**Cyber Security Advisories**

**Date: 16 December 2024**

1. **[CMTX-P112024905] CHINESE BASED THREAT ACTOR (APT 19) ACTIVITY (TLP:CLEAR)**

ALERT BRIEF:

APT 19 also known as Deep Panda,Codoso, C0d0so0 and Sunshop Group is a Chinese-based threat group. They use tools such as EMPIRE and BEACON to facilitate their operations.This group has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services, particularly focusing on espionage and intellectual property theft. In order to access shared files over SMB, APT19 uses strategies like lateral movement using legitimate accounts and sophisticated malware deployment, which frequently poses as legitimate software to avoid detection.

The group has been linked to zero-day exploits used in wateringhole intrusions as well as direct spear-phishing activity. The group is associated with other threat actors like APT10 and APT33.

IMPACTS:

APT19 Uses CVE-2021-44228 (also known as "Log4Shell") in a Variety of Products to Install the COLDSTEEL Backdoor.

DISTRIBUTION METHODS:

APT 19 employs a variety of distribution methods to compromise targets, including:

1. Spearphishing Emails: Sending emails with malicious attachments in RTF and XLSM formats

2. Watering Hole Attacks: Compromising websites to infect visitors

3. Strategic Web Compromises: Leveraging vulnerabilities in websites to redirect visitors to attacker-controlled infrastructure

4. Drive-by Downloads: Infecting users' systems by exploiting vulnerabilities in browsers and plugins

MITIGATIONS:

To mitigate the threat posed by APT 19, organizations should:

1. Implement Multi-Factor Authentication (MFA): Enhance security for user accounts.

2. Conduct Regular Security Awareness Training: Educate employees on recognizing phishing attempts and suspicious emails.

3. Keep Systems and Software Updated: Apply patches promptly to address vulnerabilities.

4. Use Advanced Threat Detection Tools: Deploy solutions that can detect and respond to sophisticated threats.

5. Monitor Network Traffic: Regularly review network logs for unusual activity.

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

1. **[CMTX-I-080122024] CrimsonRAT- APT36 campaign [TLP: AMBER]**

Threat Overview

- ------------------------ <META INFORMATION>-----------------------

Confidence- High

Risk- High

TLP:AMBER- Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

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

216.172.103.34

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

1. **[CMTX-P-122024814] Cumulative Suspicious Domains--ALERT5, TLP-RED**

Alert Brief

A set of malicious domains believed to be used by state sponsored threat actors i.e. China and DPRK for targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

download.kaspresksy.com

twitterproxy.com

gloole.net

pro-navor.com

goog1eweb.com

esh.hoovernamosong.com

googlesheet.info

thecloudnet.org

googledriver.net

share.printerjobs.xyz

ppit.microsofts.org

update.microsofts.org

news.petalossccaf.com

ns2.rtsafetech.com

indialifeshop.com

disknxt.com

miscrosofts.com

request.resolverequest.live

ns1.biteupdates.site

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

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

PREVIOUS ALERTS REFERENCE:

[CMTX-P-112024824] Cumulative Suspicious Domains--ALERT4, TLP-RED Dated 29-11-2024

[CMTX-P-112024814] Cumulative Suspicious Domains--ALERT3, TLP-RED Dated 21-11-2024

[CMTX-P-112024794] Cumulative Suspicious Domains--ALERT2, TLP-RED Dated 19-11-2024

[CMTX-P-112024784] Cumulative Suspicious Domains, TLP-RED Dated 14-11-2024

[CMTX-I-512032024] DDNS Domains Targeting Government Organizations Dated 07-03-2024

[CMTX-P302022844] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 29.03.2023

[CMTX-P302022894] BLOCKING OF DYNAMIC DNS Dated 27.03.2023

[CMTX-P-042022976] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 05.04.2022

[CMTX-P40102021] DYNAMIC DNS Increased use in RAT campaigns Dated 21.10.2021

[CMTX-P48072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

[CMTX-P49072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

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

1. **[CMTX-P-122024014] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

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

Indicators of Compromise (IOCs):

IP Addresses: Port

47.243.192.70

45.32.151.206

23.224.37.21

23.224.37.19

96.9.212.107

45.86.162.247

23.224.37.20

45.77.254.133

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

1. **[CMTX-P-122024055] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

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

Indicators of Compromise (IOCs):

