**Cyber Security Advisories**

**Date: 31 July 2024**

1. **CMTX-I-946072024: APT36 campaign**

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

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

checkdailytips.servehttp.com

\*.servehttp.com

64.188.27.144

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

1. **CMTX-I-952072024: Malicious Domains used by APT Threat Actors**

Malicious Domains used by APT Threat Actors are as follows:

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

windowsupdatebg.s.llnwi.net

connectiiest.com

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

1. **CMTX-I-954072024: Suspicious Domain Spoofing CSC domain name**

The following domain is suspected to be spoofing CSC domain name:

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

cscgov.info

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

1. **CMTX-P072024796: Atlantida Stealer**

ALERT BRIEF:

The Atlantida stealer is an information stealer malware capable of stealing sensitive data from applications like Telegram, Steam, FileZilla, web browsers, and cryptocurrency-related sources.The malware utilizes Donut shellcode and RegAsm.exe for execution.

Recently APT group Void Banshee has been observed leveraging a remote code execution vulnerability (CVE-2024-38112) in Windows Microsoft HTML (MSHTML) platforms spread via spear-phishing emails disguised as PDFs, victims are redirected to compromised websites upon opening, where an HTML Application (HTA) file downloads the Atlantida stealer.

URL's

https://fullgasesspa.cl

http://cbmelipilla.cl

https://hostalaskapatagonia.com

http://h.com:8000

HASHES

c9f58d96ec809a75679ec3c7a61eaaf3adbbeb6613d667257517bdc41ecca9ae

d8824f643127c1d8f73028be01363fd77b2ecb050ebe8c17793633b9879d20eb

87480b151e465b73151220533c965f3a77046138f079ca3ceb961a7d5fee9a33

c85eedd51dced48b3764c2d5bdb8febefe4210a2d9611e0fb14ffc937b80e302

13907caae48ea741942bce60fa32087328475bd14f5a81a6d04d82286bd28b4d

119b0994bcf9c9494ce44f896b7ff4a489b62f31706be2cb6e4a9338b63cdfdb

6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750

b371fbdce6935039218d4b4272db3521881c9cec48ef82dec1e9e0188a32d3ad

IP ADDRESS

185.172.128.95

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

1. **CMTX-P0720240508: BugSleep Malware**

Malware Alert Brief:

Bugsleep (also known as JELLYBEAN) is a C-based backdoor deployed by MuddyWater APT actors. The malware spreads via phishing emails disguised as invitations to webinars or online courses. In one of the recent campaigns, Egnyte file-sharing platform was leveraged to spread the malware. Once executed on a victim's machine, BugSleep establishes persistence mechanisms and communicates with MuddyWater's command-and-control (C2) servers to execute commands and transfer files. It uses obfuscation techniques to avoid analysis and delay execution, making it harder to detect.

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

95.164.32.69

5.252.23.52

194.4.50.133

193.109.120.59

89.221.225.81

200.200.200.248

141.98.252.143

73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e

960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809

b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca

94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472

5df724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0

39da7cc7c627ea4c46f75bcec79e5669236e6b43657dcad099e1b9214527670e

c23f17b92b13464a570f737a86c0960d5106868aaa5eac2f2bac573c3314eb0f

fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a

7e6b04e17ae273700cef4dc08349af949dbd4d3418159d607529ae31285e18f7

ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909

e2810cca5d4b74e0fe04591743e67da483a053a8b06f3ef4a41bdabee9c48cf7

90f94d98386c179a1b98a1f082b0c7487b22403d8d5eb3db6828725d14392ded

20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c7f61a

55af6a90ac8863f27b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2

f925d929602c9bae0a879bb54b08f5f387d908d4766506c880c5d29986320cf9

424a9c85f97aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4

c80c8dd7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9

c88453178f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675c

31591fcf677a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38ab

a0968e820bbc5e099efd55143028b1997fd728d923c19af03a1ccec34ce73d9b

88788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3ee

4064e4bb9a4254948047858301f2b75e276a878321b0cc02710e1738b42548ca

e7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2

1c0947258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91

8fbd374d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1

7e14ca8cb7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601bee

02060a9ea0d0709e478e2fba6e9b71c1b7315356acc4f64e40802185c4f42f1c

53b4a4359757e7f4e83929fba459677e76340cbec7e2e1588bbf70a4df7b0e97

0ab2b0a2c46d14593fe900e7c9ce5370c9cfbf6927c8adb5812c797a25b7f955

\*.egnyte.com

smartcloudcompany.com

onlinemailerservices.com

smtpcloudapp.com

softwarehosts.com

Additional IOCs related to Muddywater Group:

91.235.234.202

85.239.61.97

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

1. **CMTX-I-956072024: APT36 - IOCs of Malware Campaign**

Following IOCs are associated with APT36 malware campaign.

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

suwaq.duckdns.org

currently resolving to

66.154.103.133

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

1. **CMTX-P072024816: QuasarRAT Malware ALERT 59**

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

HASHES

3f1b0ff74433ec2acedd93a5bfef8e0c

3e0963fc309a94f182a33037bef8e44b

32cb22b72a50f887805541c4afaa34a5

2652adcc83237b04102ca1d47908ff6c

a439e91d29611fb87be0cce22aa4d442

IP ADDRESS

103.136.199.131

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

1. **CMTX-P072024806: APT17 THREAT GROUP ACTIVITY**

ALERT BRIEF:

ALIASES- Aurora Panda, Axiom Group, BRONZE KEYSTONE, Deputy Dog, Group 27, Hidden Lynx, LEAD, Tailgator Team

According to the reports, a China linked threat group APT17 is active in the cyber threat landscape which is recently observed exploiting a variant of the Rat 9002 in diskless mode.

The latest attack chains entail the use of spear-phishing lures to trick recipients into clicking on a link and even the creation of the malicious MSI package was carried out with care as it involves the installation of the legitimate Skype for Business software and in parallel the diskless version of the RAT 9002. A modular trojan, 9002 RAT comes with features to monitor network traffic, capture screenshots, enumerate files, manage processes, and run additional commands received from a remote server to facilitate network discovery.

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

HASHES

28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e

e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c

d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436

c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c

caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5

de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0

DOMAINS

themicrosoftnow.com

meeting.equitaligaiustizia.it

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

1. **CMTX-P0720240608: Beavertail Malware**

Malware Alert Brief:

The Beavertail is an information stealer malware capable of stealing sensitive data from web browsers like Chrome, Brave, and Opera, login credentials, iCloud Keychain, and more. It specifically targets cryptocurrency wallets and credit card details. Attackers trick victims (pretend to be job recruiters and invite victims to a fake job interview or create a cloned version of a legitimate website to trick victims into downloading it ) into downloading a seemingly harmless file called "MiroTalk.dmg," which is actually the BeaverTail malware.

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

95.164.17.24

0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132

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

1. **CMTX-P072024826: QuasarRAT Malware ALERT 60**

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

186.169.32.111

152.136.159.133

70.50.220.24

45.76.105.79

128.90.113.26

103.252.137.65

121.62.23.208

181.162.177.17

216.238.101.182

185.93.69.59

45.159.249.181

143.92.49.122

185.208.158.117

31.220.101.25

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

1. **CMTX-P072024836: Oneshell tool**

ALERT BRIEF:

Oneshell is a tool designed to streamline the creation and deployment of cross-platform reverse shell payloads, with a focus on reducing tool requirements and dependencies in target environments. It provides the following capabilities:

- - Implements Mutual SSL to ensure encrypted communication between a command-and-control (C2) server and a target.

- - Simplifies the deployment of reverse shells by enabling operators to easily integrate the payload into exploit scripts.

- - Minimizes dependencies to ensure compatibility across diverse environments.

- - Verifies the integrity of downloaded binaries using Treyfer CBC-MAC cryptography, ensuring secure delivery of payloads.

- - Uses AES GCM encryption for securely downloading and decrypting additional stages of the payload, maintaining both confidentiality and authenticity.

1. **CMTX-P072024135: Qilin Ransomware**

ALERT BRIEF:

Alias: Agenda Ransomware

Qilin is a ransomware usually written in GO programming language. It shares code and TTPs with the Black Basta, BlackMatter, and REvil (Sodinokibi) ransomwares.  It employs a number of methods, such as double extortion, tactics, phishing and vulnerability-exploiting, to obtain access to systems. Once on a network, the ransomware is run using parameters for disabling security and propagating among networks in the command-line arguments. The malware has been seen to travel through virtual machine architecture and disable security tools by taking advantage of several weak drivers. The ransomware malware is deployed using Cobalt Strike and Remote Monitoring and Management (RMM) tools. AGENDA ransomware is offered through the Qilin ransomware service.

