cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Free, the second-largest telecom company in France, has been hit by a cyberattack resulting in unauthorized access to personal data associated with certain subscriber accounts. The incident surfaced following an attempted sale of stolen customer data on a cybercrime forum, impacting potentially up to 19 million customers. Although passwords and bank details were not compromised, Free is alerting affected users and has filed a complaint with local authorities.

- The California Superior Court has been impacted by a cyberattack resulting in widespread technical outages. The incident has disrupted access to court services, including public-facing applications and internal operations, affecting case management and public record systems.

- AEP, a German pharmaceutical wholesaler, suffered a ransomware attack leading to partial encryption of its IT systems, impacting medicine supplies to over 6,000 pharmacies. The company, headquartered in Bavaria, has disconnected affected systems and is working with external cybersecurity experts to address the incident.

- The Housing Authority of the City of Los Angeles (HACLA) has been targeted in a ransomware attack, with the Cactus ransomware gang claiming responsibility and alleging data theft of 861 GB, including personal, financial, and backup information. This incident marks the second cyberattack HACLA has faced in recent years, following an earlier breach by LockBit in 2023.

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

- Pro-Ukraine hacktivists “Ukrainian Cyber Alliance” allegedly launched a cyberattack on the parking payment system in Tver, Russia, as part of ongoing digital assaults amidst the conflict. The attack disrupted the city's payment infrastructure, allowing residents to park for free for nearly two days.

- The French Ministry of Labor and Employment has reported a cyberattack on a service provider for its Local Missions network, which supports individuals aged 16 to 25 with employment and training. The breach, which occurred in October 2024, potentially exposed personal data, including names, birthdates, nationalities, and contact information, of young people registered in the program. Financial details, social security numbers, and identity documents were not compromised.

- Interbank, a major Peruvian financial institution, suffered a data breach in which sensitive customer data, including financial information, was reportedly exposed. The breach led to the unauthorized disclosure of personally identifiable information and account details. Investigations are ongoing to determine the extent of the compromised information and potential vulnerabilities exploited.

VULNERABILITIES AND PATCHES

- Synology addressed two critical zero-day vulnerabilities (tracked together as CVE-2024-10443) discovered during the recent Pwn2Own Ireland 2024 competition. The flaws, dubbed RISK:STATION, affected Synology Photos and BeePhotos software and could allow remote code execution on exposed NAS devices. Patches were released within 48 hours due to the high risk of exploitation, urging users to update to secure their systems.

- QNAP has patched a critical zero-day SQL injection vulnerability (CVE-2024-50387), in its SMB Service, discovered at Pwn2Own Ireland 2024. The vulnerability was patched within a week, with updates available in SMB Service version 4.15.002 or later.

- A critical vulnerability in the AI Power Complete AI Pack WordPress plugin (CVE-2024-10392) is affecting approximately 10,000 WordPress websites. The flaw enables arbitrary file uploads, potentially allowing attackers to execute code on vulnerable sites.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published its September 2024 ransomware report, highlighting emerging trends in ransomware. Noted are the rapid rise of RansomHub, which accounted for 19% of ransomware victims this month, and a shift by groups like Meow towards data extortion over encryption. The report also shows Lockbit's decline in activity, following law enforcement actions.

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

- The FBI, U.S. Treasury, and Israel National Cyber Directorate have issued joint advisory detailing updated tactics by the Iranian group Emennet Pasargad, also known as Aria Sepehr Ayandehsazan (ASA). This group, active in influence operations targeting events like the 2024 Summer Olympics, has utilized advanced methods such as fictitious hosting resellers, IP camera content harvesting, and interest in AI resources for cyber-enabled information operations.

- Researchers have conducted a five-year investigation into multiple China-based APT groups, including Volt Typhoon, APT31, and APT41/Winnti, focusing on their sophisticated attacks against Sophos network perimeter devices. The threat actors developed and deployed advanced TTPs, such as rootkits, UEFI bootkits, and backdoored Java classes, to compromise devices and target high-value entities in the Indo-Pacific, including government and critical infrastructure sectors.

- Researchers have identified that the Chinese threat actor, Storm-0940, has been using stolen credentials obtained through password spray attacks to access targeted systems. The actor operates through a covert network to obfuscate its activities, enabling access to sensitive data across various sectors. This campaign highlights the persistent and sophisticated approach of Storm-0940 in leveraging credential-based tactics.