**Cyber Security Advisories**

**Date: 19-04-2024**

1. **CMTX-P042024025 Hacktivist Group: R00TK1T ISC**

ALERT BRIEF:

The threat actor known as R00TK1T ISC is a self-proclaimed pro-Israeli and pro-Russian hacktivist group. R00TK1T employs various tactics such as distributed denial-of-service (DDoS) attacks, website defacements, and claims of database compromises or leaks. Recently R00TK1T has announced on its telegram channel for shifted its focus to India.

Mapping of TTPs used by these actors on MITRE ATT&CK Matrix:-

T1491 (Defacement)

T1498 (Network Denial of Service)

Attack Vectors

Website Defacement

DDoS

Hacktivism

Account Compromise

Previous Hacktivist Alert References:-

[CMTX-P-102023633 [Early Warning Probable hacktivist campaigns against Indian Cyber Space, TLP: AMBER October 27, 2023

[CMTX-P-102023524 [Early Warning Probable hacktivist campaigns against Indian Cyber Space, TLP: AMBER October 20, 2023

[CMTX-P-102023523 [Early Warning Probable hacktivist campaigns against Indian Cyber Space, TLP: AMBER October 11, 2023

[CMTX-P12202406 [Early Warning Probable hacktivist campaigns against Indian Cyber Space, TLP: AMBER Dec 08, 2023

[CMTX-P01203403 Hacktivist campaigns against Indian Cyber Space, TLP: AMBER Jan 29, 2024

[CMTX-P022024215 Hacktivist Campaigns against Indian Cyber Space, TLP: AMBER Feb 22, 2024

[CMTX-P032024145 Hacktivist Campaigns against Indian Cyber Space, TLP: AMBER March 14, 2024

[CMTX-P032024175 Hacktivist Group: Anon Collective, TLP: AMBER March 18, 2024

Best Practices and Recommendation for Mitigation against Website Defacement and DDOS attack is provided below.

Mitigation measures against Website Defacement:

• Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation and unknown connections in the network traffic. Enforce MFA for all users and on all VPN connections and regularly review, validate, or remove privileged accounts.

• Use the latest and updated versions of web server / applications server applications, Apply appropriate updates/patches on the OS and Application software as and when available. Always apply the patch from the official channel.

• Strict enforcement policies on popular Content Management systems (CMS) such as regular patching of CMS applications and its plug-ins such as file mangers, disabling of unused plugins, 2- Factor authentication, adequate ACLs, File type & size Upload limit etc.

• Periodically check the web server directories for any malicious/unknown web shell files, remove it as and when noticed. If found/ observed any such malicious activity, report the incident to CERT-In Incident Response Help Desk immediately. (Email: incident@cert-in.org.in)

• Enforce strict control and monitoring of Windows Native applications such as command-line, PowerShell, WinRM, Windows Management Instrumentation (WMI), and Distributed Component Object Model (DCOM).

• Enable and maintain logs of different devices and servers [Webserver Access/Error logs, Application/DB/ Firewall/IDS/FTP logs and maintain the same for all the levels. Preserving of these logs help in analyzing the incidents and known the TTP of actors.

• Use firewalls to create a buffer zone between the Internet (and other un-trusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorized protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Employ effective processes for managing changes to avoid workarounds.

• Check for unnecessary connectivity towards Content Delivery Networks, as malware are known to tunnel the connection towards these domains to hide their traffic and towards DDNS / free top level domains. Regular auditing of the failed connection attempts from DNS logs, proxy logs and to successful connection towards unknown domains. Some of the attacks use unconventional usage of DNS queries to exfiltrate interact with the attackers [DNS TXT Records.

• Conduct complete security audit of web application, web server, and database server periodically and after every major configuration change and plug vulnerabilities found. Services of CERT-In empanelled auditors may be availed. (Refer Cyber security Assurance section on website of CERT-In https://www.cert-in.org.in/).

Measures for prevention of Denial of Service (DoS/DDoS) attacks:

1. Measures for detection of attacks

• Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

• Enable adequate logging mechanisms at perimeter level, server, and system level and review the logs at frequent intervals.

• Continuously monitor the network activities & server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.

• Preserve all logs indicating type of attack and attack sources.

2. Protection measures against Distributed Denial-of-Service (DDoS)

• Thoroughly scan the network and online applications and plug any existing vulnerability in the network devices, Operating Systems, Server software and application software and apply latest patches/updates as applicable.

• Consider using a third-party DDoS protection service that can help detect and mitigate attacks, often using a combination of automated and manual techniques

• Employ defence-in-depth strategies: emphasize multiple, overlapping and mutually supportive defensive systems to guard against single point failures in any specific technology and protection method.

• Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common attack tools.

• Sudden surge in inbound traffic to any critical server or services, such as ICMP floods, UDP/TCP flood etc. could be due to Distributed Denial of Service (DDoS) attacks. If such attacks are observed, implement appropriate response measures in coordination with Internet Service Provider (ISP).

• Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services.

• To counter attacks on applications, check the integrity of critical application files periodically and in case of suspicion of attack restore applications and content from trusted backups.

• Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.

• In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

• Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.

• Use CAPTCHA challenges to verify that traffic is coming from real users rather than bots, preventing automated attacks

3. Protection Mechanisms against Hack-and-Leak

• Conduct regular vulnerability assessments to identify potential weaknesses in your systems and networks that could be exploited by hacktivists.

• Monitor social media channels for any threats or activity related to hacktivism.

• Implement secure configuration settings on systems and applications to make it more difficult for hacktivists to penetrate them.

• Encrypt sensitive data both in transit and at rest to protect against data interception and theft.

• Regularly backup important data to minimize the impact of a hack-and-leak attack.

• Limit the number of external-facing services to reduce the attack surface and make it more difficult for hacktivists to find vulnerabilities.

1. **CMTX-P0420240105 CVE-2024-3094: Critical Vulnerability Affecting XZ Utils Data Compression Library**

ALERT BRIEF:

CVE Number: CVE-2024-3094

CVSS-8.4

Targeted Product-XZ Utils Data Compression Library (versions 5.6.0 and 5.6.1)

According to the reports, it has been found that an Embedded Malicious Code Vulnerability (CVE-2024-3094) is affecting XZ Utils Data Compression Library (mainly in linux Distribution).

A backdoor is installed in the vulnerable versions, which allows attackers to execute arbitrary code and gives full access of the affected systems to the unauthorised users.

Vulnerable Versions- 5.6.0 and 5.6.1

Recommendations:

\* It is recommended for the developers and users to downgrade to an uncompromised version—such as XZ Utils 5.4.6

- - - - - ----------------------------------------ALERTEND------------------------------------------------------

1. **CMTX-I-025042024 GavaRAT - APT36 campaign**

CERT-In has identified GavaRAT which is targeting both Windows and Linux based systems. Final payload is JAVA based RAT whose first stage is a JavaScript file which is being spoofed as PDF document. Upon JavaScript file execution, a decoy file and the final payload gets downloaded. The initial stager is being sent via email links/attachments.

It is not necessary for the victim to have Java environment on the system, as the final payload includes the Java Runtime Environment. Cloud storage service (such as OneDrive) is being used to host the stager, payload and decoy file.

The malware has the following capabilities:

- File exfiltration from disk and portable media

- Remote desktop

- C&C communication for further payload deployment

The IOCs of this malware are as follows:

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

89.117.58.192

https://indianmailhub.xyz/mar/army/nc/briefcase.php

https://indianmailhub.xyz/

folder with name "java", and

file "java.zip" are created at path %PROGRAMDATA%

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

Recommendations:

- Connection to the IOCs should be blocked.

- Network DLP could be deployed, which will monitor and control data transfer over the network. Thereby, preventing sensitive information from being uploaded to external servers or cloud storage.

- Endpoint DLP could be installed on user endpoints to monitor and restrict the transfer of files and sensitive information out of the organization's network. This should be regardless of whether the transfer is via web, cloud services, or external devices.

1. **CMTX-P042024626 QuasarRAT Malware ALERT 47**

ALERT BRIEF:  
  
Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has capability of capturing screenshots, Key logger, gather System Information, remote Shell and Command execution, reversing proxy, Managing tasks and files, Configuring and building client executables.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
IP ADDRESSES: PORTS             Last Seen      Country Code  
  
139.180.210.214:509    29-08-2021    SG  
143.110.191.139:8080    02-04-2024    IN  
41.233.131.213:17    01-04-2024    EG  
45.32.247.39:1604    12-06-2020    AU  
95.214.53.95:57896    20-07-2023    PL  
175.42.16.2:4784    02-04-2024    CN  
154.39.239.150:8080    26-11-2021    SG  
161.97.162.173:4782    02-04-2024    DE  
181.162.133.144:8080    02-04-2024    CL  
200.109.22.21:443    01-04-2024    VE  
91.92.251.216:7000    02-04-2024    NL  
217.196.98.103:4782    02-04-2024    US  
185.196.10.233:4782    30-03-2024    CH  
191.82.195.251:2000    01-04-2024    AR  
147.45.41.231:1337    02-04-2024    AT  
102.117.130.51:8080    01-04-2024    MU  
194.68.32.11:443    01-04-2024    NO  
103.211.56.154:14782    27-03-2024    IN  
190.199.242.191:443    17-02-2016    VE  
103.117.102.24:10298, 10297    01-04-2024    JP  
102.117.116.119:5061, 8181, 6699    02-04-2024    MU  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.  
  
RECOMMENDATIONS  
  
- - - - - - - - - - - - - - - Recommend to monitor connection towards the mentioned IP addresses.  
- - - - - - - - - - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024945 PLUGX RAT ALERT 111**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. 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. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

IP Address: Port : Country Code

156.245.13.9:8080, 443, 80:HK

156.245.13.5:8080, 443, 80:HK

156.245.13.12:8080, 80:HK

218.189.80.44:80:HK

141.98.212.75:443:HK

91.225.217.23:80:MD

103.40.200.212:1883:IN

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

1. **CMTX-P042024805 SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as 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)

A list of Indicators of compromise is provided below for your action side.

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

IP Address: Port : Country Code

146.70.214.104:8080, 443:BR

141.255.164.10:443:CH

156.59.51.21:443:TH

103.5.184.182:8443:IN

45.147.26.253:443, 80:HK

158.247.211.154:8080, 443, 80:KR

38.54.79.167:80:US

139.180.208.107:443, 53, 44444, 80:SG

194.124.213.203:443:NL

45.146.222.12:8080, 443:RS

45.76.150.130:443:SG

66.42.50.178:443:SG

38.60.249.194:443:DE

128.14.105.154:443:US

149.28.62.7:443:US

114.143.185.84:8443:IN

185.81.114.132:443:NL

38.60.196.212:443:GB

45.76.252.128:443:US

158.247.211.154:80:KR

95.179.240.31:443:DE

139.59.40.249:80:IN

27.254.164.221:TH

192.46.212.148:IN

45.142.155.110:JP

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

1. **CMTX-P042024045 DinodasRAT Malware**

ALERT BRIEF:

It has been reported that a Linux version of a commonly known malware "DinodasRAT a.k.a. XDealer" (written in c++) is found to be affecting  Red Hat and Ubuntu systems. Its capabilities include hiding files in the directory, stealing information, receiving commands, and updating itself. It can also give attackers a remote shell to the system enabling complete control over the infected machine for data exfiltration and espionage. Once executed, DinodasRAT ensures its persistence on the host by utilizing SystemV or SystemD startup scripts depending on the victim's Linux distribution. C2 Communication occurs via TCP or UDP, while the malware utilizes the Tiny Encryption Algorithm (TEA) in CBC mode to cipher and decipher the data.

MITRE ATT&CK Identifiers:

T1041 (Exfiltration Over C2 Channel)

T1027 (Obfuscated Files or Information)

T1082 (System Information Discovery)

T1505 (Server Software Component)

T1005 (Data from Local System)

T1037 (Boot or Logon Initialization Scripts)

T1055 (Process Injection)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP ADDRESS:

199.231.211.19

HASHES:

decd6b94792a22119e1b5a1ed99e8961

8138f1af1dc51cde924aa2360f12d650

DOMAIN:

update.centos-yum.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P042024055 Critical Vulnerability (CVE-2024-2879) Impacting LayerSlider WordPress Plugin**

ALERT BRIEF:

CVE-2024-2879

CVSS- 9.8

An SQL Injection vulnerability tracked as CVE-2024-2879 is reportedly found to be impacting the LayerSlider( used for visual web content editor, a graphic design software, and a digital visual effects that allows users to create animations and rich content for their websites) plugin for WordPress. This vulnerability allows unauthenticated attackers to change additional SQL queries into already existing queries to extract sensitive information from the database.

Affected Versions- Versions from 7.9.11 through 7.10.0.

Patched Version- 7.10.1

RECOMMENDATIONS

\* Apply latest vendor specified patch ASAP to mitigate any potential threats.

REFERENCE:

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/layerslider/layerslider-7911-7100-unauthenticated-sql-injection

1. **CMTX-P042024018 REDLINE STEALER MALWARE**

ALERT BRIEF:

RedLine Stealer is a .NET-based infostealer malware that is capable of harvesting information from browsers such as saved credentials,

autocomplete data and credit card information. It is also utilized in facilitating attacker to drop another payload or launch a hidden command shell on victims' machine.

MITRE ATT&CK Identifiers

T1059 (Command and Scripting Interpreter)

T1543 (Create or Modify System Process)

T1053 (Scheduled Task/Job)

T1027 (Obfuscated Files or Information)

T1003 (OS Credential Dumping)

T1055 (Process Injection)

T1140 (De obfuscate/Decode Files or Information)

T1547 (Boot or Logon Auto start Execution)

A list of Indicators of compromise is provided below for the necessary action.

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

IP Ports    Country Code

142.202.242.190:81,US

147.45.44.50:15070,CH

195.20.16.134:46690,NL

212.224.86.223:8056,DE

45.137.22.188:55615,NL

5.42.65.67:48396,UA

5.42.81.51:20482,SE

77.223.100.247:3000,RU

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

RECOMMENDATIONS

- - - - - - - Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024065 UNAPIMON Malware**

LERT BRIEF:

MALWARE-UNAPIMON

ASSOCIATED THREAT ACTOR- EARTH FREYBUG, APT-41 [a.k.a. Axiom, Brass Typhoon (formerly Barium), Bronze Atlas, HOODOO, Wicked Panda, and Winnti

According to the reports, a new DLL based malware "UNAPIMON" written in C++ is being actively used by Chinese state-sponsored threat group "Earth Freybug" (a subgroup of APT-41). The attack flow employs two key techniques, ie, DLL hijacking and API unhooking. The attack chain begins with a legitimate executable, vmtoolsd.exe, associated with VMware Tools. The attackers inject unknown code into vmtoolsd.exe which triggers the execution of a remote scheduled task using schtasks.exe. A pre-deployed batch file named cc.bat is executed on the remote machine to gather system information. The second cc.bat file leverage the SessionEnv service to load a non-existent library, side-loading a malicious DLL.

MITRE ATT&CK Identifiers:

T1574 (Hijack Execution Flow)

T1082 (System Information Discovery)

T1574.002 (DLL Side-Loading)

T1053 (Scheduled Task/Job)

T1055 (Process Injection)

T1059 (Command and Scripting Interpreter)

T1556 (Modify Authentication Process)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASH:

62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

RECOMMENDATIONS:

\* Block attachments of file types:[exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf. Ensure to Scan all software downloaded from the Internet prior to executing.

\* Systems having an antivirus and a malware protection program on it and making sure they are always up to date. Systems and installed applications being fully patched and updated.

\* Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints. Perform regular backup of all the critical information to minimize the loss.

\* All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software.

- - - - - - --------------------------------------ALERTEND------------------------------------------------------

1. **CMTX-P042024626 QuasarRAT Malware ALERT 48**

ALERT BRIEF:

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

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

IP ADDRESSES: PORTS Last Seen Country Code

1.9.177.252:9876 04-04-2024 MY

45.13.225.104:4783 04-04-2024 DE

202.143.110.210:4782 04-04-2024 VN

47.76.214.226:9443 05-04-2024 HK

143.92.56.46:4782 14-02-2021 HK

45.63.49.44:100 04-10-2016 US

124.222.109.145:4782 04-04-2024 CN

111.92.240.15:4782 04-04-2024 HK

94.156.8.44:4787 03-04-2024 GB

212.23.222.46:1337 05-04-2024 PL

216.73.158.60:4782 05-04-2024 JP

91.92.253.176:4782 04-04-2024 NL

167.86.115.184:443 04-04-2024 DE

189.78.187.139:5000 10-03-2018 BR

181.214.147.29:4782 04-04-2024 LT

91.92.252.119:4782 05-04-2024 NL

217.63.234.90:1313 02-04-2024 NL

45.128.96.227:4782 04-04-2024 BE

124.223.48.86:4285 04-04-2024 CN

95.141.47.18:8080 15-07-2019 IT

195.128.248.208:4782 04-04-2024 UA

185.225.191.26:1337 05-04-2024 PL

84.253.244.136:4782 05-04-2024 FI

47.13.251.179:4782 05-04-2024 US

2.47.94.129:4782 04-04-2024 IT

181.162.159.238:8080 04-04-2024 CL

68.178.203.123:5552 03-04-2024 US

187.59.75.101:4782 04-04-2024 BR

103.200.124.195:4782 05-04-2024 HK

106.240.105.174:8090 04-04-2024 KR

139.28.37.14:4782 10-09-2020 UA

45.132.239.243:8088 28-12-2016 HK

143.92.56.60:4782 05-04-2024 HK

41.216.183.185:4782 04-12-2023 NL

45.132.239.244:8088 04-04-2024 HK

45.132.239.245:8088 04-04-2024 HK

185.113.143.66:1337 04-04-2024 PT

45.132.239.246:8088 04-04-2024 HK

196.117.10.2:8085 04-04-2024 MA

77.105.219.98:443 04-04-2024 SE

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

1. **CMTX-P042024905 SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as 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)

A list of Indicators of compromise is provided below for your action side.