Mapping of Attack campaign on MITRE Matrix

T1071 (Application Layer Protocol)

T1106 (Native API)

TA0011 (Command and Control)

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

HASHES

0467280ef9f3dfdd8751fa333ae17d47

0d68a310f4265821900249bec89364c2

1219809aab61a8beeb1a97864f56db8f

1410b418a078559581725d14fa389cdd

1a5ee819449d01730b45f4f714e990c8

31edb01d243e8d989eb7e5aeeeef54dc

37155f0bca29ccd6b6d4f5b2bc42eb4d

470d0261d18ed69990ce94f05d940de1

649a85bc91b81317ba7029006af78b89

64ca549e78ad1bd3a4bd2834b0f81080

6b7eeb860917aa44982d8bd2d971aff1

908a7f5bcdd8b0bc8e1f6bd86f217222

923c5af6fd29158b757fb876979d250b

9365eb8987c5e2b8c1edee23c80b37d6

a42d36f1af2c396e645ffa356fa47a1e

a7ab0969bf6641cd0c7228ae95f6d217

d67303ba66bcb4dd89de87c83f3f831f

da6dada9aa8fb55bfafb1e9c84835710

eb6fff4ee0f03ae5191f11570ff221c5

ee6a9116b3aa59833a9a051d1530c171

efb14af246edf0baed0e0a2b00676d21

f6cf6f7882e162506eade5c67535ddca

fb07f0d63f46d4df02c265d8afb5ce4e

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

1. **CMTX-P072024145: TRINITY Ransomware**

ALERT BRIEF:

Trinity ransomware, a variant of the 2023Lock ransomware is new in the cyber threat landscape. It uses double extortion technique to encrypt files and exfiltrates data from the victim’s system. It employs the ChaCha20 encryption algorithm, which is known for its speed and security. The ransomware is found to have some similarities with Venus ransomware, probably sharing a common threat actor or a codebase. It encrypts files on a victim’s computer and appends the “.trinitylock” extension to them.

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

HASHES

36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4

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

1. **CMTX-I-875072024: SpyNote -  APT36 Campaign**

Following IOCs are associated with SpyNote malware by Pakistan based APT36 threat actors targeting Android devices:

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

147.124.197.160

147.124.197.166

147.124.197.187

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

Kindly take the required actions.

1. **CMTX-I-892072024: AsyncRAT - APT36 campaign**

Following IOC is associated with AsyncRAT malware by Pakistan based APT36 threat actors targeting government officials:

- ------------- <IOC> ------------

198.23.227.175

- ------------ </IOC> ------------

Kindly take the required actions.

1. **CMTX-P072024108: Prolific RAT**

ALERT BRIEF:

ProlificRAT is a remote access trojan being offered as Malware As a service in Underground forums claimed to target Windows, Linux and MAC users.

Using ProlificRAT’s web panel, hackers can create and customize implants for Windows and Linux device capable to upload files to the victim’s machine, execute commands, find other devices on the network, run programs on the victim’s machine, to create multiple desktops, switch between different desktop instances, and set the active desktop for operations on victim machine etc.

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

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

IPs:

82.153.138.143

82.153.138.144

172.93.150.44

172.93.150.43

82.153.138.142

172.93.150.46

82.153.138.145

172.93.150.45

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

1. **CMTX-P072024098: Lumma Stealer**

ALERT BRIEF:

Lumma is a C based information-stealing malware that targets Windows systems and is distributed through illegal cracks and keygens.

It is available as a Malware as a Service. The malware is usually spread through phishing emails, fake software updates, and compromised websites. Lumma has capabilities to collect sensitive information like usernames, passwords, cryptocurrency wallets, two-factor authentication extensions, and web browsers artifacts.

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

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

Hashes

c1ee309913c08e1147f42c75546f5789

ceecadd06e68f91ab1912edc4fb2c3c3

d881547121335440ca6f3d35735d7ad2

59852582254fea82f5a5af356efa44fa

03a839ea3fa13209b5ee51f85a6c9159

cff0f0513ec4b9d0442946416ca64384

66b8683e4007fb5d6a14c2d3cfca8e07

517a260cf7c5dc7a305bc281670cec3e

3733202ff94169e9fde0d24c5483e4cb

bfcf661c2b7a99bc29144c20b79656b8

42c820c82b43d9497d9f5a190ef5dd77

80e491ae4bd95c2b23c644f7d50cc121

b296483728506b9c2152a66aeea2e82c

332f6264b2c7b5077b0425b088608c16

c68643429325001d8cd9a20e85221b86

af299f5ab6126b5ad3437f41e5e04dc1

f797689c1b5c7b1621978b6afa98f7da

5ee97a4fe0ff158dc4390ef31e4b9a3d

Domains:

doorblu.xyz

buyerbrand.xyz

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

1. **CMTX-P072024114: TrollAgent Stealer**

Malware Alert Brief:

TrollAgent is a malicious DLL information stealer developed by Kimsuky, a North Korean threat actor, using GoLang. Its capabilities include:

- - Retrieving system information

- - API hooking and reflective PE injection

- - Keystroke logging

- - Debugger detection

- - Capturing desktop screenshots

- - Enumerating running processes

- - Delaying execution

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

HASH

9e75705b4930f50502bcbd740fc3ece1

27ef6917fe32685fdf9b755eb8e97565

7b6d02a459fdaa4caa1a5bf741c4bd42

7457dc037c4a5f3713d9243a0dfb1a2c

c8e7b0d3b6afa22e801cacaf16b37355

2e5f2a154e1b67cd0d6a2f6b5feb6de7

045f28a479ba19a95c0407a663e2f188

a67cf9add2905c11f5c466bc01d554b0

3b596ca429cf1b733f1ff3676189e44a

88f183304b99c897aacfa321d58e1840

Domain

\*\*.p-e.kr/index.php

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

1. **CMTX-P-5460720249: 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

45.252.248.26

46.20.7.175

213.189.52.181

203.161.184.34

5.2.84.236

93.89.225.40

89.39.83.184

61.19.247.49

86.96.202.167

104.247.165.99

185.99.1.126

89.36.25.206

188.127.239.250

86.105.155.116

195.252.110.253

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

1. **CMTX-P-2770720249: 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

77.105.135.107

147.45.44.16

185.215.113.67

185.196.9.26

94.228.166.68

185.172.128.33

77.105.164.59

77.91.77.6

185.237.165.67

91.92.253.215

20.52.165.210

94.156.69.115

89.23.101.114

95.217.49.114

45.140.147.183

135.181.121.224

4.185.56.82

91.92.249.24

31.177.108.40

85.28.47.132

38.180.204.127

147.45.44.77

2.58.56.186

178.23.190.118

194.28.226.213

91.92.249.167

38.180.147.152

207.148.69.28

84.38.134.17

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

1. **CMTX-P-4650720249: 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

49.205.182.134

130.0.132.242

51.89.36.180

195.251.213.56

77.74.78.80

115.79.195.246

202.79.24.136

51.38.124.206

81.213.175.132

173.212.214.235

42.200.96.63

51.75.33.127

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

1. **CMTX-P-3410720249: 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

94.142.138.49

94.142.138.108

94.228.166.22

94.103.88.64

77.91.77.54

62.113.112.27

95.169.205.186

88.119.161.19

147.45.44.2

65.109.175.35

188.215.229.203

45.89.55.21

178.20.41.15

94.103.84.253

79.137.197.160

45.89.55.84

77.232.39.101

91.103.252.65

5.255.100.41

94.142.138.162

94.131.106.24

62.113.119.179

185.238.168.190

94.142.138.228

149.154.67.234

185.53.46.103

94.142.138.19

5.252.22.79

147.45.44.25

77.91.102.12

94.142.138.109

91.242.229.166

95.216.109.16

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

1. **CMTX-P-1890720249: 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

93.190.41.79

103.249.111.96

35.215.148.34

185.216.114.10

114.119.138.59

114.119.146.19

114.119.141.42

34.143.221.240

31.220.15.143

51.222.253.4

114.119.152.128

35.240.72.170

114.119.146.195

217.160.0.220

49.0.204.77

43.139.153.132

162.158.114.224

77.189.27.109

157.42.193.129

77.75.76.165

51.222.253.5

51.222.253.20

51.222.253.7

194.247.173.99

114.119.159.87

51.222.253.2

51.222.253.14

51.222.253.1

5.101.115.147

94.74.81.63

190.92.205.226

51.222.253.8

51.222.253.12

49.0.204.178

159.138.109.15

124.243.135.114

110.238.109.250

35.187.36.129

114.80.36.40

217.113.194.247

77.189.211.27

195.201.204.138

188.166.96.13

119.8.166.176

124.243.147.105

129.226.151.139

139.59.103.203

162.158.106.12

172.70.147.156

172.71.81.219

172.71.82.52

190.92.209.84

77.245.56.14

217.160.0.215

51.222.253.18

51.222.253.6

51.222.253.15

117.185.229.12

103.67.163.199

194.163.145.202

185.187.241.36

114.119.153.172

83.97.73.245

92.204.68.47

124.243.136.24

159.138.98.180

114.119.132.114

101.44.160.97

94.74.80.56

111.6.233.206

119.13.103.43

124.243.135.130

124.243.148.114

124.243.133.152

124.243.151.209

185.181.61.115

109.70.100.3

185.106.94.195

117.161.174.245

219.151.138.203

80.67.167.81

204.27.64.10

106.222.199.156

202.177.252.106

178.20.55.16

84.239.54.49

185.243.218.204

101.44.160.62

101.44.161.217

110.238.105.83

119.13.106.134

124.243.136.118

124.243.146.243

124.243.149.22

159.138.84.88

159.138.107.62

190.92.204.233

117.161.174.248

117.161.174.247

51.222.253.11

195.24.68.25

51.222.253.13

192.46.231.103

82.197.71.21

95.142.47.113

195.2.84.198

159.138.99.105

51.222.253.3

190.92.216.77

135.181.213.220

119.13.110.84

94.74.90.22

111.119.210.65

213.186.33.16

101.44.162.230

119.8.174.80

159.138.123.188

159.138.121.137

159.138.105.125

190.92.200.8

94.74.88.198

159.138.110.35

85.209.11.117

95.217.109.26

124.243.145.191

124.243.149.153

159.138.101.120

154.92.108.154

182.42.104.32

223.113.128.137

172.69.192.213

5.255.231.188

209.38.45.126

213.180.203.146

43.134.37.211

47.128.39.82

49.0.203.70

49.0.207.249

101.44.160.33

101.44.161.96

101.44.161.235

114.119.159.33

114.119.172.209

124.243.135.135

124.243.137.220

124.243.147.168

124.243.147.181

150.109.16.20

159.138.93.105

190.92.210.8

190.92.210.248

190.92.216.132

122.147.26.105

178.20.45.128

94.74.94.111

114.119.191.215

124.243.148.74

51.222.253.9

51.222.253.19

51.222.253.16

119.8.182.174

119.13.103.190

94.74.86.10

190.92.221.166

49.0.204.143

124.243.134.105

110.238.111.43

124.243.146.203

43.163.8.36

117.161.174.249

219.135.97.88

185.54.231.66

5.188.62.174

43.134.170.46

94.74.84.72

119.13.103.133

124.243.133.167

124.243.145.164

178.151.245.162

154.118.228.210

185.231.154.128

124.243.139.76

49.0.203.114

119.13.103.45

91.142.73.116

84.54.44.204

195.2.74.148

101.44.162.117

117.132.188.206

62.113.113.162

94.103.90.150

178.20.43.173

178.20.45.159

178.20.47.39

185.231.155.169

195.2.71.225

195.2.78.191

195.2.79.165

84.54.44.19

159.138.96.119

49.0.205.155

36.150.60.24

162.158.22.62

77.187.50.250

82.197.71.18

62.238.194.19

178.20.44.82

178.20.45.182

3.1.87.175

13.251.0.58

49.0.204.151

49.0.205.36

101.44.161.63

190.92.211.83

92.53.96.139

185.94.97.5

188.241.80.69

79.110.49.77

95.91.111.56

172.71.250.24

49.206.34.135

43.163.6.124

190.92.200.14

34.80.65.124

139.162.60.246

49.0.204.2

65.108.128.54

34.96.143.131

90.187.238.157

91.189.177.186

188.130.128.210

34.142.190.84

108.162.226.161

111.119.194.102

162.158.107.57

162.158.171.10

172.69.166.91

172.71.82.116

172.71.152.25

94.205.106.204

193.37.32.148

45.125.239.179

145.239.23.7

36.134.147.75

162.158.114.131

84.46.245.21

158.220.123.225

185.220.101.30

46.17.174.192

193.36.237.217

43.128.100.206

108.162.227.3

103.130.218.39

195.2.67.184

195.2.75.216

43.128.110.17

81.4.122.193

49.0.200.89

36.99.136.129

34.78.186.176

120.230.10.46

182.16.21.98

37.120.190.85

110.226.177.66

139.59.118.87

166.108.224.168

172.71.81.143

179.61.189.179

51.222.253.17

135.181.74.243

136.243.35.73

144.76.67.169

157.90.182.28

172.71.250.25

217.76.60.61

139.59.190.132

164.92.234.251

43.156.12.25

114.119.165.226

119.8.174.228

124.156.200.143

172.69.46.154

128.199.71.165

51.222.253.10

128.199.167.175

62.122.184.194

77.75.79.95

37.60.240.180

162.158.86.8

128.199.45.220

43.134.142.8

108.162.227.88

124.243.132.148

129.226.158.26

162.158.162.223

162.158.163.251

172.69.166.65

172.70.143.209

172.71.81.72

217.160.0.246

54.36.145.173

8.218.180.91

113.215.189.90

113.215.189.121

172.68.225.193

172.69.144.173

45.76.55.47

172.225.137.15

43.134.89.111

43.159.63.75

129.226.147.7

159.138.86.91

162.158.170.37

165.22.111.237

172.68.242.123

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

1. **CMTX-P-5830720249: 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

45.9.74.141

45.9.74.166

45.9.74.182

45.9.74.164

188.40.122.96

78.46.242.112

31.41.244.158

62.204.41.89

134.0.116.60

79.137.203.59

207.154.243.184

62.182.156.153

79.137.203.19

185.153.197.14

188.40.141.211

34.90.130.132

172.235.7.46

49.12.117.51

78.47.9.120

193.106.191.184

185.215.113.9

77.91.78.118

77.105.160.21

45.159.189.140

188.40.187.155

5.104.108.23

193.106.191.201

185.196.8.176

45.140.19.240

185.11.61.121

193.166.255.171

5.75.139.35

81.17.29.162

78.153.144.60

89.163.210.240

80.76.42.67

181.204.98.226

136.243.106.238

45.92.178.114

89.46.7.229

31.204.159.244

5.134.5.71

2.19.173.145

213.246.62.226

23.55.110.195

35.198.174.167

92.205.55.132

148.113.8.71

185.173.130.24

77.37.53.180

95.141.183.175

195.128.49.210

47.246.165.164

62.204.41.252

193.233.20.14

185.215.113.204

195.66.210.137

35.233.77.94

213.202.223.115

213.13.145.243

212.204.112.234

213.202.223.111

51.250.126.210

85.209.135.11

109.206.161.72

109.206.161.15

185.216.143.2

45.92.178.115

5.101.37.37

45.142.177.78

176.221.32.30

146.148.22.93

193.41.237.81

147.102.10.1

213.209.62.1

77.37.53.74

77.37.53.76

77.37.53.147

77.37.53.225

46.22.59.7

91.228.238.70

212.200.255.49

109.206.161.43

212.112.110.243

149.129.194.93

185.172.128.116

89.163.152.111

147.45.47.155

91.203.4.45

62.150.232.50

185.216.143.48

94.102.57.166

159.100.251.128

80.150.6.143

193.233.233.233

185.87.148.190

185.172.128.61

185.221.172.246

187.211.19.25

35.214.253.251

144.122.145.145

47.245.122.105

109.98.58.98

5.79.71.225

217.219.131.81

92.223.116.222

190.147.2.86

77.91.78.17

154.144.253.197

131.255.215.165

93.103.167.123

177.222.41.236

92.46.53.222

212.162.57.144

190.249.193.233

89.58.1.89

89.163.225.85

99.81.95.247

189.232.42.250

37.143.8.8

47.236.119.230

92.223.116.223

93.123.39.97

194.190.152.209

34.88.137.133

195.123.210.178

185.172.128.53

193.106.191.185

92.205.213.10

146.0.36.124

185.98.5.133

187.205.152.46

5.45.85.141

37.48.65.154

89.23.97.19

185.119.89.103

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

1. **CMTX-P-8200720249: 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

85.53.178.52

178.22.83.226

158.181.50.180

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

1. **CMTX-P-2490720249: 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

193.142.147.59

146.19.173.87

77.91.77.137

77.91.77.96

185.244.48.191

94.142.138.49

94.142.138.108

94.228.166.22

94.103.88.64

77.91.77.54

62.113.112.27

95.169.205.186

88.119.161.19

147.45.44.2

65.109.175.35

188.215.229.203

45.89.55.21

178.20.41.15

94.103.84.253

79.137.197.160

45.89.55.84

77.232.39.101

91.103.252.65

5.255.100.41

94.142.138.162

94.131.106.24

62.113.119.179

185.238.168.190

94.142.138.228

149.154.67.234

185.53.46.103

41.77.134.250

175.184.232.234

27.109.116.144

103.9.188.78

177.190.76.82

103.201.142.30

96.9.77.142

196.41.57.46

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

1. **CMTX-P-9250720249: 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

18.141.10.107

18.143.155.63

13.251.16.150

185.110.92.40

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

1. **CMTX-I-138072024: 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>----------------------------

