**Cyber Security Advisories**

**Date: 15 November 2024**

1. **CMTX-P-102024224 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

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

Indicators of Compromise (IOCs):

IP Addresses :Port

149.28.159.61

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

1. **CMTX-P-102024234 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Distribution Methods

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

Indicators of Compromise (IOCs):

IP Addresses: Port

124.71.46.137

38.54.15.240

139.84.227.139

166.88.194.63

1. **CMTX-I-080112024 : Mythic Malware- APT36 campaig**

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

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

Prevention Measures:

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

Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.).

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

For Linux- ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command)

Principle of least privilege

Firewall and network security along with regular OS updates

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

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

35.88.139.137

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

1. **CMTX-I-0230102024 : IOC of suspicious domains used for sending spear phishing mails**

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. 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. The following domain is observed as suspicious for targeting Govt /Defense users by sending spear phishing mails.

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

eoffice.cc

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

1. **CMTX-P102024115 : Active Exploitation of Critical Zimbra Postjournal Flaw (CVE-2024-45519)**

ALERT BRIEF:

Recent reports have highlighted ongoing exploitation attempts targeting a critical security flaw in Synacor's Zimbra Collaboration software, specifically in the postjournal service (CVE--45519).

This vulnerability allows unauthenticated attackers to execute arbitrary commands on affected installations, primarily through crafted email addresses that Zimbra's server processes incorrectly. The flaw was disclosed in September , with active exploitation observed shortly after the release of technical details by Project Discovery.

AFFECTED VERSION:

Zimbra 8.8.15 Patch 46

Zimbra 9.0.0 Patch 41

Zimbra 10.0.9Zimbra 10.1.1

Recommendations and Mitigations:

To protect against the identified vulnerabilities, the following actions are recommended:

1. Apply Security Patches: Ensure that the latest Zimbra patches (versions 8.8.15 Patch 46, 9.0.0 Patch 41, 10.0.9, and.1) are applied promptly to mitigate the risk of exploitation.

2. Disable Postjournal Feature: For systems where the postjournal feature is not essential, consider disabling it until the patch can be applied.

3. Remove Vulnerable Components: If immediate patching is not feasible, temporarily remove the postjournal binary as a stopgap measure.

4. Monitor Logs: Implement robust logging and monitoring of server activities to detect any unusual command executions or access attempts.

5. User Education: Train users to recognize suspicious emails and phishing attempts that may exploit this vulnerability.

6. Incident Response Plan: Develop and maintain an incident response plan to quickly address security breaches if they occur.

7. Regular Security Audits: Conduct regular audits and vulnerability assessments to identify and remediate potential weaknesses.

8. Update Security Policies: Review and update security policies to reflect best practices in response to new threats.

9. Engage with Security Communities: Stay informed on the latest threats and mitigation strategies by engaging with cybersecurity communities and forums.

10.Compliance Checks: Ensure that all security measures align with industry regulations and compliance requirements to avoid legal repercussions.

1. **CMTX-P-112024014 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

Indicators of Compromise (IOCs)

IP Addresses

158[.]247[.]252[.]152

47[.]242[.]16[.]105

64[.]176[.]69[.]95

47[.]242[.]0[.]122

8[.]210[.]6[.]230

136[.]244[.]116[.]245

1. **CMTX-P-112024024 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Distribution Methods

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

Indicators of Compromise (IOCs)

IP Addresses

109[.]176[.]19[.]62

23[.]27[.]199[.]250

198[.]13[.]34[.]16

172[.]111[.]150[.]36

1. **CMTX-I-020112024 : Malicious Domains used by Threat Actors**

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

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

their organization and its clients.

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

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

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

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

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

Prevention Measures:

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

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

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

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

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

delhipolice[.]gov[.]inh[.]no

meigov[.]info

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

1. **CMTX-P-112024164 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Distribution Methods

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

Indicators of Compromise (IOCs)

IP Addresses

5[.]188[.]34[.]139

162[.]62[.]223[.]244

144[.]76[.]60[.]136

164[.]138[.]254[.]46

166[.]88[.]194[.]63

185[.]243[.]114[.]179

38[.]54[.]15[.]240

1. **CMTX-P-112024174 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

Indicators of Compromise (IOCs)

IP Addresses

8[.]210[.]30[.]189

172[.]235[.]27[.]29

149[.]28[.]159[.]61

49[.]0[.]253[.]48

1. **CMTX-I-080112024 : CrimsonRAT- APT36 campaign**

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

Common Features of APT36 Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

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

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

64[.]188[.]25[.]79

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

1. **CMTX-P112024105 : ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2024-37383) AFFECTING ROUNDCUBE WEBMAIL**

ALERT BRIEF:

A Cross-Site Scripting (XSS) vulnerability tracked as CVE-2024-37383 affects Roundcube Webmail versions prior to 1.5.7 and 1.6.x before 1.6.71.

