**Cyber Security Advisories**

**Date: 22 May 2024**

1. **Adv/2024/May/001**

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\_Adv2024May001.txt attached**

1. **Adv/2024/May/002**

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\_Adv2024May002.txt attached**

1. **Adv/2024/May/003**

Presence of various threat actors/malware such as Sogu, Agent Tesla have been found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May003.txt attached**

1. **Adv/2024/May/004**

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\_Adv2024May004.txt attached**

1. **Adv/2024/May/005**

Presence of malicious IoCs found in Indian Cyberspace..

**IOCs: IOC\_Adv2024May005.txt attached**

1. **Adv/2024/May/006**

It has been observed that hacktivists are targeting Operational Technology (OT) devices, and compromising internet-exposed Industrial Control Systems (ICS) through their software components, such as Human Machine Interfaces (HMIs), by exploiting Virtual Network Computing (VNC) remote access software and default passwords. Hacktivists are gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs’ factory default passwords and weak passwords without multifactor authentication.

**Mitigations:-**

1. **Harden HMI Remote Access:**

* Disconnect all HMIs, such as the touchscreens used to monitor or make changes to the system, or Programmable Logic Controllers (PLCs), from the public-facing internet. If remote access is necessary, implement a firewall or Virtual Private Network (VPN) with a strong password and multifactor authentication.
* Implement multifactor authentication for all access to the OT network.
* Immediately change all default and weak passwords on HMIs and use a strong, unique password.
* Keep VNC updated with the latest version available and ensure all systems and software are up to date with patches and necessary security updates.
* Establish an allowlist that permits only authorized device IP addresses.
* Log remote logins to HMIs, taking note of any failed attempts and unusual times.

2. **Strengthen Security Posture:**

* Integrate cybersecurity considerations into the conception, design, development, and operation of OT systems.
* Practice and maintain the ability to operate systems manually.
* Create backups of the engineering logic, configurations, and firmware of HMIs to enable fast recovery.
* Check the integrity of PLC ladder logic or other PLC programming languages and diagrams and check for any unauthorized modifications to ensure correct operation.
* Be aware of cyber/physical-enabled threats. Adversaries may attempt to obtain network credentials by various physical means, including official visits, tradeshow and conference conversations, and through social media platforms.
* Take inventory and determine the end-of-life status of all HMIs.
* Implementing software and hardware limits the manipulation of physical processes, limiting the impact of a successful compromise.

3. **Limit Adversarial Use of Common Vulnerabilities:**

* Reduce risk exposure to threats by mitigating attack vectors.
* Assess the security posture of organizations by assessing the current security posture.

1. **Adv/2024/May/007**

**Google Released Security Updates for Chrome**

Google has released Beta channel ChromeOS version 15823.40.0 with Chrome Browser version 124.0.6367.95 for most ChromeOS devices and Long Term Support (LTS) Channel to 120.0.6099.309, Platform Version: 15662.105.0 for most ChromeOS devices to resolve critical vulnerability.

CVE ID: CVE-2024-4058 (Critical)

1. **Adv/2024/May/008**

It has been observed that threat actors are exploiting directory traversal vulnerabilities in software’s (e.g., CVE-2024-1708, CVE-2024-20345 etc.), which are mostly used in Critical Information Infrastructures (CIIs).

The directory traversal vulnerabilities are those vulnerabilities in which users manipulating inputs (i.e., input parameters or file paths) to access application files and directories that the developers do not intend for users to access. These exploits allow malicious cyber actors to access restricted directories and read, modify or write arbitrary files.

**Mitigation for Software Manufacturers to Prevent Directory Traversal Vulnerabilities:-**

* Generate a random identifier for each file and store associated metadata separately (e.g. in a database) rather than using user input when naming files.
* Strictly limit the types of characters that can be supplied in file names, e.g., by restricting to alphanumeric characters. The uploaded files should not have executable permissions.

**Note:** These vulnerabilities can also affect cloud services. Software manufacturers should implement the above guidance, and best practices, to prevent directory traversal vulnerabilities in cloud systems.

**Software manufacturers should follow below three principles to protect their products from falling victim to directory traversal exploits and other preventable malicious activity:**

**Principle 1: Take Ownership of Customer Security Outcomes**

1. Software developers & manufacturers should take ownership of their products & invest in securing the products of their customers as well as the public. These include providing safe building blocks for their software developers to ensure that a single developer error does not compromise the data of millions of users.

