**Cyber Security Advisories**

**Date: 31 December 2024**

1. **CMTX-I-122024874: IOAs of suspicious domains**

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>--------

app.joinindianarmy.in

careerindianairforce.cdse.in

indianairforce.afcat.in

join.indian.navy.in

joinindianarmy.in

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

1. **CMTX-I-563122024: DDNS Domains Targeting Government Organizations**

Dynamic Domain Name System (DDNS) domains are a type of DNS service that allows the automatic updating of a domain's DNS records in real time, typically associated with dynamic IP addresses. DDNS is commonly used for legitimate purposes, such as enabling remote access to devices with changing IPs, hosting servers on non-static networks, or maintaining connectivity for IoT devices.

However, threat actors often exploit the flexibility and anonymity of DDNS services to facilitate malicious activities, particularly for Command-and-Control (C2) infrastructure. By leveraging DDNS domains, adversaries can dynamically change the IP addresses of their C2 servers while retaining the same domain name, making it harder for defenders to block or monitor their operations effectively. DDNS domains are a common hallmark of low-cost, flexible, and evasive C2 infrastructure. Organizations should monitor DDNS traffic closely and implement appropriate security measures to detect and block potential misuse.

New C&Cs as DDNS domains and subdomains are being used by various China based threat-actors to target government entities in Indian cyber space:

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

drdo.gov.in.aboutcase.nl

gov.in.aboutcase.nl

indianarmy.nic.in.aboutcase.nl

mod.gov.in.aboutcase.nl

nic.in.aboutcase.nl

\*.aboutcase.nl

\*.publicvm.com

\*.work.gd

(these domains are currently resolving to IPs:

199.59.243.227

103.215.216.35

5.189.221.41)

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

All sub-domains associated with \*.<parent\_domain>.com (where \* represents any sub-domain under <parent\_domain>.com) should be considered for blocking/monitoring to ensure comprehensive coverage of potential threats originating from these domain.

Kindly take the required actions.

Recommendations:

1. Please note that it is observed, the malwares were making connections to 8.8.8.8 (Google DNS) and other open DNS to perform DNS queries for the above C&C domains. This is a malware TTP to circumvent the organizational DNS or local DNS and their respective blocklists. Hence, all the connections to 8.8.8.8 at port 53 or to open DNS must be strictly monitored. As the C&Cs are DDNS hence IP based blocking will be a short-term measure. Moreover, parent domains needs to be monitored as new sub-domains are being created at regular intervals by the threat actors.

2. Additionally, monitoring all out-bound traffic, especially the traffic that is destined to newly registered domains or belongs to the category: "uncategorized" should be inspected.

3. Various threat actors are known to leverage Dynamic DNS (DDNS) domains as C&C servers. Hence it requested to strictly BLOCK outbound communication to suspected DDNS domains.

1. **CMTX-I-389122024: SpyNote- APT36 Campaign**

Spynote is a mobile Remote Access Trojan (RAT) primarily targeting Android devices. It is designed to gain unauthorized control over infected devices, exfiltrate sensitive data, and spy on victims. Distributed via malicious apps, fake updates, or trojanized applications, Spynote disguises itself as legitimate software to trick users into installation. Once installed, Spynote exploits device permissions to perform malicious activities, including stealing credentials, recording calls, capturing screenshots, activating cameras, and exfiltrating SMS and contact lists. It can also establish persistent Command-and-Control (C2) communication to execute attacker commands.

Tactics, Techniques, and Procedures (TTPs):

> Initial Access: Delivered through phishing campaigns or third-party app stores hosting malicious APKs.

> Execution: Exploits Android device permissions to execute surveillance operations. Can send SMS messages, intercept two-factor authentication codes, or manipulate device settings.

> Persistence: Operates in stealth mode, hiding its icon and running in the background to avoid detection.

> Exfiltration: Steals data (e.g., text messages, call logs, credentials) and sends it to the attacker's C2 server. Enables real-time spying via the device’s microphone or camera.

Prevention Measures:

> Avoid downloading apps from untrusted or unofficial sources.

> Use Android's "Google Play Protect" and enable app verification.

> Grant apps only the minimum required permissions.

> Deploy mobile security solutions to detect and block malware.

> Keep Android devices and apps up to date with the latest security patches.

> Train users to recognize phishing attempts and suspicious application behavior.

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

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

182.180.104.47

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

1. **CMTX-I-389124874: AllaKore RAT Malware**

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

Key Characteristics of Pakistan based SideCopy Threat Actor

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

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

> Remote Access

> Credential Harvesting

> Data Exfiltration

> Persistence Mechanisms

Prevention Measures:

> Macro-enabled files pose a significant security risk as they can contain malicious code designed to compromise your system or steal sensitive information. Common file extensions that may include macros include .docm, .dotm, .xlsm, .xltm, .pptm, .potm, .accde, .accdr, .sldm, .ppam, and .xlam. Do not open files with these extensions unless you are certain of the sender’s identity and the file’s purpose.