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

IP Address: Port : Country Code

38.60.134.143:443:FR

38.60.191.159:443:ID

164.215.103.248:443:AZ

70.34.212.229:443:SE

199.247.23.228:443:DE

165.154.18.212:3001:JP

45.32.151.219:443:FR

94.131.10.70:443:PT

38.60.134.143:443:FR

70.34.212.229:443:SE

38.60.191.159:443:ID

45.32.151.219:443:FR

164.215.103.248:443:AZ

94.131.10.70:443:PT

139.99.50.68:443:SG

199.247.23.228:443:DE

165.154.18.212:3001:JP

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

1. **CMTX-P042024955 PLUGX RAT ALERT 112**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. 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. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

IP Address: Port : Country Code

194.124.33.123:443:CH

64.44.57.14:80, 443, 21:US

185.126.225.74:443:NL

146.66.212.82:443:RO

192.54.57.122:443:NL

38.89.72.253:443:US

45.80.208.142:443:KZ

167.179.72.177:443:JP

103.230.152.163:8080:IN

35.74.172.53:443:JP

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

.

1. **CMTX-P042024105 SectopRAT**

ALERT BRIEF:

SectopRAT, aka ArechClient2, is a .NET RAT with numerous capabilities including profiling victim systems, steal information such as browser and crypto-wallet data, and launch a hidden secondary desktop to control browser sessions. Additionally, it has several anti-VM and anti-emulator capabilities. Recently a malvertising campaign is being observed in which attacker uses the typo squatted URL of legitimate site to host the SectopRAT malware payload on it.

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

IP

45.141.87.216

Domain

nordivpn.xyz

besthord-vpn.com

HASH

e9131d9413f1596b47e86e88dc5b4e4cc70a0a4ec2d39aa8f5a1a5698055adfc

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

1. **CMTX-P042024095 VIETNAM BASED THREAT ACTOR CORALRAIDER**

ALERT BRIEF:

It has been reported that a Vietnamese-origin threat actor named "CoralRaider” is found to be targeting various nations with the aim to exfilterate credentials, financial data, and control over social media and business accounts.One of its capabilities include establishing persistence on the victim's machine. The initial attack vector starts by distributing malicious Windows shortcut files (LNK) to the victim's system which then triggers a powershell script to download and execute a "RotBot" malware (a customized variant of QuasarRAT) and XClient stealer as payloads that helps to establish C2 connection via Telegram bot. They also leverage uncommon living-off-the-land binaries (LoLBins), including Windows Forfiles.exe and FoDHelper.exe

MITRE ATT&CK Identifiers:

T1056 (Input Capture)

T1056.001 (Keylogging)

T1041 (Exfiltration Over C2 Channel)

T1005 (Data from Local System)

T1548 (Abuse Elevation Control Mechanism)

T1087 (Account Discovery)

T1059 (Command and Scripting Interpreter)

T1003 (OS Credential Dumping)

T1036 (Masquerading)

T1082 (System Information Discovery)

T1027 (Obfuscated Files or Information)

T1213 (Data from Information Repositories)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASH:

0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0

9bf684b010e4ec314d697acfac78c71ec24ba5f6e2c09b3be623ec62056aed02

d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e

c29732d898dcf116f40eea3845d4e25a240e5840378985c7f192e0443a51a228

8d200892e4f1e68373e58e7cd7119fe26769fcf609636adc727df09f2377d1c2

2c4ed97859060ea6ac5a8c2f605debf98257a96f0f3d2ddfaeb066f59a86d4af

c84ff4fb6549c36ca0028e84ea8292ee3ae438254cddd63ef3d9ea769e0a1dfd

19055fb87b9a98a75544a533ec4f14f36a09a130219b8a33a13cb6073751ff39

1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3

020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34

28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f

42654394f29f2e8db878fc4fd1c59e41afcd0add3b93f7d2f47ea3295b2bc643

075091793768885977c29a41a0ac591340ebafab26d2a65ce1dccb53997485a1

e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f

77acb85a28e79dc6479798c024282ddd54977dbff6ce40eb439b2a06ce9cb542

b2fd04602223117194181c97ca8692a09f6f5cfdbc07c87560aaab821cd29536

a3299ecee7b3f06ca106f4c5b62bf1e0f28f227df71488583d2077c7e3ee01c2

de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4

93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c

4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643

IPs

199.34.27.196

14.225.210.98

139.99.23.9

51.79.208.192

14.225.210.222

14.225.210.97

14.225.210.209

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

RECOMMENDATIONS:

\* Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

\* Restrict execution of PowerShell /WSCRIPT in enterprise environment. Ensure installation and use of latest version of PowerShell, with enhanced logging enabled, Script block logging, and transcription enabled.

1. **CMTX-P042024115 Rilide Stealer**

ALERT BRIEF:

 The Rilide stealer disguised as a legitimate Google Drive extension and monitor browsing history, capture screenshots, and inject malicious scripts to steal funds from cryptocurrency exchanges.

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

HASH

2d6829e8a2f48fff5348244ce0eaa35bcd4b26eac0f36063b9ff888e664310db

a7c07d2c8893c30d766f383be0dd78bc6a5fd578efaea4afc3229cd0610ab0cf

e394f4192c2a3e01e6c1165ed1a483603b411fd12d417bfb0dc72bd6e18e9e9d

021657f82c94511e97771739e550d63600c4d76cef79a686aa44cdca668814e0

92751fd15f4d0b495e2b83d14461d22d6b74beaf51d73d9ae2b86e2232894d7b

32a097b510ae830626209206c815bbbed1c36c0d2df7a9d8252909c604a9c1f1

c665ff2206c9d4e50861f493f8e7beca8353b37671d633fe4b6e084c62e58ed9

0ed3b92fda104ac62cc3dc0a5ed0f400c6958d7034e3855cad5474fca253125e

757855fcd47f843739b9a330f1ecb28d339be41eed4ae25220dc888e57f2ec51

3686204361bf6bf8db68fd81e08c91abcbf215844f0119a458c319e92a396ecf

d60ea266c4e0f0e8d56d98472a91dd5c37e8eeeca13bf53e0381f0affc68e78a

bb7c3b78f2784a7ac3c090331326279476c748087188aeb69f431bbd70ac6407

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

1. **CMTX-P042024115 Nova Stealer**

ALERT BRIEF:

Nova Stealer is part of a category of malicious software known as information stealers or credential stealers. It is distributed through various means, including phishing emails, malicious websites, and as a payload in other malware.  Nova Stealer Malware is offered as Malware-as-a-Service by the threat actor with various capabilities, including password exfiltration, screen recordings, discord injections, and crypto wallet hijacking.

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

HASH

fb3fbee5372e5050c17f72dbe0eb7b3afd3a57bd034b6c2ac931ad93b695d2d9

6a36f1f1821de7f80cc9f8da66e6ce5916ac1c2607df3402b8dd56da8ebcc5e2

fe7e6b41766d91fbc23d31573c75989a2b0f0111c351bed9e2096cc6d747794b

ce0e41e907cab657cc7ad460a5f459c27973e9346b5adc8e64272f47026d333d

a214bc2025584af8c38df36b08eb964e561a016722cd383f8877b684bff9e83d

53714612af006b06ca51cc47abf0522f7762ecb1300e5538485662b1c64d6f55

728953a3ebb0c25bcde85fd1a83903c7b4b814f91b39d181f0fc610b243c98d4

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

1. **CMTX-P042024125 IceRAT Malware**

ALERT BRIEF:

IceRAT malware written in JPHP act as backdoor rather than a remote access Trojan. Malware has very low detection rates, acting as a stealth malware able to steal sensitive data and financial assets from the targeted machines.

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

HASH

aab585b75e868fb542e6dfcd643f97d1c5ee410ca5c4c5ffe1112b49c4851f47

b5f740c0c1ac60fa008a1a7bd6ea77e0fc1d5aa55e6856d8edcb71487368c37c

cc15e96ec1e27c01bd81d2347f4ded173dfc93df673c4300faac5a932180caeb

d2f12dec801000fbd5ccc8c0e8ed4cf8cc27a37e1dca9e25afc0bcb2287fbb9a

f2fc27b96a4a487f39afad47c17d948282145894652485f9b6483bec64932614

f99aa62ee34877b1cd02cfd7e8406b664ae30c5843f49c7e89d2a4db56262c2e

54a992a4c1c25a923463865c43ecafe0466da5c1735096ba0c3c3996da25ffb7

4a71a8c0488687e0bb60a2d0199b34362021adc300541dd106486e326d1ea09b

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

1. **CMTX-P042024135 APT34 threat actor activity**

ALERT BRIEF:

APT34 threat actor Aliases: Oilrig, Cobalt Gypsy, Twisted Kitten

COUNTRY: Iran

Motivation: Espionage

Malware Used: - Solar and Mango Backdoor.

Targeted Sectors: Financial, Governmental, Energy, Chemical and Telecommunication

An Iran based APT group named as APT 34 is active in the cyber threat landscape particularly targeting government agencies, critical infrastructure, telecommunications, and regional entities. It mainly uses spear-phishing emails to deliver their malware to victims and malware tools such as Menorah, SideTwist, and Power Exchange. Recently a PowerShell backdoor coined as "Plink" was deployed for cyber espionage.

Threat actor uses the Solar and Mango as first-stage backdoors in their attack campaign. Both backdoors are deployed by VBS droppers, presumably spread via spear-phishing emails, deployed to collect sensitive information from major browsers and the Windows Credential Manager. Solar and Mango Backdoor are written in C#/.NET where Solar in Outer Space, then its successor Mango.

MITRE ATT&CK Mapping of the TTPs used by the threat actor is as follows:

T1584.004 Compromise Infrastructure: Server

T1608.001 Stage Capabilities: Upload Malware

T1566.001 Phishing: Spearphishing Attachment

T1053.005 Scheduled Task/Job: Scheduled Task

T1059.005 Command and Scripting Interpreter: Visual Basic

T1053.005 Scheduled Task/Job: Scheduled Task

T1036.004 Masquerading: Masquerade Task or Service

T1041 Exfiltration over C2 Channel

T1132.001 Data Encoding: Standard Encoding

T1001 Data Obfuscation

T1087.001 Account Discovery: Local Account

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

DOMAINS

defender-update.com

msoffice365cdn.com

go0gie.com

tecforsc-001-site1.gtempurl.com

IP

145.239.33.100

HASHES

f01a9a2d1e31332ed36c1a4d2839f412

d51c2ffce844d42bab2f2c3131e3dbd4

1ef78a72e4957c04197992bab2f86335

11bf5c50f45b9c8aca1d86ae2e2aec44

1DE4810A10FA2D73CC589CA403A4390B02C6DA5E

CB26EBDE498ECD2D7CBF1BC498E1BCBB2619A96C

C9D18D01E1EC96BE952A9D7BD78F6BBB4DD2AA2A

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

RECOMMENDATIONS

•\* Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

\* Restrict execution of PowerShell /WSCRIPT in enterprise environment. Ensure installation and use of latest version of PowerShell, with enhanced logging enabled, Script block logging, and transcription enabled.

- - ------------------------------------ALERTEND--------------------------------------------

1. **CMTX-P042024155 A Critical Vulnerability in Rust standard library**

ALERT BRIEF:

CVE-2024-24576

CVSS- 10

An OS Command Injection vulnerability named as BatBadBut is found in Rust(a programming language) standard library that could be exploited to target Windows users and stage command injection attacks. This vulnerability affects Windows computers. Rust standard library prior to version 1.77.2 did not properly escape arguments while invoking batch files (with the bat and cmd extensions) on Windows using the command,due to which the attacker could control the arguments passed to the spawned process to execute arbitrary shell commands by bypassing the escaping.

Affected Versions- Versions prior to 1.77.2

RECOMMENDATIONS

\* It is recommended to exercise caution when executing commands on Windows, especially to the developers.

\* To prevent the unexpected execution of batch files, it is adviced to consider moving the batch files to a directory that is not included in the PATH environment variables so that the batch files won't be executed unless the full path is specified. In this way unexpected execution of batch files can be prevented.

---------------------------------------ALERTEND---------------------------------------------

1. **CMTX-P042024165 Matanbuchus Malware**

ALERT BRIEF:

A new malware called as MATANBUCHUS is a C++ backdoor that primarily downloads and executes second-stage malware and loads arbitrary PE files or PowerShell scripts upon a victims system. The malware establishes communication with C2 server using HTTP on TCP port 80. Its capabilities include the ability to launch a .exe or .dll file in memory and custom PowerShell commands, to leverage schtasks.exe to add or modify task schedules. It uses two DLLs during the malware’s run cycle where the first DLL has an internal name of MatanbuchusDroper.dll while the second DLL is named Matanbuchus.dll.

MITRE ATT&CK Identifiers:

Obtain Capabilities (T1588)

Command and Scripting Interpreter (T1059)

Scheduled Task/Job (T1053)

Shared Modules (T1129)

Access Token Manipulation (T1134)

Process Injection (T1055)

Deobfuscate/Decode Files or Information (T1140)

Masquerading (T1036)

Process Injection (T1055)

Virtualization/Sandbox Evasion (T1497)

Input Capture (T1056)

Ingress Tool Transfer (T1105)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASHES:

41727fc99b9d99abd7183f6eec9052f86de076c04056e224ac366762c361afda

7fbaf7420943d4aa327bb82a357cd31ca92c7c83277f73a195d45bd18365cfce

af356a39a298f6a48f8091afc2f2fc0639338b11813f4f4bd05aba4e65d2bbe3

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

- - - - - - --------------------------------------ALERTEND------------------------------------------------------

1. **CMTX-I-196042024 Phishing Domains - APT36 campaign**

Following malicious domains are being used for spear-phishing purpose to target government officials:  
  
- ------------- < Phishing Domains> ------------  
e0ffice.duckdns.org  
www.e0ffice.duckdns.org  
mail.e0ffice.duckdns.org  
webdisk.e0ffice.duckdns.org  
webmail.e0ffice.duckdns.org  
- ------------- </Phishing Domains>-------------  
  
Kindly take the required actions.

1. **CMTX-P042024636 QuasarRAT Malware ALERT 49**

ALERT BRIEF:

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

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

IP ADDRESSES: PORTS Last Seen Country Code

181.214.147.29:4782 12-04-2024 LT

111.92.240.15:4782 11-04-2024 HK

181.214.147.29:4782 12-04-2024 LT

41.216.183.185:4782 04-12-2023 NL

202.143.110.210:4782 11-04-2024 VN

102.40.62.176:18 11-04-2024 EG

80.85.154.22:8080 12-04-2024 RU

103.200.124.195:4782 12-04-2024 HK

45.13.225.104:4783 05-04-2024 DE

91.92.253.11:7000 13-03-2024 NL

206.233.128.64:8080 15-03-2024 SG

106.240.105.174:8090 11-04-2024 KR

47.76.214.226:9443 12-04-2024 HK

77.105.219.98:443 11-04-2024 SE

36.251.29.215:4784 11-04-2024 CN

45.63.49.44:100 04-10-2016 US

189.78.187.139:5000 10-03-2018 BR

185.225.191.26:1337 12-04-2024 PL

124.223.48.86:4285 12-04-2024 CN

143.92.56.60:4782 12-04-2024 HK

212.23.222.46:1337 12-04-2024 PL

188.50.196.226:1337 11-04-2024 SA

91.92.252.119:4782 11-04-2024 NL

124.222.109.145:4782 11-04-2024 CN

45.128.96.227:4782 11-04-2024 US

139.28.37.14:4782 10-09-2020 UA

181.162.141.33:8080 11-04-2024 CL

128.199.66.119:18982 17-01-2024 SG

187.59.75.101:4782 11-04-2024 BR

195.128.248.208:4782 11-04-2024 UA

45.32.216.138:4782 06-10-2022 US

189.190.82.175:7777 11-04-2024 MX

190.239.205.38:3333 29-03-2022 PE

2.47.94.129:4782 11-04-2024 IT

216.73.158.60:4782 12-04-2024 US

143.92.56.46:4782 14-02-2021 HK

181.162.177.83:8080 11-04-2024 CL

45.76.123.169:4782 07-07-2018 AU

181.162.159.238:8080 11-04-2024 CL

84.253.244.136:4782 12-04-2024 FI

95.141.47.18:8080 05-04-2024 IT

91.92.253.176:4782 12-04-2024 NL

140.82.48.210:2404 16-07-2020 US

185.113.143.66:1337 07-04-2024 PT

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

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

RECOMMENDATIONS

- - - - - - - - - - - - - - - - - - Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - - - - - - - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024175 A Critical Vulnerability (CVE-2024-3273) Affecting D-Link NAS devices**

ALERT BRIEF:

CVE-2024-3273

CVSS- 7.3

An OS Command Injection vulnerability tracked as CVE-2024-3273 is recently found in  D-Link NAS devices. On successful exploitation of the vulnerability, it allows the attacker to execute arbitrary commands to gain unauthorized access.

With this, the attacker can log in to the affected system using cmd parameters in the nas-sharing.cgi CGI script for cyber espionage.

Affected Products-  D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403

RECOMMENDATIONS

\* As the POC of the exploit is publically available and Vulnerability is widely exploited, it is advised to prioritize patching this vulnerability promptly to prevent potential unauthorized access or malicious activities on vulnerable devices within an organization.

---------------------------------------ALERTEND----------------------------------------------

1. **CMTX-P042024185 Rhadamanthys Info Stealer Malware**

ALERT BRIEF:

The Rhadamanthys Stealer aka RADTHIEF, an information-stealing malware is active in the cyber threat landscape. The malware is primarily delivered through phishing campaigns, often using malicious attachments or links in emails.One of its capabilities includes collecting sensitive information from infected systems (for example system information, cookies, browsing history, saved credit card information, and data from various applications such as FTP applications, password managers, and email clients). Threat actor group TA547 uses this stealer along with other campaigns that use LNK files and PowerShell scripts hosted on remote servers to deliver Rhadamanthys stealer.

MITRE ATT&CK Identifiers

T1055- Process Injection

T1105- Ingress Tool Transfer

T1134- Access Token Manipulation

T1204.002- Malicious File

T1082- System Information Discovery

T1497.001- System Checks

T1047- Windows Management Instrumentation

T1140- Deobfuscate/Decode Files or Information

T1622- Debugger Evasion

T1059.001- PowerShell

T1095- Non-Application Layer Protocol

T1012- Query Registry

T1614- System Location Discovery

T1566.001- Spearphishing Attachment

T1620- Reflective Code Loading

T1027.010- Command Obfuscation

T1056.001- Keylogging

T1057- Process Discovery

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP ADDRESS

77.221.137.22

94.131.104.223

HASHES

375ac09d5f44849e9c888e86adc50069cdb019e3de3216264f61868bef12ca4d

0b2fe8188163d143a4c7fe09ce892dcf45fe0e43ca869ec8e65cca020ee06cb2

f5fc667d818a26fbb5c04657b131d86af1746a349ceb9d6e441d24c8673393b2

URL

https://bolibachan.com/g.txt

https://care-onboard.com/app.txt

DOMAIN:

indscpm.xyz

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

RECOMMENDATIONS

• Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

• Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Monitor users' web browsing habits; restrict access to sites with unfavourable content.

