**Cyber Security Advisories**

**Date: 30 September 2024**

1. **CMTX-P-092024085: MYTHIC/POSEIDON MALWARE CAMPAIGN**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

Threat Overview

1. Threat Campaign: Mythic/ Poseidon Malware Campaign

Mythic Malware is a sophisticated piece of software used by cyber actors (observed several campaigns from Pakistan based threat actors) to conduct various types of cyberattacks. This malware is designed to infiltrate systems, exfiltrate sensitive information, and maintain persistent access. It operates by exploiting vulnerabilities in software or operating systems to install itself covertly. Once installed, Mythic Malware can perform actions such as capturing keystrokes, accessing files, and sending data back to the attackers. Its use is primarily focused on espionage and data theft, making it a significant tool in cyber intelligence operations.

POSEIDON is a backdoor that has the ability of data mining. POSEIDON is made to specifically target POS terminals and retrieve payment card data from them. Poseidon connects to a remote command and control server over HTTP. POSEIDON can download and upload files, install keyloggers, run arbitrary code, install persistence mechanisms, and access memory to find credit card details.

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 : A cross-platform, post-exploit, red teaming framework

3. Severity: High

Affected Systems/Assets

• . Windows, Linux, and macOS platforms can host Mythic C2 servers or Agents running on these systems can be affected by Mythic.

Distribution Methods

• Phishing Emails with context aware themes and malicious attachment or links mostly from Compromised email Accounts

IP Addresses:

143.198.64.151

206.189.134.185

64.176.40.100

47.245.114.11

107.191.62.175

108.61.163.195

108.61.190.25

138.68.134.123

139.84.227.243

149.248.51.25

149.28.177.78

152.42.162.105

158.247.231.22

159.223.224.93

161.35.207.209

165.232.177.53

165.232.180.251

170.64.132.144

185.170.144.146

216.238.83.145

38.54.63.8

5.252.179.6

62.113.113.110

64.176.162.36

64.176.164.107

64.176.168.231

64.176.196.183

65.20.81.156

70.34.195.186

70.34.198.15

1. **[CMTX-P-092024095] 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:

1. 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.

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

3. 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 : Multimodular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses

103.87.10.214

139.180.193.182

14.225.192.198

151.236.15.145

185.151.146.133

213.218.255.223

216.238.68.75

23.27.101.82

37.143.131.25

38.54.50.46

38.54.76.41

38.60.199.119

38.60.199.85

38.60.217.161

45.131.179.24

45.135.118.131

45.135.118.227

45.32.32.252

5.34.176.79

80.240.16.246

1. **[CMTX-P-092024105] 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

IP Addresses

154.36.144.211

154.36.144.212

154.36.144.213

154.36.144.214

154.36.144.215

154.36.144.216

154.36.144.217

154.36.144.219

154.36.144.220

154.36.144.221

154.36.144.222

154.36.144.223

154.36.144.224

154.36.144.225

154.36.144.226

154.36.144.227

154.36.144.228

154.36.144.229

154.36.144.230

154.36.144.232

154.36.144.233

154.36.144.234

154.36.144.235

154.36.144.236

154.36.144.237

154.36.144.238

154.36.144.239

154.36.144.240

154.36.144.241

154.36.144.242

154.36.144.243

154.36.144.244

154.36.144.246

154.36.144.247

154.36.144.248

154.36.144.250

154.36.144.251

154.36.144.252

154.36.144.254

154.36.146.130

154.36.146.131

154.36.146.133

154.36.146.135

154.36.146.136

154.36.146.138

154.36.146.139

154.36.146.140

154.36.146.141

154.36.146.142

154.36.146.143

154.36.146.144

154.36.146.145

154.36.146.146

154.36.146.147

154.36.146.148

154.36.146.149

154.36.146.150

154.36.146.151

154.36.146.152

154.36.146.153

154.36.146.154

154.36.146.155

154.36.146.156

154.36.146.157

154.36.146.160

154.36.146.162

154.36.146.164

154.36.146.165

154.36.146.166

154.36.146.167

154.36.146.168

154.36.146.169

154.36.146.170

154.36.146.171

154.36.146.172

1. **[CMTX-I-876092024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

indiannavykarwar.in

indiannavyeclaim.in

indianarmynic.in

sci-dailyorderssecurelogin.in

scidailyordercure-login.in

embassyofindiaukraine.in

indianairforceapp.com

modgov.org

modgov.com

incicourtgov.com

incourtsci.com

rbigov.info

mha-gov.info

indiannavy.info

scicourtgov.com

scicourtin.com

scidailyordercure-login.in

supremecourtcase.net

incicourtgov.com

labour-gov.info

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

1. **[CMTX-P092024674] Command Injection Vulnerability Affecting Ivanti Cloud Service Appliance (CVE-2024-8190)**

Product impacted: Ivanti Cloud Service Appliance

Impact: Unauthorized access and remotely execute commands on a vulnerable CSA.

