**Cyber Security Advisories**

**Date: 15 January 2025**

1. **[CMTX-I-443012025] Malicious Domains used by Threat Actors (TLP:AMBER)**

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

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

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

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

Prevention Measures:

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

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

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

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

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

edisha.gov.in.vlew.tech

gov.in.8thpaycomission.cloud

gov.in.vlew.tech

www.cgda.gov.in.8thpaycomission.cloud

www.edisha.gov.in.vlew.tech

\*.8thpaycomission.cloud

\*.vlew.tech

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

1. **[CMTX-I-080012025] Malicious Domains used by Threat Actors [TLP: AMBER]**

Threat Overview

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

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

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

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

Prevention Measures:

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

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

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

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

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

jkpolice.gov.in.aboutcase.nl

mail.aboutcase.nl

webdisk.aboutcase.nl

whm.aboutcase.nl

www.jkpolice.gov.in.aboutcase.nl

indianoil.site

www.hpcl.io

mumbaipolice.gov.in.expertdigitalit.com

ww38.indian-army.site

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

1. **[CMTX-P-012025024] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

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.

Indicators of Compromise (IOCs):

IP Addresses :Port

18.166.152.198:8443

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

1. **[CMTX-P-012025014] 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.

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

Indicators of Compromise (IOCs):

IP Addresses: Port

114.29.254.126:80,443

114.29.254.17:80,443

114.29.254.201:80,443

114.29.254.94:80,443

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

1. **[CMTX-P-012025015] Beast Ransomware**

Threat Overview

BEAST ransomware, also known as Monster ransomware, is a ransomware-as-a-service (RaaS) that has been active since at least 2022. It targets multiple operating systems, including Windows, Linux, and VMware ESXi servers etc. The ransomware is designed to encrypt files and extort ransom payments, typically offering a unique decryption key for each infected machine.

Distribution Method:

The BEAST ransomware for Linux encrypts data in segments and employs robust encryption techniques like ECC, AES, and ChaCha. It can use many threads to encrypt files simultaneously. Every compromised computer is assigned a distinct ID and decryption key. It has two modes: Zip Wrap Mode, which encrypts files in ZIP packages to evade antivirus detection, and Normal Mode, which renames files and includes a ransom note. Command-line options for routes, functions, and external notes allow for customization. It also operates in daemon mode and shuts down virtual computers.

Threat Type: Ransomware

Severity: High

Affected Systems: Windows, Linux, and VMware ESXi servers

Preventive Measures:

• 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.

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

• Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts 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

Indicators of Compromise (IOCs):

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

HASH

66f86812a6593cdd760cd2119f8bf1a76f33a1b56ab099edc02de7b0629ea15d

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

1. **[CMTX-I-021012025] Mythic Malware- Pakistan Based Malware Campaign**

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

Common Features of Mythic Malware:

> Persistence

> Remote access and data theft

> Modular architecture and customizable

> Stealth techniques to avoid detection by security software

Prevention Measures:

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

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

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

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

> Principle of least privilege

> Firewall and network security along with regular OS updates

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

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

ntp-pool.site

currently resolving to 5.230.41.90

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

1. **[CMTX-I-025012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

bihar.aoth.xyz

biharresult.aoth.xyz

coalindia-app.com

dsde.goa.gov.inc

ebanking.indiapospzt.gov.inc

eprocure.gov.in.w3lookup.net

evisa.gov.inc

fancy.parivahan.gov.inc

gov.in.farmarlife.com

gov.in.veiw.xyz

gov.in.w3lookup.net

gov.indexp.site

i4c.mha.gov.in.farmarlife.com

iocl.cloud

media.evisa.gov.inc

media.visa.gov.inc

pmkisan.gov.inc

result.aoth.xyz

rms.indianrail.gov.in.rrbgovresult.in

scholarship.up.gov.inc

statistics.evisa.gov.inc

statistics.visa.gov.inc

student.nielit.gov.inc

visa.gov.inc

vlew.tech.aoth.xyz

www.dc.crsorgi.gov.in.cphp.info

www.ebanking.indiapospzt.gov.inc

www.evisa.gov.inc

www.i4c.mha.gov.in.farmarlife.com

www.mahapolice.gov.in.farmarlife.com

www.visa.gov.inc

\*.aoth.xyz

\*.cphp.info

\*.crsorig-gov.info

\*.dclink.shop

\*.farmarlife.com

\*.gov.inc

\*.indexp.site

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

1. **[CMTX-P-012025034] 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.

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

Indicators of Compromise (IOCs):

IP Addresses: Port

8.217.16.241:443

63.141.237.222:80,443

45.12.91.12:8080

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

1. **[CMTX-P-012025044] SHADOWPAD (POISONPLUG) Malware Campaign**

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

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

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.

Indicators of Compromise (IOCs):

IP Addresses :Port

64.176.65.49:443

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

1. **[CMTX-I-028012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

email.igov.ink

\*.igov.ink

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

1. **[CMTX-I-911012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

email.gov.in.indiandefence.nl

gov.in.indiandefence.nl

in.indiandefence.nl

\*.indiandefence.nl

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

1. **[CMTX-P-VUL-0120256615] Prominent Vulnerability List**

CERT-In has compiled a list of vulnerabilities reported and exploited recently for due consideration and prioritization. Details are attached.

File Name: vuln\_list\_0801.pdf

SHA256:0c6e39accd083c93688b696202cc20529604cdc75fd0f847463115e6f721d2a4

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

1. **[CMTX-P012025105] CRITICAL VULNERABILITIES AFFECTING IVANTI CONNECT SECURE VPN APPLIANCES**

ALERT BRIEF:

A critical zero day vulnerability tracked as CVE-2025-0282 is being exploited in the wild particularly by a China-nexus threat actor group known as UNC5337 and affecting Ivanti Connect Secure VPN, Ivanti Policy Secure, and Ivanti Neurons for ZTA Gateways.

It has been reported that some malwares are deployed to execute payloads, some of them are as follows:

SPAWN: A malware ecosystem associated with the exploitation, attributed to the China-nexus threat actor UNC.It is utilized for command-and-control communication and system exploitation.

PHASEJAM: A shell script dropper; it modifies Ivanti appliance components and establishes persistence by blocking legitimate updates. It inserts web shells, modifies critical system files, and prevents system updates.

DRYHOOK: A Python script used to harvest credentials and facilitate lateral movement within networks.It harvests sensitive credentials from the compromised systems.

Another flaw, CVE-2025-0283 is a stack-based buffer overflow vulnerability affecting Ivanti Connect Secure, Policy Secure, and ZTA Gateways, which has been actively exploited in the wild. It allows a locally authenticated attacker to escalate their privileges.

IMPACTS:

1. Unauthenticated Remote Code Execution: Successful exploitation allows attackers to execute arbitrary code remotely.

2. Data Breach: Attackers may gain access to sensitive information, including VPN session data, API keys, and user credentials.

3. System Integrity Compromise: Attackers can modify system files and disable security measures.

4. Use tools like Nmap and Dig to explore and gather information about the internal network.

5. Use the LDAP service account to query the LDAP directory and move around the network, including accessing Active Directory servers via SMB or RDP.

DISTRIBUTION METHODS:

Attack Vector: Attackers exploit the vulnerability by executing a series of pre-defined scripts that disable security features, modify system logs, and install malicious payloads.