• Systems having an antivirus and a malware protection program on it and making sure they are always up to date. Systems and installed applications being fully patched and updated.

Restrict execution of PowerShell /WSCRIPT in enterprise environment. Ensure installation and use of latest version of PowerShell, with enhanced logging enabled, Script block logging, and transcription enabled

- - - - - --------------------------------------ALERTEND-----------------------------------------------------

1. **CMTX-P042024915 SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as 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)

A list of Indicators of compromise is provided below for your action side.

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

IP Address: Port : Country Code

45.77.170.42:443:SG

154.211.4.62:443:HK

70.34.212.229:443:SE

45.32.151.219:443:FR

199.247.23.228:443:DE

141.164.35.65:443:KR

164.215.103.248:443:AZ

165.154.18.212:3001:JP

64.176.42.10:443:JP

199.247.1.201:443:DE

8.217.107.71:1723:HK

38.60.134.143:443:FR

139.99.50.68:80:SG

38.60.191.159:443:ID

165.154.220.237:80:JP

94.131.110.28:443,80,53:DE

64.176.47.234:443:JP

216.128.184.205:443:CA

139.180.206.75:443:JP

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

•    Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024965 PLUGX RAT ALERT 113**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. 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. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

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

IP Address: Port : Country Code

185.126.225.74:5050, 443:NL

194.124.33.123:5050, 443,5050:CH

155.138.246.52:53, 80, 443,53:US

64.44.57.14:21, 80, 443,21:US

31.192.235.62:53, 443,53:NL

134.122.129.154:8090, 443:HK

66.42.50.211:443:SG

38.89.72.253:443:US

47.76.44.226:21:HK

167.179.72.177:443:JP

146.66.212.82:443, 5050:RO

107.186.200.64:443:MY

192.54.57.122:443,5050:NL

45.80.208.142:443:KZ

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

Please Note: The Above IOCs are also available in CERT-In Threat

Intelligence Platform.

Recommendations:

 - Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

- - - - - - - - - - - - - - - - --------------------------ALERTEND---------------------------

1. **CMTX-P042024195 A Critical Zero day Vulnerability (CVE-2024-3400) Affecting Palo Alto Networks PAN-OS software**

ALERT BRIEF:

CVE-2024-3400

CVSS- 8.3

A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software is being reported. Successful exploitation of the vulnerability would enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Vulnerable version

PAN-OS 10.2, 11.0 and 11.1

RECOMMENDATIONS

\* As there are high chances of attacker exploiting this vulnerability, prioritize patching is advised as and when vendor releases the patch. For details about patch, please visit the vendor's official site.

https://security.paloaltonetworks.com/CVE-2024-3400

1. **CMTX-P042024038 RACCOON MALWARE**

ALERT BRIEF:

CERT-IN has been tracking prominent RATs/malware families. An uprise in activities associated with raccoon malware is reported. Raccoon is an info stealer malware available as a Malware as a Service. Raccoon malware has capability to check system settings, capture screenshots, collect basic information like OS version, IP and username and steal passwords and logins from a variety of browsers.

A list of Indicators of compromise is provided below for your action side.

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

IPs: Ports: Country Code

141.195.117.127:80,US

146.70.135.158:80,CH

192.227.94.170:80,US

64.7.199.224:80,RO

89.238.170.230:80,GB

91.198.166.140:80,PL

91.227.40.93:80,DE

91.92.255.182:80,NL

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

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

Recommendations:

- - - - ------- Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient's responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024028 REDLINE STEALER MALWARE**

ALERT BRIEF:

RedLine Stealer is a .NET-based infostealer malware that is capable of harvesting information from browsers such as saved credentials,

autocomplete data and credit card information. It is also utilized in facilitating attacker to drop another payload or launch a hidden command shell on victims' machine.

MITRE ATT&CK Identifiers

T1059 (Command and Scripting Interpreter)

T1543 (Create or Modify System Process)

T1053 (Scheduled Task/Job)

T1027 (Obfuscated Files or Information)

T1003 (OS Credential Dumping)

T1055 (Process Injection)

T1140 (De obfuscate/Decode Files or Information)

T1547 (Boot or Logon Auto start Execution)

A list of Indicators of compromise is provided below for the necessary action.

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

IP Ports    Country Code

147.45.47.65:47232,DE

162.120.71.68:4483,US

162.33.178.13:41517,US

163.5.112.53:51523,FR

173.214.165.26:8888,US

185.222.58.47:55615,NL

66.206.9.234:8888,US

86.105.227.110:81,RU

89.23.97.100:15799,RU

91.92.250.88:16964,NL

94.131.118.143:38002,FR

94.156.65.88:81,NL

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

RECOMMENDATIONS

- - - - - - - Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P042024205 CVE-2024-27309: Critical Vulnerability Affecting Apache Kafka**

ALERT BRIEF:

CVE Number: CVE-2024-27309

According to the reports, an Incorrect Authorization Vulnerability tracked as CVE-2024-27309 exists in Apache Kafka, which is an open source event streaming platform that offers high performance streaming analytics, data integration and some other purposes also. Once the flaw is successfully exploited, it allows a remote attacker to bypass certain security mechanisms since Apache Kafka cluster is now being migrated from ZooKeeper mode to KRaft mode, wherein some cases ACLs (Acces Control List) will not be correctly enforced.

Affected Versions-Apache Kafka 3.5.0, 3.5.1, 3.5.2, 3.6.0, 3.6.1

Recommendations:

\* It is recommended to follow Apache's advisory and apply specific patch.

1. **CMTX-P042024215A Critical Zero day Vulnerability (CVE-2024-3400) Affecting Palo Alto Networks PAN-OS software**

ALERT BRIEF:

PREVIOUS REFERENCE: [CMTX-P042024195 A Critical Zero day Vulnerability (CVE-2024-3400) Affecting Palo Alto Networks PAN-OS software, TLP: CLEAR, Dated 12/04/2024

It has been reported that a zero day vulnerability CVE-2024-3400 in Palo Alto Networks has been actively exploited by threat actors, particularly by UTA0218. After remotely compromising the firewall devices, threat actors deploy custom Python backdoor (UPSTYLE) on the firewall, create a reverse shell and download executables onto the device. Post-intrusion, the attacker exfiltrates configuration data from victim devices move laterally within the affected enterprise networks by extracting sensitive credentials. The attackers create a cron job that runs every minute, fetching commands from an external server.

Affected versions:

PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1

Patched Versions:

PAN-OS 10.2.9-h1

PAN-OS 11.0.4-h1

PAN-OS 11.1.2-h3

Mapping of Attack Campaign on MITRE ATT&CK Enterprise Identifiers

T1190 (Exploit Public-Facing Application)

T1059 (Command and Scripting Interpreter)

T1555 (Credentials from Password Stores)

=========IOC START===================================

HASH

3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac

35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c

755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8

adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87

c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9

fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7

96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9

448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c

e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8

161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6

Compromised S3 bucket used to host files by threat actor

nhdata.s3-us-west-2.amazonaws.com

URL

http://144.172.79.92/update.py

http://172.233.228.93/policy

http://172.233.228.93/patch

IP used by the attacker to host malicious files

66.235.168.222

172.233.228.93

198.58.109.149

File location

/var/log/pan/sslvpn\_ngx\_error.log

/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css

=============IOC END===============================

RECOMMENDATIONS

\* Apply vendor specified patch ASAP. For detection, please check the YARA Rule shared by volexity at below link:

https://github.com/volexity/threat-intel/blob/main/2024/2024-04-12%20Palo%20Alto%20Networks%20GlobalProtect/indicators/rules.yar

1. **CMTX-P042024864 Critical PuTTY Vulnerability**

ALERT BRIEF:

A new vulnerability in the PuTTY Secure Shell (SSH) and Telnet client, tracked as CVE-2024-31497 is being reported. Successful Exploitation of the vulnerability provides the attacker a number of signed messages along with the public key, enabling them to recover the private key and forge signatures.

Impacted version of putty and some other products:-

PuTTY versions 0.68 through 0.80

FileZilla (3.24.1 - 3.66.5)

WinSCP (5.9.5 - 6.3.2)

TortoiseGit (2.4.0.2 - 2.15.0)

TortoiseSVN (1.10.0 - 1.14.6)

Patched/fixed version:-

PuTTY 0.81

FileZilla 3.67.0

WinSCP 6.3.3

TortoiseGit 2.15.0.1

RECOMMENDATIONS

• Users of affected versions of PuTTY as well as related applications like FileZilla, WinSCP, TortoiseGit, and TortoiseSVN, should revoke their keys and replace them with newly generated ones using updated software versions. Users of TortoiseSVN are advised to configure TortoiseSVN to use Plink from the latest PuTTY 0.81 release when accessing a SVN repository via SSH until a patch becomes available.

1. **[CMTX-I-338042024 Phishing domain impersonating MoD website**

Following phishing domain is impersonating MoD website and being used for spear-phishing purpose:  
  
- ------------ < Phishing Domain> ------------  
mod.gov.in.reportedcase.info  
- ------------ </Phishing Domain>-------------  
  
Kindly take the required actions.

1. **CMTX-P-2100420249 Qbot Malware Alert**

Malware Alert Brief:  
  
  
Qbot (also known as QakBot) is a common trojan malware designed to steal passwords. Over time this malware has evolved from simple infostealer malware to an infostealer with a backdoor functionality. Qbot is primarily used by financially motivated actors.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
5.61.49.13    [Netherlands  
52.28.0.76    [Germany  
35.156.24.159    [Germany  
37.48.65.153    [Netherlands  
65.109.38.226    [Finland  
18.185.194.237    [Germany  
47.254.251.170    [Malaysia  
178.22.83.226    [Netherlands  
82.192.82.228    [Netherlands  
3.64.163.50    [Germany  
89.31.143.90    [Germany  
18.157.95.117    [Germany  
185.77.253.19    [Austria  
52.58.140.127    [Germany  
185.107.56.192    [Netherlands  
81.17.18.194    [Switzerland  
81.17.18.197    [Switzerland  
81.17.18.198    [Switzerland  
81.17.29.149    [Switzerland  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-9940420249 Amadey Malware Alert**

Malware Alert Brief:  
  
