**Cyber Security Advisories**

**Date: 16 August 2024**

1. **CMTX-P072024138: HorrorDead Ransomware**

ALERT BRIEF:

A new ransomware variant named as HorrorDead is active in the cyber threat landscape. The HorrorDead ransomware encrypts files with the extension “.encrypted@HorrorDeadBot” and changes the desktop wallpaper to display the ransom note.

Once it executed in victim's machine, It drops a copy of itself named “HorrorDead Ransomare.exe” inside the C:\Users\username\AppData\Roaming\ director. it performs various actions, including deleting backup copies, modifying system settings, stealing data, and disabling security features. Additionally, it has the ability to enumerate files and directories, retrieve the current user’s username, and delay its execution.

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

HASH:

6e7a64e8d70803263570dfd2eb3d05e9423cfe2c39a596e9109c4408325103f3

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

1. **CMTX-P072024148: Specula C2 Framework**

ALERT BRIEF:

Specula is a sophisticated open-source command-and-control (C2) framework that leverages Microsoft Outlook as a covert communication channel for its operations. By modifying the Windows registry, Specula transforms Outlook into a beaconing agent, allowing it to communicate with a C2 server while blending in with regular email traffic.

The framework employs Outlook to regularly transmit beacons to a C2 server, with these beacons resembling normal email activities, which makes them more difficult to identify as malicious. After the C2 server receives these beacons, it can dispatch commands back through the same channel. The compromised system then executes these commands, enabling attackers to carry out various actions, such as data exfiltration or further manipulation of the system.

Capabilities:

- - The framework can identify AppLocker policies, which control application execution on the system.

- - It has the ability to execute commands on the compromised system.

- - The framework can retrieve a list of recently executed commands.

- - It gathers information about the operating system (OS) version, last boot time, and timezone.

- - It can list directory contents, installed applications, and hotfixes.

- - Retrieves files from the Recycle Bin and recent document folders.

- - Reads the "hosts" file.

- - It can access clipboard content.

- - Enumerates printer connections, running processes, services, and service permissions.

- - Obtains the username of the currently logged-in user.

- - Lists potentially sensitive registry values.

- - Gathers information from mapped drives, network cards, and network login profiles.

- - Determines if the machine is part of a workgroup.

- - Enumerates Active Directory users.

- - Checks for vulnerabilities like AS-REP roasting.

- - Identifies users with specific password settings.

- - Enumerates Local Administrator Password Solution (LAPS) passwords.

- - Retrieves domain password policies.

- - Terminates processes.

- - Reads text aloud through the machine's speaker.

- - Manipulates clipboard content.

1. **APT28 Threat Actor: APT28 Threat Actor**

APT28, which is known to be part of the military intelligence of Russia has been involved in long-term cyber espionage campaigns targeting various countries. Recently Threat actor launch spear-phishing campaign in which attacker deployed the malware named as HATVIBE and CHERRYSPY malware (Python Backdoor). Attacker create the scheduled task for persistence. Their tactics include phishing emails, geofencing techniques, and the use of legitimate internet services to host credential-harvesting pages.

Impacts:

o Exfiltration of sensitive data.

2. Threat Type: Malware

3. Severity: High

Affected Systems/Assets

• Rejetto HTTP File Server (HFS)

Mitigation and Recommendations

• Preventive Measures:

o Patch vulnerable application:- As vulnerability persist in to Rejetto HTTP File Server which attacker exploit, it is advised to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable

• Detection Techniques:

o Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known HATVIBE and CHERRYSPY malware. Refer to the provided Annexure for specific hash values and behavioural indicators.

• Response Actions:

1. Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

2. Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Impact Assessment

• Potential Impact:

o Data Theft: HATVIB can lead to unauthorized access and theft of sensitive information.

o Historical Context: Previously, APT28 has targeted public-facing vulnerable devices using spear phishing or zero-day exploits to gain initial access. Recently, they have been involved in exploiting vulnerabilities in Microsoft Outlook to exfiltrate sensitive data.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-0820240104

Indicators of Compromise (IOCs):

• IP Addresses: 5.45.70.178, 185.158.248.198 and 45.136.198.184

• Domains: enrollmentdm.com and trust-certificate.net

• File Hashes:

MD5

o 197e86b76a41f154b64e092f7cc3b306

o d618720afd0ee49601f7933c414ffbb5

o 8e1b29046c7f5bd1ddd4f549e2555592

o 7f865b65a82dcb18385644e0fd894727

o d0c3b49e788600ff3967f784eb5de973

o 34ced721349626ce81c11693b9243c19

o 33c3e4599ad678133905e6c1589c12d2

o 8159abd281783e0ae601afce3b7d23b1

o 81cdcda59c86f8aa636810e4a085d673

o d84043b72bdceb92b2d60c2725bd674f

o 7a2a8c002a5e22c6231885e1ccf82bd1

• CVE : CVE-2024-23692

Tactics, Techniques, and Procedures (TTPs):

• Tactics: Initial Access, Execution

• Techniques: Spear Phishing Attachment, Zero day exploit.

• Procedures: Utilizes emails with malicious attachments or links; deployed python based backdoor.

References and Sources

• Source: CERT-In

1. **MYTHIC Malware Campaign: MYTHIC Malware Campaign**

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

Affected Systems/Assets

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

Distribution Methods

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

Mitigation and Recommendations :

• Preventive Measures:

o Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

o Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

o Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

o User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particulary coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

o Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

o Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-0820240105

Indicators of Compromise (IOCs):

• IP Addresses: ( attached as Mythic\_01082024.txt)

Tactics, Techniques, and Procedures (TTPs):

Privilege Escalation-

Process Injection (T1055)

Defense Evasion-

Indicator Removal on Host (T1070)

Modify Registry (T1112)

Obfuscated Files or Information (T1027)

Process Injection (T1055)

Discovery-

Query Registry (T1012)

System Information Discovery (T1082)

Command and Control-

Application Layer Protocol (T1071)

Ingress Tool Transfer (T1105)

Techniques: References and Sources

• Source: CERT-In

• Links: https://attack.mitre.org/

Attachments:

• Malicious Attachment Sample

1. **CMTX-I-404082024: Malicious Domains used by Threat Actors**

Following are the malicious domains used by threat actors as a spear-phishing website/ host malware.

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

cbigovln.site

mhagovoffice.in

cert-in.org

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

Kindly take the required actions.

1. **CMTX-P-6850820249: VenomRAT Malware Campaign**

1. Threat Campaign: VenomRAT Malware Campaign

Venom RAT (Remote Access Trojan) is a sophisticated and malicious software used by cyber actors to gain unauthorized access to victims' systems. Once installed, it allows attackers to remotely control infected computers, steal sensitive data, and perform a variety of malicious activities without the user's knowledge.

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 : A cross-platform, post-exploit tool.

3. Severity: High

Affected Systems/Assets

- Windows, Linux, and macOS platforms

Distribution Methods

- Phishing Emails with context aware themes and malicious attachment or links mostly from compromised email accounts

- Malicious Websites: Compromised or fake websites hosting the RAT as a drive-by download.

- Software Bundles: Bundled with legitimate software to deceive users into installing it.

Mitigation and Recommendations:

• Preventive Measures:

- Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs.

- Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

- User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-6850820249

Indicators of Compromise (IOCs):

• IP Addresses:

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

5.9.101.133

87.19.18.186

72.5.42.196

64.190.113.27

172.177.171.88

95.164.3.243

37.120.141.144

20.169.80.43

165.154.224.19

91.238.103.153

94.156.69.242

62.234.175.104

15.188.86.159

147.124.223.16

39.101.122.168

91.92.252.73

91.92.244.207

45.157.232.176

5.206.224.154

104.238.23.4

51.161.12.215

157.20.182.226

116.102.238.236

103.74.102.181

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

1. **APT15 Threat Actor: APT15 Threat Actor**

APT15, also known as RedLima, Vixen Panda, KE3CHANG, Royal APT, and Playful Dragon, is a Chinese state-sponsored cyber espionage group active since at least 2004. This group primarily targets government organizations, diplomatic missions, and embassies for intelligence-gathering purposes. APT15 employs a range of tools and backdoors, Operational Relay Box (ORB) networks to obscure their activities and make detection and attribution more challenging.

Recently, APT15 has been involved in reconnaissance efforts using private anonymization networks such as HiddenOrbit (RedRelay) and SuperJump (SPACEHOP). These networks are designed to obscure malicious activities and complicate tracking and attribution. HiddenOrbit, for instance, comprises several hundred virtual private servers (VPS) sourced from various hosting providers. The group's targets have included F5 BIG-IP, Fortinet FortiGate, and Checkpoint VPN gateway devices, as well as Outlook Web Access (OWA) login portals and web servers.

Impacts:

o Reconnaissance activity

o Exfiltration of sensitive data

2. Threat Type: Malware

3. Severity: High

Affected Systems/Assets

· F5 BIG-IP, Fortinet FortiGate, and Checkpoint VPN gateway devices, Outlook Web Access (OWA) login portals, and web servers

Mitigation and Recommendations

Preventive Measures:

· Patch vulnerable application: - As attacker target the vulnerable F5 BIG-IP, Fortinet FortiGate, and Checkpoint VPN gateway devices, Outlook Web Access (OWA) login portals, and web servers for initial foothold, it is advised to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Detection Techniques:

Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known NPS malware, an offensive security tool. Refer to the provided Annexure for specific hash values and behavioural indicators.

Response Actions:

1. Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

2. Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Impact Assessment

Potential Impact:

Data Theft: The attacker utilized a private anonymization network, comprising HiddenOrbit (RedRelay) and SuperJump (SPACEHOP), which includes several hundred virtual private servers (VPS) from various hosting providers and a few compromised devices. This network was used to conduct reconnaissance and exfiltrate data from the victim's machine.

Historical Context: Previously, APT15 has targeted public-facing vulnerable devices using spear phishing or zero-day exploits to gain initial access. Recently, they have been involved in exploiting vulnerabilities in vulnerable F5 BIG-IP, Fortinet FortiGate, and Checkpoint VPN gateway devices, Outlook Web Access (OWA) login portals, and web servers.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-0820240204

Indicators of Compromise (IOCs):

IP Addresses:

158.255.215.119

38.180.54.49

38.180.93.140

38.180.153.163

192.121.47.161

185.123.101.232

185.244.210.47

192.71.166.95

194.68.44.22

Tactics, Techniques, and Procedures (TTPs):

Tactics: Initial Access, Execution and Exfiltration.

Techniques: External Proxy, Exploit Public-Facing Application, Acquire Infrastructure: Virtual Private Server.

Procedures: Utilizes private anonymization network which consists of several hundred virtual private servers (VPS) provisioned from a range of hosting providers and a small number of compromised devices to conduct reconnaissance and exploitation.

1. **CMTX-P082024906: Lynx Ransomware**

Information may be shared without restriction. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.