2. Manufacturers should also implement audit mechanisms through automation to measure developer compliance with these best practices.

3. Open Source Foundation for Application Security (OWASP) & other trusted entities provide guidance on testing methods with readily available techniques and standard best practices can help software manufacturers to root out directory traversal vulnerabilities at the source.

**Principle 2: Embrace Radical Transparency and Accountability**

1. Manufacturers should lead with transparency when disclosing product vulnerabilities. They should identify and document the root causes of directory traversal vulnerabilities and declare it a business goal to work toward eliminating the entire class of vulnerability.

2. Manufacturers should maintain a modern Vulnerability Disclosure Program (VDP).

**Principle 3: Build Organizational Structure and Leadership to Achieve Goals**

1. Software and hardware manufacturing executives should make the appropriate investments and develop the right incentive structures that promote security as a stated business goal.

2. Executives should lead programs to root out entire classes of vulnerability rather than addressing them on a case-by-case basis.

3. Executives should also ensure their organization conducts reviews to detect common and well-known vulnerabilities, like directory traversal, to determine their susceptibility and implement the existing effective and documented mitigations.

4. Executives should request regular updates to assess the company’s progress at identifying recurring classes of vulnerability as well as progress to eliminate them and lend support to provide appropriate resources to continue such progress.

1. **Adv/2024/May/009**

Multiple vulnerabilities have been discovered in CyberPower's Equipment- PowerPanel. The affected versions are PowerPanel 4.9.0 and prior. The mitigations are available.

CVE ID: CVE-2024-34025 (Critical), CVE-2024-33615 (High), CVE-2024-32053 (Critical), CVE-2024-32047 (Critical), CVE-2024-32042 (Medium), CVE-2024-31856 (High), CVE-2024-31410 (Medium), CVE-2024-31409 (Medium)

1. **Adv/2024/May/010**

It has been observed that threat actors are exploiting a weakness in the NetNTLM authentication protocol using NetNTLM credential relay attacks. An attacker can trick a victim into authenticating to a malicious server, capture the NetNTLM hash obtained through malicious file shares, email links, or Cross Site Scripting (XSS) vulnerabilities in web applications and relay it to access other services or systems that trust the victim's credentials. This allows the attacker to move laterally within the network, escalate privileges, and potentially compromise the entire domain.

**Recommendations:**

* Enable Windows Firewall on all network profiles. Block inbound connections to high risk ports like 445 (SMB), 139 (NetBIOS), 389 (LDAP).
* Restrict outbound SMB and WebDAV connections to prevent outbound relay attacks.
* Allow only necessary inbound ports required for services: Identify the ports needed for essential services (e.g., RDP, HTTP, HTTPS).
* Implement Deep Packet Inspection (DPI) and Network Flow Analysis.
* Use LDAPS (LDAP over SSL/TLS) instead of clear-text LDAP where possible. Obtain a valid SSL/TLS certificate for your domain controller(s) from a trusted Certificate Authority (CA) or generate a self-signed certificate.
* Avoid using high privilege domain admin accounts for email and web browsing. Use separate unprivileged accounts for these tasks. Implement tiered admin model with dedicated admin workstations and jump servers.
* Keep systems patched and up-to-date, especially for Windows security updates.
* Deploy Multi-Factor Authentication (MFA) for all user accounts, especially for remote access and privileged accounts.
* Implement a strong password policy that requires a minimum length, complexity, and regular password changes.
* Regularly audit and review user accounts to ensure compliance with password and MFA policies.
* Implement network segmentation to limit lateral movement.
* Implement Access Control Lists (ACLs) on routers and switches to filter traffic based on IP addresses, ports, and protocols.
* Use host-based firewalls to further restrict communication between systems within the same zone.

1. **Adv/2024/May/011**

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

**IOCs: IOC\_Adv2024May011.txt attached**

1. **Adv/2024/May/012**

Presence of malicious IoCs found in Indian Cyberspace related to APT SideCopy.

