**Cyber Security Advisories**

**Date: 31-05-2024**

1. **CMTX-I-506052024 CrimsonRAT - APT36 campaign**

Recent C&C server domains of malwares used by Pakistan based threat actors to target government officials are as follows:  
  
- ------------- <C&C Domains> ------------  
waqers.duckdns.org  
\*.duckdns.org  
  
- ------------ </C&C Domains>-------------  
  
If DDNS domain like duckdns.org, is not being accessed by your organization then the parent domain can be blocked.

1. **CMTX-P052024085 Possible Exploitation of Public Facing Industrial Control Systems (ICSs)**

ALERT BRIEF:

It has been reported that various flaws in the public facing Industrial Control Systems (ICS) can leave the devices at risk of exploitation.

It is recommended that the ICS devices, which do not have a requirement of internet connectivity or online exposure should be disconnected from the internet.

Such ICS devices should be hardened to disallow remote connections from systems outside the local network to avoid  unauthorized and malicious cyber activity.

Following list contains the list of vulnerabilities that are being targeted by the attacker against the internet exposed ICS devices:

CVE-2021-22681 (CVSS-9.8)- The vulnerability allows an attacker to extract a secret encryption key used for verifying communication between Logix controllers and Rockwell Automation CompactLogix, ControlLogix, DriveLogix, Compact GuardLogix, GuardLogix, and SoftLogix devices.

CVE-2022-1159 (CVSS-6.1)- An attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code that remains undetectable to a user.

The vulnerability arises during the compilation process of the user program in Studio 5000 Logix Designer, which prepares the application for download to a Logix controller.

CVE-2023-3595 (CVSS-9.8)- It is a critical vulnerability that is actively being exploited by threat actors targeting industrial control systems, specifically Rockwell Automation controllers. The vulnerability is linked to various malware families such as TRISIS and WebShell.

CVE-2023-46290 (CVSS- 8.1)- An Improper Authentication vulnerability exists in the FactoryTalk Services Platform where an attacker could exploit this vulnerability to gain elevated privileges within the Platform.

CVE-2024-21914 (CVS-5.3)- This vulnerability affects the Rockwell Automation PanelView Plus 7 terminal. It allows a malicious user to restart the PanelView Plus 7 terminal remotely without security protections. If exploited, it could lead to the loss of view or control of the PanelView product.

CVE-2024-21915 (CVSS-9)- This vulnerability affects the Rockwell Automation Factory Talk Service Platform (FTSP). A privilege escalation vulnerability exists in FTSP. If exploited, a malicious user with basic user group privileges could potentially sign into the software and receive FTSP Administrator Group privileges.

CVE-2024-21917 (CVSS-9.1)- The vulnerability allows a malicious user to obtain the service token and use it for authentication on another FTSP (FactoryTalk Services Platform) directory. This security flaw arises due to the lack of digital signing between the FTSP service token and the directory

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

Recommendations:

\* If organizations have devices facing the public internet then it is recommended to remove connectivity for devices not specifically designed for public internet connectivity.

\* Prioritize patching these vulnerabilities promptly will help mitigate the risk of exploitation and enhance the company's overall cybersecurity posture.

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

1. **CMTX-I-509052024 Android RAT - Cumulative IOCs**

Recent C&C server IPs and Domain of  Android RAT/ Spynote malware are as follows:  
  
- ------------- <C&C IP/Domain> ------------  
v2.androidstaticserve.com  
147.124.197.187  
167.86.98.190  
45.88.188.224  
38.92.47.124  
64.188.24.72  
- ------------- </C&C IP/Domain>------------  
  
Kindly take the required actions.