Threat Overview

1. Threat Campaign: Lynx Ransomware brief

Lynx ransomware encrypt victims' data and uses fork of Inc Ransomware in attacks. They retrieve system information and geolocation from the Windows registry and can modify registry settings to change system configurations. Their capabilities also include resizing volume shadow copies, encrypting files with with the “. LYNX” extension, and placing ransom notes in multiple directories.

Impacts:

- - Delay data processing : It can delay execution using the Sleep API function.

- - System Compromise: The malware can gain unauthorized access to systems for retrieving system time, deleting shadow copies and sending the ransom note to the printer.

- - Stolen Credentials: The ransomware operators may use stolen credentials to breach targeted systems.

2. Threat Type : Ransomware

3. Severity: High

Affected Systems/Assets

- - Microsoft Windows platforms

Mitigation and Recommendations:

• Preventive Measures:

- - Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- - Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- - User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- - Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- - Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

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

1. **CMTX-I-500082024: Android RAT Latest C&C IP**

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

Common Features of Android RATs:

Remote Control

Data Theft (contacts, messages, and call logs)

Surveillance (use of camera and microphone)

Keylogging

File Manipulation

Prevention Measures:

Install Apps from Trusted Sources i.e. Google Play Store.

Update Software Regularly

Review App Permissions

Avoid Public Wi-Fi

Enable Google Play Protect

Monitor Device Activity (such as rapid battery drain or excessive data usage)

Be aware of phishing attacks and avoid clicking on suspicious links or downloading attachments from unknown sources.

Recent C&C server IP of Android RAT malware is as follows:

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

167.86.98.190

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

Network administrators may take required action against the above IP.

1. **CMTX-I-707082024: SideCopy Malware C&C Domain**

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

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

updater-cloud.us

currently resolving to IP: 185.196.9.113

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

1. **CMTX-I-808082024: Linux Malware- C&C Domain and IP**

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

Common Features of Linux ELF Malware:

Data Theft

Botnet Creation

Remote Access

Persistence

Rootkits

Ransomware

Prevention Measures:

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

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

Principle of least privilege

Firewall and network security along with regular OS updates

Recent C&C server domain and IP of malware deployed by this threat actor are as follows:

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

appupdate.firewall-gateway.de

appupdate.my-router.de

45.142.155.110

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

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

1. **CMTX-I-080082024: Spear-Phishing/Typo-Squatting Domains**

Spear-phishing emails are highly targeted phishing attacks that use personalized information to trick recipients into revealing sensitive data or performing actions beneficial to the attacker. These emails could be sent from typo-squatted domains (domains that are deliberately misspelled versions of legitimate domains) to appear highly convincing. Or the email may contain links which point to typo-squatted domains.

Common Features of Spear-Phishing Emails:

Personalized message tailored to the recipient with specific details like their name, job title, or recent activities to increase credibility (e.g. DA increase, holiday list etc.)

Typo-squatting i.e. use of domains that are slight misspellings or variations of legitimate domains (e.g., gov.info instead of gov.in).

Messages often create a sense of urgency or fear to prompt immediate action, such as claiming an account has been compromised.

Contains malicious links or attachments

Impersonation of trusted sources like colleagues, bosses, or well-known companies.

Prevention Measures:

User training and awareness to identify signs of spear-phishing and typo-squatting

Verify suspicious emails by checking the sender's email address carefully for subtle misspellings

Enable Two-Factor Authentication (2FA)

Reporting mechanisms to report suspected phishing attempts k.

Recently identified such suspicious domains are as follows:

- ------------< Suspicious Domains>---------

mea.gov.in.loqin.me

www.procurementmodgovt.info

www.mod.gov.in.army.aboutcase.nl

login-gov.info

notification-services-gov.info

procurementmodgovt.info

loqin.me

aboutcase.nl

- ------------</Suspicious Domains>---------

1. **CMTX-P-0820240205: TAG-100 CHINESE THREAT ACTOR GROUP**

A Chinese Threat Actor Group tracked as TAG 100 primarily targets perimeter appliances of prominent government and private sector organizations globally. Its focus is mainly on aerospace and defence sector. They exploit vulnerabilities in internet-facing devices to gain initial access. For initial access, the group typically uses the open-source, multi-platform Go backdoor Pantegana and SparkRAT.

CYBER IMPACTS:

1. Data Theft and Espionage: Chinese APT groups often target intellectual property, trade secrets, and sensitive business information. This can lead to the theft of proprietary technology, research data, and confidential communications, impacting competitive advantage and business integrity.

2. Network Intrusion and Persistence: These actors employ sophisticated techniques to gain and maintain access to enterprise networks. They use advanced malware, spear-phishing, and other methods to infiltrate systems and remain undetected for long periods, which complicates detection and mitigation efforts.

3.Data Exfiltration and Manipulation: Once inside a network, APT actors can exfiltrate large volumes of data or manipulate data to disrupt business operations. This can result in misinformation, loss of data integrity, and long-term operational damage.

4. Compromise of Critical Infrastructure: Some Chinese APT groups target critical infrastructure components, which can have severe consequences. This might include disrupting industrial control systems, supply chains, or other essential services.

OPERATIONAL IMPACTS:

1. Operational Disruptions: Cyber intrusions can cause significant disruptions to normal business operations. This might include system outages, interruptions in service, or delays in production and delivery, all of which can impact overall business performance.

2. Operational Complexity and Resource Drain: The complexity of defending against APTs often requires significant resources, including specialized personnel and technology. This can strain existing resources and divert attention from other critical business functions.

Threat Type : Nation State Sponsored Threat Actor Group

Severity: High

Affected Systems/Assets

• They’ve targeted various internet-facing products, including Citrix NetScaler Application Delivery Controller (ADC), Fortinet FortiGate, Citrix Netscaler Access Gateway, Zimbra Collaboration Suite, and Cisco Adaptive Security Appliance (ASA) Clientless SSL VPN.

Mitigation and Recommendations :

1. Keep systems and products updated and patched as soon as possible after patches are released. Consider leveraging a centralized patch management system to automate and expedite the process.

2. Enforce multifactor authentication (MFA) for all users, without exception .

3. Immediately remove or isolate suspected compromised devices from the network.

4. Segment networks to limit or block lateral movement .

5. Implement strict password requirements, enforcing password complexity, changing passwords at a defined frequency, and performing regular account reviews to ensure compliance.

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P-0820240205]

PREVIOUS REFERENCE: [CMTX-P072024846] SparkRAT Malware, TLP: Clear, Dated 23/07/2024

Indicators of Compromise (IOCs):

198.98.62.227

205.185.124.24

205.185.126.208

209.141.41.176

209.141.46.57

209.141.46.83

209.141.57.116

1. **CMTX-I-443082024: Linux Malware C&C Domain**

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

Common Features of Linux ELF Malware:

    Data Theft

    Botnet Creation

    Remote Access

    Persistence

    Rootkits

    Ransomware

Prevention Measures:

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

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

    Principle of least privilege

    Firewall and network security along with regular OS updates

Recent C&C server domain of Linux based malware is as follows:

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

appupdate.my-gateway.de

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

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

1. **CMTX-I-021082024 : Mythic Malware C&C IP**

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

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

Prevention Measures:

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

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

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

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

Principle of least privilege

Firewall and network security along with regular OS updates

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

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

139.84.230.205

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

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

1. **CMTX-P-0820240304 : Mirai Malware**

Threat Overview

Mirai botnet, a notorious malware family that primarily targets IoT devices. The botnet has been active since at least 2016 and has been responsible for large-scale Distributed Denial of Service (DDoS) attacks. It infects vulnerable devices by exploiting known vulnerabilities or by using default credentials. The botnet is constantly evolving, with new variants being created and distributed.

Impacts:

o Distributed Denial of Service (DDoS) attacks.

o Act as Loader for other malware

2. Threat Type: Malware

3. Severity: High

Affected Systems/Assets

• TP-Link Archer AX21, Dasan GPON Home Router, Huawei HG532, Ivanti Connect Secure, F5 Big-IP Devices and JAWS Webserver.

Mitigation and Recommendations

• Preventive Measures:

o Ensure that all IoT devices are on a separate network from systems critical for daily operations and devices are up to date.

o Keep operating systems, application software and Public facing devices/applications up-to-date.

o Implement Strong password policy and ensure that no device is running on default credentials.

• Detection Techniques:

o Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known Mirai malware. Refer to the provided Annexure for specific hash values and behavioural indicators.

• Response Actions:

1. Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

2. Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Indicators of Compromise (IOCs):

IP Addresses:

94.156.67.132

147.182.202.39

Domain

secure.microsoftconnect.net

cnc.gay

dkuug.dk

cnc.scriptkid.lol

cnc.makeyoucloud.com

report.makeyoucloud.com

stresser.pw

note.gnu.property

c.cnc.gay

HASH

0153fc5a199a9d9038b4d37c2bc7cf905b1f8750de7833a6654882a354fbb761

02fc26e59dc44b18c5e967212a60f52925d7c7f44975766a297e0b2e59427765

065a82ee9d31f9e9ddd03da625d3db80a7819a26616c2fd2b9a21d657f06926c

06c5fe0963ae516fa79d6bb20c83bf56d91be3cc7d92ac34c1fe70fd27605a0a

0a86285aca9bbe871ce35aac6681ea00f308ab0ad43063c65b74ba8422c713ab

0ab267b78d6c6d1faada747adba0da9f57ce3a7dc1b9a4e968f313dc41d6add1

0b8d87a12105ce82c9ac0412d15f1ff7158dfd951a5c50ddd63fdb449b4dc59e

0c0ce83c1318c65a53793a511deba7e69f734a1039b541a9eb76b4dbe4c71a01

0f2e429c321ebcbe09ac3d8af3e4e7de0f844569b88e045b09909cdaf1c66976

12839233423dc1fc45fd32849d987c86c6bde4863dc220003d07a5df6072a346

13d1090ad5fab5f9740a178d2a697144f908c7cfabbfd087540e94e42c937dd0

1551800e553e511bfeb80b67fcc7776f7992647e1b927c364a5d6f169bf62145

158831408d21253f07cedd1f2497a5621c1984c189016e72be82bdfdd2d548bb

15ffa9bf9057539c49c24143621c052ff28cfe4ff5136483dbc920a6c98fe2c9

183b46b436d8f64e5f0afebfbf919227d57cbaead3e4146b05bb86ed1b0bb55a

1a64a5925b936965dba1d89ec5705004c57cce67f598829ef1afb4160acb0f01

1a9b070768c54719ed95597e9d156595d391fee1d052234bf2b9ba548618aee2

1aaacb0786783211a79bcd3eeed3cb6b62c028dd4c7c780390d1b9148ece2e95

1b045eb70f645de76e3e19b717f9b25394a4a7d3cc175fcc40bb7537352208bc

1ccef0e933fa2a5f5221fd5cf46b0ce363e456150da67c22263ddbc67f922bb2

1fc2be606f48591ead7c6944098d764465389186992ec3617d9ebecfbc93b71d

20b95df69fc0828989f2aabdb8380ecbd12ce947ad6f7b511b78dbfcc5367da9

21f56998d1d755e3c5bf2b2c8d2b30dfa9b0b980b7ba030b0fe36833fb6f1847

22341cc6eaab1f0fbc221555b9cd704f051e543ee171c40206eebe20939bc2a7

2673a80badd8317fcf3e58999a2ca2c41fa11eb4abda57720fc28b48eee28224

2880a14403283b94df8f3580b3c3721592db4ab60f328c48c4108ffe51770ecd

290ccee9ba721dd8eb39af7ec7df1a9ec902e074b1eb1147bec9e5c47d837d41

2c9272b4bcd80d2dfa63ed27ad8765cfc2ae0fb6523657f6f365262197f31ff4

2f44ef9952e69fdd7420689e13f51c2d770aa202109620b8862059b1212b1a33

305a57f9733c3a2eeda30b572409a3e76c29b0a401b52d8368913829b6d92b58

31f5d76bee07c5efccb11ca3d78fc565808c335c8cd692bc342679bb56f32b8f

351d24de7d921d343617c9c47259a01d61df031337ad066ea9aba0127e2fc150

37fdbaaba3ad9e76b511802c2eb463ec46df823355ad35cf4d569c52f68ca802

388847154d57a034ca61aefe8b197693c3aa963c291fdccb3896b919f4c791b5

3988e44c2b02d01d8c07b64b5391d52785427698f8df184af515fd7213b410cd

3aa75a9bbe50392f9dcbf39bf74c3783180554a7e2945a78e3c2f546e9af1528

4082a7e2b44c63b458434e9e1607a1a1bc0e44d3e28315127dbc0ba5e37fbcea

425349fd4a124537ff5140047d825ffc11d9eb04338fc8fadef38024a8389384

434737cbb8fe0de5e52110de31e090dd6e30ce864078a655fc57d0a8861deec6

43b6f5f321f98e13510dbd75d24fefc969e4e3137af340f0694373f7712206b7

44d2d15eb7b0ae236406f0a1ce295a8740216bb64cf5834b1730291a30ecc100

486e061b178529334eab7ed516c4e8c8b7a8a92f7eec502b32c15e254f451004

4e6c64f8b0657fe75c8e7ca44db63d6280a8e51dca95c44137175783961c75e6

4ed99f035d8e454219cfa05fa027990452c39418ded114c091200ff8c55f7dae

51fcbe01154e0640d11f688e6d938474a89101f2f65dd6f83c0bb3f6b259ec86

52be68daf572b5e09a97ac28cd9a6ed967cacd34d482d050bcdbaad4201f1e94

5399d59f7c4132f674c947c582e8936f498b34e62c5bdc3960fe65a160c45ba6

5663bd9ee8de2b3a962461b839cbd042bdda097c30d3db207d62c7a3c04d2c69

59560da4441b5e239b5d330890fd163bebc42f3fc6b4b113d8332935b6da0a87

598e366d0d08ca3d960ead5ea719682cbaaebfba8c8325925cd6ed5f1eadc875

5c423b45204033041e22e25a671839b8f0bd749a685687e1c826797b4afae410

5c7a34d00d8e5044020b1e06c6385198dcab0a3576a9112f6178bb9dbbe0a189

5e0b66179fa049fb8a29c9faa4a9af7607f4a587b92ee0da9530a3cff243454e

5e8cda822836c4e6b4a840200b875ae4a2753fdc5b5ee483d225e90949472509

6109bd8e1384611575d4ba2c190ab4672e026c1a7f9d9cef352016f2103aa3e5

61fcd1e2183abe214147d85dc63aa276a8eb77a00c941ce7131a869fd3a7d70f

65ea764a4133ee23ab5efef8c0073ab3f5e0d636ccf57c8bf79ea5265be98b6b

66581bb5b57b05c3d5c300e7b86e097abbb06f857a0264ad4b2fdd46fafe795c

677eb9b809663f2f8ca2da459b13d7d722b9d86424c317f0e86f56a327d9d584

69a7b7d0382693ecc03d881a3c2a339a8ff7670b0fa51028c96a37ef8f0d4c82

6a9d1cbcb3ae89c77b83e20c7a74575a4902a49219da62a87c4078ac18cfde7b

6af97616cd66a61f437ca1b41b4f3992f5aece23a996f22c62e5724f81e99cbc

6b02a978c686ee7a23eac755cbe39704ffb156327762f338262a521c735b0c74

6c7de89b3aefb9c92b8e75a9a488a2d74ce0251fdde18237cb86c22b32d48bc7

6c9d4980463805ac8f055b6ddb73437d7f49d0f7fdb362b4659dedb041344a67

6d23f59a7d218e34a26aceefb1d8906c7831c1133dd0ade66d1e9ab35c2da7ae

6d9167ac06b45d106f83f677f025c84931a635a6509c93c4760c963e17a47c7d

6e937c7b1f6dfe25ecb7c6b6d5790023713325e214f73c4617608850d94b60b1

70b46d2d568ba750afcb5ed1e3723fa81a621cb52063f45d131a4ecb62ebaa99

71305d2b0c443a9a50492ceb49c1c812df937f58e69def3f1e472ac4dc06c9bb

7143c63137ebcbc37112cedc6a0d7ea7d06d7814d1d9ab3e34b9b732d917f50c

7169ba03c373be2b617eae2d2b926ea7ed45c81c1624f747b92d35cf3b5bdb3b

718cda06003bbd34f423bb54c023d0ff77cc3ae1bdfc5824ff4dc9f047bbc254

7433579f6c91a0d5d67705f0e95c249c1b3cba4c9576ec2c9124a3cdad4bfc94

74f5c9c9c55786beab5475ea8c49c66269db592d1419096c0664be68404b10d3

78c63f69cc8460b0c2fdd27236f4af55ef0cb49c1484219c4ab5e7d8a7023b1b

78cbe2583177766e8ccabf5ac2ecee1a790a200f1ba75033a2d771a0cbbcff93

792a7af74a88edcdad8c1e1c01d710181a2b8fc41a54ae628af0c7e9c9b625b1

79b9aedc762f5de8dc138be914938004e40e4bec4f2f03d2b7ea083b7f96853d

7a65eb84a7652ab08182cc0106d78b0f4df48ff50101462c7d82037aaf02ffb8

7d502f1f46805f496f02323272174c56f7e14a215a4ff71e5e1809638edeea77

7d98172fe60f94de609d1b7f2bdce6bc7dc478f0ca5b0bf6b4d782acc400de2b

7df0638e06ce94629f99f9a7309cfb7b8f4c308c6a80b0c1eb11a33b760f02f9

7e21ce7e069ed261cd985271bc49d9b606996b6781b11bdd8dfb429b5e028c9d

83bdb5eafdc1684794033b843c74679d1c89a76b8b3a15af02e2e6af951fd9e9

841132885078ae42a70fd265fafc4bb4ee7936f41a15203bb4dde4e2c96ba5dc

862cfbaeb973e72448aac770359e8b55a1bc8c80f6a81ac0d936e68521d2f068

86c6b88c9b3480c13afb1260b8761a68d442b6efd69ad08c3742fbe69402799c

86ca2a08d73c856db15aab5d8bde1e6be3f2f183d514c29f690e2dc8ff99d68a

8858fc8bc86a116a9ff782f775ee4156d5368f02d5d676d343da054f58e92811

897a8b0122c3938e00d67fec6b9f0d16376abed81513e512939e5dab08f68fd4

8b4ecd5e62cc3071b6d22dd2e3cd94ca3e5d6430db5d1278eba0213c0dbca534

8ff601d409dad700ddab21e097fd5c00dc883707da684c98e0bf056d8c86aeb2

912f382c585831ad8c4ebaa1413af9d78971cb5ce10807a60ab342b5e4866818

93f3a2c0cf2d94f1d0ba2ea6feb18e49ae17d2cae8522292ee6c9f9ae97685dc

962a4e4cf546bb5294a9f743759867778520e0ba712b10510f8a9ce323874d8a

99a66406ddf4038c2982aef39f0654f7e2d0046b617426ddc506bd72bde22056

9a41114465919c90d0f0847f55cf2231388b24bade7b5d77ed461c7646f245d1

9c9bbcc89b8aa0c5d9f8d2e0fa4aff20e33c8ec8213ff00fac8eb182cea2cfa2

a1093f1d1a55bf4fb1f20dbb4d8834cd40292b83087a1b278e59df71ff4d1900

aa527aa8079a738ecbaed94847cd93eafbaf45cdc6e1820a06286aef8127eeef

aab9fd38dc942e44bb94b5e991302d94ed222bb7bfd024733a15eaad9ce5840a

ad3c19afec823def5b53f480eb919b75129dc820dbead758ecc5097d3ddbacef

ad81758e534704407c258b944d43038f85b9ebbd4aa82fb7c7901975a3f991a5

adc985ac6f17faf00ebf19431246fa142fbe15497478026d1731494481aa0298

b1229bb669f3c7578cbc77e41dec812ec366394bcb344c7c65a5e8fab5fc5164

b2a8fdf8aba620c9cf0487e3898c786ec5dd695cf85a4a683ac8d1f9fa488ca4

b4bae1c8a759c8ce684bbdd069ec8c8d374cbb08722b1239f96b99073cdeda80

b6283421b72312c642e42448227e78b4f2ae8061b7237a78ca30c062505aa0d9

b62b08a40a7ac87358f574e11ddb6c147e97ddb3623015de0558752eb79d87c

b7036e4a9df7d9fe6e3c22b10b6478063b214e45a715b2186d789a8862d5f2a7

b7fccbe89d4ac662aaeec004d45752ba9d8310a1345f69b2e48787ba3a83e99a

bf95d8b3ae7addf63c7dcb802f51c583f1edfee819a6ab0a2e3dacc5f3c7044c

bfc867af7642f30292e2f1b5ed21c33cd03ceaf97915cb3581bd59037e7ca4ea

c26e3bc0584c55ecf4567a68c3af1b62e6a010df1148434fb970eed7586c1faa

c40588f2c24a5359621ce803fc862810fc0f951f81d61530563db9f9b4396bcf

c4407dfd0823aeda497835fb86320b2e0ebfbef0aad2b637ed53dcba5ffef962

c46faf99bebe65cf7f3e17ca7c83a8d93472176dd7b958ee3e0a14abb4f6908e

c5b89f0cb34ad5606ca85994852f1398d8cb17b49e4e597aa67bf8f348134266

c5cb2f215c5e3501e5a7147964f17a7832ed504b9a20961a0e495abba70ddf56

c61ac8213a2dda2614bb0edba72eb9e9d02192aa3afb47425ea5d65277d4d570

c8e4b171ef4897d4aba2be22ff7d945c9aca9b90188ec163c60c52f42f7a52a0

c8f07011c9d3cd46cdc9d1bc9cef48a36c14defb0f94dd1d3a67e085a6fac55a

c95fc10979a86a21ea98ea67ea7be90b30575a3cdcca771d8634d5f684dee779

ca02094ef881fd33c957c6ce9026fe565e3b4b56be1b74a76e8be0320d0385e3

cad967b99dc6a710c902bd5fee1ecc77a61d0bb7ca102b6f784aac8a590616cd

cc9fdea7deda4522caa70c13ee4de5bb20867868be864667609810be6ef7a46b

ccb238e9e11cb3239c7e18c05ee34f388961f2361682e452e54963a50f022c41

cf4fc3bd2d72bca914aa930d1774047fe6d734425900aeef5019e832e26a1989

cfa443a0c3c912fff2b0a6690bfc76c7eb7df06b6231ddfdda7a7112b94e4f7e

d0a580c12f9c91cd3634c2ca2b5cab7c4ae039631186ffe7564e1c3e429037af

d2f43e65b14276be4bbf03f22cb3c8c311a49d77be48c6a630716e96a40f53b1

d5ef648687ea6e11aa292482609bb0c18dfd7075f7a53892bd5cd9ed673e0c29

d69a85241607fc32d365100ad4ceacaf08d51e73ccf32de95838644f844c04d9

dfe536bddaf741c3a34b0e094597a8e2d5bc7ddef4e9486e426cddc56efdebd

e1bf2bff9b5ebdc3178f9aa9ff44961ea76ed672f88cfbba25606806010b0e5d

e38480d31f101b521c412dd69183fbc2078934d3a5df1ed9bd0095ec4de0349b

e54c7a10d975575933fc4d17164edc66352b3e4c761ab886367ab27f2b91268

e5ec3ff5d1f4f73978366d8a0638a520b0b6917bc0fc1de71d229967929a213b

e9c5e2119f21cf8e4cbdd261af84e266dc030736a195a14c951981b5798cd38b

eb96f80ca6c8026a486f7b05f72016758e26baaa99c087c371bdb932e46076be

ebd9be07d71d518acdbcc153095c14a61784ffbed44ecf6876ed3a32ba84de4f

ee23c39ec6d76f3605221ad70375b4d20689a4a89ec4cf642288877a99ffcc7e

ef0d9d0e56e8a07abaabdddfd9ed21e1c41aee14d88c9a7c4e2899e036ff541e

f1248ef627874509e9e04224a4c3e4cee0c3938515e87407d798db2f6b22ca0

f316a3f1d99b1d402003e9686d4394d96512989b4eaeb371de5c165b25b50e49

f365f400f08d0a93cc3af880c1873f74c7c3dfc11f63560108d85123437f99b8

