**Cyber Security Advisories**

**Date: 28 February 2025**

1. **[CMTX-P-012025864] 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

195.208.174.240

74.207.235.197

172.104.164.141

62.109.30.217

3.227.184.192

39.98.204.142

188.166.121.117

101.133.172.90

13.245.162.103

18.254.144.4

123.31.24.140

1.94.175.252

124.222.57.94

3.96.152.179

152.136.128.162

65.0.26.137

119.45.21.130

67.219.111.218

152.42.198.168

113.44.78.183

47.99.176.66

149.88.78.49

94.156.167.51

62.234.65.53

43.136.20.206

43.134.38.211

121.43.151.165

101.35.228.105

65.20.81.66

27.124.53.34

39.97.52.57

156.238.243.161

172.105.27.15

157.245.146.223

52.73.128.242

107.172.21.113

116.205.118.94

182.60.5.9

146.70.113.134

124.70.193.76

182.60.5.9

150.158.152.209

77.223.100.85

175.27.229.102

139.9.65.87

54.185.190.255

13.59.178.90

34.60.185.224

154.38.167.90

185.158.94.217

195.189.96.70

43.134.38.211

149.248.17.199

47.116.64.160

149.248.17.199

16.163.127.230

67.219.111.218

1.13.195.134

129.226.213.170

47.237.86.35

66.70.202.83

110.40.134.37

117.215.247.241

113.45.132.242

46.8.237.108

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

1. **[CMTX-P-012025754] 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

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

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

Indicators of Compromise (IOCs):

IP Addresses

18.254.144.4

47.120.37.153

45.204.212.245

3.15.21.172

101.201.37.74

107.172.157.80

16.163.127.230

164.92.65.135

175.178.123.40

124.220.133.70

18.234.143.128

142.171.133.69

192.227.227.198

67.219.111.218

148.135.35.239

43.134.118.131

175.27.229.102

45.92.9.110

47.97.114.229

80.79.4.177

162.212.154.121

52.53.207.84

13.245.162.103

84.32.131.58

57.181.244.184

116.205.118.94

34.67.231.17

47.112.118.101

51.84.67.174

18.231.172.87

47.119.182.115

46.8.237.108

137.184.67.135

185.235.167.122

87.106.44.241

209.97.188.10

51.15.224.30

154.31.221.204

149.104.24.149

20.8.97.47

8.138.155.217

1.13.195.134

124.70.193.76

45.116.78.250

43.143.246.38

94.156.167.51

47.120.22.59

47.94.143.32

119.45.21.130

149.248.17.199

172.104.164.141

139.224.198.190

121.36.194.30

47.245.14.36

43.154.105.145

138.197.156.131

182.60.11.201

44.222.186.172

152.136.128.162

39.101.205.127

74.207.235.197

156.244.31.115

182.60.5.9

82.148.31.69

152.42.198.168

20.8.97.44

145.131.8.169

124.222.57.94

102.117.168.67

13.66.164.102

103.101.204.67

18.231.172.87

101.43.62.241

47.116.64.160

43.136.20.206

212.51.144.135

182.60.11.201

135.125.9.127

44.203.248.108

182.60.11.201

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

1. **[CMTX-PN-012025558] CL-STA-0048 Campaign**

Alert Brief:

The CL-STA-0048 campaign involves an attacker who utilizes various tactics to evade detection, bypass security measures, and exfiltrate sensitive data from high-value targets. The attacker takes advantage of unpatched vulnerabilities in widely used services such as IIS, Apache Tomcat, and MSSQL. Adapting to evolving defenses, the attacker deploys unique and rarely seen techniques to bypass security and achieve their objectives. The main goal is to gather personal information of government employees and steal sensitive data from targeted organizations. Upon successfully compromising the victim's system, the attacker deploys multiple web shells, including ColdFusion web shells, as well as malware like PlugX and Cobalt Strike.

Technique used by attacker:[-

Hex Staging. Incrementally writes hex-encoded data into a temporary file piece by piece, using commands passed to cmd.exe. This method avoids detection systems that scan for direct file writes.

DNS Logging Service:-Used to exfiltrate command output.

KCP Protocol:-leveraging the KCP Protocol for downloading Winos4.0-based Downloader.

Malware/tool used by attacker: -

SspiUacBypass:-Open source Privilege Escalation Tools used to bypass User Account Control (UAC)

https://github.com/antonioCoco/SspiUacBypass

The Potato Suite:- A collection of various open source native Windows privilege escalation tools used to gain system-level access, allowing high-privilege operations and command execution without user interaction

https://github.com/BeichenDream/BadPotato

https://github.com/crisprss/RasmanPotato

SoftEther VPN:- flexible and multi-protocol support used for stealthy communications and bypassing network restrictions.

https://github.com/SoftEtherVPN/SoftEtherVPN

Winos4.0-Based Downloader:-written in C++ and targets the Windows platform. Winos has features that include file management, distributed denial of service (DDoS) using TCP/UDP/ ICMP/HTTP, full disk search, webcam control, and screen capturing.

Supershell:- is a C2 remote control platform accessed through a WEB service. It establishes a reverse SSH tunnel to obtain a fully interactive Shell and supports multi-platform architecture Payload.

<https://github.com/tdragon6/Supershell/tree/main>

Indicators of Compromise (IOCs):

Domain

h5.nasa6.com

test.nulq5r.ceye.io

web.nginxui.cc

sentinelones.com

mail.tttseo.com

IP

43.247.135.106

38.54.30.117

38.54.56.88

65.20.69.103

52.77.234.115

192.227.180.124

107.174.39.125

18.183.94.114

206.237.0.49

154.201.68.57

HASH

a09179dec5788a7eee0571f2409e23df57a63c1c62e4b33f2af068351e5d9e2d

edc9222aece9098ad636af351dd896ffee3360e487fda658062a9722edf02185

35da93d03485b07a8387e46d1ce683a81ae040e6de5bb1a411feb6492a0f8435

336892ff8f07e34d18344f4245406e001f1faa779b3f10fd143108d6f30ebb8a

c5af6fd69b75507c1ea339940705eaf61deadd9c3573d2dec5324c61e77e6098

8dfc107662f22cff20d19e0aba76fcd181657255078a78fb1be3d3a54d0c3d46

3503d6ccb9f49e1b1cb83844d1b05ae3cf7621dfec8dc115a40abb9ec61b00bb

0f85b67f0c4ca0e7a80df8567265b3fa9f44f2ad6ae09a7c9b7fac2ca24e62a8

525540eac2d90c94dd3352c7dd624720ff2119082807e2670785aed77746301d

af0baf0a9142973a3b2a6c8813a3b4096e516188a48f7fd26ecc8299bce508e1

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

1. **[CMTX-P012025355] Hellcat Ransomware**

Threat Overview:

Threat Campaign: HellCat Ransomware

The HellCat ransomware surfaced in the middle of 2024, uses strategies like double-extortion which entails data exfiltration before encrypting computers.It uses psychological tricks to attract attention and coerce victims into paying demands for ransom.The group targets high-value industries like government, energy, and education.It utilizes creative demands to get media attention.

The malware employs the T1486 technique (Data Encrypted for Impact) for file encryption and is distributed via malicious infrastructure linked to an onion domain. It operates primarily through a Ransomware-as-a-Service (RaaS) model, providing ransomware tools and infrastructure to affiliates in exchange for a share of the profits

HellCat exploits vulnerabilities in enterprise software tools like Jira for initial system access, using privilege escalation for persistence and lateral movement and this ransomware shares similarities with Morpheus ransomware.

Threat Type: Ransomware

Severity: High

Response Actions:

• 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.

• Update Antivirus Definitions: Ensure your antivirus software is updated with the latest virus definitions. This can usually be done through the software's update function or by downloading the latest definitions from the vendor’s website.

• 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, particularly for webmail, virtual private networks, and accounts that access critical systems to add an additional layer of security

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

• The reference link provided below is a one-stop resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential attacks:

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

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

Indicators of Compromise (IOCs):

HASH:

b834d9dbe2aed69e0b1545890f0be6f89b2a53c7 “HellCat”

f62d2038d00cb44c7cbd979355a9d060c10c9051 er.bat (Morpheus)

f86324f889d078c00c2d071d6035072a0abb1f73 “Morpheus”

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

1. **[CMTX-I-901022025] Malicious Domains used by Threat Actors**

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.prb.wb.gov.in.onlinepanel.site

ww25.cowin.gov.inwww.thanksuser.xyz

uniquesewa.site

cbigovt.com.digitalhai.com

meet.ongc.co

indanoil.in

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

1. **[CMTX-P-022025905] 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

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

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

Indicators of Compromise (IOCs):

IP Addresses

121.37.170.202

20.115.66.63

8.218.138.77

164.90.158.199

64.226.91.107

182.60.11.201

120.79.86.98

150.158.152.209

77.243.85.54

35.88.59.138

182.60.11.201

54.74.198.96

113.44.78.183

35.88.59.138

43.156.95.75

159.223.0.196

192.52.166.51

13.201.109.246

52.15.80.186

107.172.191.253

8.210.9.166

195.230.23.91

166.88.95.137

8.219.69.133

51.84.67.174

74.235.30.127

185.14.45.232

49.65.96.18

39.107.85.83

34.219.143.252

107.172.159.50

64.23.213.61

52.73.128.242

172.211.22.127

18.237.245.78

182.60.5.9

124.243.177.110

54.185.190.255

46.166.165.95

182.60.9.165

27.124.53.34

129.211.212.43

47.243.13.249

182.255.44.86

152.89.92.204

62.234.65.53

47.98.158.167

8.217.200.158

178.255.244.176

101.35.228.105

117.72.69.250

78.24.220.122

146.70.113.134

47.99.176.66

64.226.91.107

47.237.86.35

82.156.188.211

81.177.217.56

47.90.208.22

43.134.38.211

3.16.25.250

74.207.235.197

164.90.158.199

194.233.73.173

8.155.8.190

52.149.122.11

149.210.143.97

95.217.178.98

149.88.78.49

39.98.115.22

185.208.158.217

107.172.239.112

182.60.5.9

182.60.11.201

121.43.166.96

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

1. **[CMTX-P-022025018] AMOS Stealer**

ATOMIC Stealer also known as Atomic macOS Stealer is a data miner written in Go that targets the macOS environment. It can exfiltrate browser data, cryptocurrency wallets, system information, and files in the Desktop & Documents folder. Collected data is sent to C2 over HTTP. It can be distributed via phishing, malvertising, and unsigned DMG files.

