**Cyber Security Advisories**

**Date: 30 August 2024**

1. **CMTX-P-082024094: SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multimodular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses: Port

154.90.44.131

38.54.50.46

216.238.121.119

54.247.114.30

38.54.76.41

1. **CMTX-P-0820240704: PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

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

Impacts:

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

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

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

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses

38.47.220.145

38.47.220.155

38.47.220.140

45.152.65.213

45.133.239.21

193.38.137.10

103.201.131.181

1. **CMTX-I-995082024: 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.

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

ashifdigitalseva.xyz

birthdeath.in

gov-certificate.com

verifycertificate.info

viewss.click

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

1. **CMTX-P082024062: Dispossessor Ransomware**

Dispossessor (aka Radar) is a ransomware that have targeted over 40 organizations worldwide, particularly those in the healthcare, education, financial services, and transportation sectors. The threat actors behind Dispossessor gain access to networks through various means, including exploiting vulnerabilities, weak passwords, and the absence of multi-factor authentication (MFA). Once inside the victim's network, they steal data and deploy ransomware to encrypt the company's devices. The group operates using a dual-extortion model like other ransomware groups e.g.; encrypting the system's files and exfiltrating the data to hold it for ransom. The Dispossessor gang also engages in other malicious activities, such as reposting data stolen from other ransomware operations and attempting to sell it on breach markets and hacking forums.

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.

- ----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:

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

- ----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 store securely 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 address malware infections quickly and effectively and minimize damage.

• Response Actions:

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

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

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

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

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

critical systems to add an additional layer of security

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

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

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

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024062

Indicators of Compromise (IOCs):

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

radar.tld

dispossessor.com

dispossessor-cloud.com

cybershare.app

readteamcr.com

redhotcypher.com

cybernewsint.com

cybertube.video

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

1. **CMTX-P082024007: SystemBC Malware Campaign**

SystemBC is a type of malware classified as a RAT. It allows attackers to gain unauthorized access and control over an infected system. Once installed, it provides various functionalities, including remote control, data exfiltration, payload delivery, network reconnaissance, persistence, and the key features of a SOCKS proxy. While SystemBC and BlackBasta are distinct in their functions, they can be part of a coordinated attack.

Impacts:

- --- Data Loss.

- --- Infrastructure damage.

- --- Financial loss and reputation damage.

2.Threat Type: Remote Access Trojan.

3.Severity: High

Capabilities:

- -- C2 Communication: The malware can give the attacker remote control over the infected system, allowing them to perform a wide range of actions.

- -- Data Exfiltration: It steal sensitive information from the infected system, such as personal data, financial information, or corporate secrets.

- -- Payload Delivery: It can be used to deliver additional malicious payloads to the infected system, including other types of malware.

- -- Network Reconnaissance: The malware can help attackers gather information about the network, which can be useful for further attacks or lateral movement.

- -- Persistence: It can implement techniques to ensure it remains on the system and evades detection or removal efforts.

- -- SOCKS Proxy: It acts as a SOCKS proxy, letting attackers route their traffic through the infected system to conceal their IP address and evade detection.

Distribution Methods

- -- Phishing campaigns.

- -- Malicious downloads.

- -- Through exploitation of software vulnerabilities[CVE-2022-26923].

Mitigation and Recommendations

- -- Use Robust Security Software: Ensure antivirus and anti-malware solutions are up to date.

- -- Regular Updates: Keep operating systems and applications updated to patch vulnerabilities.

- -- Safe Practices: Be cautious of phishing emails, and avoid downloading or opening files from untrusted sources.

- -- Network Monitoring: Monitor network traffic for unusual patterns that might indicate a SOCKS proxy or other malicious activity.

- -- 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.

Annexure

(CERTIn-Threat Intelligence ID- CMTX-P0820240007)

Indicators of Compromise (IOCs):

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

IP Addresses:

45.155.249.97

195.2.70.38

77.238.250.123

217.15.175.191

77.238.229.63

191.142.74.28

77.238.224.56

37.221.126.202

77.238.245.233

91.196.70.160

91.142.74.28

Domains:

richardflorespoew.shop

feighminoritsjda.shop

justifycanddidatewd.shop

strwawrunnygjwu.shop

falseaudiencekd.shop

pleasurenarrowsdla.shop

raiseboltskdlwpow.shop

marathonbeedksow.shop

halagifts.com

spamicrosoft.com

preservedmoment.com

HASHES:

9ed2b4d88b263f5078003ef35654ed5c205ac2f2c0e9225d4cdb4c24a5ea9af2

949faad2c2401eb854b9c32a6bb6e514ad075e5cbe96154c172f5f6628af43ed

d512bf205fb9d1c429a7f11f3b720c74680ea88b62dda83372be8f0de1073a08

dc5c9310a2e6297caa4304002cdfb6fbf7d6384ddbd58574f77a411f936fab0b

9dc809b2e5fbf38fa01530609ca7b608e2e61bd713145f84cf22c68809aec372

fcf59559731574c845e42cd414359067e73fca108878af3ace99df779d48cbc3

cb03b206d63be966ddffa7a2115ea99f9fec50d351dce03dff1240bb073b5b50

ab1f101f6cd7c0cffc65df720b92bc8272f82a1e13f207dff21caaff7675029f

ac22ab152ed2e4e7b4cd1fc3025b58cbcd8d3d3ae3dbc447223dd4eabb17c45c

fb4fa180a0eee68c06c85e1e755f423a64aa92a3ec6cf76912606ac253973506

cff5c6694d8925a12ce13a85e969bd468e28313af2fb46797bdcf77092012732

b92cf617a952f0dd2c011d30d8532d895c0cfbfd9556f7595f5b220e99d14d64

ed062c189419bca7d8c816bcdb1a150c7ca7dd1ad6e30e1f46fae0c10ab062ef

ce1f44a677d9b7d1d62373175f5583d9e8c04e16ebd94656e21aa296e00e93d7

ccaa8c8b39cb4a4de4944200936bcd4796367c16421a89e6a7d5476ae2da78cd

7d96ec8b72015515c4e0b5a1ae6c799801cf7b86861ade0298a372c7ced5fd93

24b6ddd3028c28d0a13da0354333d19cbc8fd12d4351f083c8cb3a93ec3ae793

ab3daec39332ddeeba64a2f1916e6336a36ffcc751554954511121bd699b0caa

9c1e0c8c5b9b9fe9d0aa533fb7d9d1b57db98fd70c4f66a26a3ed9e06ac132a7

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

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

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

Common Features of SideCopy Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

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

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

157.173.198.190

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

1. **CMTX-P082024095: QWERTY INFO STEALER**

Threat Campaign:QWERTY Information Stealer

QWERTY is an information-stealing malware that primarily targets sensitive data including network adapter information, system usernames, telemetry data, and sensitive browser data like browser history etc. Other capabilities include downloading additional payloads from its command-and-control (C2) server, indexes all files in the system, and uploads them to the C2 server via HTTP POST requests.The malware uses the keyword ‘qwerty’ in HTTP calls during exfiltration. The QWERTY Info Stealer malware replicates itself across various directories.

