**Cyber Security Advisories**

**Date: 30-04-2024**

1. **CMTX-I-405042024 APT36 campaign**

Recent C&C server IP of malware used by Pakistan based APT36 threat actors is as follows:  
  
- ------------ <C&C IP> ------------  
176.107.184.36  
- ----------- </C&C IP -------------.

1. **CMTX-P042024225 Akira Ransomware**

ALERT BRIEF:

PREVIOUS REFERENCE:CMTX-P052023038 Akira Ransomware (TLP: CLEAR), dated 09/05/2023

Akira Ransomware, a notorious threat group, that has wreaked havoc across various organizations is again active in the cyber threat landscape. Earlier it used ".akira" extension but now it has changed its tactics and deploys Megazord, which uses Rust-based code and encrypts files with a “.powerranges” extension. It also deploys a Linux variant apart from Windows to target VMware ESXi virtual machines. The group employs a double-extortion technique by threatening to leak stolen data to persuade victims to pay the ransom.

MITRE ATT&CK Identifiers:

Valid Accounts- (T1078)

Exploit Public Facing Application- (T1190)

External Remote Services- (T1133)

Phishing: Spearphishing Attachment- (T1566.001)

OS Credential Dumping- (T1003)

System Network Configuration Discovery- (T1016)

System Information Discovery- (T1082)

Domain Trust Discovery- (T1482)

Process Discovery- (T1057)

Permission Groups Discovery:Local Groups- (T1069.001)

Remote System Discovery- (T1018)

Create Account: Domain Account- (T1136.002)

Remote Access Software- (T1219)

Proxy- (T1090)

Financial Theft- (T1657)

Inhibit System Recovery- (T1490)

Transfer Data to Cloud Account- (T1537)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e

bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138

73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf

1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386

aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9

7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4

36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c

3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c

ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc

dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198

131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07

9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c

9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065

2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83

7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be

95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a

0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d

C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0

aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d

18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88

5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32

8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694

892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0

7a647af3c112ad805296a22b2a276e7c

- - ----------------------------------------------------------------------------

RECOMMENDATIONS

\* Regularly update the operating system, applications, and security software. Patches often address known vulnerabilities that attackers exploit.

\* Enable MFA for critical services such as VPNs, remote desktop access, and email accounts. This adds an extra layer of security.

\* Isolate critical systems from less critical ones. Limit lateral movement for attackers within your network.

\* Educate employees about phishing techniques and safe online practices. Regular training can prevent social engineering attacks.

\* Regularly back up  data to secure, offline locations. Test backups to ensure they are functional. Consider using immutable backups to prevent ransomware from affecting backups.

\* Limit user permissions to only what is necessary for their roles. Avoid unnecessary administrative privileges

\* Deploy endpoint security solutions that detect and block malicious activity. Use behavior-based detection to identify suspicious behavior.

- - - --------------------ALERTEND----------------------------------------------

1. **CMTX-I-162042024 CrimsonRAT - APT36 campaign**

Recent C&C server IP of CrimsonRAT malware used by Pakistan based APT36 threat actors are as follows:

- ------------ <C&C Domain> ------------

zirtbox.duckdns.org

\*.duckdns.org

- ------------ </C&C Domain> -------------

Please note: It has been observed that various sub-domains having duckdns.org as parent domain is being used as C&C for the malware. Additionally, being Dynamic DNS domain the IP resolution may change at regular intervals. Hence, domain based blocking for the DDNS domain is recommended rather than current IP resolution and monitoring of parent domain is also recommended.

1. **CMTX-P042024225 Wide Exploitation of CrushFTP Virtual Filesystem Escape Vulnerability**

----------------------------------------------------------------------  
Following domain and its subdomains are being used for spear-phishing and hosting malware purpose targeting government officials:

- --------------<Malicious Domains>-----------------

www.mod.gov.in.detailedcases.info  
mod.gov.in.detailedcases.info  
\*.detailedcases.info  
www.mea.gov.in.casereports.info  
mea.gov.in.casereports.info  
\*.casereports.info  
  
- -------------</Malicious Domains>-----------------

1. **CMTX-P0420247794 GooseEgg Malware**

ALERT BRIEF:

GooseEgg, a custom privilege escalation tool used by the Russia-based threat group Forest Blizzard. GooseEgg exploits CVE-2022-38028, a Windows Print Spooler service vulnerability, to execute arbitrary commands with SYSTEM-level privileges on victim machines. Consequently, GooseEgg gains the ability to execute arbitrary commands with elevated privileges, enabling Forest Blizzard to perform various malicious activities within the compromised system. Attacker deploys GooseEgg with batch scripts (execute.bat and doit.bat). GooseEgg also creates a scheduled task for maintaining persistence.