Exploitation Steps:

1. Disable SELinux and prevent syslog forwarding.

2. Execute scripts to install malicious binaries and web shells.

3. Establish persistence to maintain access post-exploitation.

AFFECTED VERSIONS:

Ivanti Connect Secure: Versions prior to 22.7R2.5

Ivanti Policy Secure: Versions prior to 22.7R1.- Ivanti Neurons for ZTA Gateways: Versions prior to 22.7R2.3

Threat Type: Vulnerability

CVE-2025-0282, CVSS SCORE-9.0

CVE-2025-0283, CVSS SCORE-7.3

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

RECOMMENDATIONS:

1.Immediate Patching: Apply the latest patches (22.7R2.5 for Connect Secure, 22.7R1.2 for Policy Secure, 22.7R2.3 for ZTA Gateways).

2.System Scans: Conduct thorough scans for signs of compromise in the environment.

3.Monitor Logs: Regularly review application and security logs for suspicious activity.

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

INDICATORS OF COMPROMISE:

- ----------START OF IOCs----------------------

HASH

e7d24813535f74187db31d4114f607a1

4f79c70cce4207d0ad57a339a9c7f43c

61bb586dc4e047ab081ef6ca65684e48

d18e5425ecd9608ecb992606b974e15d

File names:

/home/webserver/htdocs/dana-na/auth/getComponent.cg

/home/webserver/htdocs/dana-na/auth/restAuth.cgi

/root/home/lib/libsshd.so

/root/home/lib/libsocks5.so

/root/lib/libupgrade.so

/tmp/.liblogblock.so

- ----------END OF IOCs----------------------

1. **[CMTX-P-012025905] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

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

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

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

Impacts:

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

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

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

2. Threat Type : Multi modular backdoor

3. Severity: High

Distribution Methods:

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

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-012025905]

Indicators of Compromise (IOCs):

IPs: PORTS

108.61.177.149:443

107.148.45.172:443

107.148.45.174:80

107.148.45.171:443

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

1. **[CMTX-P-012025915] 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-012025915]

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

Indicators of Compromise (IOCs):

IP Addresses: Port

121.201.74.246:5000

141.98.212.75:80

208.85.17.4:443

208.85.18.176:443

27.102.127.28:443

103.142.9.135:10000

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

1. **[CMTX-P012025205] A CRITICAL RCE FLAW (CVE-2024-52875) AFFECTING GFI KERIOCONTROL FIREWALLS , (TLP: CLEAR)**

ALERT BRIEF:

It has been reported that a critical CRLF (carriage return line feed) injection vulnerability is affecting the GFI KerioControl firewall, which can lead to one-click remote code execution (RCE) attacks. This vulnerability allows attackers to exploit HTTP response splitting, potentially leading to Remote Code Execution (RCE) via malicious HTTP response headers. Successful exploitation can allow an attacker to upload malicious files to the firewall, granting root access and permits an attacker to inject malicious inputs into HTTP response headers.

An attacker could create a malicious URL that, when clicked by an administrator, triggers the execution of a proof-of-concept (PoC) hosted on an attacker-controlled server. This PoC would then upload a harmful .img file using the firmware upgrade feature, ultimately giving the attacker root access to the firewall.

IMPACTS:

1. Remote Code Execution (RCE)

2. Unauthorized access to firewall management

3. Potential for further attacks, including Cross-Site Scripting (XSS)

AFFECTED VERSIONS: The flaw impacts KerioControl versions 9.2.5 through 9.4.5

Threat Type: Vulnerability

CVE-2024-52875

CVSS SCORE- 5.5

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

RECOMMENDATIONS and MITIGATIONS:

1. Immediate Update: Upgrade to GFI KerioControl version 9.4.5 Patch or later, released on December, .

2. Network Monitoring: Implement network monitoring for unusual traffic patterns that may indicate exploitation attempts.

3. Input Validation: Ensure proper input validation and sanitization for all user inputs, particularly those passed to HTTP headers.

4. Access Controls: Review and tighten access controls for firewall management interfaces to limit exposure.

5. Incident Response Plan: Develop or update incident response plans to address potential exploitation scenarios.

6. Threat Intelligence Sharing: Engage with threat intelligence organizations to stay informed about ongoing exploitation attempts.

7. Regular Security Audits: Conduct regular security audits and penetration testing of the firewall configurations.

8. Firewall Logging: Enable and monitor detailed logging on firewalls to detect and respond to potential exploitation attempts.

9. Patch Management: Establish a robust patch management process to ensure timely application of security updates

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

1. **[CMTX-I-032012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

apimyspeed.trai.gov.in.pirozas.lol

www.edisha.gov.in.vlecert.xyz

www.edisha.gov.in.vlew.xyz

edisha.gov.in.vlecert.xyz

edisha.gov.in.vlew.xyz

\*.pirozas.lol

\*.vlecert.xyz

\*.vlew.xyz

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

1. **[CMTX-P-6080120259] Agent Tesla Malware Alert**

Threat Overview:

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

Impacts:

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

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

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

Prevention and Mitigation:

Regular System Monitoring: Implement endpoint detection and response (EDR) tools to detect anomalous activity.

Limit User Privileges: Restrict administrative rights to reduce the impact if malware executes.

Awareness Training: Educate employees on phishing tactics to avoid opening suspicious attachments.

Use Strong Passwords: Ensure secure password policies to mitigate credential theft.Recent IOCs of Agent Tesla malware are as follows:

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

87.166.55.254 [Germany]

46.175.148.58 [Ukraine]

203.175.9.22 [Indonesia]

47.76.82.23 [China]

92.37.143.94 [Russia]

195.252.110.253 [Serbia]

103.92.235.178 [India]

213.189.52.181 [Poland]

92.205.7.112 [Germany]

95.217.148.220 [Finland]

85.10.224.196 [Germany]

93.89.225.40 [Turkey]

136.243.131.47 [Germany]

46.29.239.57 [Netherlands]

110.4.45.197 [Malaysia]

5.2.84.76 [Turkey]

89.39.83.184 [Romania]

217.116.201.44 [Turkey]

148.251.209.169 [Germany]

185.165.185.2 [Romania]

193.141.65.39 [Iran]

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

1. **[CMTX-P-9590120259] Ursnif Malware Alert**

Threat Overview:

Ursnif (also known as Gozi) is identified as a Banking Trojan, but its variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.

Impacts:

Banking Trojan: Ursnif is specialized in stealing banking information, including login credentials, credit card numbers, and transaction data.

Credential Harvesting: Steals credentials from email accounts, VPN clients, and web browsers.

Persistence Mechanisms: Uses various techniques to persist in systems and avoid detection, including injecting malicious code into legitimate processes.

Prevention and Mitigation:

Restrict Access to Financial Systems: Isolate financial operations to reduce the risk of exposure.

Secure Email Gateways: Deploy secure email solutions that prevent malicious attachments and links from reaching users.

