March 12 - 18, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point security researches have revealed a new widespread mobile botnet dubbed 'RottenSys', infecting nearly 5 million Android devices. RottenSys malware family is originally used to aggressively display ads on users' devices. As part of the botnet that is currently being built, RottenSys will contain extensive capabilities including silently installing additional apps and UI automation.

  Check Point SandBlast Mobile customers are protected against this threat

- Russia-linked Sofacy APT targets a government agency in Europe using new version of their Flash Player exploit platform dubbed 'DealersChoice'. The new DealersChoice has been delivered via phishing emails referencing the "Underwater Defence & Security" conference, taking place in the U.K. this month.

  Check Point Anti-Virus blade provides protection against this threat (Trojan.Win32. DealersChoice)

- New campaign is targeting PostgreSQL DBs with a Monero Crypto-miner. The crypto-miner is embedded at the end of an image's binary code of the Hollywood actress 'Scarlett Johansson', and has earned its operators around $65K.

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

- 'Dofoil' malware, also known as Smoke Loader, has infected nearly 400K Windows computers with Electroneum crypto-miner during a 12-hour period. The campaign has exploited a backdoored version of the popular BitTorrent client called 'MediaGet'.

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

- China-linked APT15 has targeted contractors at various UK government departments and military organizations. In the attack, ATP15 have used two new backdoors named 'RoyalCLI' and 'RoyalDNS'. The backdoors allow dropping the malicious tools on the infected systems, and have been controlled remotely via Internet Explorer components.

VULNERABILITIES AND PATCHES

- Popular text editors for Unix and Linux systems have been found vulnerable to a critical privilege escalation flaw. The flaw may allow the attackers to run malicious code on victims' machines, and resides in the way these text editors load plugins.
- Critical vulnerabilities have been discovered in three popular VPN services - HotSpot Shield, PureVPN, and Zenmate, with millions of users worldwide. Successful exploitation allows an attacker to leak user's real IP addresses and locations, and redirect victim's web traffic to a malicious site.
- 13 critical vulnerabilities and exploitable backdoors have been found in AMD's Ryzen and EPYC lines of processors. The vulnerabilities may allow an attacker to access sensitive data, install persistent malware inside a chip, and gain full access to the compromised systems.
- A critical vulnerability has been discovered in Credential Security Support Provider protocol (CredSSP). The vulnerability affects all versions of Windows could allow remote attackers to exploit RDP and WinRM to steal authentication data and run malicious code remotely.

THREAT INTELLIGENCE REPORTS

- Check Point researches have conducted an in-depth research on the ransomware-as-a-service, GandCrab. According to the report, GandCrab's developers continuously improve their malware by adopting an AGILE development process.

  Check Point SandBlast Agent, SandBlast and Anti-Bot blades provide protection against this threat
  (Ransomware.Win.GandCrab.A; Trojan Ransom.Win32.GandCrab.A)

- A new variant of the FakeBank Android banking Trojan has been seen in the wild, currently active in South Korea. The malware is capable of intercepting victim's banking-related incoming and outgoing calls, and redirecting them to scammers that steals their banking information.

  Check Point SandBlast Mobile customers are protected against this threat

- New technique dubbed 'Mosquito' allows Air-Gapped PCs to covertly exchange data via ultrasonic waves, exploiting an audio chip feature to create a speaker-to-speaker communication channel. As part of it, it converts connected speakers such as headphones or earphones into a listening device.
- Security researchers have uncovered a Mac App that mines Monero cryptocurrency in exchange for free access to premium account, as the default feature. The app, dubbed Calendar 2, causes the miner to consume more resources of the CPU than intended, and also continues the mining process even if users have cancelled the default setting