Once GooseEgg execute on machine, GooseEgg perform below four function:-

• Execute the “whoami” command to retrieve the username of the currently logged-in user

• Retrieve system information and the current system time and date

• Detect debuggers using the IsDebuggerPresent API function

• Enumerate files and directories

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASH

c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5

6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f

fd2904b9d06e210f163cb799eda9f1b4d1a51aabc80a3ecf047b448065ac132e

ea0847708231bab84c9f97d5fc1e17c46a1dbadf83cbe2808c7a2440a5c04435

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P0420247694 ToddyCat APT Activity**

ALERT BRIEF:

ToddyCat is a suspected Chinese nation-state group primarily focusing on traffic tunnelling methods and creating persistent access to compromised systems through various advanced techniques. Threat Actor is known for creation of reverse SSH tunnels, deploy SoftEther VPN, fast reverse proxy [FRP Client and renaming the executable files. Recently threat actor is using the three data collection tools to extract information from compromised systems:

• Cuthead: Designed to search and archive documents based on specified parameters such as file extensions and keywords.

• WAExp: Targets browser local storage files associated with the web version of WhatsApp.

• TomBerBil: Used for extracting browser cookies and passwords

Mapping of Attack Campaign on MITRA MATRIX

T1119 (Automated Collection)

T1090 (Proxy)

T1547.012 (Print Processors)

T1027 (Obfuscated Files or Information)

T1570 (Lateral Tool Transfer)

T1547 (Boot or Logon Autostart Execution)

T1070 (Indicator Removal)

T1070.004 (File Deletion)

T1572 (Protocol Tunneling)

T1555 (Credentials from Password Stores)

T1083 (File and Directory Discovery)

T1555.003 (Credentials from Web Browsers)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Malicious HASH

1D2B32910B500368EF0933CDC43FDE0B

5C2870F18E64A14A64ABF9A56F5B6E6B

AFEA0827779025C92CAB86F685D6429A

C7D8266C63F8AECA8D5F5BDCD433E72A

750EF49AFB88DDD52F6B0C500BE9B717

853A75364D76E9726474335BCD17E225

BA3EF3D0947031FB9FFBC2401BA82D79

HASH of Legitimate application used by threat actor

4A79A8B1F6978862ECFA71B55066AADD FRP client

1F514121162865A9E664C919E71A6F62 vpnserver\_x64.exe

6F32D6CFAAD3A956AACEA4C5A5C4FBFE vpnserver\_x64.exe

9DC7237AC63D552270C5CA27960168C3 ngrok.exe

34985FAE5FA8E9EBAA872DE8D0105005 ngrok.exe

IP

103.27.202.85

118.193.40.42

Domain

Ha.bbmouseme.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

RECOMMENDATIONS:

• Forbid the use of unused or unauthorized remote access tools. Implement technical controls to restrict access to these tools. Additionally, set up monitoring mechanisms to track the usage of approved tools and detect any unauthorized usage or suspicious activities.

• Regularly review and update the firewall deny list to include new resources and IP addresses associated with tunnelling services as they are identified. Implement monitoring and alerting mechanisms on the firewall to detect and alert administrators about any attempts to access the organization's network from deny listed cloud services.

- -------------------------------------ALERTEND------------------------------------------------------

1. **CMTX-P0420240554 Qilin Ransomware**

ALERT BRIEF:

Alias: Agenda Ransomware

Qilin is a ransomware written in the Go (Golang) programming language and bears similarities in tactics, techniques, and procedures (TTPs), as well as code similarities, to the Black Basta, BlackMatter, and REvil (Sodinokibi) ransomware groups. It uses various techniques to gain access to systems, including exploiting vulnerabilities and phishing. Once inside a network, the ransomware is executed through command-line arguments, which include options for disabling security measures and spreading across networks. The malware has been observed leveraging different vulnerable drivers to disable security tools and propagate through virtual machine infrastructure. It employs Remote Monitoring and Management (RMM) tools and Cobalt Strike for deployment of the ransomware binary.