1. **CMTX-P052024975 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:

5.252.178.31:8081, 8443:RO

103.96.131.215:80, 443:HK

45.61.60.86:80:US

167.179.112.116:443:JP

103.96.131.215:443:HK

5.252.178.31:8443:RO

103.96.131.215:80:HK

5.252.178.31:8081:RO

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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-P052024305 PLUGX RAT ALERT 119**

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

23.248.176.43:443:TW

103.107.105.56:443:HK

152.32.138.149:443:KR

45.80.211.109:80, 443, 53:US

154.84.24.174:8080, 8000:JP

103.43.18.92:80, 443:HK

103.79.120.92:443:HK

45.32.45.105:80, 443:JP

216.238.118.106:8080:BR

27.102.134.110:80, 443:KR

31.13.213.149:443, 53:US

103.107.105.110:5000, 443, 10086:HK

141.193.159.122:80, 8080, 53:HK

134.122.129.211:443:HK

103.79.120.69:443:HK

103.71.252.178:443, 53:HK

45.80.211.109:80:US

45.32.45.105:443:JP

45.80.211.109:53:US

129.211.168.154:53:CN

154.84.24.174:8080:JP

27.102.134.110:80:KR

31.13.213.149:53:US

27.102.134.110:443:KR

103.107.105.110:5000:HK

103.71.252.178:443:HK

103.71.252.178:53:HK

141.193.159.122:80:HK

103.43.18.92:80:HK

129.211.168.154:443:CN

129.211.168.154:80:CN

45.80.211.109:443:US

20.243.19.18:80:JP

129.211.168.154:8080:CN

20.243.19.18:443:JP

141.193.159.122:53:HK

154.84.24.174:8000:JP

31.13.213.149:443:US

103.43.18.92:443:HK

129.211.168.154:3306:CN

103.71.252.178:80:HK

103.107.105.110:443:HK

129.211.168.154:21:CN

141.193.159.122:8080:HK

45.32.45.105:80:JP

103.71.252.178:8080:HK

141.193.159.122:443:HK

31.13.213.149:53:US

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

1. **CMTX-P052024716 QuasarRAT Malware ALERT 53**

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           Country Code  Last Seen      
  
187.59.70.190:4782,    BR         27-05-2024  
27.124.44.81:4782,    HK         27-05-2024  
14.225.219.33:9999,    VN         27-05-2024  
101.201.150.204:8888,    CN         27-05-2024  
106.53.55.25:4782,    CN         27-05-2024  
91.92.250.222:3128,    NL         27-05-2024  
152.37.246.73:4782,    US         27-05-2024  
27.124.44.89:4782,    HK         27-05-2024  
193.34.77.188:6969,    DE         21-05-2024  
79.110.49.252:4782, 8808, 6606, 7707,    FR    27-05-2024  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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-I-515052024IOCs of Android and NanoCore RAT**

Recent C&C server Domain of  Android and NanoCore RAT malware are as follows:  
  
- -------------- <C&C Domain> ------------  
Android  RAT  
manta.brasilia.me    
ptzbubble.shop  
mzlxsilver.ddns.net  
abotsilver.ddns.net  
videoediting-da19b-default-rtdb.firebaseio.com   Note: It is advised to block the complete URL (and NOT the TLDs as they belong to Google Workspace) at the network perimeter level.  
- --------------------------------------------------  
NanoCore RAT  
orangeclub.club  
- -------------- </C&C Domain>------------.

1. **CMTX-P052024095 APT41 Chinese Threat Actor Activity**

ALERT BRIEF:

APT 41 Aliases:

RedGolf, BRONZE ATLAS, Barium, Blackfly, Brass Typhoon, Earth Baku, Red Kelpie, Wicked Panda, Winnti Group, CharcoalTyphoon,Choiceguard,Cycldek,Dalbit,EarthLusca,Earthbaku,GREF,Gallium,GraniteTyphoon,M00nlight,Moray,Othorene,Red Dev 10,RedAlpha,,Reddev4,Redkelpi,Sparklinggoblin,Tianwu,Tick,Wicked Panda,Wicked Spider.

Motivation: Cyber Espionage and Financial Motivation

Malware Used: - WyrmSpy, DragonEgg and UNAPIMON

A China based APT group, APT41 is active in the cyber threat landscape particularly targeting  government agencies, telecommunication providers, technology companies, and educational institutions. The group uses various tools and deploy malwares such as WyrmSpy, DragonEgg, Cobalt Strike, PlugX, ShadowPad, and Unapimon on vulnerable machines. The initial attack vectors to exploit vulnerabilities include supply-chain attacks, DLL hijacking and API hooking techniques.