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

Domains:

blacksaltys.com

fetchdataajax.com

foundedbrounded.org

groundrats.org

leatherbook.org

loopconstruct.com

modernkeys.org

objmapper.com

packedbrick.com

promiseresolverdev.com

rednosehorse.com

smthwentwrong.com

variablescopetool.com

Blackshelter.org

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

1. **[CMTX-P-022025915] 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

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

Indicators of Compromise (IOCs):

IP Addresses

185.208.158.217

45.76.30.116

89.147.108.143

176.31.162.105

8.138.119.106

4.197.169.184

62.109.30.217

102.117.167.10

107.173.111.26

182.60.11.201

159.223.0.196

3.68.92.103

47.106.171.201

20.8.97.39

8.218.120.126

182.60.11.201

185.235.167.143

182.60.5.9

101.133.172.90

47.115.200.80

195.158.82.221

47.99.60.17

107.173.118.149

149.104.26.229

65.0.26.137

159.223.242.185

182.60.11.201

154.38.167.90

182.60.11.201

194.171.96.118

182.60.9.165

46.8.237.108

117.50.184.22

152.42.198.168

123.11.255.4

182.60.11.201

157.245.146.223

206.189.85.172

145.131.8.169

172.105.27.15

182.60.11.201

16.171.27.214

8.142.124.166

67.219.111.218

64.227.48.216

39.98.204.142

96.9.210.77

45.76.30.116

182.60.5.9

195.208.174.240

182.60.11.201

185.43.4.72

182.60.11.201

152.89.92.204

54.176.66.101

117.215.247.241

185.158.94.217

45.251.240.55

45.251.240.55

45.251.240.55

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

1. **[CMTX-I-951022025] Malicious Domains used by Threat Actors**

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

email.gov.in.defenceindia.link

bnd.ndmc.gov.in.viewcrti.info

ww25.gov.in.birthctifecate.live

\*.defenceindia.link

\*.viewcrti.info

\*.birthctifecate.live

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

1. **[CMTX-I-080022025] Malicious Domain Imitating Indian Navy Website and Hosting APK**

A malicious domain has been identified impersonating an official Indian Navy website and is hosting a malicious APK file aimed at compromising user devices. The APK file is being used for cyber espionage, credential theft, or remote access to infected systems. The domain is also linked to a Command & Control (C2) infrastructure, facilitating remote control of compromised devices.

The IOCs of this campaign is as follows:

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

Malicious Domain: indiannavyofficial.com

The domain resolves to 66.29.153.162

APK Filename: npo.apk

SHA1 Hash: b0d3a39a40dc9db7604900545b48a54d89afbdbc

APK Behavior: Following permissions are invoked by the APK

> Internet

> Read Media (images, audio, video) and media location

> Read Contacts

> Read Call Log

> Read, write and manage external Storage

Command & Control (C2): 188.166.119.119

Port: 7774

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

1. **[CMTX-P022025925] ACTIVE EXPLOITATION OF VULNERABILITY (CVE-2025-22604) AFFECTING CACTI**

ALERT BRIEF:

An "OS Command Injection" vulnerability tracked as CVE-2025-22604 is being exploited and affecting Cacti network monitoring tool. On successful exploitation of this vulnerability,it allows a remote, privileged attacker to execute arbitrary code.

The vulnerability arises from a defect in the multi-line SNMP result parser, which allows authenticated users to inject malformed Object Identifiers (OIDs) into responses. This malformed data can lead to a command execution vulnerability when processed by certain functions, enabling attackers to execute arbitrary code on the server. As a result, they may gain access to sensitive data, potentially allowing for theft, alteration, or deletion of this information.

IMPACTS:

1. Remote Code Execution: Authenticated attackers can execute arbitrary code on the server, leading to serious security breaches.

2. Data Theft: Attackers may steal sensitive data, compromising user privacy and organizational integrity.

3. Data Manipulation: The vulnerability enables the editing or deletion of critical data, affecting operational continuity.

4. System Compromise: Full control over the server can be achieved by attackers, leading to further exploitation of connected systems.

5. Increased Attack Surface: Organizations using vulnerable versions of Cacti may become targets for other malicious activities following an initial breach.

6. Compliance Risks: Organizations may face legal repercussions for failing to protect sensitive information, potentially leading to regulatory fines.

7. Reputation Damage: Exploitation of the vulnerability can lead to loss of trust among clients and stakeholders.

8. Operational Disruption: The need to address the breaches and restore systems can lead to significant downtime and resource allocation issues

AFFECTED VERSIONS:

CVE-2025-22604 affects all versions of Cacti prior to and including 1.2.28. The vulnerability has been addressed in version 1.2.29. Organizations utilizing any version prior to this patch should be particularly vigilant.

1. **[CMTX-P022025935] Arcus Media Ransomware**

Threat Overview:

Threat Campaign: Arcus Media Ransomware

Arcus Media ransomware represents a significant threat in the cybersecurity landscape, emerging as a formidable adversary since May 2024. Operating under a Ransomware-as-a-Service (RaaS) model, it has claimed responsibility for over attacks by November 2024. The ransomware is characterized by advanced capabilities designed to maximize disruption and hinder recovery efforts.

Threat Type: Ransomware

Severity: High

Impacts of Arcus Media Ransomware:

1. Selective Encryption: The ransomware employs selective encryption techniques, encrypting files based on their size.

2. Critical Process Disruption: It targets and terminates essential business processes, including SQL servers and email clients, leading to operational paralysis.

3. Recovery Challenges: By deleting shadow backups and disabling recovery mechanisms, it complicates data restoration efforts.

4. Data Exposure Threats: Victims face threats of public data leaks if ransom demands are not met, escalating the pressure to comply.

5. Operational Success: The combination of advanced encryption and persistent disruption ensures high operational success for the attackers.

6. Financial Impact: Organizations may suffer significant financial losses due to downtime and potential ransom payments.

7. Reputational Damage: The threat of data leaks can severely damage an organization's reputation and customer trust.

8. Legal Consequences: Victims may face legal issues related to data protection regulations like GDPR.

Distribution Methods:

1. Phishing Campaigns: Targeting employees through deceptive emails to gain initial access.

2. Exploiting Vulnerabilities: Taking advantage of unpatched software or systems.

3. Malicious Attachments: Using infected files attached to emails or hosted on compromised websites.

4. Ransomware-as-a-Service (RaaS): Leveraging a RaaS model that allows affiliates to deploy ransomware for a share of the profits.

5. Remote Desktop Protocol (RDP) Exploits: Gaining unauthorized access through weak RDP configurations.

1. **[CMTX-P-VUL-022025505] 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: VULNERABILITY\_LIST\_06022025.pdf

1. **[CMTX-I-808022025] CrimsonRAT- APT36 campaign**

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

209.127.18.107

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

1. **[CMTX-I-443022025] CrimsonRAT- APT36 campaign**

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

209.126.7.21

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

1. **[CMTX-P022025144] Code injection attacks using publicly available ASP.NET machine keys**

Alert Brief:

It has been reported that threat actors are taking advantage of publicly accessible ASP.NET machine keys to inject malicious code into IIS servers and deploy the Godzilla post-exploitation framework. These keys are often exposed due to developers accidentally leaving them in the public domain, such as in documentation or code repositories, or unintentionally embedding them in their applications.

ASP.NET uses machine keys to safeguard ViewState data from tampering and unauthorized disclosure. ViewState is a mechanism that allows ASP.NET Web Forms to retain the state of a webpage and its controls across postbacks. Machine keys are essential for protecting ViewState from manipulation and exposure.

If these machine keys are compromised or made accessible, attackers can craft a malicious ViewState specific to the targeted organization and send it to their web server. When the server processes the request, it could result in the execution of malicious code, leading to the installation of the Godzilla post-exploitation framework.

Detecting/Hunting

• Microsoft has provided a list of hash values (available in the GitHub link below) for publicly disclosed machine keys. Use this list to check if any of your machine keys have been exposed in publicly accessible resources. If any are found, rotate or remove the compromised machine keys.

<https://github.com/microsoft/mstic/blob/master/RapidReleaseTI/MachineKeys.csv>

• Use Advanced Audit Policy settings to monitor configuration files and review Event ID 4663 in the Windows Security Event Log. This will help you identify any potential anomalies, unauthorized access, or suspicious file access attempts. For detailed instructions on setting up auditing, please refer to the steps outlined in the "Hunting Queries" section of the Microsoft blog, linked at the end of the alert.

