

# Analysis Report OF RAT.Bindshell.EXE

Friday, June 30, 2023 10:41 AM

## Static Analysis

• Hashes

md5,689FF2C6F94E31ABBA1DDEBF68BE810E  
sha1,69B8ECF6B7CDE185DAED76D66100B6A31FD1A668  
sha256,248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

VT Scan

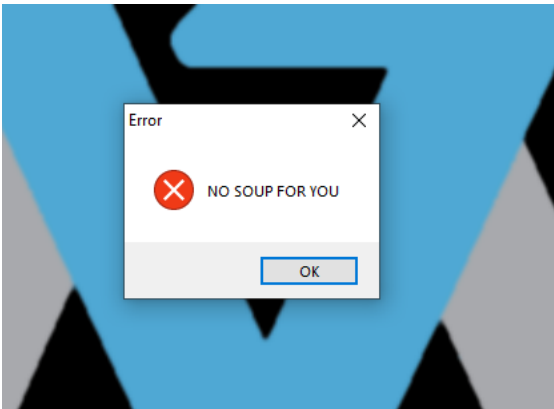
<https://www.virustotal.com/gui/file/248d491f89a10ec3289ec4ca448b19384464329c442bac395f680c4f3a345c8c>

## Floss/Strings output

```
@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
```

## Dynamic Analysis

With no internet connection :