**IOCs: IOC\_Adv2024May012.txt attached**

1. **Adv/2024/May/013**

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\_Adv2024May013.txt attached**

1. **Adv/2024/May/014**

It has been observed that in a recent campaign, threat actor MuddyWater is sending malicious PDF attachments from the compromised email ID. The malicious PDF contains links to various web hosting services where users download an archive containing a remote administration tool to compromise systems.  Adversary uses DarkBeat Command & Control (C2) as the central point to manage all the infected computers. The threat actor usually establishes a connection to C2 in one of the following ways:

a) Manually executing PowerShell code to establish a connection to C2 after gaining initial access via another method.

b) Wrapping a connector to execute the code to establish a C2 connection within the first stage payload, which is delivered in a spear phishing email.

c) Sideloading a malicious DLL to execute the code to establish a C2 connection by masquerading as a legitimate application (PowGoop and MuddyC2Go).

**IOCs: IOC\_Adv2024May014.txt attached**

1. **Adv/2024/May/015**

It has been observed that in the ArcaneDoor campaign, state-sponsored threat actors are targeting perimeter network devices of multiple vendors for cyber espionage activities.  Adversary uses sophisticated attack chains to implant custom malware (“Line Runner” & “Line Dancer”) and execute commands to compromise systems. Adversaries exploited two vulnerabilities in the management & VPN web servers for Cisco Adaptive Security Appliance (ASA) software and Cisco Firepower Threat Defense (FTD) software (CVE-2024-20353 and CVE-2024-20359).  Adversaries then deployed Line Dancer, a memory-only implant in a memory-resident shellcode interpreter that allows adversaries to upload and execute arbitrary shellcode payloads. Threat actors maintain persistence using a backdoor called Line Runner using functionality related to a legacy capability that allowed for the preloading of VPN clients and plugins on the device.

**IOCs: IOC\_Adv2024May015.txt attached**

1. **Adv/2024/May/016**

It has been observed that GoldDigger is an android trojan designed to target and exploit victims. This malware operates by infiltrating a victim’s device through deceptive means, such as posing as legitimate applications or attachments. Once installed, it performs various activities such as stealing personal and financial information such as login credentials, credit card numbers and other sensitive data. It spreads via phishing tactics, links to malicious apps, mimicking legitimate apps.

**IOCs: IOC\_Adv2024May016.txt attached**

1. **Adv/2024/May/017**

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\_Adv2024May017.txt attached**

1. **Adv/2024/May/018**

Presence of malicious IoCs are found in Indian Cyberspace related to Side Copy, AresRAT malware, Mythic malware, APT36, GavaRAT Malware, GavaRAT, ShadowPad, QuestRAT and state sponser threat actor's.

**IOCs: IOC\_Adv2024May018.txt attached**

1. **Adv/2024/May/019**

**Vulnerability in Social Connect plugin for WordPress**

Authentication bypass vulnerability has been discovered in Social Connect plugin for WordPress. The affected versions are Social Connect plugin for WordPress versions up to, and including, 1.2.

CVE ID: CVE-2024-4393 (Critical)

**Vulnerability in Startklar Elementor Addons plugin for WordPress**

Arbitrary file deletion vulnerability has been discovered in Startklar Elementor Addons plugin for WordPress. The affected versions are Startklar Elementor Addons plugin for WordPress versions up to, and including, 1.7.13.

CVE ID: CVE-2024-4346 (Critical)

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

Authentication bypass vulnerability has been discovered in Build App Online plugin for WordPress. The affected versions are Build App Online plugin for WordPress for WordPress versions up to, and including, 3.0.5.

CVE ID: CVE-2024-4186 (Critical)

**Vulnerability in Delta Electronics' Equipment**

A deserialization of untrusted data vulnerability has been discovered in Delta Electronics' Equipment- InfraSuite Device Master that allows Remote Code Execution (RCE). The affected versions are InfraSuite Device Master versions 1.0.10 and prior. The mitigations are available.

CVE ID: CVE-2023-46604 (Critical)

**Android Security Updates**

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

CVE ID: CVE-2024-0024 (High), CVE-2024-0025 (High), CVE-2024-23705 (High), CVE-2024-23708 (High), CVE-2024-23706 (Critical), CVE-2024-0043 (High), CVE-2024-23707 (High), CVE-2024-23709 (High), CVE-2023-4622 (High), CVE-2023-6363 (High), CVE-2024-1067 (High), CVE-2024-1395 (High), CVE-2023-32871 (High), CVE-2023-32873 (High), CVE-2024-20056 (High), CVE-2024-20057 (High), CVE-2024-21471 (High), CVE-2024-21475 (High), CVE-2024-23351 (High), CVE-2024-23354 (High), CVE-2023-33119 (High), CVE-2023-43529 (High), CVE-2023-43530 (High), CVE-2023-43531 (High), CVE-2024-21477 (High), CVE-2024-21480 (High)

**HPE Aruba Networking Security Updates**

HPE Aruba Networking has released security updates to address multiple vulnerabilities in its products.