Severity: Critical

Affected Systems: Ivanti Cloud Service Appliance (CSA) product, affecting versions 4.6 and earlier.

Attack vector:

Command Injection

Insufficient Input Validation

Cross-site Request Forgery

Executive Summary:

Ivanti CSA is a web-based platform that offers secure access and management for cloud services, enabling users to connect to internal network resources via a controlled gateway. CVE-2024-8190 allows threat actors with administrative privileges to gain unauthorized access and execute commands remotely on a vulnerable Ivanti Cloud Service Appliance. Since Ivanti CSA 4.6 has reached its end-of-life, it will no longer receive updates. The existence of proof-of-concept (PoC) code and ongoing discussions about potential exploitation highlight the urgent need to take action to safeguard assets from possible compromise.

Detection of compromise device:-

Check the login detail in (/var/log/messages) for failed and successful logon. For more detail, please refer the below link:

https://www.horizon3.ai/attack-research/cisa-kev-cve-2024-8190-ivanti-csa-command-injection/

1. **CMTX-I-514082024: SideCopy Malware C&C IP**

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

IP Addresses:

154.36.146.173

154.36.146.175

154.36.146.176

154.36.146.178

154.36.146.179

154.36.146.180

154.36.146.182

154.36.146.183

154.36.146.184

154.36.146.185

154.36.146.186

154.36.146.187

154.36.146.188

154.36.146.189

154.36.146.190

154.36.146.191

154.36.146.192

154.36.146.193

154.36.146.194

154.36.146.195

154.36.146.196

154.36.146.197

154.36.146.198

154.36.146.199

154.36.146.200

154.36.146.201

154.36.146.202

154.36.146.203

154.36.146.204

154.36.146.207

154.36.146.208

154.36.146.210

154.36.146.211

154.36.146.212

154.36.146.213

154.36.146.214

154.36.146.215

154.36.146.216

154.36.146.218

154.36.146.219

154.36.146.220

154.36.146.221

154.36.146.222

154.36.146.224

154.36.146.225

154.36.146.226

154.36.146.227

103.127.125.204

103.127.125.206

103.127.125.218

103.127.125.219

103.127.125.225

103.43.18.19

103.43.9.164

104.208.73.38

110.50.48.232

139.155.139.191

147.78.12.202

154.36.144.130

154.36.144.131

154.36.144.132

154.36.144.133

154.36.144.134

154.36.144.135

154.36.144.136

154.36.144.138

154.36.144.139

154.36.144.140

154.36.144.141

154.36.144.142

154.36.144.143

154.36.144.144

154.36.144.145

154.36.144.146

154.36.144.147

1. **CMTX-I-707092024: Malicious Domains used by Threat Actors [TLP: AMBER]**

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

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

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

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

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

email-gov-in.a5e1.com

email.gov.in.briefreport.nl

\*.briefreport.nl

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

1. **[CMTX-I-950092024] C2 IP of Malware Targeting Govt. Officials [TLP: AMBER]**

Threat Overview

Malware is often spread through spear-phishing emails, where attackers target specific individuals using tailored messages to trick them into clicking malicious links or downloading infected attachments. These emails appear legitimate, often impersonating trusted contacts or organizations. Once opened, the malware can steal data, provide remote access, or further infect the network.

