Check Point
SOFTWARE TECHNOLOGIES LTD.

Nov 22 – 28, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- GoDaddy has announced they suffered a data breach with data of up to 1.2 million of its customers being exposed after an unauthorized person used a compromised password to gain access to the company's Managed WordPress hosting environment.
- Iranian airline Mahan Air has been victim of a cyber-attack which resulted in its website going offline. The company still operated its flights on schedule without major disruptions.
- A threat group is leveraging a new custom-made malware called “Tardigrade”, which is spread via phishing emails or infected USB drives, to attack biomanufacturing companies. The attacks aim at intellectual property theft and eventually infect the systems with a ransomware.
- Security analysts have discovered a new malware campaign on Huawei's AppGallery catalog which led to 9,300,000 downloads from 190 different games containing the Android Trojan Cynos that is able to collect user phone number, device location and other parameters.
- A new Iranian threat actor is stealing Google and Instagram credentials belonging to Farsi-speaking targets worldwide by leveraging a Microsoft MSHTML RCE flaw tracked CVE-2021-40444 and using a new PowerShell-based stealer called PowerShortShell.

  Check Point IPS, Anti-Virus and Anti-Bot protect against this threat *(Microsoft Internet Explorer MSHTML Remote Code Execution (CVE-2021-40444); HEUR:Exploit.MSOffice.CVE-2021-4044)*

- IKEA is currently victim of a cyberattack where threat actors are targeting employees in internal phishing attacks using stolen reply-chain emails – replying on legitimate internal emails and attaching or linking to malicious documents. IKEA suppliers and business partners are compromised as well.
- A new malware campaign has been discovered on Discord deploying the Babadeda crypter to hide malware that targets cryptocurrencies, NFTs, and DeFi communities.

VULNERABILITIES AND PATCHES

- Check Point Research has identified security flaws in the smartphone chip made by Taiwanese manufacturer MediaTek, used in 37% of the world's smartphones. The security flaws were found inside the chip's audio processer. MediaTek patched the vulnerabilities, which could have enabled a hacker to eavesdrop on Android users, elevate privileges and execute commands.

  Check Point Harmony Mobile provides protection against this threat

- A researcher has demonstrated how the patch for CVE-2021-41379 can be bypassed, enabling elevation of privileges in Windows 10 and 11 and Windows Server.

- Unofficial patches have been made available to protect Windows users from a local privilege escalation zero-day flaw in the Mobile Device Management Service concerning all Windows 10 versions.

THREAT INTELLIGENCE REPORTS

- Security researchers have found CronRAT, a new remote access Trojan for Linux servers that conceals itself by hiding in tasks scheduled for execution on a date that does not exist, February 31st. The malware is used to enable server-side Magecart data theft.

- The FBI is warning of a surge in spear-phishing email campaigns targeting customers of "brand-name companies", delivered in both emails and SMS messages.

- A new JavaScript based malware strain called RATDispenser is being used to deliver remote access Trojans and info stealers and potentially steal cryptocurrency information. The delivery vector is a malicious email with an executable attachment.

- Researchers have set up 320 publicly accessible honeypots to see how quickly malicious actors would target exposed cloud services, and report that 80% of them were compromised in under 24 hours. All honeypots were compromised within a week.

- Researchers have spotted the TrickBot malware that evades detection by checking the screen resolution of a victim system, only executing on standard configurations.

For comments, please contact: TI-bulletin@checkpoint.com