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

Indicators of Compromise (IOCs):

HASH

19d87910d1a7ad9632161fd9dd6a54c8a059a64fc5f5a41cf5055cd37ec0499d (Godzilla Web shell)

1. **[CMTX-P-022025965] PlugX Malware Campaign – Immediate Action Required**

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

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

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

Indicators of Compromise (IOCs):

IP Addresses: Port

167.179.109.96

143.92.56.71

45.76.183.8

58.220.33.141

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

1. **[CMTX-I-389022025] CrimsonRAT- APT36 campaign**

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

45.61.151.96

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

1. **[CMTX-I-633012025] Malicious Domains used by Threat Actors**

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.indiandefenceforces.link

email.gov.in.indiandefenceforces.link

gov.in.indiandefenceforces.link

\*.indiandefenceforces.link

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

1. **[CMTX-P022025975] TitanPlus deploying multiple ransomware variants via shared techniques to drive expanding campaign**

Alert Brief:

TitanPlus is deploying multiple ransomware variants, including Cactus and Black Basta, as part of an expanding cyber attack campaign. This threat is characterized by the use of sophisticated techniques to deliver malware, including remote access tools (RATs) and multiple payloads through a variety of channels.

The adversary uses DLL sideloading and masquerading techniques to evade detection and deliver multiple malware payloads through sophisticated methods.

Key Characteristics:

1. Multiple Payloads: Attacks involve simultaneous deployment of several malware families like Cactus and Black Basta ransomware variants. .

2. Phishing Tactics: The initial access is typically gained via phishing emails, which may include malicious URLs or attachments that lead to infected files .

3. Obfuscation Techniques: The malware employs various obfuscation methods to evade detection, using tools like BatchShield to obscure BAT files and Python scripts .

4. WebDAV Infrastructure: Threat actors utilize WebDAV servers to host malware, allowing for easy updates and management of payloads .

5. Adapting to Defenses: Regular adaptations to the infection chain are made to improve evasion tactics, such as adding antivirus checks within scripts to alter payload delivery based on the security environment .

Impacts of the Threat:

The deployment of ransomware variants poses significant risks to organizations, including:

1. Data Loss: Critical data may be encrypted or stolen, leading to potential loss of sensitive information.

2. Operational Disruption: Ransomware attacks can halt business operations, significantly impacting productivity and revenue.

3. Financial Costs: Organizations may incur hefty costs related to ransom payments, recovery efforts, and system repairs.

4. Reputational Damage: Breaches can harm an organization’s reputation, leading to loss of customer trust.

5. Regulatory Consequences: Violations of data protection regulations can result in fines and legal action against affected organizations.

Distribution Methods

TitanPlus employs a variety of distribution methods to deliver malware, including:

1. Phishing Emails: Leading victims to malicious URLs or attachments that execute the infection chain .

2. Internet Shortcuts: Using shortcut files that download and execute malicious scripts upon opening .

3. ZIP Archives: Hosting malicious content within ZIP files that contain URL files directing users to download malware .

4. WebDAV Servers: Utilizing a network of WebDAV servers to host and distribute malware .

5. Cloud Services: Abusing services like Cloudflare to create temporary tunnels for malware distribution .

Mitigations

Organizations can implement several strategies to mitigate the risks associated with TitanPlus ransomware:

1. Email Filtering: Employ advanced email filtering solutions to detect and block phishing attempts.

2. Endpoint Protection: Deploy comprehensive endpoint protection solutions to detect and respond to malware infections.

3. Backup Strategies: Regularly back up critical data to offline or secure locations to ensure recovery in case of an attack.

4. Network Segmentation: Implement network segmentation to limit the spread of malware within the organization's infrastructure.

Recommendations

To strengthen defenses against TitanPlus and similar ransomware threats, consider the following recommendations:

1. Endpoint Logging and Auditing: Make it possible to audit registry changes in detail, keeping an eye out for changes to high-value keys (such HKLM\SOFTWARE).

2. External Access Policies: Set up the tenant settings for Microsoft Teams to prevent external communications. This can involve either prohibiting external access or restricting it to trusted domains.

3. Monitoring and Alerts: Use call and message monitoring tools to spot unusual trends (such recurring calls from unconfirmed domains) and set up alarms.

4. User Education and Awareness: Conduct frequent training sessions on identifying social engineering attempts, such as vishing, with a focus on the dangers of unsolicited requests and the significance of sender identity verification.

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

MITRE ATT&CK AND IDENTIFIERS:

Initial Access

T1566 Initial Access: Phishing

Discovery

T1016 Discovery: System Network Configuration Discovery

Execution

T1059.001 Execution: Command and Scripting Interpreter: PowerShell

Lateral Movement

T1021 Lateral Movement: Remote Services

Privilege Escalation

T1574.002 Privilege Escalation: Hijack Execution Flow: DLL Side-Loading

Persistence

T1547.001 Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Defense Evasion

T1562.001 Defense Evasion: Impair Defenses: Disable or Modify Tools

T1112 Defense Evasion: Modify Registry

T1218 Defense Evasion: System Binary Proxy Execution

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

IOCs

195.123.233.148:443

89.185.80.170:443

195.211.96.135:443

45.8.157.146:443

207.90.238.67:443

38.180.138.15:443

185.190.251.114:443

38.180.138.167:443

45.8.157.144:443

185.190.251.16:443

207.90.238.52:443

89.185.80.86:443

38.180.25.3:443

45.8.157.199:443

5.181.3.164:443

HASH:

C9471F5CF7D75495622036FE35AFC532B7A05423C05EECA5BDA08BBE91CF9D71

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

1. **[CMTX-P-022025128] DragonRank Activity**

Alert Brief:

Reports indicate that the attacker, known as DragonRank, targeted publicly exposed, unpatched, or improperly configured Internet Information Services (IIS) servers. Once the attacker gains access, they deploy the BadIIS malware and engage in SEO poisoning activities. As a result, users who send requests to the compromised server may either be redirected to illicit gambling websites or connect to attacker-controlled malicious servers that host harmful content, such as malware or phishing schemes.

Initial Infection Vector: - Exploit the publicly exposed, unpatched, or improperly configured Internet Information Services (IIS) servers.

Malware: - BadIIS malware

Mitigation Measures:

• Monitoring for abnormal IIS module installations is also critical, with a particular focus on installed images located in uncommon directories.

• Firewalls should be implemented to control and monitor network traffic to and from IIS servers, minimizing exposure to potential threats. Restrict access to the IIS server based on IP addresses if possible to minimize exposure.

• Regular monitoring of IIS server logs is essential to detect anomalies, such as unexpected module installations or changes in server behaviour.

• Strengthening security by disabling unnecessary services and features reduces the attack surface and improves overall server security.

• Turn off any IIS modules, services, or features that are not needed for your environment (e.g., FTP, WebDAV, etc.).

• Integrate IIS logs into a Security Information and Event Management (SIEM) solution to enable centralized log aggregation, correlation, and alerting. Integrate the IOCs from alerts into your SIEM, TIP, or firewall for early detection of attacks.

• Run the IIS application pool identity with the least privileges required to perform the job. Administrative access to IIS servers should be restricted, with strong, unique passwords and multi-factor authentication (MFA) enforced for all privileged accounts.

• Establish incident response protocols to address breaches quickly.

• Use advanced threat detection tools to identify suspicious activities, and

-------------------------------------------------------------------------------------------------Indicators of Compromise (IOCs):

