**Cyber Security Advisories**

**Date: 17 July 2024**

1. **CMTX-I-194062024: SpyNote - APT36 Campaign**

Recent C&C server domains of SpyNote malware (Android) used by Pakistan based threat actors to target government officials are as follows:

- -----------<C&C Domains>-----------

88c.34667.fun

903.78990.fun

56184.fun

9123.89204.fun

- -----------</C&C Domains>----------

Kindly take the required actions.

1. **CMTX-I-020062024: CrimsonRAT - APT36 campaign**

Recent C&C server IP of CrimsonRAT malware used by Pakistan based threat actors (APT36) to target government officials are as follows:

- ----------- <C&C IP> -----------

84.247.172.135

- ----------- </C&C IP> ----------

1. **CMTX-P062024005: PLUGX RAT ALERT 123**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

IP

172.111.233.105

92.243.65.119

47.238.202.81

156.224.24.129

173.199.71.152

38.60.203.233

45.249.89.43

193.134.210.123

142.93.220.126

103.79.120.68

182.16.17.206

118.107.44.132

110.173.49.214

118.107.44.133

118.194.239.90

118.107.44.134

65.20.102.39

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

1. **CMTX-P062024205: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

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

IP

185.225.19.48

103.180.161.230

176.120.74.127

154.90.58.189

38.54.32.181

38.60.193.190

182.161.66.112

98.98.170.159

38.54.112.205

156.255.3.195

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

1. **CMTX-I-021072024: Mythic Malware - APT36 campaign**

Following are the C&C of Mythic Malware. This RAT is being used by the Pakistan based APT36 group to target Linux based systems (particularly BOSS OS) in government offices.

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

67.219.108.45

64.176.8.42

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

1. **CMTX-P072024015: Circulation of Phishing email contain links to counterfeit CERT-In websites**

ALERT BRIEF:-

In continuation of our earlier alert, regarding Circulation of Phishing email contain links to counterfeit CERT-In websites, CERT-In has identified that threat actors are distributing emails that closely mimic CERT-In's official communication style when notifying affected parties about incidents( Phishing mail image is attached with image). These phishing emails include malicious links to counterfeit CERT-In websites that host harmful payloads. Additionally, attackers are employing a sophisticated social engineering technique by making phone calls and posing as representatives from trusted organizations to trick individuals to take actions on the spear phishing mails /installing malware. This tactic leverages the trust and authority associated with reputable institutions to manipulate victims.

Recommendation:-

• All emails from CERT-In are cryptographically signed and originate from designated email addresses: incident@cert-in.org.in (for incident reports), submit@cert-in.org.in (for sample analysis), advisory@cert-in.org.in, cmtx.certin@cert-in.org.in (for CMTX alerts and platform-related communications), and csk@cert-in.org.in (for Cyber Swachhta Kendra). Recipients are encouraged to verify the authenticity of each email before clicking any links or opening attachments.

• Implement robust email filtering solutions to detect and block phishing emails. Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block attachments of file types: [exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf].Ensure to scan all software downloaded from the Internet prior to executing. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).Before entering sensitive information on a website, check the URL for inconsistencies or suspicious elements. Ensure it uses HTTPS and matches the official domain.

• 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 to prevent e-mail spoofing. This will prevent malicious mails to reach your corporate mailboxes. Always verify the sender's email address and domain. Be cautious of emails from unfamiliar or suspicious addresses.

• Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Monitor users' web browsing habits; restrict access to sites with unfavourable content.

• Educate the employees about phishing techniques and the importance of verifying sender identities and URLs before clicking. Monitor the authenticity of CERT-In and other critical websites regularly.

• Promptly report any suspicious emails upon detection to incident@cert-in.org.in with detailed information like Sender's email address (including any spoofed or suspicious elements), Subject line of the email, Date and time of receipt and any attachments or links included in the email. Forward the mail as an attachment to preserve email headers and other critical metadata.

1. **CMTX-I-025072024: Suspicious Domain Spoofing State Govt. Domain**

The following suspicious domain is registered, possibly to spoof State Govt. (Jharkhand) domain:

- ---------<Suspicious Domain>--------

jharkhandmailgovt.co.in

- ---------</Suspicious Domain>-------

Kindly take the required actions.

1. **CMTX-I-080072024: Malicious Domain Spoofing CERT-In's Domain**

The following malicious domains are registered possibly to spoof CERT-In's domain:

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

certin.in

certn.in

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

Please note: CERT-In website is cert-in.org.in and mail server: mail.cert-in.org.in

1. **CMTX-I-808072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware :

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

pcdaopune.site

pcda.me

pcda.tech

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

Please note, these domains could also be used to send phishing/ malware attachment emails. Hence, emails coming from the above domains should be blocked at the gateway level.

1. **CMTX-P072024025: RADNET64 Hacktivist Group**

ALERT BRIEF:

It has been reported that hacktivist group RADNET64 (associated with the Expiravit Private Military Company) is active in cyber landscape.

Recently attacker announced on its telegram channel to target websites of India cyber space entities i.e. law enforcement agencies. The target of the group is to steal sensitive user data such as names, email addresses, and phone numbers from compromised websites and publicly leak this information on their Telegram channel. They do so by exploiting SQL injection vulnerabilities to gain access to databases and target File Transfer Protocol (FTP) servers for data theft and website defacement. The group establishes remote control and launch distributed denial-of-service (DDoS) attacks by exploiting vulnerabilities in Virtual Network Computing (VNC) servers.

Attackers used the Web shell Pack which contains various PHP files, each potentially representing a web shell script. These scripts are typically used by attackers to gain unauthorized control over a web server.

itigation measures against Website Defacement:

• Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic. Enforce MFA for all users and on all VPN connections and regularly review, validate, or remove privileged accounts.

• Use the latest and updated versions of web server / applications server applications, Apply appropriate updates/patches on the OS and Application software as and when available. Always apply the patch from the official channel.

• Strict enforcement policies on popular Content Management systems (CMS) such as regular patching of CMS applications and its plug-ins such as file mangers, disabling of unused plugins, 2- Factor authentication, adequate ACLs, File type & size Upload limit etc.

• Periodically check the web server directories for any malicious/unknown web shell files, remove it as and when noticed. If found/ observed any such malicious activity, report the incident to CERT-In Incident Response Help Desk immediately. (Email: incident@cert-in.org.in)

• Enforce strict control and monitoring of Windows Native applications such as command-line, PowerShell, WinRM, Windows Management Instrumentation (WMI), and Distributed Component Object Model (DCOM).

• Enable and maintain logs of different devices and servers [Webserver Access/Error logs, Application/DB/ Firewall/IDS/FTP logs] and maintain the same for all the levels. Preserving of these logs help in analyzing the incidents and known the TTP of actors.

• Use firewalls to create a buffer zone between the Internet (and other un-trusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorized protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Employ effective processes for managing changes to avoid workarounds.

• Check for unnecessary connectivity towards Content Delivery Networks, as malware are known to tunnel the connection towards these domains to hide their traffic and towards DDNS / free top level domains. Regular auditing of the failed connection attempts from DNS logs, proxy logs and to successful connection towards unknown domains. Some of the attacks use unconventional usage of DNS queries to exfiltrate interact with the attackers [DNS TXT Records].

• Conduct complete security audit of web application, web server, and database server periodically and after every major configuration change and plug vulnerabilities found. Services of CERT-In empanelled auditors may be availed. (Refer Cyber security Assurance section on website of CERT-In https://www.cert-in.org.in/).

Measures for prevention of Denial of Service (DoS/DDoS) attacks:

1. Measures for detection of attacks

• Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

• Enable adequate logging mechanisms at perimeter level, server, and system level and review the logs at frequent intervals.

• Continuously monitor the network activities & server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.

• Preserve all logs indicating type of attack and attack sources.

2. Protection measures against Distributed Denial-of-Service (DDoS)

• Thoroughly scan the network and online applications and plug any existing vulnerability in the network devices, Operating Systems, Server software and application software and apply latest patches/updates as applicable.

• Consider using a third-party DDoS protection service that can help detect and mitigate attacks, often using a combination of automated and manual techniques

• Employ defence-in-depth strategies: emphasize multiple, overlapping and mutually supportive defensive systems to guard against single point failures in any specific technology and protection method

• Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common attack tools.

