CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Halliburton, a leading U.S. oilfield services firm, was hit by a cyberattack that forced the company to take certain systems offline to contain the breach. Hackers gained access to some of the company's systems, prompting an ongoing investigation with the help of external contractors. No group has claimed responsibility for the attack.
- Microchip Technology, an American semiconductor manufacturer, reported a cyberattack that disrupted some of its servers and business operations. Upon detecting suspicious activity, the company isolated affected systems, shut down certain services, and initiated an investigation with external cybersecurity experts. The incident has impacted manufacturing, causing operations to run below normal levels, affecting the company's ability to fulfill orders. The full scope and impact of the attack remain unclear, and the identity of the attackers is unknown.
- The Oregon Zoo has disclosed that personal and payment information of more than 100,000 of the Zoo's visitors has been leaked. The threat actors had access to zoo's online payment platform for a period of more than 6 months, redirecting transactions from the zoo's online ticketing system and stealing full credit card details.
- Japanese car manufacturing giant Toyota has confirmed a third-party data breach of limited scope after a threat actor had leaked 240GB of data on underground cybercrime forums. Representatives have denied the threat actor's allegations that the company's U.S. branch was hacked.
- City officials in Columbus, Ohio, have warned crime victims and witnesses to remain vigilant after a ransomware gang leaked data stolen from the local prosecutor's office on the Dark Web. The Rhysida ransomware group, which had initially hit the city in July and demanded $1.9 million in Bitcoin, released 6.5 terabytes of data after the city refused to pay. The leaked information, which includes sensitive personal details, poses a particular risk to individuals escaping abusive situations.
- Hackers launched a massive distributed denial-of-service (DDoS) attack on Monobank, one of Ukraine's leading online banks. The attack, which spanned for three days, involved an unprecedented volume of 7.5 billion requests per second, but did not impact the bank's core operations. The aim of the attack appeared to be to disrupt a popular platform for raising funds for Ukraine's armed forces, a service that has gained increased usage since recent military actions.
- Researchers have identified a phishing campaign likely linked to Iranian hackers targeting a prominent Jewish religious figure. The attackers, suspected to be connected to Iranian group APT42 (also known as TA453), used spoofed emails from the Institute for the Study of War (ISW) to invite the victim to a fake podcast, ultimately delivering malware named BlackSmith via a malicious GoogleDrive link.

VULNERABILITIES AND PATCHES

- Cisco reported on eight vulnerabilities in Microsoft applications for macOS. The Microsoft apps gain entitlements and user-granted permissions which can be exploited by threat actors via injection of malicious libraries. This can allow the threat actors access to a victim's microphone, camera, screen recording, user input, stored data and more.

- Wordfence disclosed a critical vulnerability, tracked as CVE-2024-28000, in a WordPress plugin Lightspeed Cache. Used by more than 5,000,000 websites, the plugin versions up to and including 6.3.0.1 are vulnerable to privilege escalation due to mismanagement of role simulation functionality.

  Check Point IPS provides protection against this threat *(WordPress LiteSpeed Cache Plugin Privilege Escalation (CVE-2024-28000))*

- Researchers have discovered a high severity Server-Side Request Forgery (SSRF) vulnerability (CVE-2024-38206) in Microsoft Copilot Studio, enabling unauthorized access to internal service data and cross-tenant information. This vulnerability allowed the manipulation of Copilot's HTTP requests to access Microsoft's internal infrastructure, including sensitive instance metadata and Cosmos DB.

THREAT INTELLIGENCE REPORTS

- Researchers have uncovered a new phishing technique targeting mobile users via Progressive Web Applications (PWAs) and WebAPKs on both Android and iOS platforms. This method involves tricking users into installing phishing apps that mimic legitimate banking applications without traditional warnings about third-party installations. The phishing campaigns, observed primarily in Czechia but also in Hungary and Georgia, use social engineering through various delivery mechanisms. Once installed, these apps capture sensitive banking credentials and send them to different command-and-control servers managed by separate threat actors.

- Researchers have identified a state-sponsored North Korean threat actor, known as UAT-5394, using a newly developed remote access trojan called MoonPeak. This malware, evolving from the open-source XenoRAT, forms part of a broader infrastructure shift from cloud services to attacker-owned systems.

- Researchers report on a new BlindEagle, also known as APT-C-36, campaign targeting Latin American countries such as Colombia, Ecuador, Chile, and Panama. This group employs phishing emails, often impersonating governmental or financial institutions, to deliver malware. Their tactics include using publicly available Remote Access Trojans (RATs) like njRAT and AsyncRAT, which they customize for espionage or financial theft.

- The Qilin ransomware group has introduced a new tactic by deploying a custom stealer to harvest account credentials stored in Google Chrome browsers. After gaining access to a network through compromised VPN credentials lacking multi-factor authentication (MFA), Qilin used Group Policy Objects (GPOs) to spread the stealer across all domain-connected machines, potentially stealing credentials from every logged-in user.