HASH

8a49966eb90acc5c05a6bba523f1dd0d58127ab731d44c7304204fa02bf61186

bbf9d7dafba979ef9c1e8531a20d3bea1adcdbb628816ce8781d7eeb6292f265

33e5e5e773d1909004d4b38a0e4e3e97e46cbdb7b17f94b28fce2c9ad0a375d3

c732067b3d8763c248051366ab7beeae0d7fbe105884d4d3f8647e3427f36daf

59b416efff07208dc8b1c98a6f754e3abc14e55d71971ddc5581f6bc7ca45837

fe14c579308d356c64bd3be9365014de805a17abab8cb741e2817b8451a92f64

5d838c0dbf164b26c4c5dc20f96d3bf48a5f9fde88bbc1dd02c08007bb184d86

13f094d3eebe9d700360868006ac022a622ec606628adcc3782123d5092224d1

61913e0a38282a42b26aff578da17dab60ac0fbee819fa42db5497cc5cf55760

03bc0ddfa59cfa290c426396f1c5fff45bd2c3ef90152cafc7c662c075dfc7d8

f9017361349421728fc1ac1bc1549b3d23b35bd795f0a83be2e9e517bccaccdc

42906ac10d053eec10c05e2eeebcb06a7d6b307dc0d18083151dff3e0ac70022

a2a9dcdfc6f0aab577bc0f2750ff44050034c0f1c2f8b325a246f4dfe5f33219

bb9b0b20d239b2f5fe6da31fc2d13ec4ba6083238df68befd33d7521570d334e

08f965f640a3ec1c3aa9c31033455fad02550485d0d5b6fe33553d374775f18a

65967f471440449d2f1b615ff1338b8082b0481b617eda4d9f21a9f102b98859

c75a9a104e340473b72140127f3039a08f99a334887afc100d09cffa3c4c8e24

7b190719c3fb9c0bde074981adaf5b04356c9c48fa2fccdb334c4ae218f66fc0

2496bfe15e283affdfcd7f1de9134227671e2cddfb726b46829fa966abb9ac96

2ec893440e04de55bc6bbe4b1db76df532aa42d3140a15dc5365ef520a1d4247

9fbae4ed1de2b09af9a246a021f2a7fc8667492d459ac346eba6719509c41c5a

f1dcd2809a001a0d0ea3221939f7afd2ef9e5bf468709bd91abd70c902c42d45

7ccdd8966adf04ddd9b24dac0d1b8642968598a88ec3f5048b279843bffefb84

facfea68fe95fc81e3b6e04f79fbcba738c79b4de2d0238e4e5a8ba095a2516d

01577f5b0869154fb678bcf86eef50afceb5fc189c87b2085fe5fcdf74cd6ff0

a01ae86a356373f0d3e1b843f50243394308a96bd01978b33e4a91c0f0b19cce

a0bb95eafc9913633c7e27f0f1e6c81eb4c138a809c109ad3abae5fcc47c2cbd

a4906b40232726948f6a5357ad0ee9445512b422ae510d2ef08bd9cf516852bd

6edb1fd609c7e011cd42656af67baf5271d8212933a8c964604d138306b9565f

5b497b4205427198fc922c74cad8275b4256579f8bb5a1f1dbad7151630288a0

7321d599e777088356d7549e638b6b67fc43fc5c9f0c8846ee5aa7f47e35c2eb

ed3882a77cdc372f647e647b66979525a50054a580b43499ce5a97864d772730

24aafe0a2033e2e5ca231ebca0e3c56740754a97ca1f5062305e6b30222fc0ee

e09067e3e134e620b69117caf5bee54c1066b7259b74ddf2399afc64116690c9

e3197285c98965ca0522d3683c0d656e4ab1f8335ca322e1ae8c06b79dfd9b9c

1bb1187daff9610a0c142b48bc04d3e883344ca0eca8fe915d6a02fb3e7571ff

e927d6ea1fdc27c0ae9eb55254bbbd4f501f14ae02e499d7d20cdd83af479b20

df75b0b8ea1f75f0039c158c89e413ed6c4352309cc2cfa282afd1857676a88c

a35f810ed9ffd884d0599aa391d0043ad955e821f8144089116b15f01b8a932b

4091ddc3560fb60bd3ef071367fd833d67c3c6e3e81165aa3d93519b93959658

1cb60c7a121187978661b4bda84279f2324a5779b3f58bac11470a73fe544f6a

8fee015ae0e978e39af2cd1ca74b29202e702d296c110f3a7a90dfadce28d4a6

2e20ce7bc1e653737f05c910759fd2e420fe28f77f80a6d8e7c9346809e4dce7

12e4817abc69918b8556a4f18371c803db3d5191031cb56f835ec33cdb12f0d9

22cebb4f0fe6f4377e91b1e19204eff0f744d316b8c900377d8db4aa4f457801

cc67b50d746b23b9bc6fc12dde8c64d72c7f856521787b964598672d83525915

79b7fe6db452edd3077fb55906beea64c19087a19e5fb35211dd80975db74f9e

a68d83fd210b8ca21370a0f38da8fc0dd20b081e69beef911060924aa708a280

18939c40dd601550da9f07d8115f4b19bec422df4ada9358bac9bd9e9ac94e94

8ae43e6bd2cf0f8ced8f888226a4d6d06a7b03552e9af3d3cde35bb1d9724867

ffceed66dd9935c92ff7922bd5fdfde08e9a2ff78dd3a76dc65a200305779b9c

fec618c4f832d8a182fc1d3b9e58a0bff1a62241a1d17108e84ed1f0c4bb7845

6503770b34c53025793f1674af87d80a8f6ed44b5780490796012a2b771b8f84

e3c73f76f7b08ab6e223918a5b961201f60934ec95e5362529a42c1655395443

21a61777b0f725dd0dbdb2ecd0dd66e952012e94894e71c306059990c2afe377

3b8adf88b10e0c66d97b4909a17d4436a043ded5cf29c85ead22b58917e9ac7b

e8201b4a0f2619224e0720034dfc19a75f77582531bd98a2465a58bbf4a9f8c6

bf45c48b209e5004520b5d541e406c183bccb2fe81f3974c2c53be48017f74ca

02e98650e89146f0bddf29dd73165b9993d52f966d6194d375b6f0fcf737c38a

381dc36504e1b319fde9bbae0a580da9f239b8af8066638f9a4203e58dc16087

fbd3d1828592a2c1f154ebe2283643e24dee1db9f8989ce32e54b00d470a0096

521869f9ee6066c33fb1615cbcad66de157876bd08cec05597e4d3a0405efac8

eda7a7edc01392706a872a5a275940b4a4b9471dc562eb70128ee672872d1407

02dba6f34480eac1d27c83a4ff06e3ba03fc63fcf3067e0957375bfd182ed39b

8eb51f51eea27de8b976bdbcc84f4cf386256dfd9dc3702df8f839490699e173

89169f480810198a2cbb28fab15e0dfc8d1ee53981a9834cb84a84d077db3d17

6606d6e6424f7c25b922905095ba8cbff83357430bf1ef0ce0553a411fed1748

5d0b2015998a8a5a2a60ebdd2f3d6a398e533d198b9157c1558e6913330c24ba

e645ee394546db818350adfb2c55bffea78f405ac0ebb3fb1486e7d2f042c46f

0f7df7ac22957da6a793f641cda611c2c2a294355d4d19b29b6920853a012d98

b6844533bb887e870eb88fba88ed4d616ea8a9573b673faf927846c802f7817c

92e8076a59831156af5dc7058356cc0ad3dbd3c32cd84b08c3c8541ccc32d1c0

a383c13bbe949d0b6dff23e3243c7bbac1813d2ce9d99149cd5b984f051005d0

44bfb9f0e13dd72ed111b5b5600b80b305ab153a0ee2224957e76391b28ac037

3d331e6c5c1b22377b3b4aba9f71d65a10a77df6d8ee64c3a0d7d7de3d1f1565

Domain

chem-db.com

vnfll22.keeploong.com

se2.ggseocdn.com

se2.ggseocdn2.com

www.xxxx.vip

js.targetedtrafficcrew.com

all.targetedtrafficcrew.com

ll.olacityviet.com

798.toptopkm88.com

site.toptopkm88.com

link.toptoplm88.com

www.m2313.com

br.zmdesf.cn

br.ruicaisiwang.com

tz123.app

www.xiagao886.com

js.cloudflare.cyou

newth.googlecache.cc

newthmap.googlecache.cc

phpmap.googlecache.cc

vn6789sky.com

wailian.vn6789sky.com

sitemap.bet277.vip

sitemap1.bet277.vip

brcknkblue.com

wailian.brcknkblue.com

eglotanygfa.vip

wailian.eglotanygfa.vip

yyds.tmpdrsh.com

proxy.xxxx.com

tdk.798love.com

spider.xxxx.com

jumpsexxx.com

www.jumpiis8.com

six2fc.com

yitongmingde.com

qiqiguaiguai2.xyz

jsc.olacityviet.com

jsc.bet277.vip

lucky.668823.com

bb.vdfskis888.com

link.vdfskis888.com

ldy.vdfskis888.com

th.ntxx.cn

topck008.com

link.topck008.com

googleseo.life

bryyds.com

dk8.zone

dk8.land

668th.com

js.officefonts-clo.com

aafd.tv

vg9920.store

vn.coronavg99.com

coronavg99.xyz

s995.vip

zavinac.net

wailian.zavinac.net

89vq.me

tdkgpt.yyds6686.com

html.aafd.tv

IP Address

185.106.178.76

38.207.248.230

154.7.64.81

156.229.134.13

45.120.81.62

File Location

C:\\ProgramData\\Microsoft\\DRM\\\*

- --------------IOC END----------------------------------

1. **[CMTX-I-022025344] IOCs related to njRAT family**

ALERT BRIEF:

NJRAT is a.NET-based backdoor that uses a unique text-based protocol over TCP to communicate. The backdoor is capable of recording video, audio, screenshots, keystrokes, creating a reverse shell, transferring files, running files, stealing credentials, and spreading via USB drive. Malware has features to update its capability by getting plugins from a C2 server.

Recent IOCs of njRAT family are as follows:

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

Domain

9292.ddns.net

apimicrosoft.ddns.net

cj2004.duckdns.org

hakim32.ddns.net

hextoriq99.ddns.net

host-urge.at.ply.gg

koper.ddns.net

postpix.shop

sosomyhestor.ddns.net

viewi.publicvm.com

youri.mooo.com

6.tcp.eu.ngrok.io

7.tcp.eu.ngrok.io

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

1. **[CMTX-P-022025755] 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

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

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

Indicators of Compromise (IOCs):

IP Addresses:Port

64.176.53.26:443,53

70.34.215.167:443,53

64.176.6.235:443,53

38.147.172.196:80

158.247.244.252:8080,443

156.244.31.112:443

149.28.130.206:443,53

202.144.192.20:8080

70.34.215.167:443

158.247.244.252:443

167.179.109.96:443

64.176.6.235:53

64.176.53.26:443

64.176.53.26:53

64.176.53.26:443

167.179.109.96:53

70.34.215.167:53

149.28.130.206:443

158.247.244.252:8080

70.34.215.167:53

64.176.6.235:443

149.28.130.206:53

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

1. **[CMTX-P-022025765] 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

Distribution Methods:

• Shadow Pad is often delivered through DLL sideloading techniques and exploits vulnerabilities in software such as Microsoft Office IME binary or Microsoft Exchange Server. It can also been distributed through supply-chain attacks

Indicators of Compromise (IOCs):

IP : Port

95.179.134.240:53

185.167.61.21:8081,88

38.54.119.134:443

185.167.61.21:8081

185.167.61.21:88

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

1. **[CMTX-P-022025785] PurpleBravo Actor Activity**

1. Threat Campaign

PurpleBravo is a North Korean-linked threat group that primarily targets software developers in the cryptocurrency industry. The campaign utilizes malware such as BeaverTail, InvisibleFerret, and OtterCookie.

The threat actor disseminates job advertisements across at least three hiring platforms, as well as on Telegram and GitHub, while leveraging Astrill VPN to manage its command-and-control (C2) infrastructure.

BeaverTail is an information-stealing malware family initially distributed through NPM packages as a JavaScript payload before evolving into executables and downloaders targeting both Windows and macOS environments. It is used to collect cryptocurrency wallet data and browser information.

