November 13 – 19, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russia-affiliated military intelligence group SandWorm is reportedly responsible for an attack against 22 critical infrastructure companies in Denmark. The attacks, most severe in Danish history, have compromised industrial control systems and forced companies from the energy sector to work offline.

- Medusa ransomware group has claimed two attacks this week. One of the victims, Toyota Financial Services, resorted to taking its operations partially offline to prevent further damage, whilst another victim, Canadian fin-tech giant Moneris, claimed it was able to prevent critical data leakage.

- An elaborate attack on numerous European diplomatic and government entities, international organizations, and internet service providers, perpetrated by the Russia-affiliated APT29 group (AKA Cozy Bear) has been unveiled. The group launched a sophisticated phishing campaign to gain initial access and leveraged newly found WinRAR vulnerability CVE-2023-38831 to execute arbitrary code.

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

- Ransomware group AlphV/BlackCat claimed to have attacked American financial company MeridianLink. Notably, AlphV has reported the company's failure to disclose the breach to the U.S. Securities and Exchange Commission. In response, the company claimed the attack was contained.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.BlackCat, Ransomware_Linux_BlackCat)

- LockBit ransomware group added two new US victims to its list: Community Dental and Planet Home Lending. The companies hold highly sensitive medical and financial information, which LockBit threaten to publish should the requested ransom not be paid.

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

- Samsung UK discovered a year-long data breach which compromised information of the company's eCommerce site users. This week, it became apparent that an attacker exploited a vulnerability in a 3rd party vendor to access the data.

- North Carolina's Bladen county has suffered a cyber-attack which allowed hackers access to the county's data systems. Access to some of the county government's data is restricted, suggesting data was encrypted in an effort to extort ransom payment.

VULNERABILITIES AND PATCHES

- In November's Patch Tuesday, Microsoft have issued security updates for 58 flaws and five zero-day vulnerabilities. Three critical flaws were fixed: Azure information disclosure bug (CVE-2023-36052), a Remote Code Execution in Windows Internet Connection Sharing (CVE-2023-36397), and a Hyper-V escape flaw that allows executions of programs on the host with SYSTEM privileges (CVE-2023-36400).

- Vulnerability researchers have discovered new attack methods against Google Workspace and Google Cloud Platform. The methods involve exploitation of cloned machines with Google Credentials Provider for Windows, a bypass of Google's MFA process, and a password-reset bug. This could result in data exfiltration from all Google-managed platforms.

- A zero-day cross-site scripting (XSS) vulnerability (CVE-2023-37580) in Zimbra email server was detected. Four groups were observed to have exploited the flaw to steal email data, credentials and authentication tokens. Most activities are believed to have occurred after a fix was published on GitHub.

  Check Point IPS blade provides protection against this threat (Zimbra Collaboration Cross-Site Scripting (CVE-2023-37580))

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a report highlighting the activities of Russian cyber-espionage group Gamaredon and its use of a USB-propagating worm dubbed LitterDrifter. Gamaredon primarily focuses on Ukrainian targets, however LittleDrifter was observed in other countries as well. The worm spreads automatically and communicates with C2 servers to maintain persistent control across diverse targets.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Win.Gamaredon, Trojan-Dropper.WIN32.Gamaredon, Trojan.Win32.Gamaredon)

- Check Point Research witnessed an increase in cyber-crime targeting of online-shoppers as the November sales period approaches. Attackers used phishing websites designed to lure bargain shoppers, and crafted phishing emails impersonating luxury brands to steal customer's credentials.

- Check Point Research conducted an experimental deep dive to test ChatGPT's malware analysis capabilities. The findings focus on the guidance the AI system requires in order to expand its capabilities and deliver a verdict.

- Researchers have observed a recent phishing campaign by a likely Palestinian-based APT group Molerats (aka TA402, Gaza Cybergang). The group has targeted MENA based government entities using new tactics, such as the new downloader 'IronWind' and unique file attachments to evade detection.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Wins.TA402.ta)