The latest C2 of the malware targeting government officials is:

- ---------< C2 IP>---------

103.26.10.72

- ---------</C2 IP>---------

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

1. **[CMTX-P-092024125] 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

IP Addresses:

154.36.144.148

154.36.144.149

154.36.144.150

154.36.144.151

154.36.144.152

154.36.144.153

154.36.144.154

154.36.144.155

154.36.144.156

154.36.144.157

154.36.144.158

154.36.144.159

154.36.144.160

154.36.144.162

154.36.144.163

154.36.144.164

154.36.144.165

154.36.144.166

154.36.144.167

154.36.144.168

154.36.144.169

154.36.144.170

154.36.144.171

154.36.144.172

154.36.144.173

154.36.144.174

154.36.144.175

154.36.144.176

154.36.144.178

154.36.144.179

154.36.144.180

154.36.144.181

154.36.144.182

154.36.144.183

154.36.144.184

154.36.144.185

154.36.144.186

154.36.144.187

154.36.144.188

154.36.144.189

154.36.144.190

154.36.144.191

154.36.144.192

154.36.144.193

154.36.144.194

154.36.144.195

154.36.144.196

154.36.144.197

154.36.144.198

154.36.144.199

154.36.144.200

154.36.144.201

154.36.144.202

154.36.144.204

154.36.144.205

154.36.144.206

154.36.144.207

154.36.144.208

154.36.144.209

154.36.144.210

154.36.144.231

154.36.144.245

154.36.144.249

154.36.144.253

154.36.146.132

154.36.146.134

154.36.146.137

154.36.146.158

154.36.146.159

154.36.146.161

154.36.146.163

154.36.146.174

154.36.146.177

154.36.146.181

154.36.146.206

1. **[CMTX-I-007092024] Mythic Malware- APT36 campaign [TLP: AMBER]**

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.

Recent C&C server of Mythic malware and its associated IPs are as follows:

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

64.225.100.125

157.245.146.223

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

1. **[CMTX-I-940092024] Malicious Domain used by Threat Actors [TLP: AMBER]MTX-P082024115: CVE-2024-38193**

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

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

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

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

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

www.www.cms.gov.indianrail.com

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

1. **[CMTX-P-092024135] 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

IP Addresses:

142.202.205.38

34.81.228.78

64.7.198.130

45.142.166.112

149.104.2.160

38.60.255.42

47.238.98.194

103.108.67.58

34.84.134.228

1.94.136.42

192.248.183.208

34.92.77.165

172.94.9.43

154.90.58.20

172.94.9.49

2.58.15.166

172.111.244.178

154.82.85.79

103.199.16.196

107.155.55.15

45.32.148.180

118.107.44.134

103.201.131.181

172.111.233.13

118.107.44.132

1. **[CMTX-P092024944] New Variant of RansomHub Ransomware [TLP: AMBER]**

Threat Overview:

Threat Campaign: RansomHub Ransomware

The RansomHub Ransomware Group remains a significant threat in the cyber landscape, operating as a Ransomware-as-a-Service (RaaS). Their attack strategies often exploit known vulnerabilities such as CVE-2023-3519 and CVE-2020-1472, using initial access methods like phishing and password spraying. Once they breach targeted networks, they employ tactics like renaming ransomware executables to avoid detection and disabling antivirus software with legitimate tools such as TDSSKiller and LaZagne.

Recently, a new locker variant from RansomHub has been identified, specifically designed to target SFTP servers. Unlike previous variants, this one does not encrypt files on the local system. Instead, it connects to a user-specified remote SFTP server and recursively encrypts files within designated directories. This locker is compiled for Windows systems and targets ESXi, NAS, and various SFTP servers. Similar to earlier RansomHub lockers, it requires a password for execution.

Threat Type: Ransomware

Severity: High

Affected Systems: VMware ESXi, NAS, and various SFTP servers

Indicators of Compromise (IOCs):

HASH:

2d823c8b6076e932d696e8cb8a2c5c5df6d392526cba8e39b64c43635f683009

467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486

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

MITRE ATTACK IDENTIFIER:

T1486 (Data Encrypted for Impact)

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

1. **[CMTX-P-092024145] 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:

1. 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.

