TOP ATTACKS AND BREACHES

- Information of more than 80,000 security professionals and law enforcement officers is being offered for sale online, after the FBI's information sharing portal InfraGard has been breached. The attacker has gained access to InfraGard after applying to join the platform impersonating a financial corporation's CEO, then using the credentials to run a script to download the database using the portal's API.

- California's Department of Finance has been targeted by the LockBit ransomware group. LockBit claims to have stolen over 75GB of data, and is threatening to leak it if the ransom is not paid. California's Governor Office has confirmed the attack.

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

- A database containing information of more than 75,000 Uber employees has been leaked on online forums. The data was stolen from 3rd party IT service supplier Teqtivity, which provides services to Uber. According to reports, no customer data was leaked in this breach.

- Colombian power company EPM has been the victim of a ransomware attack, causing disruption to its online services. Employees were instructed to work from home as the company's IT infrastructure and website were taken down. Ransomware gang BlackCat (ALPHV) has taken responsibility for the attack, and claims to have also exfiltrated data from the company.

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

- American sports streaming provider FuboTV claims a cyberattack disrupted its service, causing blackouts during the football world cup semifinal match between Morocco and France.

- FRV, the firefighting service in Victoria, Australia, has been forced to shut down its network after being targeted by a cyberattack. According to FRV, while online systems are shut down, communication and dispatching is operated manually.

- Social media analytics site 'Social Blade' has been breached. A database containing more than 5 million records of user data has been offered for sale on online forums. The company has confirmed the breach, but claims that no user payment information has been leaked.

VULNERABILITIES AND PATCHES

- Microsoft has released December's patch Tuesday, which includes fixes for 74 security vulnerabilities across Microsoft's products. Among the vulnerabilities, 7 are considered critical, and could lead to remote code execution if exploited on non-updated servers. According to Microsoft, one of the vulnerabilities had already been exploited in the wild before the patch.

  Check Point IPS provides protection against these threats *(Microsoft Windows Client Server Run-Time Subsystem Elevation of Privilege (CVE-2022-44673); Microsoft Windows Bluetooth Driver Elevation of Privilege (CVE-2022-44675); Microsoft Windows Kernel Elevation of Privilege (CVE-2022-44683))*

- Apple has released security updates for several products, including a fix for a critical zero-day vulnerability in iOS that may have already been exploited in the wild (CVE-2022-42856).

- Fortinet has published a security advisory addressing the critical severity vulnerability CVE-2022-42475, a buffer overflow vulnerability in FortiOS SSL-VPN which allowed remote code execution on an affected system. According to Fortinet, the vulnerability was actively being exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports that Emotet has returned after a quiet summer, now the second most prevalent malware globally. Qbot has also made it back onto the index for the first time since 2021, while the Education sector remains under attack.

- Check Point researchers have published a technical analysis of the Azov wiper. While referring to itself as Ransomware, Azov does not offer its victims any recourse towards decryption. Azov modifies native executable files on affected systems, injecting them with malicious code.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Wins.Azov.A)*

- A campaign targeting political entities in Japan was discovered. MirrorFace, a Chinese APT, has been targeting a Japanese political party using spearphishing emails to gain initial access. The attackers then installed multiple spyware tools to exfiltrate credentials, documents and email messages.

- Researchers have analyzed a campaign targeting Ukrainian government organizations. The attackers spread infected versions of Windows 10 installers in the Ukrainian language to spread malware, eventually leading to data exfiltration.

- An analysis of Iranian threat group APT35 has been compiled by researchers. The researchers have linked the threat group to the Iranian IRGC. The group has been targeting diplomats, politicians, journalists, activists and academics, using phishing, compromised accounts and malware to gain access and exfiltrate information.