CVE ID: CVE-2024-26304 (Critical), CVE-2024-26305 (Critical), CVE-2024-33511 (Critical), CVE-2024-33512 (Critical), CVE-2024-33513 (Medium), CVE-2024-33514 (Medium), CVE-2024-33515 (Medium), CVE-2024-33516 (Medium), CVE-2024-33517 (Medium), CVE-2024-33518 (Medium)

1. **Adv/2024/May/020**

It has been observed that Kutaki malware is an information stealer and keylogger that hides inside legitimate Visual Basic applications. The initial infection is by using a spear-phishing email which contains a URL. Upon click, URL downloads a ZIP file which consists of an EXE file imbedded in it.  The name of the file is Tax payment challan.exe. While opening the .exe file, a BMP (BITMAP) IMAGE gets opened. In the background, multiple .exe files like "FZSTUYFK.EXE / DLPNKUFK.EXE" are executed which results in a background malicious process or activity to compromise systems.

**IOCs: IOC\_Adv2024May020.txt attached.**

1. **Adv/2024/May/021**

It has been reported that a malspam campaign is leveraging Phorpiex botnet to distribute LockBit ransomware (the LockBit Black encryptor). The email contains a malicious ZIP attachment, once extracted it includes a malicious file abusing double extension in the filename to mimic Microsoft Word document as a means of masquerading the true file type. The primary use of the Phorpiex botnet functions as a spam mailer, it has been used for ransomware delivery, distributing ransomware families such as Avaddon, GandCrab. Phorpiex uses an IP-based command and control (C2) and delivery site(s).

**IOCs: IOC\_Adv2024May021.txt attached**

1. **Adv/2024/May/022**

It has been observed that the banking trojan, CarnavalHeist, is active & uses Tactics, Techniques and Procedures (TTPs) similar to other banking trojan - Grandoreiro, Vizom, Guildma and CHAVECLOAK. The execution of banking trojan CarnavalHeist begins with a malicious LNK file, masquerading as a financially themed PDF document distributed as a malicious attachment through phishing emails. The Windows batch file serves as a wrapper for installing Python onto the target environment and subsequently executing a Python script that handles injecting the second stage payload DLL. It also starts a hidden PowerShell process and executes a base64-encoded command which acts as a loader for injecting a malicious DLL. The final execution block downloads the next payload stage using Dynamically Generate (DAG) subdomains. It attempts to steal a target’s credentials using overlay attack methodologies. An overlay attack is a technique that involves placing a fake layer on top of the user interface of desktop and mobile applications, websites, and other platforms. These fake portals or login pages would then capture credentials entered and/or redirect any further navigation from the overlay to pages or addresses decided by the threat actor.  CarnavalHeist possesses numerous capture capabilities, commonly associated with banking trojans, which include keyboard capture, screenshots and video capture.

**IOCs: IOC\_Adv2024May022.txt attached**

1. **Adv/2024/May/023**

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\_Adv2024May023.txt attached**

1. **Adv/2024/May/024**

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\_Adv2024May024.txt attached**

1. **Adv/2024/May/025**

Presence of malicious IoCs found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May025.txt attached**

1. **Adv/2024/May/026**

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\_Adv2024May026.txt attached**

1. **Adv/2024/May/027**

It has been observed that Cuttlefish is a malware platform that targets networking equipment, specifically enterprise-grade Small Office/Home Office (SOHO) routers. This malware is modular, designed primarily to steal authentication materials found in web requests that transit the router from the adjacent Local Area Network (LAN). The malware is capable of performing both DNS and HTTP hijacking for connections to private IP space. It has the ability to interact with other devices on the LAN.  It offers a zero-click approach to capturing data from users and devices behind the targeted network’s edge. It passively sniffs packets and acts only when triggered by a predefined ruleset. The packet sniffer used by Cuttlefish was designed to acquire authentication material, with an emphasis on public cloud-based services. To exfiltrate data, the threat actor first creates either a proxy or VPN tunnel back through a compromised router, then uses stolen credentials to access targeted resources.