IPs: PORT:COUNTRY CODE: LAST SCAN DATE

103.171.34.199

111.68.8.106

149.88.69.156

5.188.34.223

38.60.208.50

166.88.57.79

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

1. **[CMTX-P-122024065] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Impacts:

Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

5.252.178.185

38.54.16.200

101.99.91.218

185.228.92.25

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

1. **[CMTX-808122024] Pakistan Based Malware Campaign**

- ------------------------- <META INFORMATION>-----------------------

Confidence- High

Risk- High

TLP:AMBER- Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

Pakistan-based threat actors have increasingly targeted Indian government agencies/organisations with cyber-espionage campaigns, leveraging phishing, social engineering, and custom malware to steal sensitive information. These attacks often aim to compromise critical infrastructure and gain long-term access to systems for intelligence gathering.

Common Features of Malware Deployed

  > Phishing-Based Delivery: Malware is typically delivered through spear-phishing emails with malicious attachments or links.

  > Data Exfiltration: Designed to steal documents, credentials, and other sensitive data.

  > Persistence Mechanisms: Use of techniques like backdoors, scheduled tasks, autoruns to maintain long-term access.

  > Camouflage: Malware disguised as legitimate files or applications to evade detection.

  > C2 Communication: Use of command-and-control servers to receive instructions and exfiltrate data.

Recent C&C server IPs of malwares deployed by Pakistan-based threat actors are as follows:

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

154.53.42.194

66.219.22.102

144.126.152.205

209.126.6.227

154.38.160.218

167.86.113.241

109.123.244.46

23.88.26.187

209.126.11.251

173.249.7.111

149.102.140.36

130.185.119.198

176.57.184.97

84.247.181.64

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

1. **[CMTX-I-655122024] Malicious Domains used by Threat Actors**

- --------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

  > Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

  > Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

  > Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

  > Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

  > Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

  > Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

  > Implement Multi-Factor Authentication to add a layer of security.

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

indianoil.cn

\*.in.services

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

1. **[CMTX-I-443122024] CrimsonRAT- APT36 campaign**

- ------------------------- <META INFORMATION>-----------------------

Confidence- High

Risk- High

TLP:AMBER- Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

Common Features of APT36 Threat Actor:

  > Spear-Phishing (highly targeted and convincing phishing emails to trick victims)

  > Information Theft (documents, credentials, and personal data)

  > Remote Access

  > Credential Harvesting

  > Data Exfiltration

  > Persistence Mechanisms

Preventive Measures:

  > Be wary of unsolicited emails, especially those with attachments or links

  > Monitoring and logging to detect unusual activities indicating a compromise

  > Multi-Factor Authentication (MFA) for emails

  > Encrypt sensitive data to protect it in case of exfiltration

Recent C&C server of malware deployed by this threat actor is as follows:

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

96.47.234.145

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

1. **[CMTX-P-122024824] Cumulative Suspicious Domains**

Alert Brief

A set of malicious domains believed to be used by state sponsored threat actors i.e. China and DPRK for targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

rokth.kozow.com

apiupdate.theworkpc.com

wopc.theworkpc.com

api.stream-amazon.com

archive.beautydiary.shop

cdn.stream-amazon.com

jihu.duckdns.org

plug.active-microsoft.com

up.active-microsoft.com

up.stream-amazon.com

app.theclooxdd.xyz

apple-update-login-mail.explorate.de

apps.google-jp.com

babblekeep.com

bench-marked.com

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

1. **[CMTX-P-122024834] Cumulative Suspicious Domains**

Alert Brief

A set of malicious domains believed to be used by state sponsored threat actors i.e. China and DPRK for targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

bhtm200.com

api-outlook.com

cdn.agadatacenter.com

cg-fiber.com

dnsseed.bluematt.me

download.time-sync.org

govamazon.com

images.newsdocument.com

img.office-w.com

lbjpay.com

linux1.whoamis.info

list.whoamis.info

longlifetrump.com

microsoftasps.com

microsoftdesktop.com

mircoo.supermirco.us

mitori-net.jp

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

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

PREVIOUS ALERTS REFERENCE:

[CMTX-P-122024824] Cumulative Suspicious Domains--ALERT6, TLP-RED Dated 05-12-2024

[CMTX-P-122024814] Cumulative Suspicious Domains--ALERT5, TLP-RED Dated 03-12-2024

[CMTX-P-112024824] Cumulative Suspicious Domains--ALERT4, TLP-RED Dated 29-11-2024