• Sudden surge in inbound traffic to any critical server or services, such as ICMP floods, UDP/TCP flood etc. could be due to Distributed Denial of Service (DDoS) attacks. If such attacks are observed, implement appropriate response measures in coordination with Internet Service Provider (ISP).

• Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services.

• To counter attacks on applications, check the integrity of critical application files periodically and in case of suspicion of attack restore applications and content from trusted backups.

• Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.

• In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

• Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.

• Use CAPTCHA challenges to verify that traffic is coming from real users rather than bots, preventing automated attacks

3. Protection Mechanisms against Hack-and-Leak

• Conduct regular vulnerability assessments to identify potential weaknesses in your systems and networks that could be exploited by hacktivists.

• Monitor social media channels for any threats or activity related to hacktivism.

• Implement secure configuration settings on systems and applications to make it more difficult for hacktivists to penetrate them.

• Encrypt sensitive data both in transit and at rest to protect against data interception and theft.

• Regularly backup important data to minimize the impact of a hack-and-leak attack.

• Limit the number of external-facing services to reduce the attack surface and make it more difficult for hacktivists to find vulnerabilities.

1. **CMTX-P072024035: Suspicious domain related to threat actor**

ALERT BRIEF:

CERT-In has identified a list of malicious domains that are being used by threat actors to conduct phishing attacks, distribute malware, and facilitate command and control (C2) communications. These domains may be used to trick users into revealing sensitive information, Deploy malware and ransomware and Establish backdoors for future attacks.

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

Domains

microsoftrefer.com

mkn.ngndc.com

microsoftdnshelp.com

spa.ngndc.com

update.microsoftdirect.org

video.solarwindsweb.com

cent.teamviews.top

check.pcanywhere.top

update.networkdcm.com

router.dnserver.life

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

1. **CMTX-P072024305: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

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

IPs

118.194.250.137

38.60.212.8

64.31.63.110

158.247.243.113

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

1. **CMTX-I-022072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware :

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

nia.gov.in.incidentsreports.in

\*.incidentsreports.in

igboat.com

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

Kindly take the required actions (for both parent and sub-domains).

1. **CMTX-I-053072024: Mythic Malware - APT36 campaign**

Following is the C&C of Mythic Malware. This RAT is being used by the Pakistan based APT36 group to target Linux based systems (particularly BOSS OS) in government offices.

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

164.90.171.42

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

Kindly take the required actions.

1. **CMTX-I-0445072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware :

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

wsc.cdr.bsnlco.in

cdr.bsnlco.in

hostmaster.bsnlco.in

eoffice.erp.bsnlco.in

welcome1.bsnlfi.bsnlco.in

email.bsnlgov.com

\*.bsnlgov.com

\*.bsnlco.in

\*.bsnl.shop

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

Kindly take the required actions (for both parent and sub-domains).

1. **CMTX-P072024766: QuasarRAT Malware ALERT 57**

ALERT BRIEF:

Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has 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.

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

IP ADDRESSES

181.162.166.209

181.162.181.30

194.26.192.177

91.160.181.237

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

1. **CMTX-P072024018: Redline malware**

Malware Alert Brief:

Redline malware is a recent malware written in C# with notable growth in 2021. It includes modules of stealing credentials and collecting information from the infected machine and the capability to download remote files

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

IP

79.110.62.113

95.181.151.121

77.105.135.107

77.91.77.6

94.228.166.68

209.90.234.57

147.124.209.128

79.110.49.209

185.196.9.26

194.55.186.87

185.222.58.77

45.137.22.177

148.163.56.241

185.29.9.108

213.227.129.32

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

1. **CMTX-P072024028: RACCOON MALWARE**

ALERT BRIEF:

CERT-IN has been tracking prominent RATs/malware families. An uprise in activities associated with raccoon malware is reported. Raccoon is an info stealer malware available as a Malware as a Service. Raccoon malware has capability to check system settings, capture screenshots, collect basic information like OS version, IP and username and steal passwords and logins from a variety of browsers.

A list of Indicators of compromise is provided below for your action side.

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

IP

147.45.44.2

5.181.159.42

192.121.23.67

89.147.111.100

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

1. **CMTX-P072024015: PLUGX RAT ALERT 124**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

IP

172.111.233.26

52.197.158.117

154.19.164.242

95.179.132.24

118.193.78.44

154.19.164.179

103.107.105.213

38.89.72.38

83.229.127.159

154.19.161.234

103.107.105.205

15.235.133.1

52.195.175.82

38.54.105.221

23.94.133.94

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

1. **CMTX-P072024405: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

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

IPs

173.199.122.23

141.164.51.188

38.60.212.206

167.179.70.58

207.148.66.49

207.148.102.176

149.88.92.22

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

1. **CMTX-P072024045: IOCs Related to Chinese Threat Actor**

ALERT BRIEF:

CERT-In has identified a list of malicious domains that are being used by China based threat actors to conduct phishing attacks, distribute malware, and facilitate command and control (C2) communications. These domains may be used to trick users into revealing sensitive information, deploy malware and ransomware and establish backdoors for future attacks.

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

Domains (PDNS IP)

tigmarket.casacam.net (64.176.59.90)

update.mcrcsoft.com (8.218.234.216)

looking.dnssupportservers.com (104.233.161.173)

domains.dnssupportservers.com ( 104.233.161.173)

support.firewallsupportservers.com (104.233.161.173,104.233.173.53)

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

1. **CMTX-I-022072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware :

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

nia.gov.in.incidentsreports.info

\*.incidentsreports.info

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

Kindly take the required actions (for both parent and sub-domains).

1. **CMTX-I-0449072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware/spear-phishing website :

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

news.infoalert.net

alerts.infoalert.net

webmail.infoalert.net

info.infoalert.net

nia.gov.in.casesreported.cc

\*.casesreported.cc

\*.infoalert.net

pcdaw.cloud

pcdaw.top

pcdaw.world

pcdaw.cloud

pcdaw.xyz

pcdaw.shop

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

1. **CMTX-I-587072024: IOCs of Poseidon Stealer Targeting MacOS**

The following IOCs are associated with Poseidon malware (stealer) targeting MacOS.

- ----------------<IOCs>----------------

186.2.171.54

186.2.171.60

37.27.82.196

68.66.226.80

79.137.192.4

agov-access.com

agov-access.net

agov-ch.com

agov-ch.net

arc-download.com

arcthost.org

b2cidp-mobilier.com

eportal-be.com

eportal-bs.com

register-agov.com

register-agov.net

zestyahhdog.com

- ----------------</IOCs>---------------

1. **CMTX-I-007072024: Mythic Malware - Cumulative IOCs**

Following are the C&Cs of Mythic Malware. This RAT is being used by the Pakistan based APT36 group to target Linux based systems (particularly BOSS OS) in government offices.

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

107.172.78.188

107.174.121.75

109.123.231.134

109.248.6.225

119.76.173.60

129.226.154.137

137.184.39.229

138.197.156.131

139.59.109.136

142.93.74.10

143.110.176.131

144.202.12.174

144.86.159.57

145.131.8.169

149.104.26.229

152.42.198.168

152.42.245.111

154.38.167.90

158.247.250.154

159.223.0.196

160.238.36.36

162.251.95.44

172.104.153.104

172.105.27.15

172.174.105.127

178.128.92.166

185.158.94.217

185.16.43.59

193.201.126.69

194.163.168.80

217.12.200.158

217.79.255.137

34.95.22.12

37.187.118.185

37.27.92.9

38.242.198.230

43.134.38.211

43.135.3.17

45.133.238.221

45.14.66.194

45.156.24.8

45.95.174.253

45.95.174.39

46.8.237.108

46.8.237.247

47.109.51.223

51.15.227.211

51.254.53.14

52.183.57.173

54.173.147.137

61.14.210.209

64.227.142.233

64.23.149.255

64.23.155.109

66.70.202.83

82.65.203.196

84.21.171.55

86.38.247.225

91.107.207.2

93.127.197.83

94.198.216.204

95.111.236.195

95.164.19.54

95.164.22.13

cloudserve.store

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

1. **CMTX-P072024055: APT-40 THREAT ACTOR GROUP**

ALERT BRIEF:

ALIASES- Double Dragon and Kryptonite Panda

According to the reports, a China linked threat actor group APT-40 is active in the cyber threat landscape which primarily targets using web shells and phishing campaigns. It uses open source tools like Cobalt Strike Beacon, Powershell Empire, Meterpreter, and Mimikatz.Some other custom tools like AIRBREAK, DADBOD, DADJOKE, and BADFLICK are also used by the group.This group has exploited newly disclosed vulnerabilities, including zero-day vulnerabilities, such as Log4J (CVE-2021-44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) and Microsoft Exchange (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473). As a part of the phishing campaign, APT40 has been linked to intrusion waves delivering the ScanBox reconnaissance framework.

