**Cyber Security Advisories**

**Date: 31 January 2025**

1. **[CMTX-P012025505] ACTIVE EXPLOITATION OF A ZERO DAY VULNERABILITY AFFECTING FORTINET's PRODUCTS**

VE-2024-55591 is a critical authentication bypass vulnerability affecting FortiOS and FortiProxy systems, allowing remote attackers to gain super-admin privileges. It exploits an alternate path or channel vulnerability, enabling unauthorized access to firewall management interfaces.

This flaw has been linked to a series of cyberattacks targeting organizations with exposed firewalls on the public internet.For successful exploitation of the vulnerability,  the adversaries use a technique known as DCSync to retrieve credentials for lateral movement by utilizing the SSL VPN access.

IMPACTS:

The exploitation of CVE-2024-55591 can result in:

1. Unauthorized administrative logins to firewall management interfaces.

2. Creation of super admin and local user accounts by attackers.

3. Configuration changes, including modifications to firewall policies.

4. Establishment of unauthorized SSL VPN portals for illicit access.

5. Potential lateral movement within networks using compromised credentials.

6. Increased risk of data breaches and network infiltration.

7. Disruption of organizational operations and services.

8. Financial and reputational damage to affected organizations

AFFECTED VERSIONS:

The following versions of FortiOS and FortiProxy are impacted:

FortiOS: Versions 7.0.0 through 7.0.16 (Upgrade to 7.0.17 or above)

FortiProxy: Versions 7.0.0 through 7.0.19 (Upgrade to 7.0.20 or above) and 7.2.0 through 7.2.12 (Upgrade to 7.2.13 or above)

Threat Type: Vulnerability

CVE-2024-55591

CVSS SCORE- 9.6

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

1. **[CMTX-P-012025805] 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

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P-012025805]

Indicators of Compromise (IOCs):

IPs: PORTS

172.105.40.129

45.77.153.108

149.28.159.61

64.176.226.182

52.194.253.134

43.246.208.207

89.106.207.114

64.176.35.214

156.244.6.144

185.228.92.43

213.182.204.142

149.28.128.65

45.77.170.149

156.238.243.171

194.126.202.217

38.54.15.132

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

1. **[CMTX-P-012025705] 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

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P-012025705]

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

Indicators of Compromise (IOCs):

IP Addresses: Ports

103.107.104.61

85.90.217.44

64.176.65.165

69.172.75.148

5.8.33.81

5.188.190.39

14.128.54.54

119.28.69.128

118.107.44.132

45.76.147.80

118.107.44.134

47.243.192.70

118.107.44.133

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

1. **[CMTX-P-VUL-0120257715] Prominent Vulnerability List**

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

File Name: vuln list\_17012025.pdf

SHA256: 532a13a57a97f99f5a5f072d3c7cb8b424dd880ba0902e4fcd145a3605015762

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

1. **[CMTX-I-808012025] 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>---------

smtpmail.ongc.info

hindustanpetroleum.co

ongcindia.org

pay.benefitstrsgov.info

email.benefitstrsgov.info

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

1. **[CMTX-I-344012025] 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.

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

APT36 a.k.a. Transparent Tribe is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defence, and military targets. Malware deployed by attackers can 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

Prevention 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 IP of malware deployed by this threat actor is as follows:

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

176.56.238.177

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

Network administrators may take required action against the above IPs.

1. **[CMTX-I-563012025] 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>---------

aamantran.mod.gkv.in

sancharsaathi.com

sancharsaathi.com

sancharsaathi.fov.in

sancharsaathi.gob.com

sancharsaathi.goov.in

sancharsaathi.gvo.in

sancharsaathideac.com

tafcop.sancharsaathi.govn.com

tafcopsancharsaathi.com

img.tafcop.sancharsaathi.dov.in

notexistssancharsaathi.ogv.in

sancharsaathi.goov.in

sancharsaathi.govn.com

sancharsaathi.gvo.in

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

1. **[CMTX-I-024012025] 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 CrimsonRAT malware deployed by this threat actor and the domain hosting the malicious file are as follows:

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

185.211.5.76

154.38.175.75

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

1. **[CMTX-I-026012025] 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>---------

www.email.gov.in.departmentofdefence.cc

indianrailway-gov.info

www.serviceonline.gov.in.cscvle.space

www.esewa.punjab.gov.in.certificateverificationfromqr.in

\*.departmentofdefence.cc

\*.gov.in.cscvle.space

\*.gov.in.certificateverificationfromqr.in

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

1. **[CMTX-I-065012025] 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>-------------

bharatpetrolium.in

indianoil.co.uk

coalindiaoffiselectionunit.com

hindusthanpetroleum.com

hindustanpetroleum.co

sancharsaathi.in

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

1. **[CMTX-I-390012025] 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>-------------

cbigovt.com

dc.crsorgi.gov.in.viewcertificate.in

eolakh.gujarat.gov.in.viewcertificate.in

gujarat.gov.in.viewcertificate.in

gov.in.viewcertificate.in

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

Network administrators may take required action against the above malicious domains.