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

3. 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 : Multimodular backdoor

3. Severity: High

IP Addresses:

154.31.217.197

103.205.211.174

95.179.134.240

103.27.111.132

115.112.241.150

154.90.58.95

38.180.35.224

1. **[CMTX-P-092024155] 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

IP Addresses:

154.36.146.209

154.36.146.217

154.36.146.228

154.36.146.229

154.36.146.230

154.36.146.231

154.36.146.232

154.36.146.233

154.36.146.234

154.36.146.235

154.36.146.236

154.36.146.237

154.36.146.238

154.36.146.239

154.36.146.240

154.36.146.241

154.36.146.242

154.36.146.243

154.36.146.244

154.36.146.245

154.36.146.246

154.36.146.247

154.36.146.248

154.36.146.249

154.36.146.250

154.36.146.252

154.36.146.253

154.36.146.254

172.111.233.73

172.94.9.114

2.58.14.134

202.144.192.146

202.182.108.248

206.238.40.113

34.125.227.13

38.54.79.215

38.60.255.163

43.231.113.78

43.248.133.13

45.201.215.122

45.201.215.123

45.201.215.124

45.201.215.125

45.201.215.126

45.58.47.141

45.80.215.19

46.30.188.239

52.77.42.172

54.167.79.208

64.176.58.12

8.217.239.245

96.43.101.229

96.43.101.245

1. **[CMTX-P092024954] Relay server Nodes used by Chinese actors [TLP: RED]**

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

IP ADDRESSES:

103.106.195.155

103.110.172.118

103.120.130.114

103.139.171.238

103.147.249.126

103.161.148.42

103.163.100.105

103.203.172.126

103.206.139.103

103.207.65.11

103.210.45.36

103.211.39.110

103.213.210.46

103.217.78.42

103.217.79.31

103.221.76.184

103.250.187.137

103.252.145.75

103.4.233.18

103.42.156.18

103.44.53.68

103.44.97.168

103.48.199.88

103.75.225.110

103.77.45.143

103.78.170.45

103.90.159.38

106.51.251.167

106.51.82.45

110.173.188.164

111.92.41.85

111.92.61.39

113.193.24.15

114.143.149.210

115.114.98.18

115.242.180.154

115.242.202.110

115.242.230.194

115.242.234.242

115.242.249.70

115.244.148.142

115.245.91.98

116.75.1.215

117.193.160.165

117.211.9.4

117.211.9.44

117.217.122.92

117.217.122.99

117.239.22.170

122.160.50.212

122.162.147.15

122.168.117.103

122.169.42.170

122.180.21.10

122.185.43.6

122.187.217.130

123.255.249.118

125.16.215.122

125.18.1.42

125.22.51.182

125.62.118.152

136.232.200.46

136.232.211.246

139.167.47.70

139.167.56.10

14.141.81.74

14.194.242.66

14.98.72.62

148.113.5.21

150.129.144.136

150.129.144.147

182.70.125.139

182.70.241.234

182.71.120.18

182.74.142.101

183.82.122.123

202.131.109.90

202.131.115.90

202.134.205.103

202.140.130.240

202.47.118.229

202.88.246.161

203.92.61.146

43.248.32.18

43.255.140.13

45.112.202.22

45.114.68.218

45.115.168.110

45.115.168.47

45.115.55.18

49.205.176.104

49.205.176.138

49.205.178.101

49.248.45.155

49.249.151.252

49.36.136.97

59.144.175.16

59.90.28.227

59.92.127.214

60.243.50.97

1. **[CMTX-I-366092024] CrimsonRAT- APT36 campaign [TLP: AMBER]**

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

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

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

5.189.140.142

109.199.108.1

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

1. **[CMTX-P092024964] Relay server Nodes used by Chinese actors--ALERT2 [TLP: RED]**

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

Indicators of Compromise (IOCs):

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

IP ADDRESSES (Device Detail)

