Unmasking the Silent Spy: A Comprehensive Analysis of ComRAT v4 Malware and its Detectionthrough Python Script

Vignesh S
Dept. of Computer Science and Engineering Indian Institute of Information Technology Kottayam Kerala, India vigneshsureshcc3@gmail.com

Dr. Priya Sajan
Software Training and Development Centre Centre for Development of Advanced Computing Thiruvananthapuram, Kerala, India priyasajan@cdac.in

Abstract—*Rapid development of technologies such as automa- tion has drastically influenced human life which spiked cyber- threats. Malware is one such threat designed to cause damage to a system or network of systems.*

ComRAT v4 is the fourth iteration of the malware employed by the Russian threat actor Turla. Typically, ComRAT v4 is deployed on a system using a PowerShell script that exploits an existing backdoor and, once installed, decrypts the required payload using a scheduled Windows task. The malware avoids detection by utilizing the Gmail Web User Interface as its communication- and-command channel.

This research paper searches for the artifacts created by the ComRAT v4 malware, by preventing its communication withdomains and mitigates or minimizes the damages caused by the same.

Index Terms*—ComRAT v4, Malware, Cyber Threats*

Date of Submission: 24-07-2023 Date of acceptance: 06-08-2023

I. INTRODUCTION

Cyber-attacks are on the rise nowadays as more information is stored in inter-connected systems in the aim of automa-tion or otherwise and gaining such information implies an advantage in real scenarios like war. According to researchby Checkpoint, global cyber-attack scenarios rose by 38%in 2022, as compared to 2021[1]. In the year 2021, around 15.45% of the internet users experienced a malware-related attacks [2].

Malware or malicious software is a piece of software that causes intentional harm like stealing, encrypting and/or delet- ing data, hijacking core functionalities and so on to a com- puter, server or network. Malwares are of many kind-likeviruses, trojans, ransomware etc. Threat actors use varioustechniques like phishing, Denial-Of-Service (DOS) attack and so on to compromise a system or network of systems introducing their malware, which upon breach act as a point of further infiltration or end-point from which the informationis extracted, deleted or manipulated. Malware harms the system in a unique way determined by its creation while using different mechanisms to persist in the system unnoticed or even declare its presence in some cases. Evident from the recent news, the usage of specially crafted messages in phishing attacks which introduces a malware into the system is the most common method used by threat actors across the globe. Recently, two malicious documents from a Hungarian IP targeting the NATO Summit which upon installation steals commandeers the system was discovered by Blackberry ThreatResearch and Intelligence Team [3]. Such cyber-espionagecampaigns are also on the rise.

Turla is a Russian Advanced Persistence Threat (APT) group that targets specific high-profile organizations rather than being opportunistic in nature to become one of the oldest active cyber-espionage groups. ComRAT is a malware introduced byTurla, famous for breaching major organizations such as the US Department of Defence in 2008, Swiss defence company, RUAG in 2014. The timeline of Turla is given in the Fig 1.

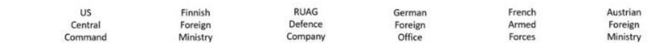


Fig. 1. Timeline of Turla ComRAT activities

ComRAT v4 is the fourth version of this malware that was introduced in 2017, generally installed in the system using a complex backdoor. ComRAT orchestrator, that is installed in "explorer.exe" via a PowerShell loader enters the system generally using a phishing attack, persists in the system by scheduling a windows task and loading the registry with an encrypted payload. All files of ComRAT are stored in a Virtual File System using FAT16 format. Turla operators use a Gmailweb user interface to pass Command-and-Control statements avoiding being flagged by antivirus software. Latest of these attacks using ComRAT v4 were reported in the early 2020.

II. COMRAT V4.0 INCIDENTS

1) **German Foreign Office Breach in 2017 [4]**: The hackers first compromised the network of the country's Federal College of Public Administration and leveraged it to breach the network of the Foreign Office in March 2017.