I**OCs: IOC\_Adv2024May027.txt attached**

1. **Adv/2024/May/028**

It has been observed that the number of threats have increased to leverage the Microsoft Graph API to facilitate communications with Command & Control (C2) infrastructure hosted on Microsoft cloud services. Graph is a Microsoft API designed to allow developers to access resources hosted on Microsoft cloud services, such as Microsoft 365. Authentication is carried out using OAuth access tokens.

The malware named as BirdyClient or OneDriveBirdyClient is abusing these facilities by deploying malicious vxdiff.dll masquerading as a legitimate file or by sideloading. The file name vxdiff.dll is the same legitimate DLL associated with an application called Apoint (apoint.exe), which is driver software for Alps pointing devices, usually found in laptops. The main functionality of BirdyClient malware is to connect to the Microsoft Graph API and use Microsoft OneDrive as a C2 server mechanism to upload and download files from it.

**IOCs: IOC\_Adv2024May028.txt attached**

1. **Adv/2024/May/029**

**Vulnerability in Social Connect plugin for WordPress**

Authentication bypass vulnerability has been discovered in Social Connect plugin for WordPress. The affected versions are Social Connect plugin for WordPress versions up to, and including, 1.2.

CVE ID: CVE-2024-4393 (Critical)

**Vulnerability in Startklar Elementor Addons plugin for WordPress**

Arbitrary file deletion vulnerability has been discovered in Startklar Elementor Addons plugin for WordPress. The affected versions are Startklar Elementor Addons plugin for WordPress versions up to, and including, 1.7.13.

CVE ID: CVE-2024-4346 (Critical)

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

Authentication bypass vulnerability has been discovered in Build App Online plugin for WordPress. The affected versions are Build App Online plugin for WordPress for WordPress versions up to, and including, 3.0.5.

CVE ID: CVE-2024-4186 (Critical)

**Vulnerability in Delta Electronics' Equipment**

A deserialization of untrusted data vulnerability has been discovered in Delta Electronics' Equipment- InfraSuite Device Master that allows Remote Code Execution (RCE). The affected versions are InfraSuite Device Master versions 1.0.10 and prior. The mitigations are available.

CVE ID: CVE-2023-46604 (Critical)

**Android Security Updates**

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

CVE ID: CVE-2024-0024 (High), CVE-2024-0025 (High), CVE-2024-23705 (High), CVE-2024-23708 (High), CVE-2024-23706 (Critical), CVE-2024-0043 (High), CVE-2024-23707 (High), CVE-2024-23709 (High), CVE-2023-4622 (High), CVE-2023-6363 (High), CVE-2024-1067 (High), CVE-2024-1395 (High), CVE-2023-32871 (High), CVE-2023-32873 (High), CVE-2024-20056 (High), CVE-2024-20057 (High), CVE-2024-21471 (High), CVE-2024-21475 (High), CVE-2024-23351 (High), CVE-2024-23354 (High), CVE-2023-33119 (High), CVE-2023-43529 (High), CVE-2023-43530 (High), CVE-2023-43531 (High), CVE-2024-21477 (High), CVE-2024-21480 (High)

**HPE Aruba Networking Security Updates**

HPE Aruba Networking has released security updates to address multiple vulnerabilities in its products.

CVE ID: CVE-2024-26304 (Critical), CVE-2024-26305 (Critical), CVE-2024-33511 (Critical), CVE-2024-33512 (Critical), CVE-2024-33513 (Medium), CVE-2024-33514 (Medium), CVE-2024-33515 (Medium), CVE-2024-33516 (Medium), CVE-2024-33517 (Medium), CVE-2024-33518 (Medium)

1. **Adv/2024/May/030**

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\_Adv2024May030.txt attached**

1. **Adv/2024/May/031**

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

**IOCs: IOC\_Adv2024May031.txt attached**

**Recommendations:**

* 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.
* Install and regularly update antivirus software.
* Conduct regular data backup practices and keep those backups offline.
* Implementing Multi-Factor Authentication (MFA) where possible.
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Protect organisation’s environment using organisational firewalls, proxies, web filtering and email filtering.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for Microsoft Office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.

1. **Adv/2024/May/032**

It has been observed that the affiliates of Black Basta, a Ransomware as a Service (RaaS) variant, are targeting Critical Infrastructure. Adversary for initial access uses techniques such as phishing and exploiting known vulnerabilities. It employs a double-extortion model, both encrypting systems and exfiltrating data. For discovery and execution, Black Basta affiliates use tools such as SoftPerfect network scanner to conduct network scanning. Tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP) are used for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons for remote access as well as for lateral movement.  Black Basta affiliates also use credential-scraping tools like Mimikatz for privilege escalation. It uses Rclone for data exfiltration.