The vulnerability results from incorrect input neutralization during the creation of web pages, particularly with regard to SVG animation attributes.

By sending a specifically constructed email with an SVG picture that has malicious properties, an attacker can take advantage of this vulnerability.

When the recipient opens the email in a vulnerable Roundcube instance, the malicious script is executed, potentially leading to unauthorized actions or theft of sensitive information

IMPACTS:

Unauthorized Access: Attackers can inject malicious JavaScript code into web pages viewed by users, leading to unauthorized actions.

Credential Theft: Phishing attacks can be launched to steal user credentials by injecting fake login forms into Roundcube's interface.

Data Exfiltration: Sensitive information, such as login credentials, can be stolen and sent to malicious servers.

AFFECTED VERSIONS:

Roundcube Webmail versions before 1.5.7

Roundcube Webmail versions 1.6.x before 1.6.7

1. **CMTX-P-112024044 : 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

Indicators of Compromise (IOCs)

IP Addresses

41[.]32[.]126[.]34

78[.]94[.]158[.]164

121[.]43[.]186[.]132

185[.]243[.]114[.]179

1. **CMTX-P-112024034 : 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

176[.]126[.]83[.]225

91[.]149[.]241[.]103

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

1. **CMTX-P112024054 : Relay server Nodes used by Chinese actors**

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[.]10[.]227[.]132

103[.]108[.]6[.]156

103[.]109[.]148[.]84

103[.]132[.]241[.]11

103[.]166[.]188[.]100

103[.]185[.]236[.]167

103[.]203[.]147[.]130

103[.]206[.]210[.]42

103[.]208[.]224[.]58

103[.]217[.]78[.]94

103[.]255[.]72[.]196

103[.]42[.]159[.]105

103[.]97[.]203[.]242

106[.]222[.]204[.]236

112[.]196[.]46[.]154

116[.]74[.]253[.]69

117[.]211[.]9[.]34

117[.]221[.]65[.]28

117[.]239[.]132[.]58

117[.]247[.]187[.]157

117[.]253[.]223[.]120

122[.]160[.]50[.]212

122[.]170[.]107[.]183

122[.]176[.]106[.]84

122[.]176[.]163[.]19

122[.]180[.]244[.]44

122[.]185[.]40[.]170

122[.]187[.]212[.]22

125[.]16[.]158[.]226

125[.]18[.]1[.]42

125[.]18[.]221[.]254

125[.]19[.]104[.]18

139[.]59[.]43[.]67

139[.]84[.]135[.]254

14[.]139[.]236[.]194

14[.]141[.]80[.]66

14[.]98[.]32[.]114

150[.]129[.]144[.]136

150[.]242[.]254[.]13

152[.]58[.]64[.]14

182[.]59[.]2[.]227

182[.]73[.]214[.]226

182[.]74[.]138[.]66

182[.]77[.]57[.]249

182[.]78[.]70[.]238

183[.]82[.]113[.]80

183[.]82[.]3[.]192

202[.]88[.]209[.]181

203[.]189[.]254[.]50

203[.]192[.]243[.]32

210[.]18[.]182[.]186

223[.]190[.]81[.]5

43[.]241[.]25[.]66

43[.]242[.]247[.]110

45[.]115[.]168[.]60

45[.]127[.]197[.]37

45[.]249[.]80[.]180

61[.]95[.]223[.]193

92[.]119[.]157[.]22

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

1. **CMTX-I-404112024 : Recent IOCs of Chinese Malware Campaign**

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

With reference to previous alert CMTX-I-808102024 dated 15th October, CMTX-I-636102024 dated 18th October and CMTX-I-404112024 dated 29th October additional IOC associated with this campaign are as follows:

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

139[.]84[.]142[.]11

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

1. **CMTX-I-445112024 : Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

indianrailwaygov[.]in[.]net

inscicourt[.]com

indianrailwaygov[.]info

gov[.]in[.]web[.]index[.]vlewcert[.]info

ebanking[.]gov[.]indiapost[.]in

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

1. **CMTX-P112024104 : Critical Vulnerability Affecting Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) devices CVE-2024-20481**

ALERT BRIEF:

A vulnerability in the Remote Access VPN (RAVPN) service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to trigger a denial of service (DoS) on the RAVPN service. The attacker could exploit this vulnerability by sending a large volume of VPN authentication requests to the affected device, leading to a DoS condition for the RAVPN service.

Depending on the severity of the attack, a device reload may be required to restore the RAVPN service. Other services unrelated to VPN functionality remain unaffected.

Attack vector

Password Spraying attack

Detection:-

CISCO Devices customer can use the tool provided by CISCO to determined whether there is any Cisco security advisories that impact a specific software release.

<https://sec.cloudapps.cisco.com/security/center/softwarechecker.x>

Determine the SSL VPN Configuration on the device. if the SSL VPN is not enabled on any interface then device is not effected with this vulnerability.

Response:-

Once a vulnerable device is identified in your environment, it is strongly recommended to apply the available patch as soon as possible. If patching is not feasible, follow the steps outlined in the recommendation section to enable early detection of any potential compromise activity.

Recommendations:-

Enable remote syslog logging to enhance the correlation and auditing of network and security incidents across various network devices.

Configure threat detection for remote access VPN services to protect against Denial of Service (DoS) attacks by automatically blocking IP addresses that exceed predefined thresholds. Additionally, manually block connection attempts from unauthorized sources.

Apply hardening measures by disabling AAA authentication, disabling Secure Firewall Posture (Host scan), and disabling Group-aliases while enabling Group-URLs in the remaining connection profiles.

1. **CMTX-I-443112024 : Mythic Malware- APT36 campaign**

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

Common Features of Mythic Malware:

>> Persistence

>> Remote access and data theft

>> Modular architecture and customizable

>> Stealth techniques to avoid detection by security software

Prevention Measures:

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

>> Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.).

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

>> For Linux- ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command)

>> Principle of least privilege

>> Firewall and network security along with regular OS updates

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

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

188[.]245[.]172[.]199

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

1. **CMTX-I-514112024 : Eliza RAT Malware- APT36**

Pakistan-based threat actors have been actively targeting Indian government and military officials with a malware variant known as Eliza RAT. This malware has been used to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments. Below are some important details:

In addition to IOCs covered in CMTX-I-023052024 and CMTX-I-50082024, additional IOCs of this campaign are as follows:

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

64[.]227[.]134[.]248

83[.]171[.]248[.]67

143[.]110[.]179[.]176

38[.]54[.]84[.]83

84[.]247[.]135[.]235

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

1. **CMTX-I-689112024 : Malicious Domains used for Phishing**

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

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

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

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

The domain listed below is being used for phishing and mimics the legitimate domain www[.]assamrifles[.]gov[.]in

- -----------< Phishing Domain>---------

www[.]assamriflesgov[.]info

- -----------</Phishing Domain>---------

1. **CMTX-P-112024184 : 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.

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P-112024184]

Indicators of Compromise (IOCs)

IP Addresses

64[.]176[.]59[.]232

95[.]179[.]220[.]191

45[.]77[.]170[.]188

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

1. **CMTX-P112024205 : EXPLOITATION OF A CRITICAL FLAW (CVE-2024-20481) AFFECTING CCISCO FIREPOWER THREAT DEFENSE (FTD) SOFTWARE AND CISCO ADAPTIVE SECURITY APPLIANCE (ASA) SOFTWARE**

ALERT BRIEF:

A zero day "Missing Release of Resource after Effective Lifetime" vulnerability tracked as CVE-2024-20481 affects Cisco Firepower Threat Defense (FTD) Software and Cisco Adaptive Security Appliance (ASA) Software.

The Remote Access VPN (RAVPN) service's resource exhaustion is the cause of the vulnerability. This vulnerability can be exploited by an unauthenticated remote attacker by flooding an affected device with VPN authentication requests.