InvisibleFerret is a set of post-compromise payloads functioning collectively as a backdoor within victim environments. It facilitates data theft, system fingerprinting, and utilizes legitimate protocols and software for communication.

OtterCookie is a post-compromise malware family that operates as a backdoor, establishing C2 connectivity and executing shell commands received from C2 servers.

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs):

IP

147.124.214.237

67.203.7.163

147.124.214.129

147.124.214.131

23.106.70.154

147.124.197.138

66.235.168.232

45.43.11.201

38.92.47.85

165.140.86.227

38.92.47.151

38.92.47.91

66.235.168.238

86.104.74.51

147.124.197.149

154.205.155.71

67.203.7.205

147.124.212.125

45.59.163.56

66.235.175.109

67.203.7.200

103.15.29.45

202.53.148.16

180.235.135.180

202.53.148.32

180.235.135.184

103.51.141.153

103.51.141.152

HASH

4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79

7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e

0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd

d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6

07183a60ebcb02546c53e82d92da3ddcf447d7a1438496c4437ec06b4d9eb287

10f86be3e564f2e463e45420eb5f9fbdb14f7427eac665cd9cc7901efbc4cc59

cde5afd20b7bb5c9457b68e02c13094125025fb974df425020361303dc6fcdfc

d0a5b9dc988834cc930624661e6e7dd1943d480d75594fff0f4bc39d229c5999

8de446957ce96826628c88da9fd4e7ff9d6327d8004afc4e9e86d59e7d6948dc

DOMAINS

pengzhoutrading.com

xiwangtechltd.com

wuxiantechltd.com

diditechltd.com

deepsealuc.com

hisolution.io

hi-devs.com

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

1. **[CMTX-I-667022025] DC RAT – Active Malware Campaign**

DC RAT (Dark Crystal RAT) is a powerful Remote Access Trojan (RAT) actively used by threat actors to conduct cyber-espionage, system control, and data exfiltration. This malware is capable of executing remote commands, stealing credentials, logging keystrokes, capturing screenshots, and establishing persistent access. It is often deployed via spear-phishing emails, malicious attachments, and fake software installers.

DC RAT has been observed in targeted cyberattacks against government, defense, financial, and critical infrastructure organizations, posing a significant security risk.

Key Features of DC RAT

> Remote System Control – Attackers can manipulate infected systems remotely.

> Keystroke Logging & Credential Theft – Monitors user activity and steals sensitive information.

> Data Exfiltration – Extracts confidential documents and personal data.

> Persistence Mechanisms – Ensures long-term access by modifying system files and registry entries.

> C2 Communication – Uses encrypted traffic to evade detection while communicating with command & control (C2) servers.

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 DC RAT malware targeting government officials is:

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

182.188.47.2

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

1. **[CMTX-I-021022025] SideCopy- C&C of Malware Campaign**

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) domain and additional malicious domains (hosting malware) used by this threat actor are as follows:

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

bsli.pcdaopune.site

winsoft.pcdaopune.site

winsofts.pcdaopune.site

sopos.mypressonline.com

\*.pcdaopune.site

h791yuwbecdn8lfcundipxyzx.canarytokens.com

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

1. **[CMTX-I-022022025] Malicious Domains used by Threat Actors**

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

email-govs.icu

in.gov.indiana.com

www.estbengalpolicegov.infogini.com

bnd.ndmc.gov.in.web.viewcrti.info

dc.csrorgi.gov.in.web.viewes.site

nrsec-gov-in.online

dfsin.top

email.g0v.in

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

1. **[CMTX-I-854022025] Recent IOCs of Chinese Malware Campaign**

Chinese-based malware is often linked to state-sponsored groups or cybercriminal organizations operating from China. This malware can target various sectors, including government (defence, external affairs etc.), finance, technology, and critical infrastructure. Its objectives range from espionage and data theft to sabotage and disruption.

Tactics, Techniques, and Procedures (TTPs)

    >> Phishing and Social Engineering: Attackers frequently use phishing emails or social engineering tactics to trick users into downloading malware or revealing sensitive information.

    >> Exploiting Vulnerabilities: Malware may exploit known software vulnerabilities to gain access to systems. This includes zero-day exploits that target unpatched software.

    >> Remote Access Trojans (RATs): Many Chinese malware variants include RATs, which allow attackers to control infected systems remotely, facilitating data exfiltration and further attacks.

    >> Command and Control (C2) Communication: Infected devices often communicate with C2 servers to receive instructions or send stolen data. This communication can be obfuscated to evade detection.

    >> Use of Malware Kits: Attackers may employ sophisticated malware kits, which simplify the creation of malware and the exploitation of vulnerabilities, making attacks more efficient.

    >> Fileless Malware: Some malware variants operate without writing files to disk, making detection more challenging. They reside in memory and execute scripts to carry out malicious activities.

Prevention Measures

    >> Regular Software Updates: Keep all software, including operating systems and applications, up to date to mitigate the risk of exploitation through known vulnerabilities.

    >> Use Security Software: Install reputable antivirus and anti-malware solutions to detect and block threats. Ensure that the software is regularly updated.

    >> Educate Users: Train employees on recognizing phishing attempts and suspicious links or attachments. Awareness can significantly reduce the risk of infection.

    >> Network Segmentation: Implement network segmentation to limit the spread of malware and protect sensitive information by isolating critical systems.

    >> Regular Backups: Maintain regular backups of important data. In the event of a ransomware attack or data breach, backups can aid in recovery without paying a ransom.

    >> Employ Firewalls: Use firewalls to monitor and control incoming and outgoing network traffic, reducing the risk of unauthorized access.

    >> Intrusion Detection Systems (IDS): Implement IDS to monitor network traffic for suspicious activity and potential intrusions.

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

rov.noon.dns04.com

picture.efanshion.com

fashion.fashpopstyle.com

comaset.ns01.info

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

1. **[CMTX-P-VUL-022025805] 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: 14022025\_VULN\_LIST.pdf

1. **[CMTX-I-039022025] Malicious/ Compromised Domains used by Threat Actors**

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/Compromised Domain>---------

bio.iircin.com

iircin.com

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

1. **[CMTX-P022025815] RA WORLD RANSOMWARE**

Threat Overview:

Threat Campaign: RA World Ransomware

RA World ransomware is a malicious software variant involved in cyber extortion campaigns, particularly linked to espionage activities by actors associated with China. This ransomware was notably used in an attack against a medium-sized software and services company in South Asia in late November 2024.

Recently, tools typically associated with China-based espionage actors were identified in a ransomware attack involving the RA World ransomware.

The following ransomware families have been linked to the use of China-linked espionage tools:

LockFile - A ransomware variant implicated in attacks attributed to the espionage group Bronze Starlight .

AtomSilo - Another ransomware family linked to the same group.

NightSky - Included in the set of ransomware used by the Bronze Starlight group.

LockBit - Frequently associated with various cybercriminal activities, also noted in the context of espionage-linked attacks

Technical Details:

1. Proxy tool NPS- The NPS (Network Proxy Service) is a proxy tool associated with cyberattacks, particularly those linked to China-based espionage operations. It has been recently reported as one of the tools used in ransomware attacks, specifically by actors involved with the RA World ransomware.

2. Toolset: The same toolset used in previous espionage attacks was employed in the RA World ransomware incident, indicating a continuity in operational tactics.

3. DLL and Payloads: The attacker used a legitimate Toshiba executable to sideload a malicious DLL, which acted as a loader for a heavily obfuscated payload. This payload was linked to a variant of PlugX, a custom backdoor associated with Chinese espionage actors 21.

Threat Type: ransomware

Severity: High

Impact:

Impacts of RA World  Ransomware:

1.Financial losses due to ransom payments.

2.Operational disruptions within targeted organizations.

3. Data theft or exposure, compromising sensitive information.

4.Long-term reputational damage to affected companies.

5. Potential legal ramifications and regulatory scrutiny following data breaches

INDICATORS OF COMPROMISE:

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

HASHES:

7bae7f21bd4adf84eb3cc281fcc3d5fc3d1e47edd0dadd86587ce8ec63df1b8f

c1e6955acdefa9769a7ae0c1abf54a26e2158154dd6ec07cc71eb06c575193d5

18127cfd08cc49be08714d29e09ec130dcc0b19b7fcddc22c71d28fd245eb1b1

e177eb358f93ccc1ac4694feb0139e82c62d767388872d359d7c2ed0a05c2726

6ac81aa8d3f9d86ad5a18ea42fa1829b055dd25f123f9ee90002d64d4ef7a394

2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813

38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25

bb5740d2129663ae1c46b1ea1bdd0b8c423b6eb8f6e6f2b0b158a9e833496a01

DOMAINS:

plugins.jetbrians.net

police.tracksyscloud.com

caco.blueskyanalytics.net

IPs:

158.247.213.167

154.223.18.123

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

1. **[CMTX-I-055022025] Malicious Domains used by Threat Actors**

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

email-govs.click

dc-crsorgi-gov.shop

dc.crsorgi.gov.in.svlprint.site

www.gov.in.cscvle.store.droft.shop

gov.in.igaxis.site

www.ladlilaxmi.mp.gov.in.consulting

mp.gov.in.consulting

\*.gov.in.consulting

\*.in.svlprint.site

\*.in.cscvle.store.droft.shop

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

1. **[CMTX-I-780022025] Malicious Domains used by Threat Actors**

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

tspscgov.info

getkavach.com

dc.crsorgi.gov.in.dcbirth.in

gov.in.dcbirth.in

indotingov.info

yrspc-gov.info

dcbirth.in

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

1. **[CMTX-I-765022025] APT36 campaign**

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 and additional IOCs of malware deployed by this threat actor is as follows:

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

https://secdesk.xyz/drivers\_files

http://secdesk.xyz:8062

secdesk.xyz

\*.secdesk.xyz

ip-api.com (genuine domain but used

by the threat actors to obtain public IP

address of the victim machine)

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

1. **[CMTX-I-680022025] Malicious Domains used by Threat Actors**

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

in.reset-password.com

email-gov-in.reset-password.com

www.reset-password.com

rrbgov.info

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

1. **[CMTX-I-685022025] Malicious Domains used by Threat Actors**

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.departmentofdefenceindia.link

email.gov.in.departmentofdefenceindia.link

\*.departmentofdefenceindia.link

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

1. **[CMTX-P-022025655] A new attack campaign called "RevivalStone" attributed to the China-based "Winnti Group"**

Alert Brief:

The Winnti Group has been actively targeting organizations in Asia, particularly Japan, with their most recent campaign known as "RevivalStone." This campaign utilizes advanced malware, specifically Winnti v5.0, which has been enhanced with features such as improved obfuscation, updated encryption algorithms, and evasion techniques against security products. The group has been noted for its sophisticated techniques and continued evolution of its malware since its initial reports dating back to 2013. Winnti v5.0 has been noted for its advanced features, including improved obfuscation, updated encryption algorithms, and enhanced evasion techniques against security measures.

