Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 9 - 15, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has revealed that the threat actor behinds last month's cyber-attack on Iran's train system is "Indra", a group that identifies itself as Iranian regime opposition. They used similar tools in an attack against companies in Syria in 2019.
- Poly Network, a China-based cross-chain decentralized finance (DeFi) platform for swapping tokens across blockchains, has suffered a major breach. The firm disclosed that attackers have stolen 611 million worth of cryptocurrencies from the network by exploiting a vulnerability in the system to plunder digital tokens.
- T-Mobile has opened an investigation regarding a data breach exposed in a forum post claiming to be selling data of over 100 million people. The company has confirmed the data included user's social security numbers, physical addresses, phone and IMEI numbers, and driver license information.
- The Federal Board of Revenue (FBR) of Pakistan has suffered a data breach during a cyber-attack. Threat actors managed to breach the Microsoft Hyper-V software and took down the official website of the agency along with all sub-domains. Network access to the agency is for sale on a Russian hacking forum.
- An archive containing 1.6 million emails with highly sensitive documents allegedly stolen from the Lithuanian Ministry of Foreign Affairs is available for sale in a hacking forum.
- The US Financial Regulatory Authority (FINRA) has warned US brokerage firms and brokers about an ongoing phishing campaign impersonating FINRA officials, tricking victims with a threat of penalties to obtain sensitive information.

  Check Point Harmony Email & Office and Anti-Phishing provide protection against this threat

- Threat actors have been attacking Microsoft Exchange servers using the ProxyShell vulnerabilities to install backdoors for later access (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).

  Check Point Sandblast and Anti-IPS blade provide protection against this threat

VULNERABILITIES AND PATCHES

- Microsoft has released its August patch Tuesday addressing 44 CVEs including yet another vulnerability in the Print Spooler component tracked as (CVE-2021-36958) that allows remote code execution, as well as an actively exploited privilege escalation zero-day in the Windows Update Medic Service (CVE-2021-36948).

  Check Point IPS blade provides protection against this threat (Microsoft Windows Update Medic Service Privilege Escalation (CVE-2021-36948))

- Adobe has released a security update that fixes a critical vulnerability in Magento and important bugs in Adobe Connect.

- A flaw has been found in Microsoft's new Windows 365 Cloud PC service. A threat actor could dump a user's plaintext credentials using Mimikatz.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its monthly threat index for July 2021, showing that while Trickbot is still the most prevalent malware, Snake Keylogger, which was first detected in November 2020, has surged into second place following an intense phishing campaign.

- A spear-phishing campaign has been targeting Office 365 customers in multiple attacks since July 2020, using Morse code and other encryption methods to evade detection. The malicious attachments have a XLS.HTML extension, so that victims would expect an xls file, while actually opening the internet browser.

  Check Point Harmony Email & Office and Anti-Phishing provide protection against this threat

- A new Android Trojan named "FlyTrap" has compromised at least 10,000 Facebook accounts in 140 counties since March 2021, through malicious apps that were uploaded to and quickly removed from Google Play, and were later available on third-party app stores, allegedly providing coupons.

- Ransomware operators such as 'Magniber' and 'Vice Society' are actively exploiting vulnerabilities in Windows Print Spooler to compromise, spread across a victim's network, and deploy their tools.

  Check Point Harmony Endpoint and Anti-Bot provide protection against this threat

- Researchers have discovered a new AdLoad adware campaign with over 150 unique samples, some of them with a valid signature, targeting Mac devices.

  Check Point Anti-Bot provides protection against this threat (Adware.Win32.Adload)

- The SynAck ransomware operators have released the master decryption keys for their operation on their data leak site, as they are soon to launch a new ransomware as-a-service called EL_Cometa.

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