TOP ATTACKS AND BREACHES

- The ALPHV/BlackCat Ransomware group has allegedly hacked Westmont Hospitality Group, one of the largest privately-held hospitality businesses in the world. They claim to have obtained access to 262GB of the company's data.

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

- PLAY ransomware group has allegedly acquired sensitive personal information from Arnold Clark, a major car dealership in the United Kingdom. The compromised data is said to include National Insurance numbers, passport information, as well as contact details such as addresses and phone numbers.

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

- The Ukrainian Computer Emergency Response Team (CERT-UA) concluded that the attacks on Ukrinform - Ukraine's national news agency – earlier this month, were performed by the Russian military cyber-espionage group, Sandworm, using five different data-wiping malware strains - CaddyWiper, ZeroWipe, SDelete, AwfulShred and BidSwipe.

  Check Point Threat Emulation provides protection against this threat (Trojan.Wins.CaddyWiper.)*

- Threat actors have breached Zacks Investment Research and accessed personal information of 820,000 customers. Zacks discovered the unauthorized access at the end of 2022, and an internal investigation found that a threat actor gained access to the network between November 2021 and August 2022.

- Threat actors have leaked a database they claim belongs to TARGET that contains information on 800K customers. The threat actors claim that the data includes GST ID, names, addresses, transactions, and more. TARGET has denied the breach, saying the data being sold on the dark web is not current and that the information was not taken directly from its systems.

- Security researchers have been observing a series of attacks against East Asian organizations, referred to as "DragonSpark". These attacks deploy the open-source malware "SparkRAT", and malware that utilizes Golang source code interpretation to evade detection. The researchers determined that it is highly probable that the attacks are being orchestrated by a Chinese-speaking actor.

- Researchers have uncovered a PlugX sample that employs sneaky methods to infect attached removable USB media devices in order to propagate the malware to additional systems.

VULNERABILITIES AND PATCHES

- The Internet Systems Consortium (ISC) has released security patches to address 4 high severity security vulnerabilities (CVE-2022-3094, CVE-2022-3488, CVE-2022-3736, and CVE-2022-3924) in the BIND DNS software suite that could lead to a DoS condition and system failures.
- Lexmark has released a security firmware update to fix a severe vulnerability (tracked as CVE-2023-23560) that could enable remote code execution on more than 100 printer models. The security issue is a server-side request forgery (SSRF) in the Web Services feature of Lexmark devices.
- Proof of Concept exploit code has been released for a critical Windows CryptoAPI vulnerability that allows MD5-collision certificate spoofing (CVE-2022-34689).

THREAT INTELLIGENCE REPORTS

- Check Point has published its Brand Phishing report for Q4 of 2022 that reveals some statistical changes in phishing campaigns. It seems that Technology was the most likely industry to be imitated by brand phishing in Q4 of 2022, followed by Shipping and Social Networks. Also, 20% of all brand phishing attempts were related to Yahoo, while DHL impersonations dropped to 16% of all phishing attempts.
- EUROPOL has successfully taken down the leak-site of the HIVE ransomware group. The United States Department of Justice announced in a press conference that they "hacked the hackers" to disrupt their operations and infrastructure. Victims received a decryption key to recover their encrypted files, preventing the payment of more than $130M.

  Check Point Harmony Endpoint and Threat Emulation provides protection against this threat (Ransomware.Win/s.Hive.)*
- A new type of ransomware called ‘Mimic’ takes advantage of the APIs of a legitimate tool called ‘Everything’ - a Windows filename search engine which offers fast searching and real-time updates. Mimic was first detected in June 2022 and primarily targets Russian and English-speaking users.

  Check Point Threat Emulation provides protection against this threat (Trojan.Win.TimEvasion.A)
- A joint advisory was issued by CISA, the NSA, and MS-ISAC, warning that attackers are increasingly exploiting legitimate remote monitoring and management (RMM) software for malicious activities.
- A campaign utilizing the "Titan Stealer" malware has been uncovered. This malware is being advertised and distributed by a threat actor through a Telegram channel. The stealer is capable of exfiltrating a wide range of information from infected Windows machines, including credentials from browsers and cryptocurrency wallets, FTP client details, screenshots, system information, and selected files.

  Check Point Threat Emulation provides protection against this threat (Infostealer.Win.PasswordStealer.A)