Jun 28 – Jul 04, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has discovered an ongoing cyber espionage operation targeting the Afghan government. Believed to be the Chinese-speaking hacker group known as "IndigoZebra", the threat actors behind the espionage leveraged Dropbox to infiltrate the Afghan National Security Council (NSC). This is the latest in longer-running activity targeting other Central Asian countries, Kyrgyzstan and Uzbekistan, since at least 2014.

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

- REvil ransomware has targeted multiple Manages Service Providers (MSPs) and their customers in a recent supply chain attack. Threat actors successfully implanted a malicious software update for IT Company Kaseya's VSA patch management and client monitoring tool, which included the malware installer. An estimated 1000 companies have been impacted by this attack.

  Check Point Harmony Endpoint provides protection against this threat

- Swedish supermarket chain Coop disclosed it has been hit by a recent Kaseya supply chain ransomware attack. The supermarket chain has shut down approximately 500 stores as a result of the attack.

  Check Point Harmony Endpoint provides protection against this threat

- LinkedIn has suffered a Data breach offering over 700 million users' data for sale in a darknet forum. The data includes email addresses, gender, full names, industrial information, and phone numbers.

- MonPass, Mongolia's major certificate authority's website, has been breached by an unknown threat actor in a supply chain attack to distribute a backdoor via its installer software with Cobalt Strike binaries. The Trojanized client was available for download between Fab 8th and Mar 3rd.

- Researchers have discovered 9 malicious Android apps on Google Play that steal Facebook users' logins and passwords. The Trojans were spread as harmless software and were installed more than 5 million times.

- US-based global insurance brokerage and risk management firm Arthur J. Gallagher (AJG) has suffered a data breach following a ransomware attack that hit its system in late September. The data leaked includes customers' personal, financial, and health information.

VULNERABILITIES AND PATCHES

- Microsoft warns of a critical "PrintNightmare" flaw (CVE-2021-34527) being exploited in the wild. The remote code execution (RCE) vulnerability affecting Windows Print Spooler is yet to be patched.
- A critical firmware vulnerability has been discovered in Microsoft NETGEAR router models. According to experts, the vulnerability is acting as a stepping stone to move parallel within the network.
- Microsoft urges Azure users to update PowerShell versions 7.0 and 7.1 to address a remote code execution vulnerability (CVE-2021-26701) that was fixed earlier this year.
- A remote code execution vulnerability has been identified in Adobe Experience Manager content-management system, used by MasterCard, LinkedIn, and Sony PlayStation consumers.

THREAT INTELLIGENCE REPORTS

- Babuk ransomware is being used in an ongoing campaign targeting victims worldwide. The Babuk operators halted their operations at the end of April after attacking the Washington DC police department. Since then, the malware builder was published by the threat actor and uploaded to VirusTotal.

  Check Point Harmony Endpoint provides protection against this threat

- The Indexsinas SMB worm that uses former NSA cyberweapons, ultimately dropping cryptominers on targeted machines, has been spotted targeting healthcare, education and telecommunications sectors in an ongoing campaign.
- A new module of TrickBot has been found. The Banking Trojan, known for stealing credentials and delivering follow-on ransomware, has added man-in-the-browser capabilities for stealing online banking credentials, potentially signaling a coming boost in fraud attacks.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.TrickBot)

- REvil ransomware has released a version for Linux operating system and is targeting VMware's ESXi virtual machine management software and network-attached storage (NAS) devices.
- Researchers have revealed a new Mirai-inspired botnet called "mirai_ptea" that leverages a vulnerability in KGUARD digital video recorders (DVR) to carry out distributed denial-of-service (DDoS) attacks.