Nov 29 – Dec 5, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has identified ongoing campaigns in Iran using socially engineered SMS messages to infect tens of thousands of citizens' devices. The SMS, impersonating Iranian government services, lures victims into downloading malicious Android apps that steal credit card credentials, personal SMS messages and 2FA codes. Threat actors then proceed to make money withdrawals, and turn infected devices into a bot, spreading the malware to others.

  Check Point Harmony Mobile provides protection against this threat

- Apple has alerted Foreign Service officers of several US Embassies that their iPhones were compromised by unknown attackers using ForcedEntry to deploy the NSO group spyware Pegasus, allowing to steal files, eavesdrop on calls and track the targets' movements.
- North Korean cyberespionage group ScarCruft (APT 37) is targeting South Korean journalists, activists, or politically relevant individuals with spear-phishing emails and smishing campaigns deploying the Chinotto backdoor.
- SideCopy Pakistani Hackers are targeting Indian and Afghan military and government officials to steal Google, Twitter and Facebook credentials to eventually gain access to government portals.
- A hacktivist threat group dubbed WIRTE, suspected to be part of the "Gaza Cybergang", has been conducting campaigns on Middle Eastern governmental targets and other high-profile organizations since at least 2019, using malicious Excel 4.0 macros.
- Los Angeles Planned Parenthood has announced being victim of a ransomware attack in October that caused a breach affecting the data of 400,000 patients, including some clinical information like diagnosis and procedures.

VULNERABILITIES AND PATCHES

- Researchers have found vulnerabilities concerning 150 multi-function printers from Hewlett Packard: CVE-2021-39237 which requires physical access could lead to information disclosure and CVE-2021-39238 - a buffer overflow that could give a way to remote code execution.
- Researchers have discovered the EwDoor botnet which targets compromised AT&T enterprise network edge devices by exploiting a severe blind command injection security flaw tracked as CVE-2017-6079.
- BlackByte ransomware affiliates are actively exploiting ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523 & CVE-2021-31207) to compromise Microsoft Exchange servers and install web shells, coin miners and ransomware.

  Check Point IPS, Harmony Endpoint and Anti-Virus provide protection against these threats *(Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Microsoft Exchange Server Security Feature Authentication Bypass (CVE-2021-31207); Ransomware.Win32.BlackByte)*
- Hackers are leveraging the CVE-2021-44077 flaw which allows unauthenticated remote code execution in the business software provider Zoho; CISA & the FBI urge organizations to promptly update and patch.

THREAT INTELLIGENCE REPORTS

- In a new phishing campaign in the UK, threat actors are exploiting the new COVID-19 variant Omicron to lure victims by emailing them about a free Omicron PCR test, eventually stealing their payment details.
- Finland's National Cyber Security Centre is warning of a large campaign targeting Finnish Android users with the FluBot banking malware, spread via SMS.

  Check Point Harmony Mobile provides protection against this threat
- The FBI warns that the Cuba ransomware gang attacked the networks of 49 US organizations making at least $43.9 million in ransom payments. Initial infection is done through the Hancitor malware.

  Check Point Threat Emulation provides protection against this threat *(Trojan.Win.Hancitor)*
- Indian, Russian and Chinese APT groups were found to be using a rich text format (RTF) template injection technique in their recent phishing campaigns.
- The Emotet malware is now spread through malicious Windows App Installer packages disguised in Adobe PDF.

  Check Point Threat Emulation provides protection against this threat *(Trojan.Wins.Emotet)*