January 30 – February 5, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has flagged the Dingo crypto Token, with a market cap of $10,941,525 as a scam. The threat actors behind the token added a backdoor function in its smart contract, to manipulate the fee. Specifically, they used the "setTaxFeePercent" function within the token's smart contract code to manipulate the buying and selling fees to an alarming 99%. The function has already been used 47 times, and investors of Dingo Token can potentially risk losing all their funds.

- Google Fi, US telecommunications and mobile internet service, has announced that data of its customers was breached as part of the T-Mobile data breach, exposing more than 37M customer records including phone numbers, SIM serial card numbers and service plan details.

- KillNet, a pro-Russian hacktivists group, has launched a wide scale operation against the US healthcare sector with multiple DDoS attacks.

- ION Group, financial software company in the UK, has been a victim of ransomware attack conducted by the LockBit ransomware gang. The threat actors targeted the ION Cleared Derivatives, a division of ION Markets, which affected some of its services.

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

- An Iranian nation-state actor dubbed NEPTUNIUM is behind a data breach that exposed personal information of more than 200K of the French magazine Charlie Hebdo's clients. The threat actors offered the alleged leaked data for sale for 20 BTC (approximately $340,000).

- Tallahassee Memorial HealthCare, Florida, has been victim of a cyber-attack that has disrupted its IT systems. While sources suspected a ransomware attack, the nature of this attack hasn't been confirmed.

- Arnold Clark, one of Europe's largest car retailer, has been a victim of a Play ransomware attack. The threat actors claim to have 467GB of data including names, contact details, dates of birth, vehicle information, passports or driver's licenses, national insurance numbers, and bank account details.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.PLAY.A)

- JD Sports, UK sportswear retailer, has announced a data breach that affected approximately 10M clients. The alleged leaked data consists of clients' online orders placed between November 2018 and October 2020, including full names, emails, phone numbers, billing details, delivery addresses, and more.

- Nantucket US Public Schools has been a victim of a ransomware attack that shut down all student and staff devices, as well as schools' security systems.

VULNERABILITIES AND PATCHES

- VMware has patched vulnerabilities affecting VMware vRealize Log Insight, which when chained together can allow remote code execution as root privileges.

  Check Point IPS provides protection against this threat (VMware vRealize Log Insight Information Disclosure (CVE-2022-31711); VMware vRealize Log Insight Directory Traversal (CVE-2022-31706))

- The French Computer Emergency Response Team (CERT-FR) has published an alert warning of an actively exploited vulnerability (tracked as CVE-2021-21974) exploited to infect VMware ESXi servers with a new ESXiArgs ransomware campaign. The attack has so far affected thousands of virtual machines, a third of which are hosted in France.

  Check Point IPS provides protection against this threat (VMWare OpenSLP Heap Buffer Overflow (CVE-2019-5544))

- Atlassian has patched a critical security flaw (tracked as CVE-2023-22501) in Jira Service Management Server and Data Center affecting versions 5.3.0 through 5.5.0. Successful exploitation might allow an attacker to impersonate another user and gain remote access to the affected system.

THREAT INTELLIGENCE REPORTS

- Check Point Research discusses TrickGate, a shellcode-based packer offered as a service to help malware evade detection. Initially observed in July 2016, TrickGate has been used by top malware families, such as Cerber, Trickbot, Maze, Emotet, REvil, Cobalt Strike, AZORult, Formbook, AgentTesla and more.

  Check Point Threat Emulation and Harmony Endpoint for Linux and Containers Runtime Security provide protection against this threat (Injector.Win.RunPE; Injector.Wins.Guanyin; Ransomware_Linux_Cerber_*; Ransomware_Linux_REvil_*; HackTool_Linux_CobaltStrike_*)

- Check Point Research exposed two malicious code packages, Python-drgn and Bloxflip, distributed by threat actors, leveraging package repositories as a reliable and scalable malware distribution channel.

- Researchers have published an analysis of the Trigona ransomware, first observed in October 2022 \nd using double-extortion technique. The ransomware adds a "._locked" extension to their file name.

  Check Point Harmony Endpoint provides protection against this threat (ransomware.win.honey)

- The Iranian nation-state hacking group OilRig (aka APT34) targets organizations in the Middle East using a new backdoor, capable of stealing users' credentials and abusing compromised mailbox accounts.

  Check Point Threat Emulation provides protection against this threat (APT.Wins.APT34)

- Researchers have discovered a new botnet, Medusa, spread via Mirai botnet targeting Linux machines. The Medusa botnet has the ability to launch DDoS attacks, bruteforce attacks, and ransomware attacks that encrypt files on compromised machines and add the ".medusastealer" extension to their file name.