Capabilities:

1. Rootkit Functionality: The Winnti malware includes rootkit capabilities allowing it to hide its presence on infected machines.

2. Remote Access: It utilizes a Remote Access Trojan (RAT) to control infected devices, enabling attackers to execute commands remotely.

3. Data Exfiltration: The malware can send sensitive data back to the attacker through encrypted communications, making detection difficult.

4. DLL Hijacking: Winnti exploits legitimate DLL files to execute malicious code, thereby bypassing security measures.

5. Service Manipulation: It can manipulate Windows services to maintain persistence on infected systems.

6. Unique Decryption Keys: The malware uses unique information from the infected device as a decryption key, complicating analysis and remediation efforts .

7. Evasion Techniques: Enhanced evasion techniques make it resilient against detection by security products.

8. Multi-Stage Deployment: The deployment process involves multiple stages, ensuring that the malware is thoroughly embedded in the system before executing malicious activities .

Distribution Methods of RevivalStone:

The RevivalStone campaign employs various distribution methods to infiltrate target organizations. Below are the primary techniques utilized:

1. Initial Intrusion Techniques:

SQL Injection Vulnerabilities: The attackers exploit SQL injection vulnerabilities found in the ERP systems of target organizations, which allows them to inject malicious code into the web server .

WebShell Deployment: Following the initial intrusion, attackers install a WebShell on the compromised web server, enabling them to maintain access and control over the system .

2. WebShell Utilization:

Types of WebShells Used: The campaign employs multiple WebShells, including:

A. China Chopper- China Chopper is identified as a generic web shell employed by a China-based attacker group. It is characterized by its unique string set, which functions as a parameter for receiving POST requests from compromised hosts. The attacker group utilizes this web shell for various activities, including executing commands and deploying malware, such as Winnti, on the target systems. The versatility and stealth of China Chopper make it a favored choice in cyber operations, allowing attackers to maintain control over compromised environments.

B. Behinder-Behinder, also referred to as "IceScorpion/ Bingxia" is a web shell developed by a Chinese-speaking programmer. It supports multiple platforms, including PHP, ASP, and JSP, and incorporates a range of backdoor functionalities. These features include:

a. File operations

b. Shell command execution

c. Proxy functions

d. Loading encrypted payloads using AES

C. sqlmap File Uploader- The sqlmap file uploader is a web shell with a graphical user interface (GUI) that facilitates file uploads. It functions as one of the payloads that can be generated by the sqlmap tool, which is commonly used for automating the process of detecting and exploiting SQL injection vulnerabilities. In the context of the described attack campaign, sqlmap was used as an initial intrusion method, which allowed attackers to deploy the associated web shells effectively. This tool's ease of use and effectiveness in bypassing security measures make it a critical asset for cyber attackers

D. UNAPIMON- One of the Winnti malware's components with detection evasion capabilities is UNAPIMON. This malware can evade analysis and monitoring by EDR and sandbox environments because it is implemented using code that stops its child processes from being watched. Winnti RAT's use of UNAPIMON in the RevivalStone campaign has been verified.

3. Lateral Movement:

Credential Harvesting: After establishing a foothold, the attackers use the WebShell to perform reconnaissance within the network, collecting credentials to facilitate lateral movement across the organization’s infrastructure .

4. Malware Deployment

Winnti Malware: The campaign relies on various versions of Winnti malware, with Winnti v5.0 being the latest iteration used during the RevivalStone attacks. This malware is capable of sophisticated evasion techniques and system manipulation.

DLL Hijacking: The execution flow of the Winnti malware involves DLL hijacking, where malicious code is executed by loading a legitimate file that is modified to include the attacker's code.

5. Rootkit Installation

Winnti Rootkit: The attackers deploy the Winnti Rootkit, which allows deeper system access and the ability to hide malicious activities from security measures

Impacts of RevivalStone:

The impacts of the campaign on targeted organizations include:

1. Financial Loss: Significant costs incurred from data breaches and recovery efforts.

2. Operational Disruption: Temporary or prolonged disruption of business operations.

3. Reputation Damage: Loss of customer trust and damage to brand reputation.

4. Data Loss: Unauthorized access and exfiltration of sensitive data.

5. Compliance Violations: Potential legal penalties due to breaches of data protection regulations.

INDICATORS OF COMPROMISE:

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

e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596

c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad

569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8

169d35bdb36c2bfcb3bbf64392de1b05d56553172a13cae43a43acbe2aa18587

b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090

4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779

1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*SEND OF IOCs\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **[CMTX-P-022025235] 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

45.76.199.23

103.244.0.126

103.218.243.167

195.211.98.122

16.162.141.226

1. **[CMTX-I-876022025] Malicious Domains used for Phishing**

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, email-based fraud and malware distribution.

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

adictrict-up-gov.info

cloudzy.com

cyberdelhipolice-gov.info

gov.in.indsx.in

indianarmy.nci.in

indiapostgovin.click

indiapostgovin.help

indiapostgovin.sbs

mailgov.top

rajsthan-gov.in.webex.com.in

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

1. **[CMTX-P-022025245] 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 : Port

38.60.199.60:443

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

1. **[CMTX-I-688022025] Malicious Domains used by Threat Actors**

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

coord.site

digilockergov.info

\*.coord.site

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

1. **[CMTX-P-022025825] Stately Taurus Activity**

Alert Brief:

Stately Taurus is a cyber threat actor group targeting organizations in ASEAN countries. Recent analysis indicates that this group has been linked to activities involving the Bookworm malware and its variants, as well as the ToneShell malware. These malicious activities have been reported in various attacks, including a notable incident in Myanmar in January .

Stately Taurus Malwares:

Bookworm: This malware has been used since 2015 and has shown versatility, allowing it to be repackaged for various operational needs. It has been confirmed that Stately Taurus continues to develop and utilize Bookworm for their attacks.

ToneShell: Believed to be used exclusively by Stately Taurus, ToneShell employs a UUID technique to represent shellcode, enhancing its stealth and efficacy in attacks.

Distribution Methods:

1. DLL Sideloading: Stately Taurus commonly employs DLL sideloading to execute payloads, which enables the execution of malicious code through legitimate software processes.

2. Malicious URLs: Attacks have involved directing victims to compromised URLs that appear to be legitimate, such as those resembling Windows update services.

Impacts of Stately Taurus Activity:

The impact of Stately Taurus's operations includes:

1. Compromise of sensitive governmental and organizational data.

2. Potential disruption of services and operations for targeted entities in the region.

3. Long-term consequences on the cybersecurity posture of affected organizations.

INDICATORS OF COMPROMISE:

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

HASHES:

cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86

fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81

5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b

243b92959cd9aa03482f3398fbe81b4874c50a5945fe6b0c0abb432a33db853f

a0887fa90f88dd002b025a97b3a57e4fdb7f5fdd725490d96776f8626f528ef2

a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927

3e137da41cb509412ee230c6d7aac3d69361358b28c3a09ec851d3c0f3853326

fdad627a21a95ea2a6136c264c6a6cc2f0910a24881118b6eabc2d6509dc8dd7

ab54af1dbe6a82488db161a7f57cd74f2dd282a9522587f18313b4e9835dc558

3cef0b5f069cc1d15d36aa83d54d2a7be79b29b02081b6592dd4714639ad0a66

43de1831368e6420b90210e15f72cea9171478391e15efdd608ad22fe916cea8

2bae8b07f5098e1ca8fb5a5776eb874072ace4e19734cba4af4450eeccde7f89

a229a2943cf8d1b073574f0c050ca06392d0525b2028f4b4b04d1e4b40110c66

9192a1c1ab42186a46e08b914d66253440af2d2be6b497c34fe4b1770c3b5e01

4a92fa725adc57d7b501f33e87230a8291cf8ad22d4d3a830293abcc0ac10d12

da8ef50fe5e571d0143a758c7c66bb55653f1f2d04f16464fc857226441d79b2

f0df09513dcf292264b3336269952c7e9ff685df8180a2035bee9f3143b36609

b7e042d2accdf4a488c3cd46ccd95d6ad5b5a8be71b5d6d76b8046f17debaa18

41276827827b95c9b5a9fbd198b7cff2aef6f90f2b2b3ea84fadb69c55efa171

167a842b97d0434f20e0cd6cf73d07079255a743d26606b94fc785a0f3c6736e

4fbfbf1cd2efaef1906f0bd2195281b77619b9948e829b4d53bf1f198ba81dc5

4e8717c9812318f8775a94fc2bffcf050eacfbc30ea25d0d3dcfe61b37fe34bb

98d6db9b86d713485eb376e156d9da585f7ac369816c4c6adb866d845ac9edc7

a02766b3950dbb86a129384cf9060c11be551025a7f469e3811ea257a47907d5

4b6f0ae4abc6b73a68d9ee5ad9c0293baa4e7e94539ea43c0973677c0ee7f8cb

eb176117650d6a2d38ff435238c5e2a6d0f0bb2a9e24efed438a33d8a2e7a1ea

DOMAINS:

