TOP ATTACKS AND BREACHES

- Hitachi Energy reported a data breach caused by the Clop ransomware group which exploited a zero-day vulnerability (CVE-2023-0669) in the Fortra GoAnywhere MFT system, which was used by Hitachi.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat *(GoAnywhere MFT Insecure Deserialization (CVE-2023-0669); Ransomware.Win.Clop)*

- A Chinese hacking group is believed to be responsible for several attacks on government organizations, leveraging a zero-day vulnerability (CVE-2022-41328) in Fortinet devices to deploy malware. This security flaw enabled attackers to execute unauthorized code or commands on multiple Fortinet solutions.

- Essendant, a wholesale distributor of office products, was allegedly hit by a LockBit ransomware attack, resulting in a significant and ongoing outage that disrupted online order placement and fulfillment, affecting the company's customers and suppliers.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win.Lockbit)*

- Reports reveal that a threat actor is offering for sale hundreds of gigabytes of data, supposedly taken from U.S. Marshals Service (USMS) servers, on a major Russian-speaking hacking forum. USMS has confirmed an ongoing investigation into a "data exfiltration event" after a ransomware attack that impacted one of its stand-alone systems in February.

- Miami-based healthcare provider Independent Living Systems (ILS) reported a data breach that exposed 4.2 million individuals' personal information, making it the biggest healthcare data breach this year.

- The NBA has informed of a data breach in which personal information of fans held by a third-party newsletter service was stolen.

- Security researchers have recently unveiled a new trend in the BianLian ransomware group's behavior, indicating that they have undergone a shift in their attack strategy. Specifically, the group's priority seems to have shifted from data encryption to data exfiltration.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.GenRansom.glsf.A)*

VULNERABILITIES AND PATCHES

- Microsoft's Patch Tuesday fixes 83 flaws, including two actively exploited zero-day vulnerabilities. Among those is also a privilege escalation vulnerability in Microsoft Outlook (CVE-2023-23397) that allows for a NTLM Relay attack against another service to authenticate as the user.

  Check Point IPS provides protection against this threat *(Microsoft Outlook Privilege Escalation (CVE-2023-23397))*

- Foxit Software patched critical remote code execution vulnerabilities (CVE-2023-27329, CVE-2023-27330, and CVE-2023-27331) in its PDF Reader and Editor software, which could expose users' systems to significant risks.

- A critical security vulnerability (CVE-2022-39214) has been detected in the iTop IT Service Management Platform. It results from inadequate authentication, enabling an attacker to exploit the vulnerability by submitting a specially-crafted request utilizing the username parameter

- Adobe have published a security advisory addressing RCE vulnerability CVE-2023-26360 affecting ColdFusion. According to the advisory, Adobe is aware of active exploitation of the vulnerability.

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed the FakeCalls Android Trojan, which can mimic over 20 financial apps and engage in voice phishing by simulating conversations with bank employees. This malware, designed for the South Korean market also extracts private data from victims' devices.

  Check Point Harmony Mobile and Threat Emulation provide protection against this threat.

- Check Point Research has discovered security flaws in chess.com that could allow users to manipulate game results. Using the vulnerability, researchers were able to reduce opponent's time and thus to win games.

- Check Point Research has analyzed the dotRunpeX injector which is used to infect systems with a variety of known malware families including Redline, Raccoon and Formbook. It is commonly distributed via phishing emails as malicious attachments and websites masquerading as regular program utilities

  Check Point Threat Emulation provides protection against this threat (Injector.Wins.dotRunpeX.A)

- Check Point Research has analyzed ChatGPT4 and identified five scenarios that allow threat actors to by bypass the restrictions and to utilize ChatGPT4 to create phishing emails and malware.

- US law enforcement detained an individual from New York who they suspect is Pompompurin, the proprietor of the BreachForums hacking forum. BreachForums is currently the biggest English speaking underground forum that sells and publishes stolen data.