1. **[CMTX-P-012025855] 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

101.36.106.114

116.62.194.46

119.28.1.231

121.43.186.132

45.142.166.112

42.99.117.95

45.142.166.112

42.99.117.95

118.193.35.61

118.193.35.61

121.43.186.132

116.62.194.46

121.43.186.132

8.209.221.211

116.62.194.46

118.193.35.61

101.36.106.114

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

1. **[CMTX-P-012025865] 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):

IP Addresses :Port

43.159.37.130

108.61.217.45

149.248.18.243

98.98.205.17

43.159.37.130

103.27.111.247

43.159.37.130

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

1. **[CMTX-I-891012025] IOCs of China-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.

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

With reference to previous alerts:

CMTX-I-512032024 dated 07/03/2024

CMTX-I-808082024 dated 06/08/2024

CMTX-I-020092024 dated 11/09/2024

Linux based malware is often packaged in the Executable and Linkable Format (ELF), is designed to target and exploit vulnerabilities in Linux operating systems. ELF malware can range from basic trojans and worms to sophisticated rootkits and ransomware. It poses significant risks to servers, IoT devices, and other systems running Linux, often aiming to steal data, create botnets, or disrupt operations.

- -------------< C&C Domain and IP>---------

anywheres.run.place

appupdate.my-router.de

appupdate.firewall-gateway.de

appsupport.my-router.de

192.109.228.147

45.142.155.110

45.142.155.113

135.181.243.34

164.132.27.225

194.126.202.217

192.51.188.47

203.159.95.7

172.252.59.191

141.94.250.144

45.142.155.117

65.20.101.19

95.179.223.245

- -------------</C&C Domain and IP>---------

1. **[CMTX-P-012025478]  Nnice Ransomware**

Threat Overview

Nnice is a type of ransomware that encrypts files on Windows systems, making them inaccessible without a decryption key. After compromising the victim's machine, the attacker escalates privileges and steals credentials, web session cookies, and other sensitive data before proceeding to encrypt the files. The ransomware adds the ".xdddd" extension to the original filenames and leaves a ransom note titled "Readme.txt" with instructions for recovery. The attackers' main goal is financial gain, demanding ransom payments for the decryption key. Nnice primarily targets industries with valuable data, such as healthcare, finance, and government sectors.

Distribution Method:

Phishing emails or via exploiting the known vulnerable Public applications

Type: Ransomware

Severity: High

Affected Systems: Windows

Indicators of Compromise (IOCs):

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

HASH

4dd08b0bab6f19d143cca6f96c8b780da7f60dbf74f1c16c3442bc9f07d38030

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

1. **[CMTX-I-044012025] 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.

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

joinindianarmy.cadc.in

pcdaopune.gov.in.webmailnic.army

pcdaopune.gov.webmailnic.army

www.pcdaopune.gov.webmailnic.army

www.pcdaopune.gov.in.webmailnic.army

nicemail.cfd

joinindianarmy.cadc.in

gail.cv

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

1. **[CMTX-P-012025488] J-magic Malware Campaign**

Threat Overview

A stealthy malware campaign known as "J-magic" has been reported, targeting Juniper enterprise-grade routers, many of which are configured as VPN gateways. The attackers deploy a J-magic agent on the affected router, disguising it as "JunoscriptService" to blend in with legitimate processes. Once installed, J-magic quietly monitors for five specific "magic packet" conditions. When the right conditions are met, it triggers a reverse shell connection to a remote IP and port specified in the packet.

Capabilities:-

• Detect debuggers and Deletes files, directories.

• Enumerates files, directories and running processes.

• Delays execution, Monitors network traffic, Establishes connections to the remote IP.

Affected Systems: - Juniper enterprise-grade routers many used as VPN gateways.

Preventive Measures:

• Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.

• Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats. A list of recent malware hashes are provided in Annexure.

• Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.

• Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts to add an additional layer of security.

–––––––––––––––––––––––––––––––––––––––––––––––––––––––

Indicators of Compromise (IOCs):

Hash

5e3c128749f7ae4616a4620e0b53c0e5381724a790bba8314acb502ce7334df2

IP Addresses

157.90.212.53

130.61.173.116

85.30.131.60

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

1. **[CMTX-P-012025498] Murdoc Botnet Campaign**

Threat Overview

The Murdoc Botnet, a variant of Mirai malware which targets IoT devices such as AVTECH cameras and Huawei HG532 routers by exploiting vulnerabilities (CVE-2024-7029 and CVE-2017-17215) and using shell scripts for malware download and execution, connecting to C2 servers for instructions. Its primary goal is to create a network of compromised devices for conducting Distributed Denial of Service (DDoS) attacks.

Capabilities:-

• Gather System Information: - Retrieve system network information, active TCP packets and Change its process name.

• Shell Script Execution: Once access is gained, it uses shell scripts to download and execute the malware.

• Command-and-Control Communication: The botnet connects to C2 servers to receive instructions and updates.

• Distributed Denial of Service (DDoS) Attacks: It can launch powerful DDoS attacks to overwhelm and disrupt targeted systems and services.

• Proxy Services: It can enable proxy services, making it harder to trace the origin of the attacks.

• Malware Updates: The botnet can update itself with new malware variants to stay ahead of security measures.

Initial Access: - Exploit the known vulnerabilities Present in AVTECH AVM1203 IP cameras (CVE-2024-7029) and Huawei HG532 devices (CVE-2017-17215)

Affected Systems: - IoT Devices (AVTECH cameras, Huawei HG532 routers).

Preventive Measures:

• Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.

• Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats. A list of recent malware hashes are provided in Annexure.

• Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.

• Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts to add an additional layer of security.

–––––––––––––––––––––––––––––––––––––––––––––––––––––––

Indicators of Compromise (IOCs):

Hash

e127153563c1e9352067e94b28687828514734d583ca6bd89ad6e9b01be46170

69405c640e224c981555509bd088ef759c584228f989e46d89e83483f9c2e4b7

IP

94.154.33.42

Domain

phhfr59rqd.parody

hsjupldf2z.pirate

9wg0dstmud.pirate

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

1. **[CMTX-I-180012025] SideCopy- C&C of 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.

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

SideCopy is a Pakistan based, sophisticated threat actor known for deploying malware to target individuals and organizations, particularly India based. Named for its technique of mimicking other well-known attack patterns, SideCopy aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems.

Common Features of SideCopy 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

Prevention 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

Latest Command & Control (C&C) IP and compromised domain used by this threat actor are as follows:

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

154.38.175.83 (C&C)

wallkings.in (compromised domain)

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

1. **[CMTX-I-765012025] 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.

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

cybercrimegov.info

depofgov.info

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

1. **[CMTX-I-680012025] Linux Malware C&C IP**

- ---------------------- <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.

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

Linux based malware is often packaged in the Executable and Linkable Format (ELF), is designed to target and exploit vulnerabilities in Linux operating systems. ELF malware can range from basic trojans and worms to sophisticated rootkits and ransomware. It poses significant risks to servers, IoT devices, and other systems running Linux, often aiming to steal data, create botnets, or disrupt operations.

Prevention Measures:

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

    Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.). ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command)

    Principle of least privilege

    Firewall and network security along with regular OS updates

Recent C&C server IP of malware targeting government officials using Linux based system is as follows:

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

176.65.141.63

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

1. **[CMTX-I-356012025] 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>-------------

adhar.birthprintportal202.xyz

api.birthprintportal202.xyz

printportal.birthprintportal202.xyz

uidai.gov.in.birthprintportal202.xyz

www.adhar.birthprintportal202.xyz

www.api.birthprintportal202.xyz

www.printportal.birthprintportal202.xyz

www.uidai.gov.in.birthprintportal202.xyz

dc.csrorgi.gov.in.phpe.site

dc.csrorgi.gov.in.web.phpe.site

mail.dc.csrorgi.gov.in.phpe.site

mail.dc.csrorgi.gov.in.web.phpe.site

mail.rudraportal.phpe.site

rudraportal.phpe.site

www.dc.csrorgi.gov.in.phpe.site

www.dc.csrorgi.gov.in.web.phpe.site

www.rudraportal.phpe.site

\*.birthprintportal202.xyz

\*.phpe.site

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

1. **[CMTX-P-VUL-012025518] Prominent Vulnerability List**

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

File Name: Prominent\_Vulnerability\_List\_29012025.pdf

SHA256: 9a1a4f52ae2adf9ba1fc8c61a61e4bba0bd4769c22e148389054c2724d466f74

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

1. **[CMTX-I-975012025] 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>-----------

