**Cyber Security Advisories**

**Date: 31 May 2024**

1. **Adv/2024/May/040**

Presence of malicious IoCs found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May040.txt attached**

1. **Adv/2024/May/041**

Presence of malicious IoCs found in Indian Cyberspace related to Keyplug & Shadowpad Malware.

**IOCs: IOC\_Adv2024May041.txt attached**

1. **Adv/2024/May/042**

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\_Adv2024May042.txt attached**

1. **Adv/2024/May/043**

A zero-day, stack buffer overflow vulnerability (CVE-2024-27130) has been discovered in the QNAP QTS operating system used in Network Attached Storage (NAS) devices. The vulnerability is present in the "No\_Support\_ACL function" of share.cgi, which is part of the QNAP QTS operating system used in NAS devices. Once the flaw is executed, it leads to Remote Code Execution (RCE) on the affected system. The vulnerability arises due to the unsafe use of the ‘strcpy’ function within the No\_Support\_ACL function.

1. **Adv/2024/May/044**

**Vulnerability in Business Directory Plugin – Easy Listing Directories for WordPress Plugin**

A time-based SQL Injection vulnerability has been discovered in Business Directory Plugin – Easy Listing Directories for WordPress plugin. The affected versions are Business Directory Plugin – Easy Listing Directories for WordPress plugin all versions up to, and including, 6.4.2.

CVE ID: CVE-2024-4443

**Vulnerability in Build App Online plugin for WordPress**

An authentication bypass vulnerability has been discovered in Build App Online plugin for WordPress. The affected versions are Build App Online plugin for WordPress versions up to, and including, 1.0.21.

CVE ID: CVE-2024-3658

1. **Adv/2024/May/045**

Microsoft released updates to address multiple vulnerabilities in its products for the month of May 2024. However, Microsoft provides patch information in the form of Knowledge Base (KB) Articles that are associated with one or more CVEs.

Please find below link for the monthly CVE - KB Correlation list of May 2024 for your perusal and necessary action.

https://nciipc.gov.in/advisories/CVE/CVE-KB/2024/May.html

The list consists of 62 CVEs and their corresponding KBs for the month of May 2024.

1. **Adv/2024/May/047**

Presence of various phishing domains have been found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May047.txt attached**

1. **Adv/2024/May/048**

Presence of malicious IoCs found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May048.txt attached**

1. **Adv/2024/May/049**

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, and features a packet signature at the start of each message that varies between samples.

**IOCs: IOC\_Adv2024May049.txt attached**

1. **Adv/2024/May/050**

Reference is made to earlier advisories on RedLine Stealer.

It has been observed that RedLine Stealer, a .NET-based infostealer malware, is active with the capabilities of harvesting information from browsers such as saved credentials, autocomplete data & credit card information. Malware is also utilized in to facilitating attackers to drop another payload or launch a hidden command shell on the victim's machine.

**IOCs: IOC\_Adv2024May050.txt attached**

1. **Adv/2024/May/051**

Reference is made to earlier advisories on Racoon Malware.

It has been observed that there is an uprise in activities associated with raccoon malware. Raccoon is an info stealer malware available as a Malware as a Service (MaaS) with the capability to check system settings, capture screenshots, collect basic information like OS version, IP & username, steal passwords and logins from a variety of browsers.

**IOCs: IOC\_Adv2024May051.txt attached**

1. **Adv/2024/May/052**

It has been observed that the threat actor BlackTech aka Circuit Panda, Earth Hundun, HUAPI, Manga Taurus, Palmerworm, Red Djinn & Temp.Overboard is active and using malwares, named Waterbear aka DBGPRINT & Deuterbear, to infect computers and steal information. Deuterbear has advanced capabilities, such as including support for shellcode plugins, avoiding handshakes for RAT operation, and using HTTPS for Command & Control (C2) communication, uses shellcode format, possesses anti-memory scanning, and shares a traffic key with its downloader, unlike Waterbear.

**IOCs: IOC\_Adv2024May052.txt attached**

1. **Adv/2024/May/053**

**Vulnerability in Pie Register - Social Sites Login Plugin for WordPress**

Authentication bypass vulnerability has been discovered in Pie Register - Social Sites Login (Add on) plugin for WordPress. The affected versions are Pie Register - Social Sites Login (Add on) plugin for WordPress versions up to, and including, 1.7.7.

CVE ID: CVE-2024-4544 (Critical)

**Vulnerability in Hash Form – Drag & Drop Form Builder plugin for WordPress**

Authentication bypass vulnerability has been discovered in Hash Form – Drag & Drop Form Builder plugin for WordPress. The affected versions are Hash Form – Drag & Drop Form Builder plugin for WordPress versions up to, and including, 1.1.0.

CVE ID: CVE-2024-5084 (Critical)

**Multiple Vulnerabilities in AutomationDirect's Equipment**

Multiple vulnerabilities have been discovered in AutomationDirect's Equipment- Productivity PLCs that can lead to remote code execution and denial of service. The mitigations are available.