Malware Detection Tools: Regularly scan systems using anti-malware solutions capable of identifying Ursnif-related activity.Recent IOCs of Ursnif malware are as follows:

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

3.115.86.44 [Japan]

3.1.63.204 [Singapore]

159.65.6.6 [Singapore]

52.221.92.67 [Singapore]

87.106.18.141 [Germany]

217.26.60.200 [Switzerland]

13.251.16.150 [Singapore]

18.178.237.95 [Japan]

83.218.160.14 [Austria]

91.195.240.85 [Germany]

185.222.58.82 [Netherlands]

185.222.57.76 [Netherlands]

185.222.58.240 [Netherlands]

147.45.67.77 [Russia]

185.222.58.80 [Netherlands]

185.222.58.87 [Netherlands]

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

1. **[CMTX-P-9130120259] Trickbot Malware Alert**

Threat Overview:

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

Impacts:

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

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

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

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

Prevention and Mitigation:

Secure Remote Desktop Protocol (RDP): Trickbot frequently exploits weak or exposed RDP services. Disable or secure RDP with strong passwords and MFA.

Patch Systems: Regularly patch operating systems and software to fix vulnerabilities Trickbot may exploit.

Network Segmentation: Implement network segmentation and least privilege principles to limit Trickbot's ability to spread laterally.

Email Protection: Since Trickbot is often distributed via phishing emails, use strong email filtering to block malicious attachments and links.

Anti-Malware and EDR Solutions: Use advanced endpoint detection and response (EDR) solutions to detect Trickbot activity and block infections early.Recent IOCs of Trickbot malware are as follows:

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

27.109.116.144 [Cambodia]

103.201.142.30 [India]

175.184.232.234 [Indonesia]

177.190.76.82 [Brazil]

41.77.134.250 [Mozambique]

196.41.57.46 [Tanzania]

96.9.77.142 [Cambodia]

34.249.180.228 [Ireland]

79.125.7.88 [Ireland]

54.194.166.138 [Ireland]

54.75.207.238 [Ireland]

159.65.6.6 [Singapore]

194.87.94.14 [Russia]

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

1. **[CMTX-P-1750120259] SocGholish Malware Alert**

Threat Overview:

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

Impacts:

Web-Based Malware: SocGholish primarily spreads through compromised websites and serves fake updates (e.g., fake Flash or browser updates).

Drive-by Downloads: Can result in the downloading of further malware, including remote access trojans (RATs) and ransomware.

Malvertising Campaigns: Often integrated into malicious advertisements on legitimate websites.

Prevention and Mitigation:

Web Filtering: Block access to known malicious websites and employ domain categorization to filter potentially harmful sites.

Disable Auto-Downloads: Ensure browsers are configured to prevent automatic downloading and execution of files.

Secure Web Browsers: Use web browsers with robust security features and regularly update them to prevent exploitation.Recent IOCs of SocGholish malware are as follows:

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

45.130.201.24 [Czechia]

34.96.205.106 [China]

185.187.241.36 [Singapore]

31.220.15.143 [Sweden]

5.101.115.147 [Estonia]

103.230.48.78 [Indonesia]

93.190.41.79 [Ukraine]

54.36.145.173 [Spain]

81.173.194.3 [Germany]

103.165.154.15 [Indonesia]

145.239.23.7 [Poland]

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

1. **[CMTX-P-5530120259] Redline Malware Alert**

Threat Overview:

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

Impacts:

Information Stealer: Redline focuses on harvesting a wide range of sensitive information, including login credentials, browser data, cryptocurrency wallets, and system information.

Credential Theft: It can steal passwords stored in web browsers, email clients, and FTP clients, leading to potential data breaches and identity theft.

Dark Web Activity: Stolen data is often sold on dark web forums, making it a lucrative tool for cybercriminals.

Remote Access and Surveillance: Redline may allow attackers to remotely control infected systems, exfiltrating more data.

Prevention and Mitigation:

Browser Security: Use secure browser settings and avoid saving passwords and sensitive information in web browsers.

Monitor Dark Web Activity: Implement tools that notify you if sensitive company or user information is posted on dark web marketplaces.

Password Manager: Encourage users to use password managers to store credentials instead of browser storage, as it provides better security.

Strong Endpoint Security: Use endpoint security solutions capable of detecting Redline-related activity such as keylogging, credential theft, and exfiltration.

Recent IOCs of Redline malware are as follows:

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

147.45.67.77 [Russia]

150.241.105.82 [Germany]

185.159.129.54 [Russia]

185.222.58.80 [Netherlands]

185.222.58.82 [Netherlands]

193.37.71.131 [Russia]

212.233.122.234 [Russia]

80.66.89.157 [Russia]

80.66.89.228 [Russia]

212.87.215.19 [Germany]

185.222.58.87 [Netherlands]

45.137.22.250 [Netherlands]

163.172.62.5 [France]

147.45.67.15 [Russia]

185.222.57.74 [Netherlands]

185.222.57.93 [Netherlands]

185.222.58.240 [Netherlands]

185.222.58.84 [Netherlands]

185.222.58.90 [Netherlands]

185.81.68.147 [Russia]

147.45.44.224 [Belize]

45.137.22.254 [Netherlands]

62.68.75.70 [Germany]

147.45.67.12 [Russia]

13.60.40.107 [Sweden]

194.59.30.189 [France]

185.222.57.90 [Netherlands]

213.248.43.127 [Russia]

89.23.97.121 [Russia]

185.222.57.81 [Netherlands]

185.222.57.76 [Netherlands]

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

1. **[CMTX-P-7360120259] Amadey Malware Alert**

Threat Overview:

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

Impacts:

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

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

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

Prevention and Mitigation:

    Disable Macros in Office Files: Malware like Amadey often spreads through documents containing malicious macros.

    Advanced Threat Protection (ATP): Use ATP solutions that include sandboxing to detect and block malware-laden attachments.

    Firewall and Network Controls: Restrict outbound connections that Amadey may use to communicate with its command-and-control (C2) servers.Recent IOCs of Amadey malware are as follows:

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

45.9.74.141 [Russia]

45.9.74.164 [Russia]

45.9.74.166 [Russia]

45.9.74.182 [Russia]

77.105.160.21 [Netherlands]

162.55.199.142 [Germany]

178.62.201.34 [Netherlands]

185.11.61.121 [Russia]

185.172.128.63 [Russia]

185.196.8.176 [Switzerland]

185.208.158.116 [Seychelles]

185.208.158.96 [Seychelles]

185.215.113.16 [Seychelles]

185.215.113.209 [Seychelles]

185.215.113.36 [Seychelles]

185.215.113.43 [Seychelles]

185.53.178.51 [Germany]

188.114.96.6 [Colombia]

188.114.97.6 [Colombia]

188.40.141.211 [Germany]

188.40.187.155 [Germany]

193.233.20.14 [Russia]

193.3.19.154 [Russia]

197.251.236.226 [Ghana]

31.41.244.146 [Russia]

45.15.156.208 [Netherlands]

45.56.230.44 [Philippines]

45.77.249.79 [Singapore]

5.42.66.32 [Finland]

5.42.67.14 [Czechia]

5.75.139.35 [Germany]

5.79.71.205 [Netherlands]

62.182.156.153 [Russia]

62.60.226.15 [Germany]

77.73.133.72 [Germany]

77.73.134.66 [Austria]

77.91.68.62 [Finland]

77.91.68.63 [Finland]

78.46.242.112 [Germany]

79.137.192.15 [Russia]

79.137.203.59 [Germany]

80.76.42.67 [Ukraine]

89.110.69.103 [Netherlands]

89.163.249.231 [Germany]

89.208.107.49 [Netherlands]

89.23.103.42 [Netherlands]

94.156.177.33 [Netherlands]

94.232.249.157 [Netherlands]

94.250.250.71 [Russia]

