Check Point
SOFTWARE TECHNOLOGIES LTD.

Jan 31 – Feb 6, 2022

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A significant Ransomware attack has disrupted operations of oil port terminals in Belgium, Germany and in the Netherlands, affecting at least 17 ports and resulting in difficulties loading and unloading refined product cargoes. The BlackCat cybercrime group is suspected to be the group behind the attack.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win.BlackCat.A-F)*

- Email accounts of News Corp journalists have been hacked as part of an espionage campaign, allegedly linked to APT actors from China. The breach is potentially jeopardizing confidential sources' anonymity.

- Russian affiliated threat actor Gamaredon is believed to be behind a cyberattack against a western governmental entity in Ukraine last month and has been active in the country since at least October.

- Researchers have found a new campaign targeting Turkish private organizations and governmental institutions attributed to Iranian state sponsored group MuddyWater. The group now uses canary tokens to track targets' infection and possibly to evade sandbox-based detection systems.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat

- A spear phishing campaign is exploiting a cross-site scripting (XSS) vulnerability in the Zimbra email platform. The campaign, called "Operation EmailThief", is allegedly distributed by Chinese actors.

- Airport services and management company Swissport has been victim of a ransomware attack on its IT infrastructure. The company announced that the attack was largely contained but the disruption caused delays for 22 flights for about 20 minutes.

- British food company KP Snacks has been hit by a Conti ransomware attack that could disrupt deliveries to supermarkets until at least the end of March. Conti appears to have stolen data and is now also "double-extorting" KP Snacks.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win32.Conti)

VULNERABILITIES AND PATCHES

- Cisco has released patches for several flaws in Cisco Small business RV series routers (RV160, RV260, RV340 and RV345) including a critical vulnerability tracked as CVE-2022-20699, which could let an unauthenticated remote hacker execute arbitrary code on the device.
- A new critical flaw tracked as CVE-2021-44142 has been found in Samba software and could allow a remote unauthenticated hacker to read or write arbitrary data from memory without having to secure administrative privileges on the affected installations.
- Tech vendor 42 Gears has released patches for a series of laws in MDM platform in web console and Linux agent, including remote code execution, command injection, hardcoded password, local privilege escalation and information disclosure vulnerabilities.
- WordPress plugin Essential Addons for Elementor is vulnerable to a critical remote code execution flaw that could enable a local file inclusion attack.

THREAT INTELLIGENCE REPORTS

- Iran linked APT35 group (aka Charming Kitten, Phosphorus) has upgraded its toolkit and is now leveraging a new PowerShell-based implant named “PowerLess Backdoor”. The code runs in a .NET application and won’t launch powershell.exe, allowing evasion from security defenses.
- BlackCat ransomware members (aka ALPHV) have previously been part of the BlackMatter/DarkSide ransomware operations.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win.BlackCat.A-F)
- The same flaw in Apple software exploited by the NSO group in iPhones, has been simultaneously leveraged by a competing Israeli firm called QuaDream. The flaw allows for a remote intrusion into iPhones without the need to open any malicious link.
- Researchers have found that Iranian threat group MosesStaff now uses previously unknown Remote Access Trojan StrifeWater as part of their ransomware arsenal. The RAT is leveraged in the initial stages of attacks and has the ability to remove itself from the system to cover tracks.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
- Chinese-linked APT cyberespionage group Antlion (aka Pirate Panda, Tropic Trooper) has been targeting Taiwanese financial organizations, exfiltrating sensitive data with custom backdoors.