172.86.109.207

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

1. **[CMTX-I-634012025] 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>-------------

indianarmy.nico.in

nicmail.nico.in

niconline.nico.in

odishalandrevenue.nico.in

ojspm.raj.nico.in

raj.nico.in

shop.nicmail.nico.in

www.cara.nico.in

www.indianarmy.nico.in

cara.nico.in

cbseitms.nico.in

hpkv.hp.nico.in

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

1. **[CMTX-I-375012025] Malicious Domains used by Threat Actors [TLP:AMBER]**

- ---------------------------------------<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.

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>-------------

email.gov.in.departmentofdefence.link

bnd.ndmc.gov.in.viewcrt.info

\*.departmentofdefence.link

\*.viewcrt.info

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

1. **[CMTX-I-201012025] 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.

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 CrimsonRAT malware deployed by this threat actor and the domain hosting the malicious file are as follows:

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

45.61.158.240

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

1. **[CMTX-P-012025744] 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

146.70.113.134

96.9.210.77

65.20.81.66

47.128.66.207

38.54.105.96

43.228.126.122

103.69.194.227

182.60.11.201

34.31.178.96

47.98.177.117

107.189.28.92

49.235.170.73

188.120.254.229

156.238.243.161

107.172.21.113

3.227.184.192

49.113.74.215

1.14.104.62

45.64.52.30

8.210.146.82

52.232.197.207

8.155.8.190

54.186.132.100

1.94.22.254

111.231.145.137

1.94.175.252

27.106.122.172

20.106.233.97

66.70.202.83

34.121.122.172

23.249.28.111

43.200.42.167

45.145.229.103

3.96.152.179

129.226.213.170

164.92.250.100

101.37.13.119

195.100.198.220

111.229.193.40

39.97.52.57

4.197.169.184

23.163.0.90

149.248.17.199

43.136.99.149

121.127.33.25

182.60.5.9

13.59.178.90

47.236.98.169

118.89.66.70

51.195.219.100

115.120.242.123

117.215.247.241

23.152.0.81

188.166.121.117

117.72.74.16

207.180.224.247

45.152.65.65

195.189.96.70

170.64.158.181

198.7.121.101

51.89.224.171

195.14.123.88

37.114.55.137

113.45.132.242

77.223.100.85

161.35.218.205

34.60.185.224

121.43.151.165

106.75.251.38

49.233.169.129

149.104.26.229

123.60.1.127

164.215.103.23

116.196.120.131

139.9.65.87

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

1. **[CMTX-P-012025865] 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):

IP Addresses

45.116.78.250

104.143.38.196

49.232.93.226

80.87.206.175

64.23.213.61

54.186.132.100

123.11.255.4

43.156.95.75

107.173.118.149

18.237.245.78

182.255.44.86

8.155.8.190

152.42.198.168

1.14.104.62

23.27.12.214

1.94.22.254

120.79.86.98

47.243.13.249

35.88.59.138

194.233.73.173

185.235.167.143

8.210.9.166

116.196.120.131

52.232.197.207

152.89.92.204

20.115.66.63

145.131.8.169

159.223.242.185

18.231.172.87

47.236.98.169

124.220.133.70

45.204.212.245

161.35.218.205

43.200.42.167

182.60.5.9

47.90.208.22

159.223.242.185

54.176.66.101

149.210.143.97

27.106.122.172

34.219.143.252

43.143.130.124

107.172.159.50

54.176.66.101

123.60.1.127

47.115.200.80

38.54.105.96

117.50.184.22

103.101.204.67

52.53.207.84

49.235.170.73

182.60.11.201

18.234.143.128

57.181.244.184

139.224.198.190

16.171.27.214

194.171.96.118

154.31.221.204

8.217.200.158

37.114.55.137

172.105.27.15

188.120.254.229

8.138.155.217

101.43.62.241

182.60.5.9

52.15.80.186

3.68.92.103

84.32.131.58

121.43.166.96

51.89.224.171

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