforts to contain and resolve the incident are ongoing.

- The United Nations Development Programme (UNDP) was targeted by the 8Base ransomware gang, resulting in data exfiltration from a locally hosted server. The breach involved human resources and procurement information. The agency emphasizing its refusal to pay the attackers' demanded ransom.

- Cherry Health, a Michigan-based healthcare provider, has suffered a significant ransomware attack impacting its operations. The attack encrypted vital data and disrupted clinical services, forcing the organization to revert to manual operations. The responsible ransomware group has not yet been publicly identified, and the extent of data exfiltration is known to affect at least 185,000 people.

- A ransomware attack, attributed to the LockBit ransomware group, recently targeted Tyler Technologies, a third-party provider to Washington D.C. city's Department of Insurance, Securities and Banking (DISB), leading to significant data compromise. The incident disrupted agency operations, and LockBit threaten to leak 1GB out of the 800GB of allegedly stolen data to pressure the agency into paying the ransom.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.LockBit.ta; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*

- Researchers have unveiled a sophisticated phishing campaign by financially motivated group Fin7, targeting IT staff within an America-based automaker company. The attacks, which targeted a major multinational car maker, utilized carefully crafted spear-phishing emails aimed at deploying the Anunak backdoor malware for financial gain and data theft.

- Microsoft has reported a significant uptick in disinformation activities by Russian entities aimed at influencing US political dynamics. These efforts include the deployment of advanced AI tools to create and spread deepfake content, targeting both social media platforms and traditional news outlets, with the primary aim of sowing discord and manipulating public perception ahead of key political events.

VULNERABILITIES AND PATCHES

- Ivanti recently issued security updates to address multiple vulnerabilities in Avalanche. These vulnerabilities, ranging from medium to critical severity, pose risks such as information disclosure, command execution, and Denial-of-Service (DoS) attacks. The update includes two critical vulnerabilities, CVE-2024-24996 and c, which both originate from heap overflows.
- Oracle's latest Critical Patch Update for April 2024 addressed multiple vulnerabilities across a wide range of products. This update includes fixes for several high-severity vulnerabilities that could allow remote code execution, data leakage, and denial of service attacks if exploited.
- Researchers have discovered CVE-2024-20697, a high-severity Remote Code Execution (RCE) vulnerability affecting the Libarchive library in Windows systems. Exploitation of this flaw allows unauthenticated attackers to execute arbitrary code via crafted archive files, potentially taking control of affected systems. The vulnerability has been patched.
- Researchers have unveiled a critical vulnerability in the Forminator plugin, impacting over 300,000 WordPress websites. The flaw (CVE-2023-5674) could allow attackers to execute arbitrary code on affected sites, posing significant security risks. It's crucial for site administrators to update the plugin to the latest version to mitigate potential exploits.

THREAT INTELLIGENCE REPORTS

- Check Point Research identified a significant surge in phishing attacks targeting major tech giants Microsoft and Google. The spike observed in Q1 2024 primarily involved sophisticated phishing tactics aimed at compromising user credentials and infiltrating organizational networks.
- CISA, FBI, Europol's EC3, and NCSC-NL released a joint a #StopRansomware advisory for Akira Ransomware, detailing observed methods and impacts across North America, Europe, and Australia since March 2023. Since January 2024, the group has affected over 250 entities, notably targeting Windows systems and VMware ESXi virtual machines, and getting approximately $42 Million in ransom payments.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.
- Researchers have reported ongoing attacks targeting over 22,500 Palo Alto firewalls due to a critical vulnerability. The vulnerability (CVE-2023-0017), if exploited, allows unauthorized access and control over the network, posing significant risks to affected organizations. The urgency of the situation is underscored by active exploitation attempts, which necessitate immediate patches and heightened security measures by all users of the impacted Palo Alto firewall models.