  
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.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
185.196.10.188    [Switzerland  
45.9.74.166    [Germany  
5.42.65.80    [Russia  
31.41.244.146    [Russia  
188.40.122.96    [Germany  
78.46.242.112    [Germany  
79.137.203.19    [Germany  
185.215.113.32    [Seychelles  
49.12.117.51    [Germany  
91.195.240.117    [Germany  
62.182.156.153    [Russia  
45.9.74.182    [Germany  
185.172.128.19    [Russia  
93.123.39.96    [Indonesia  
77.91.124.1    [Finland  
207.154.243.184    [Germany  
5.42.64.33    [Austria  
45.9.74.141    [Germany  
79.137.203.59    [Germany  
45.9.74.164    [Germany  
188.40.187.155    [Germany  
34.175.230.209    [Spain  
193.106.191.126    [Iran  
134.0.116.60    [Russia  
77.73.134.66    [Germany  
193.106.191.201    [Iran  
185.174.136.244    [Russia  
35.204.181.10    [Netherlands  
195.245.113.116    [Netherlands  
176.97.64.128    [Singapore  
185.172.128.90    [Russia  
185.172.128.65    [Russia  
34.91.32.224    [Netherlands  
193.34.42.179    [Finland  
103.237.87.56    [Vietnam  
167.235.20.126    [Germany  
185.215.113.35    [Seychelles  
34.90.130.132    [Netherlands  
89.23.103.42    [Netherlands  
95.163.98.240    [Russia  
194.105.56.41    [Latvia  
217.26.53.157    [Switzerland  
193.233.20.36    [Russia  
92.205.4.124    [Germany  
34.88.137.133    [Finland  
34.163.238.133    [France  
103.171.90.213    [Vietnam  
185.172.128.144    [Russia  
46.21.101.120    [Sweden  
80.66.75.214    [Russia  
92.46.53.222    [Kazakhstan  
95.213.137.98    [Russia  
35.233.77.94    [Belgium  
193.233.20.25    [Russia  
193.3.19.114    [Russia  
5.42.64.44    [Russia  
156.250.7.144    [China  
87.247.245.132    [Germany  
92.205.64.102    [Germany  
80.66.75.77    [Russia  
34.91.94.238    [Netherlands  
93.95.102.11    [Russia  
78.47.9.120    [Germany  
185.215.113.38    [Seychelles  
34.91.251.221    [Netherlands  
195.66.210.137    [Ukraine  
47.241.9.5    [Singapore  
93.95.102.25    [Russia  
35.234.109.94    [Germany  
51.250.126.210    [Russia  
85.209.135.11    [Egypt  
5.61.28.102    [Iran  
188.209.214.83    [Romania  
37.9.8.75    [Russia  
89.248.168.123    [Netherlands  
185.50.25.27    [Russia  
185.244.80.19    [Germany  
85.25.95.198    [Germany  
95.211.219.65    [Netherlands  
80.249.162.133    [Hungary  
176.123.7.61    [Moldova  
202.61.203.214    [Germany  
77.72.179.25    [Switzerland  
169.150.247.38    [Germany  
41.111.30.209    [Algeria  
93.85.84.71    [Belarus  
37.72.164.172    [Belgium  
176.62.173.219    [Belgium  
185.162.31.208    [Belgium  
91.92.144.116    [Bulgaria  
111.173.80.47    [China  
212.97.141.26    [Denmark  
34.88.159.22    [Finland  
5.175.14.19    [Germany  
23.55.161.64    [Germany  
23.213.161.5    [Germany  
92.205.61.170    [Germany  
185.166.21.74    [Germany  
217.144.143.34    [Germany  
192.84.143.72    [Italy  
46.17.175.112    [Lithuania  
154.41.249.177    [Netherlands  
154.41.249.233    [Netherlands  
154.62.105.61    [Netherlands  
154.62.105.89    [Netherlands  
188.212.255.110    [Romania  
79.137.192.4    [Russia  
88.212.237.4    [Russia  
93.93.88.31    [Russia  
185.87.196.126    [Russia  
185.135.83.132    [Russia  
194.67.193.68    [Russia  
45.76.181.158    [Singapore  
194.237.110.6    [Sweden  
178.210.173.37    [Turkey  
193.233.20.14    [Russia  
193.106.191.184    [Netherlands  
138.201.203.107    [Germany  
193.105.32.185    [Poland  
77.91.78.17    [Netherlands  
34.90.10.178    [Netherlands  
156.254.147.137    [China  
212.162.57.144    [Germany  
109.71.253.219    [Germany  
185.216.143.2    [Netherlands  
89.37.121.88    [Romania  
185.216.143.48    [Netherlands  
45.92.178.114    [Taiwan  
188.42.30.244    [Russia  
5.42.64.35    [Austria  
5.101.37.37    [Armenia  
185.176.188.66    [Spain  
185.70.93.244    [Spain  
83.143.220.151    [Finland  
77.37.53.247    [Germany  
92.205.197.54    [Germany  
212.102.56.19    [Germany  
103.16.198.177    [Indonesia  
35.204.41.52    [Netherlands  
95.211.155.129    [Netherlands  
37.140.192.91    [Russia  
78.108.80.146    [Russia  
80.78.251.138    [Russia  
87.236.16.14    [Russia  
87.236.16.253    [Russia  
185.50.24.83    [Russia  
31.214.178.74    [Spain  
23.0.174.120    [Switzerland  
77.123.138.234    [Ukraine  
62.204.41.104    [Russia  
91.189.114.4    [Russia  
193.106.191.218    [Iran  
185.149.40.213    [Ukraine  
23.251.131.105    [Belgium  
37.152.88.204    [Spain  
91.227.52.15    [Russia  
78.136.83.154    [Spain  
154.215.83.156    [China  
35.228.62.212    [Finland  
89.107.186.160    [Germany  
31.25.240.36    [Russia  
196.240.45.41    [South Africa  
193.106.191.185    [Iran  
80.66.64.31    [Russia  
103.67.162.213    [Vietnam  
95.163.118.168    [Russia  
37.19.194.48    [Germany  
109.206.161.72    [Netherlands  
212.32.237.90    [Netherlands  
87.242.127.163    [Russia  
77.37.53.7    [Germany  
92.205.182.151    [Germany  
184.86.103.76    [Germany  
91.240.20.44    [Netherlands  
94.142.138.4    [Netherlands  
185.113.140.157    [Portugal  
31.31.196.77    [Russia  
81.90.182.215    [Russia  
119.31.232.100    [Singapore  
31.31.205.163    [Russia  
91.92.242.139    [Netherlands  
193.104.215.64    [Ireland  
88.212.202.52    [Russia  
88.212.201.198    [Russia  
88.212.201.204    [Russia  
185.216.143.121    [Netherlands  
95.158.162.200    [Bulgaria  
104.95.186.169    [Denmark  
23.11.206.24    [Germany  
5.79.68.104    [Netherlands  
81.171.28.44    [Netherlands  
45.89.245.75    [Ukraine  
95.214.59.72    [Russia  
92.204.58.67    [Germany  
95.211.218.10    [Netherlands  
141.138.169.222    [Netherlands  
154.41.249.12    [Netherlands  
154.62.105.158    [Netherlands  
185.135.241.45    [Netherlands  
87.236.16.13    [Russia  
193.182.189.222    [Sweden  
103.233.192.221    [Thailand  
77.73.133.72    [Germany  
185.172.128.3    [Russia  
185.254.197.234    [Ukraine  
85.114.96.4    [Gaza Strip  
185.15.209.158    [Netherlands  
91.223.82.56    [Netherlands  
94.102.57.166    [Netherlands  
213.13.145.243    [Portugal  
185.66.142.35    [Netherlands  
146.70.118.226    [Germany  
185.22.66.16    [Kazakhstan  
178.162.140.132    [Netherlands  
81.171.6.66    [Netherlands  
83.217.70.126    [Belgium  
94.231.108.23    [Denmark  
213.41.95.60    [France  
34.159.237.198    [Germany  
87.230.47.59    [Germany  
193.158.75.34    [Germany  
194.145.236.227    [Germany  
195.252.157.4    [Germany  
87.236.16.91    [Russia  
87.236.16.123    [Russia  
193.109.247.75    [Russia  
217.23.143.226    [Russia  
46.21.106.116    [Sweden  
103.106.105.181    [Vietnam  
103.195.238.40    [Vietnam  
185.172.128.187    [Russia  
194.190.152.209    [Russia  
84.53.172.91    [Denmark  
31.41.244.158    [Russia  
213.34.130.138    [Netherlands  
8.222.128.131    [Singapore  
8.222.193.208    [Singapore  
195.123.210.178    [Latvia  
62.122.170.171    [Netherlands  
35.198.88.107    [Germany  
62.116.23.60    [Austria  
81.17.29.162    [Switzerland  
109.206.161.15    [Netherlands  
103.55.216.62    [Indonesia  
213.239.154.30    [Netherlands  
5.42.65.108    [Russia  
5.198.130.8    [Czechia  
185.166.104.95    [Iran  
89.42.218.147    [Romania  
95.211.144.68    [Netherlands  
93.115.28.104    [Lithuania  
83.169.5.121    [Germany  
185.149.240.213    [Russia  
185.152.65.27    [Czechia  
77.74.178.17    [Russia  
93.159.228.24    [Russia  
158.255.238.182    [Spain  
193.176.190.43    [Russia  
34.76.203.18    [Belgium  
185.18.9.13    [Belgium  
92.247.81.211    [Bulgaria  
23.38.73.27    [Germany  
77.37.53.27    [Germany  
92.205.166.137    [Germany  
156.146.33.34    [Germany  
184.30.135.150    [Germany  
91.120.20.180    [Hungary  
103.21.59.83    [India  
130.185.78.167    [Iran  
185.108.85.32    [Israel  
159.148.172.231    [Latvia  
185.176.221.103    [Latvia  
185.14.28.167    [Netherlands  
194.146.104.13    [Netherlands  
88.212.247.52    [Russia  
88.212.247.60    [Russia  
188.35.184.4    [Russia  
194.67.193.138    [Russia  
46.246.7.39    [Sweden  
103.173.227.98    [Vietnam  
103.161.184.56    [Indonesia  
203.205.10.134    [Vietnam  
103.224.247.210    [India  
154.62.105.1    [Netherlands  
185.45.192.84    [Netherlands  
92.53.85.58    [Russia  
94.75.211.145    [Netherlands  
91.183.69.112    [Belgium  
45.10.111.18    [Russia  
87.230.43.108    [Germany  
113.23.169.115    [Malaysia  
88.151.96.4    [Hungary  
151.106.67.254    [Germany  
87.233.131.58    [Netherlands  
195.128.175.9    [Denmark  
94.23.85.110    [France  
2.22.240.145    [Germany  
34.107.4.242    [Germany  
92.205.195.56    [Germany  
168.119.4.153    [Germany  
178.63.131.46    [Germany  
185.238.168.53    [Netherlands  
188.215.244.191    [Romania  
31.31.196.96    [Russia  
37.140.192.213    [Russia  
78.108.80.36    [Russia  
91.106.207.71    [Russia  
185.137.234.38    [Russia  
193.168.47.254    [Russia  
185.232.14.54    [Singapore  
85.208.22.158    [Spain  
178.211.133.17    [Spain  
5.198.252.253    [Sweden  
185.172.128.161    [Russia  
95.213.139.6    [Russia  
151.248.126.254    [Russia  
185.172.128.170    [Russia  
185.62.56.180    [Netherlands  
146.70.169.164    [Netherlands  
34.77.10.20    [Belgium  
192.132.34.7    [Italy  
2.21.146.158    [France  
185.188.106.11    [Iran  
37.48.65.148    [Netherlands  
146.255.61.215    [Austria  
213.33.117.79    [Austria  
195.130.132.9    [Belgium  
138.199.14.96    [China  
194.5.170.13    [France  
37.218.252.149    [Germany  
62.157.182.204    [Germany  
82.210.238.38    [Germany  
193.238.27.35    [Germany  
194.25.134.9    [Germany  
193.138.125.30    [Hungary  
195.228.86.32    [Hungary  
5.255.68.240    [Netherlands  
154.62.105.24    [Netherlands  
185.140.164.46    [Netherlands  
212.77.101.4    [Poland  
212.55.154.36    [Portugal  
81.19.83.36    [Russia  
81.90.180.222    [Russia  
94.100.180.150    [Russia  
95.213.188.74    [Russia  
185.195.26.107    [Russia  
203.146.117.246    [Thailand  
95.163.114.204    [Russia  
185.216.143.19    [Netherlands  
45.84.204.220    [Lithuania  
91.204.46.238    [Germany  
34.140.0.190    [Belgium  
145.14.151.112    [Netherlands  
185.222.157.149    [Spain  
80.90.16.91    [Germany  
46.246.2.15    [Sweden  
34.141.222.150    [Netherlands  
46.191.176.222    [Russia  
203.146.117.197    [Thailand  
95.163.50.150    [Russia  
95.163.114.203    [Russia  
188.42.31.12    [Russia  
94.100.180.160    [Russia  
94.231.106.76    [Denmark  
91.106.207.40    [Russia  
194.150.248.53    [Switzerland  
92.204.55.204    [Germany  
178.18.22.161    [Netherlands  
217.69.139.160    [Russia  
46.31.195.60    [France  
92.205.170.28    [Germany  
138.199.37.193    [Germany  
188.68.47.244    [Germany  
195.228.242.74    [Hungary  
34.154.230.249    [Italy  
81.198.171.116    [Latvia  
34.91.63.205    [Netherlands  
35.204.181.134    [Netherlands  
141.138.168.153    [Netherlands  
154.41.249.106    [Netherlands  
154.41.249.127    [Netherlands  
217.18.70.164    [Netherlands  
46.248.186.12    [Poland  
31.41.40.222    [Russia  
79.137.223.9    [Russia  
85.193.69.29    [Russia  
185.137.232.120    [Russia  
194.58.90.102    [Russia  
31.24.154.56    [Spain  
46.246.14.4    [Sweden  
103.171.90.204    [Vietnam  
37.218.254.120    [Germany  
5.42.65.44    [Netherlands  
185.216.143.86    [Netherlands  
195.211.124.144    [Netherlands  
37.9.13.129    [Russia  
109.206.161.43    [Netherlands  
89.208.236.251    [Russia  
217.13.100.44    [Hungary  
31.171.152.131    [Albania  
37.252.87.116    [Armenia  
139.28.4.136    [Armenia  
5.254.80.190    [Austria  
80.121.194.48    [Austria  
80.121.194.153    [Austria  
80.121.194.218    [Austria  
90.146.105.146    [Austria  
145.40.58.157    [Austria  
147.161.131.20    [Austria  
147.161.131.29    [Austria  
165.225.200.106    [Austria  
194.166.126.176    [Austria  
213.33.96.139    [Austria  
217.76.162.27    [Austria  
5.250.194.3    [Azerbaijan  
81.21.87.156    [Azerbaijan  
85.10.75.118    [Belgium  
91.86.149.218    [Belgium  
91.183.118.136    [Belgium  
94.107.149.128    [Belgium  
94.110.0.238    [Belgium  
94.110.26.208    [Belgium  
94.110.46.205    [Belgium  
94.110.52.46    [Belgium  
94.110.55.196    [Belgium  
94.110.77.54    [Belgium  
94.110.83.71    [Belgium  
94.110.101.102    [Belgium  
94.110.101.234    [Belgium  
94.110.102.4    [Belgium  
94.110.113.171    [Belgium  
94.110.115.196    [Belgium  
94.110.117.188    [Belgium  
94.110.127.254    [Belgium  
94.110.140.186    [Belgium  
94.110.161.108    [Belgium  
94.110.171.52    [Belgium  
94.110.172.3    [Belgium  
94.110.172.61    [Belgium  
94.110.175.120    [Belgium  
94.110.182.111    [Belgium  
94.110.209.165    [Belgium  
94.111.1.201    [Belgium  
94.111.38.250    [Belgium  
94.111.46.0    [Belgium  
94.111.47.248    [Belgium  
94.111.58.172    [Belgium  
45.94.28.113    [Bulgaria  
45.128.5.6    [Bulgaria  
46.237.78.67    [Bulgaria  
62.176.125.117    [Bulgaria  
77.78.30.144    [Bulgaria  
77.78.55.22    [Bulgaria  
78.83.24.255    [Bulgaria  
84.43.203.27    [Bulgaria  
84.43.241.95    [Bulgaria  
84.238.241.138    [Bulgaria  
84.238.241.158    [Bulgaria  
91.139.211.202    [Bulgaria  
93.183.129.52    [Bulgaria  
93.183.132.54    [Bulgaria  
93.183.187.209    [Bulgaria  
95.43.210.62    [Bulgaria  
95.43.223.230    [Bulgaria  
95.158.175.229    [Bulgaria  
95.168.248.175    [Bulgaria  
109.120.234.48    [Bulgaria  
109.160.73.60    [Bulgaria  
109.199.227.99    [Bulgaria  
178.169.138.253    [Bulgaria  
185.138.176.32    [Bulgaria  
185.138.177.72    [Bulgaria  
185.138.177.182    [Bulgaria  
212.21.153.193    [Bulgaria  
212.50.82.34    [Bulgaria  
212.122.186.122    [Bulgaria  
213.191.221.12    [Bulgaria  
217.145.83.23    [Bulgaria  
217.145.92.45    [Bulgaria  
8.220.113.176    [China  
169.239.158.222    [Congo (Kinshasa)  
37.244.196.129    [Croatia  
80.253.162.61    [Croatia  
161.53.212.40    [Croatia  
45.84.122.5    [Czechia  
89.221.214.115    [Czechia  
89.221.216.108    [Czechia  
89.221.217.105    [Czechia  
89.221.219.16    [Czechia  
89.221.219.78    [Czechia  
91.218.234.42    [Czechia  
109.105.40.112    [Czechia  
109.105.47.113    [Czechia  
164.215.112.154    [Czechia  
188.134.242.213    [Czechia  
212.96.162.173    [Czechia  
5.33.88.169    [Denmark  
5.56.157.182    [Denmark  
5.103.180.170    [Denmark  
77.68.238.35    [Denmark  
82.103.134.181    [Denmark  
89.239.195.148    [Denmark  
91.197.249.146    [Denmark  
146.70.89.151    [Denmark  
147.161.155.81    [Denmark  
176.62.205.96    [Denmark  
185.66.0.93    [Denmark  
185.150.198.37    [Denmark  
185.245.84.206    [Denmark  
212.27.7.99    [Denmark  
212.27.28.98    [Denmark  
212.27.29.141    [Denmark  
213.237.50.35    [Denmark  
84.52.45.7    [Estonia  
92.62.110.89    [Estonia  
185.157.109.98    [Estonia  
46.163.206.170    [Finland  
62.44.214.24    [Finland  
81.197.109.91    [Finland  
83.245.184.204    [Finland  
84.253.231.76    [Finland  
85.131.31.115    [Finland  
85.134.34.186    [Finland  
87.92.61.45    [Finland  
87.92.96.49    [Finland  
87.92.220.9    [Finland  
87.95.195.20    [Finland  
87.100.191.186    [Finland  
88.85.146.112    [Finland  
88.112.122.81    [Finland  
88.112.224.32    [Finland  
88.115.60.109    [Finland  
88.115.113.171    [Finland  
88.115.148.107    [Finland  
88.115.158.55    [Finland  
91.150.42.100    [Finland  
91.154.140.45    [Finland  
91.155.99.115    [Finland  
91.155.238.114    [Finland  
91.156.209.166    [Finland  
91.159.101.75    [Finland  
91.159.103.79    [Finland  
91.159.110.82    [Finland  
2.12.87.16    [France  
31.207.33.15    [France  
31.207.34.125    [France  
31.207.34.144    [France  
31.207.37.230    [France  
31.207.39.146    [France  
46.18.96.7    [France  
46.20.175.210    [France  
80.11.17.100    [France  
80.11.58.39    [France  
80.12.85.204    [France  
80.12.86.37    [France  
80.13.121.225    [France  
80.13.127.59    [France  
80.13.138.118    [France  
80.13.228.3    [France  
80.14.4.120    [France  
80.14.15.16    [France  
80.14.34.69    [France  
80.14.164.69    [France  
80.14.207.225    [France  
80.15.113.135    [France  
80.15.120.120    [France  
80.15.160.96    [France  
81.249.104.164    [France  
81.250.134.101    [France  
81.250.151.23    [France  
81.250.179.234    [France  
81.250.245.73    [France  
81.252.212.61    [France  
82.120.24.255    [France  
82.120.80.110    [France  
82.127.62.120    [France  
82.127.229.63    [France  
83.114.228.83    [France  
84.14.170.146    [France  
86.195.242.7    [France  
86.196.46.127    [France  
86.215.133.51    [France  
86.217.97.16    [France  
86.239.10.205    [France  
90.26.189.164    [France  
90.55.172.43    [France  
90.59.21.65    [France  
90.60.3.249    [France  
90.63.247.32    [France  
90.76.19.83    [France  
90.79.105.254    [France  
90.89.92.23    [France  
90.110.255.143    [France  
90.120.50.217    [France  
91.234.195.130    [France  
92.145.169.86    [France  
92.149.71.29    [France  
92.154.71.15    [France  
92.154.80.194    [France  
92.154.115.113    [France  
92.204.163.91    [France  
92.204.248.67    [France  
92.245.157.52    [France  
94.238.89.75    [France  
94.238.89.216    [France  
94.238.153.124    [France  
94.238.154.119    [France  
94.238.155.202    [France  
109.220.81.217    [France  
109.222.18.97    [France  
147.161.152.89    [France  
147.161.179.132    [France  
147.161.180.193    [France  
147.161.183.6    [France  
147.161.183.18    [France  
147.161.232.178    [France  
165.225.20.93    [France  
165.225.20.186    [France  
165.225.76.244    [France  
185.7.240.113    [France  
185.7.240.219    [France  
185.7.243.131    [France  
185.24.156.89    [France  
185.98.128.111    [France  
185.98.137.35    [France  
185.98.137.49    [France  
185.98.137.58    [France  
185.204.188.125    [France  
185.245.220.41    [France  
185.245.220.212    [France  
185.245.221.46    [France  
192.162.71.245    [France  
193.222.188.33    [France  
193.248.159.182    [France  
193.251.17.58    [France  
193.252.169.138    [France  
193.252.188.112    [France  
193.253.198.28    [France  
193.253.251.145    [France  
195.36.211.132    [France  
217.69.12.54    [France  
217.109.168.9    [France  
217.128.0.56    [France  
31.146.50.23    [Georgia  
31.146.247.12    [Georgia  
92.241.94.203    [Georgia  
94.43.212.16    [Georgia  
149.3.46.6    [Georgia  
176.221.255.54    [Georgia  
185.81.92.22    [Georgia  
213.131.38.170    [Georgia  
5.182.41.69    [Germany  
5.189.137.101    [Germany  
5.189.139.30    [Germany  
5.189.149.183    [Germany  
5.189.152.103    [Germany  
5.189.154.73    [Germany  
5.189.155.56    [Germany  
5.189.176.24    [Germany  
31.220.72.37    [Germany  
31.220.73.255    [Germany  
31.220.77.158    [Germany  
37.60.245.135    [Germany  
37.60.248.106    [Germany  
37.157.254.103    [Germany  
38.242.136.216    [Germany  
38.242.137.115    [Germany  
38.242.141.57    [Germany  
38.242.198.203    [Germany  
38.242.204.25    [Germany  
38.242.211.77    [Germany  
38.242.218.231    [Germany  
38.242.219.64    [Germany  
38.242.222.126    [Germany  
38.242.223.15    [Germany  
38.242.247.56    [Germany  
43.152.137.46    [Germany  
45.93.17.199    [Germany  
46.165.222.88    [Germany  
47.254.137.65    [Germany  
62.96.169.47    [Germany  
62.171.148.218    [Germany  
62.171.169.86    [Germany  
62.171.176.120    [Germany  
75.119.136.234    [Germany  
77.37.54.176    [Germany  
80.82.219.61    [Germany  
80.158.36.64    [Germany  
80.158.75.176    [Germany  
80.190.220.14    [Germany  
82.165.37.171    [Germany  
82.165.52.114    [Germany  
82.165.115.149    [Germany  
82.165.160.219    [Germany  
82.165.231.56    [Germany  
83.169.3.43    [Germany  
84.46.245.137    [Germany  
84.46.251.86    [Germany  
84.247.129.224    [Germany  
84.247.132.115    [Germany  
84.247.137.47    [Germany  
85.14.195.207    [Germany  
85.14.224.95    [Germany  
85.215.33.145    [Germany  
85.215.66.78    [Germany  
85.215.70.28    [Germany  
86.103.60.72    [Germany  
87.79.80.3    [Germany  
87.106.60.38    [Germany  
87.106.192.127    [Germany  
87.106.234.12    [Germany  
89.22.107.183    [Germany  
89.105.207.45    [Germany  
91.221.116.227    [Germany  
92.205.109.15    [Germany  
92.205.178.143    [Germany  
92.205.188.210    [Germany  
93.90.198.86    [Germany  
95.111.235.93    [Germany  
95.111.235.223    [Germany  
109.123.244.79    [Germany  
109.123.246.148    [Germany  
109.199.115.110    [Germany  
144.91.80.76    [Germany  
144.91.90.12    [Germany  
144.91.116.117    [Germany  
144.91.127.99    [Germany  
147.161.137.15    [Germany  
147.161.229.79    [Germany  
147.161.229.87    [Germany  
147.161.230.110    [Germany  
147.161.230.169    [Germany  
147.161.231.74    [Germany  
147.161.234.112    [Germany  
147.161.234.121    [Germany  
147.161.238.191    [Germany  
149.102.140.31    [Germany  
149.102.152.77    [Germany  
158.220.99.26    [Germany  
158.220.104.83    [Germany  
161.97.80.6    [Germany  
161.97.91.95    [Germany  
161.97.99.89    [Germany  
161.97.126.21    [Germany  
161.97.127.112    [Germany  
161.97.144.21    [Germany  
161.97.155.36    [Germany  
161.97.167.75    [Germany  
161.97.173.177    [Germany  
162.62.63.229    [Germany  
164.68.96.32    [Germany  
164.68.97.79    [Germany  
164.68.105.125    [Germany  
164.68.117.221    [Germany  
164.68.121.114    [Germany  
164.68.122.134    [Germany  
165.225.25.126    [Germany  
165.225.200.197    [Germany  
167.86.75.111    [Germany  
167.86.87.64    [Germany  
167.86.99.44    [Germany  
167.86.101.139    [Germany  
167.86.116.2    [Germany  
167.86.118.55    [Germany  
173.212.195.39    [Germany  
173.212.208.111    [Germany  
173.212.249.224    [Germany  
173.249.6.247    [Germany  
173.249.9.80    [Germany  
173.249.11.237    [Germany  
173.249.12.146    [Germany  
173.249.33.171    [Germany  
176.28.52.209    [Germany  
176.57.189.252    [Germany  
178.254.12.233    [Germany  
184.174.35.59    [Germany  
184.174.36.102    [Germany  
185.27.254.10    [Germany  
185.196.21.58    [Germany  
185.208.206.235    [Germany  
185.209.223.194    [Germany  
185.213.27.81    [Germany  
185.225.233.76    [Germany  
194.146.12.207    [Germany  
194.163.133.180    [Germany  
194.163.135.124    [Germany  
194.163.186.77    [Germany  
194.163.191.94    [Germany  
195.20.249.176    [Germany  
207.180.194.211    [Germany  
207.180.224.225    [Germany  
207.180.242.199    [Germany  
207.180.245.155    [Germany  
207.180.251.208    [Germany  
212.24.127.218    [Germany  
212.48.108.212    [Germany  
212.62.205.66    [Germany  
212.82.61.199    [Germany  
212.83.33.39    [Germany  
212.83.35.186    [Germany  
212.88.141.186    [Germany  
212.227.132.10    [Germany  
213.61.167.197    [Germany  
213.86.106.122    [Germany  
213.153.74.146    [Germany  
213.199.33.106    [Germany  
213.202.222.203    [Germany  
213.202.244.156    [Germany  
217.110.44.72    [Germany  
217.151.158.201    [Germany  
217.160.63.17    [Germany  
62.217.125.18    [Greece  
79.103.225.229    [Greece  