[CMTX-P-112024814] Cumulative Suspicious Domains--ALERT3, TLP-RED Dated 21-11-2024

[CMTX-P-112024794] Cumulative Suspicious Domains--ALERT2, TLP-RED Dated 19-11-2024

[CMTX-P-112024784] Cumulative Suspicious Domains, TLP-RED Dated 14-11-2024

[CMTX-I-512032024] DDNS Domains Targeting Government Organizations Dated 07-03-2024

[CMTX-P302022844] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 29.03.2023

[CMTX-P302022894] BLOCKING OF DYNAMIC DNS Dated 27.03.2023

[CMTX-P-042022976] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 05.04.2022

[CMTX-P40102021] DYNAMIC DNS Increased use in RAT campaigns Dated 21.10.2021

[CMTX-P48072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

[CMTX-P49072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

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

1. **[CMTX-P-122024844] Cumulative Suspicious Domains**

Alert Brief

A set of malicious domains believed to be used by state sponsored threat actors i.e. China and DPRK for targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

nexcomke.splynx.online

remote-advantage.com

santimetrz.com

saofuwang4.com

second-handgoods.com

securitysuccinct.com

seed.bitcoinstats.com

sitf.net

sqdtsj.com

swaggate.com

tigmarket.casacam.net

topistmall.com

transcom.giize.com

wa-blast.shop

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

1. **[CMTX-P-VUL-1220243315] Prominent Vulnerability List**

CERT-In has compiled a list of vulnerabilities reported and exploited recently for due consideration and prioritization.

1. **[CMTX-P-122024105] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

|  |
| --- |
| Indicators of Compromise (IOCs): |
| IPs: Ports |
| 148.66.5.50 |
| 148.66.5.53 |
| 103.171.34.199 |
| 148.66.5.54 |
| 148.66.5.52 |
| 148.66.5.51 |
| 111.68.8.106 |
| 38.60.208.50 |
| 5.188.34.223 |
| 161.97.107.93 |
| 45.128.153.73 |
| 134.122.133.80 |
| 2.58.14.134 |
| 166.88.57.79 |
| 149.88.69.156 |

1. **[CMTX-P-122024205] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Impacts:

Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

5.252.178.185

149.28.128.65

103.85.25.166

149.28.146.215

38.54.16.200

101.99.91.218

94.131.119.167

64.31.63.110

185.228.92.25

149.28.159.61

136.244.116.245

64.176.49.76

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

1. **[CMTX-I-554122024] Malicious Domains used by Threat Actors**

- ---------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

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

www.jcb-drdogov.in.net

www.email.gov.in.mailindia.one

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

1. **[CMTX-P122024704] Guptiminer Malware**

Alert Brief:

Guptiminer is a highly sophisticated malware campaign attributed to North Korean state-sponsored cyber actors. It is used by attackers to distribute backdoors and XMRig cryptocurrency miners within victim networks. The malware is typically delivered through phishing emails, malicious websites, or by exploiting vulnerabilities in outdated software.

IMPACTS:

• System Performance Degradation: The mining activity consumes substantial computational power, which can slow down the infected machines, cause overheating, and reduce the lifespan of hardware components.

• Security Concerns: Beyond mining, the malware can potentially open the door for further attacks, such as data exfiltration, espionage, or even ransomware deployment. The persistence and stealthy nature of Guptiminer can allow other malware to be deployed on the same compromised systems.

Threat Type: MALWARE

Severity: High

Technical Details:

Attacker behind Guptiminer Malware employs a man-in-the-middle (MitM) attack to replace legitimate software packages with malicious payloads. Guptiminer utilizes advanced techniques like DNS manipulation, DLL side loading, and embedding malicious payloads in image files to evade detection.

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

IP: Port

98.142.254.216

37.0.12.55

185.230.64.218

185.248.163.233

79.141.165.25

193.42.36.158

82.117.255.26

103.249.84.136

146.70.145.185

95.164.10.164

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

1. **[CMTX-I-633122024] Malicious Domains used by Threat Actors**

- ----------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

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

www.centralgov.info

delhipolicegov.inh.no

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

1. **[CMTX-P-122024775] DOGCALL MALWARE**

Threat Overview:

Dogcall RAT (also known as RokRat), is a sophisticated Remote Access Trojan (RAT) used by the North Korean threat group APT37 (also known as Reaper, Inky Squid, RedEyes, ScarCruft).It leverages social engineering techniques like spear-phishing etc to deploy malware. It has been employed in targeted cyber espionage campaigns primarily against South Korean government, military organizations, journalists, activists, and North Korean defectors. The malware employs multi-stage infection chains, often initiated via oversized Windows Shortcut (LNK) files disguised as legitimate documents or embedded within malicious Hangul Word Processor (HWP) files and utilizes legitimate cloud services for command-and-control purposes to evade detection. It has also been reported that it uses cloud storage APIs like pCloud, Dropbox, and Yandex, and is capable of capturing screenshots, logging keystrokes, and evading analysis with anti-virtual machine detections.