138.201.203.107 [Germany]

185.81.68.147 [Russia]

185.81.68.148 [Russia]

185.232.14.78 [Singapore]

31.41.244.10 [Russia]

46.173.214.183 [Russia]

188.114.96.0 [Colombia]

193.42.32.29 [Slovakia]

193.106.191.184 [Iran]

185.11.61.104 [Russia]

193.106.191.185 [Iran]

193.106.191.201 [Iran]

78.47.9.120 [Germany]

85.17.31.122 [Netherlands]

45.15.156.169 [Netherlands]

185.196.10.34 [Switzerland]

85.17.31.82 [Netherlands]

5.42.65.1 [Netherlands]

79.98.25.1 [Lithuania]

176.113.115.139 [Russia]

178.88.168.55 [Kazakhstan]

5.79.71.225 [Netherlands]

92.113.68.44 [Germany]

77.91.78.118 [Netherlands]

5.42.66.0 [Russia]

85.118.98.225 [Georgia]

91.151.136.100 [Unknown]

77.91.68.18 [Finland]

62.204.41.252 [Russia]

95.101.193.200 [Denmark]

188.42.224.102 [Netherlands]

91.151.136.144 [Georgia]

91.151.136.252 [Georgia]

212.162.57.144 [Germany]

80.66.75.11 [Russia]

91.151.136.204 [Unknown]

91.151.136.220 [Unknown]

91.151.137.8 [Unknown]

104.79.38.8 [Germany]

109.206.161.43 [Netherlands]

157.230.122.233 [Germany]

185.147.125.147 [Russia]

185.183.35.23 [Netherlands]

185.232.14.223 [Singapore]

185.38.109.109 [Czechia]

188.246.228.115 [Russia]

209.250.227.192 [Russia]

212.93.103.235 [Latvia]

212.93.111.241 [Latvia]

213.36.253.2 [France]

217.175.24.118 [Russia]

23.55.51.171 [Japan]

35.234.77.182 [Germany]

37.243.69.72 [Saudi Arabia]

43.240.239.73 [Korea, South]

45.93.20.135 [Russia]

77.77.68.124 [Iran]

82.192.82.226 [Netherlands]

83.217.70.126 [Belgium]

84.103.237.61 [France]

85.249.168.74 [Russia]

91.113.171.6 [Austria]

91.151.136.102 [Georgia]

91.151.136.104 [Unknown]

91.151.136.158 [Unknown]

91.151.136.159 [Unknown]

91.151.136.160 [Unknown]

91.151.136.168 [Georgia]

91.151.136.173 [Georgia]

91.151.136.179 [Unknown]

91.151.136.184 [Georgia]

91.151.136.203 [Georgia]

91.151.136.232 [Georgia]

91.151.136.240 [Georgia]

91.151.136.78 [Unknown]

91.151.137.2 [Unknown]

91.151.137.35 [Unknown]

91.151.138.147 [Georgia]

91.184.121.10 [Georgia]

91.220.113.239 [Iran]

93.158.134.90 [Russia]

185.196.8.126 [Seychelles]

89.35.131.209 [Armenia]

193.124.185.114 [Netherlands]

34.246.200.160 [Ireland]

91.202.233.180 [Russia]

185.172.128.100 [Russia]

45.15.156.216 [Germany]

104.97.15.165 [Netherlands]

45.159.189.140 [Netherlands]

159.100.251.128 [Switzerland]

78.153.144.60 [Poland]

185.215.113.38 [Seychelles]

91.203.4.45 [Ukraine]

23.3.109.48 [Germany]

91.151.136.128 [Unknown]

188.114.96.9 [Colombia]

54.251.113.207 [Singapore]

147.45.47.155 [Russia]

91.151.137.42 [Unknown]

49.12.117.51 [Germany]

194.39.65.28 [Kazakhstan]

103.21.25.245 [Thailand]

91.151.136.136 [Unknown]

185.196.10.188 [Seychelles]

103.241.48.46 [Germany]

104.124.54.145 [India]

130.193.51.109 [Russia]

151.234.167.4 [Iran]

151.234.196.57 [Iran]

153.92.203.121 [Germany]

165.231.2.187 [South Africa]

178.134.211.72 [Georgia]

185.211.86.67 [Iran]

185.215.113.205 [Seychelles]

185.215.113.217 [Seychelles]

185.22.66.15 [Kazakhstan]

185.22.66.16 [Kazakhstan]

185.242.250.251 [Spain]

185.81.129.98 [Latvia]

188.122.125.53 [Iran]

204.18.117.61 [Iran]

204.18.24.201 [Iran]

212.114.128.66 [Germany]

213.202.229.103 [Germany]

213.238.176.93 [Turkey]

23.200.13.65 [France]

23.200.13.67 [France]

37.255.100.77 [Iran]

37.48.65.152 [Netherlands]

37.48.65.155 [Netherlands]

46.48.94.246 [Russia]

5.114.130.210 [Iran]

5.114.177.216 [Iran]

5.122.52.35 [Iran]

5.250.82.42 [Iran]

5.250.86.168 [Iran]

5.250.87.203 [Iran]

80.210.202.162 [Iran]

82.98.170.50 [Spain]

91.151.136.111 [Unknown]

91.151.136.125 [Unknown]

91.151.136.143 [Georgia]

91.151.136.161 [Georgia]

91.151.136.171 [Georgia]

91.151.136.212 [Unknown]

91.151.136.91 [Unknown]

91.151.137.15 [Georgia]

91.151.137.23 [Georgia]

91.151.137.38 [Unknown]

91.151.137.57 [Unknown]

92.205.15.171 [Germany]

92.205.20.191 [Germany]

212.32.237.90 [Netherlands]

94.131.102.113 [Ukraine]

92.205.57.102 [Germany]

62.204.41.145 [Russia]

91.199.27.139 [Iran]

92.205.48.200 [Germany]

79.137.192.18 [Russia]

37.48.94.74 [Netherlands]

194.105.56.41 [Latvia]

139.185.34.131 [Unknown]

212.32.237.101 [Netherlands]

158.58.12.202 [Iran]

169.197.100.20 [Unknown]

185.106.92.127 [Netherlands]

185.114.247.54 [Russia]

185.115.78.239 [Iran]

185.204.181.34 [Iran]

185.209.162.226 [Netherlands]

188.213.180.195 [Iran]

188.68.47.60 [Germany]

193.188.135.22 [Lebanon]

194.247.187.181 [Germany]

194.99.110.214 [Germany]

195.234.5.202 [Ukraine]

2.191.59.103 [Iran]

2.57.217.119 [Georgia]

204.18.167.9 [Iran]

208.82.75.19 [Germany]

212.204.75.54 [Germany]

212.93.112.52 [Latvia]

212.93.113.186 [Latvia]

212.93.117.130 [Latvia]

212.93.121.214 [Latvia]

31.184.197.244 [Russia]

31.214.178.109 [Spain]

37.255.76.6 [Iran]

45.9.191.182 [Netherlands]

5.125.12.83 [Iran]

5.209.136.51 [Iran]

5.209.170.33 [Iran]

5.209.192.33 [Iran]

5.209.99.132 [Iran]

5.210.189.255 [Iran]

5.213.217.24 [Iran]

5.213.224.250 [Iran]

5.214.151.216 [Iran]

5.214.207.143 [Iran]