Threat Type: Info Stealware

Severity: High

Impacts:

1.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.

2. Personal data Loss.

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

Distribution Methods: The malware is often spread through phishing emails, malicious attachments, or compromised websites, making it crucial for users to be cautious with unknown sources.

Mitigation and Recommendations:

1. Security Software:Utilize and keep your antivirus and anti-malware tools up-to-date. These solutions help detect and block malwares.

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.

7. Ensure to scan all software downloaded from the Internet prior to executing. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).Before entering sensitive information on a website, check the URL for inconsistencies or suspicious elements. Ensure it uses HTTPS and matches the official domain.

8. 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].

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P082024095]

Indicators of Compromise (IOCs)

DOMAIN:

hxxp://mailservicess.com

HASHES:

e70f64a374e1784942c771940f07f08cdee78144f2135bf1665557d1fcee0f16

2d40e892e059850ba708f8092523efeede759ecd6e52d8cb7752462fcdb6f715

1. **CMTX-P082024104: Beavertail Malware Campaign**

Threat Overview

1. Threat Campaign: Beavertail Malware Campaign

BeaverTail, which is an information stealer and loader associated with North Korean hackers (DPRK) initially targeted macOS systems has expanded its reach to Windows systems. The malware's core functionality includes collecting sensitive information and executing another tool called InvisibleFerret. The delivery method for macOS systems involves the threat actors posing as job recruiters and directing victims to download a malicious file from a cloned version of a legitimate site. As for Windows systems, the specific initial access method is not known.

Impacts:

– Steal Sensitive Information

– Financial loss

2. Threat Type: Information Stealer and Loader

3. Severity: High

Capabilities:

– Exfiltrates victim’s keychain data

– Gathers data from browser directories

– Collects information related to cryptocurrency wallet browser extensions

– Sends exfiltrated data to the command-and-control (C2) server

– Downloads additional payloads from the C2 server

– Retrieves and executes additional malicious Python scripts

– Reads files and attempts to execute various functions related to data exfiltration and payload download

Distribution Methods

• Phishing campaigns to deceive the victim into downloading and installed an infected version of legitimate application to deliver BeaverTail Malware.

Mitigation and Recommendations

– Use Robust Security Software: Ensure antivirus and anti-malware solutions are up to date. Keep operating systems and applications updated to patch vulnerabilities.

– Safe Practices: Be cautious of phishing emails, and avoid downloading or opening files from untrusted sources. 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 Monitoring: Monitor network traffic for unusual patterns that might indicate a sign of compromise or other malicious activity.

– 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.

– Regular Audit: - Organizations should conduct a periodic security assessment, hardening, and architecture review of critical assets exposed over the Internet.

– Least Privilege: - Security administrators should apply the Principle of Least Privilege to all systems and services.

Response Actions:

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

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

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

Annexure

(CERTIn-Threat Intelligence ID- CMTX-P082024104)

Indicators of Compromise (IOCs):

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

IP Addresses:

95.164.17.24

URL

hxxp://185.235.241.208:1224

HASHES:

9abf6b93eafb797a3556bea1fe8a3b7311d2864d5a9a3687fce84bc1ec4a428c

0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132

09a508e99b905330a3ebb7682c0dd5712e8eaa01a154b45a861ca12b6af29f86

0ce264819c7af1c485878ce795fd4727952157af7ffdea5f78bfd5b9d7806db1

104926c2c937b4597ea3493bccb7683ae812ef3c62c93a8fb008cfd64e05df59

1123fea9d3a52989ec34041f791045c216d19db69d71e62aa6b24a22d3278ef9

121ca625f582add0527f888bb84b31920183e78c7476228091ff2199ec5d796b

12c0f44a931b9d0d74a2892565363bedfa13bec8e48ff5cd2352dec968f407ee

1b21556fc8ecb9f8169ba0482de857b1f8a5cb120b2f1ac7729febe76f1eea83

1c905fa3a108f4c9bc0578882ce7af9682760b80af5232f130aa4f6463156b25

1f9169492d18bffacebe951a22495d5dec81f35b0929da7783b5f094efef7b48

2618a067e976f35f65aee95fecc9a8f52abea2fffd01e001f9865850435694cf

40645f9052e03fed3a33a7e0f58bc2c263eeae02cbc855b9308511f5dc134797

41a912d72ba9d5db95094be333f79b60cae943a2bd113e20cc171f86ebcb86cf

4c465e6c8f43f7d13a1b887ff26d9a30f77cf65dd3b6f2e9f7fe36c8b6e83003

4c605c6ef280b4ed5657fe97ba5b6106b10c4de02a40ae8c8907683129156efd

592769457001374fac7a44379282ddf28c2219020c88150e32853f7517896c34

61dff5cbad45b4fe0852ac95b96b62918742b9c90dd47c672cbe0d1dafccb6c5

6465f7ddc9cf8ab6714cbbd49e1fd472e19818a0babbaf3764e96552e179c9af

6b3fce8f2dad7e803418edd8dfc807b0252705c11ec77114498b01766102e849

700a582408cbda7ee79723b3969b8d10d67871ea31bb17c8ca3c0d94b481aa8c

709820850127201a17caab273e01bb36ce185b4c4f68cd1099110bb193c84c42

72ebfe69c69d2dd173bb92013ab44d895a3367f91f09e3f8d18acab44e37b26d

75f9f99295f86de85a8a2e4d73ed569bdb14a56a33d8240c72084f11752b207e

785f65f1853a08b0e86db5638fbd76e8cad5fe1359655716166a76035261c0be

7b718a46ae4de09ed4f2513df6e989afe1fbb1a0f59511a4689fac5e1745547d

7f8bb754f84a06b3e3617dd1138f07a918d11717cc63acaef8eb5c6d10101377

845d7978682fa19161281a35b62f4c447c477082a765d6fedb219877d0c90f31

9867f99a66e64f6bce0cfca18b124194a683b8e4cb0ced44f7cb09386e1b528d

9ae24a1912e4b0bab76ae97484b62ea22bdc27b7ea3e6472f18bf04ca66c87de

a2f8de3c5f5f6ecbf29c15afd43a7c13a5bf60023ecb371d39bcca6ceef1d2b7

b5f151f0a4288e148fd10e19c78399f5b7bdff2ad66940fadd20d6eae4b7518b

b833f40b2f3439f317cf95980b29bddd2245d2acc2d5c11e9690dd2fa4289585

c8c11f9b308ea5983eebd8a414684021cc4cc1f67e7398ff967a18ae202fb457

ceb59dbaf58a8de02f9d5e9b497321db0a19b7db4affd5b8d1a7e40d62775f96

d8f065d264b1112d6ee3cf34979289e89d9dcb30d2a3bd78cc797a81d3d56f56

db6e75987cabdbfc21d0fdcb1cdae9887c492cab2b2ff1e529601a34a2abfd99

de42155e14a3c9c4d919316d6ba830229533de5063fcd110f53e2395ef3aa77a

e2a940c7d19409e960427749519dc02293abe58a1bef78404a8390f818e40d08

fc9bb03998a89524ce5a0f859feb45806983aa4feb5f4d436107198ca869ff6f

ff620bd560485c13a58a0de941bd3e52943036e6a05306e928f7c626998822fb

da6d9c837c7c2531f0dbb7ce92bfceba4a9979953b6d49ed0862551d4b465adc

2d8a5b637a95de3b709780898b7c3957f93d72806e87302f50c40fe850471a44

C5a73896dc628c23a0b6210f50019445e2b8bfc9770f4c81e1fed097f02dfade

fd9e8fcc5bda88870b12b47cbb1cc8775ccff285f980c4a2b683463b26e36bf0

d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6

36cac29ff3c503c2123514ea903836d5ad81067508a8e16f7947e3e675a08670

0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd

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

1. **CMTX-P-5870820249: Threat Actor Group-110 (TAG 110) Recent IOCs**

Threat actor groups TAG 110/UAC 0063, linked to Russia-aligned threat activity group, are conducting cyber espionage campaigns against government institutions, research facilities, and critical infrastructure. These groups employ spear-phishing, exploit software vulnerabilities, and deploy Hatvibe and Cherryspy malware to infiltrate systems and exfiltrate sensitive data.

Common Features of 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

Defense Evasion: Encrypted/Encoded File

Distribution Methods:

Spear phishing

Exploit Public-Facing Application

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

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

enrollmentdm.com

errorreporting.net

experience-improvement.com

game-wins.com

internalsecurity.us

lanmangraphics.com

retaildemo.info

shared-rss.info

telemetry-network.com

tieringservice.com

trust-certificate.net

5.45.70.178

45.136.198.18

45.136.198.184

45.136.198.189

46.183.219.228

84.32.188.23

185.62.56.47

185.158.248.198

185.167.63.42

194.31.55.131

212.224.86.69

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

1. **CMTX-I-445082024: CrimsonRAT Malware C&C IP**

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

Common Features of APT36 Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

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

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

138.201.245.101

37.60.236.186

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

1. **CMTX-P082024115: CVE-2024-38193**

ALERT BRIEF:

According to various reports, threat actors like the Lazarus Group has been actively exploiting the zero day vulnerability tracked as CVE-2024-38193. The vulnerability is still being exploited and is affecting the Microsoft Windows system specifically the Ancillary Function Driver for WinSock (Windows 10 & 11 and Windows server 2012 & above). As demonstrated by recent events involving North Korean hackers, the exploitation of this vulnerability could result in privilege escalation and the distribution of rootkits by threat actors. Recently while exploiting CVE-2024-38193, the Lazarus threat actors have used the Fudmodule malware to evade detection and targeted the cryptocurrency and aviation sectors. Some other associated malwares used are DarkMe, Ransom X, and DarkGate.

FUDMODULE- FudModule is a rootkit which is used by the state-sponsored hacking group from North Korea, "Lazarus Group". The rootkit has an ability to integrate with other malwares such as the Kaolin RAT. It enables the attackers to gain kernel-level access to Windows machines and disable security software. Earlier also it has exploited vulnerabilities like CVE-2024-38193 etc.

DARKME- The DarkMe malware is a RAT that is used by the APT group Water Hydra also known as DarkCasino. It collects system information, registers with a C2 server, and can perform actions such as data exfiltration and remote control.  DarkMe's technical behavior includes packet structure, DLL loader characteristics, and payload assembly process.

DARKGATE- This malware has capabilities of RAT and acts as Malware-as-a-service (MaaS) and is distributed through various methods like phishing emails,fake software installers and "ClickFix" for malware delivery .It has been observed using different scripting interpreters, such as AutoIt and AutoHotKey, in its infection chain to evade detection.

Threat Type: Vulnerability

CVSS Score: 7.8

Severity: High

Mitigation and Recommendations

1. Apply Security Patches: Vendors often release security patches specifically addressing vulnerabilities. Regularly check for and apply these patches to minimize risk.

2. Update Software: Ensure that all affected softwares are updated to the latest version provided by the vendor. Vulnerability fixes are typically included in updates or patches.

3. Review and Harden Configurations: Review the configuration settings of the affected software or system. Apply security best practices and harden configurations to reduce exposure to exploitation.

4. Principle of Least Privilege: Limit user and application permissions to the minimum necessary to reduce potential attack vectors.

5. Monitor for Suspicious Activity: Implement monitoring solutions to detect unusual or unauthorized activities, especially those attempting to escalate privileges.

6. Regular Updates: Keep your systems and software up to date with the latest security patches and updates.

7. Network Segmentation: Segment your network to limit the spread of malware and reduce the impact of a potential breach.

8. Backup: Regularly back up important data and system configurations. This will help in recovery if an exploitation incident occurs.

9. 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.