A successful exploit can use up all available resources, which would cause the RAVPN service on the compromised device to be denial of service (DoS).

Reloading the device might be necessary to restore the RAVPN service, depending on the severity of the attack.

Following are the products that are NOT affected by this vulnerability:

1. IOS Software

2. IOS XE Software

3. Meraki products

4. NX-OS Software

5. Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Softwar

Threat Type: Vulnerability

(CVE-2024-20481)

CVSS SCORE-5.8

IMPACT:

1. Denial of Service (DoS): The RAVPN service may be interrupted, and in order to restore functioning, a device reload may be necessary.

2. Resource Exhaustion: If the attack uses up all of the system's resources, performance may suffer or the service may stop entirely.

1. **CMTX-I-863112024 : SideCopy- C&C of Malware Campaign**

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

Common Features of SideCopy Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Prevention Measures:

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

Monitoring and logging to detect unusual activities indicating a compromise

Multi-Factor Authentication (MFA) for emails

Encrypt sensitive data to protect it in case of exfiltration

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

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

84[.]247[.]176[.]126

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

1. **CMTX-I-9907112024 : Malicious Domains used by Threat Actors**

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

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

www[.]attendance[.]in

gov[.]information[.]in

www[.]joinindianarmy[.]in

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

1. **CMTX-P112024405 : IMMEDIATE PATCHING REQUIRED FOR ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2024-5910) IN PALO ALTO NETWORK EXPEDITION**

ALERT BRIEF:

It has been reported that a critical vulnerability tracked as CVE-2024-5910 is being actively exploited in the wild and affecting Palo Alto Networks’ Expedition.

Attackers with network access to Palo Alto Networks Expedition may be able to take over an Expedition admin account if authentication for a crucial function is missing.

Expedition is a tool that helps with enrichment, tuning, and configuration migration. This problem puts credentials, configuration secrets, and other data that are imported into Expedition at risk.

This flaw might be used by an attacker to change the admin account password. To reset the password to the default values, an attacker would have to send a request to a certain endpoint. To exploit this vulnerability, specialized programming or coding is not necessary.

Threat Type: Vulnerability

CVE-2024-5910

CVSS SCORE-9.3

Severity: High

Affected Version:

Expedition 1.2 < 1.2.92

IMPACT:

1. Unauthorized Access: The Palo Alto Networks Expedition platform may allow attackers to access vital features without authorization.

2. Admin Account Takeover: The flaw might enable attackers to gain control of the system by taking over admin accounts.

3. Sensitive Data Exposure: Credentials, configuration secrets, and other private information uploaded into Expedition may be vulnerable to theft.

4. Service Disruption: If this vulnerability is exploited, it may result in service interruptions that compromise the system's availability and integrity.

5. Expanded Attack Surface: The compromised system could be used as a launchpad for further attacks within the network, increasing the overall attack surface.

MITIGATIONS AND RECOMMENDATIONS:

1. Apply Security Patches: Ensure that your Palo Alto Networks Expedition platform is patched and updated to version 1.2.92 or later, as this patch addresses the vulnerability.

2. Restrict Network Access: Limit access to the Expedition platform to authorized users, hosts, or networks. Implement proper network segmentation and access controls

3. Monitor System Logs: Keep a close eye on system logs to detect any unauthorized access attempts or other suspicious activities. Early detection can help minimize the impact of a security breach.

4. Implement Intrusion Detection Systems (IDS): Use IDS to monitor and alert on any unusual activities targeting the Expedition platform

5. Regular Security Audits: Conduct regular security audits and assessments to identify and address vulnerabilities in your network infrastructure

6. Educate Employees: Train employees on recognizing phishing attempts and following best security practices to reduce the risk of initial access

7. Backup Data: Regularly back up critical data and ensure that backups are stored securely and can be restored quickly in the event of an attack

1. **CMTX-P-112024314 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

Indicators of Compromise (IOCs):

IP Addresses :Port: Country Code

107[.]148[.]37[.]16

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

1. **CMTX-P-112024414 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Distribution Methods

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

Indicators of Compromise (IOCs)

IP Addresses

67[.]217[.]228[.]253

223[.]26[.]52[.]163

1. **CMTX-I-556112024 : ActionRAT Malware- APT36 campaign**

Pakistan-based threat actors have been actively targeting Indian government and military officials with a malware variant known as ActionRAT. This malware has been used to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments. Below are some important details:

Key Characteristics of APT36 Threat Actor

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

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

>> Remote Access

>> Credential Harvesting

>> Data Exfiltration

>> Persistence Mechanisms

Prevention Measures:

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

>> Monitor network traffic for anomalies, especially data exfiltration activities to external C2 servers.