f5f8e55936ef14319e29dc28d4148abb78dfdbe1c02ff014019df2c5f5c3efc0

fd0dd3117cd2967d8ccca0ce3be00edd2d9fdf20f449658b675f45891d27bdcb

fd5ea97a30f5dbad6b2cecf8a4655030ad119db187350efce96b6568f0b378b6

fd6a14c9a4c6d89e7593cdc93395c2d4b160a0535f95b72f8821c5521bfff9d4

fe11948d337576b8ce44232f6e5976a0fd059464e8ee3a9cf94f8507359d4fcf

fe7877b0e29401cba1af0d27b5facce07ed3c6077677dc7b5de46621a3fd8402

fe98134f4cea1a5ba1655552c97d04427f3dbef1c5719bfba958a6b9d54c42f7

1. **CMTX-P-0820240404: Critical Alert: APT41 Threat Actor Campaign**

Threat Overview

Threat Campaign: APT41 Threat Actor

Recent reports indicate that the threat actor has begun employing a combination of malware, open-source tools, and projects in their campaigns. They have developed a specialized loader to directly inject a proof-of-concept for CVE-2018-0824 into memory, exploiting a remote code execution vulnerability to achieve local privilege escalation. The actor has used Shadowpad, Cobalt Strike, and Filezilla for transferring files between endpoints, and the WebPass tool for dumping credentials. In this campaign, the Shadowpad malware exploited an outdated, vulnerable version of the Microsoft Office IME binary as a loader, which then loaded a customized second-stage loader to deploy the final payload.

The threat actor deployed the backdoors via webshell, reverse shell and RDP.

Impacts:

o Information gathering and exfiltration

2. Threat Type: Malware(Shadow pad and Cobalt Strike) and tool (local privilege escalation and web browser credentials)

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses

103.96.131.84

58.64.204.145

Domain

w2.chatgptsfit.com

HASH

2e46fcadacfe9e2a63cfc18d95d5870de8b3414462bf14ba9e7c517678f235c9

eba3138d0f3d2385b55b08d8886b1018834d194440691d33d612402ba8a11d28

1. **CMTX-P082024028 : Critical Alert: AzzaSec Ransomware**

Threat Overview

1. Threat Campaign: AzzaSec Ransomware brief

A new ransomware variant named as Azzasec is active in the cyber threat landscape. Azzasec encrypts the files on Windows machines and operates as ransomware-as-a-service (RaaS). The Azzasec ransomware encrypts files with the extension “.AzzaSec” and changes the desktop wallpaper to display the ransom note.

Impacts:

- -- System Compromise: The malware can gain unauthorized access to systems for retrieving system time.

- -- Personal Information Loss.

- -- The malware granting attackers control over the system.

2. Threat Type : Ransomware

3. Severity: High

Affected Systems/Assets

- - - Microsoft Windows platforms

Distribution Methods:

1. Phishing: Malicious code is delivered via email attachments (Macros,PDFs) that execute when opened.

2. Torrent Websites: Malware is distributed disguised as legitimate files on peer-to-peer file-sharing sites.

3. Malicious Ads: Malware is spread through online advertisements that exploit browser vulnerabilities or redirect users to malicious sites.

Indicators of Compromise (IOCs):

• HASH:

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

58b45bfd8430d8b24f9142278ff206261ab3d1100b3c98b0fdfcefdddf2fd05d

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

1. **CMTX-P082024035: Info Stealer**

Threat Overview

1.Threat Campaign:Information Stealer Malware Campaign

There are a number of sophisticated, information-stealing malwares which have the capabiity to exfiltrate sensitive data from infected systems with the target to cause cyber espionage. Some of them are are mentioned below along with their capabilities:

VIDAR STEALER- The Vidar Stealer is written in C++ with the capability to  gather a variety of data from compromised systems such as cookies, history, and logs from web browsers etc. It contains an updated grabber component, a new format for the acquired data, and a "Command and Control" server for cyber espionage. It runs as "vidar.exe" in infected hosts' Task Managers.

SYNC SCHEDULER- The Sync-Scheduler malware is a C++ document stealer that targets and exfiltrates data from user directories (like Documents, Downloads, and Desktop, focusing on file types such as Word documents etc) by using defense evasion and anti-analysis techniques. It distributes itself through file-nesting within Office documents. The payload of the approach is embedded in a Word document, which is embedded in a PowerPoint presentation.

TEABOT- This Android banking tojan is also known as "Anatsa". This trojan masquerades as legitimate software, enticing users to download them. TeaBot spreads through seemingly harmless dropper applications on the Google Play Store. These applications deceive users into unwittingly installing the malicious payload. Once installed, it exfiltrates sensitive banking credentials and financial information from global financial apps.

STATC STEALER- This stealer is also known as CRUDETAKE. which is a C#-based information stealer, targets browser credentials and employs Windows PowerShell for exfiltration. It stealthily extracts sensitive data from victims’ systems, including passwords, cookies, and cryptocurrency wallet information, targets data and credentials from web browsers, desktop applications, FTP clients (FileZilla), and cryptocurrency wallets.  It encrypts the stolen data and adds it to a text file in the victim's Temp directory before exfiltrating it to the attacker's server.

META STEALER- Meta Stealer is also known as Redline stealer. It is a sophisticated, information-stealing malware known for its ability to exfiltrate sensitive data from infected systems. Primarily targeting personal and financial information, Redline Stealer is distributed through phishing campaigns, malicious downloads, and exploit kits hosted on compromised or malicious websites.

PLANET STEALER- Planet Stealer is a Go-based information stealer capable of stealing passwords, web session cookies, autofill data, and credit card information from Gecko and Chromium browsers. The malware uses various techniques such as an "Exodus Injection" to extract recovery phrases, an anti-virtual machine method to evade detection, and collects information from applications like Discord and FileZilla FTP client.

STRELA STEALER- StrelaStealer is a dynamic data-stealing malware that primarily targets email credentials and is distributed through spam emails with attachments like ISO files or ZIP files containing JavaScript payloads. The malware specifically steals login data from popular email clients.

Impacts:

- -Stolen credentials are traded on underground forums and dark web marketplaces, where they are available for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to your corporate networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.

- -Personal Information Loss.

- -The malware can download and execute additional malicious software, granting attackers control over the system.

2.Threat Type: Stealware

3.Severity: High

Affected Systems/Assets

- -Web Browsers: (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.

- -(Cookies and Session Tokens): Steals cookies and session tokens to maintain or hijack sessions.malware can extract saved login details.

- - Files server and Remote Desktop Access ApplicationsSteals credentials for FTP servers used for file transfers.Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing).Cryptocurrency Wallets: Digital wallets used for managing cryptocurrencies.

- -Email Accounts: Captures login information for email accounts from various providers

- -Social Media and Financial Accounts:

- -Documents and Files: Steals documents and files from the local file system and m ay target files stored in cloud services if credentials for such services are captured.

Distribution Methods

- -Phishing Emails with context aware themes and malicious attachment or links

- -Malvertising: Spread through malicious online ads.

- -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

Mitigation and Recommendations

•Preventive Measures:

- -Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

- -Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- -Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

•Detection Techniques:

- -Monitor Network Traffic: Look for unusual data transfers or connections to malicious servers listed in Annexure

- -Regular Scans: Run regular security scans on browsers and FTP clients to detect and remove malware.

Response Actions:

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

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

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

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

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

Impact Assessment

•Potential Impact:

- -Data Theft: Redline can lead to unauthorized access and theft of sensitive information.

- -Privacy Violations: Compromised data can be used for identity theft, social engineering attacks, or other privacy invasions.

- -Network Compromise: Further infections can occur if the malware spreads across connected systems.

- -Operational Disruption: The campaign can cause significant downtime and operational inefficiencies.

- -Spreading Malware: The malware could spread to other systems within a network, increasing the scope of the attack.

1. **CMTX-P082024916: CMoon Worm Malware**

Threat Overview

1. Threat Campaign: CMoon Worm Malware brief

CMoon is a .NET worm that copies itself to a newly created folder named after the antivirus software it detected on the compromised device or one resembling a system folder if no AVs are detected.

CMoon worm malware can capture screenshots, carry out DDoS attacks, and extract information from various applications such as web browsers, crypto wallets, and messaging apps. It focuses on files with specific keywords or extensions, such as "secret" or "password," and sends the gathered data to a remote server through encrypted TCP connections.