1. **CMTX-I-587082024: Suspicious Domains used by Threat Actors**

The following domains are suspicious and may possibly be used for malicious purposes, such as spear-phishing websites/ hosting malware/ sending spear-phishing emails. Network administrators may kindly monitor these domains in their network.

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

api.embassyofindiaukraine.in

app.embassyofindiaukraine.in

demo.embassyofindiaukraine.in

gov.embassyofindiaukraine.in

gov.in.inwww.embassyofindiaukraine.in

gov.inwww.embassyofindiaukraine.in

gov.www.embassyofindiaukraine.in

in.inwww.embassyofindiaukraine.in

inwww.embassyofindiaukraine.in

mea.gov.embassyofindiaukraine.in

mea.gov.inwww.embassyofindiaukraine.in

mea.gov.www.embassyofindiaukraine.in

nktofimv.embassyofindiaukraine.in

staging.embassyofindiaukraine.in

usawww.embassyofindiaukraine.in

vtbicmqj.embassyofindiaukraine.in

certin.attendence.in

www.admin.embassyofindiaukraine.in

www.backend.embassyofindiaukraine.in

www.gov.embassyofindiaukraine.in

www.gov.in.inwww.embassyofindiaukraine.in

www.gov.www.embassyofindiaukraine.in

www.in.inwww.embassyofindiaukraine.in

www.inwww.embassyofindiaukraine.in

www.mea.gov.embassyofindiaukraine.in

www.mea.gov.inwww.embassyofindiaukraine.in

www.mea.gov.www.embassyofindiaukraine.in

www.cert-inempanelled.com

www.ecloudgov.info

\*.embassyofindiaukraine.in

\*.ecloudgov.info

\*.attendence.in

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

1. **CMTX-I-765082024: Malicious Domain used by Pakistan based 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 for additional layer of security  
  
- ----------< Malicious Domain>---------  
mail-sec.in      
- ----------</Malicious Domain>---------

1. **CMTX-P082024956: Styx Stealer**

Styx Stealer, a successor to the older Phemedrone Stealer, has emerged as a powerful information-stealing malware. It can extract browser data, cryptocurrency wallet details, and instant messenger conversations from platforms like Telegram and Discord. Styx Stealer boasts several advanced features, including auto-start functionality, clipboard monitoring, cryptocurrency wallet clipping, improved anti-analysis techniques, and the capability to transmit data via Telegram.

Threat Type: Infostealer

Severity: High

Impacts:

1.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.

2. Personal data Loss.

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

Distribution Method: Spread through spearphishing emails

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 store securely 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.

• Response Actions:

- - --- 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.

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

- - --- Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts, particularly for webmail, virtual private networks, and accounts that access critical systems to add an additional layer of security

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

1. **CMTX-I-995082024: Malicious/ Suspicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

exciselicense-gov.info

epfogov.in

indianrailgov.in

jkpolice.gov.in.casereports.nl

ep-gov.info

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

1. **CMTX-P-082024114: RedJuliett Threat Actor Campaign**

Flax Typhoon, also known as Ethereal Panda or RedJuliett, is a Chinese state-sponsored cyber espionage group that employs living-off-the-land binaries (LOLBins) and legitimate tools like China Chopper and SoftEther VPN to establish and maintain persistent access to compromised networks while minimizing the use of malware. The group has utilized the Acunetix web vulnerability scanner for detecting the vulnerable applications of victim and the open-source tool SQLMap to perform SQL injection. After gaining initial access, the group  exploited the  privilege vulnerability (CVE-2016-5195) for lateral movement and deployed open-source web shells such as devilzShell and AntSword.

Impacts: Information gathering and exploitation

Severity: High

Mitigation and Recommendations

Preventive Measures:

Patch vulnerable application: - As attacker target the vulnerable Public facing devices and applications, it is advised for routine vulnerability patching to add extra layer of defense.

Detection Techniques:

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

The threat actor has been using VPN nodes to route their traffic, which can mask their true origin and complicate efforts to trace their activities. By closely monitoring these VPN connections, you can identify unusual patterns or anomalies that may signal malicious behavior, helping to detect and address the threat actor's activities before they escalate.

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

CERTIn-Threat Intelligence ID- [CMTX-P-082024114]

Indicators of Compromise (IOCs):

IP Addresses

120.53.104.31

101.43.38.242

176.119.150.92

103.149.48.189

154.197.99.11

45.77.42.65

108.61.181.104

Domain

cktime.ooguy.com

asljkdqhkhasdq.softether.net

vpn472462384.softether.net

www.sofeter.ml

vpn437972693.sedns.cn

www.dns361.tk

eec2.test.thinkyes.tw

HASH

5437d0195c31bf7cedc9d90b8cb0074272bc55df

0cc0ba859981e0c8142a4877f3af99d98dc0b707

cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1

2c95b971aa47dc4d94a3c52db74a3de11d9ba658

7992c0a816246b287d991c4ecf68f2d32e4bca18

9f01fc7cad8cdd8d934e2d2f033d7199a5e96e4a

1. **CMTX-P-082024125: STORMBAMBOO THREAT ACTOR CAMPAIGN**

Threat Overview

Threat Campaign: STORMBAMBOO THREAT ACTOR

A Chinese state-sponsored Advanced Persistent Threat (APT) group, "STORMBAMBOO" (aka Evasive Panda and Daggerfly) is known for its sophisticated cyber-espionage operations. It uses many techniques to deliver malware in infected systems, out of which one is DNS poisoning, which spreads malware via insecure software update mechanisms. The Threat actor group has the capability to compromise systems across Windows, macOS, Linux, and Android platforms since it includes variants like Macma (a macOS backdoor), Nightdoor (a new addition to the MgBot framework) and  MgBot (also known as POCOSTICK).

Two of the many techniques used by Stormbamboo is "watering hole attacks" and "supply chain attacks" to compromise websites and infilterate organizations via compromised Internet Service Providers (ISPs) respectively.

Another technique for obfuscating malicious activities is C2 (command and control) communication via TCP or OneDrive.

MACMA-MacMa is a macOS-based backdoor malware attributed to the cyber-espionage group Daggerfly/StormBamboo. It utilizes the info tool to collect system information, including hardware UUID, serial number, macOS version, current privileges and screen capture resizing and improved logging.