\*.meacases.report

mea.gov.in.meacases.report

www.mea.gov.in.meacases.report

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

1. **CMTX-I-432072024: Ahmyth Android Trojan**

Following IOCs are associated with AhMyth android trojan used by threat actors to target mobile devices:

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

3.106.41.21

64.227.190.73

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

1. **CMTX-P072024155: CUTTLEFISH MALWARE**

ALERT BRIEF:

ALIAS: SILENTDUCK

A recently discovered malware tracked as "Cuttlefish" is active in the cyber threat landscape. Small office/home office (SOHO) and enterprise-grade routers are allegedly its target, and its objectives include network traffic monitoring and obtaining authentication information via HTTP GET and POST requests. It also has the ability to intercept data and perform DNS & HTTP hijacking, rerouting traffic to malicious websites and use compromised router to establish a VPN or proxy, giving attackers continuous access to the network. Cuttlefish uses a zero-click methodology which enables it to collect data without requiring user input with the aim to steal authentication details and other sensitive data from web requests that go over the compromised router. It poses a serious risk to cloud security because it focuses on publicly accessible cloud-based services.

Also, the malware shows code similarities with HiatusRAT, suggesting a possible connection to China-based threat actors.

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

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

IPs

156.254.120.5

107.189.28.251

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

1. **CMTX-P072024124: TAG-109 Threat actor**

Alert Brief:

An uptick in malicious activity by China State-sponsored TAG-109 is being reported. Notably, this group is utilizing Cloudflare, a content delivery network (CDN) provider, to disguise their command and control (C2) communications by routing them through the custom backdoor known as KEYPLUG. This modular backdoor has been shared among various Chinese state-sponsored threat groups and has been prominently employed by groups such as RedGolf (APT41) and Brass Typhoon.

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

Domain

allianz-pc.com

cimtag.com

ellisysplus.com

idrech.com

iservius.com

klsvp.com

latarstore.com

leftwroldnet.com

llskyc.com

meacosafety.com

prellox.com

rkaks.com

salvaweb.com

setigt.com

site-coinberry.com

softonmic.com

stackcentertech.com

tvfmrp.com

IP Address

2.58.15.51

5.255.99.47

5.255.103.38

45.129.199.208

46.102.174.7

77.83.198.41

82.117.255.89

85.239.55.47

89.147.108.226

89.150.40.23

89.207.129.143

94.140.115.128

146.70.135.243

185.244.129.90

185.244.129.218

193.168.141.28

195.123.218.38

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

1. **CMTX-P072024846: SparkRAT Malware**

ALERT BRIEF:

SparkRAT is a cross-platform and full-featured Remote Administration Tool (RAT) written in Go. Its capabilities include file and process management, file transfer, remote desktop monitoring and screen capture, system information collection, and terminal access for command execution, among others.

Recently TAG-100 (cyber-espionage threat actor) has been observed using the open-source, multi-platform Go backdoor to gain control over compromised systems and execute various malicious activities.

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

HASHES

23efecc03506a9428175546a4b7d40c8a943c252110e83dec132c6a5db8c4dd6

ec45da0ca70a9b71652cc95d51665f7ad568294bd5652c395a119bccd613e9b4

b8cab11421eb4731c16cf3c34ca2b3f2a758d5e112f877b90a18b3e146c8add0

IP ADDRESSES

216.238.68.36

209.141.50.215

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

1. **CMTX-P072024118: BITRAT**

ALERT BRIEF:

Bitrat is a backdoor which written in C++ programming language with various capabilities. It can perform file operations, execute remote commands, gather system information, record audio, control webcams, take screenshots, engage in crypto mining, browse websites, participate in DDoS attacks, log mouse and keyboard interactions, and even force a BSOD (Blue Screen of Death). BitRAT is delivered via phishing emails with malicious attachments or fake browser updates. Once executed, BitRAT clears DNS cache, downloads additional code (e.g., PowerShell), and installs related malware (like: LummaC2 information-stealer).

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

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

Hashes:

8b424e81e72bead6c3067c2988c62d52fd7456ceda8a6eb8f09fa9d884274c62

07f48be354055f9d3fa9b68dcebd2fce3545c0da52e1b426bc11f35d7fd62e06

2dd362ecd871dc5fb308a1d1629a657f2e3144c181e6450756e2865b6f0869ca

9943bf1e938bb44dc25c1cfe778b93ac58b16715ff651d42672a6820b182e0bc

df333a05baa016edd27d2e1c54710c52d58d319b48557b21fb90a632613c8738

IPs:

159.100.13.218

176.113.115.177

163.172.59.233

31.173.88.81

163.172.112.161

193.34.77.154

50.114.185.59

77.91.101.145

45.207.52.74

8.208.27.150

185.157.160.136

213.152.162.69

213.152.186.40

46.196.24.72

46.226.163.38

52.67.176.25

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

1. **CMTX-P072024134: APT45 Threat actor**

Alert Brief:

APT45, a North Korean cyber operator, has conducted espionage campaigns targeting critical infrastructure. Threat actor relies on a mix of publicly available tools such as 3PROXY, malware modified from publicly available malware such as ROGUEEYE,QUINSTATUS and custom malware families. Description of prominent Malware Family / Tool recently used by threat actors were:-

3PROXY is a lightweight proxy server that is publicly available and open sourced on GitHub.

QUINSTATUS is a backdoor written in Pure Basic. Its primary goal is to perform system survey and download a second-stage payload. It beacons to its C2 server and from the C2 server response it interprets certain HTTP status codes as control commands to take certain actions. In addition, it can erase itself.

ROGUEEYE is a backdoor written in C++ that communicates via a custom binary protocol over TCP. Supported commands include screen capture, file execution, file download, process creation, and configuration update.

BEBANSHELL is a backdoor written in C that communicates via a custom binary protocol over TCP. Supported backdoor commands include reverse shell, file transfer, file deletion, process termination, and user enumeration.

COUNTERLOOP is a C/C++ proxy. It accepts the IP and port over the command-line and uses a custom protocol over TCP. A custom handshake is used when making connections.

