**Cyber Security Advisories**

**Date: 30 October 2024**

1. **[CMTX-I-636102024] Recent IOCs of Chinese Malware Campaign**

Threat Overview

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.

With reference to previous alert CMTX-I-808102024 dated 15th October, 2024, additional IOC associated with such campaign are as follows:

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

188.208.141.218

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

1. **[CMTX-P-102024144] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses :Port

103.27.109.72:443

45.124.254.93:80

64.176.229.94:443

216.173.67.244:443

1. **[CMTX-P-102024154] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses: Port

47.243.41.120:443, 8080

202.91.36.213:5000

45.86.163.207:80

91.132.139.154:443

47.243.192.70:443, 8080

104.238.161.50:443

8.218.183.252:443

149.88.69.123:8001

64.227.133.228:8080

1. **[CMTX-P102024164] Relay server Nodes used by Chinese actors**

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

Confidence- High

Risk- High

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

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

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

Indicators of Compromise (IOCs):

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

IP ADDRESSES

|  |
| --- |
| 103.123.27.189 |
| 103.141.52.28 |
| 103.162.157.33 |
| 103.175.171.102 |
| 103.188.236.137 |
| 103.211.36.163 |
| 103.215.152.172 |
| 103.217.78.136 |
| 103.220.208.250 |
| 103.228.78.86 |
| 103.244.121.91 |
| 103.251.16.113 |
| 103.54.76.232 |
| 103.83.220.161 |
| 111.93.109.66 |
| 114.143.237.50 |
| 115.242.202.110 |
| 115.244.187.238 |
| 117.232.88.97 |
| 117.242.156.74 |
| 117.247.229.182 |
| 117.251.17.23 |
| 122.168.120.151 |
| 122.176.140.129 |
| 122.180.245.231 |
| 125.20.115.70 |
| 136.232.82.210 |
| 14.102.44.190 |
| 14.99.63.150 |
| 150.129.105.52 |
| 150.129.127.2 |
| 182.69.183.79 |
| 182.74.138.66 |
| 183.82.117.176 |
| 183.82.122.123 |
| 183.82.144.24 |
| 202.173.127.22 |
| 203.109.81.139 |
| 206.84.233.217 |
| 210.18.155.213 |
| 45.115.168.25 |
| 45.117.30.5 |
| 49.205.217.110 |
| 59.182.50.247 |
| 59.92.70.111 |
| 1.6.225.34 |
| 103.106.195.155 |
| 103.107.60.17 |
| 103.133.122.127 |
| 103.133.28.5 |
| 103.154.57.41 |
| 103.162.198.36 |
| 103.171.203.56 |
| 103.19.133.150 |
| 103.226.187.227 |
| 103.24.173.118 |
| 103.47.104.8 |
| 103.48.109.118 |
| 106.201.243.186 |
| 106.51.38.180 |
| 106.51.87.172 |
| 110.227.250.114 |
| 114.143.149.210 |
| 115.242.226.22 |
| 115.247.15.194 |
| 115.247.158.194 |
| 115.96.25.136 |
| 117.195.115.153 |
| 117.195.201.34 |
| 117.211.168.157 |
| 117.221.65.66 |
| 117.242.146.18 |
| 117.247.187.152 |
| 117.250.68.203 |
| 122.160.5.148 |
| 122.166.168.55 |
| 122.186.81.242 |
| 124.123.92.80 |
| 125.16.179.90 |
| 14.102.163.70 |
| 14.139.200.220 |
| 14.141.245.162 |
| 14.141.81.74 |
| 143.244.132.86 |
| 150.129.105.108 |
| 150.129.47.195 |
| 160.202.10.234 |
| 175.101.3.99 |
| 182.71.120.18 |
| 183.82.105.29 |
| 183.82.2.199 |
| 202.131.138.172 |
| 202.179.92.77 |
| 202.88.253.6 |
| 203.192.233.106 |
| 36.255.9.150 |
| 45.112.202.22 |
| 45.116.3.210 |
| 45.64.212.115 |
| 49.205.176.86 |
| 49.206.199.2 |
| 49.43.219.48 |
| 59.144.175.16 |
| 59.96.56.48 |
| 60.254.0.150 |
| 61.0.203.235 |
| 61.246.171.138 |