NIGHTDOOR- The Nightdoor malware, also referred to as NetMM and Suzafk is primarily used by chinese espionage group "stormbamboo". It can leverage malicious downloaders on both Windows and macOS platforms to deploy itself alongside another backdoor named MgBot.This malware gains initial access through trojanized installers disguised as legitimate software, specifically named "certificate.exe" for Windows and "certificate.pkg" for macOS.

MgBot-MgBot is a backdoor, which is also known as EggRoll,that hijacks a normal service  and masquerades as that service's DLL. A separate dropper starts the service and loads and executes malware in the context of svchost.exe. EGGROLL is capable of creating and deleting files, taking screenshots, obtaining the drive type and free space on disk. It also injects code into Explorer.exe and can run simultaneously as DLLs launched by rundll32.exe

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.

3. Increased Security Costs: To defend against sophisticated APT threats, enterprises often need to invest heavily in advanced security measures, including threat detection systems, incident response capabilities, and regular security assessments.

4. 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.

5. Strategic Disruption: In some cases, the exposure of strategic plans or sensitive negotiations can disrupt business strategies, partnerships, or market positioning

Threat Type: Nation State Sponsored APT group

Severity: High

Distribution Methods: The group has been observed using spearphishing as an initial attack vector to deploy various malware in infected machines.

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-082024125

Indicators of Compromise (IOCs):

IPs

158.247.214.28

210.16.188.116

114.64.255.138

103.96.129.32

103.96.128.22

103.96.130.102

103.96.128.198

103.96.130.86

188.116.22.44

116.255.137.251

103.96.128.8

45.125.67.220

103.96.130.103

103.253.43.195

103.96.131.146

114.64.255.176

103.253.43.167

91.242.241.188

38.180.94.244

139.84.175.17

103.96.128.9

139.84.168.41

103.96.130.104

103.96.128.135

45.125.67.201

45.125.67.223

103.96.128.11

103.96.128.15

118.123.1.155

188.208.141.172

114.64.255.171

139.84.167.197

103.96.129.223

45.125.67.166

103.96.128.14

HASHES

ee28b3137d65d74c0234eea35fa536af

ce5fdde7db4ee41808f9c7d121311f78

acfc69c743b733dd80c1d551ae01172b

6abf9a7926415dc00bcb482456cc9467

4c8a326899272d2fe30e818181f6f67f

4958ede3b968ad464c983054479bf4d2

2a6c10a34fa1e2a38673f4ca20c303a1

25e4eef79ad4126d5dc5567949848070

049e8677406de5f0061f3960f9655b5f

1. **CMTX-P082024108: Critical Alert: REDLINESTEALER Malware Campaign**

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-P082024108)

Indicators of Compromise (IOCs):

IP Addresses

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

185.196.9.26

185.215.113.22

20.52.165.210

185.215.113.67

89.23.101.114

45.66.231.214

147.45.44.56

147.45.44.16

91.92.249.167

89.23.97.185

88.99.151.68

77.105.164.59

207.148.69.28

147.45.44.139

5.189.138.247

185.215.113.25

5.42.92.213

178.23.190.118

176.111.174.140

103.249.201.12

91.92.240.171

45.140.147.183

38.180.147.152

95.217.124.248

65.108.21.23

94.131.106.53

31.177.108.40

91.92.242.175

51.89.205.200

185.215.113.9

52.143.157.240

51.195.145.80

23.41.187.30

147.45.47.36

5.42.92.213

135.181.10.210

178.63.237.121

103.211.207.57

91.92.248.194

193.233.255.34

45.9.91.71

194.163.130.75

1. **CMTX-P-082024135 : 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.

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.

13. 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].

14. Ensure to scan all software downloaded from the Internet prior to executing. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).Before entering sensitive information on a website, check the URL for inconsistencies or suspicious elements. Ensure it uses HTTPS and matches the official domain.

15. Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent to prevent e-mail spoofing. This will prevent malicious mails to reach your corporate mailboxes. Always verify the sender's email address and domain. Be cautious of emails from unfamiliar or suspicious addresses.

16.Regularly monitor all  outbound traffic, particularly traffic destined for newly registered domains or Dynamic DNS (DDNS) and Domain Generation Algorithms (DGA) domains.

17. 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-082024135

Indicators of Compromise (IOCs):

IP Addresses:

103.238.227.183

18.141.169.162

103.238.225.248

45.133.239.200

52.35.227.119

101.36.106.114

118.194.239.90

118.193.35.61

216.238.113.209

43.246.208.107

118.107.44.134

118.107.44.132

118.107.44.133

107.173.63.250

54.209.202.56

103.215.78.57

109.104.155.162

54.193.45.167

1. **CMTX-P-082024145: SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multimodular backdoor

3. Severity: High

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-0820240404

Indicators of Compromise (IOCs):

IP Addresses

103.238.227.183

134.122.189.25

45.77.133.154

95.179.235.165

198.13.51.5

167.179.106.174

8.210.167.64

38.180.35.224

45.77.170.31

8.217.84.192

103.85.25.166

199.247.23.228

103.27.109.206

149.28.146.215

47.242.52.22

154.31.217.197

8.218.193.197

38.6.193.22

202.61.87.139

202.182.118.85

143.244.138.90

1. **CMTX-I-680082024: CrimsonRAT- APT36 campaign**

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

Common Features of APT36 Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

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

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

96.47.232.202

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

1. **CMTX-I-636082024: Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

epgov.info

jharkhandmailgov.info

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

1. **CMTX-I-179082024: CrimsonRAT- APT36 campaign**

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

Common Features of APT36 Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

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

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

newpdfngos.xyz

79.143.190.33

online-mall.net

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

Network administrators may take required action against the above IOCs.

1. **CMTX-I-432082024: 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>-----------

194.195.87.110

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

1. **CMTX-P-082024155: VELVETSHELL MALWARE**

Threat Overview

Threat Campaign: VELVET SHELL

VelvetShell is a malware which is a hybrid customized version of two open-source tools namely "TinyShell" (a Unix backdoor) and "3proxy" (a proxy tool). The malware is used by a Chinese APT group called "Velvet Ant". Once the malware is deployed, it enables remote access, file uploads, and further code execution while evading detection by standard security tools.

The malware has exploited a zero-day vulnerability (CVE-2024-20399) in Cisco switches to deploy custom malware, gaining deep control over compromised systems for both data exfiltration and persistent access. It also allowed attackers with valid admin credentials to escape the NX-OS command line interface and execute commands on the underlying Linux operating system. Before deploying VELVETSHELL by injecting a malicious library into legitimate processes, the "Velvet Ant" APT group conducts reconnaissance through extended ping commands and network path mapping.

