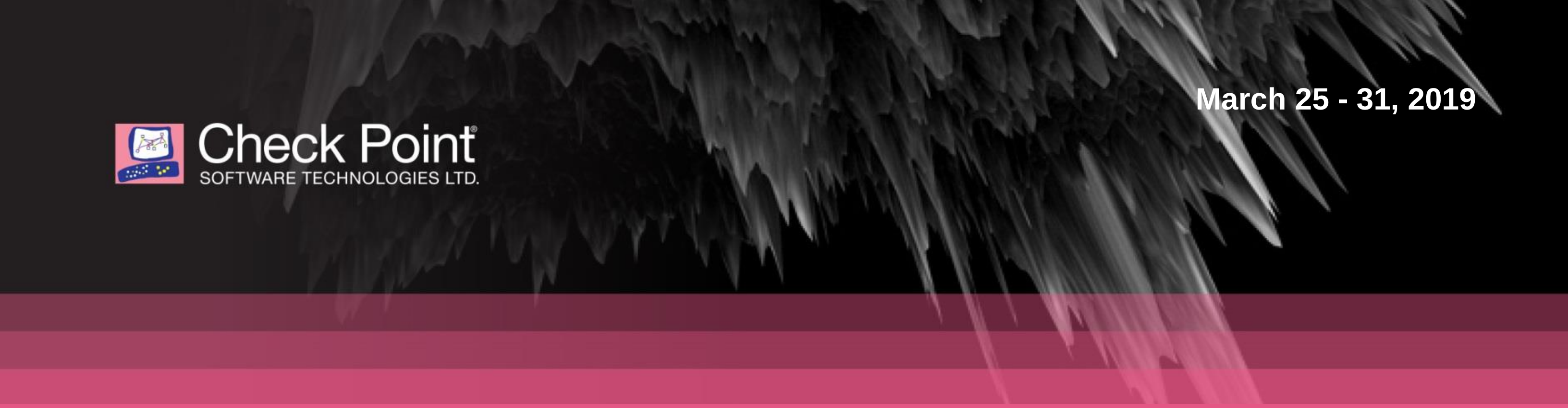

March 25 - 31, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- ASUS, one of the world's biggest computers companies, has unintentionally implanted backdoors on thousands of customer computers after hackers compromised its Live Update utility. The attack was apparently a part of a supply chain attack conducted by an APT group which surgically targeted a specific pool of users by hardcoding a list of MAC addresses into the malware.

- Toyota Motor Corporation has suffered a major data breach that exposed details and personal information of around 3.1 million customers after unknown attackers managed to gain access to one of the company's servers in Japan.

- Hackers have stolen nearly $19 million worth of cryptocurrency from the South-Korean cryptocurrency exchange Bithumb after compromising a number of EOS and XRP wallets belonging to the company. While still under investigation, it is believed that the hack was conducted with the help of an insider.

- A new credential harvesting campaign is targeting South Asian governments, using replica webpages of legitimate entities prompting the users to log into their mail accounts. The campaign, dubbed "LUCKY ELEPHANT", was apparently carried out by an Indian APT group.

- A new campaign of the North-Korean APT group Lazarus has been detected, targeting Windows and macOS users by delivering macro-weaponized documents containing malicious PowerShell scripts. The campaign is targeting companies in the crypto and fintech industries.

- The emergency tornado alarm systems of two towns in Texas have been compromised by hackers. The alarms went on and off repeatedly for about two hours in the middle of the night as a result of the attack, causing panic among residents.

- The recent activity of Iran-linked cyber-espionage group Elfin, also known as APT33, has been covered in a recent report after the group was observed actively targeting major organizations and institutions in the US and Saudi Arabia.

VULNERABILITIES AND PATCHES

- Two unpatched Zero-day vulnerabilities have been discovered in the latest versions of Microsoft Explorer and Edge browsers allowing remote attackers to bypass the same-origin security policy, which prevents websites from making unauthorized requests from other websites and passing content.

  Check Point IPS blade will provide protection against this threat in its next online package

- A critical flaw has been reported in Magento CMS platform, allowing remote attackers to perform SQL injection attacks and steal sensitive information from the databases of vulnerable websites.
- Security researchers have found 36 vulnerabilities in the LTE protocol used by most mobile carriers. The flaws may allow attackers to modify transferred data, spoof content, send or accept invalid messages.
- Privilege escalation and arbitrary code execution vulnerabilities have been discovered in Huawei PCManager tool, referenced as CVE-2019-5241 and CVE-2019-5242 respectively.
- A zero-day vulnerability has been found in TP-Link SR20 smart home routers, intended to connect IoT devices, which allows attackers on the same network to execute arbitrary commands as root user on connected devices and gain control of them.

THREAT INTELLIGENCE REPORTS

- A new variant of the AZORult data stealer has been observed in the wild, written in C++ and carrying the ability to establish Remote Desktop Protocol (RDP) connections to the compromised machines.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (InfoStealer.Win32.AZORult; Trojan.Win32.AZORult)

- A new ransomware, called Unnam3d R@nsomware, is moving victims' files into password-protected RAR archives and demanding a $50 Amazon gift card code in order to get the archive password.

  Check Point SandBlast provides protection against this threat

- Security researchers have discovered Gustuff, a new Android Banking Trojan utilizing accessibility services to autofill fields inside various banking and cryptocurrency applications in order to make fraudulent transactions. Gustuff infects users via compromised SMS messages and uses the infected device's contacts list to further spread the malware.

  Check Point SandBlast Mobile customers are protected from this threat

- Researchers have discovered a government Android spyware available on Google Play Store. The spyware, Exodus, disguises as service applications from mobile operators and aimed at Italian users.

  Check Point SandBlast Mobile customers are protected from this threat