cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The German air traffic control agency, Deutsche Flugsicherung, has confirmed a cyberattack that impacted its administrative IT infrastructure. The extent of data accessed is still under investigation, and flight operations remained unaffected. No threat actor has claimed responsibility yet, though the attack is suspected to have been caused by APT28, a threat actor linked to Russia's GRU.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(APT.Win.APT28; APT.Wins.APT28.ta.*)*

- Transport for London (TfL) public transit agency has experienced a cyber-attack that resulted in online outages affecting TfL's customer-facing and back-office systems. It included ticketing, real-time Tube information, and limited staff access, causing delays in customer service responses. No customer data compromise has been reported, and no threat actor has claimed responsibility yet.

- The Montana branch of a leading American healthcare provider Planned Parenthood has been a victim of a ransomware attack claimed by RansomHub ransomware group. The attack resulted in the theft of 93GB of sensitive data, primarily affected the organization's administrative IT systems.

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

- US semiconductor supplier Microchip Technology was hit by a cyber-attack claimed by Play ransomware gang, which resulted in the theft of employee data, including contact information and passwords. The attack disrupted multiple facilities, impacting the company's order fulfillment.

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

- CERT-UA and MILCERT have detected and analyzed two cyber-attacks against Ukrainian military personnel, involving fake APK downloads designed to steal sensitive data like login credentials and GPS locations. The attacks employed HYDRA malware and modified legitimate military applications, aiming to compromise mobile devices used in military operations.

  Check Point Harmony Mobile protects against this threat.

- Car rental giant Avis has suffered a data breach in which attackers accessed a business application and stole customers' personal information, including names and other undisclosed sensitive data. No threat actor has claimed responsibility yet.

- CBIZ Benefits & Insurance Services has disclosed a data breach resulting from unauthorized access to client information. The breach affected nearly 36K individuals, exposing names, contact details, Social Security numbers, retiree health information, and welfare plan details.

VULNERABILITIES AND PATCHES

- Google has released its September Android security update which addresses 34 vulnerabilities, including CVE-2024-32896, a high-severity elevation of privilege flaw in Pixel devices. This actively exploited vulnerability could allow attackers to bypass Android protections and elevate privileges.
- Veeam has issued security updates to address 18 high and critical severity vulnerabilities across the company's products. Among the vulnerabilities is CVE-2024-40711, a critical remote code execution (RCE) vulnerability in Veeam Backup & Replication (VBR) software. This vulnerability allows attackers to potentially take complete control of the system without authentication.
- Apache has patched a vulnerability in its OFBiz software, CVE-2024-45195, which allows attackers without credentials to execute arbitrary code on Linux and Windows servers through unauthenticated direct request attacks and a forced browsing weakness.
  Check Point IPS blade provides protection against this threat *(Apache OFBiz Remote Code Execution (CVE-2024-45195))*
- Zyxel has acknowledged fixes for an OS command injection vulnerability, CVE-2024-7261, affecting some of its access point and security router devices. This vulnerability stems from improper neutralization of special elements in the "host" parameter within the CGI program, allowing unauthenticated attackers to execute OS commands via a crafted cookie.

THREAT INTELLIGENCE REPORTS

- Check Point Research explores the most prominent hacking groups involved in the #FreeDurov campaign following the arrest of Telegram CEO Pavel Durov. The campaign involved major hacking groups like the pro-Russian Cyber Army of Russia Reborn and pro-Islamic RipperSec, which executed distributed denial of service (DDoS) attacks against over 50 targets in France.
- The FBI, CISA and NSA have analyzed the activities of Russian GRU Unit 29155 (Cadet Blizzard, Ember Bear), which have conducted cyber operations targeting global critical infrastructure since at least 2020. These operations have included the deployment of WhisperGate malware against Ukraine, website defacements, and data exfiltration. The threat actors disrupted aid efforts to Ukraine and targeted sectors such as government, finance, transportation, energy, and healthcare worldwide.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Trojan.Win.WhisperGate; Trojan.Wins.WhisperGate.ta.; Trojan.Wins.WhisperGate)*
- Researchers have shared a technical analysis of Akira Ransomware, outlining its use of dual extortion tactics affecting various industries since April 2023. Among discussed techniques embedding ransom notes within executables, targeting volume shadow copies for deletion, and manipulating Windows Restart Manager to close files for encryption.

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