5.22.28.86 [Iran]

5.239.173.157 [Iran]

5.255.125.140 [Netherlands]

5.52.128.194 [Iran]

5.57.226.202 [Spain]

78.24.220.111 [Russia]

80.90.18.102 [Germany]

84.53.133.249 [Spain]

86.55.76.122 [Iran]

87.249.38.126 [Russia]

89.33.96.78 [Romania]

89.40.243.56 [Iran]

91.151.136.189 [Unknown]

91.151.138.183 [Georgia]

91.212.166.67 [Russia]

93.186.137.168 [Greece]

95.181.182.182 [Russia]

95.211.227.207 [Netherlands]

185.172.128.5 [Russia]

212.32.237.91 [Netherlands]

151.236.102.251 [Russia]

212.27.63.112 [France]

5.44.111.112 [Germany]

193.42.33.74 [Slovakia]

118.193.34.185 [China]

89.37.121.88 [Romania]

185.56.218.10 [Italy]

87.230.98.78 [Germany]

89.252.163.94 [Turkey]

91.151.136.142 [Unknown]

109.239.54.153 [Germany]

120.60.22.96 [India]

164.215.198.21 [Iran]

185.5.82.66 [Germany]

194.146.59.71 [Serbia]

194.163.38.170 [Singapore]

2.189.243.232 [Iran]

202.45.144.21 [Nepal]

213.158.90.44 [Greece]

31.192.20.100 [Georgia]

34.79.105.147 [Belgium]

37.157.197.121 [Czechia]

43.159.20.120 [Singapore]

46.21.97.151 [Sweden]

5.113.154.163 [Iran]

5.119.208.181 [Iran]

5.213.146.183 [Iran]

5.22.57.112 [Iran]

5.250.97.198 [Iran]

5.53.55.200 [Iran]

5.75.55.17 [Iran]

8.222.233.183 [Singapore]

83.122.20.165 [Iran]

89.248.161.167 [Netherlands]

89.47.198.209 [Iran]

91.151.136.131 [Georgia]

91.151.137.48 [Unknown]

92.54.203.4 [Georgia]

95.163.118.168 [Russia]

95.211.219.65 [Netherlands]

95.25.198.122 [Russia]

185.66.142.35 [Netherlands]

195.123.210.178 [Latvia]

37.230.117.113 [Russia]

46.173.214.218 [Russia]

109.106.253.13 [Singapore]

156.67.214.130 [Singapore]

185.215.113.17 [Seychelles]

188.225.10.62 [Russia]

193.17.199.27 [Switzerland]

194.36.124.45 [Hungary]

202.61.232.70 [Germany]

23.61.0.215 [Singapore]

34.154.31.121 [Italy]

35.198.131.110 [Germany]

37.232.98.169 [Georgia]

37.48.65.154 [Netherlands]

5.113.131.134 [Iran]

5.214.104.252 [Iran]

5.250.203.133 [Azerbaijan]

5.62.252.188 [Iran]

58.65.179.22 [Pakistan]

82.138.56.234 [Russia]

85.118.117.33 [Georgia]

85.249.167.138 [Unknown]

89.108.86.20 [Russia]

91.151.136.115 [Unknown]

91.151.136.124 [Georgia]

91.151.136.233 [Georgia]

91.151.137.52 [Unknown]

92.205.0.58 [Germany]

92.38.128.246 [Russia]

93.174.125.153 [Greece]

95.181.226.152 [Russia]

95.211.228.155 [Netherlands]

95.25.55.45 [Russia]

95.25.6.34 [Russia]

95.38.60.9 [Iran]

212.32.237.92 [Netherlands]

36.86.63.182 [Indonesia]

46.173.214.213 [Russia]

128.140.224.132 [Romania]

149.126.4.66 [Switzerland]

149.126.4.83 [Switzerland]

185.147.125.145 [Russia]

185.166.104.95 [Iran]

185.51.188.47 [Hungary]

188.130.251.30 [Kazakhstan]

192.9.180.162 [Kazakhstan]

195.170.63.162 [Russia]

23.34.46.187 [Denmark]

31.184.217.23 [Russia]

37.243.8.239 [Saudi Arabia]

46.163.119.242 [Germany]

5.209.120.48 [Iran]

5.23.54.22 [Russia]

5.233.244.219 [Iran]

5.250.106.35 [Iran]

5.74.179.183 [Iran]

78.140.140.243 [Netherlands]

80.82.78.114 [Netherlands]

81.171.8.143 [Netherlands]

91.151.136.103 [Unknown]

91.151.136.105 [Unknown]

91.151.136.120 [Unknown]

91.151.136.200 [Georgia]

91.151.136.214 [Unknown]

91.151.136.234 [Georgia]

91.151.136.89 [Georgia]

91.151.136.92 [Georgia]

91.151.137.13 [Unknown]

91.151.137.22 [Georgia]

91.242.19.216 [Azerbaijan]

91.37.212.64 [Germany]

92.204.239.213 [Germany]

92.204.58.28 [Germany]

92.63.104.16 [Russia]

93.170.52.17 [Russia]

95.154.242.80 [Greece]

109.237.138.42 [Germany]

130.193.55.158 [Russia]

146.66.155.5 [Austria]

158.58.15.31 [Iran]

158.58.66.204 [Iran]

178.209.115.167 [Russia]

185.176.189.102 [Spain]

185.205.186.49 [Cyprus]

185.215.113.25 [Seychelles]

185.216.143.86 [Netherlands]

185.87.148.190 [Czechia]

188.121.110.182 [Iran]

188.229.76.164 [Iran]

188.245.229.107 [Iran]

195.252.110.134 [Serbia]

2.147.237.79 [Iran]

31.14.14.191 [Romania]

31.177.76.32 [Russia]

37.221.194.125 [Germany]

37.243.207.55 [Saudi Arabia]

37.243.238.124 [Saudi Arabia]

37.27.14.218 [Finland]

5.123.120.241 [Iran]

5.123.83.165 [Iran]

5.209.88.8 [Iran]

5.210.154.147 [Iran]

62.219.67.159 [Israel]

81.27.251.50 [Finland]

83.167.24.2 [Russia]

87.236.102.210 [Netherlands]

89.108.120.215 [Russia]

89.221.218.19 [Czechia]

89.42.218.250 [Romania]

91.151.130.78 [Georgia]

91.151.136.116 [Georgia]

91.151.136.170 [Georgia]

91.151.136.193 [Unknown]

91.151.136.199 [Georgia]

91.151.136.210 [Unknown]

91.151.137.16 [Unknown]

91.151.137.55 [Unknown]

93.110.127.193 [Iran]

93.119.92.51 [Iran]

94.101.182.2 [Iran]

95.162.241.142 [Iran]

194.87.102.61 [Russia]

188.114.97.0 [Colombia]

51.250.126.210 [Russia]

92.53.96.102 [Russia]

139.45.197.119 [Netherlands]

178.162.170.131 [Netherlands]

72.246.28.100 [Germany]

141.98.9.201 [Netherlands]

178.162.132.113 [Netherlands]

81.19.89.16 [Russia]

104.108.145.136 [Germany]

185.149.40.213 [Ukraine]

188.164.195.42 [Spain]

195.252.110.165 [Serbia]

34.242.73.233 [Ireland]

34.91.251.221 [Netherlands]

45.92.156.177 [Netherlands]

78.41.204.29 [Netherlands]