1. **[CMTX-P-102024045]: Critical Alert: MYTHIC Malware Campaign**

Threat Overview

1. Threat Campaign: Mythic 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.

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

Indicators of Compromise (IOCs):

• IP Addresses:

|  |
| --- |
| 170.64.225.181 |
| 167.71.217.124 |
| 157.245.195.246 |
| 170.64.225.181 |
| 139.59.109.136 |
| 167.99.6.167 |
| 23.163.0.90 |
| 35.88.139.137 |
| 104.131.172.8 |
| 157.245.195.246 |
| 13.60.157.223 |
| 195.100.198.220 |
| 20.174.169.119 |
| 160.238.36.36 |
| 209.38.45.156 |
| 152.67.149.246 |
| 149.104.26.229 |
| 129.211.212.43 |
| 213.252.246.168 |
| 172.201.107.88 |
| 45.141.59.99 |
| 35.204.187.119 |
| 13.58.109.128 |
| 52.25.188.122 |
| 81.0.218.25 |
| 94.232.40.36 |
| 5.230.70.43 |
| 178.156.133.137 |
| 95.164.22.13 |
| 195.189.96.70 |
| 185.245.106.251 |
| 20.115.66.63 |
| 13.52.44.164 |
| 8.210.9.166 |
| 195.208.174.240 |
| 89.31.122.21 |
| 51.15.227.211 |
| 3.15.21.172 |
| 103.117.101.73 |
| 52.128.230.44 |
| 176.31.162.105 |
| 54.226.62.246 |
| 54.74.198.96 |
| 35.177.104.235 |
| 52.128.230.45 |
| 52.128.230.42 |
| 44.201.155.166 |
| 164.90.158.199 |
| 195.231.58.21 |
| 66.70.202.83 |
| 54.247.71.250 |
| 162.120.71.226 |
| 13.66.164.102 |
| 47.245.14.36 |
| 14.225.217.205 |
| 47.76.51.11 |
| 64.23.213.61 |
| 3.227.184.192 |
| 141.164.45.186 |
| 149.210.143.97 |
| 155.138.154.222 |
| 47.76.61.197 |
| 52.128.230.43 |
| 54.158.206.132 |
| 107.172.159.50 |
| 162.212.154.121 |
| 44.224.147.7 |
| 35.246.57.139 |
| 13.245.162.103 |
| 94.232.40.36 |
| 62.109.30.217 |
| 3.82.219.218 |
| 80.87.199.167 |
| 23.163.0.90 |
| 14.225.217.205 |
| 73.213.108.128 |
| 170.64.225.181 |
| 137.220.57.209 |
| 178.156.133.137 |
| 104.131.172.8 |
| 94.232.40.36 |
| 51.15.227.211 |
| 51.15.227.211 |
| 213.252.246.168 |
| 78.24.220.122 |
| 23.163.0.90 |
| 188.120.254.229 |
| 213.252.246.168 |
| 176.31.162.105 |
| 14.225.217.205 |
| 87.120.114.216 |
| 14.225.217.205 |
| 178.156.133.137 |
| 146.190.5.183 |
| 185.43.4.72 |
| 185.43.4.80 |
| 139.59.109.136 |
| 185.43.4.73 |
| 104.131.172.8 |
| 46.166.165.95 |
| 170.64.225.181 |
| 143.198.204.173 |
| 164.90.158.199 |
| 192.236.209.198 |
| 45.61.152.130 |
| 164.90.158.199 |
| 34.101.140.123 |
| 176.31.162.105 |
| 164.90.158.199 |
| 167.71.234.132 |
| 87.120.114.217 |
| 87.120.114.216 |
| 185.43.4.72 |
| 167.71.234.132 |
| 94.232.40.36 |
| 157.245.195.246 |
| 14.225.217.205 |

1. **[CMTX-P-8650920249] Threat Actor Group (TAG)-102- Advanced Cyber Espionage Group**

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

Confidence- High

Risk- High

TLP:RED- For the eyes and ears of individual recipients only,

no further disclosure.