IRONSTORM is a backdoor written in C that can operate over HTTP and IRC. The backdoor has the capability of loading plugins, uploading and downloading files, providing reverse shell, spawning processes, and uploading basic system information to its configured C2 servers

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

HASH

0ed084c48634e8497c7eda51570793c1

0d696d27bae69a62def82e308d28857a

0a5a3d31346f91bffcfc69950bac18c3

079b4588eaa99a1e802adf5e0b26d8aa

028693c655be9ced65a5fdd419f870c1

0055a266aa536b2fdadb3336ef8d4fba

3e9ee5982e3054dc76d3ba5cc88ae3de

3a3bad366916aa3198fd1f76f3c29f24

31b6d895da1fbe17d45b3905b71bdb94

2e18350194e59bc6a2a3f6d59da11bd8

2cc302d80050dd10e8d8c489e5873a1c

2124d4562f79f2a2c0edf94e6ced8e10

17335705966160a4c5da10b596d83f72

152b264288bcf5dc02222cee49587b8e

11ec5eb513e5a4d9d35be0b8c3335099

0f9b876031ffc16c7eedfeaf2ca9dc5b

640e70b0230dc026eff922fb1e44c2ea

59ec24539c786e6ac9467dad3183c280

4e66cfd161c2318bd3da6dd82fc5c56b

4d30612a928faf7643b14bd85d8433cc

4bb54e135302bf3c21bff89177f70759

43e756d80225bdf1200bc34eef5adca8

41882402c8937f2ba2c4791c081f54c3

3fd8b6fc3b5778b6552289a5c01433bc

88f9824b5a76591d62d391e6b1ef1d31

7c30ed6a612a1fd252565300c03c7523

769617b07d0a455fd666418bafbdae1b

72a22afde3f820422cfdbba7a4cbabde

6dad4ad013a1991695302bdd34fbb566

6c2b947921e7c77d9af62ce9a3ed7621

b48a887f303c6e01ce054353f8318523

9b9d4cb1f681f19417e541178d8c75d7

9767aa592ec2d6ae3c7d40b6049d0466

f8f7eced1411d76e2a0319151ecf80b7

cf236bf5b41d26967b1ce04ebbdb4041

cdeae978f3293f4e783761bc61b34810

c55a5596265921d653778e6db3a50ea1

c027d641c4c1e9d9ad048cda2af85db6

befba41ba023bb72f70b5ef904517d8f

f49c34718ad43d37624d4bddf70fe79b

f2132947d0668084620c7687342c7bb9

eb4c52b2c9564583f244570528f3f6a1

dd9625be4a1201c6dfb205c12cf3a381

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

1. **CMTX-I-911072024: 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>----------------------------

admitcard.ordnancerecruitment.com

apply.ordnancerecruitment.com

mail.ordnancerecruitment.com

webmail.ordnancerecruitment.com

\*.ordnancerecruitment.com

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

1. **CMTX-P072024522: Threat actors exploit recent CrowdStrike update issue**

ALERT BRIEF:

It has been reported that threat actors are distributing a data wiper malware masquerading as a CrowdStrike update installation. This campaign takes advantage of the recent CrowdStrike update issue, which caused Windows systems to crash into a Blue Screen of Death (BSOD) state. This allows attackers to spread malware by using filenames that look like those of legitimate CrowdStrike files. The Wiper malware was delivered using pdf file containing link to zip which in turn contains the actual payload. The wiper malware overwrites the system files with zero bytes.

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

1bbb795ce19f4dcc4ac9f8e8c12f3452f1f07c68a53ef631c76e392e1d06ea43

96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8

4491901eff338ab52c85a77a3fbd3ce80fda738046ee3b7da7be468da5b331a3

1fa1f7f0089f89e07406412c257ae546bb9728f7055f804e800e6c41a682c882

865347471135bb5459ad0e647e75a14ad91424b6f13a5c05d9ecd9183a8a1cf4

https[:]//link.storjshare.io/s/jwyite7mez2ilyvm2esxw2jq3apq/crowdstrikeisrael/update.zip

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

1. **CMTX-P072024165: LOSTINFO RANSOMWARE**

ALERT BRIEF:

According to the reports, a sample of a new ransomware family called as "LostInfo" has been discovered. LostInfo alters the filenames of affected files by appending a random ID and the extension “.lostinfo.”. After encryption, a ransom note titled “README.TXT” is generated, warning the victim that their files have been encrypted. Its capabilities include enumerating files and directories, shutting down operating processes, delaying execution, retreiving the logged-in user's username, querying system information, and verifying default system language.

Some of its other capabilities are:-

• Lists all physical and external hard disks attached to the machine.

• Lists running processes

• Uses the AdjustTokenPrivileges API call to grant SeTakeOwnershipPrivilege token higher access.

• Checks the machine's external IP address with iplogger.co, a legitimate IP search service.

• Checks memory for virtual machine (VM)-related strings.

• Sends HTTP GET request to https://iplogger.co/162c65.torrent, which currently shows a PNG image.

• Sends HTTP GET requests to http://c.pki..Google/r/gsr1.crl and http://c.pki.goog/r/r4.crl to download the certificate revocation list (CRL) files from Google Trust Services.

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

HASHES

6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0

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

1. **CMTX-P072024856: Play Ransomware**

ALERT BRIEF:

Aliases: PlayCrypt and Balloonfly

The Play ransomware group has allegedly developed a new Linux variant specifically targeting VMWare ESXi environments. When operating within an ESXi environment, this variant scans and initiates shutdowns for all VMs using the command: /bin/sh -c “for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"; otherwise, it will terminate and delete itself. Additionally, recent reports suggest that Play has entered into a collaboration with Prolific Puma, a threat group known for providing illicit infrastructure to various cybercriminals.

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

HASHES

021036dfac5f804fca6b6f3c084094349971bd6a7b78e44ca1a333f98b6666e1

7a55c8391fda90a5d4653fdebe2d685edb662859937e14b6756f45e29b76901d

IP ADDRESSES

108.61.142.190

45.76.165.129

URL's

http://108.61.142.190/1.dll.sa

http://108.61.142.190/64.zip

http://108.61.142.190/winrar-x64-611.exe

http://108.61.142.190/PsExec.exe

http://108.61.142.190/host1.sa

http://108.61.142.190/FX300.rar

Domains

lcmr.info

kwfw.me

vqbl.info

mmhp.link

pkil.me

iwqe.info

hibh.info

apkh.info

bltr.me

thfq.info

jhrd.me

iing.info

znuc.info

zfrb.info

ztqs.info

gunq.link

ylvq.me

whry.me

vgkb.info

flbe.link

pxkt.me

ukwcc.info

xzdw.info

ojry.link

mcmb.info

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

1. **CMTX-P-9110720249: Mirai Botnet Campaign**

Malware Alert Brief:

Mirai botnet targets networked devices running Linux. Mirai primarily focuses on online consumer devices like IP cameras and home routers. It spreads by scanning and exploiting the vulnerable Internet of Things (IoT) devices. Once infected, attackers make the devices a part of their Mirai-based botnet which they use later for conducting DDoS attacks.

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

15.235.209.194

107.172.193.113

109.98.208.52

147.78.103.120

163.172.185.194

167.88.161.40

178.215.236.169

178.215.236.209

185.196.8.198

185.196.8.213

188.132.234.16

193.141.60.143

193.35.18.172

193.35.18.42

194.169.175.3

194.169.175.31

194.49.94.79

2.59.254.14

205.185.120.173

205.185.122.208

216.219.94.5

216.219.94.57

37.139.128.239

38.45.200.163

45.131.111.250

45.56.96.91

45.88.90.129

5.181.80.120

80.66.79.43

87.246.7.195

89.190.156.145

91.208.206.151

93.123.39.224

93.123.85.135

79.132.128.112

79.143.189.101

168.119.59.237

171.22.30.126

185.14.29.231

vps-a907fa49.vps.ovh.ca

taxinhanhlongan.com

www.taxinhanhlongan.com

www.xelientinhmiennam.com

botnet.4gnekoland.top

xelientinhmiennam.com

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

1. **CMTX-P072024175: RA WORLD RANSOMWARE**

ALERT BRIEF:

RA World is a multistage ransomware family that primarily targets healthcare and financial sectors with multi-stage attacks and double extortion techniques. It first acquires access via compromised domain controllers and delivers their components to the SYSVOL sharing path of a machine Group Policy Object (GPO) to enable privilege escalation and ransomware delivery on victim systems. The malware employs anti-AV strategies and exploits GPO settings to allow PowerShell script execution.

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

HASHES

330730d65548d621d46ed9db939c434bc54cada516472ebef0a00422a5ed5819

a8315e4d502f7693c95be64ed27b44eae722aa7b1987b32e49cb48763e91d5e8

51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc

9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

dffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

feab413f86532812efc606c3b3224b7c7080ae4aa167836d7233c262985f888c

07ab218d5c865cb4fe78353340ab923e24a1f2881ec7206520651c5246b1a492

a4dfa099e1f52256ad4a3b2db961e158832b739126b80677f82b0722b0ea5e59

62cd46988f179edf8013515c44cbb7563fc216d4e703a2a2a249fe8634617700

ab7d8832e35bba30df50a7cca7cefd9351be4c5e8961be2d0b27db6cd22fc036

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

1. **CMTX-P072024144: Daggerfly threat Actor Activity**

ALERT BRIEF:

The cyber threat group Daggerfly, also known as Evasive Panda, is a Chinese-speaking Advanced Persistent Threat (APT) actor. Their attack begins by exploiting a vulnerability in Apache HTTP servers to deliver the MgBot malware. This malware then deploys the Macma backdoor on macOS devices, which has recently been updated with new features and capabilities, including screen capture resizing and enhanced debug logging. Additionally, Daggerfly has introduced a new Windows backdoor called Nightdoor (also known as NetMM) to their arsenal. Nightdoor creates specific folders to store encrypted network configuration data, allowing it to evade detection and maintain communication with its command and control (C2) server.

