Check Point Research

WEEKLY INTELLIGENCE REPORT

January 10-16, 2023

TOP ATTACKS AND BREACHES

- Britain's international mail service, Royal Mail, has had its operations disrupted by a cyberattack. The service has instructed its users not to post mail, as it is unable to dispatch packages to their destinations. The LockBit ransomware gang has been confirmed as the perpetrator of the attack, and is threatening to leak stolen data if its ransom demand is not met.

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

- All departing flights in the United States were grounded for several hours, as the Federal Aviation Administration suffered a communications outage due to a corrupted database file. In its initial investigation into the case, the FAA has not found evidence of a cyberattack.
- Russian-affiliated hacktivist group 'NoName057(16)' has initiated DDoS attacks against NATO member states during the past week, specifically targeting financial institutions in Denmark, and websites of Czech Republic's presidential election candidates. As a result, code-management platform GitHub, where the group's DDoS project was being maintained, has disabled the group's accounts.
- Canada's largest alcohol supplier, the government corporation LCBO, has had its website hacked. According to a statement released by the company, attackers had injected malicious code that was used to steal customers' payment information from the company's checkout page.
- Personal information of more than 2 million Japanese citizens has been leaked online, following a breach of a server belonging to a third-party vendor which provides services to two insurance companies.
- The public school district of Des Moines, Iowa, has announced that the school year will be extended after the district has been forced to shut down schools for several days due to a ransomware attack. Information regarding the attackers and any potential stolen data has not been disclosed.
- Cyber criminals have offered to sell access to Telegram's servers. The sellers, who have priced their offer at $20,000 on an online underground marketplace, claim to be able to access any Telegram conversation going back months, by using an insider employee accomplice.
- Researchers have analyzed a Gootkit campaign targeting Australia's healthcare sector. The campaign used Search Engine Optimization poisoning to push malicious results to victims who would search for common healthcare terms in Australia, and also abused the legitimate program VLC Media Player.

  Check Point Anti-bot provides protection against this threat *(Trojan.Win32.Gootkit)*

VULNERABILITIES AND PATCHES

- Microsoft has released January's patch Tuesday, which includes fixes for 98 security vulnerabilities across Microsoft's products, including one known to be exploited in the wild (CVE-2023-21674). Among the vulnerabilities, 11 are considered critical, and could lead to remote code execution.

  Check Point IPS provides protection against these threats (e.g., Microsoft Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege (CVE-2023-21674))

- Adobe has released security updates for many of its products. The update includes fixes for multiple critical severity vulnerabilities, which could lead to remote code execution.

- Cisco had disclosed two vulnerabilities affecting some of its router products, among them a critical severity vulnerability that allows remote code execution. However, despite being aware of a proof-of-concept for exploitation, the company will not release updates as the routers have reached end-of-life.

- Juniper networks has patched security vulnerabilities affecting several of its products. Some of the vulnerabilities addressed are considered critical, and could allow remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research is seeing attempts by Russian cybercriminals to bypass OpenAI's restrictions, to use ChatGPT for malicious purposes. In underground hacking forums, hackers are discussing how to circumvent IP addresses, payment cards and phone numbers controls – all of which are needed to gain access to ChatGPT from Russia.

- Check Point Research shows that in December, Qbot banking Trojan overtook Emotet to be the most prevalent malware after its return last month, impacting 7% of organizations worldwide. Blockchain-enabled Trojan Glupteba returned to the top ten list for the first time since July 2022. Android malware Hiddad made a comeback, and education continued to be the most impacted industry worldwide.

- Researchers have discovered an Android spyware campaign, attributed to the StrongPity APT group, in which the campaign's payload is delivered by a malicious version of the Telegram Android app.

  Check Point Harmony Mobile provides protection against this threat

- Activity attributed to a new, yet-unaffiliated APT group has been observed by researchers in the Asia-Pacific region. The group has targeted military and government agencies in multiple Asian countries, and delivered sophisticated custom malware with the goal of espionage.

- A spyware campaign targeting Iranian citizens has been found by researchers. The campaign is delivered using malicious VPN installers, commonly used to evade government internet censorship in Iran.