Impacts:

Dogcall RAT can have severe impacts, including:

1). Data Exfiltration: Stealing sensitive information such as login credentials, communication data, and browser data.

2). Keylogging: Logging keystrokes to capture sensitive information

3). Screen Capture: Capturing screenshots of the victim's machine

4). Audio Capture: Recording audio from the victim's microphone

5). File Manipulation: Downloading and uploading files on the victim's system

6). Credential Harvesting: Stealing credentials stored in web browsers and Windows Credential Manager

Threat Type: Malware

Severity: High

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

Indicators of Compromise (IOCs):

HASHES:

358122718ba11b3e8bb56340dbe94f51

936888d84b33f152d39ec539f5ce71aa

c811d0fd97bf3b5e3c69ca8a7ff2aac3

804a8c076b4aaa2e21ab4f06453d1c4e

12dd4814056582a6b6dc90920e3a8913

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

1. **[CMTX-I-588122024] Threat Actors Using Legitimate Web Services/APIs for Data Exfiltration**

- -----------------------------<META INFORMATION>------------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

- ---------------------------<SHA1 Hashes>-----------------------

998f8ebecf89612d486522f168cc8f8ba67bdd7c

6f1a8ab4a2ab6d00fed67ef802573bd9635363c3

b7751a4a1d595df34783ad22898e0c28fccb2886

ccce17e5e24daa3e07167c16eb8f1fdc0b843ca7

70a4fc6db6b65c300cc45abea681f06d9daeb18f

fce13fed9387035f72c9bd9346a0501c57ec463e

- ------------------------- </SHA1 Hashes>----------------------

Additional domains for other cloud/ API services to be MONITORED for malware exhibiting similar TTPs:

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

api.telegram.org

telegram.org

discord.com

discord.com/api/

api.slack.com

slack.com

api.dropboxapi.com

dropboxapi.com

api.dropbox.com

dropbox.com

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

1. **[CMTX-I-328122024] Malicious Domains used by Threat Actors**

- -----------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

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

rbi-gov.info

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

1. **[CMTX-P-122024885] Exfiltration Risk from PowerSCP Stealer**

Threat Overview:

PowerSCP Stealer is a PowerShell-based credential stealer specifically targeting Windows systems. Upon execution, PowerSCP Stealer downloads SSH/Utility Download, creates SSH key pair and sets the SSH Key Access Control.

The malware also performs port scanning, port selection, creates persistence and exfiltration of  data from victim machine. Stealer exploits the Secure Copy Protocol (SCP) for data exfiltration and uses deceptive password prompts to collect valid windows login credentials.

Stealer validates the credentials before sending them to its command-and-control (C2) server. This validation ensures that only verified credentials are exfiltrated, enhancing its utility for further malicious activities like second-stage malware deployment or credential broker transactions.

Impacts:

Credential Theft: Successful credential exfiltration can lead to unauthorized access to sensitive systems.

System Compromise: The malware can facilitate further attacks, including secondary malware deployment.

Data Breach: Organizations may face data breaches that can damage their reputation and financial standing.

Threat Type: Malware

Severity: High

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

Indicators of Compromise (IOCs):

IP

185.255.178.85

HASHES

7ff6e1696b4e9a247041e9d1b37120c7ef0671eb69b832d0c19fefc1088d53e2

facd14a7014e3a7d87955ed0be09e11df31d107ec58b7b53f6d7dae1b4a85cd4

2d046eb280238dfa5fbe15d0c3e0dfbde38bfcec7ee8b8b51e9887c840009842

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

1. **[CMTX-P122024995] Active Exploitation of a Critical Flaw (CVE-2024-50623) Affecting CLEO's File Transfer Products**

ALERT BRIEF:

A critical vulnerability, classified as "Unrestricted Upload of File with Dangerous Type" and tracked as CVE-2024-50623, has been discovered in Cleo's file transfer products, including Cleo Harmony, VLTrader, and LexiCom. This vulnerability allows unauthenticated remote code execution due to the lack of restrictions on file uploads.

