Oct 25 – Nov 1, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A cyberattack has disrupted gasoline sale in Iran. Fueling machines showed a message saying "cyberattack 64411", the number being the phone number for the office of Iran's Supreme Leader, and a reference to the attack on Iran's railway system attributed to the Indra attack group.

- The North Korean threat group Lazarus (AKA Hidden Cobra) has conducted a supply-chain campaign against IT companies and think tanks. They used a new variant of the BLINDINGCAN backdoor in combination with the MATA framework and some of their old malware.

  Check Point Threat Emulation, Anti-Virus and Anti-Bot provide protection against these threats *(RAT.Win32.BLINDINGCAN; Trojan.Win32.MATA; Botnet.Win32.HiddenCobra)*

- Data of a healthcare patients of Fullerton Health in Singapore, both personal and financial, has been breached. Threat actors attacked a third party vendor, Agape Connecting People, providing an appointment booking platform to Fullerton.

- The Black Shadow threat actors have breached systems of the Israeli Internet company Cyberserve, causing disruptions for many Israeli websites. During this attack, the hackers stole the private data located on the servers and published a part of it, including data belonging to the LGBTQ dating app Atraf.

- Cybercriminals have started selling variants of the Snake malware on dark web forums for as low as $25. This could explain the spike that Check Point researchers see in Snake's use in recent campaigns.

  Check Point Anti-Bot and Threat Emulation provide protection against this threat *(Backdoor.Win32.Snake; Ransomware.Win.Snake)*

- Security researchers have uncovered a new phishing campaign distributing the Squirrelwaffle loader to install malware such as Cobalt Strike and Qbot. Squirrelwaffle also communicates with a remote server in order to collect secondary payloads, making it a versatile tool.

  Check Point Anti-Bot and Threat Emulation provide protection against these threats *(Win32.CobaltStrike; Trojan-Downloader.WIN32.Qbot)*

VULNERABILITIES AND PATCHES

- A security researcher has discovered a Windows zero-day vulnerability tracked as CVE-2021-34484, which could allow privilege elevation. The exploit affects all versions of Windows and requires a threat actor to know another user's user name and password to trigger the vulnerability.
- Threat actors target macOS systems using the Shrootless vulnerability - CVE-2021-30892. The flaw enables a malicious actor to create a specially crafted file intended to hijack the installation process. The bug was fixed in Apple's latest security update.
- The recently disclosed high-severity vulnerability in the OptinMonster plugin affects roughly a million WordPress websites. The flaw, tracked as CVE-2021-39341, allows unauthorized API access to sensitive information. All OptinMonster plugin users are advised to upgrade to version 2.6.5 or above.
- Adobe has provided urgent fixes for 92 vulnerabilities, more than 60 of which pose a risk of remote code execution. Adobe claims that the bugs were not exploited in the wild.
- CISA urges admins to patch a critical vulnerability in the Discourse forum, tracked as CVE-2021-41163. With a CVSS score of 10/10. the flaw could allow an unauthenticated threat actor to execute code remotely. Forum admins should update their systems to version 2.7.9 or later.
- Google has released a new version of Chrome, which contains a fix for a total of seven vulnerabilities, with two being zero-days that are known to have been exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Researchers have uncovered a new Hive ransomware variant that encrypts Linux and FreeBSD operating systems. This version is still buggy but expected to be fixed soon.
- The FBI has released an alert saying that the Ranzy Locker ransomware operators compromised at least 30 US companies this year. Most victims said that the hackers infiltrated their networks via brute-forcing RDP credentials, exploiting vulnerable Microsoft Exchange servers, or using stolen credentials.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Hive)
- Threat actors have used 151 Android apps with 10.5 million downloads to subscribe victims to premium subscription services. 80 of the apps in the "UltimaSMS" campaign were found on Google Play. The attackers likely made millions of dollars in fraudulent subscription charges.

  Check Point Harmony Mobile provides protection against this threat
- Researchers have discovered a new sophisticated Android malware dubbed AbstractEmu. This malware is equipped with root capabilities and can take complete control of infected devices while evading detection. The malware was bundled with legitimate apps, and distributed via well-known app stores.

  Check Point Harmony Mobile provides protection against this threat