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

TAG-102, known by various aliases such as Bronze Highland, Daggerfly, Evasive Panda, and StormBamboo, is a sophisticated Chinese Advanced Persistent Threat (APT) group. Active since at least 2012, this group is primarily involved in cyber espionage, targeting organizations, governments, and individuals.

TAG-102 employs highly sophisticated tools and techniques for long-term espionage, utilizing both custom malware and publicly available tools. The group has demonstrated the ability to compromise Windows, Linux, macOS, and Android systems.

103.133.136.126

103.133.136.14

103.133.136.226

103.253.43.167

103.253.43.195

103.253.43.207

103.253.43.227

103.96.128.103

103.96.128.107

103.96.128.11

103.96.128.12

103.96.128.127

103.96.128.13

103.96.128.132

103.96.128.135

103.96.128.14

103.96.128.15

103.96.128.178

103.96.128.198

103.96.128.22

103.96.128.26

103.96.128.30

103.96.128.35

103.96.128.44

103.96.128.5

103.96.128.7

103.96.128.8

103.96.128.9

103.96.128.99

103.96.129.11

103.96.129.16

103.96.129.205

103.96.129.223

103.96.129.234

103.96.129.30

103.96.129.32

103.96.129.5

103.96.129.56

103.96.130.10

103.96.130.102

103.96.130.103

103.96.130.104

103.96.130.113

103.96.130.119

103.96.130.246

103.96.130.86

103.96.131.12

103.96.131.146

103.96.131.24

106.126.3.32

110.81.153.67

110.81.153.70

114.64.255.138

114.64.255.171

114.64.255.176

116.255.137.251

118.123.1.155

125.65.40.181

128.199.119.158

139.84.167.197

139.84.168.41

139.84.170.230

139.84.175.17

158.247.214.28

185.132.125.101

188.116.22.44

188.208.141.172

192.243.127.104

195.54.171.4

210.16.188.116

38.180.94.244

38.180.94.57

45.125.67.166

45.125.67.192

45.125.67.201

45.125.67.220

45.125.67.223

45.32.240.55

91.242.241.188

webmaillll.qqmail.website

1. **[CMTX-I-335102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

meagov.org

scigov.xyz

govscicourt.com

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

1. **[CMTX-I-345102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

www.email.gov.in.indianarmy.pl

email.gov.in.indianarmy.ml

\*.indianarmy.pl

\*.indianarmy.ml

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

1. **[CMTX-P-2521020249] SocGholish Malware Alert**

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

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

Threat Overview:

SocGholish uses social engineering to infect systems: it tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

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

77.245.56.14

93.190.41.79

45.130.201.24

164.52.214.211

92.205.49.95

217.160.0.220

31.220.15.143

5.101.115.147

217.160.0.215

92.204.68.47

185.216.114.10

217.160.0.246

195.24.68.25

94.130.138.216

35.215.148.34

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

1. **[CMTX-P-102024174] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses :Port

146.70.247.109:443

217.69.15.243:443

65.20.76.134:443

108.61.217.45:80

1. **[CMTX-P-8211020249] Redline Malware Alert**

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

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

Threat Overview:

Redline malware is a recent malware written in C# with notable growth in 2021. It includes modules of stealing credentials and collecting information from the infected machine and the capability to download remote files.