89.108.118.65 [Russia]

89.108.94.98 [Russia]

89.163.152.111 [Germany]

89.163.210.240 [Germany]

93.158.210.46 [Netherlands]

93.186.201.118 [Germany]

95.163.98.240 [Russia]

81.246.65.148 [Belgium]

104.121.145.3 [Germany]

109.239.56.200 [Germany]

94.247.135.60 [Kazakhstan]

194.59.167.224 [Lithuania]

139.45.197.15 [Netherlands]

139.45.197.105 [Netherlands]

139.45.197.116 [Netherlands]

139.45.197.121 [Netherlands]

139.45.197.122 [Netherlands]

141.98.9.203 [Netherlands]

86.111.241.251 [Poland]

62.213.66.135 [Russia]

81.19.83.40 [Russia]

109.95.212.121 [Russia]

141.8.193.61 [Russia]

147.45.48.96 [Russia]

185.26.122.11 [Russia]

185.79.236.160 [Russia]

45.141.56.116 [Seychelles]

31.41.244.158 [Russia]

185.215.113.9 [Seychelles]

31.214.178.16 [Spain]

185.176.43.50 [Bulgaria]

152.89.198.124 [Russia]

35.198.88.107 [Germany]

80.69.67.6 [Netherlands]

2.56.90.84 [Netherlands]

213.202.223.112 [Germany]

86.107.198.184 [Kazakhstan]

88.116.203.166 [Austria]

185.176.43.106 [Bulgaria]

88.86.116.142 [Czechia]

92.205.3.88 [Germany]

178.77.108.29 [Germany]

185.97.115.26 [Kazakhstan]

5.45.87.105 [Netherlands]

85.17.9.164 [Netherlands]

185.240.248.69 [Portugal]

109.172.113.122 [Russia]

188.120.245.195 [Russia]

185.215.113.66 [Seychelles]

38.132.119.166 [Unknown]

213.202.223.111 [Germany]

43.240.239.82 [Korea, South]

141.138.168.119 [Netherlands]

78.135.114.63 [Turkey]

37.114.32.204 [Germany]

37.48.65.143 [Netherlands]

23.34.45.202 [Denmark]

139.45.197.250 [Netherlands]

139.45.197.251 [Netherlands]

185.176.43.39 [Bulgaria]

212.204.112.241 [Germany]

46.36.222.191 [Estonia]

5.104.108.23 [Germany]

77.74.178.17 [Russia]

81.19.89.17 [Russia]

84.234.98.183 [Romania]

91.220.207.116 [Moldova]

80.123.152.172 [Austria]

23.200.13.148 [France]

5.175.14.17 [Germany]

5.175.26.196 [Germany]

23.3.109.41 [Germany]

80.237.133.199 [Germany]

91.250.65.240 [Germany]

92.204.221.63 [Germany]

92.205.13.101 [Germany]

92.205.209.38 [Germany]

185.79.156.51 [Iran]

185.166.104.3 [Iran]

95.211.160.134 [Netherlands]

109.106.240.161 [Netherlands]

46.242.128.49 [Poland]

89.108.90.34 [Russia]

92.63.100.60 [Russia]

185.4.65.168 [Russia]

195.209.42.123 [Russia]

217.25.34.238 [Sweden]

212.146.85.35 [Romania]

37.220.86.117 [Germany]

185.216.143.121 [Netherlands]

188.68.47.9 [Germany]

217.69.254.102 [Germany]

5.10.248.145 [Iran]

88.214.28.7 [Netherlands]

88.214.28.211 [Netherlands]

185.7.214.51 [Russia]

194.163.35.203 [Singapore]

41.115.3.196 [South Africa]

46.232.181.187 [Switzerland]

103.171.90.217 [Vietnam]

81.19.89.18 [Russia]

109.106.254.113 [Singapore]

178.162.140.132 [Netherlands]

185.118.190.160 [Spain]

185.126.219.16 [Turkey]

185.210.144.149 [Singapore]

212.57.118.242 [Russia]

217.21.72.194 [Singapore]

23.40.113.49 [France]

31.47.255.204 [Germany]

35.200.202.118 [India]

37.9.13.129 [Russia]

47.57.233.126 [China]

5.181.216.144 [Singapore]

80.83.116.64 [Germany]

81.19.83.42 [Russia]

89.108.84.26 [Russia]

93.92.100.86 [Netherlands]

95.100.73.207 [Germany]

77.91.77.82 [Netherlands]

81.171.6.66 [Netherlands]

103.145.50.126 [India]

178.172.161.124 [Belarus]

178.250.12.15 [Germany]

185.104.248.144 [Russia]

185.216.143.48 [Netherlands]

194.15.46.77 [Netherlands]

212.77.100.137 [Poland]

31.14.220.15 [Romania]

31.41.244.11 [Russia]

35.234.65.96 [Germany]

45.92.178.114 [Taiwan]

5.35.247.12 [Germany]

80.69.164.230 [Finland]

81.19.83.41 [Russia]

82.103.139.33 [Denmark]

82.200.204.13 [Kazakhstan]

83.217.80.31 [Belgium]

91.232.155.81 [Finland]

92.204.68.19 [Germany]

31.177.80.32 [Russia]

37.243.35.232 [Saudi Arabia]

46.21.101.120 [Sweden]

92.205.175.169 [Germany]

93.12.27.42 [France]

128.199.114.207 [Turkey]

185.21.152.91 [France]

185.210.147.132 [Singapore]

185.244.51.134 [Russia]

212.204.112.234 [Germany]

213.159.7.249 [Turkey]

34.91.99.250 [Netherlands]

35.234.76.210 [Germany]

37.230.112.146 [Russia]

37.243.43.30 [Saudi Arabia]

5.198.130.8 [Czechia]

85.115.25.218 [Germany]

86.105.14.12 [Italy]

89.107.184.2 [Germany]

91.193.180.124 [Russia]

92.205.64.128 [Germany]

92.53.96.41 [Russia]

77.91.68.52 [Finland]

103.186.208.163 [Indonesia]

188.114.97.7 [Colombia]

62.140.250.154 [Russia]

77.91.124.20 [Germany]

154.216.17.4 [Lithuania]

194.58.112.165 [Russia]

46.173.214.37 [Russia]

5.182.39.138 [Portugal]

89.108.108.16 [Russia]

176.53.146.188 [Russia]

80.245.171.70 [Greece]

83.150.215.94 [Turkey]

91.92.144.116 [Bulgaria]

109.95.212.54 [Russia]

3.126.205.164 [Germany]

5.252.229.24 [Poland]

88.217.171.167 [Germany]

109.206.161.114 [Netherlands]

185.176.43.35 [Bulgaria]

31.177.80.70 [Russia]

152.89.235.20 [Slovenia]

193.124.185.53 [Netherlands]

212.39.90.61 [Bulgaria]

35.198.85.242 [Germany]

35.233.77.94 [Belgium]

37.48.65.153 [Netherlands]

46.163.119.134 [Germany]

82.103.129.71 [Denmark]

82.192.82.227 [Netherlands]

82.79.165.52 [Romania]

92.204.58.67 [Germany]

92.60.224.35 [Serbia]

93.115.28.104 [Lithuania]

95.211.218.10 [Netherlands]

87.238.164.232 [Belgium]

212.15.168.69 [Croatia]

23.34.32.139 [Denmark]

