July 31 – August 6, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Prospect Medical Holdings, a major healthcare services provider that operates 16 hospitals and 166 outpatient clinics and centers in the US, suffered a significant ransomware attack. The attack has disrupted the company's operations in at least three states, and forced hospitals to divert patients to other facilities. No ransomware gang has publicly claimed responsibility for the attack yet.

- Serco Inc, a contractor of the US government, has suffered a data breach that affected the personal information of over 10K individuals. The compromised data has been stolen from a third-party vendor's MoveIT managed file transfer (MFT) server and consists of names, US Social Security numbers, date of birth, email address, health benefits information and more.

- The American video game giant Activision, which is the creator of 'Call of Duty' online game, has allegedly experienced a cyber-attack and took 'Call of Duty' (Modern Warfare 2) game offline as a precaution. Researchers investigated and found that Call of Duty players have been hit with malware that automatically spreads through multiplayer lobbies.

- The American apparel retailer, Hot Topic, has confirmed a possible data breach that potentially resulted in the exposure of clients' personal information. The breach was due to credential-stuffing attacks that occurred between February 7th and June 21st this year. The stolen data consists of full names, email addresses, orders history, phone numbers, four last digits of saved payment cards and more.

- The Colorado Department of Higher Education (CDHE) has disclosed a data breach that exposed the data of employees and students who attended a public high school, college or university in the state over a period of more than a decade leading up to 2020. The stolen data includes personal information such as full names, US Social Security numbers, student identification numbers, and other education records.

- Kenya's government has been a victim of a massive DDOS (Distributed Denial of Service) attack that impacted the eCitizen portal that serves as a platform for the public to access over 5,000 government services. The attack was conducted by the Russia affiliated hacktivists group Anonymous Sudan.

- LockBit ransomware gang has claimed responsibility for a cyber-attack on West Oaks School, a school for children with special educational needs in England. The threat actors allegedly gained access to the school's databases, however, currently the scope of the event is still unclear.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Lockbit; Ransomware.Wins.Lockbit)

VULNERABILITIES AND PATCHES

- Microsoft fixes a security issue that could lead to an unauthorized access to Custom Code functions used for Power Platform custom connectors. This issue can lead to an information disclosure of sensitive information that was embedded in the Custom Code function.

- Mozilla has released patches for several vulnerabilities in Firefox 116, of which nine flaws are rated with high severity. Among the fixed vulnerabilities is the Stack buffer overflow in StorageManager flaw (CVE-2023-4050) which could result in a potentially exploitable crash which could lead to a sandbox escape.

- PaperCut has patched a critical security vulnerability (CVE-2023-39143) in its NG/MF print management software. Successful exploitation could allow an unauthenticated attacker to perform remote code execution on unpatched PaperCut servers running on Windows.

THREAT INTELLIGENCE REPORTS

- Check Point researchers share the latest findings of NPM-based vulnerabilities that were discovered in over 50 popular packages, putting countless projects and organizations at risk.

  Check Point CloudGuard CNAPP provides protection against this threat

- Researchers have identified social engineering attack campaign that uses credential theft phishing lures sent as Microsoft Teams chats, conducted by the Russian APT29 (aka Midnight Blizzard, NOBELIUM, Cozy Bear). The APT group uses Teams user profiles taken from previously compromised small-businesses and tricks users into approving multifactor authentication (MFA) prompts, aiming to steal credentials from targeted organizations.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Win.APT29; APT.Wins.APT29)

- A novel phishing tactic leverages Google Accelerated Mobile Pages (AMP), an open-source HTML framework, to embed malicious links within their phishing emails. Hosted on trusted domains, these links have proven highly effective in targeting enterprise employees, making detection more challenging.

- Researchers have discovered an AI-driven malicious tool called FraudGPT, which has emerged two weeks after WormGPT in the darkweb. This malicious tool is being promoted as an "exclusive bot" used for offensive activities such as crafting spear phishing emails, creating cracking tools, carding, and more; all this without real proofs to its success yet.

- An Android malware dubbed SpyNote is actively targeting multiple European banking clients in a widespread campaign. The malware is spread through phishing or smishing campaigns, while fraudulent activities utilize a combination of remote access Trojan (RAT) capabilities and phishing attacks.