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

|  |
| --- |
| 185.196.9.26 |
| 185.215.113.67 |
| 88.99.151.68 |
| 45.132.1.33 |
| 185.159.129.54 |
| 193.37.71.131 |
| 147.45.67.15 |
| 45.137.22.171 |
| 80.66.89.228 |
| 136.244.88.135 |
| 5.254.73.99 |
| 188.114.96.3 |
| 188.114.97.3 |
| 45.9.73.169 |
| 45.137.22.252 |
| 93.115.91.27 |
| 185.222.58.236 |
| 108.61.177.169 |
| 65.21.18.51 |
| 185.215.113.22 |
| 185.222.58.250 |
| 163.172.24.191 |
| 185.222.58.245 |
| 193.26.115.118 |
| 89.105.223.196 |
| 212.233.122.234 |
| 185.222.58.233 |
| 185.222.58.80 |
| 147.45.47.192 |
| 185.222.58.248 |
| 5.206.227.2 |
| 45.137.22.123 |
| 176.111.174.140 |
| 213.248.43.53 |
| 212.233.122.248 |
| 154.216.20.204 |
| 45.137.22.91 |
| 185.215.113.25 |
| 213.248.43.54 |
| 185.222.58.247 |
| 185.222.58.48 |
| 95.179.250.45 |
| 91.211.248.215 |
| 95.216.232.170 |
| 31.42.189.18 |
| 45.89.247.82 |
| 185.222.58.74 |
| 91.92.242.38 |

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

1. **[CMTX-P-102024184] 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:

|  |
| --- |
| 45.207.211.215 |
| 158.247.252.115 |
| 154.90.62.14 |
| 103.201.130.43 |
| 185.200.64.79 |
| 35.189.170.190 |
| 154.204.176.79 |
| 172.94.111.241 |
| 101.36.105.222 |
| 18.162.154.219 |
| 140.210.28.101 |
| 45.32.105.184 |

1. **[CMTX-P-9271020249] Trickbot Malware Alert**

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

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

Threat Overview:

Trickbot is a highly modular malware, capable of performing a number of actions on a network such as steal information or drop ransomware.

Impacts:

    Banking Trojan and Botnet: Initially designed to steal banking credentials, Trickbot evolved into a highly modular botnet used for a range of malicious activities, including credential theft, ransomware deployment, and spreading malware.

    Ransomware Delivery: Trickbot is often used as a precursor to ransomware attacks, delivering ransomware payloads like Ryuk or Conti after the initial infection.

    Lateral Movement: It can move laterally within infected networks, compromising multiple machines and exfiltrating sensitive data.

    Credential Harvesting: Trickbot steals credentials from browsers, email clients, and other applications, often leading to further compromise of systems.

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

175.184.232.234

27.109.116.144

41.77.134.250

177.190.76.82

196.41.57.46

103.201.142.30

96.9.77.142

194.87.94.14

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

1. **[CMTX-P-7781020249] Amadey Malware Alert**

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

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

Threat Overview:

Amadey is a simple Trojan bot. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware.

Impacts:

Botnet Activity: Amadey is a botnet malware used for data collection and launching additional payloads, including other malware.

Credential Theft and Surveillance: Capable of collecting system information and stealing credentials from browsers.

Ransomware Deployment: Often used as an entry point to deploy ransomware.

