Check Point
SOFTWARE TECHNOLOGIES LTD.

Dec 13 – 19, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has reported that an Iranian threat group commonly associated with the local regime, “Charming Kitten”, has been attempting to exploit the Log4j vulnerability against 7 Israeli targets in Government and business sectors.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*

- State-sponsored Iranian APT group MuddyWater has allegedly targeted an Asian airline with a new backdoor called “Aclip” that uses Slack to obfuscate operational communications. It is likely that threat actors successfully accessed reservation data in the process.

- British online classified advertisement website Gumtree.com has suffered a data leak and confirmed that attackers accessed customers email addresses, contact names and phone numbers only by pressing the F12 key in a web browser to see the site’s HTML source code.

- Conti Ransomware gang is leveraging the Log4j flaw as initial access for lateral movement on VMware vCenter affecting US and Europe based networks.

  Check Point Harmony Endpoint, IPS, Threat Emulation and Anti-Bot provide protection against this threat

- Microsoft Exchange Outlook Web Access servers are being targeted by hackers leveraging a malicious IIS web server module “Owowa” in an attempt to steal credentials and remotely execute commands.

- Researchers warn of a phishing campaign taking advantage of the new “Spider-Man: No Way Home” movie release: Phishing sites requiring registration with credit card details for victims to purchase copies of the movie are used to steal payment info and infect the system with Trojans and Adware.

- The TinyNuke malware is again propagating in France in a credential and data theft campaign targeting logistics, transportation and other sectors: threat actors are using invoice-themed email bates containing a ZIP executable that will drop the payload.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat

VULNERABILITIES AND PATCHES

- Google researchers have analyzed the NSO group "zero-click" exploit and found that it is possible for a mobile device to be compromised only by receiving an SMS via iMessage. Experts qualified the exploit as the most "sophisticated and terrifying they've ever seen".
- Lenovo laptops are vulnerable to two flaws; CVE-2021-3922 and CVE-2021-3969 which are privilege elevation vulnerabilities in the ImControllerService. Hackers could execute commands with administrator privileges and install malware.
- Microsoft requested admins to immediately update the latest Minecraft server to protect against new Khonsari Ransomware attempts to leverage the Log4j vulnerability CVE-2021-44228.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*
- Western Digital urges its users to upgrade their WD My Cloud devices to get security updates on the firmware to protect their data from attacks leveraging CVE-2021-35941 (Authenticated factory reset flaw) and CVE-2018-18472 (Critical root command execution flaw).

  Check Point IPS provides protection against this treat *(Western Digital MyBook Live Remote Code Execution (CVE-2018-18472))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has spotted "Twizt", a new variant of the Phorpiex botnet responsible for stealing nearly half a million dollars' worth of cryptocurrency through a technique called "crypto clipping". Twizt can steal cryptocurrencies during transactions by automatically substituting the intended wallet address with the threat actor's wallet address and can operate without active C&C servers.

  Check Point Anti-Bot provides protection against this threat *(Worm.Win32.Phorpiex)*
- Check Point Research has discovered a Win32 executable Trojan identified as StealthLoader, installed through exploits of the Log4j flaw. StealthLoader delivers a crypto coin miner to the infected machine.

  Check Point Threat Emulation provides protection against this threat
- Meta has banned a few spy-for-hire companies from its platform, accusing them of running fake accounts to target tens of thousands people for surveillance purposes, in more than 100 countries.
- The Anubis banking Trojan is being leveraged in cybercrime campaign impersonating the French telecommunication provider Orange. The malware can extract finance related data and more from the victim's device after encouraging them to disable Google Play Protected.

  Check Point Harmony Mobile provides protection against this threat