July 19-25, 2021

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- US officials have reported that Chinese state-sponsored threat actors successfully breached 13 US oil and natural gas pipeline companies between 2011 and 2013. The hackers gained initial access using a spear-phishing campaign, and their main goal was to gain strategic access and disrupt US pipeline operations.
- The French National Agency for Cyber Security has warned about a campaign attributed to Chinese APT31 targeting compromised routers of several French entities in order to perform stealth reconnaissance.
- CISA has alerted on numerous malware found on Pulse Secure devices exploiting vulnerabilities (CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, CVE-2021-2289). Researchers found 13 unique malware on compromised Pulse Connect Secure devices, most of them webshells.

  Check Point IPS and Harmony Endpoint provide protection against these threats (Pulse Connect Secure File Disclosure (CVE-2019-11510); Web Servers Malicious URL Directory Traversal)
- The StrongPity APT group was first observed using malware intended for Android mobiles, targeting Syria. The group conducted a watering-hole attack, compromised the official Syrian E-Gov website, and posted the Android Trojan on the Syrian Government website instead of a legitimate APK.
- The Israeli NSO group has been accused of deploying its surveillance tool, Pegasus, to penetrate smartphones and exfiltrate personal information, records, and data from high-profile targets including government officials, journalists, and activists around the globe.
- Researchers have found over 80 misconfigured Amazon S3 buckets holding more than 1,000 GB of sensitive data related to about 100 municipalities across the Northeast of the US. They believe that the misconfigured buckets were all linked to the information management company PeopleGIS.

VULNERABILITIES AND PATCHES

- A local privilege escalation vulnerability dubbed Sequoia (CVE-2021-33909) allows attackers to gain root privileges by exploiting a flaw in default configurations of the Linux Kernel's filesystem.
- A high severity vulnerability, CVE-2021-3438, has been found in a driver used by HP, Xerox, and Samsung printers. The flaw allows an attacker to gain admin privileges using the vulnerable driver without requiring user interaction. The bug can be abused even when the printer is not connected to the targeted device.
- Microsoft has addressed PetitPotam, a security flaw in Windows that can force remote Windows servers to authenticate with an attacker and share NTLM authentication certificates. Microsoft recommends disabling NTLM where it is not necessary or using signing features such as SMB signing.

Check Point IPS will provide protection against this threat in its upcoming packages (Microsoft Active Directory Certificate Services NTLM Relay)

- Fortinet has published a patch for FortiManager and FortiAnalyzer network management solutions to fix CVE-2021-32589. The vulnerability could allow an unauthenticated threat actor to execute arbitrary code with the highest privileges on compromised systems.
- Atlassian has released a fix for CVE-2020-36239, a flaw in Jira Data Center products. The vulnerability can allow remote unauthenticated attacker to execute arbitrary code due to a missing authentication flaw.
- A security researcher has revealed that the Windows 10 and Windows 11 registry files are accessible to users with low privileges on a device. By using Windows shadow volumes, a threat actor can steal the NTLM hashed password of an elevated account and reach higher privileges.

THREAT INTELLIGENCE REPORTS

- Check Point Research has reported that XLoader, a successor of the prevalent Info Stealer malware Formbook, now also operates on macOS. XLoader is being offered in an underground forum as a botnet loader service that can recover passwords from web browsers and some email clients.

Check Point Threat Emulation, Anti-Bot and Anti-Virus provide protection against these threats (Trojan.WIN32.Formbook; InfoStealer.Win.Formbook; Banking.Win32.Formbook; Trojan.Mac.XLoader)

- Chrome & Telegram became the new targets of the upgraded macOS malware XCSSET which is capable of stealing information from Notes, WeChat, Skype, or Telegram and enables its operators to steal accounts.

Check Point Threat Emulation and Anti-Virus provides protection against these threats (Trojan.Mac.XCSSET)

- The NPM malware has exploited ChromePass, Google Chrome's legitimate password-recovery tool to steal passwords and credentials. The malware, which has over 2,000 downloads, also provides advanced capabilities, such as screen and camera access, directory listing, and shell command execution.