Impacts:

- - - exhibiting credential access, discovery, spyware, and stealware capabilities

2. Threat Type : Stealware

3. Severity: High

Distribution Methods

• Infection chain begins when victims download files that seem to be legitimate documents but are actually self-extracting archives. These archives include both the authentic document and the malicious payload.

Mitigation and Recommendations :

• Preventive Measures:

o Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

o Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

o Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

o User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particulary coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

o Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

o Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

1. **CMTX-P082024926: IOCs related to different RAT families**

1. Threat Campaign: CERT-IN has been tracking prominent malware families such as LummaC2, Redline Stealer, SolarMarker RAT, Rhadamanthys Stealer,Raccoon Stealer and Warzone RAT reportedly active in cyber threat landscape.

LummaC2 is a C based information-stealing malware that targets Windows systems and is distributed through illegal cracks and keygens. It is available as a Malware as a Service. Malware has capabilities to collect various system data, steals files, and extracts sensitive information from cryptocurrency wallets, two-factor authentication extensions, and web browsers artifacts.

Redline Stealer is a sophisticated, information-stealing malware known for its ability to exfiltrate sensitive data from infected systems. Primarily targeting personal and financial information, Redline Stealer is distributed through phishing campaigns, malicious downloads, and exploit kits hosted on compromised or malicious websites.

SolarMarker RAT aka Jupyter Infostealer, Yellow Cockatoo and Polazert is an information-stealing malware capable of backdooring machines and harvesting various credential information, including computer names, admin privileges, cookies, web data, browser password manager information, and logins for crypto-wallets and remote access applications.

Rhadamanthys Stealer aka RADTHIEF, an information-stealing malware is primarily delivered through phishing campaigns, often using malicious attachments or links in emails.One of its capabilities includes collecting sensitive information from infected systems (for example system information, cookies, browsing history, saved credit card information, and data from various applications such as FTP applications, password managers, and email clients).

Raccoon Stealer is one of the most well-known and widely used information-stealing malware families. The malware steals data from applications, including login credentials, credit card information, browsing history, cookies, and cryptocurrency wallet accounts.

Warzone aka Ave Maria is a C++ based backdoor that uses custom protocol over TCP to communicate with attacker infrastructure. Its capabilities include recording video, screenshots, keystrokes, remote desktop, transferring files, executing files, creating a reverse shell and stealing credentials stored by web browsers, email clients, and the Windows Credential Manager. Warzone malware use the dynamic DNS service, Bypassing UAC and create persistence on victim machine.

Impacts:

- -Stolen credentials are traded on underground forums and dark web marketplaces, where they are available for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to your corporate networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.

- -Personal Information Loss.

- -The malware can download and execute additional malicious software, granting attackers control over the system.

2. Threat Type : Stealware

3. Severity: High

Affected Systems/Assets

- -Web Browsers: (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.

- -(Cookies and Session Tokens): Steals cookies and session tokens to maintain or hijack sessions.malware can extract saved login details.

- - Files server and Remote Desktop Access Applications Steals credentials for FTP servers used for file transfers.Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing).Cryptocurrency Wallets: Digital wallets used for managing cryptocurrencies.

- -Email Accounts: Captures login information for email accounts from various providers

- -Social Media and Financial Accounts

- -Documents and Files: Steals documents and files from the local file system and may target files stored in cloud services if credentials for such services are captured.

Distribution Methods

- -Phishing Emails with context aware themes and malicious attachment or links

- -Malvertising: Spread through malicious online ads.

- -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

Mitigation and Recommendations

Preventive Measures:

- -Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

- -Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- -Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

Detection Techniques:

- -Monitor Network Traffic: Look for unusual data transfers or connections to malicious servers listed in Annexure

- -Regular Scans: Run regular security scans on browsers and FTP clients to detect and remove malware.

Response Actions:

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

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

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

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

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

Impact Assessment

Potential Impact:

- -Data Theft: Stealwares can lead to unauthorized access and theft of sensitive information.

- -Privacy Violations: Compromised data can be used for identity theft, social engineering attacks, or other privacy invasions.

- -Network Compromise: Further infections can occur if the malware spreads across connected systems.

- -Operational Disruption: The campaign can cause significant downtime and operational inefficiencies.

- -Spreading Malware: The malware could spread to other systems within a network, increasing the scope of the attack.

1. **CMTX-P082024018: REDLINESTEALER Malware Campaign**

•Limited Sharing (TLP-AMBER): Limited disclosure; recipients can only spread this information on a need-to-know basis within their organization and its clients.

Threat Overview

1.Threat Campaign: REDLINESTEALER information stealer Malware Campaign

Redline Stealer is a sophisticated, information-stealing malware known for its ability to exfiltrate sensitive data from infected systems. Primarily targeting personal and financial information, Redline Stealer is distributed through phishing campaigns, malicious downloads, and exploit kits hosted on compromised or malicious websites.

Impacts:

- -Stolen credentials are traded on underground forums and dark web marketplaces, where they are available for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to your corporate networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.

- -Personal Information Loss.

- -The malware can download and execute additional malicious software, granting attackers control over the system.

2.Threat Type: Stealware

3.Severity: High

Affected Systems/Assets

- -Web Browsers: (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.

- -(Cookies and Session Tokens): Steals cookies and session tokens to maintain or hijack sessions.malware can extract saved login details.

- - Files server and Remote Desktop Access ApplicationsSteals credentials for FTP servers used for file transfers.Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing).Cryptocurrency Wallets: Digital wallets used for managing cryptocurrencies.

- -Email Accounts: Captures login information for email accounts from various providers

- -Social Media and Financial Accounts:

- -Documents and Files: Steals documents and files from the local file system and m ay target files stored in cloud services if credentials for such services are captured.

Distribution Methods

- -Phishing Emails with context aware themes and malicious attachment or links

- -Malvertising: Spread through malicious online ads.

- -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

Mitigation and Recommendations

•Preventive Measures:

- -Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

- -Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- -Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

•Detection Techniques:

- -Monitor Network Traffic: Look for unusual data transfers or connections to malicious servers listed in Annexure

- -Regular Scans: Run regular security scans on browsers and FTP clients to detect and remove malware.

Response Actions:

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

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

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

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

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

Impact Assessment

•Potential Impact:

- -Data Theft: Redline can lead to unauthorized access and theft of sensitive information.

- -Privacy Violations: Compromised data can be used for identity theft, social engineering attacks, or other privacy invasions.

- -Network Compromise: Further infections can occur if the malware spreads across connected systems.

- -Operational Disruption: The campaign can cause significant downtime and operational inefficiencies.

- -Spreading Malware: The malware could spread to other systems within a network, increasing the scope of the attack.

Annexure

(CERTIn-Threat Intelligence ID- CMTX-P082024018)

Indicators of Compromise (IOCs):

IP Addresses:

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

5.254.80.190

95.217.124.248

95.216.104.115

52.143.157.240

77.105.164.59

20.52.165.210

88.99.151.68

194.28.226.213

65.108.21.23

93.115.91.27

51.195.145.80

140.82.32.9

85.28.47.132

84.38.129.31

91.92.249.167

38.180.147.152

91.92.242.175

91.92.240.171

94.131.106.53

185.237.165.67

38.180.203.208

5.254.73.99

77.105.135.107

31.177.108.53

31.177.108.40

147.45.44.16

89.23.101.114

193.3.19.146

94.141.120.170

147.45.47.104

176.111.174.140

185.215.113.67

185.196.9.26

185.215.113.9

207.148.69.28

5.42.92.213

5.42.92.213

193.233.255.34

13.60.40.107

185.196.9.26

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

1. **CMTX-I-025082024: Mythic Malware- APT36 campaign**

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

Common Features of Mythic Malware:

    Persistence

    Remote access and data theft

    Modular architecture and customizable

    Stealth techniques to avoid detection by security software

Prevention Measures:

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

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

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

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

    Principle of least privilege

    Firewall and network security along with regular OS updates

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

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

138.68.134.123

170.64.132.144

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

1. **CMTX-I-50082024: 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 an additional layer of security

Recent such malicious domains identified are as follows:

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

admin-support.in

support-wing.in

desk-info.in

mail-admin.in

mail-official.in

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

1. **CMTX-I-389082024: 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 an additional layer of security

Recent such malicious domains identified are as follows:

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

tn.gov.in.report

www.health.kerala.gov.in.report

tnhealth.tn.gov.in.report

www.tnhealth.tn.gov.in.report

gov.in.report

kerala.gov.in.report

health.kerala.gov.in.report

goadpse.gov.in.report

nic.in.ac

kar.nic.in.ac

\*.gov.in.report

\*.in.ac

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

1. **CMTX-P082024045: DeathGrip Ransomware**

1. Threat Campaign: DeathGrip Ransomware brief

A new ransomware variant called as "DeathGrip" is active in the cyber threat landscape and it operates as Ransomware-as-a-Service (RaaS). It is based on LockBit 3.0 and Yashma/Chaos ransomwares, and some other ransomware tools. DeathGrip is designed to encrypt data and add a ".DeathGrip" extension to its filenames. It encrypts files using AES-256 CGM, disables backups, and employs anti-analysis techniques. Once the encryption process is done, DeathGrip creates a ransom note on a desktop wallpaper (which it placed by changing the original) and in a text file titled "read\_it.txt".It promotes its services through Telegram and other underground forums.

Impacts:

2. Threat Type : Ransomware

3. Severity: High

Affected Systems/Assets

- - - Microsoft Windows platforms

Distribution Methods

- - -Malware is primarily distributed via backdoor/loader-type trojans, drive-by (stealthy/deceptive) downloads, online scams, malicious attachments or links in spam emails/messages, malvertising, suspicious download sources (e.g., freeware and third-party websites, P2P sharing networks, etc.), fake updaters, and illegal software activation ("cracking") tools.

- - -Phishing Emails with context aware themes and malicious attachment or links

- - -Malvertising: Spread through malicious online ads.

- - -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

- - -Malware is primarily distributed via backdoor/loader-type trojans, drive-by (stealthy/deceptive) downloads, online scams, malicious attachments or links in spam emails/messages, malvertising, suspicious download sources (e.g., freeware and third-party websites, P2P sharing networks, etc.), fake updaters, and illegal software activation ("cracking") tools.

Mitigation and Recommendations:

• It is strongly advised that downloading should be done only from reputable and official sources. Since programs obtained from third parties may include malware, all programs must be updated and activated using the features and tools supplied by authorized developers.

• It is also advised to exercise caution when browsing because dangerous and fraudulent content frequently looks innocent and real. It's important to handle incoming emails and other messages carefully. It is not advisable to open attachments or links included in suspicious or irrelevant emails since they may spread infection.

• Installing and maintaining an up-to-date reliable anti-virus program is crucial for user and device safety.

