TOP ATTACKS AND BREACHES

- PharMerica, a provider of pharmacy services across the U.S., disclosed a data breach impacting approximately 5.8 million of its patients. Money Message ransomware gang claimed the attack during April, and threatened to leak 4.7 TB of stolen data.

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

- A new ransomware strain called MalasLocker is actively targeting Zimbra servers, encrypting files, stealing emails and demanding a ransom payment. Instead of demanding a traditional ransom, the MalasLocker group requests a charity donation as a form of payment.

- FIN7, the financially motivated group that is also known as Sangria Tempest, has recently reemerged with ties to attacks that aimed to deploy Clop ransomware on victims' networks. This marks the group's first ransomware campaign since late 2021. The group is primarily targeting organizations in the retail, hospitality, and healthcare sectors.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware_Linux_Clop)

- A new ransomware group known as RA Group has breached several organizations in the U.S. and South Korea with double extortion attacks. The ransomware operation may be using an encryptor based on leaked source code for the Babuk ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.win.rank, Ransomware.Win.TouchTrapFiles.A; TS_Ransomware.Win.Babuk.A; Ransomware.Win.Babuk.A)

- ScanSource, a major U.S. based technology distributor, experienced multi-day outages due to a ransomware attack. The company is working to restore its systems and has engaged with external experts to investigate the incident.

- Luxottica, a leading eyewear company, has confirmed a data breach that occurred in 2021 after the personal information of approximately 70 million individuals was leaked for free on hacking forums.

- Threat actors have launched new phishing campaigns that use cloned websites posing as legitimate CapCut popular video-editing sites to distribute info-stealing malware.

VULNERABILITIES AND PATCHES

- Threat actors are actively targeting vulnerable websites using the WordPress Elementor plugin following the release of a proof-of-concept exploit. The plugin, which has millions of installations, has a critical vulnerability (CVE-2023-32243) that allows attackers to execute arbitrary code and gain control over affected websites.
- Cisco has issued a warning about critical vulnerabilities affecting its switches. The vulnerabilities (CVE-2023-20159, CVE-2023-20160, CVE-2023-20161, and CVE-2023-20189) reportedly have public exploit code available.
- Apple has released patches addressing three exploited zero-day vulnerabilities (CVE-2023-28204, CVE-2023-32373 and CVE-2023-32409) in the WebKit engine used by Safari and other Apple products.
- CISA has issued a warning about an Address Space Layout Randomization (ASLR) bypass vulnerability (CVE-2023-21492) affecting Samsung mobile devices. The vulnerability is being exploited ITW.

THREAT INTELLIGENCE REPORTS

- Check Point Research had discovered a custom firmware implant tailored for TP-Link routers that has been linked to a Chinese state-sponsored APT group tracked as Camaro Dragon, which shares similarities with Mustang Panda. The implant was used in targeted attacks aimed at European foreign affairs entities, and it features several malicious components. This includes a custom backdoor named “Horse Shell”, which enables the attackers to maintain persistent access, build anonymous infrastructure and enable lateral movement into compromised networks.

  Check Point Quantum IoT Protect and Threat Emulation provide protection against this threat (APT.Wins.HorseShell)

- Check Point identified malicious extensions for Visual Studio Code (VSCode) with over 45,000 downloads that steal personally identifiable information (PII) and enable backdoor access to users' systems. Among those extension are “prettiest java”, “darcula dark” and “python-vscode”.
- The FBI, CISA, and ACSC warn that the BianLian ransomware group has shifted its tactics to extortion-only attacks. Instead of encrypting files and demanding a ransom, the group now focuses on stealing sensitive data and threatening to release it unless a payment is made.

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

- A cybercrime gang tracked as “Lemon Group” has been detected infecting almost 9 million of Android devices with a malware called Guerilla. The malware is capable of stealing sensitive information, performing ad fraud, and installing additional malicious apps.