TOP ATTACKS AND BREACHES

- Sensitive personal information of more than 56,000 Washington D.C. residents, including an undisclosed number of Senators and members of Congress, has been leaked on a darkweb forum. The leak occurred after the D.C. Health Link marketplace, a health insurance marketplace used by businesses and residents of Washington D.C. was breached.

- Medusa and Vice Society ransomware groups leaked sensitive data that was stolen from Minneapolis Public Schools and West Virginia Berkeley County Schools, respectively, in February ransomware attacks. Last year, the Vice Society group has targeted the Los Angeles Unified school district.

  Check Point Threat Emulation provides protection against these threats *(Trojan.Wins.ViceSociety.*, Ransomware.Wins.Medusalocker.*)*

- Israel's National Cyber Directorate has asserted that Iranian APT group MuddyWater, known to be affiliated with Iran's Ministry of Intelligence and Security, is behind the cyberattack on the Technion, one of Israel's leading universities. The attack was masked as a regular ransomware attack and had significantly disrupted the university's activities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

- American telecom giant AT&T has notified 9 million customers that some of their information was leaked in a data breach at a third party marketing vendor. According to AT&T, sensitive financial and personal information was not impacted in the breach.

- After a three month period of no observed activity, a new Emotet malware campaign has been detected in the wild. Emotet, which is delivered via malicious email messages, can deploy various additional malware (including ransomware) once it has successfully infected a victim's network.

  Check Point Harmony Endpoint, Threat Emulation, IPS and Anti Bot provide protection against this threat
  (Trojan.Wins.Emotet.; Worm.Win.Emotet.*; Emotet Exploit Kit Landing Page; Emotet Maldoc Download Page; Dropper.Win.GenDrop.la.E; Trojan.Win32.Emotet)*

- One of the largest engineering firms in Canada, Black & McDonald, has suffered a ransomware attack. The firm, which is a prominent contractor for the Canadian Department of Nation Defense, has not disclosed the impact of the attack.

VULNERABILITIES AND PATCHES

- Google has published Android's security advisory for the month of March. The patch contains fixes for dozens of vulnerabilities affecting Android's system and various components. Some of the vulnerabilities are considered critical, and could lead to remote code execution on an unpatched Android device.
- Cisco has released a security patch to address CVE-2023-20049, a denial of service vulnerability affecting many of the company's router products. The vulnerability allowed remote attackers to send malformed packets that would cause the router's line card to reset, triggering the denial of service condition.
- Fortinet has released an advisory covering CVE-2023-25610, a critical heap buffer underflow vulnerability affecting many of its products. The vulnerability is of critical severity, and could lead to either denial of service or remote code execution on unpatched Fortinet products.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have uncovered a cyber-espionage campaign by Chinese APT group SharpPanda. The campaign has targeted government entities in South-East Asia, and has utilized the Soul framework to establish access to vicitms' network and exfiltrate information.

  Check Point Threat Emulation and Anti-bot provide protection against this threat (Trojan.WIN32.SharpPanda)

- Researchers have observed multiple campaigns abusing Google advertisements to lead users to download malicious droppers masked as legitimate programs. In one campaign, the end stage payload was the RedLine stealer, while another would lead to Ursnif or Vidar infections.

  Check Point Threat Emulation provide protection against these threats (Trojan.Wins.RedLineStealer.ta.A/B/E and Infostealer.Win.RedLine.A-D)

- Analysis of a campaign targeting Indian and Pakistani Android users has been published. The targets were approached by romance scams on messaging apps, and were then convinced to chat via a supposedly more secure app, which turned out to be a remote access Trojan.
- A Chinese campaign targeting SonicWall Secure Mobile Access devices was discovered. In the campaign, the threat actors used a sophisticated malware capable of maintaining persistence in SonicWall security appliances even after firmware upgrades. The malware allowed theft of credentials and shell access to the device.
- Researchers have identified a new botnet malware dubbed GoBruteforcer, which is targeting web servers. The malware, which is written in Golang, attempts to gain access to web servers by brute force and deploys an IRC bot for C&C communication.