>> Multi-Factor Authentication (MFA) for emails

>> Encrypt sensitive data to protect it in case of exfiltration

Indicators of Compromise (IOCs) associated with this malware is as follows:

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

192[.]99[.]241[.]4

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

1. **CMTX-P112024984 : Relay server Nodes used by Chinese actors--ALERT10**

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[.]101[.]100[.]218

103[.]123[.]227[.]38

103[.]162[.]71[.]6

103[.]171[.]40[.]150

103[.]172[.]86[.]6

103[.]176[.]134[.]194

103[.]201[.]147[.]62

103[.]217[.]79[.]92

103[.]241[.]46[.]157

103[.]255[.]180[.]238

103[.]8[.]167[.]195

103[.]82[.]146[.]149

103[.]83[.]254[.]2

103[.]95[.]48[.]161

106[.]201[.]228[.]169

106[.]51[.]226[.]157

106[.]51[.]61[.]98

106[.]51[.]66[.]32

111[.]93[.]186[.]42

112[.]196[.]48[.]210

116[.]193[.]137[.]181

120[.]138[.]7[.]206

122[.]160[.]165[.]64

122[.]160[.]79[.]230

122[.]169[.]103[.]42

122[.]176[.]106[.]86

122[.]185[.]218[.]26

122[.]186[.]73[.]146

123[.]201[.]117[.]6

124[.]123[.]100[.]84

125[.]16[.]19[.]194

137[.]59[.]79[.]5

139[.]59[.]80[.]77

14[.]194[.]176[.]226

150[.]129[.]170[.]125

182[.]69[.]176[.]253

182[.]78[.]194[.]130

182[.]79[.]110[.]182

183[.]82[.]109[.]25

202[.]131[.]96[.]169

202[.]47[.]118[.]229

27[.]107[.]148[.]186

36[.]255[.]232[.]78

36[.]255[.]233[.]5

43[.]227[.]22[.]154

43[.]248[.]32[.]245

45[.]248[.]158[.]42

49[.]205[.]177[.]67

49[.]249[.]110[.]182

59[.]88[.]205[.]22

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

1. **CMTX-P-112024214 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-112024214

Indicators of Compromise (IOCs):

IP Addresses :Port

103[.]152[.]254[.]63:443

1. **CMTX-P-112024224 : 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

23[.]224[.]37[.]22

106[.]54[.]54[.]119

1. **CMTX-I-333112024 : APT36 campaign**

APT36 a.k.a. Transparent Tribe is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defence, and military targets. Malware deployed by attackers can remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

Common Features of APT36 Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Prevention Measures:

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

Monitoring and logging to detect unusual activities indicating a compromise

Multi-Factor Authentication (MFA) for emails

Encrypt sensitive data to protect it in case of exfiltration

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

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

198[.]46[.]177[.]73

212[.]8[.]240[.]221

104[.]144[.]198[.]105

178[.]238[.]229[.]192

181[.]215[.]47[.]169

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

1. **CMTX-I-214112024 : Malicious Domain used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

majhinaukri[.]co

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

1. **CMTX-P-112024018 : RustDoor Malware**

Threat Overview

1. Threat Campaign: RustDoor Malware

RustDoor, also referred to as Thiefbucket, is a Remote Access Trojan (RAT)(written in Rust Language) targeting macOS systems, with a particular focus on cryptocurrency firms. The malware is typically distributed by masquerading as legitimate software updates—such as updates for Microsoft Visual Studio—or as job offers packaged in ZIP archives. These archives contain malicious shell scripts that, when executed, retrieve the RustDoor implant from attacker-controlled domains. To avoid detection, the scripts may also display decoy files to mislead users.

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.