Attackers are exploiting this weakness to upload malicious files to the autoruns/ subdirectory of the affected program, enabling them to automatically execute their payloads. The exploitation of this vulnerability has been linked to several malware families, including Safepay and Termite Ransomware.

Threat Type: Vulnerability

CVE-2024-50623

CVSS SCORE-5.3

Annexure CERTIn-Threat Intelligence ID- [CMTX-P-122024995]

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

Indicators of Compromise (IOCs):

Malicious File Location (check installation directory of Harmony/VLTrader/Lexico)

Cleo####.jar (ex: [cleo.5264.jar/cleo.6597.jar](http://cleo.5264.jar/cleo.6597.jar) etc)

hosts/main.xml file or a hosts/60282967-dc91-40ef-a34c-38e992509c2c.xml

IP Address

185.181.230.115

80.67.5.133

5.181.158.25

185.162.128.133

184.107.3.70

195.123.224.8

184.107.3.196

176.123.5.126

5.149.249.226

185.181.230.103

209.127.12.38

181.214.147.164

192.119.99.42

1. **[CMTX-I-890122024] Malicious Domains used by Threat Actors**

- ------------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

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

www.the-night-of-travestie.de

(currently resolving to 89.107.186.220)

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

1. **[CMTX-I-122024871] Malicious Domains used by Threat Actors**

- ------------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

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

indianairforce.website

www.indianairforce.nia.in

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

1. **[CMTX-P-VUL-1220240015] Prominent Vulnerability List**

CERT-In has compiled a list of vulnerabilities reported and exploited recently for due consideration and prioritization.

1. **[CMTX-P-122024854] Cumulative Suspicious Domains--ALERT10, TLP-RED**

Alert Brief

A set of malicious domains believed to be used by state sponsored threat actors i.e. China and DPRK for targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

cdn.imango.ink

cisco.893yakuza.com

com.updatesrvers.org

mail.whoamis.info

poer.whoamis.info

tools.daji8.me

www.whoamis.info

www.aihkstore.com

icw.imiul.com

randzalo.com

finisherrebuilt.net

adfs.updatesrvers.org

cdn.d22.me

club.01010555.com

d22.me

dar515.top

diplom77hj.com

mgm4adminsi.com

mlcorsoft.xyz

paloaltonetworkhelp.com

www.amazonbuypro.com

www.cementbridge.com

www.paloaltonetworkhelp.com

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

PREVIOUS ALERTS REFERENCE:

[CMTX-P-122024844] Cumulative Suspicious Domains--ALERT9, TLP-RED Dated 05-12-2024

[CMTX-P-122024834] Cumulative Suspicious Domains--ALERT8, TLP-RED Dated 05-12-2024

[CMTX-P-122024844] Cumulative Suspicious Domains--ALERT7, TLP-RED Dated 05-12-2024

[CMTX-P-122024824] Cumulative Suspicious Domains--ALERT6, TLP-RED Dated 05-12-2024

[CMTX-P-122024814] Cumulative Suspicious Domains--ALERT5, TLP-RED Dated 03-12-2024

[CMTX-P-112024824] Cumulative Suspicious Domains--ALERT4, TLP-RED Dated 29-11-2024

[CMTX-P-112024814] Cumulative Suspicious Domains--ALERT3, TLP-RED Dated 21-11-2024

[CMTX-P-112024794] Cumulative Suspicious Domains--ALERT2, TLP-RED Dated 19-11-2024

[CMTX-P-112024784] Cumulative Suspicious Domains, TLP-RED Dated 14-11-2024

[CMTX-I-512032024] DDNS Domains Targeting Government Organizations Dated 07-03-2024

[CMTX-P302022844] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 29.03.2023

[CMTX-P302022894] BLOCKING OF DYNAMIC DNS Dated 27.03.2023

[CMTX-P-042022976] DYNAMIC DNS (DDNS) DOMAINS used in Malware Campaigns Dated 05.04.2022

[CMTX-P40102021] DYNAMIC DNS Increased use in RAT campaigns Dated 21.10.2021

[CMTX-P48072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

[CMTX-P49072021] Increased DYNAMIC DNS use in APT/ Malware Campaigns URGENT Dated 20.07.2021