103.106.177.59

103.56.225.98

103.71.65.195

115.247.81.194

117.217.122.95

117.239.217.50

117.247.80.46

122.165.246.70

122.165.58.180

122.185.124.50

137.59.84.18

139.167.236.238

146.196.120.121

150.129.144.133

182.70.241.223

183.82.114.69

202.78.232.61

45.114.157.131

49.207.186.28

59.94.32.54

59.96.60.156

61.2.213.239

61.2.47.100

61.3.164.76

1.6.225.35

103.112.14.26

103.156.138.142

103.203.224.198

103.206.56.158

103.230.153.106

103.70.160.229

103.71.76.238

114.79.133.35

115.241.146.2

117.232.83.227

117.242.44.69

117.247.177.185

117.247.180.186

122.166.101.85

122.166.52.212

122.179.139.227

122.180.240.186

122.200.16.7

123.201.9.50

14.97.193.82

150.107.116.158

150.107.233.178

150.107.254.238

175.176.185.138

180.179.218.42

182.72.92.110

182.73.69.26

182.76.26.75

183.82.112.94

183.82.250.138

202.63.117.67

203.92.47.234

223.31.154.242

43.227.23.227

43.249.52.78

45.248.163.50

49.248.22.202

61.12.84.212

61.247.235.41

27.109.13.154

125.23.98.30

203.92.56.78

103.170.90.68

115.96.27.150

64.227.130.48

103.107.36.39

103.107.37.105

103.112.85.196

103.86.43.117

103.97.203.234

103.97.203.36

106.222.205.251

106.51.66.181

106.51.86.115

111.92.61.44

115.96.211.18

124.123.123.79

143.244.136.24

180.211.102.106

182.74.138.66

183.82.106.192

183.83.147.46

202.164.53.142

210.18.189.45

43.241.144.123

45.64.95.5

1. **[CMTX-I-521092024] Malicious Domains used by Threat Actors [TLP: AMBER]**

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

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

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

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

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

support-panel.in

serviceonline.bihar.gov.in.inbex.site

crsorgi.gov.in.inbex.site

bankofbaroda.e-nidhi.in

bpsc.e-nidhi.in

ftp.e-nidhi.in

incometax.e-nidhi.in

indiapost.gov.in.e-nidhi.in

irctc.gov.co.in.e-nidhi.in

mail.e-nidhi.in

mes.gov.in.e-nidhi.in

mha.gov.in.e-nidhi.in

ns.e-nidhi.in

patna.secretariat.e-nidhi.in

ssc.nic.in.e-nidhi.in

upsssc.e-nidhi.in

\*.e-nidhi.in

\*.inbex.site

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

1. **[CMTX-I-388092024] Android RAT Latest C&C IP [TLP: AMBER]**

Android Remote Access Trojans (RATs) are malicious software designed to remotely control and monitor Android devices. These trojans can access sensitive information, such as contacts, messages, emails, and even capture keystrokes and screenshots. They can also exploit device functionalities, including the camera and microphone, posing significant privacy and security threats.

Common Features of Android RATs:

Remote Control

Data Theft (contacts, messages, and call logs)

Surveillance (use of camera and microphone)

Keylogging

File Manipulation

Recent C&C server IP along with associated domain of Android RAT malware deployed by APT36 threat actor are as follows:

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

134.255.183.33

downlaods.org (malware hosting)

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

1. **[CMTX-I-901092024] Malicious Domains used by Threat Actors [TLP: AMBER]**

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

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

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

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

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

\*.gov.in.webindexes.info

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

1. **[CMTX-P092024964] Interactsh Tool [TLP: AMBER]**

Tool Overview:

Interactsh is an open-source tool that operates on a server-client model, enabling users to identify blind Out-of-Band (OOB) vulnerabilities that conventional testing methods might overlook. It detects out-of-band interactions by generating dynamic URLs; when these URLs are accessed by the target, they trigger a callback. This callback can then be used to identify potential vulnerabilities.

Originally, the Interactsh tool was designed for use by Red Teams during penetration testing. However, it has now gained popularity among attackers as well. Interactsh can be integrated with OWASP ZAP through the OAST add-on.

Attackers are leveraging various third-party open-source tools to test their exploits, finding it convenient to use these resources. This trend makes it challenging for defenders to block such traffic effectively based solely on services, IP addresses, or servers.

Features of Interactsh

• DNS/HTTP(S)/SMTP(S)/LDAP Interaction

• CLI / Web / Burp / ZAP / Docker client

• AES encryption with zero logging

• Automatic ACME based Wildcard TLS w/ Auto Renewal

• DNS Entries for Cloud Metadata service

• Dynamic HTTP Response control

• Self-Hosted Interactsh Server

• Multiple domain support (self-hosted)

• NTLM/SMB/FTP(S)/RESPONDER Listener (self-hosted)

• Wildcard / Protected Interactions (self-hosted)

• Customizable Index / File hosting (self-hosted)

• Customizable Payload Length (self-hosted)

• Custom SSL Certificate (self-hosted)

Detection & Prevention Steps

• Analyze security logs for unusual activity that might indicate misconfigurations. Check the logs for any incoming requests, Look for unusual patterns that may indicate malicious activity, such as repeated requests or requests from unexpected locations. This helps in identifying interactions initiated by an attacker.