• Preventive Measures:

- - - Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- - - Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- - - User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- - - Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- - - Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions

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

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P082024045]

Indicators of Compromise (IOCs):

HASHES:

e173dd358ec750f561ec4eec0c6d75e8709bc32fbe43a5e9a92dd0db96c82b58

274844568a6a9ce334d71efeac21f528d7b54b2cd4377c978cc1270c6ad986c4

f9600b1b06588e3815a55eb81e35289f7b9a5749ae623550734c5f3d8c04e038

8ae1d9e815abc504d01b48ecf21e4133b34b4b3e4a0e93804f44f8a9b328bd5d

6bce98ce8751d6f87e97578a05e606a0b699f24c1a69b96cd28ef88d4984fe71

DOMAIN:

[https://master-repogen.vercel.app]https://master-repogen.vercel.app

1. **CMTX-P082024064: Arc Silt Malware**

Threat Overview

1.    Threat Campaign: ArcSilt Malware

ArcSilt is a custom malware family that targets small home and office (SoHo) routers, DVR and IP camera appliances, network-attached storage (NAS), and other internet-facing devices. The malware is likely used as part of a China-nexus covert infrastructure network, based on observed technical artifacts and alignment with the tactics of China-nexus threat actors. The malware's targeting of various router models and its association with a campaign exploiting zero-day vulnerabilities demonstrate its evolving capabilities and potential impact on network security.

Impacts:

Information gathering and exfiltration

2.    Threat Type: Malware

3.    Severity: High

Affected Systems/Assets

SOHO router devices, including end-of-life Cisco RV320/RV325 routers, Ivanti Pulse Secure VPN , ASUS router models, and QNAP devices.

Mitigation and Recommendations

Preventive Measures:

Patch vulnerable application: - As attacker target the vulnerable Microsoft tracked as CVE-2018-0824 , it is advised to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Detection Techniques:

Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known ArcSilt malware. Refer to the provided Annexure for specific hash values and behavioural indicators.

Response Actions:

Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Annexure

Indicators of Compromise (IOCs):

IP Addresses

104.136.191.151

108.6.49.39

113.61.182.254

115.21.190.71

119.246.51.206

119.247.246.237

121.148.244.135

122.215.187.23

124.244.34.180

125.59.116.52

140.228.220.56

141.164.125.246

152.165.225.48

156.155.142.146

157.131.181.118

157.157.36.129

172.118.29.20

173.174.92.59

175.117.39.52

176.37.208.150

176.38.36.25

180.69.134.173

181.129.53.59

184.152.74.92

184.68.123.18

192.230.136.217

198.217.121.198

203.173.189.80

203.218.198.139

207.183.188.149

207.44.27.95

209.202.217.22

210.242.252.145

211.208.120.162

211.219.150.242

212.244.34.194

212.37.113.58

213.21.86.45

216.165.244.2

216.240.37.130

216.83.134.2

219.73.104.250

219.73.46.174

219.78.219.98

220.82.139.190

221.118.2.22

221.127.9.62

223.18.252.82

24.159.100.85

24.29.84.189

27.35.41.184

37.70.32.89

4.1.125.201

45.75.70.137

47.14.103.129

47.156.128.136

50.64.172.221

57.132.188.99

58.153.68.126

58.176.16.134

59.10.175.233

59.120.179.63

61.238.197.81

61.92.101.142

67.85.43.183

68.168.164.163

68.190.82.158

70.81.228.83

71.83.253.238

71.90.41.193

72.43.187.155

75.139.203.104

76.166.225.186

76.95.189.107

81.227.99.38

81.93.194.232

84.1.30.86

84.216.27.65

85.229.72.27

86.115.58.202

86.97.107.121

87.199.82.136

87.248.1.96

89.23.245.206

92.119.93.183

92.33.203.8

96.42.108.78

96.57.195.131

HASH

edc1a18ab0ed73927bfe3e1ce8fe7493676b8ef32582e018e2cf8df73d59dcda

41a3bcb4efc85f3da23c8294be005399ac8137077c30f25a98f0ceea5466fbf9

464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd

13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13

72b3414f9a6fa2fd02d172fe391197d937448ad8d286c8f631595695c22535f9

9508e50f5a2b674e914b79a2da441fffa561fa73f7a29cf61f9d2156c498e44e

07b4b7c933357b9c608867fb90e004fb78d139a2eab6be1152c90309fea78fe5

361a9b8a99afcfadf0210c92c907681662ce8d88b4dc0d0042fd208f31323621

1. **CMTX-P082024936: QuasarRAT Malware**

1. Threat Campaign: QuasarRAT Malware

Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely observed used in malware campaigns. Quasar RAT has capability of capturing screenshots, Key logger, gather System Information, remote Shell and Command execution, reversing proxy, Managing tasks and files, Configuring and building client executables.

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 publicly available Windows backdoor

Distribution Methods

• Spread through spearphishing emails or exploitation of vulnerabilities in public-facing applications.

Mitigation and Recommendations :

• Preventive Measures:

o Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block attachments of file types:[exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf]. Ensure to scan all software downloaded from the Internet prior to executing.

o Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

o Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

o User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particulary coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

o Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

o Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024936

Indicators of Compromise (IOCs):

• IP ADDRESSES

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

95.214.27.172

46.101.68.183

115.79.141.193

87.19.18.186

87.89.82.13

94.156.69.158

181.161.2.204

178.215.236.251

103.252.123.135

103.136.199.168

91.92.244.12

193.42.11.9

121.43.97.90

157.10.51.167

5.44.252.181

45.76.85.168

194.163.171.74

2.58.56.192

185.161.210.49

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

1. **CMTX-P082024946: Mimic Ransomware**

Threat Overview

1. Threat Campaign: Mimic Ransomware brief

Mimic Ransomware, also known as N3ww4v3 involves the targeting and exploitation of MSSQL database servers to gain initial access to victims' system. Finally, the payload disables recovery by deleting data backups and corrupting the disk in addition to cleaning up the other tools that were deployed.

Impacts:

- - -- Personal Information Loss.

- - -- The malware granting attackers control over the system.

- - -- Targeting and exploitation of MSSQL database servers

2. Threat Type : Ransomware

3. Severity: High

Mitigation and Recommendations:

• Preventive Measures:

- - - Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- - - Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- - - User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- - - Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- - - Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024946

Indicators of Compromise (IOCs):

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

• HASHES:

558147caa20eddf708986e89d7f000809025c5ade03fda1f352dba513e8f1454

804de08fb28dcae51efca2960de3dc9460114fc8d376ad6a966144cb55aa9f75

d13b43518d0ed2fe938e186eb218debd15022b9803c0d330363ca40830db9a77

ae7031dfae21616d7eec326c16ebac7f9d911a354ba32dd4b4c458fe50351805

04ba9dd2d3127511af52e1be3015e0424491cfb2133f90f8b5b5cac2e33166d4

89672638152c13d10ae8afa03df7798081d025939bcfae354e8540cdda2cf16a

549a883cb3d923eb0b45248d6f46bd2859a3265f203e6019f3e4b9df6c9f9813

d04904e32b5cb0f9b559855fac81d62c6ad0472dc443be02f08b6fe4a7d56f71

73de5c6390f26133f20208367c4398798fd4dc1e9986bdfb7fea9288f4f53efa

0964ec866b24eea67c8e7b11060acbf9455e182d0ff97987114c291d29e54f73

4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a

cdb0c28ec03ffbf66309d74d537b8157161cf775ee00a49398e97e4bf735d7d9

81423f5454208e958aa183c2850809620676485c63aab07d91a6f85c1d9b4e72

• IP ADDRESES:

91.203.134.122

80.66.76.30

194.26.135.76

• DOMAIN:

times.windowstimes.online

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

1. **CMTX-P082024038: Cronus Ransomware**

1. Threat Campaign: Cronus Ransomware brief

A new ransomware variant named Cronus is currently active in the cyber threat landscape. It operates by disguising itself in documents that appear to be legitimate. Once it executed, it deploys a PowerShell script to load its ransomware payload, which encrypts files and alters their extensions with random characters.

- --Distribution Method:

1.Phishing: Ransomware is delivered via malicious email attachments or links.

2.Malicious Ads: Ads leading to malicious sites or downloads.

3.Compromised Websites: Websites with vulnerabilities or malicious content distributing the ransomware.

Impacts:

- -- Personal Information Loss.

- -- The malware granting attackers control over the system.

Capabilities:

Cronus ransomware is capable of encrypting files, renaming extensions, displaying ransom notes, and altering system settings. It uses advanced techniques like PowerShell scripting and reflective DLL loading to evade detection and can spread across networks.

2. Threat Type : Ransomware

3. Severity: High

Mitigation and Recommendations:

• Preventive Measures:

- - - Regularly patch and update software and operating systems to the latest available versions.

- - - Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- - - User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- - - Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- - - Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

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

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024038

Indicators of Compromise (IOCs):

• HASHES/URL:

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

69b6bc4db69680118781e7a9f2580738088930fa04884755f23904fa19e638e3

629587e592130b86418d17d6b8cc52b6f378f39f1b5e8caa4038cfa7120b2a53

dd78c6dc62463aba24cdbea3968cbcc1c7b97a736ef069d99d6512b10c5e91f3

URL:

hxxps://eternal.lol/file/

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

1. **CMTX-I-993082024: 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 an additional layer of security

With reference to previous alert, CMTX-I-501072024 dated 30/07/2024 where the parent and associated subdomains were informed, additional malicious subdomain is as follows:

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

indianarmy.nic.in.aboutcase.nl

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

1. **CMTX-P-082024065: SHADOWPAD (POISONPLUG) Malware Campaign**

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multimodular backdoor

3. Severity: High

Distribution Methods:

• ShadowPad 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

Mitigation and Recommendations :

1. Patch Management: Regularly update and patch all software, operating systems, and applications to close vulnerabilities that malware could exploit.

2. Endpoint Protection: Utilize robust endpoint protection solutions, including antivirus and anti-malware tools, to detect and block known threats.

3. Network Segmentation: Divide your network into segments to limit the spread of malware. Ensure that critical systems and sensitive data are isolated from less secure network areas.

4. Access Controls: Implement strict access controls and adhere to the principle of least privilege, ensuring that users and systems have only the permissions they need.

5. Regular Backups: Maintain regular, secure backups of critical data and systems. Store backups offline or in a manner that prevents network access.

6. Security Awareness Training: Educate employees on cybersecurity best practices, including how to recognize phishing attempts and handle suspicious emails or attachments.

7. Intrusion Detection and Prevention: Implement intrusion detection and prevention systems (IDPS) to monitor network traffic and identify unusual or malicious activities.

8. Application Whitelisting: Use application whitelisting to ensure only approved applications can run on your systems, blocking unauthorized or potentially harmful software.

9. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address weaknesses in your security posture.

10. Threat Intelligence: Stay updated on emerging threats and vulnerabilities by subscribing to threat intelligence services for the latest information on new malware and attack techniques.

11. Incident Response Plan: Develop and regularly update an incident response plan to ensure a swift and effective response in the event of a security breach.