> Additionally, avoid clicking "Enable Content" or "Enable Macros" unless sure the file is safe.

> Always verify the source and inspect suspicious files carefully before opening or enabling any potentially harmful features.

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

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

> Multi-Factor Authentication (MFA) for emails

> Encrypt sensitive data to protect it in case of exfiltration

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

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

microsoftstores.zapto.org

\*.zapto.org

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

1. **CMTX-P-122024724: 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-122024724

Indicators of Compromise (IOCs):

IP Addresses :Port

43.246.210.196

104.167.16.95

103.152.254.152

117.50.213.101

45.76.209.205

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

1. **CMTX-P-122024714: 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-122024714

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

Indicators of Compromise (IOCs):

IP Addresses: Port

154.19.85.71

207.148.126.75

210.16.103.3

95.179.222.27

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

1. **CMTX-P122024545: Active Exploitation of a Critical Flaw**

ALERT BRIEF:

It has been reported that a critical vulnerability tracked as CVE-2024-53677 is being exploited by cybercriminals and affecting Apache Struts. Exploitation attempts using various malware families and techniques such as path traversal and authentication bypass are being used for exploitation.

File upload parameters can be changed by an attacker to allow path traversal, which in certain cases may result in the uploading of a malicious file that can be used to carry out Remote Code Execution.

The threat actor might also be able to upload random payloads to vulnerable systems, which they might then use to execute instructions, steal information, or download other payloads for further exploitation.

AFFECTED VERSIONS:

Struts 2.0.0 through Struts 2.3.37 (End of life)

Struts 2.5.0 through Struts 2.5.33 (End of Life)

Struts 6.0.0 through Struts 6.3.0.2

Threat Type: Vulnerability

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

1. **CMTX-I-309124874: IOCs of China-based Malware Campaign**

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

Tactics, Techniques, and Procedures (TTPs)

> Phishing and Social Engineering: Attackers frequently use phishing emails or social engineering tactics to trick users into downloading malware or revealing sensitive information.

> Exploiting Vulnerabilities: Malware may exploit known software vulnerabilities to gain access to systems. This includes zero-day exploits that target unpatched software.

> Remote Access Trojans (RATs): Many Chinese malware variants include RATs, which allow attackers to control infected systems remotely, facilitating data exfiltration and further attacks.

> Command and Control (C2) Communication: Infected devices often communicate with C2 servers to receive instructions or send stolen data. This communication can be obfuscated to evade detection.

> Use of Malware Kits: Attackers may employ sophisticated malware kits, which simplify the creation of malware and the exploitation of vulnerabilities, making attacks more efficient.

> Fileless Malware: Some malware variants operate without writing files to disk, making detection more challenging. They reside in memory and execute scripts to carry out malicious activities.

Prevention Measures

> Regular Software Updates: Keep all software, including operating systems and applications, up to date to mitigate the risk of exploitation through known vulnerabilities.

> Use Security Software: Install reputable antivirus and anti-malware solutions to detect and block threats. Ensure that the software is regularly updated.

> Educate Users: Train employees on recognizing phishing attempts and suspicious links or attachments. Awareness can significantly reduce the risk of infection.

> Network Segmentation: Implement network segmentation to limit the spread of malware and protect sensitive information by isolating critical systems.

> Regular Backups: Maintain regular backups of important data. In the event of a ransomware attack or data breach, backups can aid in recovery without paying a ransom.

> Employ Firewalls: Use firewalls to monitor and control incoming and outgoing network traffic, reducing the risk of unauthorized access.

> Intrusion Detection Systems (IDS): Implement IDS to monitor network traffic for suspicious activity and potential intrusions.

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

115.61.168.143

103.238.227.183

115.61.169.139

103.238.225.248

182.114.110.170

116.206.178.67

howtotopics.com

thelocaltribe.com

councilofwizards.com

goclamdep.net

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

1. **CMTX-I-626124874: IOAs of suspicious domains**

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>----------

sci-gov.info

assamrifles.gov.in.lazetoys.com

maharashtra.gov.in.studentemarks.in

rmc.gov.in.webstatarchive.com

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

1. **CMTX-P-VUL-1220243314: 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:  Prominent\_CVE\_List.pdf

SHA256: 37cdf3b4fc669227225b8882d8d0e80bfd05158268f0b90de1b919ce0a07b79a

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

1. **CMTX-P-122024734: 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

216.238.106.150

103.82.143.13

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

1. **CMTX-P-122024248 : HiatusRAT Targeting IoT Devices**

Threat Overview

HiatusRAT is a sophisticated Remote Access Trojan (RAT) that has evolved significantly since its emergence in July 2022. Initially targeting outdated business-grade routers/ network edge routers, it now focuses on IoT devices, particularly Chinese-branded web cameras and DVRs. Its capabilities include remote control, passive traffic collection, execute remote control commands, covert command-and-control functions, convert infected devices into SOCKS5 proxies for attackers.