2) French Armed Forces breached in 2018

3) **Austrian Foreign Office in 2020 [5]:** ORF, state broad- caster Austrian Radio, reported that a command-line module was used by the attackers to send a four-byte TCP request to an external server. That downloads the malware dropper, which in turn places turla' s trojan. Deployed as a so-called fileless attack, the malware's operators were able to revisit freshly disinfected servers with subtly altered strains, reacting to countermeasures on the fly.

III. METHOD OF PROPAGATION

A. *Installation and Properties*

ComRAT v4 malware is installed into the system using an already existing loophole such as leaked credentials orvia phishing and already existing turla backdoor. Once the malware enters a system, the installer is a PowerShell script that loads an encrypted payload into the registry and once decrypted, payload loads an orchestrator dll into explorer.exe which is the default file explorer in Windows. This orchestra- tor injects an encrypted communication module into default web browser of the system which shall provide a stealthier communication through windows named pipes. Orchestrator possess a virtual File System (VFS) in File Allocation Table 16 (FAT-16) format which is encrypted with AES-256 in XTSmode. Figure 2 shows the method of persistence and operationof the ComRAT v4 malware

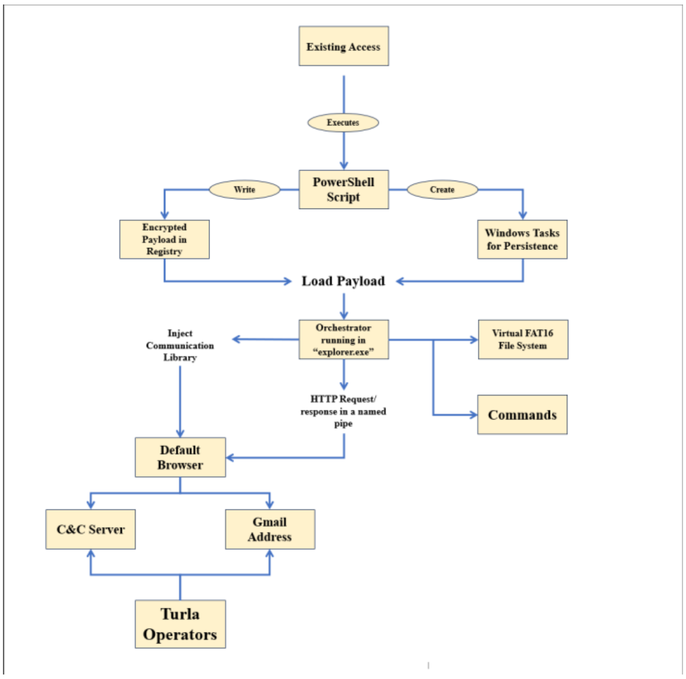

Existing Access
Executes
PowerShell Script
Write
Create
Encrypted Payload in Registry
Windows Tasks for Persistence
Load Payload
Inject Communication Library
Orchestrator running in "explorer.exe"
Virtual FAT16 File System
HTTP Request/ response in a named pipe
Commands
Default Browser
C&C Server
Gmail Address
Turla Operators

Fig. 2. ComRAT v4: Persistence and operation

B. *Communication and Command*

ComRAT v4 malware uses two modes of communicationand command channels: HTTP and EMAIL:

1) **HTTP channel** also known as legacy as it was usedin the older versions of the ComRAT v4 malware and it is believed that this channel is used as to avail theuse of the same servers while also

providing a common interface for the controlling the victims of any version.

2) **Email channel** is a communication channel used bythe ComRAT orchestrator to communicate with their servers using Gmail which reads email addresses and authenticates cookies while connecting to the basic htmlview of Gmail. “Gumbo HTML Parser” is used to parse the HTML page and reads only the emails of its interest and downloading the attachments with commands whichare disguised as “.docx” files upon which the necessary commands are executed and information is exported with the help of the backdoor. The usage of Gmail enables to stay undetected by antivirus software.

