July 24 – 30, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Norwegian government has reported that a software platform, used by 12 key ministries, suffered a cyberattack. It happened after hackers exploited a zero-day authentication bypass vulnerability in Ivanti's Endpoint Manager Mobile (EPMM).

- Maximum, a contractor providing services to the U.S. government, including federal and local healthcare programs and student loan servicing, disclosed a data breach linked to Cl0p's MOVEit attack. The breach compromised personal information of more than 8 million customers.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *((Progress MOVEit Transfer Multiple Vulnerabilities); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)*

- The Hawaii Community College has acknowledged paying a ransom to ransomware actors to thwart the leakage of personal information of 28,000 individuals. NoEscape ransomware gang claimed responsibility for this attack.

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

- Security researchers have recently uncovered a campaign they assess might be tied to the North Korean APT37 group. In this campaign, threat actors employed counterfeit US military job-recruitment documents as bait to entice individuals into downloading malware hosted on legitimate, yet compromised Korean websites.

  Check Point Harmony Endpoint provides protection against this threat *(APT.Win.APT37)*

- Estonian crypto-payments service provider CoinsPaid has announced that it experienced a cyber-attack on July 22nd that resulted in the theft of $37,200,000 worth of cryptocurrency. CoinsPaid is blaming the attack on the North Korean hacking group Lazarus.

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

- NATO is investigating an alleged data-theft hack on its unclassified information-sharing platform, the COI Cooperation Portal (dnbl.ncia.nato.int). The SiegedSec group claimed responsibility for the attack.

- Researchers have revealed a deceptive installer posing as a genuine Microsoft Visual Studio installer, delivering a Cookie Stealer. This installer is distributed through various deceptive methods like phishing websites, third-party platforms, social engineering, and misleading ads.

VULNERABILITIES AND PATCHES

- Ivanti, a US-based IT Software Company, has recently addressed an actively exploited zero-day authentication bypass vulnerability affecting its Endpoint Manager Mobile (EPMM) mobile device management software (previously known as MobileIron Core).

  Check Point IPS Blade provides protection against this threat (Ivanti Endpoint Manager Mobile Authentication Bypass (CVE-2023-35078))

- CISA released five Industrial Control Systems advisories that provide timely information about current security issues, vulnerabilities, and exploits.

- Researchers have recently published a comprehensive list of vital security updates and vulnerability patches for WordPress.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have revealed vulnerabilities in internet-connected workout equipment, including popular brands like Peloton. Exploiting those vulnerabilities could potentially provide threat actors with access to user databases, thereby exposing sensitive data of Peloton users.

- Researchers have discovered two new related Android malware families, dubbed CherryBlos and FakeTrade, which are involved in cryptocurrency mining and financially motivated scam campaigns targeting Android users.

- Researchers have identified a malicious phishing campaign attempting to deploy the notorious Agent Tesla infostealer. The campaign utilizes malspam techniques, disguising the malicious payload as a price quotation request from a seemingly legitimate South Korean company within the mining and metals industry.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (InfoStealer.Win.Agenttesla; Technique.Win.LinkRemote.la.)*

- Security researchers found a new initial-access campaign called 'Nitrogen' that misuses Google and Bing ads to target users searching for certain IT tools. The campaign aims to gain entry into enterprise environments to deploy further malware, possibly ransomware.

- Researchers have uncovered a new campaign involving the installation of the PurpleFox malware on poorly managed MS-SQL servers. PurpleFox facilitates the downloading of various second-stage payloads.