|  |
| --- |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCSTART\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |
| 77.91.78.17 |
| 185.196.10.188 |
| 45.9.74.182 |
| 78.46.242.112 |
| 193.233.20.14 |
| 62.204.41.252 |
| 193.3.19.154 |
| 193.106.191.201 |
| 62.204.41.89 |
| 79.137.203.59 |
| 188.40.187.155 |
| 176.113.115.201 |
| 207.154.243.184 |
| 89.163.249.231 |
| 78.47.9.120 |
| 193.42.33.74 |
| 45.9.74.164 |
| 31.41.244.146 |
| 31.41.154.129 |
| 185.215.113.35 |
| 77.73.134.66 |
| 195.2.70.68 |
| 194.190.152.209 |
| 45.202.35.101 |
| 45.9.74.166 |
| 185.11.61.121 |
| 185.215.113.204 |
| 185.215.113.101 |
| 45.9.74.141 |
| 49.12.117.51 |
| 185.196.8.176 |
| 77.91.124.1 |
| 77.91.124.207 |
| 31.41.244.237 |
| 46.8.231.42 |
| 80.66.75.214 |
| 31.177.76.32 |
| 31.177.80.32 |
| 62.204.41.79 |
| 35.187.168.7 |
| 92.43.25.99 |
| 34.163.37.95 |
| 80.66.89.124 |
| 194.163.35.54 |
| 62.204.41.87 |
| 188.40.141.211 |
| 62.182.156.153 |
| 185.174.136.244 |
| 77.105.160.21 |
| 89.163.210.240 |
| 34.88.137.133 |
| 158.196.149.66 |
| 81.30.189.18 |
| 185.232.14.89 |
| 37.247.10.18 |
| 185.196.8.126 |
| 213.202.223.111 |
| 89.163.152.111 |
| 91.228.238.70 |
| 85.209.135.11 |
| 85.209.11.155 |
| 34.77.123.245 |
| 5.75.139.35 |
| 185.215.113.16 |
| 194.163.38.5 |
| 5.104.108.23 |
| 35.198.88.107 |
| 81.17.29.162 |
| 119.18.58.248 |
| 77.72.17.124 |
| 185.231.220.10 |
| 80.66.75.114 |
| 212.204.112.234 |
| 5.181.86.244 |
| 92.204.58.67 |
| 34.89.169.66 |
| 193.167.100.88 |
| 89.163.220.66 |
| 92.60.224.35 |
| 129.132.80.25 |
| 45.15.156.208 |
| 89.163.155.199 |
| 185.215.113.26 |
| 213.202.223.115 |
| 31.41.244.10 |
| 91.192.226.152 |
| 35.187.35.15 |
| 23.215.121.14 |
| 176.126.172.243 |
| 156.67.212.207 |
| 34.90.10.178 |
| 35.228.19.145 |
| 212.204.112.241 |
| 77.91.124.20 |
| 129.132.18.8 |
| 35.204.250.43 |
| 79.110.62.15 |
| 35.233.77.94 |
| 35.234.76.210 |
| 31.41.244.158 |
| 213.202.229.103 |
| 34.76.205.124 |
| 213.202.223.113 |
| 92.205.111.226 |
| 77.73.133.72 |
| 138.201.203.107 |
| 62.204.41.182 |
| 192.121.16.27 |
| 77.91.124.242 |
| 91.189.114.25 |
| 31.41.244.15 |
| 62.122.170.171 |
| 195.251.3.214 |
| 147.32.80.105 |
| 95.211.227.207 |
| 104.155.66.110 |
| 87.62.82.197 |
| 213.246.57.71 |
| 129.241.56.201 |
| 185.37.231.211 |
| 46.16.234.119 |
| 94.247.170.66 |
| 3.126.57.221 |
| 35.205.156.75 |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCEND\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |

1. **[CMTX-P-8701020249] Agent Tesla Malware Alert**

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

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

Threat Overview:

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

Impacts:

    Keylogger and Credential Stealer: Agent Tesla focuses on capturing keystrokes, clipboard data, screenshots, and harvesting credentials stored in browsers and email clients.

    Data Exfiltration: It can exfiltrate data through various channels like email, FTP, or HTTP.

    Widespread Use: Frequently used in phishing campaigns, targeting users through malicious attachments.

|  |
| --- |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCSTART\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |
| 46.175.148.58 |
| 110.4.45.197 |
| 213.189.52.181 |
| 217.116.201.44 |
| 193.141.65.39 |
| 37.27.98.198 |
| 93.216.70.207 |
| 148.66.136.151 |
| 195.252.110.253 |
| 92.37.142.45 |
| 47.76.82.23 |
| 37.247.119.59 |
| 5.2.84.236 |
| 85.26.241.192 |
| 93.89.225.40 |
| 144.217.198.22 |
| 103.6.196.236 |
| 148.251.209.169 |
| 92.205.7.112 |
| 167.235.180.68 |
| 78.128.81.95 |
| 185.191.171.10 |
| 185.191.171.16 |
| 49.36.188.172 |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCEND\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |

1. **[CMTX-I-845102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

loginmygov.info

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

1. **[CMTX-I-850102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

ww25.indian.airforce.life

serviceonline.gov.in.viewcerts.org

ww38.iwww.joinindiannavy.com

viewcert.life

tpplus.top

\*.indian.airforce.life

\*.in.viewcerts.org

\*.joinindiannavy.com

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

1. **[CMTX-P-8851020249] Supershell Malware**

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

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

Threat Overview:

Supershell is a popular Chinese web based open-source command and control (C2) platform that supports multi-platform architecture client payloads (e.g. Windows, Linux, Android, FreeBSD).It provides a reverse secure shell (SSH) tunnel to obtain a fully interactive shell, remote system management, execute interactive scripts, and perform various remote operations using its fully interactive shell.

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

45.32.63.2

45.15.143.197

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

Recent SuperShell C2 infrastructure has also been observed in FortiManager zero-day (CVE-2024-47575)attack.CVE-2024-47575 is a critical vulnerability in Fortinet's FortiManager that allows a threat actor to execute arbitrary code or commands against vulnerable FortiManager devices.Detailed advisory can be accessed from the below URL:

https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

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

45.32.41.202

158.247.199.37

104.238.141.143

195.85.114.78

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

1. **[CMTX-P102024055] Adversary-in-the-middle (AiTM) Phishing Attack Bypass MFA**

Threat Overview

Adversary-in-the-middle (AiTM ) phishing is a type of an identity-based attack where a person/organization’s digital identity (passwords, email addresses etc), personally identifiable information (PII) are targeted to gain unauthorized access to sensitive data and systems.

These attacks use social engineering in order to encourage the victim to open the email or text message and click on the malicious link, which takes them to a malicious website that frequently mimics a genuine login portal (spoofed login page for Microsoft O365) or a blurred document that could only be viewed by inputting O365 credentials

AiTM phishing allows a threat actor to bypass multi-factor authentication (MFA) by inserting a proxy between the victim and a legitimate login portal to steal credentials and session tokens using token hijacking technique.

Some AiTM phishing kits and attack tools include Evilginx 3.0, Modlishka, Muraena, Mamba 2FA, Tycoon 2FA, and NakedPages which function to steal MFA session tokens by acting as a reverse proxy.

Threat Type: Adversary-in-the-middle (AiTM) Phishing Attack

Severity: High

Indicators of Compromise (IOCs):

IPs

24.123.192.166

72.43.174.83

47.45.234.127

74.143.2.14

20.190.151.0/24

20.190.181.0/24

185.220.101.102

188.213.202.0/24

193.37.33.0/24

172.183.249.139

45.143.82.229

69.5.53.144

179.41.183.40

141.136.92.76

180.247.187.17

203.109.207.210

179.68.204.121

Domains/URLs

https[:]//susgdoxu3o8p.larksuite.com/wiki/I4H9wTK4piqxTvk7mfIuLi8usjg?from=from\_copylink

https[:]//pub-d75bb1be9d414347a8fca3ada45e0c35.r2.dev/link.html

https[:]//rccgnet.org/protect.php

loancalculatorforrealtors.com

savio.com

HASHES

5259e3c268399650190597840f2b26301b1ce7cf06aa331ff4be5e732eebb1c4

618c564c8ffd0f3a87cb749da711e0b16184fd68edbed215fc540b0c71076766

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

1. **[CMTX-P102024065] FORTINET VULNERABILITIES**

ALERT BRIEF:

The "A Missing Authentication for Critical Function vulnerability" CVE-2024-47575 (CVSS score: 9.8) affects FortiManager, a centralized management platform for Fortinet's security appliances. Attackers are actively exploiting this vulnerability through various vectors, including unpatched systems exposed to the internet.