State actors are known to exploit compromised devices as part of anonymization or Operational Relay Box (ORB) networks. These covert infrastructures obscure the origin and destination of malicious traffic. Such mesh networks often consist of compromised devices or actor-controlled virtual private servers (VPS), utilizing multiple hops between entry and exit points to complicate tracking and attribution efforts.

1. Impacts:

o Remote device takeover and control

o Unauthorized access to surveillance systems

o Potential network compromise

o Data exfiltration risks

2. Threat Type: Remote Access Trojan (RAT)

3. Severity: High

4. Distribution Methods:

o Scanning campaigns targeting vulnerable IoT devices

o Exploitation of unpatched vulnerabilities

o Telnet access exploitation

o Brute force attacks using tools like Medusa

Capabilities:

• Remote device control and takeover

• Passive traffic collection

• Functions as covert C2 infrastructure

• Reconnaissance capabilities

• SOCK Proxy servers / relay traffic systems

Attack Methods:

• Exploits multiple CVEs targeting IoT devices

• Uses publicly available tools (Ingram for scanning, Medusa for brute-forcing)

• Targets devices with telnet access

• Exploits weak vendor-supplied passwords

Mitigation and Recommendations:

• Limit and Isolate IoT Devices: Restrict or isolate vulnerable devices from the main network. `Replace Unsupported / End of Life devices.

• Regular Patching and Updates: Apply firmware, OS, and software patches immediately. Remove unsupported devices.

• Strong Passwords: Avoid default passwords; use unique, complex passwords and enforce policies and Audit administrative accounts

• Multi-Factor Authentication: Implement wherever possible.

• Security Monitoring: Log network activity and set up alerts for unusual behavior.

• Network Segmentation: Segment networks to reduce risk and exposure and Scan and mediate unnecessary open ports

Indicators of Compromise (IOCs):

• Targeted TCP Ports: 23, 26, 554, 2323, 567, 5523, 8080, 9530, 56575

• Scanning tools: Ingram (webcam-scanning tool), Medusa (brute-force tool)

• Targeted devices: Xiongmai and Hikvision devices with telnet access

1. **CMTX-P-122024258: Advisory on Ransomware As a Service continuous exploitation of "Bring Your Own Vulnerable Driver" (BYOVD) Techniques for Defense Evasion**

Key Observations:

• Adoption by Ransomware Groups: Analysis of recent incidents has revealed widespread use of BYOVD techniques by ransomware groups for defense evasion, persistence, and privilege escalation. Ransomware groups such as BlackByte, Qilin, Embargo, DragonForce, Akira, Kassieka, and RansomHub have been observed implementing BYOVD to bypass security tools and escalate privileges on compromised systems.

• Exploitation of Vulnerable Drivers: Attackers typically identify signed drivers with known vulnerabilities, which can be easily obtained from online repositories like LoLDrivers.io. These drivers are then deployed onto victim systems, either as part of a larger attack chain or bundled with malicious payloads, to exploit their vulnerabilities and gain elevated privileges.

Recent Attacks Utilizing BYOVD:

• Kasseika (January 2024): Exploited a vulnerable driver, viragt64.sys (part of the VirIT antivirus software), to disable security processes and facilitate the ransomware execution.

• Akira (March 2024): Abused the zamguard64.sys driver from Zemana Anti-Malware to disable EDR at the kernel level. Akira has evolved its tactics, focusing on data exfiltration while continuing to leverage BYOVD techniques.

• Qilin (July 2024): Used the amsdk.sys driver (CVE-2024-1853) to terminate processes and evade security measures. This attack was part of the group’s double-extortion approach.

• BlackByte (July 2024): Deployed a series of vulnerable drivers (RtCore64.sys, DBUtil\_2\_3.sys, zamguard64.sys, gdrv.sys) to bypass security defenses and facilitate encryption.

• RansomHub (August 2024): Exploited a vulnerable driver through a new tool, EDRKillShifter, to disable security tools and escalate privileges before deploying ransomware.

• Embargo (October 2024): Used Sysmon64.sys as part of an attack that leveraged safe mode and BYOVD techniques to disable EDR before ransomware deployment.

Why is BYOVD Concerning?

The increasing use of BYOVD techniques is concerning as it allows attackers to bypass even advanced defenses like Endpoint Detection and Response (EDR) tools. It enables them to:

• Gain kernel-level access: Exploiting vulnerable drivers enables attackers to perform privileged actions on a victim’s system, often undetected by traditional security tools.