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

HASHES

26a5a7e71a601be991073c78d513dee3

87c88f06a7464db2534bc78ec2b915de

6a9bc68c9bc5cefaf1880ae6ffb1d0ca

64454645a9a21510226ab29e01e76d39

e2175f91ce3da2e8d46b0639e941e13f

9f89f069466b8b5c9bf25c9374a4daf8

187d6f2ed2c80f805461d9119a5878ac

ed7178cec90ed21644e669378b3a97ec

5bf7560d0a638e34035f85cd3788e258

e02be0dc614523ddd7a28c9e9d500cff

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

1. **CMTX-P0720240408: Eldorado RANSOMWARE**

ALERT BRIEF:

A new ransomware variant named as Eldorado is active in the cyber threat landscape, written in Go programming language which provides cross-platform capabilities. Eldorado encrypts the files on both Linux and Windows machines and operates as ransomware-as-a-service (RaaS). Eldorado uses the ChaCha20 algorithm for file encryption. Eldorado also has the ability to encrypt network shares and delete shadow volume copies on compromised Windows machines to prevent recovery.

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

Hashes:

1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b

7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd

cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7

b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de

dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33

8badf1274da7c2bd1416e2ff8c384348fc42e7d1600bf826c9ad695fb5192c74

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P072024505: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

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

IPs

38.60.193.190

173.199.122.23

158.247.243.113

38.54.32.181

103.85.25.166

185.76.78.78

103.51.110.5

38.60.212.8

103.56.19.182

38.54.110.69

103.46.225.24

38.54.32.181

158.247.232.103

158.247.194.252

64.176.53.99

64.176.48.152

45.61.60.86

154.90.58.189

158.247.232.103

152.32.155.25

45.133.238.183

158.247.232.103

154.211.4.62

45.133.238.183

139.180.193.182

139.180.193.182

103.51.110.5

45.76.165.217

141.164.62.87

118.194.250.137

134.122.189.32

118.194.251.224

64.31.63.110

8.218.214.23

45.135.118.227

8.218.214.23

103.96.131.215

8.218.214.23

103.46.225.24

103.43.19.239

38.54.96.34

38.54.84.31

70.34.212.229

103.56.19.183

38.60.193.190

173.199.122.23

158.247.243.113

103.85.25.166

185.76.78.78

38.60.212.8

103.56.19.182

64.176.53.99

45.61.60.86

154.90.58.189

152.32.155.25

154.211.4.62

139.180.193.182

139.180.193.182

45.76.165.217

118.194.250.137

134.122.189.32

118.194.251.224

64.31.63.110

103.96.131.215

103.43.19.239

38.54.96.34

38.54.84.31

70.34.212.229

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

1. **CMTX-P072024065: SNEAKY CHEF THREAT ACTOR**

ALERT BRIEF:

A new Chinese threat actor tracked as "SneakyChef" known for using the SugarGh0st RAT is targeting government agencies, research institutions, and organizations worldwide. It uses two methods for initial access ie, LNK-based infection chain (the attached RAR archive contains a shortcut file (LNK) and a hidden folder) and HTA-based infection chain (the attached RAR archive contains an HTML application).It lures to trick victims to open infected attachments and spreads malware called "SugarGh0st" and "SpiceRAT via SFX RAR files and using a legitimate executable named “RunHelp.exe” to sideload a malicious DLL loader.

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

HASHES

dde3e5dca9e0498db558dd8e83f27143ad86cd0fcca1a33964ee4f3100682db8

0374a9812c7e43db1bde605cc3decff3d77c8b041b959a5422e4da0b60e0f6dc

427b6dc489cbfad36413fce6f71e82e158a6632c9986c1dee1af7676a129f048

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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.

• 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.

1. **CMTX-I-520072024: Malicious Domain**

Following malicious domain is a spear-phishing domain resembling the legitimate domain - email.gov.in:

- -------<Malicious Domain>--------

email-govs.online

- -------</Malicious Domain>-------

Kindly take the required actions.

1. **CMTX-P-3610720249: Amadey Malware Alert**

Malware Alert Brief:

Amadey is a simple Trojan bot. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware.

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

5.42.64.33

188.40.122.96

78.46.242.112

62.182.156.153

207.154.243.184

79.137.203.19

62.204.41.89

185.196.10.188

172.235.7.46

89.23.103.42

5.42.65.80

79.137.203.59

58.151.148.90

134.0.116.60

201.119.80.250

201.191.99.134

187.212.179.222

200.63.106.141

148.230.249.9

183.100.39.16

211.119.84.112

190.147.2.86

138.201.203.107

185.215.113.204

62.204.41.252

211.168.53.110

175.119.10.231

46.100.50.5

119.204.11.2

213.172.74.157

34.77.75.99

193.233.20.14

31.41.244.158

187.212.189.36

211.202.224.10

154.144.253.197

123.140.161.243

188.40.187.155

216.10.241.193

218.152.239.123

116.58.10.60

131.255.215.165

5.42.64.44

109.121.204.14

187.152.16.32

189.156.142.25

201.103.72.200

187.225.250.47

93.123.39.97

189.61.54.32

186.182.55.44

211.119.84.111

201.184.36.53

211.181.24.133

211.40.39.251

211.181.24.132

189.233.87.39

41.248.131.169

196.189.156.245

211.171.233.129

185.153.197.14

210.182.29.70

148.101.154.174

211.171.233.126

190.220.21.28

189.163.62.83

187.152.16.20

189.181.17.240

185.215.113.35

185.18.245.58

187.212.202.48

139.162.59.22

201.103.29.42

123.213.233.131

187.211.22.3

95.86.30.3

190.28.110.209

185.215.113.14

201.233.78.169

181.128.122.163

91.189.114.21

187.152.17.215

181.204.98.226

185.215.113.9

220.125.3.190

60.246.120.127

190.145.136.42

189.195.132.134

193.233.20.36

181.80.7.220

91.195.240.123

190.92.174.37

189.171.99.107

185.215.113.15

103.91.187.97

125.7.253.10

189.232.122.29

177.129.90.106

93.118.137.82

190.156.239.49

202.89.233.101

185.172.128.19

45.113.122.63

93.103.167.123

152.231.127.144

189.189.237.188

217.219.131.81

176.45.6.236

123.212.43.225

181.52.122.51

190.147.128.172

34.88.137.133

5.42.66.0

103.21.59.149

103.21.59.80

111.118.215.242

187.134.49.9

34.141.179.97

181.129.118.140

195.85.218.100

130.204.29.121

192.143.194.137

78.89.199.216

102.189.56.158

201.119.127.82

151.233.51.166

187.212.236.44

188.237.2.116

179.152.58.121

200.122.37.247

187.204.69.21

187.199.128.51

190.13.174.94

177.222.41.236

212.112.110.243

175.145.157.179

111.90.144.246

23.251.131.105

2.185.214.11

187.134.57.210

77.29.44.244

220.82.134.210

189.146.249.153

187.211.171.94

189.163.124.171

189.181.34.217

89.249.221.146

109.121.206.13

186.112.15.126

102.187.251.219

3.126.205.164

164.100.190.66

216.10.241.95

176.29.154.25

201.119.90.100

190.218.158.53

109.98.58.98

190.98.23.157

188.49.167.201

181.123.219.23

62.150.232.50

89.135.141.31

187.134.43.24

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P-5210720249: Agent Tesla Malware Alert**

Malware Alert Brief:

Agent Tesla usually spreads through phishing. However, the malware has a function which allows it to run automatically from a USB stick. At present, Agent Tesla is able to operate exclusively on Windows machines.