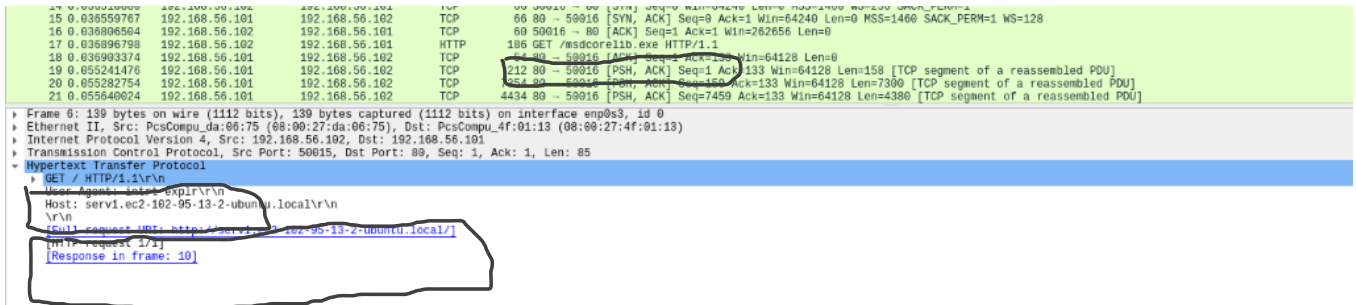


## Network Indicators

With Internet connection having fake http server using inetsim

### Wireshark reading

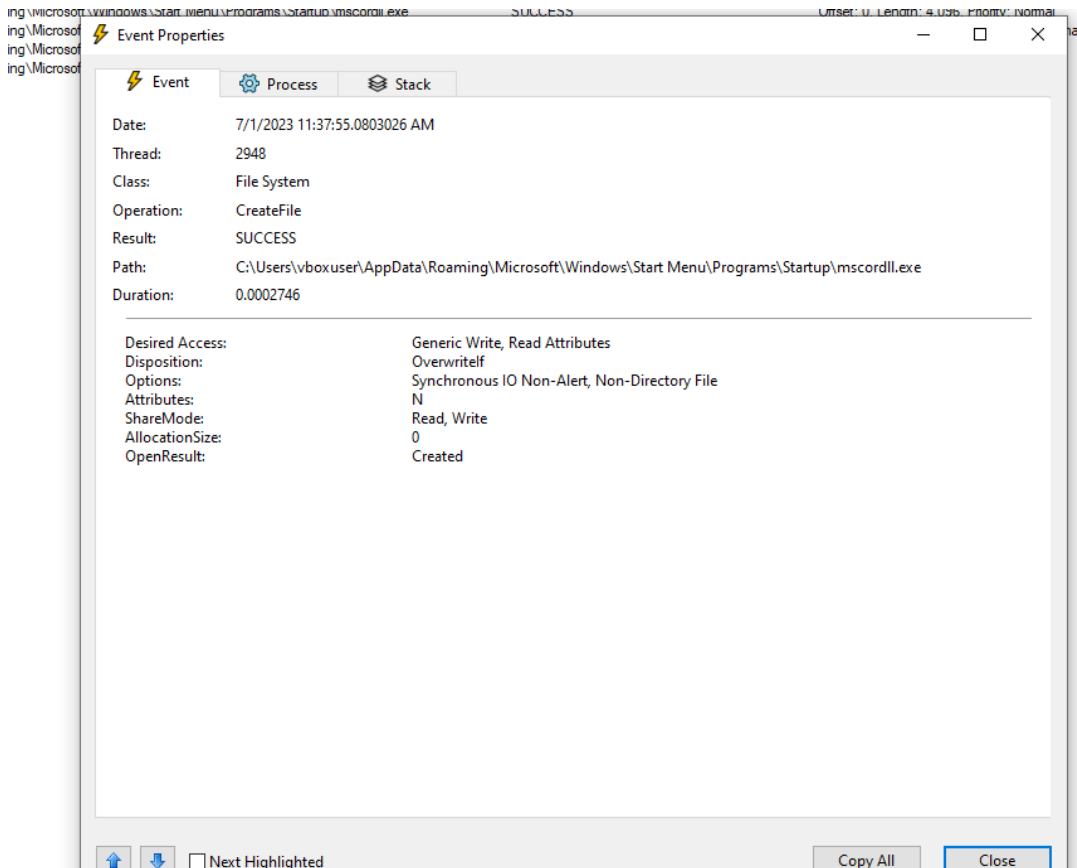
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.102	192.168.56.101	DNS	94	Standard query 0x7841 A serv1.ec2-102-95-13-2-ubuntu.local
2	0.000175999	192.168.56.101	192.168.56.102	DNS	110	Standard query response 0x7841 A serv1.ec2-102-95-13-2-ubuntu.local A 192.168.56.101
3	0.017272668	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [SYN] Seq=0 Win=0 MSS=1460 WS=256 SACK_PERM=1
4	0.017308473	192.168.56.101	192.168.56.102	TCP	60	80 → 50015 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
5	0.017525243	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6	0.017843741	192.168.56.102	192.168.56.101	HTTP	239	GET / HTTP/1.1
7	0.017854241	192.168.56.101	192.168.56.102	TCP	54	80 → 50015 [ACK] Seq=1 Ack=86 Win=64256 Len=0
8	0.030570600	192.168.56.101	192.168.56.102	TCP	204	80 → 50015 [PSH, ACK] Seq=1 Ack=86 Win=64256 Len=156 [TCP segment of a reassembled PDU]
9	0.030919389	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [ACK] Seq=86 Ack=151 Win=261888 Len=0
10	0.030935087	192.168.56.101	192.168.56.102	HTTP	312	HTTP/1.1 200 OK (text/html)
11	0.031091168	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [ACK] Seq=86 Ack=409 Win=261632 Len=0
12	0.032957398	192.168.56.101	192.168.56.102	TCP	54	80 → 50015 [FIN, ACK] Seq=409 Ack=86 Win=64256 Len=0
13	0.033185159	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [ACK] Seq=86 Ack=410 Win=261632 Len=0
14	0.036168888	192.168.56.102	192.168.56.101	TCP	60	50015 → 80 [ACK] Seq=86 Ack=410 Win=261632 Len=0



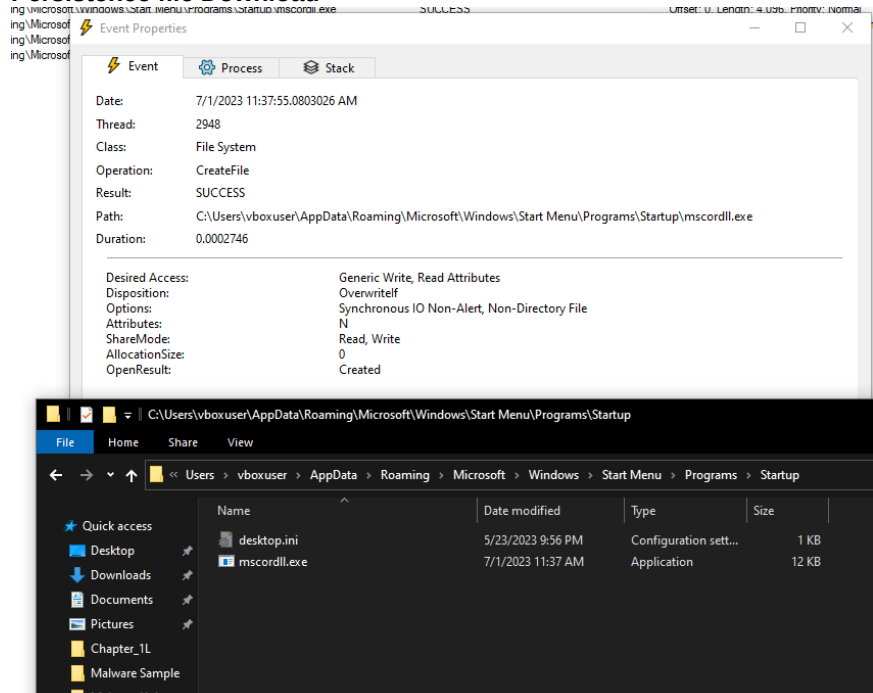
Potential file download msdcorelib.exe

## Host Based Indicator

### 1. Creation of file in Startup folder for persistence



## Persistence file Download



The remote address can be anything because its on 0.0.0.0

TCPView - Sysinternals www.sysinternals.com

File Edit View Process Connection Options Help

Process Name Process ID Protocol State Local Address Local Port Remote Address Remote Port Create Time Module Name Sent Packets