143.233.204.187    [Greece  
147.102.14.28    [Greece  
185.162.236.210    [Greece  
185.162.237.94    [Greece  
185.234.52.108    [Greece  
62.77.128.22    [Hungary  
185.205.248.103    [Hungary  
1.6.5.223    [India  
14.139.231.176    [India  
116.72.18.120    [India  
117.251.87.31    [India  
220.158.183.155    [India  
5.160.140.181    [Iran  
5.200.65.139    [Iran  
5.201.241.30    [Iran  
5.201.241.117    [Iran  
5.201.243.101    [Iran  
5.201.244.136    [Iran  
5.201.245.100    [Iran  
5.201.245.203    [Iran  
5.201.246.131    [Iran  
5.201.247.125    [Iran  
5.201.250.96    [Iran  
5.201.251.231    [Iran  
5.201.252.197    [Iran  
5.212.199.187    [Iran  
5.212.201.237    [Iran  
5.212.217.78    [Iran  
5.212.254.201    [Iran  
5.212.255.89    [Iran  
5.215.192.117    [Iran  
5.215.201.39    [Iran  
5.215.224.54    [Iran  
5.215.233.202    [Iran  
5.215.237.47    [Iran  
5.215.239.23    [Iran  
5.215.250.16    [Iran  
5.217.2.207    [Iran  
5.217.2.235    [Iran  
5.217.4.156    [Iran  
5.217.5.249    [Iran  
5.217.7.227    [Iran  
5.217.9.59    [Iran  
5.217.12.181    [Iran  
5.217.12.254    [Iran  
5.217.13.12    [Iran  
5.217.13.17    [Iran  
5.217.14.123    [Iran  
5.217.14.185    [Iran  
5.217.17.109    [Iran  
5.217.18.136    [Iran  
5.217.18.183    [Iran  
5.217.21.13    [Iran  
5.217.21.90    [Iran  
5.217.23.130    [Iran  
5.217.23.164    [Iran  
5.217.24.81    [Iran  
5.217.26.50    [Iran  
5.217.27.15    [Iran  
5.217.27.83    [Iran  
5.217.27.245    [Iran  
5.217.28.254    [Iran  
5.217.29.45    [Iran  
5.217.32.7    [Iran  
5.217.35.91    [Iran  
5.217.36.50    [Iran  
5.217.36.180    [Iran  
5.217.37.7    [Iran  
5.217.37.91    [Iran  
5.217.39.43    [Iran  
5.217.40.120    [Iran  
5.217.40.173    [Iran  
5.217.40.210    [Iran  
5.217.41.100    [Iran  
5.217.42.45    [Iran  
5.217.43.203    [Iran  
5.217.44.41    [Iran  
5.217.44.138    [Iran  
5.217.45.136    [Iran  
5.217.46.211    [Iran  
5.217.47.22    [Iran  
5.217.47.133    [Iran  
5.217.51.106    [Iran  
5.217.52.42    [Iran  
5.217.53.109    [Iran  
5.217.55.220    [Iran  
5.217.57.35    [Iran  
5.217.57.74    [Iran  
5.217.57.188    [Iran  
5.217.58.174    [Iran  
5.217.60.226    [Iran  
5.217.60.239    [Iran  
5.217.62.25    [Iran  
5.217.62.167    [Iran  
5.217.69.3    [Iran  
5.217.71.106    [Iran  
5.217.71.135    [Iran  
5.217.73.136    [Iran  
5.217.74.38    [Iran  
5.217.75.40    [Iran  
5.217.75.126    [Iran  
5.217.75.241    [Iran  
5.217.84.61    [Iran  
5.217.88.201    [Iran  
5.217.89.203    [Iran  
5.217.90.168    [Iran  
5.217.92.160    [Iran  
5.217.92.168    [Iran  
5.217.93.19    [Iran  
5.217.94.107    [Iran  
5.217.94.146    [Iran  
5.217.99.109    [Iran  
5.217.100.66    [Iran  
5.217.101.155    [Iran  
5.217.102.124    [Iran  
5.217.106.14    [Iran  
5.217.107.250    [Iran  
5.217.111.137    [Iran  
5.217.114.200    [Iran  
5.217.115.217    [Iran  
5.217.117.123    [Iran  
5.217.118.1    [Iran  
5.217.118.57    [Iran  
5.217.118.166    [Iran  
5.217.120.243    [Iran  
5.217.121.138    [Iran  
5.217.121.246    [Iran  
5.217.122.121    [Iran  
5.217.124.101    [Iran  
5.217.124.239    [Iran  
5.217.125.134    [Iran  
5.217.126.154    [Iran  
5.217.127.70    [Iran  
5.217.127.151    [Iran  
5.217.144.173    [Iran  
5.217.144.243    [Iran  
5.217.146.92    [Iran  
5.217.147.14    [Iran  
5.217.147.156    [Iran  
5.217.149.68    [Iran  
5.217.149.84    [Iran  
5.217.150.224    [Iran  
5.217.151.106    [Iran  
5.217.153.2    [Iran  
5.217.153.123    [Iran  
5.217.155.218    [Iran  
5.217.156.186    [Iran  
5.217.157.7    [Iran  
5.217.158.117    [Iran  
5.217.162.113    [Iran  
5.217.162.125    [Iran  
5.217.162.152    [Iran  
5.217.166.173    [Iran  
5.217.166.241    [Iran  
5.217.167.97    [Iran  
5.217.167.117    [Iran  
5.217.167.183    [Iran  
5.217.171.130    [Iran  
5.217.171.190    [Iran  
5.217.173.139    [Iran  
5.217.175.249    [Iran  
5.217.208.24    [Iran  
5.217.211.79    [Iran  
5.217.212.85    [Iran  
5.217.212.157    [Iran  
5.217.213.82    [Iran  
5.217.214.223    [Iran  
5.217.220.116    [Iran  
5.217.221.230    [Iran  
5.217.221.244    [Iran  
5.217.222.90    [Iran  
37.32.9.200    [Iran  
37.98.21.237    [Iran  
37.98.22.90    [Iran  
37.98.23.7    [Iran  
37.98.23.219    [Iran  
37.98.24.145    [Iran  
37.98.24.249    [Iran  
37.98.25.110    [Iran  
37.98.29.231    [Iran  
37.98.33.122    [Iran  
37.98.35.189    [Iran  
37.98.37.122    [Iran  
37.98.38.137    [Iran  
37.98.41.113    [Iran  
37.98.41.220    [Iran  
37.98.44.145    [Iran  
37.98.44.195    [Iran  
37.98.45.22    [Iran  
37.98.45.213    [Iran  
37.98.49.52    [Iran  
37.98.52.127    [Iran  
37.98.55.55    [Iran  
37.98.55.131    [Iran  
37.98.55.213    [Iran  
37.98.57.163    [Iran  
37.98.58.140    [Iran  
37.98.60.16    [Iran  
37.98.60.142    [Iran  
37.98.63.124    [Iran  
46.209.20.166    [Iran  
86.107.208.92    [Iran  
89.45.50.179    [Iran  
89.45.57.229    [Iran  
89.45.59.46    [Iran  
89.45.60.79    [Iran  
89.45.62.26    [Iran  
89.45.62.86    [Iran  
89.45.63.17    [Iran  
94.183.73.245    [Iran  
94.183.75.229    [Iran  
109.108.162.175    [Iran  
109.108.166.178    [Iran  
109.108.167.248    [Iran  
109.108.169.77    [Iran  
109.108.176.57    [Iran  
109.108.176.212    [Iran  
109.108.177.90    [Iran  
109.108.178.108    [Iran  
109.108.179.72    [Iran  
109.108.188.217    [Iran  
109.108.191.250    [Iran  
151.244.86.14    [Iran  
185.73.0.54    [Iran  
188.209.199.39    [Iran  
188.209.201.249    [Iran  
188.209.204.168    [Iran  
188.209.206.90    [Iran  
188.209.207.179    [Iran  
193.151.148.82    [Iran  
37.236.58.87    [Iraq  
37.238.4.36    [Iraq  
37.239.155.87    [Iraq  
78.18.150.130    [Ireland  
78.19.113.51    [Ireland  
85.134.166.208    [Ireland  
89.126.18.89    [Ireland  
193.120.65.211    [Ireland  
194.46.230.164    [Ireland  
2.54.85.227    [Israel  
2.55.80.235    [Israel  
31.168.134.133    [Israel  
31.168.171.91    [Israel  
62.219.210.120    [Israel  
81.218.174.194    [Israel  
82.81.134.35    [Israel  
141.226.123.14    [Israel  
147.236.34.77    [Israel  
212.150.65.140    [Israel  
213.151.38.23    [Israel  
213.151.38.140    [Israel  
213.151.38.175    [Israel  
213.151.38.234    [Israel  
213.151.40.104    [Israel  
213.151.41.183    [Israel  
213.151.42.150    [Israel  
213.151.43.99    [Israel  
213.151.44.167    [Israel  
213.151.45.68    [Israel  
213.151.45.209    [Israel  
213.151.45.219    [Israel  
213.151.46.32    [Israel  
213.151.47.16    [Israel  
213.151.47.130    [Israel  
2.56.251.19    [Italy  
2.235.146.20    [Italy  
5.62.74.196    [Italy  
31.7.149.208    [Italy  
37.100.88.38    [Italy  
45.135.137.7    [Italy  
45.135.137.143    [Italy  
46.28.120.23    [Italy  
46.141.127.114    [Italy  
46.149.169.239    [Italy  
51.179.67.143    [Italy  
62.94.241.233    [Italy  
77.244.188.27    [Italy  
78.152.121.26    [Italy  
80.76.90.197    [Italy  
93.48.194.153    [Italy  
93.49.164.11    [Italy  
93.51.12.142    [Italy  
93.55.232.244    [Italy  
93.56.69.58    [Italy  
94.126.8.129    [Italy  
101.58.149.4    [Italy  
109.168.33.147    [Italy  
109.168.76.98    [Italy  
109.168.91.222    [Italy  
109.238.20.114    [Italy  
138.66.33.228    [Italy  
151.11.249.46    [Italy  
151.29.159.210    [Italy  
151.42.239.191    [Italy  
151.55.165.136    [Italy  
159.255.152.102    [Italy  
159.255.153.157    [Italy  
185.7.115.188    [Italy  
185.105.104.225    [Italy  
185.135.94.17    [Italy  
185.147.116.65    [Italy  
185.147.116.122    [Italy  
185.152.148.243    [Italy  
185.178.8.38    [Italy  
188.95.77.219    [Italy  
192.145.127.210    [Italy  
194.21.40.146    [Italy  
194.62.63.229    [Italy  
212.183.182.8    [Italy  
213.137.36.214    [Italy  
213.140.12.136    [Italy  
92.253.92.88    [Jordan  
212.35.64.106    [Jordan  
212.35.65.235    [Jordan  
85.29.129.98    [Kazakhstan  
156.225.106.26    [Kenya  
197.157.231.18    [Kenya  
197.157.231.29    [Kenya  
203.254.254.92    [Korea, South  
46.99.128.61    [Kosovo  
84.22.59.149    [Kosovo  
78.89.160.245    [Kuwait  
77.38.232.255    [Latvia  
89.111.39.186    [Latvia  
185.8.63.100    [Latvia  
212.142.75.166    [Latvia  
93.126.227.213    [Lebanon  
94.187.97.153    [Lebanon  
94.187.98.3    [Lebanon  
94.187.98.25    [Lebanon  
94.187.98.26    [Lebanon  
94.187.98.153    [Lebanon  
94.187.98.160    [Lebanon  
94.187.101.142    [Lebanon  
94.187.101.192    [Lebanon  
94.187.103.90    [Lebanon  
94.187.103.188    [Lebanon  
94.187.104.144    [Lebanon  
94.187.105.41    [Lebanon  
94.187.105.116    [Lebanon  
94.187.108.58    [Lebanon  
94.187.108.211    [Lebanon  
94.187.108.235    [Lebanon  
94.187.111.244    [Lebanon  
94.187.113.83    [Lebanon  
94.187.114.194    [Lebanon  
94.187.115.9    [Lebanon  
94.187.115.111    [Lebanon  
94.187.116.215    [Lebanon  
94.187.118.104    [Lebanon  
94.187.118.236    [Lebanon  
109.233.17.4    [Lebanon  
178.135.1.39    [Lebanon  
178.135.98.4    [Lebanon  
178.135.98.228    [Lebanon  
178.135.99.21    [Lebanon  
178.135.99.78    [Lebanon  
178.135.100.83    [Lebanon  
178.135.102.120    [Lebanon  
178.135.102.173    [Lebanon  
178.135.103.71    [Lebanon  
178.135.103.126    [Lebanon  
178.135.103.204    [Lebanon  
178.135.104.245    [Lebanon  
178.135.105.175    [Lebanon  
178.135.106.62    [Lebanon  
178.135.107.19    [Lebanon  
178.135.108.14    [Lebanon  
178.135.108.235    [Lebanon  
178.135.109.39    [Lebanon  
178.135.109.234    [Lebanon  
178.135.110.109    [Lebanon  
178.135.110.226    [Lebanon  
178.135.112.170    [Lebanon  
178.135.113.22    [Lebanon  
178.135.113.76    [Lebanon  
178.135.113.89    [Lebanon  
178.135.113.233    [Lebanon  
178.135.115.92    [Lebanon  
178.135.117.1    [Lebanon  
178.135.117.14    [Lebanon  
178.135.117.63    [Lebanon  
178.135.118.12    [Lebanon  
178.135.119.83    [Lebanon  
178.135.119.90    [Lebanon  
178.135.119.241    [Lebanon  
185.176.208.179    [Lebanon  
185.187.130.65    [Lebanon  
213.204.88.54    [Lebanon  
37.156.219.26    [Lithuania  
45.93.138.104    [Lithuania  
80.209.238.216    [Lithuania  
84.15.148.195    [Lithuania  
84.15.246.98    [Lithuania  
89.40.14.61    [Lithuania  
109.235.67.173    [Lithuania  
159.148.10.94    [Lithuania  
185.69.54.17    [Lithuania  
185.81.165.119    [Lithuania  
193.219.38.181    [Lithuania  
193.219.160.77    [Lithuania  
195.14.184.158    [Lithuania  
212.24.111.210    [Lithuania  
41.77.23.242    [Madagascar  
165.225.194.112    [Mexico  
188.169.162.44    [Mexico  
37.233.13.101    [Moldova  
46.55.75.171    [Moldova  
80.245.80.16    [Moldova  
91.242.106.130    [Moldova  
178.168.83.202    [Moldova  
185.202.93.61    [Moldova  
41.214.189.196    [Morocco  
41.214.191.67    [Morocco  
31.201.45.247    [Netherlands  
31.201.96.116    [Netherlands  
37.1.220.113    [Netherlands  
45.81.227.19    [Netherlands  
45.82.65.137    [Netherlands  
45.88.3.46    [Netherlands  
45.155.249.100    [Netherlands  
57.67.219.1    [Netherlands  
80.65.122.229    [Netherlands  
80.89.228.235    [Netherlands  
89.39.107.39    [Netherlands  
109.107.161.176    [Netherlands  
147.161.172.35    [Netherlands  
147.161.172.90    [Netherlands  
147.161.172.197    [Netherlands  
147.161.173.30    [Netherlands  
149.18.45.99    [Netherlands  
165.225.240.93    [Netherlands  
165.225.240.222    [Netherlands  
178.159.39.111    [Netherlands  
185.45.194.180    [Netherlands  
185.132.133.46    [Netherlands  
213.196.40.51    [Netherlands  
154.113.23.103    [Nigeria  
154.113.157.26    [Nigeria  
62.128.242.85    [Norway  
77.40.165.178    [Norway  
77.106.169.102    [Norway  
77.222.174.113    [Norway  
79.161.78.15    [Norway  
81.167.18.57    [Norway  
88.84.34.196    [Norway  
88.93.174.108    [Norway  
89.162.91.9    [Norway  
92.62.37.31    [Norway  
147.161.146.34    [Norway  
147.161.146.117    [Norway  
147.161.147.78    [Norway  
185.97.196.25    [Norway  
193.90.184.41    [Norway  
193.214.114.175    [Norway  
193.214.200.202    [Norway  
213.138.173.159    [Norway  
213.234.85.203    [Norway  
217.144.76.162    [Norway  
31.172.186.140    [Poland  
37.109.8.19    [Poland  
46.20.52.97    [Poland  
62.69.229.105    [Poland  
78.10.140.3    [Poland  
81.26.0.222    [Poland  
83.238.161.216    [Poland  
85.28.142.36    [Poland  
85.115.214.229    [Poland  
85.194.244.69    [Poland  
85.194.244.99    [Poland  
85.198.224.219    [Poland  
85.237.173.118    [Poland  
89.25.128.193    [Poland  
90.156.4.15    [Poland  
91.189.73.107    [Poland  
91.194.228.186    [Poland  
91.203.159.124    [Poland  
91.227.3.77    [Poland  
93.105.88.206    [Poland  
93.190.36.169    [Poland  
94.231.52.36    [Poland  
95.160.202.6    [Poland  
95.175.16.237    [Poland  
109.196.37.240    [Poland  
109.196.41.239    [Poland  
153.19.139.37    [Poland  
176.221.113.210    [Poland  
178.213.143.46    [Poland  
178.219.122.229    [Poland  
185.6.113.180    [Poland  
185.242.154.58    [Poland  
188.191.217.135    [Poland  
193.106.229.51    [Poland  
195.26.78.12    [Poland  
195.164.130.171    [Poland  
195.164.131.192    [Poland  
195.164.132.178    [Poland  
195.164.134.71    [Poland  
195.164.134.187    [Poland  
195.164.134.228    [Poland  
195.164.140.194    [Poland  
195.164.146.5    [Poland  
195.164.152.10    [Poland  
195.164.158.253    [Poland  
195.164.159.203    [Poland  
195.164.159.247    [Poland  
195.164.210.187    [Poland  
195.164.211.79    [Poland  
195.164.220.1    [Poland  
195.164.223.143    [Poland  
195.164.223.242    [Poland  
195.164.225.71    [Poland  
195.164.225.105    [Poland  
195.164.226.112    [Poland  
195.164.254.209    [Poland  
195.164.254.244    [Poland  
212.2.109.7    [Poland  
212.127.93.76    [Poland  
212.191.184.36    [Poland  
213.73.13.99    [Poland  
213.92.204.175    [Poland  
213.136.248.139    [Poland  
217.28.145.14    [Poland  
217.171.49.91    [Poland  
89.153.109.149    [Portugal  
193.236.40.17    [Portugal  
213.205.75.155    [Portugal  
5.2.234.186    [Romania  
5.2.245.172    [Romania  
5.2.249.227    [Romania  
46.214.70.35    [Romania  
46.214.105.198    [Romania  
79.112.180.185    [Romania  
79.113.222.21    [Romania  
79.118.203.215    [Romania  
80.97.1.13    [Romania  
86.120.14.79    [Romania  
86.121.235.174    [Romania  
86.123.97.217    [Romania  
86.123.150.105    [Romania  
86.125.32.56    [Romania  
86.125.129.237    [Romania  
86.127.78.229    [Romania  
86.127.213.194    [Romania  
89.40.182.3    [Romania  
89.165.141.199    [Romania  
92.85.192.99    [Romania  
92.87.22.226    [Romania  
93.115.94.3    [Romania  
94.52.82.52    [Romania  
109.96.62.50    [Romania  
109.98.76.254    [Romania  
109.98.101.46    [Romania  
188.27.62.115    [Romania  
188.173.125.10    [Romania  
188.173.245.254    [Romania  
193.226.53.37    [Romania  
5.188.107.131    [Russia  
31.31.196.253    [Russia  
45.80.70.51    [Russia  
45.146.165.51    [Russia  
45.147.178.134    [Russia  
46.43.201.52    [Russia  
46.46.155.210    [Russia  
46.138.240.39    [Russia  
46.165.16.3    [Russia  
46.165.20.106    [Russia  
46.167.96.3    [Russia  
46.229.134.82    [Russia  
77.87.85.246    [Russia  
78.25.100.102    [Russia  
78.25.109.142    [Russia  
78.25.124.54    [Russia  
78.108.65.213    [Russia  
78.140.249.19    [Russia  
79.173.89.132    [Russia  
83.222.14.12    [Russia  
83.222.15.129    [Russia  
83.242.226.158    [Russia  
84.201.185.250    [Russia  
84.204.174.158    [Russia  
85.26.139.161    [Russia  
85.234.36.116    [Russia  
87.248.224.34    [Russia  
89.111.137.188    [Russia  
89.111.144.106    [Russia  
89.249.18.15    [Russia  
89.249.132.49    [Russia  
91.215.122.228    [Russia  
91.219.99.184    [Russia  
92.50.143.142    [Russia  
93.100.184.111    [Russia  
93.187.181.10    [Russia  
95.153.237.40    [Russia  
95.165.13.65    [Russia  
95.165.30.225    [Russia  
95.165.162.46    [Russia  
95.165.197.115    [Russia  
95.183.15.109    [Russia  
109.188.143.76    [Russia  
109.201.213.39    [Russia  
109.235.190.81    [Russia  
165.225.90.229    [Russia  
165.225.91.56    [Russia  
176.57.69.39    [Russia  
176.111.252.38    [Russia  
176.118.12.9    [Russia  
176.124.35.248    [Russia  
178.72.74.212    [Russia  
178.207.9.194    [Russia  
185.10.0.3    [Russia  
185.17.36.229    [Russia  
185.26.120.110    [Russia  
185.26.121.135    [Russia  
185.46.97.123    [Russia  
185.194.105.218    [Russia  
188.242.69.100    [Russia  
188.242.238.153    [Russia  
188.243.110.58    [Russia  
188.243.117.222    [Russia  
193.109.246.58    [Russia  
194.135.7.190    [Russia  
195.210.178.58    [Russia  
212.21.26.184    [Russia  
213.87.14.158    [Russia  
217.16.27.159    [Russia  
217.112.42.91    [Russia  
31.166.15.43    [Saudi Arabia  
78.93.153.215    [Saudi Arabia  
78.93.154.27    [Saudi Arabia  
78.93.157.159    [Saudi Arabia  
98.98.138.31    [Saudi Arabia  
213.230.21.244    [Saudi Arabia  
5.22.186.86    [Serbia  
93.87.82.118    [Serbia  
93.87.127.47    [Serbia  
93.187.241.128    [Serbia  
93.187.241.240    [Serbia  
93.187.242.100    [Serbia  
93.187.242.201    [Serbia  
93.187.243.32    [Serbia  
93.187.243.106    [Serbia  
178.220.122.254    [Serbia  
178.221.149.155    [Serbia  
178.222.70.78    [Serbia  
178.222.243.70    [Serbia  
212.62.37.75    [Serbia  
212.62.37.221    [Serbia  
212.200.36.199    [Serbia  
212.200.127.97    [Serbia  
164.90.100.100    [Singapore  
164.90.100.139    [Singapore  
46.175.6.220    [Slovakia  
62.197.218.4    [Slovakia  
86.110.242.203    [Slovakia  
94.136.146.246    [Slovakia  
95.105.223.109    [Slovakia  
95.105.252.197    [Slovakia  
185.160.110.221    [Slovakia  
188.121.160.26    [Slovakia  
213.108.127.249    [Slovakia  
37.18.230.156    [Slovenia  
37.18.234.156    [Slovenia  
192.71.244.130    [Slovenia  
41.160.73.210    [South Africa  
41.206.213.12    [South Africa  
102.132.207.212    [South Africa  
155.93.168.120    [South Africa  
188.164.22.35    [South Africa  
31.210.227.14    [Spain  
37.61.145.171    [Spain  
45.128.8.16    [Spain  
77.26.210.153    [Spain  
82.223.5.25    [Spain  
85.50.170.99    [Spain  
85.54.140.249    [Spain  
85.85.246.143    [Spain  
85.87.24.147    [Spain  
85.87.115.208    [Spain  
85.152.20.17    [Spain  
87.221.27.46    [Spain  
89.29.188.50    [Spain  
89.29.229.4    [Spain  
90.164.27.9    [Spain  
91.116.216.43    [Spain  
92.53.196.153    [Spain  
92.58.166.35    [Spain  
92.187.56.252    [Spain  
95.18.173.18    [Spain  
139.47.103.206    [Spain  
147.156.43.36    [Spain  
161.111.84.8    [Spain  
170.253.36.22    [Spain  
176.57.104.205    [Spain  
178.237.154.31    [Spain  
178.251.18.61    [Spain  
185.238.232.70    [Spain  
188.171.46.55    [Spain  
188.240.134.105    [Spain  
193.111.53.176    [Spain  
193.176.100.158    [Spain  
194.8.141.196    [Spain  
194.30.32.66    [Spain  
194.30.35.130    [Spain  
194.30.99.150    [Spain  
207.188.131.205    [Spain  
212.81.201.45    [Spain  
212.81.209.102    [Spain  
212.142.155.119    [Spain  
212.230.181.116    [Spain  
212.231.184.53    [Spain  
212.231.184.190    [Spain  
213.27.214.89    [Spain  
213.60.180.154    [Spain  
213.195.123.44    [Spain  
213.195.125.197    [Spain  
196.202.146.102    [Sudan  
2.65.63.32    [Sweden  
5.150.254.86    [Sweden  
31.208.97.133    [Sweden  
46.246.6.10    [Sweden  
62.220.167.82    [Sweden  
65.99.164.19    [Sweden  
77.53.177.133    [Sweden  
81.93.142.130    [Sweden  
81.170.179.238    [Sweden  
81.170.255.232    [Sweden  
84.216.172.122    [Sweden  
84.218.32.105    [Sweden  
85.89.68.220    [Sweden  
85.227.86.37    [Sweden  
85.227.86.157    [Sweden  
92.32.70.143    [Sweden  
94.103.198.61    [Sweden  
94.254.30.73    [Sweden  
95.209.130.109    [Sweden  
95.209.132.225    [Sweden  
147.161.151.94    [Sweden  
147.161.188.165    [Sweden  
155.4.204.164    [Sweden  
155.4.225.214    [Sweden  
185.6.9.89    [Sweden  
193.181.48.45    [Sweden  
194.15.212.161    [Sweden  
195.54.113.239    [Sweden  
195.170.187.86    [Sweden  
195.178.173.82    [Sweden  
213.112.238.77    [Sweden  
213.113.208.220    [Sweden  
213.115.200.188    [Sweden  
80.254.186.53    [Switzerland  
82.192.232.14    [Switzerland  
84.254.108.242    [Switzerland  
84.254.111.111    [Switzerland  
91.132.136.27    [Switzerland  
95.143.60.112    [Switzerland  
109.205.171.140    [Switzerland  
157.143.75.41    [Switzerland  
165.225.94.137    [Switzerland  
185.149.92.88    [Switzerland  
185.149.92.124    [Switzerland  
185.160.246.189    [Switzerland  
193.246.181.160    [Switzerland  
213.158.147.115    [Switzerland  
213.160.43.142    [Switzerland  
41.93.33.43    [Tanzania  
5.26.33.30    [Turkey  
5.26.169.79    [Turkey  
5.26.215.72    [Turkey  
93.89.64.6    [Turkey  
151.250.59.14    [Turkey  
178.242.189.122    [Turkey  
195.46.130.8    [Turkey  
195.46.130.105    [Turkey  
5.58.52.110    [Ukraine  
5.58.106.110    [Ukraine  
31.135.153.109    [Ukraine  
31.202.79.104    [Ukraine  
37.25.117.126    [Ukraine  
91.196.148.183    [Ukraine  
109.108.69.179    [Ukraine  
165.225.94.107    [Ukraine  
171.25.169.67    [Ukraine  
176.32.4.41    [Ukraine  
176.38.17.223    [Ukraine  
176.103.58.43    [Ukraine  
176.118.49.233    [Ukraine  
178.158.245.43    [Ukraine  
185.126.112.254    [Ukraine  
185.199.97.82    [Ukraine  
193.34.92.107    [Ukraine  
193.93.217.2    [Ukraine  
217.77.220.248    [Ukraine  
168.253.63.123    [Zimbabwe  
185.172.128.127    [Russia  
35.198.77.44    [Germany  
87.230.98.78    [Germany  
80.150.6.138    [Germany  
95.100.158.57    [Germany  
45.9.74.5    [Germany  
92.205.64.87    [Germany  
41.107.244.233    [Algeria  
83.217.92.214    [Belgium  
23.34.44.220    [Denmark  
2.21.23.144    [France  
2.22.28.161    [France  
104.125.3.26    [France  
23.55.161.185    [Germany  
202.61.232.169    [Germany  
79.172.211.3    [Hungary  
5.79.71.225    [Netherlands  
154.41.249.121    [Netherlands  
154.41.249.206    [Netherlands  
191.96.63.243    [Netherlands  
31.14.220.15    [Romania  
5.101.153.166    [Russia  
85.119.149.37    [Russia  
151.248.116.239    [Russia  
185.172.128.142    [Russia  
45.80.180.85    [Singapore  
5.42.66.0    [Russia  
194.14.254.76    [Belgium  
92.204.239.213    [Germany  
81.171.8.143    [Netherlands  
95.100.158.19    [Germany  
80.67.16.8    [Germany  
37.235.63.40    [Austria  
49.44.53.43    [India  
185.216.143.63    [Netherlands  
72.246.29.124    [Germany  
213.239.154.31    [Netherlands  
217.6.73.195    [Germany  
23.2.13.146    [Germany  
23.2.13.8    [Germany  
217.148.3.184    [Switzerland  
156.253.117.154    [China  
85.10.51.135    [Croatia  
45.153.241.70    [Germany  
77.37.53.228    [Germany  
92.205.196.1    [Germany  
134.119.225.201    [Germany  
103.163.138.8    [Indonesia  
46.17.175.217    [Lithuania  
5.44.45.201    [Netherlands  
5.79.68.103    [Netherlands  
154.62.105.111    [Netherlands  
45.67.38.85    [Romania  
185.175.158.40    [Russia  
91.192.111.86    [Spain  
195.192.255.150    [Spain  
2.21.22.177    [Switzerland  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-5500420249 Emotet Malware Alert**