[http://www.fjke5oe.com]www.fjke5oe.com

update.fjke5oe.com

[http://www.i5y3dl.com]www.i5y3dl.com

[http://www.hbsanews.com]www.hbsanews.com

[http://www.b8pjmgd6.com]www.b8pjmgd6.com

[http://www.zimbra.page]www.zimbra.page

[http://www.ggrdl4.com]www.ggrdl4.com

[http://www.gm4rys.com]www.gm4rys.com

IPs

123.253.32.15

123.253.35.231

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

1. **[CMTX-P-VUL-022025835] 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: 21022025\_VULN\_LIST.pdf

1. **[CMTX-I-344022025] Threat Actors Using Cloud-Based File Storage Domains**

Threat actors are leveraging blockchain technology to store malicious payloads and using Linux remote agents & RATs (Remote Access Trojans) to gain persistent access to target systems. Additionally, blockchain-based file storage is being misused for stealthy data exfiltration and malware distribution.

Prevention Measures:

> Monitor outbound connections to blockchain nodes and unusual network activity.

> Restrict execution of unverified Linux remote agents & enforce strict privilege controls.

> Audit crontabs regularly (crontab-l & /etc/crontab) for unauthorized entries.

> Harden SSH & system configs to prevent unauthorized remote access.

> Regularly audit installed agents and remove suspicious binaries.

With Ref. to previous alerts:

CMTX-I-014092024 dated 25/09/2024

CMTX-I-446092024 dated 06/09/2024

CMTX-I-443092024 dated 04/09/2024

CMTX-I-514052024 dated 31/05/2024

CMTX-I-137032024 dated 22/03/2024

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

http://mainnet-seed-0002.nkn.org

https://saadac2.mywire.org

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

1. **[CMTX-I-911022025] Malicious Domains used by Threat Actors**

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

andhrauniversity.edu.in.services

co.in.services

cse.ap.gov.in.services

delhigovt.nic.in.services

ega.in.services

greentrends.in.services

jk.gov.in.services

mediaplayer.in.services

nic.in.services

njad.in.services

rtps.assam.gov.in.services

sarathi.parivahan.gov.in.services

sbilife.co.in.services

trafic.in.services

vahan.parivahan.gov.in.services

verifydocument.in.services

\*.in.services

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

1. **[CMTX-I-100022025] CrimsonRAT- APT36 campaign**

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>---------

107.189.26.70

94.72.108.218

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

1. **[CMTX-I-975022025] Mythic Malware- APT36 campaign**

Mythic is an advanced, customizable Command and Control (C2) framework primarily used by threat actors to control and manage malware operations. Mythic is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, MacOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents e.g. Apollo (Windows), Poseidon (Linux, MacOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Common Features of Mythic Malware:

  > Persistence

  > Remote access and data theft

  > Modular architecture and customizable

  > Stealth techniques to avoid detection by security software

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.).

  > For Windows- Uncheck "Hide extensions for known file types" in File Explorer's Folder Options under the View tab to display file extensions

  > For Linux- 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 of Mythic malware is as follows:

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

188.166.237.148

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

1. **[CMTX-P022025845] ACTIVE EXPLOITATION OF CVE-2024-24919 AFFECTING CHECK POINT NETWORK GATEWAY**

We are providing an update regarding the previously issued alert [CMTX-P022025845] on  active exploitation of CVE-2024-24919 affecting Check Point Network Gateway (TLP: CLEAR). Below, we have shared the Indicators of Compromise (IOCs) related to this campaign. We request you to take appropriate measures to mitigate any potential threats to your systems.

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

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

Domains:

updata.dsqurey.com

time.dsqurey.com

dscriy.chtq.net

system.chtq.net

updata.chtq.net

network.oossafe.com

notes.oossafe.com

caba.superdasqe.me

ccs.superdasqe.me

czs.superdasqe.me

kzb.superdasqe.me

HASH:

8d44f2f442ca8f2fbbf75086a6f8d518c300ca93fe9957a9716076919b475865

83c1a668ab06f55e6879593ca24eed9f78832be97ac90bb74ef5828067f2d900

c19be7a006bd2ba8deb56dcc6127a76f9624c6f1392a1794870dbed6f1a81bd5

c4db25ab55af2e943a297a5ecf7a62acc3ad8897ec8ba4ab3226a138da237b82

28e6362ecf033b2a26c7457dcbd7ad2ab34e253fb08666d39073391a1254ea41

7416f6b69b34b3a36a86e50808e1dc47f4dc665bfd6f394cef65e0ba5eaf961b

bc490047fe6e0b0000c6cd147d3cf483105c92cf00450bfe35ac70f276a9e5c8

c5f8a256d0969e253633160b9728b6c2bc044f536e92af178a05a598aaa09c1f

a2bb321d41b2300e80f9400950fa2125470d5b3927933ab4d6397f0cbf81532a

d74b6b2129936377aaccc619bcfd4df4ffbe2f35f960a4b043b23ae78a31ec35

366ea3377eaefa28b655b530710c03fb2ace67bb531b1820e916cb02023892ba

f8915c5be0649642dac22572355f1462972f5087471f66f6a243f2374b208eb8

b38dab1ee402f731313d697d5d79372ae97fcab5704077771b5b82e705e0cd6d

625ed0e0ad7d3fbf2738349c767a7990c9f0d388de66104e11df3e0c4632033c

431a630983cd327fc70ea49b3a5497a179dbde19d8f13d2cfceef4e47613024b

e1d72b0cfc3342b8a6436e3047c3cc54246c346ac179e459d07620d192ba6e01

fa7f2ddf91980d639a87465bd2a38eaa44d6079b11ace3b2b3dff03caed66de5

b28bc39e569aa0cfe984c341830cb037c5305877ba22a940c3bdaeb43ca87878

571607c7f55c3616e4c58db15e3d55317da10294dbc10e0cd1ed24879b8fc051

bc5b2ef81593095696433877cccb0ab75ef942258ef4795de5538df842d952f4

fa3a3351cd55089d40a7311e4bfaf15e4247416f78383d94ad58809467429b3e

2df4c7bfa608ca88d9d659358894226910850ac0d7e566c6c10ec2727361d47b

b66660dfe1ce69f706aaa412fcd3ff18554d604df59c09adc2a8117417967ce9

7b8ea6b1e2a29190cb28fc98ef837bf4a7a0b71b84177ce9395a5113a843c4d3 ( Ransomware)

de4bb30e400f081601d4091206ba6c04ac502f50e0dbac879db8c0202bff8108 ( Ransomware)

5dc36e687a7fa3cfbf845e8a53173f37ac38559b6b87f9dcf609a72b3f284035 ( Ransomware)

37039a761114251f4556e4fe41c3ec01b7206a483c4698ffe5a0f1617a8bc26b ( Ransomware)

fcb8bf42d852526214578ab4b477b29f2412a7a931c6353db4fa6c221661edf4 ( Ransomware)

ceac8b67f19d596b2c2f34d682f88c717d11dd4c1144e2e7439b6bb78adb1736 (CQHashDump tool)

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

1. **[CMTX-I-112022025] Malicious Domains used by Threat Actors**

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

trending.hammersmith.com.my

dashboard.india.gov.in.hammersmith.com.my

copper.kbccompany.in

\*.hammersmith.com.my

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

1. **[CMTX-I-441022025] Malicious Domains used by Threat Actors**

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

accountmygov.info

crsorgi.gov.in.web.i.viewcert.org

crsorgi.gov.in.web.index.php.auth.viewcert.org

crsorgi.gov.in.web.index.php.viewcert.org

crsorgi.gov.in.web.viewcert.org

dc.crsorgi.gov.in.web.index.php

dc.crsorgi.gov.in.web.index.php.viewcert.org

digitalguidegov.in.zjhcwthm.a2hosted.com

gov.in.web.index.php.viewcert.org

gov.in.web.viewcert.org

in.web.index.php.auth.viewcert.org

in.web.viewcert.org

mail.viewcert.org

ww25.gov.incometaxindia.org

www.dev.incometaxindia.org

www.gov.incometaxindia.org

www.home.incometaxindia.org

www.incometaxindia.org

\*.incometaxindia.org

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

1. **[CMTX-P022025625] Auto-color Malware**

Threat Overview:

Auto-color is an emerging Linux backdoor malware, which employs various obfuscation and evasion techniques to avoid detection and maintain persistent access to compromised systems. Initially, the malware renames itself to a benign-looking name, making it difficult for administrators to identify. However, the typical methods for such malware include phishing emails, compromised software downloads, or exploiting known vulnerabilities in Linux systems. The malware's ability to grab payload data suggests a sophisticated pre-installation method that may involve pre-compilation targeting specific systems

Indicators of Compromise (IOCs):

Hashes:

270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43

65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4

83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a633

a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d53d0a

bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f02d6b

e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc3048f7

85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042bb255

bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b051510d1ca

IPs:Port

146.70.41.178:443

216.245.184.214: 443

146.70.87.67:443

65.38.121.64: 443

206.189.149.191: 443

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

1. **[CMTX-I-820022025] WhatsApp Web QR Code Phishing Targeting Government Officials**

Recently, threat actors have been observed targeting government officials by sending attachments containing links that prompt users to scan malicious QR codes, impersonating legitimate WhatsApp Web login prompts. Once scanned, the attacker's device gains persistent access to the victim’s WhatsApp account (session hijacking). This allows the attacker to read, send and receive messages, steal contacts and manipulate conversations. The attacker remains logged in until manually removed, maintaining access while covertly monitoring user activity.