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

HASH

f97261da97cfd3a907f19931008ac34dde2898415bd96387caef03e840403e7c

003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef

1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e

dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313

570cd76bf49cf52e0cb347a68bdcf0590b2eaece134e1b1eba7e8d66261bdbe6

eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0

d8a49e688f214553a7525be96cadddec224db19bae3771d14083a2c4c45f28eb

955cee70c82bb225ca2b108f987fbb245c48eefe9dc53e804bbd9d55578ea3a4

fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced

5687b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595

49079ea789e75736f8f8fad804da4a99db52cbaca21e1d2b6d6e1ea4db56faad

5c52e41090cdd13e0bfa7ec11c283f5051347ba02c9868b4fddfd9c3fc452191

4c3b9a568d8911a2a256fdc2ebe9ff5911a6b2b63c7784da08a4daf692e93c1a

ef9aebcd9022080189af8aa2fb0b6594c3dfdc862340f79c17fb248e51fc9929

0cabb6780b804d4ee285b0ddb00b02468f91b218bd2db2e2310c90471f7f8e74

3894a8b82338791764524fddac786a2c5025cad37175877959a06c372b96ef05

3a6605266184d967ab4643af2c73dafb8b7724d21c7aa69e58d78b84ebc06612

65441ea5a7c0d08c1467e9154312ac9d3fdd3ca9188b4234b5944b767d135074

IP

103.243.212.98

103.96.131.150:40020

103.96.128.44

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

1. **CMTX-I-170072024: Malicious Domains used by Threat Actors**

Malicious Domains used by APT Threat Actors are as follows:

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

checksec.in

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

Kindly take the required actions.

1. **CMTX-I-590072024: 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>------------

drivestransfer.com

warfarestudies.in

eoffice-sparrow.online

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

1. **CMTX-I-765072024: Mythic Malware IOCs**

Following are the C&C of Mythic Malware. This RAT is being used by various threat actors to target Linux based systems.

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

139.59.86.97

139.84.217.198

143.110.176.131

159.223.224.93

165.232.177.53

64.227.141.158

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

1. **CMTX-P072024605: 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

141.164.36.138

207.246.106.76

95.179.235.165

154.31.217.197

154.205.138.51

154.205.138.51

154.205.138.51

139.99.36.29

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

1. **CMTX-P072024065: PLUGX RAT ALERT 126**

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

38.47.220.137

18.141.169.162

23.227.203.181

109.61.43.46

49.232.102.51

38.47.220.31

47.238.138.224

104.251.122.107

23.227.203.181

23.227.203.181

104.251.122.107

104.251.122.107

104.251.122.107

47.238.138.224

104.251.122.107

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

1. **CMTX-I-680072024: Malicious IP Hosting Malware**

Following IP is being used to host malware targeting users in Indian cyber space.

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

159.65.146.80

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

Kindly take the required actions.

1. **CMTX-P072024866: Stargazer Goblin recent activity**

ALERT BRIEF:

Recently a threat group named Stargazer Goblin which provides, operates, and maintains the Stargazers Ghost Network and distributes malware and links via their GitHub Ghost accounts has been found active. In recent campaigns the threat group has been found using GitHub repositories along with compromised WordPress sites to distribute password-protected archives that contain malware families like Atlantida Stealer, Rhadamanthys, Lumma Stealer, and RedLine. This modern method of malware distribution involves utilizing ghost accounts across different platforms and may incorporate AI for more precise targeting.

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

IP ADDRESSES

147.45.47.64

185.172.128.95

147.45.44.73

89.23.98.116

147.78.103.199

HASHES

2B6C8AA2AC917D978DFEC53CEF70EACA36764A93D01D93786CC0D84DA47CE8E6

385EBE3D5BD22B6A5AE6314F33A7FA6AA24814005284C79EDAA5BDCF98E28492

2EBF051F6A61FA825C684F1D640BFB3BD79ADD0AFCFF698660F83F22E6544CBA

AB59A8412E4F8BF3A7E20CD656EDACF72E484246DFB6B7766D467C2A1E4CDAB0

060DE3B4CF3056F24DE882B4408020CEE0510CB1FF0E5007C621BC98E5B4BDF3

64A49FF6862B2C924280D5E906BC36168112C85D9ACC2EB778B72EA1D4C17895

148C456E83E746A63E54EC5ABDA801731C42F3778E8EB0BF5A5C731B9A48C45D

2F5624DCDA1D58A45491028ACC63FF3F1F89F564015813C52EEBD80F51220383

98B7488B1A18CB0C5E360C06F0C94D19A5230B7B15D0616856354FB64929B388

A484FA09BE45608E23D8E67CD28675FA3E3C4111AF396501385256CE34FF1D95

8D8D7EB1180C13ED629DCEAC6C399C656692A6476C49047E0822BEC6156A253A

URL's

https://considerrycurrentyws.shop

https://deprivedrinkyfaiir.shop

https://detailbaconroollyws.shop

https://distincttangyflippan.shop

https://greentastellesqwm.shop

https://horsedwollfedrwos.shop

https://innerverdanytiresw.shop

https://lamentablegapingkwaq.shop

https://macabrecondfucews.shop

https://messtimetabledkolvk.shop

https://patternapplauderw.shop

https://relaxtionflouwerwi.shop

https://sideindexfollowragelrew.pw

https://slamcopynammeks.shop

https://standingcomperewhitwo.shop

https://stickyyummyskiwffe.shop

https://sturdyregularrmsnhw.shop https://understanndtytonyguw.shop

https://vivaciousdqugilew.shop

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

1. **CMTX-P072024185: Rhysida Ransomware**

ALERT BRIEF:

Previous Alert Reference :[CMTX-P062023265] Rhysida Ransomware, TLP: CLEAR, dated 10/07/2023

RHYSIDA is a ransomware usually written in C++. It operates as ransomware-as-a-service (RaaS) model and employs double extortion tactic, where they not only encrypts the victim’s data but also threaten to release it publicly if the ransom is not paid. They gain initial access using Cobalt Strike beacons for deploying malicious IP scanners through malvertising campaigns, exfiltrating sensitive data for extortion purposes, phishing campaigns, exploiting vulnerabilities (e.g. Zerologon), and leveraging remote services such as VPNs. Lately it was reported that Rhysida Ransomware Group has employed a new "Oyster Backdoor" (aka Broomstick and CleanUpLoader) variant in their operation.

The malware propagates via malvertising campaigns, often delivered through trojanized installers that introduce a backdoor into infected systems. It was noted that the malware establishes persistence by creating scheduled tasks and embeds itself into the system through the execution of legitimate software installers. This backdoor can connect to a command-and-control (C2) server to gather details about the compromised device, including the hardware specifications, installed software, and operating system (OS).

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

HASHES

0a7fd836d36ed8e8e9aa7bc41fdc9242333e8469059dec8886b7d935f3651679

0c8e88877383ccd23a755f429006b437

1e256229b58061860be8dbf0dc4fe67e

3225b95fc72f238ab1e53bfabc11b551

44c7d18633b5741db270a6bd378b6f3c

569d2b5701755260514fe1563d7530bb

59a9ca795b59161f767b94fc2dece71a

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

1. **CMTX-I-634072024: Malicious IP Hosting Malware**

Following IP is being used to host malware targeting users in Indian cyber space.

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

157.245.100.177

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

Kindly take the required actions.

1. **CMTX-P072024128: Blacksuit Ransomware (Rebrand of Royal Ransomware)**

ALERT BRIEF:

A new ransomware called "Blacksuit" has emerged and is reported to exhibit characteristics similar to Royal Ransomware. BlackSuit uses double-extortion technique to leak stolen data and uses a string “delete”, which allows the ransomware executable to delete itself after encryption and it also contains the string “disablesafeboot” which allows it to remove the current safeboot entry and then restart the machine. To gain initial access it uses phishing techniques and exploit vulnerabilities in public-facing applications. This ransomware is executed via the command line with a required argument "-name". To establish SSH connection, it has been found using tools such as Chisel and Cloudflared, as well as Secure Shell (SSH) Client, OpenSSH and MobaXterm.