I**OCs: IOC\_Adv2024May032.txt attached**

1. **Adv/2024/May/033**

**Vulnerability in DigiWin EasyFlow .NET**

A SQL injection vulnerability has been discovered in DigiWin EasyFlow .NET that allows unauthorized access to read, modify, and delete database records, as well as execute system commands.

CVE ID: CVE-2024-4893 (Critical)

1. **Adv/2024/May/034**

Reference is made to earlier advisories on Sandworm aka APT44 & Seashell Blizzard.

It has been observed that threat actor Sandworm aka APT44 & Seashell Blizzard is deploying Kapeka dropper to the targeted systems, potentially through exploitating the vulnerability or by supply chain attack. Kapeka dropper is deployed along with tools like  LOADGRIP (loader), GOSSIPFLOW (proxy), and BIASBOAT (Linux variant of Kapeka). Kapeka is used in the intrusion that led to the deployment of Prestige ransomware.

Kapeka dropper deploys the backdoor, establishes persistence for it and deletes itself using a batch script. The backdoor writes its configuration to the registry and begins communicating with its Command & Control (C2) server, waiting for tasks to execute. Kapeka provides Sandworm ability to update its configuration, read and write files, launch processes or payloads, execute arbitrary commands, and upgrade the backdoor. The execution of payloads run as a child process of the backdoor, and results of tasks are encrypted and sent back to the C2. During setup, Kapeka also performs some initial fingerprinting of the system, collecting details including user, computer, and domain name, OS version, and architecture, before sending them to its C2.

**IOCs: IOC\_Adv2024May034.txt attached**

1. **Adv/2024/May/035**

Reference is made to earlier advisories on Mustang Panda aka Bronze President, TA416, RedDelta and Earth Preta.

It has been observed that Mustang Panda is introducing a variety into its intrusion techniques – changing container files (e.g. Virtual Hard Disk (VHD) file), using alternative file extensions to disguise executable files and using new legitimate executables to side-load malicious DLLs to deploy e PUBLOAD and TONESHELL malware implants.

When a VHD file opens, the file is mounted as a VHD drive that contains three hidden folders and one shortcut (LNK) file. The hidden folders contain legitimate EXE files and malicious DLL files. The EXE file then side-loads the malicious DLL file. Once executed, the malware replicates itself under C:\Users\Public\Libraries and creates a registry run key named DropboxCrashHandler for persistence. The DLL file decodes, injects, and executes a PE file in memory. The PE file is encoded as a series of UUID strings, and is decoded into binary using the UUIDFromStringA function. The PE file has been modified to be executable as shellcode, and is executed using EnumSystemLocalesA. The PE file is a variant of TONESHELL.

**IOCs: IOC\_Adv2024May035.txt attached**

**Yara Rule: Adv2024May035\_Yara\_Rule.txt attached**

1. **Adv/2024/May/036**

Reference is made to earlier advisories on Emissary Panda.

It has been observed that threat group Emissary Panda is regularly creating new SysUpdate infrastructure, which presents a set of characteristics that have been synonymous with the tool for some time. The group is continuing to use both Windows and Linux variants of its SysUpdate tool, and numerous Command & Control (C2) communication routes such as HTTP, HTTPS, and DNS. The threat group is targeting Critical Infrastructure, specifically government, finance & insurance, software & services, and transportation organisations. It has also been found that Emissary Panda is using the shadowpad in its campaign alongside its custom tooling.

**IOCs: IOC\_Adv2024May036.txt attached**

**Yara Rule: Adv2024May036\_Yara\_Rule.txt attached**

1. **Adv/2024/May/037**

Presence of malicious IoCs found in Indian Cyberspace.

**IOCs: IOC\_Adv2024May037.txt attached**

1. **Adv/2024/May/038**

Presence of malicious IoCs found in Indian Cyberspace related to APT SideCopy & Lazarus Group.

**IOCs: IOC\_Adv2024May038.txt attached**

1. **Adv/2024/May/039**

Reference is made to earlier advisory with subject "Phishing Attack" and Advisory No: Adv/2024/Apr/041 dated 26 Apr 2024.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024May039.txt attached**