**Cyber Security Advisories**

**Date: 30 Apr 2024**

1. **Adv/2024/Apr/032**

Based on analysis, please find attached malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**IOCs: IOC\_Adv2024Apr032.txt attached**

**Recommendation:**

* It is recommended that organisations should apply the attached IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

1. **Adv/2024/Apr/033**

Presence of various threat actors/malware such as POISONPLUG aka ShadowPad, Sogu RAT, GRAYRABBIT Malware, UNC 5007, UNC 3569, Sandworm, Kimsuky APT & Muddy Water have been found in Indian Cyberspace.

**IOCs:**

IOC\_Adv2024Apr033\_APT.txt attached

IOC\_Adv2024Apr033\_ShadowPad.txt attached

IOC\_Adv2024Apr033\_Sogu RAT.txt attached

IOC\_Adv2024Apr033\_GRAYRABBIT Malware.txt attached

IOC\_Adv2024Apr033\_UNC 5007.txt attached

IOC\_Adv2024Apr033\_UNC 3569.txt attached

IOC\_Adv2024Apr033\_Sandworm.txt attached

IOC\_Adv2024Apr033\_Kimsuky APT.txt attached

IOC\_Adv2024Apr033\_Muddy Water.txt attached

**Recommendation:**

* It is recommended that organisations should apply the attached IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

1. **Adv/2024/Apr/034**

It has been reported that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The Spear-phishing email contains a hyperlink. Upon click, it opens a cloned phishing page of mod.gov.in. Inside, the page there is a download button. On clicking download button, it gives a pop-up which prompts for username and password of NIC email account.

**IOCs: IOC\_Adv2024Apr034.txt attached**

1. **Adv/2024/Apr/035**

It has been observed that Akira ransomware affiliates has released an upgraded version of ESXi ransomware with additional capabilities. Threat actors are deploying latest version of Akira ransomware Akira\_v2. It is written in Rust programming language. Akira\_v2 accepts command line arguments similar to the previous ESXi targeting encryptors used by various ransomware actors. The encryptor supports a range of command line arguments enabling it to execute customizable encryption tasks. These arguments include directives for specifying a starting path, a build and options to stop virtual machines, encrypt only virtual machine disk files and adjust the number of operational threads.

Below Cryptographic algorithms indicates a possible multi-layered approach to encryption processes:-

**Keccak F1600 hash function (sha3) -**This function speeds up the efficiency of hash calculations, which allows an increased capability to process large volumes of data during the encryption process.

**Sosemanuk stream cipher-**Stream ciphers, like Sosemanuk, are leveraged as an optimization technique used to speed up the encryption process.

**Tiny Encryption Algorithm-**Presence of Tiny Encryption Algorithm with its simple and lightweight function indicates a possible layered approach encryption, with a focus on the DELTA constant enhancing encryption uniqueness and used as an anti-forensics technique.

**IOCs: IOC\_Adv2024Apr035.txt attached**

1. **Adv/2024/Apr/036**

It has been observed that threat actor CoralRaider uses RotBot, a customized variant of QuasarRAT and Xclient stealer, as payloads in the campaign to steal victims' credentials, financial data and social media accounts. The threat actor uses the dead drop technique, where a legitimate service is abused to host the information related to the Command & Control (C2) infrastructure. The threat actor has used a telegram bot as C2 to exfiltrate the victim’s data. The attack begins when the user opens a malicious Windows shortcut file, which downloads and executes an HTML Application File (HTA) from an attacker-controlled download server. The HTA file executes an embedded obfuscated Visual Basic Script. The malicious Visual Basic script executes an embedded PowerShell script in the memory, which decrypts and sequentially executes three other PowerShell scripts that perform anti-VM and anti-analysis checks, bypass the User Access Controls, disables the Windows and application notifications on the victim’s machine, and downloads and runs the RotBot.

**IOCs: IOC\_Adv2024Apr036.txt attached**

1. **Adv/2024/Apr/037**

Presence of various AsyncRAT & SOGU/PLUGX malwares have been found in Indian Cyberspace.

**IOCs: IOC\_Adv2024Apr037.txt attached**

1. **Adv/2024/Apr/038**

It has been observed that threat actors in their cyber espionage campaign "operation FlightNight" are targeting Indian government entities and energy sector. Adversaries are delivering information stealer via a phishing email, masquerading as an invitation letter. The phishing email is attached with decoy PDF document that contains an ISO file, the malware in an executable form and a shortcut file (LNK) to activating the malware.  After malware execution, adversaries utilise Slack channels as exfiltration points to upload confidential internal documents, private email messages, and cached web browser data to Command & Control (C2) server.

Adversaries use modified open-source post exploitation tool HackBrowserData that not only has the capability to steal browser login credentials, cookies, web browser history but also implemented new functionalities, such as communication through Slack channels, document stealing, and malware obfuscation for the evasion.

Adversaries are targeting multiple government entities that includes agencies responsible for electronic communications, IT governance, national defense and private Indian energy companies for exfiltrating financial documents, personal details of employees, details about drilling activities in oil and gas.

**IOCs: IOC\_Adv2024Apr038.txt attached**

1. **Adv/2024/Apr/040**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

**IOCs: IOC\_Adv2024Apr040.txt attached**

1. **Adv/2024/Apr/041**

It has been reported that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The Spear-phishing email contains a malicious link. Upon clicking the hyperlink, it opens a mimicked/cloned phishing page of ‘Zimbra’ with the title ‘Zimbra Log in’. It gives a pop-up, which prompts for username and password of Zimbra mail account.

**IOCs: IOC\_Adv2024Apr041.txt attached**