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

203.175.9.22

203.161.184.34

45.252.248.26

89.39.83.184

46.20.7.175

213.189.52.181

188.127.239.250

93.89.225.40

5.2.84.236

104.247.165.99

188.241.183.45

61.19.247.49

86.96.202.167

45.134.160.220

185.146.87.128

176.126.200.8

89.45.67.2

188.40.116.241

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

1. **CMTX-P-9710720249: Emotet Malware Alert**

Malware Alert Brief:

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

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

51.89.36.180

49.205.182.134

51.38.124.206

115.79.195.246

130.0.132.242

195.251.213.56

161.0.153.60

83.110.222.32

51.75.33.127

51.159.23.217

81.213.175.132

159.65.6.6

59.93.12.150

5.196.108.185

61.76.222.210

202.79.24.136

173.212.214.235

77.74.78.80

119.59.116.21

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

1. **CMTX-P072024075: CRITICAL VULNERABILITIES IN OPENSSH**

ALERT BRIEF:

CVE-2024-6409

CVSS-7

Impacted Versions:

Red Hat Enterprise Linux 9 (versions 8.7p1 and 8.8p1)

CVE-2024-6387

CVSS-8.1

A Signal Handler Race Condition vulnerability tracked as CVE-2024-6409 exists in OpenSSH mainly impacting Red Hat Enterprise Linux 9.Exploitation of this vulnerability could allow attackers to gain unauthorized access to systems, execute malicious commands, exfiltrate sensitive data, or launch further attacks within the network. The race condition and RCE potential are triggered in the privsep child process, which runs with reduced privileges compared to the parent server process.

The race condition vulnerability CVE-2024-6387 (codenamed regreSSHion) affects OpenSSH server component. When succesfully exploited, it allows an attacker to execute arbitrary code with the highest privileges on Linux systems that rely on the GNU C Library (glibc), subvert security mechanisms, data theft, and even maintain persistent access

Recommendations:

\* As the vulnerabilities have their potential for exploitation by threat actors targeting OpenSSH , therefore it is crucial to prioritize patching these vulnerabilities promptly to mitigate the risk of potential cyberattacks on company's assets.

1. **CMTX-P-8440720249: Qbot Malware Alert**

Malware Alert Brief:

Qbot (also known as QakBot) is a common trojan malware designed to steal passwords. Over time this malware has evolved from simple infostealer malware to an infostealer with a backdoor functionality. Qbot is primarily used by financially motivated actors.

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

5.61.49.13

185.53.178.52

178.22.83.226

3.64.163.50

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

1. **CMTX-P-8450720249: Raccoon Malware Alert**

Malware Alert Brief:

Raccoon Stealer is one of the most well-known and widely used information-stealing malware families. The malware steals data from applications, including login credentials, credit card information, browsing history, cookies, and cryptocurrency wallet accounts.

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

193.142.147.59

146.19.173.87

77.91.77.137

77.91.77.96

185.244.48.191

77.91.77.116

77.91.77.54

94.142.138.49

45.67.231.10

178.20.41.15

94.142.138.108

88.119.161.19

94.228.166.19

94.228.166.22

5.42.64.7

91.103.252.65

94.142.138.228

94.103.88.64

62.113.119.179

188.119.112.93

94.142.138.162

193.233.132.15

62.113.112.27

94.103.84.253

65.109.175.35

77.91.78.50

88.119.161.188

77.232.39.101

83.217.11.10

147.45.44.2

45.8.144.53

188.215.229.203

45.153.241.131

79.137.197.160

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

1. **CMTX-P-4660720249: SocGholish Malware Alert**

Malware Alert Brief:

SocGholish 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.