WyrmSpy primarily masquerades as a default Android system app used for displaying notifications to the user. It collects a wide range of data from infected devices, includingLog file,photos,device location,SMS messages and audio recordings.

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

T1203 (Exploitation for Client Execution)

T1056.001 (Keylogging)

T1574 (Hijack Execution Flow)

T1021 (Remote Services)

T1588 (Obtain Capabilities)

T1071 (Application Layer Protocol)

T1566 (Phishing)

T1195 (Supply Chain Compromise)

T1190 (Exploit Public-Facing Application)

T1090 (Proxy)

T1574.001 (DLL Search Order Hijacking)

T1005 (Data from Local System)

T1136 (Create Account)

T1059 (Command and Scripting Interpreter)

T1070 (Indicator Removal)

T1135 (Network Share Discovery)

T1070.003 (Clear Command History)

T1036.004 (Masquerade Task or Service)

T1003 (OS Credential Dumping)

T1102 (Web Service)

T1055 (Process Injection)

T1014 (Rootkit)

T1071.002 (File Transfer Protocols)

T1547 (Boot or Logon Autostart Execution)

T1568 (Dynamic Resolution)

T1021.001 (Remote Desktop Protocol)

T1566.001 (Spearphishing Attachment)

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

IPs

47.241.218.217

121.40.54.49

121.43.176.66

120.78.223.152

47.242.56.232

47.75.49.89

161.117.253.231

47.242.108.245

59.188.221.36

47.56.159.124

116.62.152.217

116.62.219.141

47.52.164.5

121.40.58.4

116.196.85.213

8.219.55.216

173.248.242.38

121.199.44.128

DOMAINS

cresimplify.com

bauism.com

elinestable.com

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

RECOMMENDATIONS:

• Forbid the use of unused or unauthorized remote access tools. Implement technical controls to restrict access to these tools. Additionally, set up monitoring mechanisms to track the usage of approved tools and detect any unauthorized usage or suspicious activities.

• Regularly review and update the firewall deny list to include new resources and IP addresses associated with tunnelling services as they are identified. Implement monitoring and alerting mechanisms on the firewall to detect and alert administrators about any attempts to access the organization's network from deny listed cloud services.

• 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.

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

.

1. **CMTX-I-410052024 CrimsonRAT - APT36 campaign**

Recent C&C server domains of malwares used by Pakistan based threat actors to target government officials are as follows:  
  
- ---------------------------------------- <C&C Domains> --------------------------------------------  
qheelsec.duckdns.org IP resolutions: 66.63.163.148  
waqers.duckdns.org IP resolutions: 94.72.105.227, 104.223.106.8  
- ---------------------------------------- </C&C Domains>--------------------------------------------  
  
If DDNS domain like duckdns.org, is not being accessed by your organization then the parent domain can be blocked.

1. **CMTX-P052024168 Trickbot malware**

Malware Alert Brief:

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

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

103.9.188.78:Cambodia

96.9.77.142:Cambodia

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

RECOMMENDATIONS:

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

1. **CMTX-P052024188 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP:

172.104.32.244:Singapore

Domains:

artemis-rat.com

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

RECOMMENDATIONS:

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

1. **CMTX-P052024158 SocGholish malware**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

124.223.193.173:China

217.182.194.108:France

47.128.16.182:Singapore

47.128.20.238:Singapore

47.128.22.14:Singapore

47.128.27.101:Singapore

47.128.29.145:Singapore

47.128.30.168:Singapore

47.128.30.187:Singapore

47.128.34.89:Singapore

47.128.42.233:Singapore

47.128.44.156:Singapore

47.128.46.18:Singapore

47.128.46.224:Singapore

47.128.48.202:Singapore

47.128.49.147:Singapore

47.128.51.251:Singapore

47.128.54.230:Singapore

47.128.55.248:Singapore

47.128.56.166:Singapore

47.128.60.70:Singapore

47.128.60.119:Singapore

47.128.60.249:Singapore

47.128.61.184:Singapore

47.128.63.36:Singapore

47.128.63.73:Singapore

47.128.96.157:Singapore

47.128.116.36:Singapore

47.128.119.31:Singapore

47.128.122.47:Singapore

47.128.122.75:Singapore

47.128.125.144:Singapore

47.128.126.129:Singapore

159.89.203.182:Singapore

171.227.37.12:Vietnam

147.78.47.230:Panama

128.199.208.123:Unknown

115.74.153.72:Vietnam

47.242.4.67:China

103.108.130.210:Indonesia

188.166.96.229:Russia

167.172.65.123:Turkey

92.205.49.95:Germany

118.27.99.23:Japan

103.153.2.74:Indonesia

188.166.176.89:Singapore

152.32.128.214:China

150.109.173.178:Thailand

38.45.127.226:China

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

RECOMMENDATIONS:

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

1. **CMTX-P052024198 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

45.113.122.63:India

192.250.235.41:Singapore

45.113.122.219:India

156.238.243.27:China

8.210.9.129:China

5.42.96.7:Russia

46.105.133.232:Poland

45.113.122.172:India

119.18.58.248:India

109.232.238.98:France

45.113.122.178:India

103.21.58.141:India

103.53.43.143:India

34.90.184.114:Netherlands

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

RECOMMENDATIONS:

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

1. **CMTX-P052024208 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.42.65.85:Russia

94.232.249.14:Netherlands

65.108.19.239:Germany

65.21.14.164:Finland

194.28.226.213:Germany

91.92.249.167:Netherlands

185.65.105.50:Netherlands

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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-P052024178 Ursnif malware**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

18.143.155.63:Singapore

18.141.10.107:Singapore

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

RECOMMENDATIONS:

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

1. **CMTX-P052024148 Emotet Malware**

Malware Alert Brief:

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

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

119.59.116.21:Thailand

168.197.45.36:Argentina

42.200.107.142:China

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

RECOMMENDATIONS:

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

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

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

1. **CMTX-P-052024105 ShrinkLocker Ransomware**

Alert Brief:

ShrinkLocker is a new ransomware variant, written in Visual Basic Script (VBScript). It uses BitLocker (a legitimate encryption technology) to target vulnerable systems. Once intrusion into the victim machine is successfully done, the variant first checks if the target machine's operating system is running Windows versions later than Vista before initiating encryption with BitLocker. With the use of Bitlocker, the script changes the operating system’s boot parameters and encrypts the hard disk partitions. It has the capability to infect both older and newer versions of the Windows operating system upto Windows Server 2008.

MITRE ATT&CK Enterprise Identifiers:

T1047 (Windows Management Instrumentation)

T1562.004 (Disable or Modify System Firewall)

T1059.001 (PowerShell)

T1059.005 (Visual Basic)

T1070.001 (Clear Windows Event Logs)

T1486 (Data Encrypted for Impact)

T1112 (Modify Registry)

T1529 (System Shutdown/Reboot)

T1041 (Exfiltration Over C2 Channel)

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

HASH:

842f7b1c425c5cf41aed9df63888e768

EMAILS:

onboardingbinderatproton.me

conspiracyid9atprotonmail.com

URL:

https://scottish-agreement-laundry-further.trycloudflare.com/updatelog

https://generated-eating-meals-top.trycloudflare.com/updatelog

https://generated-eating-meals-top.trycloudflare.com/updatelogead

https://earthquake-js-westminster-searched.trycloudflare.com:443/updatelog

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

RECOMMENDATIONS:

\* Recommended to monitor connection towards the mentioned URLs. The list may include compromised URL resources as well. Blocking the URL is solely the recipient responsibility after diligently verifying them without impacting the operations.

\* Regularly update the operating system, applications, and security software. Patches often address known vulnerabilities that attackers exploit.

\* Enable MFA for critical services such as VPNs, remote desktop access, and email accounts. This adds an extra layer of security.

\* Isolate critical systems from less critical ones. Limit lateral movement for attackers within your network.

\* Educate employees about phishing techniques and safe online practices. Regular training can prevent social engineering attacks.

\* Regularly back up  data to secure, offline locations. Test backups to ensure they are functional. Consider using immutable backups to prevent ransomware from affecting backups.

\* Limit user permissions to only what is necessary for their roles. Avoid unnecessary administrative privileges.

\* Deploy endpoint security solutions that detect and block malicious activity. Use behavior-based detection to identify suspicious behavior.