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs):

Hash:

51a88646f9770e09b3505bd5cbadc587abb952ba

5ec7497107478f08ca5018bf659f9340880c059c

a246db8fe1a4f385ed5e2eed5087a60fd2be6b5a

254aad39a432ff0df2ce35cc4ff3578afe1dc1df

f669fba857401406db6b35958d5f57d9d8030f56

f11ca6e92a3f2af3590021d1475a740e6246347e

c401c8aafc28317828f6b648a3abf6e01d05efae

Domains:

taurihostmetrics[.]com

wiresapplication[.]com

juchesoviet48[.]com

IPs:

185.234.216[.]180

139.59.182[.]234

62.204.41[.]73

1. **CMTX-I-500112024 : CrimsonRAT- APT36 campaign**

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

Common Features of APT36 Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Prevention Measures:

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

Monitoring and logging to detect unusual activities indicating a compromise

Multi-Factor Authentication (MFA) for emails

Encrypt sensitive data to protect it in case of exfiltration

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

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

qhev18[.]duckdns[.]org

167[.]160[.]167[.]18

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

1. **CMTX-I-331112024 : AsyncRAT Malware**

AsyncRAT is a backdoor written in .NET that primarily uses unique binary protocol to communicate over TCP. The backdoor can run shell commands and download plugins, which may be kept in the registry or run immediately in memory. Plugins can add features like file transfer, keylogging, video recording, screenshot capture, and cryptocurrency mining. Additionally, ASYNCRAT provides a plugin that targets login credentials kept by web browsers running on Chromium and Firefox. Once executed, AsyncRAT establishes command-and-control (C2) communication with its server and allows threat actors to remotely control compromised systems.

Impacts:

>> Once executed, AsyncRAT establishes command-and-control (C2) communication with its server and allows threat actors to remotely control compromised systems.

>> The backdoor allows attackers to Execute remote commands, Log keystrokes, Exfiltrate data and deploy additional malware.

>> AsyncRAT can be used to spread laterally across the network, potentially infecting other systems and creating a broader security breach.

>> AsyncRAT often includes features to evade detection and maintain persistence on the infected system, making it challenging to remove and recover from the infection.

Prevention Measures:

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

>> Monitoring and logging to detect unusual activities indicating a compromise

>> Multi-Factor Authentication (MFA) for emails

>> Encrypt sensitive data to protect it in case of exfiltration

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

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

103[.]195[.]100[.]105

207[.]231[.]111[.]82

45[.]88[.]186[.]211

78[.]161[.]46[.]79

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

1. **CMTX-I-993112024 : CrimsonRAT- APT36 campaign**

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

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

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

5[.]189[.]183[.]63

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

1. **CMTX-I-025112024 : SideCopy- C&C of Malware Campaign**

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

Common Features of SideCopy Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Prevention Measures:

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

Monitoring and logging to detect unusual activities indicating a compromise

Multi-Factor Authentication (MFA) for emails

Encrypt sensitive data to protect it in case of exfiltration

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

- ------------- < C&C\_Domain>----------

drivebrox[.]xyz

- ------------- </C&C\_Domain>----------

1. **CMTX-P-112024364 : 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

109[.]61[.]43[.]46

185[.]92[.]221[.]230

199[.]247[.]18[.]127

45[.]133[.]239[.]183

70[.]34[.]255[.]119

23[.]224[.]37[.]18

1. **CMTX-P-112024784 : Cumulative Suspicious Domains**

Alert Brief

A set of malicious domains believed to be used in advanced persistent threat (APT) campaigns targeting critical infrastructure, sensitive data, or high-value assets is listed below:

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

update[.]networkdcm[.]com

server[.]imtokem[.]pro

tigmarket[.]casacam[.]net

linux[.]shopingchina[.]net

tgsoft[.]shop

test[.]securityhealthservice[.]com

ftp[.]gulliverwear[.]com

securityhealthservice[.]com

question[.]onedumb[.]com

tlahainasunset[.]com

cg-fiber[.]com

updatecdn[.]xyz

kingcloud[.]online

server[.]nowanubis[.]com

apple-update-login-mail[.]explorate[.]de

tracksonwall[.]com

checkstatus[.]biz

www[.]microsoft-mstsc[.]com

ftp[.]afol[.]dns05[.]com

v1[.]cloud-v2[.]com

ns2[.]citynetwork[.]lv

www[.]sincere-home[.]com

15a[.]ispcdn[.]com

swaggate[.]com

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