• Disable security tools: Malicious drivers can disable critical processes related to security and defense mechanisms, leaving systems more vulnerable to additional attacks.

• Establish persistence: Once deployed, these vulnerable drivers can remain on systems, providing attackers with ongoing access.

1. **CMTX-P-122024744: 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

38.54.87.113

103.51.144.19

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

1. **CMTX-P-122024754: 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

45.139.225.108

8.209.221.211

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

1. **CMTX-I-670124874: 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>----------

www.email.gov.in.indiandefence.link

email.gov.in.indiandefence.link

\*.indiandefence.link

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

1. **CMTX-I-954122024: CrimsonRAT- APT36 campaign**

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

Common Features of APT36 Threat Actor:

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

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

  > Remote Access

  > Credential Harvesting

  > Data Exfiltration

  > Persistence Mechanisms

Preventive Measures:

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

  > Monitoring and logging to detect unusual activities indicating a compromise

  > Multi-Factor Authentication (MFA) for emails

  > Encrypt sensitive data to protect it in case of exfiltration

Recent C&C server of CrimsonRAT malware deployed by this threat actor and the domain hosting the malicious file are as follows:

- ---------- < C&C and Malware Hosting>--------

sub172.duckdns.org

209.145.52.172

beycloud.com

- ---------- </C&C and Malware Hosting>---------

1. **CMTX-I-511122024: 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>-------

170.64.175.56

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

1. **CMTX-I-338122024: Malware Targeting Government Officials via Spear-Phishing**

Spear-phishing is a highly targeted cyber-attack technique where malicious emails are crafted to appear legitimate and deceive specific individuals or organizations. Unlike generic phishing campaigns, spear-phishing emails are tailored using personal or organizational details, making them more convincing and harder to detect. Once the victim interacts with the email, the attacker often deploys malware that establishes deep persistence within the compromised system and network.

How Malware Spreads via Spear-Phishing Emails?

> Malicious Attachments: The email may include files that appear harmless (e.g., invoices, reports) but contain malware payloads.

> Embedded Links: URLs that direct victims to malicious websites, leading to automatic malware downloads or credential harvesting.

> Execution of Malware: Once executed, the malware begins to collect information, escalate privileges, and establish communication with the attacker’s Command and Control (C2) server.

> Establishing Deep Persistence: Registry Modifications, Scheduled Tasks, Windows service, Cron jobs on linux machines.

Prevention Methodology

1. Avoid Clicking on Spear-Phishing Emails

> What needs to be Checked:

>> Unexpected Requests: Emails asking for urgent action, such as fund transfers or sharing sensitive information.

>> Suspicious Sender Addresses: Look for slight misspellings or inconsistencies in the sender’s email address.

>> Unusual Attachments or Links: Be wary of unexpected file formats or shortened URLs.

> What needs to be Done:

>> Hover over links to view the actual URL before clicking.

>> Verify the email sender by contacting them through known, official channels.

>> Report suspected phishing emails to your organization’s IT or security team.

2. Unhide File Extensions

> Many spear-phishing attacks use hidden file extensions to disguise malware (e.g., report. pdf. exe may appear as report. pdf).

> How to Unhide Extensions:

>> On Windows:

Open File Explorer.

Click on the View tab in the ribbon menu.

Check the box for File name extensions. This will display extensions for all files.

>> On macOS:

Open Finder.

Go to Finder Preferences.

Under the Advanced tab, check the option for Show all filename extensions.

Recent IOCs of malware targeting government officials via spear-phishing emails are as follows:

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

Network-based

updates.biossysinternal.com

biossysinternal.com

\*.biossysinternal.com

egovservice.in (Compromised Domain)

File-based [SHA1 Hash]

55a498a344aa07756ac834528d1c208d8051232e

b22f0923d8675131dd3bb12a10813db9dccdcfda

73e20089de1d25d44cfc9db4b3076eba0e90c48a

a5bf390da990cb962ff046b1cecc76d76815fc5f

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

1. **CMTX-P-122024764: 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 side-loading techniques and exploits vulnerabilities in software such as Microsoft Office IME binary or Microsoft Exchange Server. It can also be 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

45.32.51.228

95.179.156.122

46.17.41.154

185.167.62.10

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

1. **CMTX-I-512122024: 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>------------

onlineppa.tn.gov.in.web-download.online

gov.in.web-download.online

web-download.online

\*.web-download.online

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

1. **CMTX-I-256122024: 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>------------

mail-section.in

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

1. **CMTX-P-122024804: 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

156.244.7.170

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

1. **CMTX-P-122024794: 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

45.76.157.243

47.108.134.116

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

1. **CMTX-P-122024844 : 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.

Indicators of Compromise (IOCs):

IP Addresses :Port

118.194.249.212

1. **CMTX-P-122024824 : 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

149.28.148.15

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