February 27 – March 5, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The American fast food chain Chick-fil-A has released an announcement revealing a credential stuffing attack occurred on their website and mobile app. The attack exposed over 71K customers' accounts data, including names, email addresses, mobile payment numbers and masked credit or debit card numbers, and threat actors may have used account balance to make purchases**.**
- Pierce Transit, a public transit operator that serves over 18K people daily in Washington State, has been a victim of a ransomware attack conducted by LockBit gang. The ransomware group claimed it stole correspondence, non-disclosure agreements, customer data, contracts and more.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win.Lockbit)
- Satellite TV giant Dish Network confirmed it has been a victim of a ransomware attack. The attack caused an internal systems outage that affected the company's internal communications, customer call centers, and websites. In addition, the threat actors extracted data that possibly include personal information. Researchers indicated that Black Basta ransomware operation is behind the attack, however the ransomware group has not yet claimed responsibility for the hack.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win.BlackBasta)
- Digital banking platform Hatch Bank has become the second known victim (after Community Health Systems in February) of the remote code execution vulnerability in Fortra's GoAnywhere file-transfer software (tracked as CVE-2023-0669). The Cl0p ransomware gang has claimed responsibility for the attack, claiming to have also stolen data from 130 additional organizations.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (GoAnywhere MFT Insecure Deserialization (CVE-2023-0669); Ransomware.Win.Clop)
- The websites of nine hospitals in Denmark have been shut down due to distributed-denial-of-service (DDoS) attacks performed by a relatively new hacktivists group known as Anonymous Sudan. According to the group's Telegram channel, the group warned it would attack Denmark healthcare infrastructure after an activist burned a Koran in front of the Turkish embassy in Stockholm.
- British retailer WH Smith suffered a data breach in which personal information of former and current employees was leaked, including names, addresses, National Insurance numbers and dates of birth. The company stated that there has been no impact on the trading activities of the group.

VULNERABILITIES AND PATCHES

- Researchers have released a report on ZK Framework vulnerability (tracked as CVE-2022-36537) in ConnectWise R1Soft Server Backup Manager software. The information disclosure vulnerability could lead to remote code execution and the installation of malicious drivers that function as backdoors.

  Check Point IPS provides protection against this threat *(ZKoss Authentication Bypass(CVE-2022-36537))*

- Microsoft has issued six out-of-band security updates for 'Memory Mapped I/O Stale Data (MMIO)' information disclosure vulnerabilities in Intel CPUs (tracked as CVE-2022-21123, CVE-2022-21125, CVE-2022-21127 and CVE-2022-21166). Successful exploitation might allow an attacker to read privileged data across trust boundaries.

- Cisco has published an advisory of critical severity vulnerabilities (tracked as CVE-2023-20078 and CVE-2023-20079) impacting 6800, 7800, and 8800 series IP phones. Successful exploitation might cause a remote command execution on the affected system.

THREAT INTELLIGENCE REPORTS

- Researchers have analyzed the increasing use of Microsoft OneNote documents to deliver malware. This trend is gaining popularity following the fact that Microsoft disabled macros by default, minimizing the effectiveness of Office documents as attack vectors, and given that OneNote can also run scripts.

  Check Point Harmony Endpoint provides protection against this threat *(Exploit.Win.OneNote)*

- Researchers have uncovered a malware distribution campaign that is delivering the LokiBot information stealer via business email compromise (BEC) phishing emails. This malware is designed to steal sensitive information from victims' systems, such as passwords and banking information.

  Check Point Threat Emulation, Harmony Endpoint and Anti-Bot provide protection against this threat *(Botnet.Win.Lokibot)*

- Researchers have analyzed MQsTTang, a new custom backdoor used by the Chinese APT group Mustang Panda (aka PlugX) as part of an ongoing campaign targeting political and governmental organizations in Europe and Asia. MQsTTang backdoor might allow the attacker to execute arbitrary commands on a victim’s machine.

  Check Point Threat Emulation, Harmony Endpoint and Anti-Bot provide protection against this threat *(RAT.Win.PlugX)*

- The cyberespionage APT group Iron Tiger (aka APT27, Emissary Panda, IronPanda) has made an update to the custom malware family called SysUpdate. The new version includes new features and components that enable the malware to compromise Linux systems.