MITRE ATT&CK Identifiers

T1190 Exploit Public-Facing Application

T1566 Phishing

T1070.004 Indicator Removal: File Deletion

T1562.009 Impair Defenses: Safe Mode Boot

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

HASHES

1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c

449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b

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

1. **CMTX-P072024876: RansomHub Ransomware**

ALERT BRIEF:

Ransomhub is a ransomware-as-a-service (RaaS) developed using Go and C++, designed to target Windows, Linux, and ESXi operating systems. The newest variant, which is Go-based, offers rapid encryption and can evade shutdown attempts on virtual machines (VMs). It also employs gobfuscate, a technique for obscuring Go binaries, similar to what was used in earlier versions of Ransomhub.

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

HASHES

342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b

56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763

60b477dab8494d3a049cf3b17118a4124b68f9f7d3dcc3c92026ac86b00aae1e

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

1. **CMTX-I-400072024: Mythic Malware- APT36 campaign**

Following are the C&C of Mythic Malware. This RAT is being used by various threat actors to target Linux based systems.

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

107.172.100.174

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

Kindly take the required actions.

1. **CMTX-P072024886: QuasarRAT Malware ALERT 61**

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

193.107.109.76

41.216.183.103

85.28.47.123

66.42.35.73

149.102.139.193

45.141.215.199

184.145.64.135

181.162.141.21

193.29.13.46

188.173.86.179

5.253.246.44

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

1. **CMTX-I-500072024: Mythic Malware- APT36 campaign**

Following are the C&C of Mythic Malware. This RAT is being used by various threat actors to target Linux based systems.

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

47.245.114.11

service-desk.duckdns.org

hansesecure.com

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

1. **CMTX-I-401072024: 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>------------

cert-in.otg.in

cisf-gov.info

www.cisf-gov.info

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

1. **CMTX-I-501072024: Suspicious Domains used by Threat Actors**

Following suspicious domains have been registered and may be used by threat actors to host malicious code/malware/spear-phishing website :

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

www.mod.gov.in.aboutcase.nl

aboutcase.nl

hamraazmp8.fov.in

fov.in

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

1. **CMTX-P072024874: IOCs related to Cobalt strike Malware**

A new Python-based loader is observed which is being used by threat actors to install Cobalt Strike malware in various organizations' networks. The attackers are utilizing open-source Python scripts and native Windows tools for network reconnaissance, lateral movement, and executing Cobalt Strike. To deploy the final CAB file, they're employing tools like Impacket, WMIC, PsExec, and RDP. Once Cobalt Strike is installed, the attackers use the Windows utility SDelete to remove traces of the malicious CAB file and Python loader, covering their tracks.

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

Hash

07f16089e8d2441ee45fca10d60bc73706a257d8a671ff37c1c6576314bdf075

ffa2a6f7ed648f72edcd5a831801775031238400bd820e0d67a854f393dd0f2d

a345df96afef04dc306952628dccc5bb06760c1a4d2959695dcf1b5cb13bb2d4

eaebd076cbcc60548fd5a0d601ffd46b920113826af9ca8a05bce9e00192b064

5cbf9e10e95248156116b4242a3f61efd1baf7b869fddbc05891df3fae2268d6

afe441f6c74a5efc9eb2728cb4440edd35a0d0bcc3bd979210a726b178ecdb0a

Bb847988de11f71d9f8d5001b07c86eedfb9b1647161f11a2366783270bdb256

C2

comnetserv.com

URL:

https[:]//comnetserv.com:8400/https.cab

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

1. **CMTX-P072024964: Critical vulnerability (CVE-2024-37085) in ESXi hypervisors**

ALERT BRIEF:

A critical vulnerability (CVE-2024-37085) in ESXi hypervisors is being exploited by ransomware operators to gain full administrative access on domain-joined ESXi hypervisors. ESXi is a popular bare-metal hypervisor widely used in corporate networks, making it a prime target for threat actors. The vulnerability stems from a default setting that grants full administrative access to the "ESX Admins" domain group without proper validation. Analysts have identified three exploitation methods:

1. Adding a user to the "ESX Admins" group.

2. Renaming any domain group to "ESX Admins" and adding a user to it.

3. Utilizing an existing member of the "ESX Admins" group.

This vulnerability is the latest in a series of ESXi vulnerabilities targeted by threat actors, including the Storm-0506 threat actor and Black Basta ransomware operators.

Recommendations:-

Protect your system by installing the latest VMware security updates, enforcing multifactor authentication (MFA) on all accounts, and removing any MFA exemptions to prevent unauthorized access.

Proactive threat hunting is necessary to investigate alerts related to suspicious group additions, account manipulation, and compromised account activity to quickly identify and respond to potential security threats.

References:-

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505>

<https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/>

1. **CMTX-P072024896: Mirai Botnet Campaign**

Malware Alert Brief:

Mirai botnet targets networked devices running Linux. Mirai primarily focuses on online consumer devices like IP cameras and home routers. It spreads by scanning and exploiting the vulnerable Internet of Things (IoT) devices. Once infected, attackers make the devices a part of their Mirai-based botnet which they use later for conducting DDoS attacks.