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

91.92.249.11

178.128.102.212

185.216.114.10

93.190.41.79

103.249.111.96

5.101.115.147

35.215.148.34

213.186.33.16

114.119.141.42

101.91.134.204

223.109.255.151

195.201.194.151

103.82.240.139

47.128.32.133

49.0.203.114

51.222.253.1

51.222.253.3

51.222.253.4

51.222.253.6

51.222.253.14

51.222.253.19

190.92.215.177

86.98.154.198

217.160.0.215

195.24.68.25

159.138.97.11

157.66.54.6

178.128.219.34

92.205.49.95

148.113.1.51

5.255.231.12

92.53.96.139

77.245.56.14

61.0.15.110

154.118.228.210

183.82.123.94

114.119.159.87

114.119.146.195

114.119.152.128

51.222.253.5

114.119.153.172

92.204.68.47

117.161.174.247

190.92.211.113

51.222.253.2

31.220.15.143

77.75.76.165

185.231.154.128

101.44.160.121

51.222.253.11

51.222.253.7

49.0.204.165

124.243.139.76

110.238.110.188

119.13.104.114

190.92.202.87

117.182.208.253

121.237.36.27

162.158.114.241

171.22.249.9

171.22.249.101

171.22.249.221

194.116.249.203

194.116.249.206

194.116.250.21

82.197.71.20

91.223.126.235

49.204.23.35

110.227.110.117

182.156.18.179

84.33.236.97

84.33.236.205

23.109.225.97

185.211.158.160

193.233.88.38

43.163.3.58

94.74.94.111

111.119.200.110

111.119.217.148

114.119.191.215

119.8.162.74

119.13.101.219

124.243.134.234

159.138.96.251

159.138.123.64

190.92.208.108

190.92.212.63

31.223.188.65

31.223.188.128

128.199.167.175

192.46.231.103

110.238.104.205

141.101.68.106

51.222.253.10

114.119.172.73

111.119.214.206

51.222.253.15

190.92.214.171

141.101.68.107

124.243.136.24

190.92.216.77

190.92.221.220

159.138.110.8

159.138.96.146

124.243.136.43

49.0.204.2

159.138.108.179

190.92.214.209

190.92.208.153

135.181.213.220

83.99.151.65

111.7.96.161

118.123.105.93

222.219.134.71

82.197.71.16

82.197.71.21

83.99.151.64

83.99.151.66

83.99.151.67

83.99.151.68

83.99.151.69

83.99.151.70

83.99.151.71

107.189.3.11

172.71.98.69

49.0.200.245

49.0.204.134

101.44.160.241

101.44.163.107

119.8.163.201

119.13.102.240

124.243.135.186

124.243.148.74

124.243.148.82

190.92.218.118

114.119.146.19

51.222.253.9

51.222.253.13

124.243.135.107

51.222.253.17

124.243.135.66

34.79.230.17

119.8.169.196

119.8.175.217

119.13.103.45

124.243.144.80

162.158.107.71

190.92.208.1

190.92.208.245

114.119.138.59

91.142.73.116

195.2.67.184

51.222.253.20

119.8.186.126

94.74.81.63

190.92.210.227

5.188.62.140

119.8.189.12

172.71.98.68

101.44.161.177

190.92.205.226

94.74.91.67

124.243.144.175

124.243.151.1

124.243.135.236

159.138.98.152

119.8.162.110

124.243.134.232

110.238.106.18

119.13.100.156

119.13.110.84

139.162.60.246

188.212.124.233

172.69.155.45

84.54.44.204

93.170.204.28

195.2.74.148

8.219.166.38

94.74.80.161

94.74.90.22

94.74.90.143

110.238.105.3

114.119.183.4

119.8.163.102

119.13.102.22

119.13.107.143

124.243.132.70

166.108.232.146

190.92.205.164

190.92.206.187

51.222.253.8

51.222.253.16

51.222.253.18

185.187.241.36

190.92.213.192

167.235.231.110

101.44.160.236

111.119.205.23

159.138.98.180

124.243.150.200

190.92.210.9

114.119.132.114

110.238.111.141

117.161.89.218

101.44.160.97

101.44.162.117

101.44.160.20

101.44.161.93

119.8.164.26

159.138.103.36

190.92.213.10

94.74.86.81

114.119.174.174

114.119.191.138

114.119.173.19

190.92.209.184

124.243.134.156

159.138.108.228

190.92.213.201

117.132.188.206

36.182.48.65

154.86.18.70

223.244.35.77

103.186.99.142

107.189.12.210

37.1.218.194

46.8.157.151

62.113.113.162

94.103.90.150

95.142.47.113

178.20.43.173

178.20.45.128

178.20.45.159

178.20.47.39

185.231.155.169

195.2.71.225

195.2.78.191

195.2.79.165

195.2.84.198

43.163.8.148

49.0.203.31

51.222.253.12

101.44.163.57

110.238.109.14

110.238.109.61

110.238.111.42

111.119.210.65

119.8.182.174

119.13.100.168

119.13.101.51

119.13.103.190

124.243.132.203

124.243.134.205

124.243.136.110

124.243.149.14

159.138.107.151

159.138.123.134

93.158.90.32

83.97.73.245

101.44.160.41

94.74.86.10

159.138.122.45

124.243.136.12

94.74.92.178

159.138.105.133

124.243.136.249

159.138.121.61

178.150.14.250

34.79.246.102

154.54.249.195

217.113.194.32

217.113.194.33

217.113.194.34

217.113.194.35

217.113.194.36

217.113.194.37

217.113.194.38

217.113.194.39

217.113.194.40

217.113.194.41

217.113.194.42

217.113.194.43

217.113.194.44

217.113.194.45

217.113.194.46

217.113.194.47

145.220.91.19

81.22.58.168

84.54.44.19

13.251.83.12

43.163.1.85

114.119.131.182

114.119.188.66

159.138.88.36

190.92.201.109

190.92.216.141

206.189.88.174

145.239.23.7

119.13.100.165

49.0.207.93

94.74.80.56

62.122.184.194

81.4.122.193

34.22.148.59

36.182.49.7

103.231.84.214

172.68.225.246

183.234.187.219

162.158.22.63

172.68.224.134

164.52.25.202

49.0.204.178

94.74.86.40

94.74.90.154

114.119.130.213

124.243.150.219

190.92.213.44

86.48.11.54

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

1. **CMTX-P-2370720249: Redline Malware Alert**

Malware Alert Brief:

Redline malware is a recent malware written in C# with notable growth in 2021. It includes modules of stealing credentials and collecting information from the infected machine and the capability to download remote files

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

94.156.67.67

185.215.113.67

89.23.100.222

5.42.65.92

185.196.9.26

94.228.166.68

147.45.78.229

185.172.128.33

85.28.47.7

4.184.236.127

135.181.121.224

185.237.165.67

77.91.77.6

31.177.108.40

213.142.159.9

38.180.147.152

147.45.44.16

91.92.242.175

91.92.241.104

65.108.27.131

5.189.138.247

91.92.249.24

4.185.27.237

157.90.5.250

91.92.255.143

45.140.147.183

95.216.104.115

147.45.44.97

147.45.47.93

212.86.114.67

91.92.249.167

91.199.154.172

95.164.89.184

5.42.65.63

94.232.249.14

185.237.165.180

194.26.232.43

43.155.163.53

20.197.224.66

89.23.99.151

4.185.56.82

77.105.135.107

91.92.253.215

77.105.164.59

79.110.62.16

94.232.249.204

147.45.44.12

185.146.173.237

147.45.44.112

95.217.124.248

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

1. **CMTX-P-5940720249: Trickbot Malware Alert**

Malware Alert Brief:

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

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

41.77.134.250

175.184.232.234

27.109.116.144

103.9.188.78

96.9.77.142

103.201.142.30

177.190.76.82

196.41.57.46

203.192.253.24

188.68.103.150

123.231.180.130

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

1. **CMTX-P-2500720249: Ursnif Malware Alert**

Malware Alert Brief:

Ursnif (also known as Gozi) is identified as a Banking Trojan, but its variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.

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

87.106.18.141

51.178.140.154

159.65.6.6

13.251.16.150

18.141.10.107

185.110.92.41

18.143.155.63

185.95.74.36

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

1. **CMTX-I-389072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware/spear-phishing website :

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

\*.chatgpt-gov.info

\*.mea-gov.info

\*.homeaffairs-gov.info

\*.checkgov.info

\*.secured-mygov.info

\*.ugov.info

email.checkgov.info

mail.homeaffairs-gov.info

ftp.homeaffairs-gov.info

webdisk.homeaffairs-gov.info

webmail.homeaffairs-gov.info

login-microsoftonline.ugov.info

webdisk.ugov.info

webmail.ugov.info

pay.chatgpt-gov.info

mail.mea-gov.info

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

1. **CMTX-I-993072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware/spear-phishing website :

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

\*.app-mygov.info

\*.confidentialreports.info

\*.dashboard-mygov.info

\*.delhipolice-gov.info

\*.ecb-gov.info

\*.moegov.info

\*.mohfw-gov.info

\*.mp-gov.info

\*.myservicegov.info

\*.npcigov.info

\*.parichay.online

\*.parivahan-gov.info

\*.serviceonline-mygov.info

echallan.parivahan-gov.info

echalllan.parivahan-gov.info

email.delhipolice-gov.info

email.gov.in.parichay.online

email.moegov.info

email.parichay.online

gov.in.parichay.online

in.parichay.online

lyncdiscover.moegov.info

mail.parivahan-gov.info

mea.gov.in.confidentialreports.info

msoid.moegov.info

pay.moegov.info

sip.moegov.info

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

1. **CMTX-I-995072024: Malicious Domains used by Pakistan based Threat Actors**

Following malicious domains are being used by Pakistan based threat actors to host malicious code/malware/spear-phishing website :

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

\*.maildrive.email

email.gov.in.file.maildrive.email

email.gov.in.maildrive.email

mail.gov.in.sites.default.files.attachment.maildrive.email

mail.gov.in.sites.default.files.attachment.pdf.maildrive.email

mail.maildrive.email

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

Kindly take the required actions (for both parent and sub-domains).

1. **CMTX-P072024095: MYTHIC MALWARE**

ALERT BRIEF:

Mythic is a command-and-control (C2) framework used by threat actors for various malicious activities. The agents can perform tasks like executing commands, downloading files, and interacting with the user through an interactive shell. Mythic supports multiple communication profiles, including JSON and P2P connections. The framework is highly customizable and provides flexibility in designing and leveraging agents within the system. Recent updates to Mythic include features like interactive tasking, push C2 capabilities, dynamic file browsing, and database migrations.

A list of Indicators of compromise is provided below for your action side.

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

IPs

13.48.128.36

13.60.75.58

142.93.74.101

16.171.113.251

164.90.230.221

18.176.67.169

37.27.92.91

43.135.3.171

45.156.24.81

47.245.14.36

91.107.207.21

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

1. **CMTX-P072024105: RipperSec Hacktivist Group**

ALERT BRIEF:

RipperSec, a Malaysian hacktivist group supporting Palestine, has been actively operating in the cyber landscape. They are known for conducting DDoS attacks and leaking data. Their Telegram channel serves as a platform where they not only carry out their own attacks but also share and endorse attacks and leaks from other groups. The attacker utilized MedusaL4 to carry out Layer 4 DDoS attacks, leveraging both UDP and TCP protocols. In the past, the attacker employed MegaMedusa, a nodejs-based DDoS tool available on GitHub, known for its ability to bypass numerous security measures, including captchas.

Mitigation measures against Website Defacement:

• Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic. Enforce MFA for all users and on all VPN connections and regularly review, validate, or remove privileged accounts.

• Use the latest and updated versions of web server / applications server applications, Apply appropriate updates/patches on the OS and Application software as and when available. Always apply the patch from the official channel.

• Strict enforcement policies on popular Content Management systems (CMS) such as regular patching of CMS applications and its plug-ins such as file mangers, disabling of unused plugins, 2- Factor authentication, adequate ACLs, File type & size Upload limit etc.

• Periodically check the web server directories for any malicious/unknown web shell files, remove it as and when noticed. If found/ observed any such malicious activity, report the incident to CERT-In Incident Response Help Desk immediately. (Email: incident@cert-in.org.in)

• Enforce strict control and monitoring of Windows Native applications such as command-line, PowerShell, WinRM, Windows Management Instrumentation (WMI), and Distributed Component Object Model (DCOM).

• Enable and maintain logs of different devices and servers [Webserver Access/Error logs, Application/DB/ Firewall/IDS/FTP logs] and maintain the same for all the levels. Preserving of these logs help in analyzing the incidents and known the TTP of actors.

• Use firewalls to create a buffer zone between the Internet (and other un-trusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorized protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Employ effective processes for managing changes to avoid workarounds.

• Check for unnecessary connectivity towards Content Delivery Networks, as malware are known to tunnel the connection towards these domains to hide their traffic and towards DDNS / free top level domains. Regular auditing of the failed connection attempts from DNS logs, proxy logs and to successful connection towards unknown domains. Some of the attacks use unconventional usage of DNS queries to exfiltrate interact with the attackers [DNS TXT Records].