IV. INDICATORS OF COMPROMISE

Indicators of compromise are the artifacts that are left by a malware in an infected system that is used by security experts to analyse the malware and detect any future intrusion at- tempts. The indicators of compromise of ComRAT v4 malwarewere identified by the researchers at the cyber security firm, ESET [6]. The IOCs are listed below.

A. Hashes

These hashes are the encrypted payloads that enter the sys- tem through phishing attacks or an already existing backdoor which installs and loads the ComRAT v4 malware.

1) 4D8B1F4ACC638080054FFBB4CEF2559583A22DC6
(PowerShell dropper)
2) DD7006D16D8E121FCE8F2905433474ECCED75CC0
(ComRAT orchestrator)
3) 0139818441431C72A1935E7F740A1CC458A63452
(ComRAT orchestrator)
4) 0AB87F7BDF7D9E54BA33FE715C11E275D5DCCE15
(ComRAT orchestrator)

The hash (1) is a PowerShell dropper that loads a encrypted orchestrator into the registry and a windows scheduled task that decrypts orchestrators (2,3,4). Looking for these hashes in a system can prevent the infection at its initial stage.

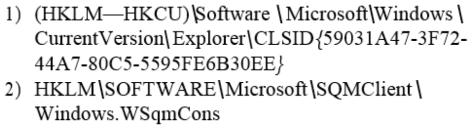
B. Paths

The paths and files that are created by the malware for its own purposes are indicators that a malware infection is existent on a system. These paths can be detected by identifying particular files in the given directory. Such paths are used by the ComRAT v4 malware for storing various information and they are identified to be:

1) %TEMP%\FXSAPIDebugTrace.txt
2) %TEMP%\iecache.bin

C. Registry

Registry value that indicates a malware is present in the system by identifying entries that are created by the malware. Registry entries made by ComRAT v4 malware are:



1) (HKLM—HKCU)\Software \Microsoft\Windows \
CurrentVersion\Explorer\CLSID{59031A47-3F72-44A7-80C5-5595FE6B30EE}
2) HKLM\SOFTWARE\Microsoft\SQMClient \
Windows.WSqmCons

D. Network

A malware extracts using various methods, one of the most common methods for such an extraction is to upload a filein a malicious domain created and hosted by the attackers. Detecting or prevention of access to these domains at the root level can prevent information loss. The ComRAT v4 malware used a vast list of domains to extract information, some of which are given below:

1) arinas.tk
2) bedrost.com
3) branter.tk
4) bronerg.tk
5) celestyna.tkand many more.

V. PROPOSED SOLUTION

Our proposed solution detects or prevents the usage of identified indicators of compromise along with the prevention of attack through some commonly used mechanism.

A. Identifying created temp file

Paths that are created by the ComRAT v4 malware can be identified by using a python script that iterates a list of path IOCs that are read from a file. The script runs continuously and an alert is generated upon the detection of infection in the system.

```
for fil in files:
if (os.path.isfile(fil)):flag=1
print("ComRAT v4 Malware Detected")else:
pass
```

Here “files” is the list of files that are created by the malware.

B. Identifying created Registries

A python script can use the inbuilt domain “winreg” to open keys. An existent key will open without error, however a non- existent key will raise an error.

C. Blocking identified domains at Host File

One of the most important factors of any malware infection upon its entry into the system is to extract information and pass it on to the threat actors for different purposes, which is usually done with the help of domains that are created and hosted by the threat actors itself. Preventing access to such malicious domains that are identified by redirecting these requests to
0.0.0.0 will defend against information exportation.

```
for domain in block_list:
if domain not in host_file :host_file.write('0.0.0.0
'+domain+'\n')
```

“block list” is the list of domains that are created in accor- dance with the network IOCs that are used by the ComRATv4 malware to export information. However, editing the hosts file in windows require administrator privileges.

