Check Point
SOFTWARE TECHNOLOGIES LTD.

Sept 13 - 19, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has seen a global surge in the black market for fake COVID-19 vaccine certificates on Telegram, following US President Biden's vaccine mandate announcements. The black market has expanded to serve 28 countries, including Austria, UAE, Brazil, UK, Singapore and more. The price for fake vaccine certificates has jumped globally, including in the US, where the price doubled from $100 to $200.
- The South Africa Ministry of Justice has been a victim of a ransomware attack which encrypted all of its systems and caused child maintenance payments to be suspended.
- Japanese Medical technology company Olympus has announced being victim of a ransomware attack that impacted their EMEA IT systems: the ransom note leads to a possible BlackMatter group attribution.
- The US Republican Governors Association has been targeted in March by Chinese group Hafnium exploiting Microsoft Exchange email servers.
- State-sponsored APT groups have been exploiting a vulnerability in a Zoho single sign-on and password management solution, allowing attackers to take over vulnerable systems.
- Microsoft has announced that several threat actors are exploiting the newly patched Windows MSHTML remote code execution security flaw CVE-2021-40444, using malicious Office documents.

  Check Point IPS provides protection against this threat *(Microsoft Internet Explorer MSHTML Remote Code Execution (CVE-2021-40444))*
- The US Federal Trade Commission is warning of sextortion schemes aimed at the LGBTQ+ community on online dating apps like Grindr and Feeld: After luring victims into sending sexually explicit photos of themselves, scammers threaten to leak them to third parties should victims refuse to send payment.
- A Zloader campaign is disabling Microsoft Defender Antivirus on computers to avoid detection. New attack vectors include TeamViewer Google ads, redirecting targets to fake download websites.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Banker.Wins.Zloader)*

VULNERABILITIES AND PATCHES

- Four security flaws have been reported in Microsoft's Open Management Infrastructure (OMI) agents installed on Azure Linux VMs. The vulnerabilities could allow privilege escalation and remote code execution. Following the report, these vulnerabilities are widely exploited in the wild.

  Check Point IPS provides protection against this threat *(Microsoft Open Management Infrastructure Remote Code Execution (CVE-2021-38647))*

- Apple has issued security patches for two zero-day vulnerabilities exploiting iPhones and Macs, tracked as CVE-2021-30860 and CVE-2021-30858, allowing malicious documents to execute commands and giving way for infections from highly invasive NSO group Pegasus spyware.

- After releasing 60 updates, including a patch for the PrintNightmare vulnerability CVE-2021-36958, Microsoft informed of network printing problems on a large scale. CVE-2021-36958 has been commonly exploited by threat actors & ransomware gangs to obtain system privileges on vulnerable devices.

- Driver flaw CVE-2021-3437 is exposing millions of HP OMEN gaming computers to an attack that can lead hackers to trigger denial-of-service or escalate privileges and disable security solutions.

- Google has issued Chrome 93.0.4577.82 for Windows, Mac, & Linux to patch eleven vulnerabilities, including two zero-days, CVE-2021-30632 and CVE-2021-30633 already exploited in the wild.

  Check Point IPS provides protection against this threat *(Google Chrome V8 Out-of-Bounds Write (CVE-2021-30632))*

THREAT INTELLIGENCE REPORTS

- The Biden administration has announced they would start sanctioning against crypto exchanges, wallets, and traders that ransomware threat actors use to convert ransom payments into fiat money.

- Security experts have found malicious Linux binaries made for the Windows Subsystem for Linux (WSL), showing that hackers are looking for new procedures to compromise Windows computers.

- Online romance scams have caused losses of more than $113 million since early 2021 according to the FBI. In these scams, attackers typically reach out to their victims via dating apps, and convince them to invest money in fraudulent websites or applications.

- Security researchers have found an unofficial Cobalt Strike Beacon version for Linux used in attacks targeting organizations globally.

  Check Point Anti-Bot provides protection against this threat *(Backdoor.Win32.CobaltStrike)*

- The Grief ransomware gang has warned their victims they would delete the encryption key used to retrieve their files and data if they attempted to hire the services of a negotiation firm.