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

cnc.gay

plt.got

c.cnc.gay

167.114.58.192

ody.cc

cnc.changeme.com:23

report.changeme.com:23

anything.line.pm:1357

79.110.48.149

murder.getwecked00s.site

45.139.104.237

0033f5f8005311c9c4c604dfcae1c325c13e25d387d508ef09a0d3c46ee1878f

00b1719bcbe8c3d0ac1dbb832f70effef2727fc72341e5d5ded2806471d79efe

01e2398d902788b4588b4989cb9a5754796b745a93ee36cadb50bbd13601b80d

023a49b27d0b741a27487cc730e2289da4170336dc2c106db22e8fa3864d3c02

0475d01daf7a71c6b2848d41874677b213ac2a4424480f9461b3b5c8f88090d8

07187c015807e634dcaf197e31e8cd75a5ba2449fb4f4732071ec3177cb32c1a

083ba1efb00f3b29f6d8039651f70b1675de9989268286a42c3108d24641eade

091c4ef0148bc44478d681335c883f23a563f88aaabf35e593d337da24990071

0a4c287dec0a422532525541789be8816c01f97215a89827dda56bc87973f889

13d4f1418dc39a7c62eba0aa3f7bffffe8520c815fca7323885d5a1d489914a0

141d737bfa524f8f9eac5916254a41de7e2028a4c0ac48c625813d4d1a7e9aff

14bd4fcc884c4c5551cf22fa039f9659b26059c1fed55626594f30c03baaaaae

190575fdf27e02d8a206e80cf921585d5c4cc697626f017068647d40f105c61e

1956bdc9801052595d6eaa3c06a8527650565283ed8ff724547a73c4d9bd7c12

1ead7c0e36daaaf19d8585ee1d139c119956b31de4dae1a97aea4a072a3abdfc

20a578fb2d77275c1534e3ef9855be4cbe6b46212cd0e2f305703068e2b10f52

2113000e737f24d6e493aad01ec3b56faa6c7a5a75e44b3aeabe1ca24bc6496c

25899af171ebc5fde600bf75d7a21b6a3fa7c897beec4c0ae94921d045b92983

27cedeb75c3b1b6e2fa1e50221328842b4d84003d86326e80e24311dbab1b09b

290003fbe8263b9154d8f3b8d1d20d653308aa1d0870abf91973783530a82f46

29b70630adf4ecf9eb1dd5df9899f9542ccb3d7a85af1718f3b97557cce2bcd9

2d1fd93daf8cadaf775a8cd4e21f8b7b1759442bd260eb6dde3aee319adae117

2dc2a80a2efb9645af51f4f46155ea0f892c708893af275eba9124f1f5cbe68f

31ad277c16cdc259497ab5db299c3f87221928a01e76631e8cfb7df26106e417

36be17f7768af170bb9ba3c735358954499c85806a4ee4dbee72aae3194b2f60

36ed7a5fc2d1481cdac140383ff21a418b62ea5eb89f281e02fe88e9ee0efb96

3c43687169bda628f828b3434c3003e26552e6f735cb7c40144ee6ff84abe504

401d789a04c0201b56c4c1dca8aef1a2caa40862b9894a9c804359798b8cd52f

45b65e58acbc62d6f3d6ef963e2073fbbfc74286262c37f926191f2f079ca7e7

4a94fd59ccad0498fb468d55329fe4561e665eb3e0cdad84d2dd6a2981f1dae1

4cb346d4d3d74834a6b0a38e94579004208987b7456182ff8c57211f3eec88b1

4ce9e9ce07fde4d497b2ee41722235d3f1d6c9d2db61e14e4ca051945eeac9c2

4d7dba594f1b1ecc774273f9b123b6a3323e52fe7a0867855c71c209c0451274

4f4b8b2f3d72a132e630d1d291eac52d83c4af83cf995d90df091489b70bd015

50d5adf3fe714dd90ccca2be09a4f2747e59f2ab7062ab1694b32d8229b3b1de

5173d02ba7cbf126a39236469ce63c17a254f4514f7d5eaaf4319849b9df8aa3

51f1f17b881650e8867fcbc946c360b75d247bfa87f93f2475bdeddb43d2d3ac

52bf6f6138431d0b70cb961229157e4fff23860254b5e17a1ffb1824ebbea951

6190f7604c0626659ef32410a6a9c4cb8e4f177ee70280a4dd3ba9846811b360

6229fee20030855f79c1d7cdc46f7bd99c66ab3b5c43231a18cff274f2b0c389

66777076015f1d1cadffc40dd42833cf2c8e39c8af0fb85cfe91c7ab7a345a97

6777759e7eb132e7cb7407fca9b9232f5c3c6670a55c51c45414d7ec76dc6755

6903abd56d3aa8a257873d82078efc6b62f1ede8d4ecbfcecac16ef5284225e4

6dddcfe85776f92e849d5508640b145601a76c9b8198ff7b7f4835a7348852a1

712df663c1dd5bd81a9dd306a60fed7953c8af307105f636473c31b62e92b87a

7159ce8936876604360ceb0b04952a9ca51da613abba85a9ac71ceeffe93c57b

719be1eb8b47ccd3965b2b322779691a41ed4cd05f1b9b7400a26784b58f83ac

73ece8ffa7c0f7f625a070aa3e98d0eb450716927cec046803c8b818bfcbc9d6

784c8c92cca6c853aa6b58dd889a0f9a4c34debe78222484d9d98cc1934666fc

7d601bcda5ade867eaf14c072284230423cf982e16f52dd967deeb4f2b98766f

80a769d76865dd611e66ef156e8d372395d51e456b58effd6d3352e9a63da54e

81deff088c5f1260a9de0d608f79a5381dae89fe931b73f1d6d67180110516fd

932248bb66ac77faa9fd08566d42cfc8c96a3e546b589c10fd5a510b3689ef74

93c4e8e920431c7ce25489f588972ac3519f56ab2a431b1e13156b552ef9b8a2

9766875d82e5599c77c81676dc70a5a8c961969118ffd1290ddc85f6adb0c295

99268a9efed25cea2f19bdab93a45db02e732ff9f83766253c81d7081fb55d02

997dc2c4d2bd168c91372605da660258079498863a3b4cd89b59c28c31da66cf

9c733a9e8b16df61405d68ccea597cbdc4ced0fc4341b33fb2b1fd6a048a445b

9d579e8e7e759e39005c26c765b701f888ac92bb4aec92bdd4dfed214b9d0d05

9f45a29efc1847736dd5c6ecb1be34c68e166ab425dd2a5a2292510f9ba24d0d

a2f3c9e7622b68f6666d3564a8e787062892dbd213211db6d2c22a3fbfd7ae60

a7c2e271ce0e080d41c0ae77f0e8dbc948971f1e7ca4216aa0846e19852cf436

a9e1002039e7461417fcea8207e1fc40f8fd410f8832c95dc8ec433e9bd87446

aad1f6ce22b76840f48ea105dca1e148009efc88bb61e976db71e202da575967

abfab304a3a038fefbe7d9036b114d8444dab674c586e4188f2816b52e3b0250

ace2ca17705685c14550a92213962c018fd59aaf9abe26d08a5cc039afa56a09

ad11b92ed4deed68028f03ddf1015921ddde7bd7ad32c558a94b5c086d447971

aeebf8fc948df5e09d3cfa18af9a1434190aa9df0d8d80b7207581ee10dcb9cd

b30091aa6f51c9010ebf6dec90021adf9324cbe4e4af48019d9f39ad38a7af51

b605d21ddadc2730fca438f3c0fe8ef9f7434c584790f52887557ec2be14884e

ba0d738a8c4874b981d7ee947aca2b9d85bf4541a6bc40bef6b38e5f4ad0e2b8

befaa32a827c2c95d3d7eecce0eac8d7a2577d1d2768379edc4be98b4f6dc5d2

bf56971c99b5814e7b5b279de5e1f52dc4d5d1c882eb205c89d8f43915dc4e99

c6603610d98124953b9b6e4355611cb0588507a8a003aff36771937b43e2acd0

c70cb60d7cf98c639312bfcf14a288134ab6aafd46398fe1282f0d5b29ea56aa

c7cf6499237b2611f00d215353cbade38ac544466632dfa509ef587ca1b08d8d

c8fdfcaf40e1cecd084c2e82a4d42403081a417963aa82bc728cdf2c48e2ae4b

ca5627db65263e9364b0cedae55033104c5ab9329bc8d7d6a15826523e661e90

cbe3077abc42c9e725ee561b8e369c9e5b3819d762d8fa9889b27c1e10dfb8b3

cd5ca0370619259fc385632d34a65107ce8b1c007cf929d8b8d7a61caba89bad

d6017a5b017445b838c47fd50e221040a76da98347d62bdef8f5189e77cf475a

d86d6baecc112f04b102d51e7ae87c75ea3ce9bbe6cab2f4478f3dbfb8b16696

dbac84bdd9a8a03ef51ccef848415b6a51134e7fe7e989c03ede5dc0efc96758

dd8de16eb479f077153fa6e8a55e8df53743dd7ad53233083e830f97c9b2ec37

de5219af868b27a6c6e87a1209f89066de21ea13a465be7ac3c0824195f89651

de7180890f7b637715a40f9ea508ce41e98f4630128a4d6758bbf3006d21ceef

df065b1ec4361ccb97a485a3c56cccd5136621f7d47ee329c700d023c1f789f8

e0359c24f30051f398d82f1fb33074dfd92c5398c430a0212d3dda11d8b9b807

e43ff8806acfb6b6948ceb1d70ae71416b258aa01660b24568f0d8f26186cefd

e461540e87413db101b297145bba8c1b2c96a773830c7d9163452cd9010c86cf

e736083406f59d08530e51a4e510409469845c6957b43aa9ad9877817ebb2013

ea34be57e26322312d30b6ec0c94fe036e9fb85aaf276e83f79ba0e6a5893c62

eb2c0d50d32ebf8d18e82dd780c2432f4010e5dd8f0cc84c04a10f03f8399a6d

f05016d9c95a68cfadd4e354c81809c6feed2ec68ede47da8ab045ff1e77b01a

f453efd6ef97e455a2ec84746952de84144316ef7a64341d877e50c17f155313

f464fa3b519281da4a3eaf90dc0e1c3e4afa382a24ed13984464e50eef3b2b99

f7da370bf9cda4070a9b218091c6accae1e8466c862221593110a092253c4680

fbb3b2954509b6d7e0b40aa5f1b83ef73ee941ff91bc84ebe08fc12692a2cc27

fd0d79cab966d8819b211cc990f7edda5b3b6af1d470131dc8af20d1618d8472

fdc1557aec79bb4ee05ca34ef83a767ba2ef02c656366b220fd4019b522ad83b

fea75216e03adfa13ee6e3d54394fa33680341e6d3094d8c240ff7bb01febc0c

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

1. **CMTX-I-323072024: SideCopy - IOCs of Malware Campaign**

The following domain is malicious and hosting malware associated with Pakistan based SideCopy threat actor:

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

campusportals.in

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

1. **CMTX-I-325072024: Recent IOCs of Malware Campaign**

The following domains are hosting malware:

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

uploadfiles24.online

www.rockcreekdds.com (Compromised domain)

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

1. **CMTX-I-335072024: CrimsonRAT - APT36 campaign**

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

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

new146.duckdns.org

167.160.166.146

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

1. **CMTX-I-901072024: CrimsonRAT- APT36 campaign**

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

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

209.145.48.30

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

1. **CMTX-I-345072024: Suspicious Domains used by Threat Actors**

Following suspicious domains have been registered and may be used by threat actors to host malicious code/malware/spear-phishing website :

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

mod.gov.in.armycases.report

mea.gov.in.armycases.report

armycases.report

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