Prevention Measures:

> Do NOT scan unknown QR codes received via email, messages, or websites.

> Verify linked devices in WhatsApp settings and remove any unrecognized sessions.

> Enable two-step verification in WhatsApp for added security.

> Log out of all devices if you suspect unauthorized access.

> Report suspicious activity to WhatsApp and update your app regularly.

Recent IOCs of this campaign are as follows:

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

acc.mail-open.com

account.mail-open.com

csp.mail-open.com

events.api.mail-open.com

live.mail-open.com

mailairforce.mail-open.com

mofamyanmar.mail-open.com

outlook.mail-open.com

reporting.mail-open.com

\*.mail-open.com

1. **[CMTX-I-860022025] Malicious Domains used by Threat Actors**

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

email.gov.in.indiadefencedepartment.link

\*.indiadefencedepartment.link

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

1. **[CMTX-I-352022025] Malicious Domains used for Phishing**

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

indiaapostgovin.click

indiapostgov.ink

efilegovinfo.com

indiaapostgovin.help

homeaffairs-gov.info

dc.csrogi.gov.in.web-index.cloud

pay-specificity.verifycentralid-gov.inc.expreseeable.com

verifycentralid-gov.inc.expreseeable.com

cogov.in.rs

patnahighcourt.onlinepanel.in.net

mahaprisons.onlinepanel.in.net

aiimsexams.onlinepanel.in.net

agricoop.gov.in.onlinepanel.in.net

jointerritorialarmy.onlinepanel.in.net

bcclweb.onlinepanel.in.net

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

1. **[CMTX-I-699022025] SideCopy- C&C of Malware Campaign**

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 (hosting malware) used by this threat actor are as follows:

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

93.123.109.214

aintssa.in (compromised domain)

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

1. **[CMTX-P-VUL-022025715] Prominent Vulnerability List**

Alert Brief:

It has been discovered that North-Korea linked threat actors are found to be using different malwares (RustDoor and "Koi" Stealer)to target cryptocurrency sector primarily. A Rust-based macOS malware "RustDoor" disguised as a software update along with a new variant of "Koi Stealer" were used in the campaign by North Korean APT groups.

The malware uses rare evasion techniques (namely, manipulating components of macOS to remain under the radar) to avoid detection on macOS. This campaign aims to steal sensitive data and cryptocurrency from users in the cryptocurrency sector. The attackers utilize social engineering techniques to infiltrate networks and compromise endpoints, highlighting a sophisticated approach to cybercrime.

RustDoor: First discovered in February 2024, RustDoor is a highly advanced backdoor malware that mostly targets macOS users, especially those involved in the cryptocurrency industry. It first obtains access through social engineering techniques, frequently posing as genuine Visual Studio software upgrades or through phony employment offers that result in malicious ZIP packages that include shell scripts.

Koi Stealer: The Koi Loader/Koi Stealer malware, linked to North Korean actors, is targeting the cryptocurrency sector since January 2025. The campaign uses social engineering to trick freelance developers into running malicious software disguised as job offers or updates, including a Visual Studio challenge named "SlackToCSV.".

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

HASHES:

a900ec81363358ef26bcdf7827f6091af44c3f1001bc8f52b766c9569b56faa5

baa676b671e771bf04b245e648f49516b338e1f49cbd9b4d237cc36d57ab858d

76f96a35b6f638eed779dc127f29a5b537ffc3bb7accc2c9bfab5a2120ea6bc9

adde2970b40634e91b9ef8520f8e50eaa7901a65f9230e65d7995ac1a47700ef

c379f4ab29a49d4bccb232c8551d1b8b01e64440ea495bbabef9010a519516c3

a5b7ddd12539ce3e8c08bed5855ddcea3217d41d7d4c58fcc1a7e01336b38912

b5412375477a180608bf410f5cb36b4a0949bee7663648a06879f42be9a3b6bc

b5119a49830a2044f406645c261e54ab335c9b1e1ed320df758405a8147fae88

17064520feaf5804aa725e123b24fd0f73f8afc9b7f4361650cd11ddf4ee768f

8be62324fe5af009c12fb9afc8d4f47d12c98ea680bff490b3f5e0c72c8f9617

77361f7ef25a0185636a0fc6deff2e9986720223da9d6b1494f671082105bebb

27fcc3278afbbec44737e9f72666946607fea819f5b1cb9fbbe268037a561f0b

97abafff549ea21797c135c965c5e4a46a44ec7353b2edd293e8a22d5954b6aa

c42b103b42d7e9817f93cb66716b7bf2e4fe73a405e0fbbae0806ce8b248a304

8f0e2b8b3e07f5761066cb00bc0db10d68c56ada8c054e9f07990cc1ac5ae962

DOMAINS:

apple-ads-metric.com

visualstudiomacupdate.com

IPs:

5.255.101.148

31.41.244.92

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

1. **[CMTX-P-022025745] RUSTDOOR AND "KOI" STEALER USED BY NORTH-KOREA APT GROUP**

Alert Brief:

It has been discovered that North-Korea linked threat actors are found to be using different malwares (RustDoor and "Koi" Stealer)to target cryptocurrency sector primarily. A Rust-based macOS malware "RustDoor" disguised as a software update along with a new variant of "Koi Stealer" were used in the campaign by North Korean APT groups.

The malware uses rare evasion techniques (namely, manipulating components of macOS to remain under the radar) to avoid detection on macOS. This campaign aims to steal sensitive data and cryptocurrency from users in the cryptocurrency sector. The attackers utilize social engineering techniques to infiltrate networks and compromise endpoints, highlighting a sophisticated approach to cybercrime.

RustDoor: First discovered in February 2024, RustDoor is a highly advanced backdoor malware that mostly targets macOS users, especially those involved in the cryptocurrency industry. It first obtains access through social engineering techniques, frequently posing as genuine Visual Studio software upgrades or through phony employment offers that result in malicious ZIP packages that include shell scripts.

Koi Stealer: The Koi Loader/Koi Stealer malware, linked to North Korean actors, is targeting the cryptocurrency sector since January 2025. The campaign uses social engineering to trick freelance developers into running malicious software disguised as job offers or updates, including a Visual Studio challenge named "SlackToCSV.".

Distribution Methods :

1. Phishing Campaigns: RustDoor is often distributed through deceptive emails that entice users to download malicious attachments or links.

2. Malicious Websites: It can also be downloaded from compromised or fake websites that mimic legitimate services.

3. Drive-By Downloads: Exploits vulnerabilities in browsers or plugins to automatically install the malware without user consent.

4. Malicious Downloads: Koi Stealer is often bundled with legitimate software downloaded from untrustworthy sources.

5. Social Engineering: Attackers may use social engineering tactics to trick users into installing the malware.

6. Exploit Kits: It can be delivered via exploit kits that take advantage of software vulnerabilities.

INDICATORS OF COMPROMISE:

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

HASHES:

a900ec81363358ef26bcdf7827f6091af44c3f1001bc8f52b766c9569b56faa5

baa676b671e771bf04b245e648f49516b338e1f49cbd9b4d237cc36d57ab858d

76f96a35b6f638eed779dc127f29a5b537ffc3bb7accc2c9bfab5a2120ea6bc9

adde2970b40634e91b9ef8520f8e50eaa7901a65f9230e65d7995ac1a47700ef

c379f4ab29a49d4bccb232c8551d1b8b01e64440ea495bbabef9010a519516c3

a5b7ddd12539ce3e8c08bed5855ddcea3217d41d7d4c58fcc1a7e01336b38912

b5412375477a180608bf410f5cb36b4a0949bee7663648a06879f42be9a3b6bc

b5119a49830a2044f406645c261e54ab335c9b1e1ed320df758405a8147fae88

17064520feaf5804aa725e123b24fd0f73f8afc9b7f4361650cd11ddf4ee768f

8be62324fe5af009c12fb9afc8d4f47d12c98ea680bff490b3f5e0c72c8f9617

77361f7ef25a0185636a0fc6deff2e9986720223da9d6b1494f671082105bebb

27fcc3278afbbec44737e9f72666946607fea819f5b1cb9fbbe268037a561f0b

97abafff549ea21797c135c965c5e4a46a44ec7353b2edd293e8a22d5954b6aa

c42b103b42d7e9817f93cb66716b7bf2e4fe73a405e0fbbae0806ce8b248a304

8f0e2b8b3e07f5761066cb00bc0db10d68c56ada8c054e9f07990cc1ac5ae962

DOMAINS:

apple-ads-metric[.]com

visualstudiomacupdate[.]com

IPs:

5[.]255[.]101[.]148

31[.]41[.]244[.]92

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

1. **[CMTX-P-022025585] 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 : Port

45.83.130.69:8080, 80, 443, 8443

207.148.72.105:53, 443

154.90.63.250:443

194.87.18.73:443

38.60.250.74:443

45.32.151.219:443

104.238.135.232:80

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

1. **[CMTX-P-022025485] 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

103.43.18.92:80, 443

194.56.225.13:53, 80, 443

20.2.64.10:80, 443

5.253.41.53:80, 443

5.34.176.111:80, 443

64.176.6.235:53, 443

158.247.244.252:443, 8080

103.244.0.125:53, 443

182.255.45.230:80

38.54.94.86:443

154.90.48.107:8081

2.58.14.207:80

103.87.8.172:53

121.43.132.252:443

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