Malware Alert Brief:  
  
  
Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
61.76.222.210    [Korea,  South  
103.253.75.46    [Thailand  
103.85.95.5    [Indonesia  
195.144.11.124    [France  
195.144.11.125    [France  
51.89.36.180    [Poland  
112.213.89.73    [Vietnam  
81.213.175.132    [Turkey  
115.79.195.246    [Vietnam  
193.53.245.52    [Turkey  
130.0.132.242    [Italy  
202.79.24.136    [Cambodia  
89.121.205.18    [Romania  
173.249.6.108    [Germany  
161.0.153.60    [Trinidad and Tobago  
77.74.78.80    [Russia  
197.245.25.228    [South Africa  
51.159.23.217    [France  
173.212.214.235    [Germany  
139.59.107.152    [Singapore  
93.89.224.199    [Turkey  
49.205.182.134    [India  
5.196.108.185    [Netherlands  
159.89.0.247    [Germany  
51.75.33.127    [Poland  
219.92.13.25    [Malaysia  
5.12.246.155    [Romania  
89.25.223.211    [Poland  
118.101.24.148    [Malaysia  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-8320420249 Agent Tesla Malware Alert**

Malware Alert Brief:  
  
Agent Tesla usually spreads through phishing. However, the malware has a function which allows it to run automatically from a USB stick. At present, Agent Tesla is able to operate exclusively on Windows machines.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
203.175.9.22    [Indonesia  
45.252.248.26    [Vietnam  
61.19.247.49    [Thailand  
86.96.202.167    [United Arab Emirates  
194.36.191.196    [Netherlands  
61.19.247.160    [Thailand  
185.99.1.126    [Bosnia and Herzegovina  
5.255.100.203    [Netherlands  
103.55.39.182    [Indonesia  
5.56.37.3    [Hungary  
45.134.160.220    [Romania  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-2770420249 SocGholish Malware Alert**

Malware Alert Brief:  
  