• Conduct complete security audit of web application, web server, and database server periodically and after every major configuration change and plug vulnerabilities found. Services of CERT-In empanelled auditors may be availed. (Refer Cyber security Assurance section on website of CERT-In https://www.cert-in.org.in/).

Measures for prevention of Denial of Service (DoS/DDoS) attacks:

1. Measures for detection of attacks

• Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

• Enable adequate logging mechanisms at perimeter level, server, and system level and review the logs at frequent intervals.

• Continuously monitor the network activities & server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.

• Preserve all logs indicating type of attack and attack sources.

2. Protection measures against Distributed Denial-of-Service (DDoS)

• Thoroughly scan the network and online applications and plug any existing vulnerability in the network devices, Operating Systems, Server software and application software and apply latest patches/updates as applicable.

• Consider using a third-party DDoS protection service that can help detect and mitigate attacks, often using a combination of automated and manual techniques

• Employ defence-in-depth strategies: emphasize multiple, overlapping and mutually supportive defensive systems to guard against single point failures in any specific technology and protection method

• Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common attack tools.

• Sudden surge in inbound traffic to any critical server or services, such as ICMP floods, UDP/TCP flood etc. could be due to Distributed Denial of Service (DDoS) attacks. If such attacks are observed, implement appropriate response measures in coordination with Internet Service Provider (ISP).

• Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services.

• To counter attacks on applications, check the integrity of critical application files periodically and in case of suspicion of attack restore applications and content from trusted backups.

• Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.

• In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

• Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.

• Use CAPTCHA challenges to verify that traffic is coming from real users rather than bots, preventing automated attacks

3. Protection Mechanisms against Hack-and-Leak

• Conduct regular vulnerability assessments to identify potential weaknesses in your systems and networks that could be exploited by hacktivists.

• Monitor social media channels for any threats or activity related to hacktivism.

• Implement secure configuration settings on systems and applications to make it more difficult for hacktivists to penetrate them.

• Encrypt sensitive data both in transit and at rest to protect against data interception and theft.

• Regularly backup important data to minimize the impact of a hack-and-leak attack.

• Limit the number of external-facing services to reduce the attack surface and make it more difficult for hacktivists to find vulnerabilities.

1. **CMTX-P072024115: Atomic Stealer (AMOS Variant)**

ALERT BRIEF:

Atomic macOS Stealer or “AMOS” is an information stealer which is again active in the cyber threat landscape primarily targeting macOS devices. The malware can be disseminated via a number of techniques, including as fake websites, malware downloads, malvertising campaigns, False meeting scheduling software or Google advertisements impersonating services like Slack etc. It can steal sensitive information such as credentials, browser data, cookies, cryptocurrency wallets, and keychain data. Over time, modifications to the malware have included payload encryption and hidden detection strings.

