TOP ATTACKS AND BREACHES

- The American Bar Association (ABA), the largest global association of lawyers and legal professionals, has suffered a data breach with hackers gaining access to older credentials of 1,466,000 members. The breach was first detected on March 17th, 2023, and involved login credentials and salted passwords to ABA's old website

- Capita, a professional outsourcing company based in London, has provided an update on a recent cyber incident they experienced, acknowledging that data was exfiltrated from their systems one week prior to the outage. The company revealed that approximately 4% of its server infrastructure was accessed by hackers who stole files. The BlackBasta ransomware group, known to operate from Russian-speaking regions, has been identified as the perpetrator of the attack.

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

- Researchers have discovered that last month's 3CX Software supply chain attack was allegedly caused by an additional prior supply chain compromise. In that case, suspected North Korean attackers breached the site of stock trading automation company "Trading Technologies", to push its trojanized software builds, and among other victims to infect 3CX.

- Point32Health, a New England health insurance firm serving over two million people, is grappling with a ransomware attack. Systems are offline, and authorities have been notified. No ransomware group has claimed responsibility.

- Researchers have discovered that an Iranian hacking group, previously known as Phosphorous, and now tracked under the name Mint Sandstorm, is conducting cyberattacks on US critical infrastructure. Mint Sandstorm is believed to be linked to the Iranian government and the Islamic Revolutionary Guard Corps (IRGC).

- Security researchers have recently discovered the presence of Trigona ransomware on inadequately secured MS-SQL servers. Trigona is a relatively new type of ransomware that was first identified in October 2022. Another research team had previously pointed out that Trigona and the CryLock ransomware share certain similarities.

  Check Point Threat Emulation provides protection against these threats *(Ransomware.Wins.Trigona.A; Trojan.Wins.Crylock.ta.A)*

VULNERABILITIES AND PATCHES

- A number of vulnerabilities in Cisco and VMware products have been addressed with critical security updates in order to prevent malicious actors from exploiting them to run arbitrary code on affected systems. The most severe vulnerability is a command injection flaw in Cisco Industrial Network Director (CVE-2023-20036).

- Fortra has published the summary of their investigation of the zero-day remote code execution vulnerability (CVE-2023-0669) in its GoAnywhere MFT tool, actively exploited by ransomware groups to steal sensitive data.

  Check Point IPS provides protection against this threat *(VER0 GoAnywhere MFT Insecure Deserialization (CVE-2023-0669))*

- Oracle has released April's security patch, which includes fixes for 433 vulnerabilities, including 70 which are considered critical.

THREAT INTELLIGENCE REPORTS

- Check Point Brand Phishing Report for Q1 2023 shows changes in the most imitated brands by cyber criminals. Walmart, a multinational retail giant, took the top spot with 16% of all attempts, climbing from 13th place in Q4 2022 due to a phishing campaign related to a supply system collapse. DHL held onto second place with 13%, followed by Microsoft with 12%.

- The Check Point research team has uncovered new techniques used by the Raspberry Robin malware. These methods include several anti-evasion techniques, obfuscation, and anti-VM measures. The malware also exploits two vulnerabilities in Win32k (CVE-2020-1054 and CVE-2021-1732) in order to elevate its privileges.

  Check Point Threat Emulation and IPS provide protection against this threat *(Trojan.Wins.RaspberryRobin; Microsoft Win32k Elevation of Privilege (CVE-2021-1732), Microsoft Win32k Elevation of Privilege (CVE-2020-1054))*

- Researchers have discovered a macOS malware named RustBucket that communicates with C2 servers and is suspected to be associated with a North Korean state-sponsored threat actor known as BlueNoroff, a sub-group of Lazarus Group.

- The Cybersecurity & Infrastructure Security Agency has released a new Malware Analysis Report on the ICONICSTEALER infostealer. This infostealer has been identified as a variant of malware used in the supply chain attack against 3CX's Software.

  Check Point Threat Emulation provides protection against this threat *(InfoStealer.Wins.IconicStealer)*