12. Monitoring and Logging: Implement comprehensive monitoring and logging practices to detect and analyze unusual activities that may indicate a breach. Regularly monitor all  outbound traffic, particularly traffic destined for newly registered domains or Dynamic DNS (DDNS) and Domain Generation Algorithms (DGA) domains.

13. Recommend to monitor DNS traffic to detect DNS tunneling such as Unusual DNS request/ response. Watch for anomalies like unusually large DNS queries or responses, an excessive number of DNS requests from a single source, or large amounts of data within DNS queries. or requests directed at unfamiliar or suspicious domains, as these can indicate potential tunneling activity.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-0820240405

Indicators of Compromise (IOCs):

IP Addresses

156.238.243.171

38.180.191.141

154.39.142.24

45.249.89.54

103.176.70.194

45.125.32.218

154.23.240.92

154.90.59.6

95.179.163.123

154.90.55.78

101.36.124.31

154.90.59.6

101.36.124.31

1. **CMTX-P-082024055: 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

38.147.172.16

208.85.16.252

45.139.226.104

45.152.66.25

103.234.54.179

45.139.226.104

208.85.16.252

45.139.226.104

38.147.172.16

45.139.226.104

208.85.16.252

45.139.226.104

45.144.137.116

176.119.203.246

38.147.172.16

38.89.72.133

38.147.171.189

45.144.136.250

83.229.127.115

83.229.127.136

142.252.0.73

165.154.8.67

45.145.228.85

45.144.136.250

192.189.2.23

192.189.2.23

1. **CMTX-P082024064: GobRAT Malware**

1.    Threat Campaign: GobRAT Malware

GobRAT is a remote access Trojan (RAT) written in Go, designed to infect Linux routers. It features several capabilities, including disabling firewalls, establishing persistence through cron jobs, registering SSH public keys for remote access, and executing DDoS attacks. Initial access is gained by exploiting vulnerabilities in internet-exposed routers with open Web-based User Interfaces (WEBUI). Once access is secured, a loader script is deployed, disguised as the Apache daemon process to evade detection. This loader script then installs the GobRAT malware on the compromised router.

Impacts:

o   Information gathering and exfiltration

2.    Threat Type: Malware

3.    Severity: High

Affected Systems/Assets

Linux routers devices, PostgreSQL and Redis

Mitigation and Recommendations

Preventive Measures:

Patch vulnerable application: - As attacker target the vulnerable Linux routers devices, PostgreSQL and Redis , it is advised to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Detection Techniques:

Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known GobRAT malware. Refer to the provided Annexure for specific hash values and behavioural indicators.

Response Actions:

Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Annexure

Indicators of Compromise (IOCs):

IP Addresses

38.54.84.238

38.60.223.51

38.54.56.5

38.60.221.63

38.180.66.147

38.60.221.174

38.60.223.81

38.60.221.39

38.180.66.147

38.54.85.246

38.60.221.32

1. **CMTX-P082024058: Blacksuit Ransomware**

Threat Overview

1. Threat Campaign: Blacksuit Ransomware

Blacksuit Ransomware, a possible rebrand Royal ransomware is reportedly active in the cyber threat landscape. Phishing emails are a primary method used by BlackSuit threat actors to gain initial access and may exploit vulnerabilities in public-facing applications also. Once inside the victim's network, they disable antivirus software, use legitimate remote access tools like AnyDesk and MobaXterm to establish and maintain access to compromised systems. BlackSuit first exfiltrates and extorts data before encryption, and if the ransom isn't paid, it publishes the victim's data on a leak site.

Impacts:

- -- Personal Information Loss.

- -- The malware granting attackers control over the system.

- -- Financial loss and reputation damage.

Capabilities:

- --Self-Deletion: Can remove its own file after encrypting.

- --Initial Access: Gets in through phishing or exploiting weaknesses in online apps.

- --SSH Access: Utilizes tools such as Chisel and SSH clients for remote access and control.

- --Command and Control: Communicates with C2 servers using legitimate and open-source tools.

- --Persistence: Maintains long-term access through remote monitoring tools and malware.

- --Lateral Movement: Spreads across networks using RDP, PsExec, and SMB.

2. Threat Type : Ransomware

3. Severity: High

Mitigation and Recommendations:

• Preventive Measures:

Remove unnecessary access to administrative shares, particularly ADMIN$ and C$. If ADMIN$ and C$ are required for operational purposes, restrict access to only essential service or user accounts and continuously monitor for any unusual activity. Employ a host-based firewall to permit connections to administrative shares via SMB solely from a restricted group of administrator machines

Regularly patch and update software and operating systems to the latest available versions.

- - - Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- - - User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

- - - Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- - - Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

• Response Actions:

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

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

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

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

5. Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts particularly for webmail, virtual private networks, and accounts that access

critical systems to add an additional layer of security

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024058

Indicators of Compromise (IOCs):

• HASHES/URLs/IPs/Domains:

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

URLs

hxxps://1tvnews.af/xmlrpc.php

hxxps://avpvuurwerk.nl/xmlrpc.php

hxxps://beautyhabits.gr/xmlrpc.php

hxxps://interpolyaris.ru/xmlrpc.php

hxxps://libertygospeltracts.com/xmlrpc.php

hxxps://oldtimertreffen-rethem.de/xmlrpc.php

hxxps://stroeck.at/xmlrpc.php

hxxp://megupdate.com/

hxxp://zoommanager.com/

myappearinc.com/acquire/draft/c7lh0s5jv

pastebin.mozilla.org/Z54Vudf9/raw

IPs

147.135.36.162

152.89.247.50

47.87.229.39

147.135.11.223

193.235.146.104

193.149.176.157

140.82.48.158

185.7.214.218

45.61.136.47

5.181.234.58

45.141.87.218

184.174.96.16

89.251.22.32

135.148.67.84

180.131.145.85

180.131.145.61

185.190.24.103

144.202.120.122

155.138.150.236

140.82.18.48

45.76.225.156

Domains

Abbeymathiass.com

Mail.abbeymathiass.com

Store.abbeymathiass.com

Mail.turnovercheck.com

Store.turnovercheck.com

turnovercheck.com

Hourlyprofitstore.com

tumbleproperty.com

myappearinc.com

parkerpublic.com

ciborkumari.xyz

Hashes:

af9f95497b8503af1a399bc6f070c3bbeabc5aeecd8c09bca80495831ae71e61

C4A2227CD8D85128EAFEF8EE2298AA105DA892C8B0F37405667C2D1647C35C46

8d16a23d5a5630502b09c33fbc571d2261c6c98fecc3a79a1e1129354f930d0a

01ce9cfebb29596d0ab7c99e8dbadf1a8409750b183e6bf73e0de021b365be13

a0a4a99948e12309f54911264261d96f0e40d5fd695bab82e95fbc1f9024482e

146335b1be627318ac09476f0c8f8e6e027805e6077673f72d6dce1677a24c78

9493b512d7d15510ebee5b300c55b67f9f2ff1dda64bddc99ba8ba5024113300

E813F8FAF3AA2EB20E285596413F5088B2D7FD153FE9F72F3FF45735D0FDDCED

25A6F82936134A6C5C0066F382530B9D6BF2C8DA6FEAFE028F166B1A9D7283CF

e3d7c012040962acd66f395d1c5c5f73f305aa1058f2111e8e37d9cb213b80c4

C798B2690C5F16EB2917A679AF3117CFE9C7060FA8BC84FFC3159338EF33508E

3c8c1b1f53e0767b7291bb1ae605ffa62a93e9c8cc783e4ca47ac84b48320d59

ee6ec2810910c6d2a2957f041edd1e39dca4266a1cc8009ae6d7315aba9196f5

68c57daed0e5899c49b827042bcf3bbeba33b524bd83315a44d889721664dc34

bbb7404419f91f82cedfec915931a9339f04165b27d8878d63827c9ee421ed62

338228a3e79f3993abc102cbac2ff253c84965213d59ac30892538cdd9b0a22b

3041dfc13f356c2f0133a9c11a258f87cb7de1e17bc435e9b623d74bc5e1c6be

8F87A1542EE790623896BBAAB933D1883484DE02A7B3D65D6C791D50173A923D

f02af8ffc37d1874b971307fdec80e33e583b56d9ebabda78a4b8ad038bc3bf0

b028eaa0ec452c6844881dc34be813834813a40591b89ea9a57dd4fb4084e477

ae724dce252c7b05a84bc264993172cf86950d22744b5e3a1b15ba645d9d3733

141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944

e87512ea12288acec611cf8e995c4ced3971d9e35c0c5dcfd9ee17c9e3ed913d

f805dafb3c0b7e18aa7d8c96db8e8d4e9301ff619622d1aecc8080e0ecd9ebbe

6332f189cc71df646ff0f1b9b02a005c9ebda3fe7b9712976660746913b030de

420db40d26d309d3dba3245abb91207f1bca050530545a8048f856e5840d22a2

1743494f803bbcbd11150a4a8b7a2c5faba1223da607f67d24b18ca2d95d5ba3

216047c048bf1dcbf031cf24bd5e0f263994a5df60b23089e393033d17257cb5

be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1

d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681

8a983042278bc5897dbcdd54d1d7e3143f8b7ead553b5a4713e30deffda16375

b8c4aec31c134adbdbe8aad65d2bcb21cfe62d299696a23add9aa1de082c6e20

342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee

4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce

a83a5810ea7a4f02d4623c509dd9b88ad4e432177143e9e9b2b30f9b2943a1b0

8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451

74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c

0a9a342cf4b9ccba811922b32c55498a3448b198702e2ec17269653c161bbda3

82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58

41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d

3288f6f98bc2445f4ad688b562fe12414893c1ac

585b05b290d241a249af93b1896a9474128da969

dd37973be7e6ede23c131a48919a4f6e1fb49328

b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf

1206bd44744d61f6c31aba2234c34d3e35b5bac7

790d40cd16fb458bf99e3600bce29eca06d40b56

a84ed0f3c46b01d66510ccc9b1fc1e07af005c60

c96154690f60a8e1f2271242e458029014ffe30a

0488348645ebb39ee7a51a09f2705c87d89d27f1

7902b08fb184cfb9580d0ad950baf048a795f7c1

65dc04f3f75deb3b287cca3138d9d0ec36b8bea0

92283d4d0e7e730c3f4f5485bfa48cb6

50cc3a3bca96d7096c8118e838d9bc16

57bd8fba4aa26033fa080f390b31ed0e

5cb9d80f82f674b065c3d80816a370c4

0191d87b91f1545e13b3af4a442ae949

cdcf4f24dc07d5da5be076793983a308

527c71c523d275c8367b67bbebf48e9f

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

1. **CMTX-P-082024085: Dark Crystal RAT (DC RAT)**

Threat Overview:

DarkCrystal RAT also known as DCRat is a commercial Russian backdoor which operates as a Malware-as-a-Service (MaaS). It has been associated with various malware families such as BlackMatter, Cerber, Cobalt Strike, Ficker Stealer, QakBot, REvil, and Ryuk. For its command and control communications, it uses SSL/TLS certficates. The malware allows threat actors to gain unauthorized access to infected systems and perform various malicious activities such as data theft and system control. It can steal information from the following sources like Browser cookies,Browser stored passwords ,Browser stored form content ,Browser history ,Stored credit cards (via Windows DPAPI & Chrome SQLite Database),Telegram,Discord tokens, keyloggers, etc.

