Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An attack targeting Snowflake customer databases, identified as the work of threat actor UNC5537, has led to significant data theft and extortion. UNC5537 used stolen Snowflake customer credentials, obtained mainly from infostealer malware to access and exfiltrate large volumes of data from Snowflake instances. The compromised accounts lacked multi-factor authentication and often had outdated credentials, facilitating the attacks. Snowflake has already notified around 165 affected organizations and are collaborating with law enforcement to investigate the breaches.

- American insurance giant, Globe Life, is investigating a potential data breach of one of its web portals, which may have exposed consumer and policyholder information. The breach prompted Globe Life to remove external access to the portal, and the full extent of the incident is currently being assessed by security experts. Representatives said they believe the breach was contained to the specific portal.

- A data breach has exposed old marketing data from cybersecurity company Cylance, affecting 34 million customer and employee emails and personally identifiable information. The data, being sold on underground marketplaces by threat actor Sp1d3r for $750,000, stems from a third-party platform and dates back to 2015-2018. Cylance confirmed the legitimacy of the data, however claimed that no current Cylance customers or sensitive information are impacted.

- The city of Cleveland has suffered a cyber incident, forcing it to shut down its city hall and affecting several internal systems and software platforms. Officials say affected systems will stay offline until the incident is more thoroughly investigated, and they are currently working to secure and restore services.

- The town of Arlington, Massachusetts, has disclosed that over $445,000 were paid to threat actors in a recent business email compromise attack. The cyber criminals used compromised business accounts, social engineering and spoofing to impersonate vendors with whom the town does business. According to the town's statement, no sensitive data was compromised in the campaign.

- Japanese media group KADOKAWA Group reported a recent cyber-attack which has disrupted multiple websites, including the Niconico Service, KADOKAWA Official Site, and more. The attack led to the shutdown of affected servers to protect data. In an announcement, KADOKAWA said they are investigating the incident with external experts and law enforcement to determine if any sensitive information was leaked, and that they are working to restore their systems.

VULNERABILITIES AND PATCHES

- Microsoft's June 2024 Patch Tuesday addressed 51 vulnerabilities including 18 remote code execution flaws, among which is one critical vulnerability (CVE-2024-30080), and one zero-day flaw (CVE-2023-50868). The updates cover various Microsoft products, with significant patches for remote code execution vulnerabilities in Microsoft Office and privilege elevation flow in Windows Kernel.

  Check Point IPS blade is protecting against this threat *(Microsoft Message Queuing Remote Code Execution (CVE-2024-30080))*

- Researchers have revealed 24 vulnerabilities after a comprehensive analysis of a popular ZKTeco biometric terminal. The list of flaws includes 6 SQL injection vulnerabilities, 7 buffer overflow, 5 command injection, and 6 arbitrary file read/write flaws. Exploiting these weaknesses could allow authentication bypass, data leaks, and network access breaches.

- Researchers have discovered a high-severity flaw, CVE 2024-21754, in Fortinet firewall firmware, which could potentially expose sensitive information such as passwords to attackers. This vulnerability allowed unauthorized users to decrypt configuration backup files and access user credentials. The flaw was disclosed to Fortinet and addressed in FortiOS v7.4.4.

THREAT INTELLIGENCE REPORTS

- Check Point Research published its Global Threat Index for May 2024, highlighting that the Phorpiex botnet is being used to distribute LockBit Black ransomware via millions of phishing emails, marking a significant malspam campaign. Additionally, the LockBit3 ransomware group activity has resurged, accounting for 33% of ransomware attacks after a recent disruption. This resurgence follows law enforcement action that had temporarily halted their operations by exposing leaders and releasing decryption keys. The report also highlights the prevalence of malware families such as FakeUpdates, Androxgh0st, and Qbot.

- Check Point Research warns about online phishing scams related to summer vacations. In May 2024, CPR detected a significant surge in summer-related cyber scams, highlighting the need for travelers to stay informed and proactive in safeguarding their personal information. Specifically, a notable surge in newly created domains related to holidays or vacations was observed, with a significant increase compared to the same period last year.

- Check Point highlights a sophisticated DLL sideloading attack designed to steal login credentials and credit card information from users of online payment systems, banks, and crypto exchanges. This attack exploits legitimate business applications to run compromised DLL files, making detection difficult. The specific described attack involved the Casbaneiro banking trojan, which used legitimate resources hosted on Amazon AWS and GitHub to sideload a malicious DLL.