Mapping of Attack campaign on MITRA Matrix

T1071 (Application Layer Protocol)

T1106 (Native API)

TA0011 (Command and Control)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASHE

5e9fc42cf65e1a87e953d00cb2755d3b5b00c1414259534c3a85742295bb6ff9

65709a9094831646a4dd573651ab74321d3a0b643a1833c4050959f4ec3bf93b

ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca8643908261638b256

dfd93f8290b6bab8f56da255737cc8c3b7b97261e4294ce39f52c7e778e1524b

117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464

37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6

e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Recommendations:-

• Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

• Ransomware infections primarily keep data as hostage. Therefore, maintain offline backups of critical data and ensure that these backups stay up to date to prevent data loss in event of ransomware infection.

• All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software.

• Periodic Backups and restoration tests to check the restoration integrity.

• For detailed recommendations please refer to "Best Practices and Remedial measures" on https://www.cyberswachhtakendra.gov.in/alerts/ransomware.html

Other references:

https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

- - - - - --------------------------------ALERTEND-------------------------------------------------------------------------

1. **CMTX-I-712042024 SideCopy Malware C&C IP**

Following is the latest C&C IP address of a Pakistan based SideCopy malware campaign targeting government officials:  
  
- --------------<C&C> ---------------  
213.136.94.11  
- -------------</C&C> ---------------  
  
Kindly take the required actions.

1. **CMTX-P042024265 Critical Vulnerability (CVE-2024-3902) in Citrix uberAgent**

ALERT BRIEF:

A new vulnerability tracked as CVE-2024-3902 is found to be affecting Citrix uberAgent, a specialized tool used for user experience monitoring and security analytics in Citrix deployments and virtualized environments. On successful exploitation of the flaw, this may result in the escalation of privileges of the attacker if there is at least one configured CitrixADC metric and specific Citrix session metrics configured (for versions 7.0 – 7.1.1).

This vulnerability only impacts uberAgent and does not impact any other Citrix or Cloud Software Group products.

AFFECTED VERSION:

Citrix uberAgent before 7.1.2

RECOMMENDATIONS:

\* Organizations using affected software should immediately upgrade to version 7.1.2 or later of Citrix uberAgent.

\* Temporarily they can disable CitrixADC Metrics and adjust WMI Provider Settings (for specific versions).

- - ------------------------------------ALERTEND------------------------------------------------------

1. **CMTX-P042024255 Critical Vulnerability (CVE-2024-27956) Affecting WP‑Automatic plugin for WordPress**

ALERT BRIEF:

CVE-2024-27956

CVSS-9.9

It has been reported that an SQL injection vulnerability tracked as CVE-2024-27956 is affecting the WP‑Automatic plugin for WordPress that could allow site takeovers and malicious activities. It allows atackers to gain unauthorized access to websites, create fake admin accounts (like those starting with “xtw”), upload malicious files, and potentially take full control of affected sites. They also create backdoors and obfuscating codes to enhance the longevity of their access.

VULNERABLE VERSION: <= 3.92.0

PATCHED VERSION: 3.92.1

RECOMMENDATIONS:

\* Since the exploitation is in the wild and there are high chances of site compromise, therefore, it is recommended to patch this vulnerability on priority to prevent unauthorized access and data breaches that could result from exploitation.

1. **CMTX-P042024048 Sharp Stealer**

ALERT BRIEF:

Sharp Stealer is information or credential stealer malware written in .NET. Primarily sharp stealer is used by attacker to Collect sensitive user files, Retrieve session data and credentials from various applications and services, including gaming clients, messaging applications, email clients, FTP clients, and VPN tools.

Besides these, stealer can

1. Store the collected data into text files and Send it to a Telegram bot

2. Access web browser profiles for stored web session cookies, credentials, and browsing data

3. Access cryptocurrency wallets and files to harvest credentials

4. Check the machine’s external IP address and geolocation, Retrieve processor information to detect sandbox environments and Enumerate running processes

5. Capture desktop screenshots and the victim’s clipboard data

Attack vector used by Sharp Stealer is:-

Reflective Code Loading

Access Token Manipulation

Time Based Evasion

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASH

b6e763d6b886308df0e0c3e9342dd83dba88d68eb312e0540b24d8dcdcaa1920

42efd817539480fb44da60d797908869af796df6bfb700980709ccf483e92b96

f0bc0f948edb5c15f936234b0453290c135def1fc8dc29e344f4d816ee16110f

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

- - - -------------------ALERTEND----------------------------------------------