Impacts:

1. The RAT may employ techniques to ensure it remains on the system even after initial cleanup attempts. These mechanisms make it difficult to identify and remove the RAT.

2. Installation of Additional Malware: Once the RAT is on a system, attackers can use it to install other types of malware, including ransomware, spyware, or additional RATs.

3. The RAT can be used to spread laterally across a network, potentially compromising other systems and increasing the scope of the attack.

4. System Manipulation: The RAT can be used to modify system settings, install additional malware, and perform other actions that compromise the integrity of the system.

Threat Type: Backdoor

Severity: High

Mitigation and Recommendations

1. Security Software:Utilize and keep your antivirus and anti-malware tools up-to-date. These solutions help detect and block Remote Access Trojans (RATs).

2. Patching and Updates:Regularly update your software and systems to address vulnerabilities that could be exploited by malware.

3. Network Security:Implement robust firewall and network monitoring solutions to detect and block malicious activity.

4. User Training:Educate users about recognizing phishing attempts and other social engineering tactics. Awareness is key to preventing RAT infections.

5. Incident Response Plan:Develop and maintain a comprehensive incident response plan. This ensures quick action in case of security breaches.

6. Data Backups: Regularly back up important data and ensure that backups are secure and accessible.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-082024085

Indicators of Compromise (IOCs):

IPs

1.23.216.249

1.23.216.6

103.140.155.26

103.15.255.128

103.155.3.96

103.175.180.31

103.175.75.231

103.186.41.84

103.217.242.247

106.219.186.248

106.222.216.246

106.76.244.16

110.226.173.54

115.99.76.34

117.207.13.199

122.172.61.28

122.173.50.168

146.196.47.184

152.58.197.127

152.58.208.195

152.58.238.146

152.58.77.35

152.59.102.61

152.59.37.135

152.59.90.116

157.48.120.233

175.101.108.163

27.6.189.22

49.36.24.246

49.47.218.168

49.47.218.233

67.205.154.243

1. **CMTX-P-082024075: AsyncRAT**

Threat Overview

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:

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

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

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

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

Threat Type: Malware

Severity: High

Mitigation and Recommendations

• Preventive Measures:

1. Proactive Security Software: Make use of the most recent anti-virus and anti-malware programs that are able to identify and stop AsyncRAT and related attacks.

2. Patch management refers to the process of routinely updating software, operating systems, and apps to address vulnerabilities that malware may exploit.

3. Firewall and Network Security: Set up firewalls and network security configurations to prevent incoming and outgoing traffic that appears suspicious or may be connected to Remote Access Protocol (RAT) interactions.

4. Email security: Use email filters to identify and stop dangerous attachments and phishing emails, which are frequent RAT delivery channels.

5. User Education: Teach staff members and users how to spot phishing scams, dubious links, and other social engineering ploys used to disseminate remote access Trojans.

6. Least Privilege Principle: To lessen the possible impact of an account being compromised, restrict user permissions to only those required for their position.

• Detection Techniques:

1. Network traffic analysis: Look for unusual or suspicious activity in the network traffic that could point to the existence of a RAT.

2. Endpoint Detection and Response (EDR): Make use of EDR tools to keep an eye out for malware activity on endpoints and to get thorough forensic data.

3. Frequent Scans: To find and fix potential vulnerabilities, conduct frequent security scans and vulnerability assessments.

• Response Actions:

1. Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

2. Restoration: To be sure that there are no leftover virus traces, restore impacted computers from clean backups.

3. Communication: As appropriate, notify internal teams and any potentially impacted customers, as well as other pertinent stakeholders.

Indicators of Compromise (IOCs):

A reference file is attached for your reference.

1. **CMTX-P082024064: Quad7 Botnet**

Threat Overview

1.    Threat Campaign: Quad7 Botnet

The "Quad7 botnet", aka Botnet 777 was first reported by researchers in October 2023, is a network of around 10,000 nodes engaged in stealthy brute-force attacks on Microsoft Azure, using TCP port 7777. Named for the xlogin: banner on port 7777, this botnet was initially believed to target high-profile users, but recent data shows no specific targeting pattern. The botnet’s operations involve compromising routers,  mainly infecting Asus, TP-LINK routers and IP cameras, while the new 63256 botnet primarily targets Asus routers. The Quad7 botnet remains active and resilient, with evolving tactics and many compromised devices. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale.

Impacts:

Account compromise, sensitive Data Exposure, and reputation Damage etc.

2.    Threat Type: Malware

3.    Severity: High

Affected Systems/Assets

Microsoft Azure instances, Asus and TP-LINK routers

Mitigation and Recommendations

Preventive Measures:

- --Maintaining Up-to-Date Firmware

- --Implement Robust Security Practices such as using strong, unique passwords, MFA, disabling unused services

Detection Techniques:

- --Monitoring for unusual spikes in traffic, unexpected outbound connections, or communication with known malicious IP addresses.

- -- Establishing and monitoring baselines for normal network and system behavior to detect deviations indicative of botnet activity.

- -- Identifying patterns of communication typical of C2 servers, such as regular check-ins or encrypted channels.

- --Detecting unusual or unauthorized processes and services running on endpoints that could be part of a botnet.

Response Actions:

- --Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

- --Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

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

Annexure

Indicators of Compromise (IOCs):

IP Addresses

151.236.20.185

151.236.20.211

104.168.152.139

142.11.205.164

23.227.196.73

23.254.201.175

23.254.209.118

1. **CMTX-P082024078: SolarMarker RAT Malware Campaign**

1.Threat Campaign: SolarMarker RAT Malware

SolarMarker RAT alias Polazert, Yellow Cockatoo and Jupyter, is a remote access Trojan that is Developed in Microsoft .NET framework. Attacker use Google search redirection and drive-by compromise tactics to drop the SolarMarker RAT on the host system. SolarMarker RAT is capable of collecting the following types of information from the infected system like Computer name, operating system (OS), system architecture, Data about the current user, credentials Stored in web browser.

Impacts:

- -Stolen credentials are traded on underground forums and dark web marketplaces, where they are available for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to your corporate networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.

- -Personal Information Loss.

- -The malware can download and execute additional malicious software, granting attackers control over the system.

2.Threat Type: Stealware

3.Severity: High

Affected Systems/Assets

- -Web Browsers: (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.

- -(Cookies and Session Tokens): Steals cookies and session tokens to maintain or hijack sessions.malware can extract saved login details.

- - Files server and Remote Desktop Access Applications Steals credentials for FTP servers used for file transfers.Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing).Cryptocurrency Wallets: Digital wallets used for managing cryptocurrencies.

- -Email Accounts: Captures login information for email accounts from various providers

- -Social Media and Financial Accounts:

- -Documents and Files: Steals documents and files from the local file system and m ay target files stored in cloud services if credentials for such services are captured.

- -Sectors where SolarMarker has been particularly active include small and medium-sized businesses (SMEs), government, healthcare, and education.

Distribution Methods

- -Phishing Emails with context aware themes and malicious attachment or links

- -Malvertising: Spread through malicious online ads.

- -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

Mitigation and Recommendations

•Preventive Measures:

- -Set up filtering rules in your email security solution to block malicious attachments and URLs. This requires updating your email security gateway or software to detect and filter out suspicious emails. Ensure that your email security  solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs..

- -Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

- -Password Management: Encourage the use of unique, strong passwords for each service and implement multi-factor authentication (MFA) to add an extra layer of security

•Detection Techniques:

- -Monitor Network Traffic: Look for unusual data transfers or connections to malicious servers listed in Annexure

- -Regular Scans: Run regular security scans on browsers and FTP clients to detect and remove malware.

Response Actions:

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

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

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

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

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

Indicators of Compromise (IOCs):

IP Addresses:

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

146.70.80.66

193.29.104.25

217.138.215.105

185.236.203.159

23.29.115.186

212.237.217.136

146.70.145.242

146.70.80.83

185.243.113.47

185.243.115.88

217.138.215.79

146.70.160.62

2.58.15.214

46.30.188.221

91.206.178.133

193.29.56.179

212.237.217.133

2.58.14.183

78.135.73.176

45.86.163.163

212.237.217.156

67.43.234.109

146.70.71.135

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

1. **CMTX-P082024088: Spark RAT Malware Campaign**

1.Threat Campaign: Spark RAT Malware

SparkRAT is a cross-platform and full-featured Remote Administration Tool (RAT) written in Go. Its capabilities include file and process management, file transfer, remote desktop monitoring and screen capture, system information collection, and terminal access for command execution, among others. SparkRAT uses the WebSocket protocol for communication with the C2 server and features an upgrade system that allows it to automatically update to the latest version available on the C2 server upon startup

Impacts:

- -Personal Information Loss.

- -The malware can download and execute additional malicious software, granting attackers control over the system.

2.Threat Type: Malware

3.Severity: High

Capabilities:

- -It can capture system information, create files, create processes, delete files, and download files on the victim system.

- -It can restart or shut down the operating system, capture screenshots, self-update to the latest version, and terminate running processes.

Distribution Methods

- -Phishing Emails with context aware themes and malicious attachment or links

- -Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

Mitigation and Recommendations

- -Regularly patch and update software and operating systems to the latest available versions.

- -Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser.  Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

- -User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful  infections.

- -Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

- -Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

Response Actions:

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

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

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

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

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

Annexure

(CERTIn-Threat Intelligence ID- CMTX-P082024088)

Indicators of Compromise (IOCs):

IP Addresses:

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

103.108.41.146

38.54.94.13

67.217.62.106

138.68.127.131

37.1.213.121

38.54.94.13

175.178.126.203

101.43.187.44

47.97.185.22

117.50.76.61

83.221.206.30

110.42.250.96

170.64.181.207

84.32.214.103

103.253.43.208

47.236.43.52

103.108.41.147

103.118.41.11

137.184.68.203

211.155.101.2

121.37.111.182

27.124.40.170

27.124.40.175

38.154.74.20

46.254.21.214

118.190.161.229

101.35.198.64

157.119.101.234

23.224.176.82

1.94.11.195

161.35.28.74

116.62.145.180

45.145.229.159

47.96.129.195

116.63.145.255

120.220.61.6

103.108.41.148

15.168.125.19

185.56.139.92

43.136.35.213

47.105.208.58

1.15.135.238

31.41.221.123

63.250.53.103

23.225.14.151

154.90.48.200

67.219.106.134

140.238.9.202

47.106.152.139

68.168.211.94

139.180.180.177

27.124.40.169

38.60.199.70

8.149.228.52

58.37.81.238

154.90.44.78

121.4.140.182

107.175.254.117

8.210.81.164

106.54.232.49

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