Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An ongoing espionage campaign targeting dozens of organizations in Taiwan has been discovered. Researchers have attributed the activity to a Chinese APT group dubbed Flax Typhoon, which overlaps with Ethereal Panda. The threat group minimizes the use of custom malware, and instead uses legitimate tools found in victims' operating systems to conduct its espionage operations.

- Pro-Russian hackers have disrupted train services in northwest Poland by gaining access to the railway's designated frequencies. The hackers broadcasted the Russian national anthem, as well as a speech of the Russian president Putin during the attack.

- Dutch cloud and hosting giant Leaseweb has notified customers that it had been affected by a security breach. The company claimed to be working on restoring critical systems, after it was forced to disable them in response to the attack.

- French employment government agency Pôle emploi has disclosed a breach, with personal information of up to 10 million registered users having been leaked. The breach has reportedly occurred via a 3rd party IT vendor Majorel, which had been affected by ransomware group Cl0p's in the MOVEit campaign.

  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)*

- London area Metropolitan Police has declared a red alert after personal information including photos of all 47,000 of the police force's personnel has been leaked in a breach of 3rd party contractor. The Police fears the information will get to terrorist and criminal groups, and has said it may be forced to pull undercover officers from sensitive operations.

- Financial advising firm Kroll has announced that personal information related to the bankruptcy cases of crypto firms BlockFi, FTX and Genesis was exfiltrated by a threat actor. According to Kroll, the threat actor used a SIM swapping attack, where they convinced mobile provider T-Mobile to transfer a Kroll employee's phone number to the attacker without the victim's authorization.

- Ransomware group Black Cat has claimed responsibility for breaching Japanese watch manufacturer SEIKO. The group claims to have stolen files from the SEIKO's network, and threatens to leak them if the ransom is not paid. The company has previously acknowledged the breach.

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

VULNERABILITIES AND PATCHES

- IT Software company Ivanti has published a security advisory regarding vulnerability CVE-2023-38035 affecting its Ivanti (MobileIron) Sentry product. The vulnerability allows API authentication bypass, and is considered critical. While no patch has been released, Ivanti has posted RPM scripts to address it.

  Check Point IPS blade provides protection against this threat *(Ivanti MobileIron Sentry Authentication Bypass (CVE-2023-38035))*

- Juniper Networks has updated last week's security advisory regarding its firewall products. It has been discovered that the series of previously-reported medium-severity vulnerabilities (CVE-2023-36844 to CVE-2023-36847) can be used in conjunction to create a critical threat of unauthenticated remote code execution by a network attacker. Juniper has released updated versions to cover the vulnerabilities.

- Researchers warn of active exploitation of newly-discovered WinRAR zero-day vulnerability CVE-2023-38831. The vulnerability allows threat actors to deliver malware using benign WinRAR archive files, and has been used in a campaign targeting brokers and traders since April. WinRAR's latest released version covers this vulnerability.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published 2023's mid-year security report which shows 8% increase in weekly cyber-attacks in the second quarter of the year. The report also reveals that in the first half of 2023, a total of 48 ransomware groups have publicly extorted more than 2,200 organizations worldwide.

- Check Point Research demonstrates the effectiveness of DeepDNS, Check Point's novel artificial neural network that blocks DNS-related threats. Among others, the tool has successfully detected a new CoinLoader malware campaign, which employs a DNS backup channel.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Wins.Coinloader)*

- Check Point Research highlights that in comparison to other industries, the Education/Research sector experiences the highest rate of cyberattacks, with a vast disparity. In 2023, this sector has witnessed an average of 2256 weekly cyber-attacks per organization, while the APAC region recorded the highest rate of weekly cyberattacks per Education organization.

- Researchers have identified a novel geo-location malware dubbed Whiffy Recon. The malware is delivered via Smoke Loader, a common downloader vector used by threat actors to distribute additional payloads. Whiffy Recon continuously scans for nearby Wi-Fi networks, and then uses the legitimate Google Geolocation API to pinpoint the victim's location as they travel.

  Check Point Threat Emulation provides protection against this threat