D. Blocking Ad sites at the host

Adware is one of the most common ways in which malwaresintrude into a system. Ads act as lure to attract users into entering malicious contents that can provide an entry pointinto the system. This can prevented in a similar way as to blocking the blacklisted domains that were identified as the IOCs, browser based adware from an API can be retrieved using ”requests.get()” in the “requests” module can be blockedoff in the host file as previous with administrator privileges.

```
bad_domains = requests.get(url).text.splitlines()
```

Here, ”url” is the variable that stores the link to access theAPI

E. Blocking ports used by ComRAT v4 malware and othercommonly used ports

ComRAT v4 malware commonly uses the ports 80 and 443. Creation of a firewall that destroys the packages that access these ports along with some other common ports that areused for remote access such as port 3389, 23, 2323 provide enhanced protection against malwares, specifically, ComRAT v4 malware. Such a firewall can be created in python script using the “scapy” package to drop all package that accesses these ports mentioned in a list “blocked_ports”.

```
try:
```

```
path =
winreg.OpenKeyEx(loc,r"SOFTWARE\\ Microsoft\\SQMClient\\Windows.WSqmCons\\")
flag = 1
print("ComRAT v4 Malware Detected")except  FileNotFoundError:
pass

if src_port in blocked_ports or dst_portin blocked_ports:
print(f"Blocked packet:
{packet.summary()} using port
{src_port} or {dst_port}")return
```

Similarly, all the registry entries that are created can be lookedand the ComRAT v4 malware can be detected.

If either source port (src port) or destination port (dst port) is one of the blocked ports, then an alert is generated and the packet is dropped, else the packet is send to its destination,

F. Blocking HTTP requests

HTTP requests in these days are very dangerous as thereis no encryption is provided and the transfer occurs in plain text and hence there is no protection to the data being transferred. ComRAT v4 malware makes use of HTTP as a Communication and Command (C&C) channel along with its previous variants. Hence blocking all HTTP requests can be used in defending malware attack while not disrupting the regular functions of the system. A python script with “BaseHTTPRequestHandler” from the “http.server” package can be used to send response code “403” to HTTP requests.

```
def do_GET(self):
self.send_response(403) self.send_header('Content-type',
'text/html') self.end_headers()
```

VI. CONCLUSION AND FUTURE SCOPE

Malicious applications or Malwares pose a significant risk to the security of data in computer systems, data centres, and other similar environments. Cyber espionage groups such as Turla, which uses custom-built complex malwares such as the ComRAT v4 malware, the fourth version of the malware, to exploit sensitive networks and acquire information according to Russian geopolitical interests, are on the rise as cyber warfare intensifies. ComRAT v4 is a very complex malware with AES encryption and its own Virtual File System that uses Gmail Web User Interface to execute Communication and Control channel to avoid automatic detection by antivirus applications. However, the indicators of compromise (IOCs) ofComRAT v4 malware, i.e., the paths, registries, and network access, can be used to detect and defend against the aforemen-tioned malware. Since its inception in 2007 by Turla, however,ComRAT has targeted and attacked high-profile targets such as foreign ministries, defense networks, and highly sensitive government networks. After successfully breaching the United States Department of Defense in 2008, variants of this malware were detected in 2013, 2014, 2017, 2019, and most recently in 2020 targeting similar highly sensitive networks. A variant of this malware with enhanced capabilities may shortly reappear.

REFERENCES

[1] https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global- cyberattacks/
[2] https://aag-it.com/the-latest-ransomware- statistics/#::text=During%202021%2C%20at%20least%2015.45,of%20 cyber%20breaches%20in%202022
[3] https://thehackernews.com/2023/07/romcom-rat-targeting-nato-and- ukraine.html
[4] https://www.securityweek.com/turla-backdoor-controlled-email-attachments/
[5] https://www.theregister.com/2020/02/14/austria foreign ministryhack turla group allegs/
[6] https://github.com/eset/malware-ioc/blob/master/turla/misp-turla- comrat-v4-event.json