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.

Threat Type: Malware

Severity: High

Mitigation and Recommendations:

1.Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

2.Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

3.Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

4.Regular Password Resets: Implement a process for regular password resets enterprise-wide. This practice ensures that passwords are updated periodically, reducing the likelihood of compromised credentials remaining in use for extended periods.

5.Deploy Robust Anti-Malware and Virus Software: Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software. Regularly update this software to protect against the latest threats. Effective anti-malware solutions can detect and block infostealers and other malicious software that attempts to install or execute on a device.

6.Block Malicious Sites and Links: Configure your anti-malware and antivirus software to prevent access to websites and online resources that are known to distribute malicious links or attachments. This proactive approach helps to safeguard users from inadvertently visiting harmful sites that could compromise device security.

7. Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for known VelvetShell malware.

8. By enhancing logging, implementing continuous monitoring, and conducting systematic threat hunts on key organizational choke points, organizations can better detect and counteract advanced persistent threats such as ‘Velvet Ant’.

9. Restrict outbound internet access for devices: To minimize the risk of switches being exploited by external threats or communicating with malicious actors, restrict their ability to initiate outbound connections to the internet. Implement stringent firewall rules and access control lists (ACLs) to ensure that only essential traffic is permitted, thereby strengthening the security of your network infrastructure.

10. Consistently review and apply patches to all network devices to address newly identified vulnerabilities, such as CVE-2024-20399, and minimize the risk of exploitation. Use automated tools like vulnerability scanners to detect and prioritize vulnerabilities in network equipment.

Monitoring and Detection:

1. Enable Syslog on All Switches: Configure all network switches to send log data to a centralized Syslog server. Cisco switches offer various logging levels for different modules. By default, they only log failed authentication attempts. To also capture successful authentication attempts, consider setting the AUTHPRIV level to 6.

2.Set Up SIEM Integration: Link switch logs with a Security Information and Event Management (SIEM) system to correlate events and detect anomalies.

3.Configure Alerts: Leverage syslog data to establish alerts for detecting suspicious activities. For example, set up alerts for SSH connections originating from unauthorized jump hosts and for SSH connections made from network equipment.

Annexure

Previous Alert Reference : [CMTX-P062024065] Velvet ant Threat Actor, TLP: CLEAR, Dated :19/06/2024

CERTIn-Threat Intelligence ID- [CMTX-P-082024155]

Indicators of Compromise (IOCs):

IPs:

202.61.136.158

103.138.13.31

HASHES:

d663b323d132a3c811bb53a48a686ea85c6bf8faeef3b48dfa93528be8f4133b

9a7a24b1c785b3c7c39f7e33e99897290165693dea1f46ed4f3c7919aef93928

75fa71e65344b61a80f0e598349b735912be39d04a7e2159748423bd860d3454

be852d7a59ba168d93eb975fbed652617046433e6fdc177d0087331f9a095f02

0acc25396ef78c00631c64df538678a323982115bafbfa7487a4370d4b4129ac

859c823eb3e7420e0db234ba224764faa62d391bddd25e9ad415b11d853741f9

9b9d2da73b510276d38d1698f3b87671958e338b40230e6a004ccaf3dcceb03b

b4d71b0ac0bc1495789501f9afce6f950b601a36c0836534294640f2db6b2f40

3a6a5b1d76dfcac5920e6e9163c08543304ba013425eb2c2e64071b15d26996e

bdf8a8c7f0298484dc95895dbddf367689ca361618453597129343838b94debb

7c9336afd7530576b6a0f2e978b36955e8f264fee429d810309ce157a4918aaa

c456747731141c2ea0f8e69f89193e8bb823da4667527fe90b614b97f1d425ae

55d6c4a95b5172ea47381ab66ea9ea37fa0afb53b9bb10a1d752ac4acc8f6cd4

527df166af23cd0d139ebad9d219f125137b5a7b619fa50e5e245ccaf8c0b7d6

4965f809b71ffb71fe8456d88dcd0a80a99fa6aa4ffd6ba96e1a1d810d41bbd0

b5aa86fd97624a317945d110541a07fc80b83dd960fbf16642720fc275d8f04f

9092cdd52109531f9f58c28bda25b0c3f82d9bd2d261ce5fcb0137873dbb0868

bcbc3184756a6cacfd5ca2b879708cfd015e84050c9b9ede096cfb70282f870c

febe116a87860e42bbcfd7c6e2c710446f33bdacc56e990f69493837c01f1059

7e118a6c4d6f162d8c6a53faf972bd3e675da7f9d0a0b67a1988b4e2102ebb53

cc48a02f06066a37c90d063b6d28ae17d9503e4ba6df69aef1b55b5fa5a5ff48

562974ea1325a88c916a55719fb9263eb6c710ba281fdee4ba7e9a98a3f4a5a8

92b2535373e55b16b6f3b2d134a1d5545e837d3c19fff4cead4e92558e302b6e

a9556cc05422cae960e36f76eeff7168b8e3cfeb16a20855a93d4f2ed4a65a8b

821d0cdc3e8a735976045ecb1afd1c0170bf39701d2da118b9533a45383a9ebe

436f35dc69bbe7cb8cf5430b52c3aedace099730245de57e004dc1f6531ae262

13f3c05cc348ecb47c4e86d1fb522fdf499a6fb23e0cc6370f4618137f055b04

3d9aaac0a8e5c7eadd79d8d5c16119d04f4e9db7107fc44a1e32a8746a1ec375

1. **CMTX-P082024834: MoonPeak Malware Campaign**

1. Threat Campaign: MoonPeak Malware Campaign

MoonPeak, a variant of the open-source remote access Trojan (RAT) XenoRAT, is utilized by the North Korean threat group known as UAT-5394. This campaign involves a PowerShell script that downloads a malicious RTF file from a remote host. The script alters the RTF file's header to transform it into a GZIP file containing the MoonPeak malware, which is then executed. Once executed, MoonPeak establishes communication with a command-and-control (C2) server to receive further instructions and carry out malicious activities on the victim's machine.