5.104.105.148 [Germany]

35.198.184.5 [Germany]

62.128.24.24 [Germany]

89.107.186.22 [Germany]

92.204.239.180 [Germany]

92.205.48.195 [Germany]

92.205.58.141 [Germany]

92.205.145.64 [Germany]

92.205.178.72 [Germany]

134.119.225.197 [Germany]

103.106.2.243 [Iran]

84.33.192.223 [Italy]

195.210.46.48 [Kazakhstan]

81.171.28.45 [Netherlands]

95.211.222.118 [Netherlands]

139.45.197.106 [Netherlands]

139.45.197.107 [Netherlands]

86.111.240.167 [Poland]

185.135.90.85 [Poland]

89.41.38.22 [Romania]

46.173.214.237 [Russia]

91.217.9.244 [Russia]

92.53.96.174 [Russia]

212.46.196.134 [Russia]

109.106.253.146 [Singapore]

152.89.234.15 [Slovenia]

5.57.227.251 [Spain]

91.201.60.22 [Sweden]

185.117.88.231 [Sweden]

193.10.166.38 [Sweden]

77.74.178.23 [Switzerland]

176.105.232.182 [Ukraine]

5.101.2.252 [Russia]

77.91.124.1 [Finland]

89.163.210.241 [Germany]

188.209.214.83 [Romania]

31.204.159.244 [Netherlands]

185.216.143.122 [Netherlands]

23.34.32.199 [Denmark]

151.236.71.248 [Russia]

154.216.18.77 [Lithuania]

176.53.96.78 [Turkey]

178.250.9.178 [Germany]

185.146.84.86 [Romania]

185.216.143.82 [Netherlands]

185.242.116.106 [Russia]

185.41.68.197 [Poland]

188.225.46.129 [Russia]

193.105.32.185 [Poland]

193.146.5.15 [Spain]

193.238.27.35 [Germany]

193.24.237.217 [Germany]

194.163.42.80 [Singapore]

213.189.208.22 [Russia]

23.2.13.201 [Germany]

3.248.33.252 [Ireland]

37.48.65.150 [Netherlands]

5.134.5.184 [Belgium]

5.45.76.212 [Netherlands]

77.36.149.86 [Iran]

82.192.82.228 [Netherlands]

84.53.172.48 [Denmark]

85.17.4.234 [Netherlands]

89.42.218.209 [Romania]

89.46.7.229 [Romania]

91.203.110.222 [Germany]

91.225.219.118 [Netherlands]

92.205.168.25 [Germany]

92.205.168.27 [Germany]

92.63.97.198 [Russia]

136.243.106.238 [Germany]

193.143.1.5 [Russia]

89.249.18.14 [Russia]

195.141.66.190 [Switzerland]

104.87.211.224 [Germany]

23.34.35.157 [Denmark]

34.159.238.10 [Germany]

109.237.134.6 [Germany]

109.237.140.10 [Germany]

130.226.161.34 [Denmark]

130.59.31.251 [Switzerland]

134.119.249.12 [Germany]

159.253.19.119 [Estonia]

164.138.222.99 [Bulgaria]

178.236.137.206 [Russia]

185.73.193.119 [Russia]

195.211.239.254 [Russia]

195.245.112.20 [Netherlands]

195.80.169.2 [Slovakia]

212.27.63.104 [France]

23.34.44.98 [Denmark]

37.202.3.139 [Germany]

5.101.114.138 [Estonia]

5.175.14.129 [Germany]

77.244.243.49 [Austria]

80.85.141.74 [Netherlands]

82.98.171.58 [Spain]

83.220.173.53 [Russia]

89.219.33.51 [Kazakhstan]

91.134.38.117 [Singapore]

91.199.25.52 [Poland]

91.227.16.11 [Russia]

147.45.47.35 [Russia]

62.1.46.51 [Greece]

45.84.1.183 [Russia]

103.234.116.174 [India]

139.45.197.114 [Netherlands]

141.98.9.202 [Netherlands]

163.172.30.144 [France]

178.217.97.215 [Russia]

185.217.99.236 [Israel]

185.71.67.208 [Russia]

194.14.254.138 [Belgium]

217.21.190.142 [Belgium]

3.126.57.221 [Germany]

31.220.121.183 [Germany]

35.198.141.149 [Germany]

5.45.124.68 [Estonia]

5.45.82.49 [Russia]

51.159.19.127 [France]

51.250.126.250 [Russia]

51.250.74.162 [Russia]

62.146.104.29 [Germany]

77.221.130.2 [Russia]

77.87.195.43 [Ukraine]

78.128.76.240 [Bulgaria]

82.98.169.75 [Spain]

89.184.92.67 [Ukraine]

91.204.46.247 [Germany]

92.205.213.10 [Germany]

92.205.232.231 [Germany]

92.205.239.100 [France]

92.53.96.108 [Russia]

141.98.9.20 [Netherlands]

79.137.203.19 [Germany]

185.45.112.70 [Netherlands]

104.108.145.236 [Germany]

129.232.217.83 [South Africa]

141.44.46.52 [Germany]

185.216.143.63 [Netherlands]

188.225.40.162 [Russia]

194.135.231.42 [Russia]

194.163.35.221 [Singapore]

37.46.112.100 [Netherlands]

78.41.204.27 [Netherlands]

86.111.242.129 [Poland]

91.201.52.210 [Russia]

92.205.52.180 [Germany]

92.205.6.179 [Germany]

92.53.96.29 [Russia]

95.142.40.100 [Russia]

95.163.114.204 [Russia]

185.196.8.37 [Seychelles]

79.96.222.35 [Poland]

103.97.91.4 [Nigeria]

104.121.145.167 [Germany]

104.121.145.208 [Germany]

104.86.44.97 [Germany]

104.87.225.85 [Germany]

129.159.22.4 [Unknown]

178.218.216.42 [Russia]

178.255.45.196 [Poland]

185.117.132.1 [Cyprus]

185.194.237.150 [Germany]

185.253.212.22 [Poland]

185.71.67.17 [Russia]

194.88.154.189 [Poland]

195.181.166.177 [Sweden]

195.190.28.230 [Netherlands]

2.23.13.10 [France]

213.227.143.4 [Netherlands]

217.19.237.54 [Belgium]

217.21.72.19 [Singapore]

23.34.32.138 [Denmark]

23.34.46.198 [Denmark]

37.243.18.74 [Saudi Arabia]

46.31.193.48 [France]

5.175.14.230 [Germany]

5.255.103.21 [Netherlands]

5.255.68.245 [Netherlands]

51.250.80.146 [Russia]

62.204.41.87 [Russia]

62.210.16.61 [France]

62.77.158.60 [Lithuania]

79.124.16.230 [Bulgaria]

82.98.157.127 [Spain]

85.142.116.250 [Russia]

85.25.141.41 [France]

86.104.73.213 [Kazakhstan]

89.161.175.161 [Poland]

91.220.207.117 [Moldova]

91.226.30.3 [Russia]

92.205.30.124 [Germany]

93.125.99.62 [Belarus]

95.211.197.140 [Netherlands]

103.163.138.56 [Indonesia]

104.79.39.37 [Germany]

164.138.212.80 [Spain]

185.114.245.123 [Russia]

185.173.104.194 [Iran]

185.32.57.56 [Russia]

188.164.194.34 [Spain]

191.96.207.97 [Netherlands]

194.190.152.209 [Russia]

23.34.42.29 [Denmark]

23.62.61.24 [Netherlands]

37.228.94.132 [Russia]

37.230.159.101 [Russia]

5.35.96.131 [Russia]

5.44.111.124 [Germany]

5.45.116.223 [Estonia]

5.45.125.181 [Estonia]

51.252.133.55 [Saudi Arabia]

51.252.244.93 [Saudi Arabia]

80.113.1.11 [Netherlands]

82.202.165.4 [Russia]

84.53.172.33 [Denmark]

84.53.172.9 [Denmark]

92.205.4.124 [Germany]

93.158.223.21 [Netherlands]

95.101.193.91 [Denmark]

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

1. **[CMTX-P-6110120259] Emotet Malware Alert**

Threat Overview:

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.