• Configure alerts for specific triggers (e.g., certain payloads being hit) to notify potential attacks in real-time.

1. **[CMTX-I-884092024] Mythic Malware- APT36 campaign [TLP: AMBER]**

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

Recent C&C server of Mythic malware is as follows:

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

111.38.218.247

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

Network administrators may take required action against the above indicators of compromise (IOC).

1. **[CMTX-I-014092024] Malware Campaign Exfiltrating Data via Google API [TLP: AMBER]**

CERT-In has observed an unconventional malware technique, wherein the malware is exfiltrating documents on victim's machine to Google User account via API. Pakistan-based threat actors are sending emails containing malicious links. These links download malware which is disguised as legitimate documents. Upon execution the malware establishes persistence and starts exfiltrating the documents.

Conventionally, the data is exfiltrated to a attacker-controlled Command and Control (C2) IP/Domain. But in recent case, Google User account API was used to avoid suspicion in network traffic and bypass traditional defences. The following domains can be detected in network traffic:

- -----------< Domains to be Monitored>--------

oauth2.googleapis.com

apps.googleusercontent.com

googleapis.com

googleusercontent.com

- -----------</Domains to be Monitored>--------

- -----------< Malicious IP>--------

38.180.191.134

- -----------</Malicious IP>--------

Please note: These domains are legitimate domains and recently being used by threat actors to quickly and covertly transfer data without raising immediate suspicion. Moreover, it does not require an additional application to be installed in the victim machine for the data upload.

This tactic and technique of the attacker is similar to the previous alerts shared,

Ref:

CMTX-I-443092024 dated 04/09/2024

CMTX-I-137032024 dated 22/03/2024

CMTX-I-514052024 dated 31/05/2024

where malware made use of popular messaging platforms for exfiltrating data on victim's machine.

Action Required:

- - Network administrators must monitor traffic towards the above domains. Any POST requests/ large number of requests should be scrutinized to determine if they are legitimate or associated with phishing/ malware activity. If any unauthorized requests/ traffic are detected, these should be investigated, and remedial measures should be taken.

- - Appropriate actions could be taken against malicious IP

1. **[CMTX-I-333092024] CrimsonRAT- APT36 campaign [TLP: AMBER]**

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

1. **[CMTX-I-452092024] Malicious Domains used by Threat Actors [TLP: AMBER]**

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

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

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

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

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

coord-dept.in

uidai-gov.info

\*.uidai-gov.info

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

As threat actors are creating several sub-domains for malicious parent domains on a regular basis, hence it is necessary to block the parent domain as well as all of its possible sub-domains beforehand. This could be done by blocking the parent domain as a wildcard domain '\*.phishing-domain.com', where \* corresponds to the wildcard.

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

1. **[CMTX-P092024974] EDR Disable tool used by Threat actors, TLP:STRICT+AMBER**

Tools Overview:

Threat actors frequently employ various tools and techniques to disable Endpoint Detection and Response (EDR) systems. Recently, there have been observations of their use of legitimate system tools and commands to disable security features, as well as custom tools designed to bypass or disable security solutions. Some of the notable custom tools and malware utilized by threat actors include:

1. HRSword, commonly known as "Tinder Sword," is a standalone security analysis tool designed for comprehensive system monitoring and analysis, including process management and network oversight. However, threat actors have been seen exploiting this utility to disable and bypass legitimate EDR protections on targeted systems.

2. The EDR Silencer tool utilizes the Windows Filtering Platform (WFP) to prevent Endpoint Detection and Response (EDR) agents from reporting security events to their servers.

3. EDRSandBlast is an open-source tool that bypasses EDR systems by exploiting signed vulnerable drivers.

4. AuKill , EDRKillShifter, and Terminator (Spyboy) tools which utilize the "Bring Your Own Vulnerable Driver" (BYOVD) approach, where legitimate but outdated drivers are exploited to disable EDR functions, blocking detection and response capabilities, typically through varying system processes.

These tools are evolving, demonstrating capabilities like dynamic driver loading, memory-only execution, and disabling user land/kernel-level security mechanisms.