Impacts:

– Steal Sensitive Information

– Provide remote access of machine

2. Threat Type: Remote Access Trojan

3. Severity: High

Capabilities:

– Conducts API hooking and reflective portable executable (PE) injection

– Retrieves the system language and the machine’s geolocation using the Windows registry

– Detects debuggers

– Delays execution using the Sleep API function for evasion

– Performs self-deletion

– Retrieves the username of the currently logged-in user

– Retrieves system information

– Detects virtual machine (VM) environments by checking for VM-related strings in memory

– Terminates running processes

– Delays execution using the Sleep API function for evasion

Distribution Methods:

Spear-phishing campaign

Mitigation and Recommendations

– Be cautious of phishing emails, and avoid downloading or opening files from untrusted sources. 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.

– Restrict execution of PowerShell /WSCRIPT in enterprise environment. Ensure installation and use of latest version of PowerShell, with enhanced logging enabled. Script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

– Network Monitoring: Monitor network traffic for unusual patterns that might indicate a sign of compromise or other malicious activity.

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

– Deploy Robust Anti-Malware and Virus Software: Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software. Regularly update this software to protect against the latest threats. Effective anti-malware solutions can detect and block malicious software that attempts to install or execute on a device.

– Block Malicious Sites and Links: Configure your anti-malware and antivirus software to prevent access to websites and online resources that are known to distribute malicious links or attachments. This proactive approach helps to safeguard users from inadvertently visiting harmful sites that could compromise device security.

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

Response Actions:

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

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

Annexure

(CERTIn-Threat Intelligence ID- CMTX-P082024834)

Indicators of Compromise (IOCs):

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

IP Addresses:

167.88.173.173

95.164.86.148

80.71.157.55

84.247.179.77

45.87.153.79

45.95.11.52

104.194.152.251

27.255.81.118

212.224.107.244

27.255.80.162

210.92.18.169

91.194.161.109

HASH

0b8897103135d92b89a83093f00d1da845a1eae63da7b57f638bab48a779808e

2b35ef3080dcc13e2d907f681443f3fc3eda832ae66b0458ca5c97050f849306

4108c5096a62c0a6664eed781c39bb042eb0adf166fcc5d64d7c89139d525d4f

44e492d5b9c48c1df7ef5e0fe9a732f271234219d8377cf909a431a386759555

4599a9421e83fb0e2c005e5d9ac171305192beabe965f3385accaf2647be3e8e

58fdc1b6ce4744d6331f8e2efc4652d754e803cae4cc16101fc78438184995e6

97ba8d30cf8393c39f61f7e63266914ecafd07bd49911370afb866399446f37d

a80a35649f638049244a06dd4fb6eca4de0757ef566bfbe1affe1c8bf1d96b04

b8233fe9e903ca08b9b1836fe6197e7d3e98e36b13815d8662de09832367a98a

f4aa4c6942a87087530494cba770a1dcbc263514d874f12ba93a64b1edbae21c

facf3b40a2b99cc15eee7b7aee3b36a57f0951cda45931fcde311c0cc21cdc71

0ed643a30a82daacecfec946031143b962f693104bcb7087ec6bda09ade0f3cb

41d4f7734fbf14ebcdf63f51093718fd5a22ec38a297c0dc3d7704a3fb48b3f9

6a3839788c0dafe591718a3fb6316d12ccd8e82dbcb41ce40e66b743f2dd344d

148c69a7a1e06dc06e52db5c3f5895de6adc3d79498bc3ccc2cbd8fdf28b2070

1ad43ddfce147c1ec71b37011d522c11999a974811fead11fee6761ceb920b10

458641936e2b41c425161a9b892d2aa08d1de2bc0db446f214b5f87a6a506432

8a4fbcdec5c08e6324e3142f8b8c41da5b8e714b9398c425c47189f17a51d07b

293b1a7e923be0f554ec44c87c0981c9b5cf0f20c3ad89d767f366afb0c1f24a

6bf8a19deb443bde013678f3ff83ab9db4ddc47838cd9d00935888e00b30cee6

72a25d959d12e3efe9604aee4b1e7e4db1ef590848d207007419838ddbad5e3f

15eee641978ac318dabc397d9c39fb4cb8e1a854883d8c2401f6f04845a79b4b

3e39fc595db9db1706828b0791161440dc1571eaa07b523df9b721ad65e2369b

f928a0887cf3319a74c90c0bdf63b5f79710e9f9e2f769038ec9969fcc8ee329

27202534cc03a398308475146f6710b790aa31361931d4fe1b495c31c3ed54f7

DOMAINS

nsonlines.store

yoiroyse.store

pumaria.store

nmailhostserver.store

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

1. **CMTX-I-781082024: Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

cert-in.net

cert-in.info

cert-in.co

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

1. **CMTX-P082024976: 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 :

1.Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

2.Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

3.Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

4.Regular Password Resets: Implement a process for regular password resets enterprise-wide. This practice ensures that passwords are updated periodically, reducing the likelihood of compromised credentials remaining in use for extended periods.

5.Deploy Robust Anti-Malware and Virus Software: Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software. Regularly update this software to protect against the latest threats. Effective anti-malware solutions can detect and block infostealers and other malicious software that attempts to install or execute on a device.

6.Block Malicious Sites and Links: Configure your anti-malware and antivirus software to prevent access to websites and online resources that are known to distribute malicious links or attachments. This proactive approach helps to safeguard users from inadvertently visiting harmful sites that could compromise device security.

7. Disabling Credential Caching: As an additional security measure, disable the Windows operating system’s credential caching feature on devices where credentials are not necessary. This prevents the operating system from storing login information locally, reducing the risk of credential theft if a device is compromised.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024976

Indicators of Compromise (IOCs):

• IP ADDRESSES

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

146.70.113.183

187.212.230.171

47.236.182.237

116.97.240.228

204.12.245.100

185.196.11.85

126.221.213.41

76.71.94.235

82.157.51.56

81.68.190.186

167.86.115.184

14.35.42.91

176.31.92.202

181.161.30.246

181.162.184.197

123.113.8.123

200.106.116.97

95.214.27.173

172.10.234.10

191.17.96.243

121.169.59.210

188.55.200.160

83.168.110.21

5.182.205.114

83.229.69.9

172.86.110.12

163.5.160.202

176.126.113.158

104.237.252.41

136.244.118.208

141.134.11.187

181.162.135.102

193.233.74.21

216.224.126.132

216.224.126.168

223.155.16.167

223.155.16.181

223.155.16.191

41.216.183.228

45.138.16.215

47.109.27.54

62.60.210.205

72.77.89.178

87.89.82.13

91.92.254.28

92.40.112.165

93.86.35.172

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

1. **CMTX-P082024664: Ransom Hub Ransomware**

Ransom Hub Ransomware Group has gained significant prominence in the ransomware landscape since mid-2024, particularly following the takedown of major groups like Lock Bit and AlphV. This group has reportedly attacked organizations across various sectors, including healthcare, government, finance, and education. The group operates using a dual-extortion model like other ransomware groups e.g.; encrypting the system's files and exfiltrating the data to hold it for ransom. In previous campaign, attackers gained initial access by exploiting the Zero logon vulnerability (CVE-2020-1472), to gain domain administrator privileges and take control of the entire domain.

