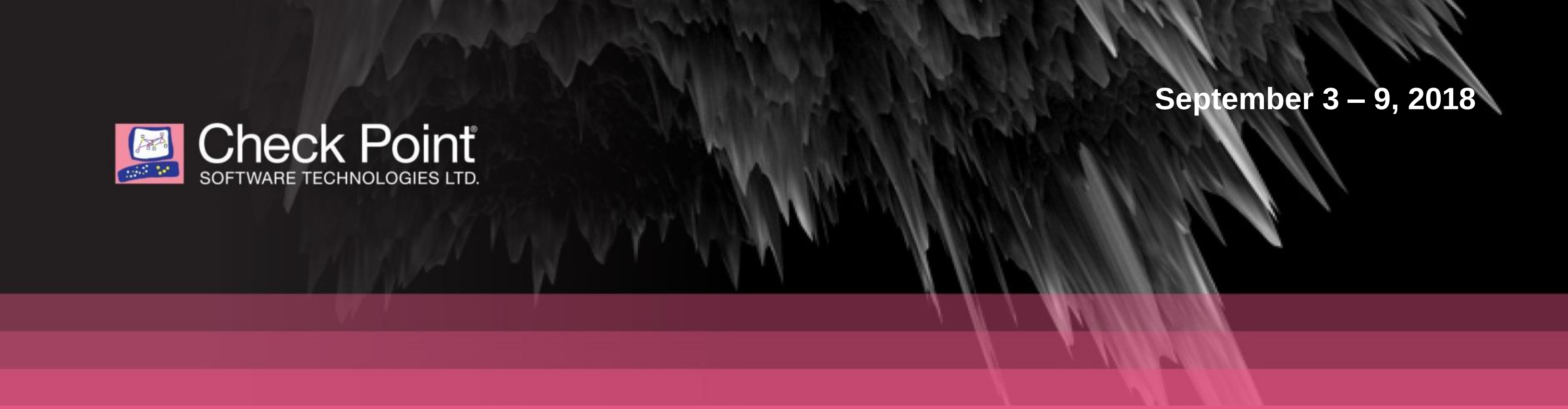

Check Point
SOFTWARE TECHNOLOGIES LTD.

September 3 – 9, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point security researches have revealed ‘Domestic Kitten’, an ongoing targeted surveillance operation that originates in Iranian government entities. Through the use of mobile applications, the operation uses decoy content to entice victims to download the applications, which are in fact loaded with spyware collecting massive amount of sensitive details.

  Check Point SandBlast Mobile customers are protected from this threat

- Security researches have revealed a new campaign attributed to the Iran-linked APT, OliRig, targeting a Middle East government entity. The campaign leverages a new variant of the OopsIE Trojan that implements new evasion capabilities including anti-analysis and anti-virtual machine capabilities.

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

- British Airways has fallen victim to a major data breach exposing personal details of up to 380,000 of its customers. The stolen data includes customers' names and addresses, along with financial information and credit card data used for flight booking.

- Schneider Electric, the energy and Automation Corporation, has revealed that USB drives shipped with the "Conext ComBox" and "Conext Battery Monitor” products were infected with malware. The USB drives were probably exposed to a malware during manufacturing at a third-party supplier’s facility.

- The chrome extension MEGA has been hacked and replaced by a malicious version of the extension in the web store. The compromised version featured login credentials and cryptocurrency key theft. Upon discovery, Google removed it from the Chrome web store.

- A new threat group dubbed ‘PowerPool’ has been carrying out a malicious campaign which targets multiple countries including Germany, Chile, India and Russia. The malware spread in the attack exploits a zero-day vulnerability which was exposed during August 2018.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.Win32.PowerPool)

VULNERABILITIES AND PATCHES

- Multiple vulnerabilities have been discovered in Opsview Monitor, IT monitoring software for networks and applications. The flaws could allow an attacker local privilege escalation and remote code execution.
- Privilege escalation bug has been found in the popular VPN clients "NordVPN" and "ProtonVPN" used to set up a secure tunnel. The bug may allow an attacker to run arbitrary code that may pass on to the service and execute with system rights under Windows.

  Check Point IPS blade provides protection against this threat (Cisco Smart Install Remote Code Execution)
- Cisco has released a security patch addressing 32 vulnerabilities, Three of which are rated critical, including the Apache Struts remote code execution vulnerability already exploited in the wild.

  Check Point IPS blade provides protection against this threat (Apache Struts Remote Code Execution, Adobe Acrobat and Reader Use after Free)

THREAT INTELLIGENCE REPORTS

- Security researchers have discovered that the new exploit kit 'Fallout' is being used in a Malvertising campaign to distribute GandCrab Ransomware in the Middle East. Fallout fingerprints the user browser profile and delivers malicious content if the user profile matches a target of interest.

  Check Point SandBlast and IPS provide protection against this threat (Fallout Exploit Kit Landing Page)
- Security researches have managed to decrypt 512-bit RSA key and reveal a new piece of malware exploiting an Adobe Flash zero-day exploit. Dubbed "Chainshot", the malware has been leveraged on multiple targeted attacks to activate a downloader for the final payload in a malicious chain reaction.
- Security researchers have discovered that thousands of vulnerable MikroTik routers have been compromised, allowing remote attackers to monitor and capture all of their network traffic, and to perform CoinHive mining code injection.

  Check Point IPS blade provides protection against this threat (MikroTik RouterOS Winbox Authentication Bypass)
- A new Monero Cryptomining campaign has been uncovered, exploiting the Apache Struts vulnerability. Dubbed "CroniX", the malware targets Linux systems and has the abilities to halts other cryptojacking activity, kill process utilizing 60% of the CPU or more, and launch executables with fake process names.

  Check Point IPS blade provides protection against this threat (Apache Struts Remote Code Execution)