Indicators of Compromise (IOCs):

URL

http[:]//down-tencent.huorong.cn/upgrade8/1721095305/upgrade.html

http[:]//down-tencent.huorong.cn/upgrade8/1722942353/upgrade-x64.conf

http[:]//down-tencent.huorong.cn/upgrade8/1722942353/upgrade.html

1. **[CMTX-P092024984] Relay server Nodes used by Chinese actors--ALERT3 [TLP: RED]**

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

Indicators of Compromise (IOCs):

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

IP(Device detail) Port No.

103.109.44.91

103.132.243.178

103.172.145.9

103.206.105.146

103.217.78.205

103.238.110.253

103.253.203.10

103.62.237.194

103.88.129.62

103.94.110.68

111.90.169.44

115.245.114.178

115.245.162.102

116.193.131.8

117.200.73.245

117.247.80.114

117.248.109.65

122.180.242.203

14.99.243.254

182.70.243.110

202.56.217.234

219.91.211.168

43.249.53.202

45.249.80.153

103.112.85.196

103.113.0.140

103.170.42.198

103.186.220.54

103.207.11.186

103.214.226.55

103.240.205.248

103.249.83.115

103.252.168.29

103.26.48.114

103.3.40.246

103.80.64.59

103.88.236.90

116.72.136.232

117.242.153.226

118.185.212.210

122.200.16.13

136.232.188.126

139.5.102.245

14.139.236.195

14.143.7.170

183.82.109.228

202.142.102.106

202.53.71.18

203.101.65.14

210.18.176.91

210.212.72.165

223.29.195.222

49.207.12.152

49.45.130.114

61.12.70.242

110.227.185.86

103.154.55.82

103.138.154.163

103.204.52.52

103.208.224.218

103.216.71.93

103.83.255.26

103.95.48.188

106.222.204.32

116.193.137.181

117.219.45.21

119.82.83.50

122.172.84.114

122.176.27.18

14.102.44.139

183.82.109.55

183.82.251.184

183.87.185.177

202.131.117.118

202.164.50.130

43.242.247.50

43.243.83.96

43.255.141.181

45.113.249.87

45.115.168.45

45.116.228.210

49.37.152.57

61.0.40.54

1.22.207.17

1. **[CMTX-P-092024175] 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:

1. 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.

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

3. 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 : Multimodular backdoor

3. Severity: High

IP Addresses:

46.246.98.47

95.179.244.134

136.244.71.74

139.180.219.37

141.164.35.65

149.28.186.14

151.236.23.49

156.244.8.15

185.76.78.78

192.71.213.155

198.41.192.142

199.247.10.114

217.69.6.191

38.60.199.205

45.158.168.113

45.249.89.54

45.80.215.133

64.176.47.234

64.176.49.76

77.91.103.168

89.38.128.94

95.179.254.184

1. **[CMTX-P-092024165] 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

IP Addresses:

103.101.178.212

103.107.104.4

103.107.104.57

103.166.228.185

103.234.54.179

134.122.133.80

134.122.133.86

134.122.133.95

148.66.5.50

148.66.5.51

148.66.5.52

148.66.5.53

148.66.5.54

154.205.136.105

154.212.150.43

154.212.150.45

154.213.18.220

154.213.18.226

154.213.18.240

156.251.18.26

172.111.233.31

216.238.113.209

38.180.75.197

47.243.61.114

52.128.229.100

52.128.229.101

52.128.229.102

52.128.229.98

52.128.229.99

103.101.178.210

103.101.178.211

103.101.178.213

103.140.186.35

103.56.18.101

107.148.32.206

118.107.44.133

154.212.150.52

154.86.159.140

172.111.245.99

172.94.9.72

182.71.135.166

27.124.3.250

27.124.43.98

45.86.162.28

1. **[CMTX-P-7040920249] Agent Tesla Malware Alert [TLP:RED]**

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

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

93.216.70.207

162.241.224.14

103.192.80.246

213.189.52.181

46.175.148.58

148.66.136.151

47.76.82.23

92.205.7.112

192.185.190.185

37.27.98.198

78.128.81.95

35.198.173.35

148.251.209.169

166.62.27.188

45.252.248.26

173.254.31.34

193.141.65.39

195.205.152.179

110.4.45.197

106.0.62.69

199.79.62.115

162.214.80.31

184.168.111.8

192.254.225.166

188.127.239.250

217.116.201.44

195.252.110.253

167.235.180.68

162.254.34.31

87.250.224.36

119.59.123.82

185.166.84.140

103.6.196.236

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