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

HASH

524e68bb9f2db1c40442c1920ed3923af6e34dad89d3a21a764bc72f46d58507

52a491e575dbf28cb09a8f8eca9c65106ef80f8a6b71025ab3f654a8ca7daab1

9c6277de5a37df2754202e715b0e75aa2d1019dd6d07c7fba872463bac060c27

72b8e3ed01160c4a04615288e363a8e7ae2f4520142d3635539cb6ded6862064

ff677c786e213dd10a19ce3dda7fa0a84906073d6257e07c8f10799ca4427916

375d82829498952f1ad26b008e28830d44d1c5e0816b0ddd98a01021fbe49b65

2ea505b7390b1d4049bfd7f65369c7b8cf3d73d8e78735a5a4aea08d1992f854

59e01f2574529ba39df389efd5f0125243c198ee5feddeddd6e2dabcb6ba4eda

1cd69417715dbc3678f1dbe48412feee1a0e180558025b7969f5895b4518b0c6

adc98a9c2d48bb07268492fba21b244df759a9b68b82566bc9e36c62787add8c

74936df9195dd93ba1f8d8b9400a86a54e330ee8f4bf0f81a1e09be45c0eace4

5f8f38b6b67e709201c43969e6e061224339506465e1bed77a2b69d6b5431984

c0fd75f58992f8db0177dd72f1c3fcbf54bef9efd13c320828d1c4ec3792886c

934e5fa89afbd0943bd30a4b738f260a793e358c23e910d3609335d6b5e7d746

dab7a26ee9fd6b0b894feb9d27bb153a4a972f7abaaa7f693a096fe1db810b6b

e3b38b38a40998dd92c01ae9a510f8cff547e1ac9195537358638c2d5c0f445d

95ac8da032abe33c904d111a85ec85e0218450d70f823f8665251fefd18a8e4f

4c5b0fc8031c4e562a7b031643b597b22d4303cd81863fa806e5b75a7dd0d245

c66870d05cb57e7da5bee78dbf06736e6eb835af12bb4dc41ff8c6f7095f33f6

5c8ed4af2767fe79362b446055cae131f529505a3762b58c56a3a95dbcdb0997

9205ca45db823c1cec33f3be5bb6f120283eaa00b9f3f55032f997015418131f

a4c0dec57ca53951d6a28c5115c20de6476418d83d7a5d0f1b3e966d3ed9c96e

d069b96a4f6406bf71b58f868233925f9be7f0bd80df1f8be79a519c2d305cac

52e68ae7a13e40d2104c710c61afe44f293db67c409a2e42d80630e2d1f3839c

1df8842e85450aa7500fcebad9f2fab15a8d57c8be373aff67235c8ce62012d5

884d1be850bedb9bae63425d4d9bc5282ea64b630b763a2210c9f365ebe297d0

1415c63e775f6386cb6d3c19fc648b3a4b1918e21963299e31d542c5ca1b4a3d

70e2ac8f964cb11deca86b66c1c5b4652903cd015555525079d623654a3e139a

dcaf94000914a308af3995b837f67883a43fa06f762d929c3e0a821559d41fd8

7a855163833c1929ade941810ac52d3d48d548f12d09cbb8455389966cecd067

6de66aacad3818ceaf43e7afd6d34866bd9aea16e2e3c01fda6c4ef00a7e1a75

63f0d760320ba9b1848ad15f3e8a353894e55bd94d496a633feb087afb829481

39c17a3d9e0c437da4aad1fc857a08f0e490100ddb38ba7b4174c7d498274dcb

c2abd5751623d3e10db08ac321468c34df17cda13d88a0fab0f0e6772f28d33d

8d3488dc7094d4ebcfb8b14c8a529962bcd59a3a6eefb4782cecaab030d40458

8b59ad82154a6adf6089f6677084b2a0901ea28121f6c41790bbdcd6a91f40bb

fdedf90596e979da02278048ff27c039f1248999fff97eca6c699f5b301aa1d3

44f28fa870a4446fa103f170c4f8f1e9e9eaf878a09d5d6dc2b449070517955e

e15d92f68e3b45c2a2a006fd50a1e7b2f282a34c45b99dc9c75d08142a8ae3b1

0da7db9e8e8fb663f8ce9669d3c84135e46ecc324c7e310f3890d2085ced4b09

4bed7470adb077ecbc026bf79873b938f3ae916f91b7438d5d21feeb0cfaedce

34e6c18727bc97b09dab9b102caa0645d1f8fe4bb60431dc17dbfd1a1385f653

7ec3df2c270cbeb8d5175380b43a95cfe058f1370e2eddb9b9ff6cafaff349e3

87f8a7e2dade5e254a963aebf08b761646dcb12edeee77c6daabfc4f66fa21e3

4b7dd47ffd935452ee800738d06018971f0a5de128f1112b32db46fd8b542106

04307810eecbd26d515347de67138d28eb77140cfb8c45f87fc995304119cf31

b2231e20286e6f0b857aed6c0c226e7d37b9d7535651f750016ff98401f11e39

0809b0cc7ee352c4018b328aa93dbd4ae8123171bbcf83c96d021051fee07cb2

12ad931b90652cfc309f50077571499c1057af579af6625f8ffa4bca19327c4b

dec0d31ad746792c26a12fb095da2af9ddcea164eb8cd65a64925d479f613b1a

b34ce45f69f88d3557078090ce5c9294beef21bb8545215e539248e71683dde0

f43cd92dd68caab186d0645842cac591575976f0b404ee808b4975734f303ff3

3d5b3f4e66f8719e2d5379b89bfe0e528d7f0bf17213ade885b3173a18c0bb4e

1c6d45ac85e5607c181a8f8d83b2a9860041efbad3b13d557bf30d362f451df6

02dec85bdc6fcd691e5f197320fe4cda6ff3fe047148d2cde11a2cb2f2280542

903ddbfbdab17ca5ac005dbc578ede2ac35bc8c486026faf380430756ba4cb81

578d81b595bc7afaeaf15c8b152e8be33e7b6b11bf6a9e4889c5c5330a3a8d12

413f10ff4bc2f67171d51b5c1b934be0cf8b8587545c07be1adbd09335c30dd3

71ff7475e88b1d891003d68335d453e0d9b6b5618e7a7f803b3b72b6c4d309ad

721968433143492ae06ff7cd1e1e13c7b2ca57973c6c7a66a3d49f072fff6d3a

6c367c35891ec6a313e004eab21f096b0a1148e269cff2d7ea1f4e57373e9658

2e9aedc0f329b6e97d77d4a74f960ff5f55f24aba8106d1ce4a391ae4719a68d

0484ca3a654971f2695d7e4a3e8c07e66aee517f8f18c825cf20b21a4ea058e2

9202a526a24cce9b7a6d868ada67b3f288d191c42afb88a0007a8dc88e91ea45

3005f36eac3a329dddc2d33df57e83facd8921973eb27b2638f0af5378c39eb4

d8252fffe5fbe840b7e7aa6384fb764640ed3a62644b0d88ebe285e45b3509d3

132eba1617430cc4bffc57a6b0ad40771f125f29899e2e22bfd2153afe094f49

f99fa0f825e4fdb914ea6c7ae5622c355d2aa1af4dfa7aeeb78bc4e3346e92d9

004e5668f93678e2e2daeb35a55918392a3c5c4393f6e4016ebecda253ae9a60

f9e7399894a01a1904999886246a1122d11bd6e078bc4aed97e3f863ef5b2ee0

f879827ec5ffcb9decb4d21e07b7c875ca7fe9d4512f5d893bcf743074c0fe35

f308ca3ebffcc2bece737c5da512001fcd29f5d858e99b8595d9258e4f5116b1

e7ea4e3001a48244b5855496bb15cf623aefe7d7d6ac6a62f5df24f738c47d41

a8600b0a19a02b1fd3139b229231d33b9547c35500128725f0d409257dbe78b9

2cd07af80537ad7017196dccf58c9a9ad777c27cc5e05f5250e9227f6a0ccc4a

00314201bc44e087192706bd68c5b8e99365d1bba5e3086853e868750b47e5a0

17f15559a365da31b3ab7f617215dda3157492331069af0e7179982dc40c6ffc

59d7014af0a3d3f8c95bcc8df57d66c76f65ce55e2f01f1b6625176ac883bee8

aa44da474a2b372cb912f9a65f8a0d5af028db361674f0d183a8eb5955a2f0e2

3c2468cb86f08520453bd7906b1411a45ce22bc22b0e94f635a250c366ba4d98

0a9d10c32082459685f58da4e9da4aca196a9f68a67b17b3def3050d422812f5

f5fa7b688df5c39c8dc9bd07e36c230abecbbbe42cfa55e3e61df8829ceb3500

4b8ccbb4fa8958a118aed3ab5082b10536aa856ec9f005b6d048f9d411e187c5

10ffae85efc9c293c9087990ce5332167983a43de0fd79d75b70edc831bb9ae8

12c4a4b4caa5784161d62e7ddd348a63c79c251f0430091592f39b5ddbf7278f

51b8c21e8ddee86a2a2f6dcce8836c54466c57ca077af18bb39a4bbb0826f674

7934eb7a9168371bd573e06d4908be74c5563c7b78084f56cec80a84f9c2ad33

5a614b017e44fd74ff484ef52dd945b044c5f31d08c54110a141aa74189b0d33

67c72d7760f0740a26dee5132e73c7d1bcbe0c511beee346dc8f952514160ba1

918a28abaee643d4cf21552925ba1e48bad78dae379cce2a15c6de2435d2f11b

63eba1135abf855c94c9683ae94e2aa44de0c42f642b94a633fbef77c4d7f59f

bb9d336d0829e27307496f2f4f274df19e691e9d3748caa9cc8b78cb807b2b7f

2626aaee671bf33490722bbe1e811f5cb4bbe5590520ae329411af07aa40d36a

ffe6d690409dea3d4c2013917aee663b91ecc2730cb31e0a40b802dbbcaec714

b2ee82ee7f1134bb707eb6d5391397203a9c345e4dc2910ea984b023eb9133d4

65f920ced707567ea9986f02f70227a25c9f19892b307d16c5dadd44dc70427d

1e02d68b2b3289d47599b80ec38163bd81ebaf1119b4f072b5887828e3836ec8

4af4db2396b4e133a84c27ccce3e7220f1da8042e8a5652c2a7e9fc5b9b41670

ad6b6c59b1137d5e74aeebc3ab1861cf6d182c494aeb0a1b7f36909b62324f8b

b336955a68bec8e0fe63039ea3ba05f88bda91c4cae156cd5b298742907940f8

1949678b50814d55fe32449524eb3bd31f8cf0ed7c950b2632f62fedfc84e7f7

56764f0289bb90cce43ea6a63d031482e9c9f9e9817a453f20da12997829d8c8

a8db9c7d50eb44e51672a67a8b266c634e55b167e1c703a3acc380d850015f35

a600d5229ac8f5672f33fb93ea8d5b2126e71a5186d874a93bb4d2dfc528a2e2

272bd0cd4c05dedc2caaf930dd292fbf55bbbd37c066648d194cd131882edb33

271d55c5f38a1963188dbf459200971dd8fd57a9a5677ecbd5a097c3e5664990

3267dea0a5db0a594741d8904439d6a697f52090e3929a511ec58747fdae9740

3f3aee19707b1796d0b0fbaf29f2d7b104c906dee434ccd3b55844a925002b1a

4df168341c64cbd6cbe79f991f395de75f15111ed9bd8d28c0ae059fd44a62bd

2762811f0da444436119db881b65e805bf2e0601c52368932c98df5e3f8feac3

e13aa64a3e1e9bba9a95178555d17696a065c282885db027c6083798ffbef19c

c7c566115c649725d0c4bdba7a1ac06b2f1147c37dbcebfaabbe44ceadb0e94f

0904841428f8a3191d9d8422f844e6bdb51376eee651feaa8ebbf89645c75fd4

c4a28a2f9eb7eda80bd7ba81d5b5f53940ef81567f35670403e345d1c103964a

090d137a45609a2eaae697ab5b6f8ad90dd8f718a39fe24ece1b0b9e011f03f7

ce1d6a4b13b1f4c98525b23b08779473675f934fd4548cd5c15e9bb7cccf0a9b

3445da3c67fc31f54a0fed15780e39a4ae232db7dd9889ae60ebb7334ca24aae

5514103105a97cdc85fdbf5d17204771d371f2fa95390c10de4a38597355de19