Another vulnerability "A use of externally-controlled format string vulnerability" tracked as CVE-2024-23113 (CVSS score: 9.8), relates to a case of remote code execution that affects FortiOS, FortiPAM, FortiProxy, and FortiWeb.

This vulnerability has been reported to be exploited in the wild, but we have yet to confirm the claims, and exploit code is not publicly available.

Threat Type: VULNERABILITIES

Severity: High

1. **[CMTX-P102024075] CRITICAL VULNERABILITIES IN IVANTI PRODUCTS**

ALERT BRIEF:

Two critical vulnerabilities affecting Ivanti Endpoint Manager and Ivanti Cloud Services Application (CSA) are as follows:-

1) CVE-2024-29824 (CVSS score:9.6) -

An Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability tracked as CVE-2024-29824 exists in the Core server of Ivanti Endpoint Manager (EPM) which is exploited in the wild.

On successful exploitation, it allows an unauthenticated attacker to execute arbitrary code. Its non-weaponized code is publicly available.

Mitigation:

Patch and Update: Patching CVE-2024-29824 must be prioritized right away in order to protect against potential intrusions and system breaches because of its critical nature, active exploitation in real-world settings, and the potential for serious effects on your company's assets.

Apply the latest security patches to mitigate the risk of cyber attack in the organization.

2).CVE-2024-9379 (CVSS score: 6.5) -

SQL injection in the admin web console of Ivanti Cloud Services Application (CSA)  before version 5.0.2 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.

AFFECTED VERSION:

5.0.1 and prior

RESEOLVED VERSION:

5.0.2

Mitigation:

Customers should update to CSA 5.0.2 if they are using CSA 5.0.1 or earlier.

1. **[CMTX-I-420102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

meagov.online

supremecourt.sc

crsorgi.gov.in.phpne.xyz

joinindianarmy.nia.in

www.joinindianarmy.nia.in

\*.gov.in.phpne.xyz

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

1. **[CMTX-P-102024194] 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

116.62.194.46

116.206.178.34

116.206.178.67

167.179.100.144

207.246.106.38

34.92.30.54

1. **[CMTX-P-102024204] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses :Port

149.28.128.65

1. **[CMTX-P-102024085] ACTIVE EXPLOITATAION OF A CRITICAL FLAW (CVE-2024-9680) AFFECTING FIREFOX AND FIREFOX EXTENDED SUPPORT RELEASE (ESR)**

ALERT BRIEF:

According to various reports, a zero day vulnerability ("use-after-free vulnerability") tracked as CVE-2024-9680 is being exploited in the wild and affecting Firefox and Firefox Extended Support Release (ESR).

It puts system integrity and data security at serious risk by enabling attackers to run arbitrary code without user input.  Such remote code execution vulnerabilities can be exploited, either as part of a watering hole attack or by means of a drive-by download campaign that tricks users into visiting fakewebsites.

AFFECTED VERSIONS:

Firefox 131.0.2

Firefox ESR 128.3.1, and

Firefox ESR 115.16.1.

Threat Type: Vulnerability

Severity: High

1. **[CMTX-P102024214] Relay server Nodes used by Chinese actors**

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

Confidence- High

Risk- High

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

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

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

Indicators of Compromise (IOCs):

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

IP ADDRESSES

1.22.54.106

103.107.36.188

103.112.47.166

103.120.190.200

103.138.154.168

103.14.233.146

103.172.83.85

103.172.87.250

103.216.71.93

103.219.41.8

103.6.187.250

103.77.45.4

103.92.162.150

106.222.210.36

106.51.48.117

106.51.87.226

112.196.48.211

112.196.76.181

115.241.97.11

115.242.249.70

115.244.231.202

115.244.251.110

115.97.103.117

115.98.232.203

117.217.122.104

117.217.122.96

117.223.113.167

117.247.229.197

117.254.196.169

122.175.40.128

148.113.3.144

150.129.131.26

182.70.125.175

182.73.157.238

183.82.32.166

183.82.97.212

183.87.217.123

202.134.190.5

202.140.130.230

202.21.46.196

202.88.244.141

223.30.117.234

27.107.116.106

45.113.105.122

49.205.172.233

49.45.130.115

59.144.173.18

59.184.103.220

59.184.99.53

59.95.252.22

60.243.50.97

61.2.142.121

1. **[CMTX-P102024095] ACTIVE EXPLOITATION OF A CRITICAL VULNERABILITY (CVE-2024-28987) AFFECTING SOLARWINDS HELP DESK SOFTWARE**

