Check Point Research
WEEKLY INTELLIGENCE REPORT
August 7 – 13, 2023

TOP ATTACKS AND BREACHES

- The Belt Railway Company of Chicago, the largest intermediate switching terminal railroad in the United States, is currently conducting an investigation into an attack executed by the Akira ransomware group. This group has included the company on its leak site, asserting the theft of 85 GB of data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Akira.A; Trojan.Win.Krap.gl.D)

- The UK's Electoral Commission, responsible for the voter registry, recently revealed a significant security breach. "Hostile actors" accessed their systems for over a year, spanning from August 2021 to October 2022. According to the commission, this breach potentially exposed the personal data of all UK citizens who registered to vote between 2014 and 2022.

- A recent report reveals that the Knight Ransomware, a variant of Cyclop Ransomware-as-a-Service, is currently spreading via an ongoing spam campaign using deceptive TripAdvisor complaint-themed emails to target unsuspecting users.

- Researchers have identified a cyberespionage group called 'MoustachedBouncer' using adversary-in-the-middle (AitM) attacks through Belarusian ISPs to target foreign embassies in Belarus. The report disclosed five separate campaigns, suggesting the threat actors have been operational since 2014, with AitM tactics used at Belarusian ISPs since 2020.

- The Department of Social Services (DCC) in Missouri has issued a cautionary notice regarding the exposure of protected Medicaid healthcare data due to a data breach. This incident occurred when IBM, which is a vendor that is providing services to DCC fell victim to a MOVEit data theft attack carried out by the Clop ransomware gang.

- Researchers have discovered an intrusion into a Russian missile engineering organization, NPO Mashinostroyeniya. Within this organization, they identified two instances of North Korea-related compromise of sensitive internal IT infrastructure, which included an email server, and the use of a Windows backdoor called OpenCarrot.

- The U.S. government released a report on the Lapsus$ hacking and extortion group, uncovering their predominant use of familiar tactics like SIM swapping, as well as exploiting known enterprise network vulnerabilities and technology provider protocols to access valuable data illicitly.

VULNERABILITIES AND PATCHES

- Microsoft outlined critical vulnerabilities in the CODESYS V3 software development kit (SDK). These vulnerabilities impact all versions before 3.5.19.0, posing significant risks to operational technology infrastructure, including the potential for RCE and DoS attacks.

- Researchers discovered a vulnerability in Microsoft's Visual Studio Code (VS Code) code editor and development environment concerning the handling of secure token storage. Malicious extensions can exploit it to access authentication tokens stored within Windows, Linux, and macOS credential managers.

- Ford has issued an alert about a buffer overflow vulnerability (CVE-2023-29468) in its widely-used SYNC3 infotainment system, potentially enabling remote code execution. However, the company assures that this vulnerability doesn't impact vehicle driving safety.

THREAT INTELLIGENCE REPORTS

- Check Point Research shared information about modus operandi of Rhysida ransomware group, based on recent CPIRT response on Rhysida attack against an educational institution. The report also highlights significant similarities of Rhysida group to Vice Society ransomware, which mostly targeted education and healthcare since 2021.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Rhysida, Ransomware.win.honey; Ransomware.Wins.Rhysida)*

- Check Point Research reports that, over the last four weeks, approximately 1 in 29 healthcare organizations in the United States were attacked by ransomware. Healthcare currently holds the unfortunate distinction of being the most affected industry by ransomware. In 2022, the healthcare sector witnessed a staggering 78% surge in cyberattacks, with an average of 1,426 attempted attacks per week per organization.

- Check Point Research's July Most Wanted Malware Report unveils that Remcos RAT rose to third place, due to malicious downloaders carrying RAT distributed through fake websites last month. Anubis, the mobile banking Trojan, dethrones SpinOk from the top spot in mobile malware.

- Researchers have discovered a LATAM-focused threat actor targeting FinTech users. This campaign employs a modified BX RAT called JanelaRAT, utilizing diverse TTPs, including DLL side-loading, dynamic C2 infrastructure, and a multi-stage attack approach.

- In a globally coordinated operation led by INTERPOL, a well-known 'phishing-as-a-service' (PaaS) platform named '16shop' has been dismantled. The platform's operator and a facilitator were apprehended by Indonesian authorities, while another individual was arrested in Japan.