Impacts:

Modular Banking Trojan: Initially designed to steal banking credentials, Emotet evolved into a highly modular botnet used to deliver other malware, including ransomware.

Email Thread Hijacking: Emotet hijacks ongoing email conversations, making phishing emails appear more legitimate to recipients.

Spreading Capabilities: Emotet can self-propagate through network shares and brute-force weak passwords.

Ransomware Deployment: Often serves as a precursor to ransomware like Ryuk or Conti, deploying secondary payloads after infecting systems.

Prevention and Mitigation:

Strong Email Security: Use email filtering to block malicious attachments and links. Emotet is commonly distributed via phishing emails.

Disable Macros in Office Files: Emotet often uses malicious macros in Microsoft Office documents. Disable macros where possible.

Patch Vulnerabilities: Ensure all systems are up-to-date with security patches to prevent the exploitation of known vulnerabilities.

Network Segmentation: Limit the spread of malware by segmenting networks and applying strict access controls.Recent IOCs of Emotet malware are as follows:

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

103.253.75.46 [Thailand]

193.53.245.52 [Turkey]

50.35.17.13 [United States]

64.227.166.13 [United States]

202.79.24.136 [Cambodia]

184.180.181.202 [United States]

185.183.16.47 [Spain]

197.232.36.108 [Kenya]

134.209.144.106 [United States]

115.79.195.246 [Vietnam]

89.25.223.211 [Poland]

139.59.67.118 [India]

81.213.175.132 [Turkey]

51.38.124.206 [Germany]

77.74.78.80 [Russia]

104.131.123.136 [United States]

173.249.6.108 [Germany]

86.98.143.163 [United Arab Emirates]

159.65.6.6 [Singapore]

82.137.29.8 [Romania]

161.0.153.60 [Trinidad and Tobago]

5.196.108.185 [Netherlands]

154.127.113.242 [South Africa]

51.15.7.145 [Netherlands]

181.80.129.181 [Argentina]

216.117.129.6 [United States]

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

1. **[CMTX-P-2930120259] Raccoon Stealer Malware Alert**

Threat Overview:

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

Impacts:

Information Stealer: Primarily used for stealing sensitive information, such as login credentials, cryptocurrency wallets, and browser-stored data.

Modular Malware: Capable of adapting its functionalities and payloads, making it highly versatile.

Dark Web Sales: Data stolen by Raccoon is often sold on the dark web, leading to identity theft and financial fraud.

Prevention and Mitigation:

Browser Hardening: Use browser settings that disable storing credentials and autofill data.

Monitoring Dark Web Activity: Organizations can monitor if their data appears in known dark web marketplaces.

Regular Password Changes: Encourage frequent password updates to reduce the risk of long-term credential exposure.Recent IOCs of Raccoon Stealer malware are as follows:

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

185.244.48.191 [Netherlands]

146.19.173.87 [Seychelles]

88.119.161.19 [India]

176.124.218.249 [Russia]

88.119.171.79 [Netherlands]

178.20.47.114 [Russia]

77.91.77.96 [Germany]

94.228.166.19 [Russia]

5.252.21.236 [Netherlands]

62.113.112.27 [Russia]

65.109.175.35 [Finland]

39.106.247.148 [China]

88.119.161.188 [India]

94.103.88.64 [Russia]

103.251.237.123 [China]

188.215.229.203 [Netherlands]

142.132.225.253 [Germany]

147.45.44.25 [Belize]

91.103.252.193 [Netherlands]

91.103.252.65 [Netherlands]

193.233.132.231 [Malaysia]

45.133.216.170 [Latvia]

62.113.119.179 [Russia]

45.143.223.133 [Netherlands]

77.75.230.93 [Czechia]

8.219.4.230 [Singapore]

94.131.97.157 [Czechia]

45.8.144.187 [Netherlands]

178.20.41.15 [Russia]

149.154.67.234 [Russia]

5.42.67.16 [Czechia]

188.119.112.93 [Netherlands]

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

1. **[CMTX-I-781012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

email.gov.in.ministryofdefenceindia.link

www.email.gov.in.ministryofdefenceindia.link

ministryofdefenceindia.link

\*.ministryofdefenceindia.link

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

1. **[CMTX-I-445012025] Malicious Domains used by Threat Actors**

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

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

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

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

Prevention Measures:

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

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

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

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

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

ail-govs.icu

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

1. **[CMTX-P012025204] FunkSec Ransomware**

Threat Overview:

Threat Campaign: FunkSec Ransomware

FunkSec Ransomware remains a significant threat in the cyber landscape, operating under the Ransomware-as-a-Service (RaaS) model. The cybercriminals associated with FunkSec are reportedly leveraging artificial intelligence (AI) to design and improve their malware tools. They recently launched a data leak site (DLS), where they share breach announcements, a custom-developed DDoS tool, and their ransomware service, which is available for use by other cybercriminals.

The latest update to FunkSec Ransomware, version 1.5, was released on their DLS site, boasting a low detection rate and enhanced capabilities. In addition to the ransomware itself, FunkSec offers several other malicious tools for sale or distribution on their platform:

FDDOS DDoS Tool: A Python-based tool that enables Distributed Denial-of-Service (DDoS) attacks through HTTP or UDP flood methods.

JQRAXY\_HVNC: A tool designed for remote desktop management, automation, and data interaction, consisting of both a server and a client.

Funkgenerate for Password Lists: A tool for smart password generation and scraping, capable of extracting emails and potential passwords from specified URLs while also suggesting new password ideas.

These tools highlight the growing sophistication and multi-faceted approach of FunkSec's operations, making it a significant player in the cybercrime ecosystem.

Threat Type: Ransomware

Severity: High

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.

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

• 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>

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

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P012025204]

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

Indicators of Compromise (IOCs):

HASH:

c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c

66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd

dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac

b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb

5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd

e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22

20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d

dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966

7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603

Domains:

pke2vht5jdeninupk7i2thcfvxegsue6oraswpka35breuj7ttz2erid.onion

7ixfdvqb4eaju5lzj4gg76kwlrxg4ugqpuog5oqkkmgfyn33h527oyyd.onion

funknqn44slwmgwgnewne6bintbooauwkaupik4yrlgtycew3ergraid.onion

funkttkovrk7ctnggbjnthdajav4ggex53k6m2x3esjwlxrkb3qiztid.onion

funkiydk7c6j3vvck5zk2giml2u746fa5irwalw2kjem6tvofji7rwid.onion

funk4ph7igelwpgadmus4n4moyhh22cib723hllneen7g2qkklml4sqd.onion

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