Check Point Research
WEEKLY INTELLIGENCE REPORT
August 8-14, 2022

TOP ATTACKS AND BREACHES

- Cisco confirms it has been breached by the Yanluowang ransomware group in late May 2022. The initial access was gained after the threat actor gained an employee's Google account credentials, saved in their browser, and after getting an MFA push accepted by the user. The company says that while there have also been signs of pre-ransomware activity, no ransomware has been deployed on Cisco's systems. Additionally published are the claims of the attackers, which claim to have obtained 2.8GB of data and source code - claims which have been minimized by the company.

- 7-Eleven Denmark confirmed that a ransomware attack was behind the closure of 175 stores in the country last week, without revealing information on the group responsible. The company didn't mention if the attackers also stole data in addition to encrypting their systems. No ransomware operation has claimed responsibility for the attack yet.

- Researchers have detected a wave of attacks generated during January 2022, towards military industrial complex enterprises and public institutions in Eastern Europe and Afghanistan. These attacks were linked to a successful campaign by the Chinese APT tracked TA428, which used a new Windows malware as a backdoor to the networks of dozens of targets, sometimes hijacking their IT infrastructure.

- The pro-Russian hacker group Killnet publicly targeted Lockheed Martin this past week, calling other hacker groups to join in on attacks. At this point Killnet claims to be responsible for a recent DDoS attack on the company, and tells they have obtained personal data of the company's employees; claims which were denied by the American corporation.

- Researchers found that a cross-platform instant messenger application, popular among the Chinese market and known as 'MiMi', has been Trojanized since late May 2022 with a backdoor named rshell as a part of APT27's new campaign.

- CISA and FBI warn organizations in the US of the resurfacing of Zeppelin ransomware as a service, which has evolved with new attack and encryption tactics in its recent campaigns, and continues to target various industries with emphasis on the health sector, as well as critical infrastructure organizations.

  Check Point Harmony Endpoint, Threat Emulation and Anti-Virus provide protection against this threat *(Ransomware.Win32.Zeppelin.TC)*

VULNERABILITIES AND PATCHES

- Check Point Research analyzed the payment system built into Xiaomi smartphones powered by MediaTek chips. During these reviews, CPR discovered vulnerabilities that could allow forging of payment packages or disabling the payment system directly, from an unprivileged Android application.

- Microsoft issued a total of 121 patches in its August Patch Tuesday, including fixes for the actively exploited zero-day vulnerability tracked CVE-2022-34713 (aka 'DogWalk') - Microsoft Windows Support Diagnostic Tool (MSDT) remote code execution vulnerability.

  Check Point Threat Emulation and IPS provide protection against this threat *(Exploit.Multi.CVE-2022-34713.a.TC.*; Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution (CVE-2022-34713))*

- Cisco patched a high severity vulnerability (tracked CVE-2022-20866) affecting its Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software. Successful exploitation can allow unauthenticated attackers to retrieve an RSA private key remotely.

THREAT INTELLIGENCE REPORTS

- Researchers at Spectralops.io, a Check Point company, have detected ten malicious packages on PyPI, a leading repository of software for the Python programming language. The security threat allows malicious actors to run malicious code on target machines, enabling attackers to steal private data and personal credentials of developers. The threat actors would leverage misleading names and descriptions of familiar packages to dupe users into installation.

- The US State Department offers a $10 million reward for information on five individuals associated with the notorious and dismantled Conti ransomware group, alongside reveling the face of a member of the operation and details regarding the other operators and their additional associations.

- Researchers have followed the evolution of the Android banking Trojan SOVA that targets over 200 financial applications, and has evolved rapidly since its first release in September 2021. In its latest versions, the malware improved its code to help operating in a stealthier manner, and added an interesting new Android ransomware module.

  Check Point Harmony Mobile provides protection against this threat

- Several groups (Silent, Quantum, and Roy/Zeon), which split from the Conti operation, have taken on its phishing tactic named BazarCall ('call-back') as a leading method to obtain access to victims' network. This supplies a more trustworthy social engineering layer that makes early detection more difficult.

- Meta published the actions they took against two espionage operations (by Bitter APT and APT36) in South Asia, which used its social media platforms to distribute malware to potential targets.