CVE ID: CVE-2024-24851 (High), CVE-2024-24946 (High), CVE-2024-24947 (High), CVE-2024-24954 (High), CVE-2024-24955 (High), CVE-2024-24956 (High), CVE-2024-24957 (High), CVE-2024-24958 (High), CVE-2024-24959 (High), CVE-2024-24962 (Critical), CVE-2024-24963 (Critical), CVE-2024-22187 (Critical), CVE-2024-23315 (High), CVE-2024-21785 (Critical), CVE-2024-23601 (Critical)

**Vulnerability in Country State City Dropdown CF7 plugin for WordPress**

SQL Injection vulnerability has been discovered in Country State City Dropdown CF7 plugin for WordPress. The affected versions are Country State City Dropdown CF7 plugin for WordPress versions up to, and including, 2.7.2.

CVE ID: CVE-2024-3495 (Critical)

1. **Adv/2024/May/054**

Reference is made to earlier advisories on Racoon Malware.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024May054.txt attached**

1. **Adv/2024/May/055**

Reference is made to earlier advisories on RedLine Stealer.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024May055.txt attached**

1. **Adv/2024/May/056**

It has been observed that NJRAT, a .NET-based backdoor, uses a unique text-based protocol over TCP to communicate with its Command & Control (C2) Server. The backdoor is capable of recording video, audio, screenshots, keystrokes, creating a reverse shell, transferring files, running files, stealing credentials, and spreading via USB drive. Malware has features to update its capabilities by getting plugins from a C2 server.

**IOCs: IOC\_Adv2024May056.txt attached**

1. **Adv/2024/May/057**

Reference is made to earlier advisories on GHOST RAT Malware.

**IOCs: IOC\_Adv2024May057.txt attached**

1. **Adv/2024/May/058**

Reference is made to earlier advisories on  QuasarRAT Malware .

It has been observed that threat actors are using QuasarRAT , a Windows Remote Administration Tool (RAT) coded in C# to compromise targets. QuasarRAT has the capability of capturing screenshots, key logger, gather system information, remote shell and command execution, reversing proxy, managing tasks and files, configuring and building client executables.

**IOCs: IOC\_Adv2024May058.txt attached**

1. **Adv/2024/May/061**

It has been observed that VacBan Stealer, a new type of malware, evolved from a previous variant known as Creal Stealer, exhibits both spyware and stealware capabilities. The malware is primarily written in Python, making it versatile and capable of operating on various systems. The initial attack vector starts through phishing emails, malicious attachments, or downloads from compromised websites. The major capabilities of malware include targeting and extracting sensitive information from infected devices, such as login credentials and cryptocurrency wallet data, browser cookies, saved passwords, retrieving the version information of the machine’s Operating System (OS). Adversaries store collected data into text files such as crpasswords.txt, crcookies.txt, crcreditcards.txt, crautofills.txt, crhistories.txt, and crbookmarks.txt inside the Temp directory, drops a copy of itself inside the Startup folder for persistence, enumerate files and directories, delaying execution using the Windows API Sleep function and detect debuggers using the IsDebuggerPresent API function.

I**OCs: IOC\_Adv2024May061.txt attached**

1. **Adv/2024/May/062**

A Cross Site Scripting (XSS) vulnerability (CVE-2023-40000) has been discovered in the LiteSpeed Cache plugin for WordPress that allows to inject malicious scripts, such as redirects, advertisements, and other HTML payloads into websites which will be executed when guests visit vulnerable sites. Adversaries after exploiting the vulnerability may create new admin users with the names wpsupp‑user and wp‑configuser. LiteSpeed Cache is a tool used on many WordPress websites to make them load faster. Successful exploitation of the vulnerability can allow adversaries to take over the website, change its content, or even use it to spread malware.

**Affected Version**- older than 5.7.0.1

**Security Update:** Update it to latest version 6.2.0.1, link given below:

 https://wordpress.org/plugins/litespeed-cache/advanced/

**Recommendations:-**

* Install and regularly update antivirus software.
* Install Updates and Patched regularly.

**Reference**: CERT-IN [CMTX-P052024035]

1. **Adv/2024/May/063**

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\_Adv2024May063.txt attached**

1. **Adv/2024/May/064**

Presence of malicious IoC related to Agent Tesla is found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May064.txt attached**

1. **Adv/2024/May/065**

Reference is made to earlier advisory on above subject with advisory No-  Adv/2024/Jan/054 dated 23 Jan 2024.

**IOCs: IOC\_Adv2024May065.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/May/066**

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.  This hyperlink is currently not working. However, the domain is known for compromising the user credentials/propagate malware payload when active.

**IOCs: IOC\_Adv2024May066.txt attached**

1. **Adv/2024/May/068**

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\_Adv2024May068.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.