CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Clop ransomware gang exploited a zero-day vulnerability (CVE-2024-50623) in Cleo's Secure File Transfer products and is extorting 66 companies following alleged data theft. The attackers have given the victims 48 hours to initiate ransom negotiations before publicly disclosing their identities. This incident mirrors Clop's previous exploitation of zero-day flaws in platforms like Accellion FTA, GoAnywhere MFT, and MOVEit Transfer.

  Check Point Harmony Endpoint, Threat Emulation and IPS provide protection against this threat
  (Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta. ; Cleo Arbitrary File Upload (CVE-2024-50623))*

- Pittsburgh Regional Transit (PRT) experienced a ransomware attack last week, resulting in service disruptions to its rail system and customer service operations. While transit services have resumed normal operations, certain rider services, such as processing ConnectCards, remain affected. The investigation, involving law enforcement and cybersecurity experts, is ongoing, with no confirmation yet regarding data theft or the group responsible for the attack.

- Cyberhaven has been a victim of a cyber-attack that resulted in distribution of a malicious update for its Chrome browser extension. The compromised extension was able to exfiltrate users' sensitive information, including authenticated sessions and cookies.

- Cariad, Volkswagen's automotive software subsidiary, exposed data from 800,000 electric cars, including sensitive geo-location information, due to misconfigured IT applications. The exposed data included details of vehicles from VW, Seat, Audi, and Skoda, with precise locations for 460,000 cars and pseudonymized user data. The Chaos Computer Club identified the vulnerability, enabling access to terabytes of unprotected customer information stored in Amazon cloud storage.

- Japan Airlines has resumed to normal activity following a cyberattack that caused delays in domestic and international flights. The attack involved a sudden surge in network traffic, indicative of a distributed denial-of-service (DDoS) attack, affecting data communication with external systems. No customer information was leaked, and flight safety remained uncompromised.

- ZAGG Inc., a consumer electronics accessories maker, has disclosed a data breach resulting in the exposure of customers' payment card information. The breach occurred between October and November 2024, due to malicious code injected into the FreshClick app, a third-party application provided by their e-commerce platform, BigCommerce.

- The European Space Agency's (ESA) official merchandise store was hacked, causing it to display a fake payment page designed to steal customer payment card details.

VULNERABILITIES AND PATCHES

- A critical SQL injection vulnerability (CVE-2024-45387), rated 9.9 on the CVSS scale, has been identified in Apache Traffic Control versions 8.0.0 and 8.0.1. The flaw allows privileged users with specific roles to execute arbitrary SQL commands in the database via crafted PUT requests. The issue has been patched in version 8.0.2.

  Check Point IPS provides protection against this threat (Apache Traffic Control SQL Injection (CVE-2024-45387))

- A critical vulnerability (CVE-2024-52046) with a maximum CVSS score of 10.0, has been disclosed in Apache MINA, a Java network application framework. The flaw arises from the ObjectSerializationDecoder's use of Java's native deserialization protocol without adequate security measures, enabling attackers to execute remote code by sending malicious serialized data.

- Palo Alto Networks has disclosed an actively exploited Denial of Service (DoS) vulnerability (CVE-2024-3393) affecting PAN-OS software. The flaw allows unauthenticated attackers to send malicious packets that force affected firewalls into reboot or maintenance mode, disrupting firewall protection. The issue impacts devices with DNS Security logging enabled and has been patched in versions PAN-OS 10.1.14-h8, 10.2.10-h12, 11.1.5, and 11.2.3.

- A high-severity OS command injection vulnerability (CVE-2024-12856), has been discovered in Four-Faith router models F3x24 and F3x36. Exploitation is possible if attackers authenticate using default credentials, potentially leading to unauthenticated OS command execution. Over 15,000 internet-facing devices are at risk, with evidence suggesting active exploitation since at least early November 2024.

THREAT INTELLIGENCE REPORTS

- Researchers have observed "OtterCookie", a new malware used in the North Korean-associated Contagious Interview campaign. This financially motivated campaign targets a broad range of victims and is active in Japan. OtterCookie communicates via Socket.IO, executes shell commands to exfiltrate sensitive data, including cryptocurrency keys, and uses clipboard data collection to enhance its capabilities.

- Researchers have identified heightened activity by the Paper Werewolf (aka GOFFEE) cluster, conducting at least seven campaigns targeting Russian organizations since 2022. Using phishing emails with malicious macros and tools like PowerShell and PowerRAT, the group conducts cyber espionage and destructive actions, including disabling IT infrastructure and changing account credentials. Their arsenal includes custom implants, reverse shells, and malicious IIS modules for credential harvesting.

- Researchers have analyzed the increased activity from botnets like the Mirai variant "FICORA" and the Kaiten variant "CAPSAICIN," which exploit long-standing vulnerabilities in D-Link devices to execute malicious commands via the HNAP interface.