Threat Type: Vulnerability

ALERT BRIEF:

The SolarWinds Web Help Desk software has been identified with a critical vulnerability tracked as CVE-2024-28987, which carries a CVSS score of 9.1. This flaw is characterized by hard-coded credentials that can be exploited by unauthorized users to gain access and modify sensitive data within the system. The vulnerability allows unauthenticated attackers to remotely read and alter help desk ticket details, which may include sensitive information such as passwords and service account credentials

1. **[CMTX-I-650102024] Malicious Domains used by Threat Actors**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

www.ijoinindianarmy.niin.in

ijoinindianarmy.niin.in

cbigov.online

supremecourt.site

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

1. **[CMTX-I-514102024] Recent IOCs of Chinese Malware Campaign**

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

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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.

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

65.20.73.88

Persistence (Registry entry): HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AutoLaunch

Malware dropped at location: %ProgramData%\AdobeAutoLaunch\

(the legitimate application name may change as the malicious file is being sideloaded

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

1. **[CMTX-P-092024165] PlugX Malware Campaign – Immediate Action Required**

Alert brief:

Interlock Ransomware is a notable cyber threat characterized by its double-extortion tactics. This report outlines key findings related to their attack methods, motivations, and recommended mitigations to bolster defences.

Ransomware Family: Interlock

Threat Actors: A sophisticated group engaged in double-extortion tactics. Their operations indicate experience and a focused approach to targeting businesses across various sectors, including healthcare, technology, and government.  This group has demonstrated a focus on virtual environments, employing tactics to compromise systems and disrupt operations. Notably, INTERLOCK establishes command-and-control (C2) through a scheduled task using an anonymized network, which enhances its stealth and sophistication.

Recommendation Steps:

1. Enhance Security Awareness Training:

o Conduct regular training sessions for employees to recognize phishing attempts and avoid downloading suspicious software or clicking on untrusted links.

2. Implement Strong Access Controls:

o Use least privilege access for user accounts, especially for service accounts. Ensure that users only have access to the data and systems necessary for their roles.

3. Regularly Update and Patch Systems:

o Maintain an effective patch management program to ensure all systems and software are updated to protect against known vulnerabilities.

4. Deploy Advanced Threat Detection Solutions:

o Utilize robust EDR solutions that can detect unusual behavior, such as unauthorized access to Azure services or abnormal file transfers.

5. Monitor Network Traffic:

o Implement network monitoring tools to detect and alert on anomalous traffic patterns, particularly toward cloud storage services.

6. Use Multi-Factor Authentication (MFA):

o Enforce MFA for all accounts, especially those with administrative privileges, to reduce the risk of unauthorized access.

7. Implement Data Loss Prevention (DLP) Solutions:

o Use DLP tools to monitor and protect sensitive data, ensuring that unauthorized data transfers are detected and blocked.

8. Regularly Back Up Data:

o Perform regular backups of critical data and ensure that these backups are stored offline or in a secure cloud environment. Test backup restoration processes frequently.

9. Establish Incident Response Plans:

o Develop and regularly update an incident response plan that includes procedures for responding to ransomware attacks, including communication strategies and recovery steps.

10. Conduct Security Assessments:

o Perform regular security assessments and penetration testing to identify and remediate vulnerabilities in your systems and network architecture.

11. Collaborate with Threat Intelligence Sources:

o Stay informed about the latest threats by collaborating with threat intelligence organizations and sharing information with industry peers.