Check Point Research

WEEKLY INTELLIGENCE REPORT

July 4 – 10, 2022

TOP ATTACKS AND BREACHES

- An anonymous hacker identified as “ChinaDan” has claimed to have a stolen a database from the Shanghai National Police (SHGA) that includes sensitive data of 1 billion Chinese citizens, and offered to sell it for 10 bitcoins (approximately $200,000). He allegedly stole more than 22 terabytes of data including names, addresses, birthplace, national ID numbers, mobile numbers and criminal records. This event could be considered the largest data leak ever.

- A Russian espionage group, APT 29 (aka Cozy Bear or Nobelium), has been linked to phishing attacks targeting Italy. The APT group has used the malicious HTML dropper EnvyScout to perform DLL hijacking. The group has been performing espionage campaigns since at least 2014.

- The TrickBot Gang has shifted to targeting Ukraine during the Russian invasion. Researchers indicate at least six campaigns executed by Trickbot gang that took place between mid-April and mid-June using IcedID, CobaltStrike, AnchorMail, and Meterpreter.

  Check Point Threat Emulation, Harmony Endpoint and Anti-Bot provide protection against these threats

- A malicious actor has published the database of the Federal Electricity Commission (CFE) of Mexico with more than 14 million customer records.

- The comic reading platform Mangatoon has been victim of data security breach resulting from weak credentials of an Elasticsearch server that revealed 23 million accounts’ personal information.

- US cybersecurity and intelligence agencies have issued a joint advisory warning against North Korean State-Sponsored cyber actors that use the Maui ransomware to encrypt servers responsible for healthcare services of several Healthcare and Public Health (HPH) organizations.

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

- A new ransomware gang dubbed “0mega” has been targeting organizations worldwide using a double-extortion attack technique. The ransomware appends the “.0mega” extension to the encrypted files’ names and creates customized ransom notes named “DECRYPT-FILES.txt”. This operation launched in May 2022, and demands millions of dollars in ransoms.

VULNERABILITIES AND PATCHES

- A newly observed phishing campaign has leveraged the recently disclosed Follina security vulnerability (tracked CVE-2022-30190) to distribute a backdoor called Rozena on Windows systems.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina*)

- Google has released a patch to for an actively exploited in the wild vulnerability (CVE-2022-2294) in the WebRTC component in Chrome for Android, which could be used for remote code execution and DoS attacks. WebRTC (Web Real-Time Communications) is a component that provides real-time audio and video communication capabilities in browsers without the need to install plugins or download native apps.
- Microsoft has patched a previously disclosed 'ShadowCoerce' vulnerability that allowed attackers to use Windows servers as a target for NTLM relay attacks.
- Django, an open source Python-based web framework, has issued a fix to a high severity SQL Injection vulnerability in its new releases, tracked as CVE-2022-34265.

THREAT INTELLIGENCE REPORTS

- Check Point Research shares recent findings on Amazon-related phishing attacks. A large increase in phishing emails relating to the Amazon Prime Day has been observed during June 2021, as well as suspicious new domains that were created with the term “Amazon”.

  Check Point Harmony Email & Office provide protection against this threat

- Researchers have discovered a new Linux Malware dubbed OrBit. The malware implements advanced evasion techniques and gains persistence on the machine by hooking key functions, provides the threat actors with remote access capabilities over SSH, harvests credentials, and logs TTY commands.
- Researchers have discovered a new ransomware family called RedAlert (aka N13V) that is capable of encrypting both Windows and Linux VMWare ESXi servers in attacks on corporate networks.
- Researchers have issued a warning regarding a series of cyberattacks linked to a threat cluster tracked as Raspberry Robin. The campaign involves a worm that spreads over USB devices or shared folders, leveraging compromised QNAP (Network Attached Storage or NAS) devices as stagers, and using specifically crafted Microsoft links (LNK files) to infect its victims.