May 27 – June 2, 2024

Check Point Research WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- ShinyHunters, a notorious cybercrime gang offered for sale on a cybercrime forum data of Ticketmaster, ticket sales and distribution company, and of Santander bank. The alleged breaches have resulted in the potential exposure of personal data belonging to millions of customers. Some assumption claim that actor gained access to Ticketmaster and Santander by using the stolen credentials of a single employee of Snowflake, a large cloud storage company.

- Researchers have uncovered a malware attack where over 600,000 SOHO routers were taken offline across a single ISP's network, resulting in hardware-based replacement of the affected devices. The analysis revealed that the attack was conducted with the Chalubo RAT, and featured advanced obfuscation techniques and was aimed at permanent hardware disablement. This incident significantly disrupted services in smaller towns and less developed areas.

- Japanese crypto exchange DMM Bitcoin confirmed a data breach that resulted in the loss of 4,502.9 BTC ($308 million). The incident is said to be one of the largest crypto heists and involves funds being moved to multiple wallets. Investigations are ongoing to track the stolen assets and notify affected parties.

- Sav-Rx, a U.S. based prescription management company, recently disclosed a significant data breach affecting over 2.8 million Americans. This incident, which occurred in 2023, involved the theft of personal data from Sav-Rx's systems. The company has confirmed that sensitive personal information was compromised but assured that no payment information was included in the breached data.

- Christie's, the world's largest auction house, has been breached by the RansomHub ransomware group. The attack has potentially exposed sensitive information of 500,000 of Christie's clients and led to a shutdown of the website right before its spring sales in New York began.

  Check Point Threat Emulation provides protection against this threat (Trojan.Wins.Imphash.taim.JI, Trojan.Wins.Imphash.taim.HQ)

- The Seattle Public Library experienced a ransomware attack that has disabled its digital services, including the wireless network, staff and patron computers, and online catalog. The library's 27 branches continue to operate manually for book and CD lending.

- The BBC Pension Fund has reported a breach, where unauthorized access was gained to steal personal information of the enrolled staff. The breach was conducted by cybercriminals aiming to exploit sensitive member data for fraudulent purposes.

VULNERABILITIES AND PATCHES

- Check Point has issued a warning about a high score zero-day vulnerability (CVE-2024-24919) exploited In the Wild, affecting its Security Gateways with IPsec VPN in Remote Access VPN community and the Mobile Access software blade. Exploitation of this vulnerability could allow threat actors to access certain information on internet-connected Gateways with remote access VPN or mobile access enabled.

  Check Point IPS provides protection against this threat (Check Point VPN Information Disclosure (CVE-2024-24919))

- TP-Link has patched a critical vulnerability (CVE-2024-5035) in the C5400X gaming router, which allows remote code execution. The vulnerability stemmed from improper handling of input in the 'rftest' binary accessible via network service ports.

THREAT INTELLIGENCE REPORTS

- Check Point Research has examined a group of malicious packers based on the Nullsoft Scriptable Install System (NSIS), uncovering mechanisms for evading detection and delivering malware payloads. In this technical analysis, CPR highlights the packer's flexibility and persistent threat in cyber environments, identifying multiple malware types such as loaders, stealers, and Remote Access Trojans.

  Check Point Threat Emulation provides protection against this threat (Packer.Win.NSISCrypter., Trojan.Win.Shellcode.F, Trojan.Win.Shellcode.G)*

- Europol, in coordination with international law enforcement agencies, conducted a disruptive operation against botnets, dubbed Operation Endgame, targeting the dropper malware ecosystem. Notably, the operation disrupted the infrastructure of 100 malware servers including of Trickbot, IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee, alongside the arrest of key individuals involved in distributing dropper malware. Reportedly, many of interrupted malware are regularly used by multiple ransomware groups, including BlackBasta, Revil and Conti.

- Researchers have shared information on the obfuscation tactics of Water Sigbin (8220 Gang), a China-linked threat actor deploying cryptocurrency mining malware. The group exploited Oracle WebLogic vulnerabilities (CVE-2017-3506 and CVE-2023-21839) using PowerShell scripts and sophisticated encoding methods, including hexadecimal encoding of URLs and fileless execution via .NET reflection techniques in PowerShell scripts.

  Check Point IPS provides protection against this threat (Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271), Oracle WebLogic Server Improper Access Control (CVE-2023-21839))

- Researchers observed an escalation in attacks targeting operational technology (OT) devices, particularly those with poor security and internet exposure. These attacks, notably by nation-backed groups like the IRGC-affiliated CyberAv3ngers, demonstrate the vulnerability of OT systems across various sectors.