  
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.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
45.130.201.22    [Bulgaria  
185.216.114.10    [Turkey  
103.249.111.96    [China  
45.130.201.24    [Bulgaria  
77.245.56.14    [Netherlands  
5.101.115.147    [Estonia  
35.215.148.34    [China  
35.213.134.69    [Singapore  
114.119.146.19    [Singapore  
93.190.41.79    [Ukraine  
114.119.159.87    [Singapore  
217.160.0.215    [Germany  
103.90.234.120    [Vietnam  
31.220.15.143    [Sweden  
103.233.193.206    [Thailand  
114.119.138.59    [Singapore  
43.243.118.8    [Singapore  
101.44.248.101    [China  
114.119.141.42    [Singapore  
103.116.18.240    [India  
109.125.100.73    [Germany  
77.75.77.72    [Czechia  
5.61.51.32    [Netherlands  
8.217.184.171    [China  
101.44.250.38    [China  
103.247.11.149    [Indonesia  
182.253.182.66    [Indonesia  
35.213.179.55    [Singapore  
128.199.79.68    [Singapore  
194.247.173.99    [Ukraine  
34.22.161.106    [Belgium  
117.241.42.70    [India  
18.201.62.166    [Ireland  
3.38.76.70    [Korea,  South  
45.82.65.67    [Netherlands  
109.248.14.9    [Russia  
47.128.27.112    [Singapore  
47.128.58.169    [Singapore  
168.138.161.115    [Singapore  
172.70.143.88    [Singapore  
203.117.159.21    [Singapore  
154.118.228.210    [Tanzania  
165.154.118.169    [Thailand  
27.71.226.176    [Vietnam  
27.77.231.52    [Vietnam  
27.77.234.40    [Vietnam  
116.107.217.237    [Vietnam  
171.250.222.211    [Vietnam  
114.119.146.195    [Singapore  
52.76.164.223    [Singapore  
195.201.106.142    [Germany  
114.119.152.128    [Singapore  
43.225.54.142    [India  
176.9.17.6    [Germany  
15.206.238.26    [India  
77.245.57.108    [Netherlands  
185.187.241.36    [Singapore  
103.195.240.100    [Vietnam  
103.241.24.178    [Indonesia  
35.213.157.114    [Singapore  
103.14.99.210    [India  
52.193.33.255    [Japan  
27.147.219.90    [Bangladesh  
65.108.203.133    [Finland  
37.247.65.3    [Germany  
78.49.13.19    [Germany  
178.18.252.24    [Germany  
159.65.149.19    [India  
5.61.55.96    [Netherlands  
47.128.115.150    [Singapore  
178.128.58.178    [Singapore  
217.115.34.254    [Sweden  
185.181.61.115    [Unknown  
103.67.163.199    [Vietnam  
45.64.96.61    [Indonesia  
114.119.153.172    [Singapore  
101.44.248.16    [China  
101.44.248.25    [China  
13.212.139.47    [Singapore  
103.28.36.229    [Vietnam  
195.24.68.25    [Russia  
103.41.206.215    [Indonesia  
65.109.92.51    [Finland  
43.252.212.83    [Malaysia  
36.133.172.82    [China  
178.128.222.61    [Singapore  
138.201.223.146    [Germany  
94.198.140.19    [Austria  
77.71.114.10    [Bulgaria  
176.151.25.212    [France  
132.195.105.167    [Germany  
5.255.231.52    [Russia  
5.255.231.108    [Russia  
95.163.255.3    [Russia  
176.100.243.133    [Russia  
43.255.154.55    [Singapore  
47.128.32.70    [Singapore  
47.128.98.124    [Singapore  
47.128.99.203    [Singapore  
114.119.132.207    [Singapore  
114.119.150.227    [Singapore  
172.71.82.62    [Singapore  
103.216.113.30    [Vietnam  
103.74.120.142    [Vietnam  
103.111.187.214    [Indonesia  
148.66.132.187    [Singapore  
203.147.24.238    [Thailand  
202.29.173.62    [Thailand  
139.162.60.246    [Singapore  
46.142.26.17    [Germany  
89.14.169.175    [Germany  
93.132.25.83    [Germany  
43.242.126.162    [India  
182.253.119.226    [Indonesia  
34.253.48.150    [Ireland  
45.128.163.132    [Lithuania  
91.92.252.144    [Netherlands  
195.23.56.180    [Portugal  
35.213.152.73    [Singapore  
43.163.8.36    [Singapore  
47.128.30.115    [Singapore  
162.158.162.74    [Singapore  
165.154.224.61    [Singapore  
103.142.88.58    [Indonesia  
119.59.104.24    [Thailand  
27.77.230.72    [Vietnam  
103.31.251.235    [Indonesia  
135.181.213.220    [Finland  
92.53.96.139    [Russia  
103.21.59.22    [India  
217.160.0.246    [Germany  
65.108.64.210    [Finland  
135.181.74.243    [Finland  
135.181.79.106    [Finland  
135.181.180.59    [Finland  
95.91.104.243    [Germany  
136.243.228.198    [Germany  
159.89.110.144    [Germany  
182.253.247.198    [Indonesia  
80.66.79.9    [Moldova  
178.128.115.77    [Singapore  
51.20.182.8    [Sweden  
119.42.79.89    [Thailand  
134.236.98.71    [Thailand  
178.150.14.250    [Ukraine  
27.75.158.77    [Vietnam  
116.100.222.30    [Vietnam  
116.104.160.95    [Vietnam  
171.247.243.190    [Vietnam  
171.248.222.228    [Vietnam  
171.254.2.236    [Vietnam  
36.133.35.23    [China  
112.78.177.135    [Indonesia  
47.128.31.255    [Singapore  
47.128.97.43    [Singapore  
47.128.113.20    [Singapore  
47.128.123.254    [Singapore  
27.77.235.183    [Vietnam  
113.20.31.21    [Indonesia  
171.253.51.66    [Vietnam  
103.164.192.81    [Indonesia  
220.158.236.241    [Bhutan  
139.99.53.127    [Thailand  
103.166.9.110    [Indonesia  
5.61.48.253    [Netherlands  
65.21.232.254    [Finland  
213.186.33.16    [France  
43.157.66.187    [Germany  
91.248.178.47    [Germany  
172.71.160.141    [Germany  
103.88.169.6    [Indonesia  
111.68.117.200    [Indonesia  
111.68.127.170    [Indonesia  
115.85.74.114    [Indonesia  
121.100.4.170    [Indonesia  
35.204.196.112    [Netherlands  
91.92.241.96    [Netherlands  
94.156.69.36    [Netherlands  
192.140.149.81    [Pakistan  
47.128.16.20    [Singapore  
47.128.16.66    [Singapore  
47.128.16.88    [Singapore  
47.128.16.101    [Singapore  
47.128.16.122    [Singapore  
47.128.17.187    [Singapore  
47.128.18.14    [Singapore  
47.128.18.17    [Singapore  
47.128.18.170    [Singapore  
47.128.18.222    [Singapore  
47.128.18.236    [Singapore  
47.128.18.247    [Singapore  
47.128.19.252    [Singapore  
47.128.20.11    [Singapore  
47.128.20.34    [Singapore  
47.128.20.121    [Singapore  
47.128.20.190    [Singapore  
47.128.21.26    [Singapore  
47.128.21.118    [Singapore  
47.128.21.151    [Singapore  
47.128.22.85    [Singapore  
47.128.22.171    [Singapore  
47.128.22.237    [Singapore  
47.128.23.50    [Singapore  
47.128.23.92    [Singapore  
47.128.23.253    [Singapore  
47.128.25.57    [Singapore  
47.128.25.179    [Singapore  
47.128.25.186    [Singapore  
47.128.25.195    [Singapore  
47.128.25.231    [Singapore  
47.128.26.33    [Singapore  
47.128.27.38    [Singapore  
47.128.28.22    [Singapore  
47.128.28.92    [Singapore  
47.128.28.122    [Singapore  
47.128.29.61    [Singapore  
47.128.29.97    [Singapore  
47.128.31.4    [Singapore  
47.128.31.39    [Singapore  
47.128.31.63    [Singapore  
47.128.31.201    [Singapore  
47.128.31.239    [Singapore  
47.128.32.16    [Singapore  
47.128.32.107    [Singapore  
47.128.32.158    [Singapore  
47.128.32.236    [Singapore  
47.128.33.28    [Singapore  
47.128.33.48    [Singapore  
47.128.34.18    [Singapore  
47.128.34.52    [Singapore  
47.128.34.159    [Singapore  
47.128.34.163    [Singapore  
47.128.34.191    [Singapore  
47.128.34.216    [Singapore  
47.128.34.251    [Singapore  
47.128.34.252    [Singapore  
47.128.35.88    [Singapore  
47.128.35.173    [Singapore  
47.128.35.235    [Singapore  
47.128.36.143    [Singapore  
47.128.36.146    [Singapore  
47.128.38.101    [Singapore  
47.128.39.121    [Singapore  
47.128.39.208    [Singapore  
47.128.39.238    [Singapore  
47.128.40.54    [Singapore  
47.128.41.92    [Singapore  
47.128.41.154    [Singapore  
47.128.41.192    [Singapore  
47.128.41.207    [Singapore  
47.128.41.241    [Singapore  
47.128.42.45    [Singapore  
47.128.42.56    [Singapore  
47.128.42.214    [Singapore  
47.128.42.223    [Singapore  
47.128.43.242    [Singapore  
47.128.43.249    [Singapore  
47.128.44.31    [Singapore  
47.128.44.35    [Singapore  
47.128.44.99    [Singapore  
47.128.44.165    [Singapore  
47.128.45.102    [Singapore  
47.128.45.147    [Singapore  
47.128.45.246    [Singapore  
47.128.46.48    [Singapore  
47.128.47.49    [Singapore  
47.128.47.75    [Singapore  
47.128.47.215    [Singapore  
47.128.49.28    [Singapore  
47.128.49.60    [Singapore  
47.128.49.88    [Singapore  
47.128.49.123    [Singapore  
47.128.49.146    [Singapore  
47.128.49.156    [Singapore  
47.128.49.221    [Singapore  
47.128.50.38    [Singapore  
47.128.50.42    [Singapore  
47.128.50.249    [Singapore  
47.128.51.43    [Singapore  
47.128.51.165    [Singapore  
47.128.51.252    [Singapore  
47.128.52.17    [Singapore  
47.128.52.26    [Singapore  
47.128.52.140    [Singapore  
47.128.52.173    [Singapore  
47.128.53.2    [Singapore  
47.128.53.32    [Singapore  
47.128.53.37    [Singapore  
47.128.53.65    [Singapore  
47.128.53.113    [Singapore  
47.128.53.114    [Singapore  
47.128.53.159    [Singapore  
47.128.53.211    [Singapore  
47.128.54.72    [Singapore  
47.128.54.78    [Singapore  
47.128.54.106    [Singapore  
47.128.54.153    [Singapore  
47.128.55.75    [Singapore  
47.128.56.111    [Singapore  
47.128.57.77    [Singapore  
47.128.57.121    [Singapore  
47.128.57.178    [Singapore  
47.128.58.111    [Singapore  
47.128.59.10    [Singapore  
47.128.59.26    [Singapore  
47.128.59.28    [Singapore  
47.128.59.89    [Singapore  
47.128.59.109    [Singapore  
47.128.59.158    [Singapore  
47.128.59.169    [Singapore  
47.128.59.194    [Singapore  
47.128.59.228    [Singapore  
47.128.60.181    [Singapore  
47.128.61.53    [Singapore  
47.128.61.54    [Singapore  
47.128.61.57    [Singapore  
47.128.61.88    [Singapore  
47.128.61.140    [Singapore  
47.128.62.23    [Singapore  
47.128.63.37    [Singapore  
47.128.63.77    [Singapore  
47.128.63.147    [Singapore  
47.128.63.163    [Singapore  
47.128.63.229    [Singapore  
47.128.96.60    [Singapore  
47.128.96.61    [Singapore  
47.128.96.155    [Singapore  
47.128.96.185    [Singapore  
47.128.96.214    [Singapore  
47.128.97.14    [Singapore  
47.128.97.62    [Singapore  
47.128.97.108    [Singapore  
47.128.97.126    [Singapore  
47.128.97.169    [Singapore  
47.128.98.7    [Singapore  
47.128.98.82    [Singapore  
47.128.99.37    [Singapore  
47.128.99.92    [Singapore  
47.128.110.18    [Singapore  
47.128.110.189    [Singapore  
47.128.110.224    [Singapore  
47.128.111.182    [Singapore  
47.128.111.206    [Singapore  
47.128.111.216    [Singapore  
47.128.112.32    [Singapore  
47.128.112.38    [Singapore  
47.128.113.123    [Singapore  
47.128.113.209    [Singapore  
47.128.114.57    [Singapore  
47.128.114.149    [Singapore  
47.128.114.184    [Singapore  
47.128.115.76    [Singapore  
47.128.115.128    [Singapore  
47.128.115.134    [Singapore  
47.128.116.13    [Singapore  
47.128.116.40    [Singapore  
47.128.116.56    [Singapore  
47.128.116.195    [Singapore  
47.128.116.205    [Singapore  
47.128.117.30    [Singapore  
47.128.117.150    [Singapore  
47.128.117.190    [Singapore  
47.128.118.19    [Singapore  
47.128.118.29    [Singapore  
47.128.118.33    [Singapore  
47.128.118.43    [Singapore  
47.128.118.68    [Singapore  
47.128.118.122    [Singapore  
47.128.118.242    [Singapore  
47.128.119.206    [Singapore  
47.128.120.236    [Singapore  
47.128.121.6    [Singapore  
47.128.121.33    [Singapore  
47.128.121.85    [Singapore  
47.128.121.130    [Singapore  
47.128.121.190    [Singapore  
47.128.122.5    [Singapore  
47.128.122.61    [Singapore  
47.128.122.249    [Singapore  
47.128.122.255    [Singapore  
47.128.123.114    [Singapore  
47.128.123.192    [Singapore  
47.128.124.10    [Singapore  
47.128.124.232    [Singapore  
47.128.124.246    [Singapore  
47.128.125.137    [Singapore  
47.128.126.72    [Singapore  
47.128.126.137    [Singapore  
47.128.126.214    [Singapore  
47.128.127.35    [Singapore  
47.128.127.89    [Singapore  
47.128.127.145    [Singapore  
103.253.145.216    [Singapore  
114.119.149.81    [Singapore  
114.119.149.150    [Singapore  
124.6.63.115    [Singapore  
149.28.149.167    [Singapore  
1.1.227.194    [Thailand  
101.108.183.239    [Thailand  
203.113.114.94    [Thailand  
37.115.152.141    [Ukraine  
109.70.100.67    [Unknown  
27.73.20.249    [Vietnam  
27.75.149.22    [Vietnam  
27.75.156.72    [Vietnam  
27.75.159.233    [Vietnam  
27.77.237.89    [Vietnam  
116.100.217.33    [Vietnam  
171.234.164.1    [Vietnam  
171.247.245.204    [Vietnam  
171.250.221.71    [Vietnam  
171.253.51.77    [Vietnam  
171.254.218.11    [Vietnam  
194.233.72.194    [Singapore  
103.28.36.224    [Vietnam  
171.238.63.40    [Vietnam  
47.128.19.48    [Singapore  
47.128.19.60    [Singapore  
65.108.227.178    [Finland  
182.253.152.152    [Indonesia  
154.159.243.188    [Kenya  
18.136.249.219    [Singapore  
47.128.16.27    [Singapore  
47.128.16.44    [Singapore  
47.128.16.164    [Singapore  
47.128.16.189    [Singapore  
47.128.17.40    [Singapore  
47.128.17.53    [Singapore  
47.128.17.58    [Singapore  
47.128.17.85    [Singapore  
47.128.17.114    [Singapore  
47.128.17.125    [Singapore  
47.128.17.168    [Singapore  
47.128.17.225    [Singapore  
47.128.18.43    [Singapore  
47.128.18.74    [Singapore  
47.128.18.87    [Singapore  
47.128.18.129    [Singapore  
47.128.18.139    [Singapore  
47.128.18.180    [Singapore  
47.128.19.94    [Singapore  
47.128.19.228    [Singapore  
47.128.20.19    [Singapore  
47.128.20.105    [Singapore  
47.128.20.237    [Singapore  
47.128.20.240    [Singapore  
47.128.20.243    [Singapore  
47.128.21.17    [Singapore  
47.128.21.119    [Singapore  
47.128.21.137    [Singapore  
47.128.21.196    [Singapore  
47.128.21.210    [Singapore  
47.128.21.227    [Singapore  
47.128.21.254    [Singapore  
47.128.22.29    [Singapore  
47.128.22.45    [Singapore  
47.128.22.116    [Singapore  
47.128.22.182    [Singapore  
47.128.23.61    [Singapore  
47.128.23.76    [Singapore  
47.128.23.84    [Singapore  
47.128.23.105    [Singapore  
47.128.23.113    [Singapore  
47.128.23.120    [Singapore  
47.128.23.129    [Singapore  
47.128.23.193    [Singapore  
47.128.24.5    [Singapore  
47.128.24.96    [Singapore  
47.128.25.21    [Singapore  
47.128.25.109    [Singapore  
47.128.25.138    [Singapore  
47.128.25.148    [Singapore  
47.128.25.216    [Singapore  
47.128.25.218    [Singapore  
47.128.25.227    [Singapore  
47.128.25.246    [Singapore  
47.128.26.13    [Singapore  
47.128.26.32    [Singapore  
47.128.26.60    [Singapore  
47.128.26.72    [Singapore  
47.128.26.117    [Singapore  
47.128.26.124    [Singapore  
47.128.26.129    [Singapore  
47.128.26.220    [Singapore  
47.128.26.245    [Singapore  
47.128.27.39    [Singapore  
47.128.27.120    [Singapore  
47.128.27.127    [Singapore  
47.128.27.129    [Singapore  
47.128.27.141    [Singapore  
47.128.27.235    [Singapore  
47.128.28.26    [Singapore  
47.128.28.88    [Singapore  
47.128.28.110    [Singapore  
47.128.28.238    [Singapore  
47.128.29.16    [Singapore  
47.128.29.28    [Singapore  
47.128.29.126    [Singapore  
47.128.29.146    [Singapore  
47.128.29.193    [Singapore  
47.128.29.200    [Singapore  
47.128.29.236    [Singapore  
47.128.30.6    [Singapore  
47.128.30.95    [Singapore  
47.128.30.108    [Singapore  
47.128.30.188    [Singapore  
47.128.30.247    [Singapore  
47.128.31.14    [Singapore  
47.128.31.52    [Singapore  
47.128.31.98    [Singapore  
47.128.31.111    [Singapore  
47.128.31.160    [Singapore  
47.128.31.186    [Singapore  
47.128.32.7    [Singapore  
47.128.32.103    [Singapore  
47.128.32.196    [Singapore  
47.128.33.30    [Singapore  
47.128.33.147    [Singapore  
47.128.33.160    [Singapore  
47.128.33.186    [Singapore  
47.128.34.8    [Singapore  
47.128.34.64    [Singapore  
47.128.34.101    [Singapore  
47.128.34.123    [Singapore  
47.128.34.180    [Singapore  
47.128.34.208    [Singapore  
47.128.34.244    [Singapore  
47.128.35.20    [Singapore  
47.128.35.78    [Singapore  
47.128.35.89    [Singapore  
47.128.35.134    [Singapore  
47.128.35.166    [Singapore  
47.128.35.167    [Singapore  
47.128.35.192    [Singapore  
47.128.36.23    [Singapore  
47.128.36.28    [Singapore  
47.128.36.35    [Singapore  
47.128.36.165    [Singapore  
47.128.36.184    [Singapore  
47.128.36.245    [Singapore  
47.128.37.11    [Singapore  
47.128.37.156    [Singapore  
47.128.37.159    [Singapore  
47.128.37.253    [Singapore  
47.128.38.42    [Singapore  
47.128.38.74    [Singapore  
47.128.38.86    [Singapore  
47.128.38.157    [Singapore  
47.128.38.230    [Singapore  
47.128.39.27    [Singapore  
47.128.39.124    [Singapore  
47.128.39.219    [Singapore  
47.128.40.27    [Singapore  
47.128.40.45    [Singapore  
47.128.40.88    [Singapore  
47.128.40.96    [Singapore  
47.128.40.114    [Singapore  
47.128.40.153    [Singapore  
47.128.40.237    [Singapore  
47.128.41.61    [Singapore  
47.128.41.90    [Singapore  
47.128.41.93    [Singapore  
47.128.41.104    [Singapore  
47.128.41.165    [Singapore  
47.128.42.82    [Singapore  
47.128.42.136    [Singapore  
47.128.42.162    [Singapore  
47.128.43.69    [Singapore  
47.128.44.24    [Singapore  
47.128.44.48    [Singapore  
47.128.44.87    [Singapore  
47.128.44.130    [Singapore  
47.128.44.168    [Singapore  
47.128.44.243    [Singapore  
47.128.45.58    [Singapore  
47.128.45.110    [Singapore  
47.128.45.206    [Singapore  
47.128.45.223    [Singapore  
47.128.45.237    [Singapore  
47.128.45.243    [Singapore  
47.128.45.255    [Singapore  
47.128.46.60    [Singapore  
47.128.46.75    [Singapore  
47.128.46.84    [Singapore  
47.128.46.91    [Singapore  
47.128.46.158    [Singapore  
47.128.46.167    [Singapore  
47.128.47.19    [Singapore  
47.128.47.25    [Singapore  
47.128.47.82    [Singapore  
47.128.47.116    [Singapore  
47.128.47.166    [Singapore  
47.128.47.173    [Singapore  
47.128.47.184    [Singapore  
47.128.47.205    [Singapore  
47.128.47.232    [Singapore  
47.128.48.249    [Singapore  
47.128.49.36    [Singapore  
47.128.49.57    [Singapore  
47.128.49.79    [Singapore  
47.128.49.188    [Singapore  
47.128.49.200    [Singapore  
47.128.49.243    [Singapore  
47.128.50.50    [Singapore  
47.128.50.76    [Singapore  
47.128.51.27    [Singapore  
47.128.51.31    [Singapore  
47.128.51.60    [Singapore  
47.128.51.84    [Singapore  
47.128.51.102    [Singapore  
47.128.51.123    [Singapore  
47.128.51.175    [Singapore  
47.128.51.204    [Singapore  
47.128.52.35    [Singapore  
47.128.52.85    [Singapore  
47.128.52.98    [Singapore  
47.128.52.142    [Singapore  
47.128.52.214    [Singapore  
47.128.52.242    [Singapore  
47.128.53.10    [Singapore  
47.128.53.64    [Singapore  
47.128.53.68    [Singapore  
47.128.53.97    [Singapore  
47.128.53.112    [Singapore  
47.128.53.157    [Singapore  
47.128.53.223    [Singapore  
47.128.54.10    [Singapore  
47.128.54.41    [Singapore  
47.128.54.151    [Singapore  
47.128.54.196    [Singapore  
47.128.55.249    [Singapore  
47.128.56.242    [Singapore  
47.128.57.2    [Singapore  
47.128.57.19    [Singapore  
47.128.57.39    [Singapore  
47.128.57.71    [Singapore  
47.128.57.96    [Singapore  
47.128.57.113    [Singapore  
47.128.57.193    [Singapore  
47.128.58.106    [Singapore  
47.128.59.21    [Singapore  
47.128.59.213    [Singapore  
47.128.60.6    [Singapore  
47.128.60.63    [Singapore  
47.128.60.148    [Singapore  
47.128.60.220    [Singapore  
47.128.60.224    [Singapore  
47.128.60.229    [Singapore  
47.128.61.117    [Singapore  
47.128.61.143    [Singapore  
47.128.61.201    [Singapore  
47.128.61.217    [Singapore  
47.128.61.222    [Singapore  
47.128.61.242    [Singapore  
47.128.62.35    [Singapore  
47.128.62.42    [Singapore  
47.128.62.94    [Singapore  
47.128.62.97    [Singapore  
47.128.62.134    [Singapore  
47.128.62.167    [Singapore  
47.128.62.170    [Singapore  
47.128.62.195    [Singapore  
47.128.63.11    [Singapore  
47.128.63.49    [Singapore  
47.128.63.70    [Singapore  
47.128.63.93    [Singapore  
47.128.63.136    [Singapore  
47.128.63.154    [Singapore  
47.128.63.243    [Singapore  
47.128.63.255    [Singapore  
47.128.96.89    [Singapore  
47.128.96.104    [Singapore  
47.128.96.137    [Singapore  
47.128.97.109    [Singapore  
47.128.97.114    [Singapore  
47.128.97.133    [Singapore  
47.128.97.146    [Singapore  
47.128.97.174    [Singapore  
47.128.98.31    [Singapore  
47.128.98.77    [Singapore  
47.128.98.142    [Singapore  
47.128.98.213    [Singapore  
47.128.99.120    [Singapore  
47.128.99.122    [Singapore  
47.128.99.218    [Singapore  
47.128.109.52    [Singapore  
47.128.109.74    [Singapore  
47.128.110.80    [Singapore  
47.128.110.222    [Singapore  
47.128.111.41    [Singapore  
47.128.111.67    [Singapore  
47.128.111.178    [Singapore  
47.128.111.198    [Singapore  
47.128.111.202    [Singapore  
47.128.111.215    [Singapore  
47.128.111.236    [Singapore  
47.128.112.43    [Singapore  
47.128.112.69    [Singapore  
47.128.112.111    [Singapore  
47.128.112.197    [Singapore  
47.128.112.226    [Singapore  
47.128.112.229    [Singapore  
47.128.113.12    [Singapore  
47.128.113.121    [Singapore  
47.128.113.126    [Singapore  
47.128.113.138    [Singapore  
47.128.113.182    [Singapore  
47.128.113.197    [Singapore  
47.128.114.87    [Singapore  
47.128.114.169    [Singapore  
47.128.114.174    [Singapore  
47.128.115.55    [Singapore  
47.128.115.172    [Singapore  
47.128.115.179    [Singapore  
47.128.115.200    [Singapore  
47.128.115.236    [Singapore  
47.128.116.8    [Singapore  
47.128.116.86    [Singapore  
47.128.116.139    [Singapore  
47.128.116.147    [Singapore  
47.128.117.19    [Singapore  
47.128.117.57    [Singapore  
47.128.117.209    [Singapore  
47.128.117.212    [Singapore  
47.128.117.230    [Singapore  
47.128.117.249    [Singapore  
47.128.118.13    [Singapore  
47.128.118.170    [Singapore  
47.128.119.76    [Singapore  
47.128.119.82    [Singapore  
47.128.119.93    [Singapore  
47.128.119.132    [Singapore  
47.128.119.189    [Singapore  
47.128.119.237    [Singapore  
47.128.120.42    [Singapore  
47.128.120.81    [Singapore  
47.128.120.109    [Singapore  
47.128.120.144    [Singapore  
47.128.120.183    [Singapore  
47.128.120.198    [Singapore  
47.128.120.201    [Singapore  
47.128.120.220    [Singapore  
47.128.121.8    [Singapore  
47.128.121.150    [Singapore  
47.128.121.151    [Singapore  
47.128.121.152    [Singapore  
47.128.121.231    [Singapore  
47.128.121.252    [Singapore  
47.128.122.17    [Singapore  
47.128.122.25    [Singapore  
47.128.122.63    [Singapore  
47.128.122.93    [Singapore  
47.128.122.203    [Singapore  
47.128.122.214    [Singapore  
47.128.122.223    [Singapore  
47.128.122.244    [Singapore  
47.128.122.245    [Singapore  
47.128.123.52    [Singapore  
47.128.123.77    [Singapore  
47.128.123.128    [Singapore  
47.128.123.155    [Singapore  
47.128.123.184    [Singapore  
47.128.123.197    [Singapore  
47.128.123.198    [Singapore  
47.128.123.216    [Singapore  
47.128.123.244    [Singapore  
47.128.124.47    [Singapore  
47.128.124.114    [Singapore  
47.128.124.174    [Singapore  
47.128.125.26    [Singapore  
47.128.125.41    [Singapore  
47.128.125.64    [Singapore  
47.128.125.255    [Singapore  
47.128.126.41    [Singapore  
47.128.126.70    [Singapore  
47.128.126.75    [Singapore  
47.128.126.184    [Singapore  
47.128.126.204    [Singapore  
47.128.127.16    [Singapore  
47.128.127.101    [Singapore  
47.128.127.161    [Singapore  
47.128.127.182    [Singapore  
47.128.127.197    [Singapore  
47.128.127.199    [Singapore  
101.108.181.209    [Thailand  
27.75.150.4    [Vietnam  
27.77.226.139    [Vietnam  
115.72.89.98    [Vietnam  
198.13.57.137    [Japan  
111.90.150.254    [Malaysia  
65.108.125.120    [Finland  
81.169.145.166    [Germany  
103.197.48.54    [Bangladesh  
65.108.110.26    [Finland  
92.193.128.121    [Germany  
103.133.222.170    [Indonesia  
125.165.105.186    [Indonesia  
35.213.138.88    [Singapore  
47.128.19.75    [Singapore  
192.248.57.142    [Sri Lanka  
27.65.112.184    [Vietnam  
27.75.145.117    [Vietnam  
27.76.199.204    [Vietnam  
27.77.229.229    [Vietnam  
103.106.105.141    [Vietnam  
116.111.99.221    [Vietnam  
171.233.180.135    [Vietnam  
171.248.217.160    [Vietnam  
114.119.132.114    [Singapore  
36.99.136.129    [China  
5.61.56.88    [Netherlands  
172.68.124.145    [Armenia  
172.68.124.149    [Armenia  
34.79.127.104    [Belgium  
45.128.96.175    [Bulgaria  
77.75.79.54    [Czechia  
81.0.246.95    [Germany  
94.130.219.241    [Germany  
103.167.217.137    [Indonesia  
202.47.77.130    [Indonesia  
115.187.18.66    [Nepal  
95.163.255.6    [Russia  
114.119.138.214    [Singapore  
114.119.144.202    [Singapore  
159.65.5.167    [Singapore  
171.233.180.82    [Vietnam  
182.16.53.82    [China  
35.195.133.193    [Belgium  
223.93.159.12    [China  
175.106.11.59    [Indonesia  
178.218.144.64    [Italy  
220.151.9.22    [Japan  
93.174.93.215    [Netherlands  
47.128.50.123    [Singapore  
47.128.119.4    [Singapore  
47.128.122.83    [Singapore  
51.79.163.195    [Singapore  
89.187.163.213    [Singapore  
118.139.180.32    [Singapore  
172.71.82.79    [Singapore  
168.76.20.229    [South Africa  
79.116.183.64    [Spain  
27.73.22.202    [Vietnam  
27.75.145.247    [Vietnam  
88.201.251.215    [Russia  
101.44.249.146    [China  
101.44.250.68    [China  
81.4.122.193    [Netherlands  
65.108.0.71    [Finland  
103.101.193.50    [Indonesia  
45.82.178.26    [Netherlands  
89.248.174.9    [Netherlands  
93.100.106.136    [Russia  
114.119.156.95    [Singapore  
206.189.144.61    [Singapore  
130.255.166.121    [Sweden  
182.52.197.27    [Thailand  
93.187.205.58    [Turkey  
27.75.144.248    [Vietnam  
116.96.164.56    [Vietnam  
116.106.110.192    [Vietnam  
116.107.190.144    [Vietnam  
171.247.98.136    [Vietnam  
54.36.145.173    [Spain  
103.108.130.209    [Indonesia  
103.235.74.153    [Indonesia  
213.186.33.17    [France  
217.160.0.93    [Germany  
202.51.96.18    [Indonesia  
5.181.157.12    [Moldova  
5.255.231.136    [Russia  
147.45.50.19    [Russia  
213.180.203.197    [Russia  
47.128.42.139    [Singapore  
114.119.137.101    [Singapore  
114.119.147.87    [Singapore  
217.160.0.220    [Germany  
65.108.46.72    [Finland  
65.108.78.33    [Finland  
162.158.95.55    [Germany  
103.27.72.14    [Malaysia  
128.199.160.240    [Singapore  
159.89.194.187    [Singapore  
157.230.253.117    [Turkey  
92.204.68.47    [Germany  
178.25.242.225    [Germany  
103.133.215.180    [India  
95.163.255.9    [Russia  
47.128.30.42    [Singapore  
114.119.148.1    [Singapore  
92.204.239.29    [Germany  
91.121.173.82    [France  
139.59.93.126    [India  
85.209.11.117    [Russia  
89.109.47.18    [Russia  
94.237.65.192    [Singapore  
96.9.211.191    [Singapore  
114.119.128.237    [Singapore  
114.119.132.57    [Singapore  
114.119.154.229    [Singapore  
162.158.162.138    [Singapore  
163.44.198.63    [Singapore  
172.70.147.177    [Singapore  
172.70.188.98    [Singapore  
156.146.57.135    [Unknown  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-1760420249 Raccoon Malware Alert**

