TOP ATTACKS AND BREACHES

- Japan's Port of Nagoya, which handles 10% of Japan's trade volume, has shut down its activity for 2 days after being hit by a ransomware attack. The port's management attributed the attack to LockBit ransomware group.

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

- A February ransomware attack on the Law Foundation of Silicon Valley - a pro bono law firm from California, has now resurfaced as it reportedly lead to the exposure of information of nearly 42,000 people. The leak included Social Security numbers and other personal information, affecting both clients and staff members. The attack was claimed in March by the AlphV/Black Cat ransomware group.

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

- 500GB of data has leaked from American television channel Nickelodeon as a result of a suspected breach. The data includes scripts, animation files and full episodes of content, and has been confirmed by the TV channel as legitimate, yet decades old. The said breach occurred during January this year, due to an authentication vulnerability on a feedback portal.

- The Cyber Partisans, a Belarusian hacktivist group, is claiming to be behind a significant attack on the Belarusian State University (BSU). While the attack has been denied by the university, its systems are down and the hacktivist group claims to obtain 3 terabytes of data, and to have encrypted and wiped computers and servers, among others.

- The Ukrainian hacktivist group IT Army of Ukraine took responsibility for the confirmed DDoS attack on the website and mobile app of the Russian state-owned Railway Company RZD. The attack lasted several hours and reportedly affected the ability to purchase tickets online.

- Researchers have identified a BlackByte ransomware intrusion in a customer's environment, where the attack chain was completed in less than five days, leading to significant business disruption.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.Blackbyte)*

- Researchers have detected a new advanced Voice Phishing (vishing) attack toolset called 'Letscall'. It has been primarily targeting individuals in South Korea, yet has the potential to expand to other regions.

VULNERABILITIES AND PATCHES

- Progress Software has disclosed and patched another critical SQL injection vulnerability (CVE-2023-36934) in MOVEit Transfer. Exploiting this vulnerability could potentially provide unauthorized access to the MOVEit Transfer database.
- Over 300,000 Fortinet firewalls found at risk due to a critical remote code execution vulnerability (CVE-2023-27997; CVSS score of 9.8) in FortiOS. The vulnerability may have been exploited in attacks. Fortinet has released a security advisory urging users to update their firewalls to the latest firmware version.

  Check Point IPS provides protection against this threat *(Fortinet Multiple Products Heap-Based Buffer Overflow (CVE-2023-27997))*
- Google has published July's security advisory for Android, which includes fixes for 46 security vulnerabilities. Google claims that three of the vulnerabilities were being actively exploited in the wild.
- Decentralized social network Mastodon has issued a security update to fix critical vulnerabilities (including CVE-2023-36460) with the potential to affect millions of users.

THREAT INTELLIGENCE REPORTS

- Check Point Research uncovered a recent campaign called SmugX, targeting government entities in Europe, with a focus on foreign and domestic policy entities. The campaign utilizes HTML Smuggling, a technique in which attackers hide malicious payloads inside HTML documents. The campaign overlaps with a previously reported activity attributed to Chinese threat actors RedDelta and Mustang Panda.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Wins.MustangPanda; APT.Win.PlugX)*
- Check Point Research has released June 2023's threat index, highlighting that the Trojan Qbot has been the most prevalent malware so far in 2023. In addition, SpinOk mobile Trojan took top spot in June for the first time.
- Check Point Research shares insights and warnings regarding cybercriminals targeting online shoppers during Amazon Prime Day, occurring on the 11th and 12th of July, while already seeing an increase in fake Amazon websites used for phishing.
- The CISA and FBI have collaborated to issue an advisory addressing the growing threat of Truebot malware variants in the United States and Canada. This malware is employed by cybercriminal groups such as the CL0P Ransomware Gang and operates as a botnet.

  Check Point Threat Emulation provides protection against this threat *(Botnet.Wins.TrueBot)*