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

1. **[CMTX-P-122024905] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Impacts:

Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IPs: PORTS

38.60.212.8

207.246.119.197

185.167.61.85

95.179.221.218

199.247.2.134

103.56.19.182

8.218.25.58

139.84.139.121

107.148.37.16

154.205.145.210

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

1. **[CMTX-P-122024915] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs):

IPs: PORTS

103.47.224.142

156.251.17.206

38.54.105.187

167.179.89.246

107.155.56.15

108.61.223.127

107.155.56.4

45.32.248.110

107.155.56.87

185.239.226.65

45.142.166.112

158.247.252.115

2.58.14.121

192.248.166.186

154.90.47.123

38.54.40.60

45.80.215.133

5.34.176.124

103.200.97.150

172.94.9.12

43.226.229.35

110.50.48.232

207.148.126.75

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

1. **[CMTX-I-020122024] CrimsonRAT- APT36 campaign**

- -------------------------- <META INFORMATION>-----------------------

Confidence- High

Risk- High

TLP:AMBER- Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

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

94.177.123.112

getsecurechat.com

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

1. **[CMTX-I-007122024] Malicious Domains used by Threat Actors**

- ---------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

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

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

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

certin.online

indian.army.be

www.pmjay.gov.in.crsor.live

pahchanindia.xyz

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

1. **[CMTX-P-122024178] Relay server Nodes used by Chinese actors**

- - ------------------------ <META INFORMATION>----------------------------

Confidence- High

Risk- High

(TLP-RED): No disclosure; recipients cannot spread this information to anyone, but in case of a meeting TLP-RED information is limited to those present in the meeting.

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

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest.  In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

Indicators of Compromise (IOCs):

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

IP ADDRESSES

1.22.124.190

1.22.44.234

103.157.238.251

103.171.40.154

103.172.97.15

103.211.36.165

103.211.39.110

103.216.236.100

103.224.245.22

103.229.26.5

103.246.62.34

103.3.228.82

103.44.97.109

103.48.199.195

103.6.157.53

103.70.128.18

103.87.58.48

103.96.16.246

103.98.85.246

106.222.204.147

106.222.205.31

110.227.205.171

112.196.6.238

116.206.222.44

117.211.9.4

117.221.65.8

117.252.10.178

122.164.12.195

14.142.239.2

14.195.204.66

182.71.103.226

182.74.138.66

202.179.83.149

202.191.65.86

223.29.203.138

27.116.48.45

38.137.59.48

45.115.168.14

45.115.168.35

45.115.168.71

49.205.176.25

49.36.83.173

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

1. **[CMTX-P-122024935] PHPsert Web shell**

Threat Overview:

PHPsert is a PHP-based web shell used by China based threat actors in their cyber espionage campaign. PHPsert web shell uses various code obfuscation techniques, including XOR encoding, hexadecimal character representation, string concatenation, and randomized variable names for evading static analysis and detection.

Capabilities of PHPsert:

• Capability to retrieve the attacker-provided PHP code from attacker controlled server.

• Execute the payload downloaded from attacker controlled server.

• Keep changing its variant by doing minor differences in their implementation.

Annexure

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

Indicators of Compromise (IOCs):

HASHES:

2e2cf8a4a0e7decceb8e22536b13173479da0d13

3035d8846d7a9f309f2d24daba6ac33ad99524fc

399776991a094e1ee78b2a915bf4491e67c04ec7

3a688c844259822c51ceb3aea508303c4a654eb3

4d6947a19dd9a420c22fee39fac8b4df95a47569

63cea28d927f8e629377399fa08a9cb4fd0c6238

6549e50645bb1c02e4972651d335a75cb6d5aa74

83ca53c95705352ff60149b0b17a686956e23172

b2811cb4d0afe13d2722093039a72588c348dcfd

c0e03fce8f7f51e91da79f773aa870f0897b0ee2

cb6726fb3f7952ede04ed22d2c72389255991827

d57fa43944676c56e66f4b20ffa3d82048e354fd

IP

185.76.78.117

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

1. **[CMTX-I-122024874] IOAs of suspicious domains**

- ----------------------------------<META INFORMATION>----------------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.

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

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

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

app.joinindianarmy.in

careerindianairforce.cdse.in

indianairforce.afcat.in

join.indian.navy.in

joinindianarmy.in

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