d7629e5a04234cdd18dd4160af076e9285e552ad58b587e9f27850294ff9dd82

e952e1b3ecaad6fb5fac0f27584545775b0925b1ca6d8fcc580eb39ad6fb057b

08fecfdb478d29462ead6eab2cdad9c7a0b3c4b3d773008b1fc3a7d6f9f6b7b9

89f32c810f6586d82f781b4d8c9aa216630763ff4db68142f97d896a329f8ca0

0114d2be7bd8173b00b33661d8c68f166fcf2947f2186390d8d1e147cffa1106

d7381ac17a73eebefccc23276dbba1f12355a72464e6ee5cf2c32f6e667066f1

02bdf1603201056f6d727ab50031045a9e4fe4adf3900df33155e03aeacbdd10

3e7bc744357dfe564348a43e06939be9f36e6de579862f692767b7961ea6d6e0

265be54ad654b87299d17e46c9ad457c2332f19bb7fd29987c43a929ef75eea2

9561fa879659e487cee5b53ce3cccc2b7679d454b9783e2a4eb1ee3e1aff9858

7e2c2e145c61d40d30b75ba5dc93a67c06454aab185d60aeec2e46f0f9ab5d8c

fb87cad7ea6b7ae5b9d98c5a68b8757af0e53a7356542913077df3a12f6ab1fc

2df5ca21b1dbad29e83588c2f92d1436a1cb0fb85ac81399bcd6ea06bca478c1

56b13d498cb1ff041ff17e2885f47f042202e4464152ae2e6bd4449ed063d005

c7abd3488396bfa516d92db302dfb4afe918227887d525bc7532b089a22fd9cb

90c74b20d1a4c694acbce85acabb6e5cf41fcbe44f572e4b3fb4bccbb143478c

cc3fb47817e1e51ccfd7aa285499cd68fef26432f644a8d41b274e83c8ba72d9

a2dcdaea9216f5ae20280ec9300b3960b50c0fb9ac0b43b1e8be489ea0652151

c14eabf47239a73c8717a6b4616fbb7747c30fe64052a9c9935379a7209034b9

209752dcad956a82a2e7eebc95b9c7d1cf30448b0bd4048dcfad750aeda1de71

222089b7d97c29653d8f20a75351b5da6c4da1db670f24cb803117c6259099dc

32a57ca62f25827d3b165da59f9916bbf29eb665646718ae1a8be65e21d68fef

beb58b9be08331538c7d1857d45a6fafebf692dd08d4a469bc7afef8e1573a50

f13047924d4d00284aeb4de68b8b0fc5a72f2e0338dae5e0a1fb24ebd0de7684

f24eb2f694de88d9dc6a36b64eeb641161a11942f19a6de29acf75ae098d6d53

de5338c884bdb173703d029bdb60d3172a4d80b3509b6a64251ba43580f01d50

4bfb3c34ff74b6006d1240710c9f77317f5378a442c9b79043f956d606782064

5d064f87aac36c462aacd93f761793de322b4c8946b87806ef98af57a1b9d468

da444f479d4c730723cb59e02aac962a1b5fe39c9fda2428e66c59a6d9cd16ca

1d9685f44e396a92fd32c6be1d956a42e1943d112297e8634601f081a59301c5

75827477288e00ddc416bcbc3ff8c1b02a3e9cf6263838bb5a47b89d0ab36f19

6dae9ff692a17d57bf572f8ce61c9a2e00a21d33abe4d755099cfa65bef2a894

IPs

5.42.65.107

193.233.132.126

193.233.132.131

193.233.132.132

193.233.132.137

193.233.132.138

193.233.132.155

193.233.132.168

193.233.132.188

77.221.151.54

77.221.151.41

77.221.151.45

77.91.77.87

77.91.77.88

77.91.77.178

77.91.77.189

Several Mac software installers (DMGs) in the wild are dropping the malware variant. These are mentioned below:

appcoinmap.info\_Launcher\_v.3.68.dmg

Brew\_v.9.98.dmg

Brew\_v.2.87.dmg

Wasper.dmg

Launcher\_v.1.82.dmg

PartySetup.dmg

PartyLauncher.dmg

CrackInstall.dmg

SpectraLauncher.dmg

chrome.dmg

Tunnelblick\_4.0.1\_build\_9164.dmg

NightVerse.dmg

Arc.dmg

Tunnelblick\_4.0.1\_build\_1606.dmg

UMG.dmg

openvpn-connect\_6820\_signed.dmg

openvpn-connect\_1140\_signed.dmg

openvpn-connect\_8390\_signed.dmg

Calendly\_v.6.67.dmg

Figma\_v.6.60.dmg

Figma\_v.1.76.dmg

VorionSetup.dmg

DockerApp.dmg

UniAPT-Launcher.dmg

Apple\_App\_v1\_22.dmg

ArcSetup.dmg

TradingView\_mac.dmg

slack\_mac.dmg

Cozy World Launcher.dmg

Astration.dmg

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

1. **CMTX-P072024134: IOCs related to Chinese Threat Actor Campaign**

ALERT BRIEF:

A suspected Chinese state-sponsored activity using a custom backdoor [Shadowpad, PlugX] and the offensive security tool [Cobalt strike] is being observed. The group utilizes living-off-the-land (LOLBin) techniques, relying on legitimate software[Windows Remote Management (WinRM) for lateral movement] and operating system components to gain and maintain long-term access to victim networks, minimizing the use of traditional malware and maintain persistence on compromised servers using tools such as China Chopper web shell.

T1053.005 (Scheduled Task)

T1059 (Command and Scripting Interpreter)

T1071.001 (Web Protocols)

T1105 (Ingress Tool Transfer)

T1203 (Exploitation for Client Execution)

T1480.001 (Environmental Keying)

T1547.009 (Shortcut Modification)

T1566.001 (Spear phishing Attachment)

A list of Indicators of compromise is provided below for your action side.

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

137.220.36.87

45.77.42.65

139.84.144.144

4.230.17.48

38.54.79.52

172.174.247.59

154.197.99.202

103.149.48.189

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

1. **CMTX-P072024555: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

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

IP

152.32.201.190

31.192.107.196

158.247.243.113

207.246.119.197

64.176.6.27

45.77.249.197

65.20.83.141

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

1. **CMTX-P072024055: PLUGX RAT ALERT 125**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

ip

27.102.129.217

45.80.215.169

156.59.39.99

103.46.185.52

23.248.176.6

154.31.218.222

172.111.233.36

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P072024125: Active Exploitation of a Critical Vulnerability (CVE-2024-4577) Affecting PHP**

ALERT BRIEF:

CVE-2024-4577

CVSS-9.8

A critical remote code execution vulnerability tracked as CVE-2024-6409, a PHP vulnerability that affects installations running CGI mode is being reported. It is also shared that numerous exploit attempts to abuse this vulnerability by threat actors using various malware families such as Gh0st RAT, RedTail cryptominers, XMRig, DDoS is observed. The vulnerability is caused by the way PHP and CGI handlers parse certain Unicode characters, which can enable an attacker to achieve remote code execution (RCE).

AFFECTED VERSION:

PHP (versions 8.1.\*, before 8.1.29, 8.2.\* before 8.2.20, and 8.3.\* before 8.3.8)

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

Gh0st RAT Malware

147.50.253.109

146.19.100.7

23.237.182.122

HASH

A646ebf85afa29ae1c77458c575b5e4b0b145d813db028435d33b522edccdc0e

RedTail Malware

185.172.128.93

HASH

2c602147c727621c5e98525466b8ea78832abe2c3de10f0b33ce9a4adea205eb

0d70a044732a77957eaaf28d9574d75da54ae430d8ad2e4049bd182e13967a6f

ab897157fdef11b267e986ef286fd44a699e3699a458d90994e020619653d2cd

9753df3ea4b9948c82310f64ff103685f78af85e3e08bb5f0d0d44047c63c315

19a06de9a8b66196fa6cc9e86824dee577e462cbeaf36d715c8fea5bcb08b54d

Muhstik malware

IP addresses

147.139.29.220

86.48.2.49

185.201.8.176

194.59.165.52

156.67.218.115

Domains

p.findmeatthe.top

p.deutschland-zahlung.eu

p.shadow-mods.net

HASH

9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572

1ae2fef05798f0f27e9de76fcef0217f282090fab1ba750623ca36b413151434

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

1. **CMTX-I-932072024: SideCopy - IOCs of Malware Campaign**

The following IOCs are associated with Pakistan based SideCopy malware campaign:

- ----------------------------------- <IOCs> --------------------------------

vocport.com

mazagondoc.com

http://vocport.com/Contactus

https://mazagondoc.com/images/AdobeArm.exe

api.ipify.org (non-malicious domain, but used to identify the

public IP address of the infected system)

- ---------------------------------- </IOCs> --------------------------------

1. **CMTX-P072024786: QuasarRAT Malware ALERT 58**

ALERT BRIEF:

Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has 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.

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

IP ADDRESSES

154.221.25.6

49.234.24.181

45.66.231.209

37.183.240.233

144.126.157.31

45.94.31.65

181.162.170.67

47.238.53.31

191.93.113.10

5.45.64.184

185.106.93.204

62.234.31.44

202.103.157.162

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

1. **CMTX-I-942072024: Malicious Domain Spoofing CERT-In's Domain**

The following malicious domains are registered possibly to spoof CERT-In's domain:

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

cert-in.co.in

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