Malware Alert Brief:

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.

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

37.49.230.152 [Netherlands

185.244.48.191 [Netherlands

193.142.147.59 [Seychelles

94.142.138.108 [Netherlands

94.131.106.24 [Netherlands

195.20.16.155 [Russia

178.20.41.15 [Russia

195.20.16.127 [Russia

5.42.64.7 [Russia

62.113.112.27 [Russia

146.19.173.87 [Seychelles

185.225.73.151 [Bulgaria

193.106.191.199 [Russia

89.44.9.86 [France

65.109.175.35 [Finland

89.208.103.4 [Germany

188.119.112.93 [Netherlands

91.103.252.156 [Netherlands

94.103.84.253 [Russia

94.103.88.64 [Russia

146.70.86.235 [Netherlands

94.142.138.162 [Netherlands

188.215.229.203 [Netherlands

45.9.74.36 [Germany

45.9.74.34 [Germany

95.164.17.125 [Netherlands

94.131.97.129 [Iran

77.232.39.101 [Russia

94.142.138.208 [Russia

45.67.35.164 [Netherlands

94.142.138.24 [Netherlands

94.142.138.124 [Netherlands

94.142.138.191 [Russia

94.142.138.213 [Russia

176.113.115.213 [Russia

62.113.119.179 [Russia

37.49.230.219 [Netherlands

45.84.0.80 [Moldova

45.8.144.152 [Netherlands

88.210.9.212 [Netherlands

94.142.138.228 [Russia

94.142.138.19 [Netherlands

91.103.252.65 [Netherlands

78.153.130.123 [Austria

80.92.204.202 [Germany

91.227.40.93 [Cyprus

185.17.40.132 [Poland

79.137.206.76 [Finland

94.131.98.22 [Sweden

91.92.255.182 [Netherlands

91.242.229.16 [Netherlands

45.140.146.169 [Moldova

45.159.251.32 [Portugal

77.91.73.154 [Germany

84.32.188.111 [Netherlands

91.215.85.226 [Russia

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP/Domain addresses.

The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **[CMTX-P-7940420249 Ursnif Malware Alert**

Malware Alert Brief:  
  
  
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.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
87.106.18.141      
83.218.160.14    [Austria  
3.115.86.44    [Japan  
52.221.92.67    [Singapore  
3.1.63.204    [Singapore  
18.178.237.95    [Japan  
104.87.220.57    [Germany  
185.49.68.137    [Germany  
185.49.68.140    [Germany  
91.195.240.85    [Germany  
91.228.166.47    [Slovakia  
91.195.240.19    [Germany  
34.143.166.163    [Singapore  
38.239.98.13    [China  
34.128.82.12    [Indonesia  
133.125.38.187    [Japan  
34.126.189.157    [Singapore  
31.31.205.163    [Russia  
51.79.137.110    [Singapore  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **[CMTX-P-1520420249] Trickbot Malware Alert**

Malware Alert Brief:  
  
  
Trickbot is a highly modular malware, capable of performing a number of actions on a network such as steal information or drop ransomware.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
175.184.232.234    [Indonesia]  
27.109.116.144    [Cambodia]  
41.77.134.250    [Mozambique]  
103.75.32.173    [India]  
185.68.93.17    [Bulgaria]  
177.190.76.82    [Brazil]  
45.221.8.171    [Uganda]  
114.7.243.26    [Indonesia]  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-6280420249 Redline Malware**

Malware Alert Brief:

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

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

185.172.128.33 [Russia

45.15.156.167 [Netherlands

45.15.156.142 [Netherlands

185.215.113.67 [Seychelles

5.42.65.0 [Russia

194.87.107.145 [Russia

4.185.137.132 [Germany

185.125.50.49 [Russia

65.108.20.226 [Germany

135.181.49.54 [Germany

147.45.45.81 [Netherlands

89.23.100.222 [Russia

195.20.16.134 [Russia

77.221.156.45 [Russia

2.58.56.216 [Germany

46.29.234.85 [Lithuania

5.189.138.247 [Germany

91.92.243.162 [Bulgaria

91.92.249.24 [Bulgaria

45.76.46.64 [France

91.92.250.88 [Netherlands

89.23.96.163 [Russia

94.131.118.143 [France

147.45.47.65 [Russia

89.23.97.100 [Russia

185.133.40.202 [Russia

62.122.184.51 [Russia

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP/Domain addresses.

The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations..

1. **CMTX-P042024646 Cerber Ransomware**

ALERT BRIEF:  
  
According to the reports, threat actors are exploiting unpatched Atlassian servers to disseminate a Linux variant of the Cerber (also known as C3RB3R) ransomware. The attacks leverage CVE-2023-22518, a critical security vulnerability impacting the Atlassian Confluence Data Center and Server that allows an unauthenticated attacker to reset Confluence and create an administrator account. Cerber ransomware is coded in C++, employs a primary payload as a loader for additional C++-based malware, obtained from a command-and-control (C2) server, before erasing its own traces from the infected host. Furthermore, they're exploiting the newly created admin account to install the Effluence web shell plugin, thereby allowing threat actors to execute arbitrary commands on victims' system.  
  
=========IOC START===================================  
  
IP ADDRESS  
45.145.6.112  
  
HASHES  
  
4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe  
1849bc76e4f9f09fc6c88d5de1a7cb304f9bc9d338f5a823b7431694457345bd  
ce51278578b1a24c0fc5f8a739265e88f6f8b32632cf31bf7c142571eb22e243  
  
=============IOC END===============================  
  
Recommendations:  
• Due to its critical nature and potential impact, apply vendor specified patch ASAP.  All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software.  
• Ransomware infections primarily keep data as hostage. Therefore, maintain offline backups of critical data and ensure that these backups stay up to date to prevent data loss in event of ransomware infection.  
• Periodic Backups and restoration tests to check the restoration integrity.  
• For detailed recommendations please refer to "Best Practices and Remedial measures" on https://www.cyberswachhtakendra.gov.in/alerts/ransomware.html  
- - --------------------ALERTEND----------------------------------------------

1. **CMTX-I-395042024 Malicious Domains - Spear-Phishing Campaign**

Following malicious domain and its subdomains are being used for spear-phishing purpose to target government officials:  
  
- ---------------<Malicious Domains>-----------------  
dropmediabox.cloud-india.live  
hal-india-co-in.cloud-india.live  
rti-application.cloud-india.live  
ssifs.cloud-india.live  
dark.cloud-india.live  
mega.cloud-india.live  
onedrive.cloud-india.live  
netflix.cloud-india.live  
mp6-ihq.cloud-india.live  
aps.cloud-india.live  
i.cloud-india.live  
www.cloud-india.live  
\*.cloud-india.live  
- --------------</Malicious Domains>-----------------  
  
Kindly take the required actions.