Jan 17 – 23, 2022

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new cyber-espionage campaign by the Arabic-speaking APT group Molerats (aka Gaza Cybergang) has been targeting victims in the Middle East, specifically high-profile targets in the banking, NGOs and political sectors in Palestine and Turkey. The group leverages cloud services like Google Drive or Dropbox to host malicious payloads and for command-and-control.

  Check Point Threat Emulation provides protection against this threat

- The cryptocurrency exchange platform Crypto.com has announced that 483 user accounts were compromised in a recent hack, resulting in $35 million worth of unauthorized withdrawals.

- A Red Cross contractor was victim of a cyberattack which resulted in a breach of personal data concerning over half a million people of the refugees program “Restoring Family Links”. The incident forced the Red Cross to shut down the IT systems supporting the program.

- A new password stealing malware dubbed BHUNT has been targeting crypto wallets worldwide, most victims being in India. BHUNT is suspected to be using cracked software installers as an infection vector.

- The Central Bank of Indonesia has announced that their networks were hit by a ransomware attack last month. Threat actors stole non-critical data concerning the Bank’s employees before encrypting the systems. The Conti gang has claimed the attack after leaking part of the allegedly stolen files.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)

- A new email phishing campaign is impersonating Maersk Shipping to lure victims into downloading the STRRAT remote access Trojan. Once installed, it can steal information and pop ransom notes for a fake ransomware, to distract the victim from the data leak.

  Check Point Threat Emulation provides protection against this threat

- A significant cyber-espionage phishing campaign has been targeting 15 entities, mostly in the energy and industrial sectors, since at least 2019.

VULNERABILITIES AND PATCHES

- Zoho has released a patch for a critical flaw (CVE-2021-44757) in Desktop Central and Desktop Central MSP that could be leveraged to read unauthorized data or write an arbitrary .zip file on a server.
- McAfee Enterprise has issued a patch for CVE-2022-0166, a high severity local privilege escalation vulnerability that could allow threat actors to execute arbitrary code with SYSTEM privileges.
- Two critical security vulnerabilities in Control Web Panel (CVE-2021-45467 and CVE-2021-45466) could be leveraged to achieve pre-authenticated remote code execution on compromised servers.
- Cisco Systems has released a fix for CVE-2022-20649, a critical remote code execution vulnerability in Redundancy Configuration Manager for StarOS software that could be leveraged by a remote hacker to execute arbitrary code and take control of the affected computers.

THREAT INTELLIGENCE REPORTS

- Check Point Research has found that in Q4, DHL replaced Microsoft as the most imitated brand in phishing attacks trying to steal victims' credentials and payment details.
- A new UEFI firmware-level rootkit dubbed MoonBounce has been deployed by the Chinese-speaking group APT41, aka Winnti. Researchers found that the backdoor is used to enable the deployment of user-mode malware that will execute further payloads from the internet.

  Check Point Threat Emulation provides protection against this threat *(Backdoor.Win32.Winnti)*
- Interpol and the Nigerian Police Force have arrested 11 suspects connected to an international business email compromise (BEC) campaign that targeted over 50,000 victims.
- A new phishing campaign is imitating the US Department of Labor with emails that are sent from spoofed domains, inviting the recipients to submit bids to eventually steal their Office 365 credentials.
- The FBI has officially linked the Diavol ransomware operation to the TrickBot hacking group.

  Check Point Harmony Endpoint and Anti-Bot provide protection against these threats
- Experts have found an Internet Relay Chat (IRC) bot written in Go programming language, disguised as adult games, and being leveraged to target Korean users with denial-of-service (DDoS) attacks.
- A coalition of 10 law enforcement authorities from different countries coordinated by Europol has taken down VPNLab.net that was used by ransomware actors and cybercriminals for malware distribution.
- Researchers have found that White Rabbit, a newly discovered ransomware family, is possibly linked to the financially motivated group FIN8.