After that attacker used several dual-use tools for facilitate remote access, discover and retrieve information before deploying ransomware. Recently group has also introduced a new endpoint detection and response (EDR) disabling tool to evade detection during their attacks.

Impacts:

Personal Information Loss

The malware granting attackers control over the system

Financial loss and reputation damage

Threat Type: Ransomware

Severity: High

Mitigation and Recommendations:

Preventive Measures:

o Patch management: Regularly patch and update software and operating systems to the latest available versions.

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

o Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

o Regular Password Resets: Implement a process for regular password resets enterprise-wide. This practice ensures that passwords are updated periodically, reducing the likelihood of compromised credentials remaining in use for extended periods.

o 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.

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 address malware infections quickly and effectively and minimize damage.

Response Actions:

o 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.

o 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.

o Deploy Robust Anti-Malware and Virus Software: Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software. Regularly update this software to protect against the latest threats. Effective anti-malware solutions can detect and block info stealers and other malicious software that attempts to install or execute on a device.

o Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

o Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

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

o 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>

Annexure

CERTIn-Threat Intelligence ID- CMTX-P082024664

Indicators of Compromise (IOCs):

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

HASH

02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292

34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087

7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a

8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7

ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00

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

1. **CMTX-P082024165: ACTIVE EXPLOITATION OF PUBLIC FACING APPLICATION VULNERABILITIES BY IRANIAN THREAT ACTORS**

ALERT BRIEF:

According to various reports, Iran based threat actors are actively exploiting public facing application vulnerabilities to gain initial access to networks and deploy ransomware. They are affecting various products like Citrix Netscaler, F5 BIG-IP,Pulse Secure/Ivanti VPNs,PanOS Firewalls, Check Point Security Gateways etc. Some of the targeted vulnerabilities include:

1) Citrix Netscaler:

CVE-2019-19781(CVSS- 9.8): A path traversal vulnerability allowing unauthenticated attackers to access arbitrary files on the server.

CVE-2023-3519(CVSS-8.8): A vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway that could allow an unauthenticated attacker to execute arbitrary code.

Exploitation: Iranian actors have utilized these vulnerabilities to gain initial access to corporate environments, often leveraging compromised Citrix systems as a foothold for further attacks.

2) F5 BIG-IP:

CVE-2022-1388(CVSS-9.8): A critical vulnerability in the iControl REST API, which allows attackers to execute arbitrary commands with elevated privileges.

Exploitation: This vulnerability has been exploited to gain administrative access to affected systems, facilitating lateral movement and establishing persistence within networks.

3) Pulse Secure/Ivanti VPNs:

CVE-2024-21887( CVSS-9.1): A critical vulnerability in Pulse Secure VPN that allows unauthenticated attackers to execute commands and access sensitive data.

Exploitation: Attackers have used this vulnerability to bypass VPN protections, gaining unauthorized access to sensitive network segments and deploying ransomware.

4) PanOS Firewalls:

CVE-2024-3400(CVSS-10): A vulnerability in Palo Alto Networks' PanOS that allows attackers to execute arbitrary code with elevated privileges.

Exploitation: Exploited to bypass security controls and gain control over network firewalls, facilitating further attacks on internal systems.

5) Check Point Security Gateways:

CVE-2024-24919(CVSS-8.6): A vulnerability in Check Point’s security appliances that allows for unauthorized access and potential privilege escalation.

Exploitation: Used to compromise gateway appliances, which serve as entry points for ransomware deployment and network infiltration.

Threat Type: Vulnerability

Severity: High

Mitigation and Recommendations:

1) Patch and Update: Apply the latest security patches. Ensure that all systems, including Citrix Netscaler, F5 BIG-IP, Pulse Secure/Ivanti VPNs, PanOS firewalls, and Check Point Security Gateways, are updated to address these vulnerabilities.

(Please note that simply applying patches for the CVEs mentioned may not fully address the issue if your network was already compromised by these actors while the device was still vulnerable. It is highly recommended to conduct further investigation into the use of stolen credentials to detect any attempts by the threat actors to gain access to other parts of the network)

2) Network Segmentation: Implement network segmentation to limit the spread of an attack and contain potential breaches within isolated segments.

3) Monitor and Detect: Enhance monitoring and detection capabilities to identify suspicious activities and potential exploitations. Regularly review logs for unusual access patterns.

4) Access Controls: Enforce strict access controls and least privilege principles to minimize the risk of unauthorized access and exploitation.

5) Incident Response: Develop and test incident response plans to ensure preparedness for ransomware and other cyber attack scenarios.

6) Threat Intelligence: Stay informed about emerging threats and vulnerabilities. Engage with threat intelligence services to receive timely updates and actionable information

7) Multi-Factor Authentication (MFA):

Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

8). Backup: Regularly back up important data and system configurations. This will help in recovery if an exploitation incident occurs.

1. **CMTX-I-950082024: QuasarRAT- Deployed by Pakistan based Threat Actors**

Quasar is a fast and light-weight publicly available Windows remote administration tool coded in C#, often used by Pakistan based threat actors. Quasar RAT has capability of capturing screenshots, key logging, gather system information, remote shell and command execution. It has been observed that, it is deployed at a later stage in malware deployment.

Common Features of APT36 Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

Prevention Measures:

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

    Monitoring and logging to detect unusual activities indicating a compromise

    Multi-Factor Authentication (MFA) for emails

    Encrypt sensitive data to protect it in case of exfiltration

Recent C&C server domain and IP of QuasarRAT malware are as follows:

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

pensionrrcell.duckdns.org

185.161.208.116

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