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	924	TCP	Listen	0.0.0.0	135	0.0.0.0	0	6/28/2023 1:46:24 AM	RpcSs	
System	4	TCP	Listen	192.168.56.102	139	0.0.0.0	0	7/1/2023 11:50:24 AM	System	
svchost.exe	1520	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	6/28/2023 1:46:30 AM	CDPSvc	
RAT.Unknown.exe	3132	TCP	Listen	0.0.0.0	5555	0.0.0.0	0	7/1/2023 11:54:14 AM	RAT.Unknown.exe	
lsass.exe	676	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	6/28/2023 1:46:24 AM	lsass.exe	
wininit.exe	524	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	6/28/2023 1:46:24 AM	wininit.exe	
svchost.exe	1292	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	6/28/2023 1:46:25 AM	EventLog	
svchost.exe	1132	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	6/28/2023 1:46:25 AM	Schedule	
spoolsv.exe	2336	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	6/28/2023 1:46:25 AM	Spooler	
services.exe	668	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	6/28/2023 1:46:26 AM	services.exe	
[Time Wait]		TCP	Time Wait	192.168.56.102	57000	192.168.56.101	443			
[Time Wait]		TCP	Time Wait	192.168.56.102	57001	192.168.56.101	443			
RAT.Unknown.exe	3132	TCP	Close Wait	192.168.56.102	57002	192.168.56.101	80	7/1/2023 11:54:14 AM	RAT.Unknown.exe	1
RAT.Unknown.exe	3132	TCP	Close Wait	192.168.56.102	57003	192.168.56.101	80	7/1/2023 11:54:14 AM	RAT.Unknown.exe	1
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	6/28/2023 1:46:26 AM	System	

Time	Process Name	PID	Operation	Path	Result	Detail
12:06:...	RAT.Unknown.exe	3132	TCP Receive	Flarevm:5555 -> www.inetism.org:40230	SUCCESS	Length: 3, seqnum: 0, connid: 0
12:06:...	RAT.Unknown.exe	3132	TCP Send	Flarevm:5555 -> www.inetism.org:40230	SUCCESS	Length: 149, starttime: 5289836, endtime: 5289836, seqnum: 0
12:08:...	RAT.Unknown.exe	3132	TCP Receive	Flarevm:5555 -> www.inetism.org:40230	SUCCESS	Length: 0, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	3132	TCP Disconnect	Flarevm:5555 -> www.inetism.org:40230	SUCCESS	Length: 0, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	3132	TCP Disconnect	Flarevm:57082 -> www.inetism.org:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	3132	TCP Disconnect	Flarevm:57083 -> www.inetism.org:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Connect	Flarevm:57106 -> www.inetism.org:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvbuf: 0
12:08:...	RAT.Unknown.exe	8620	TCP Send	Flarevm:57106 -> www.inetism.org:http	SUCCESS	Length: 85, starttime: 5302605, endtime: 5302605, seqnum: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57106 -> www.inetism.org:http	SUCCESS	Length: 150, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57106 -> www.inetism.org:http	SUCCESS	Length: 258, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Connect	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvbuf: 0
12:08:...	RAT.Unknown.exe	8620	TCP Send	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 132, starttime: 5302609, endtime: 5302609, seqnum: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 158, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 1460, seqnum: 0, connid: 0
12:08:...	RAT.Unknown.exe	8620	TCP Receive	Flarevm:57107 -> www.inetism.org:http	SUCCESS	Length: 96, seqnum: 0, connid: 0

### Base64 encoded information coming from tcp socket

[illegible]

**The RAT have Command injection utility**  
**Some commands are ipconfig**

[illegible]

```
jguNTYyMTAyC1AgIFNlYm5ldCBNYXNrIC4gLiA0IC4gLiA0IC4gLiA0IC4gLiA6ID1INS4
XRld2F5IC4gLiA0IC4gLiA0IC4gLiA0IDogCg==" | base64 -d

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . :
Link-local IPv6 Address . . . . . : fe80::be38:5ea3:50d1:dcf5%6
IPv4 Address. . . . . : 192.168.56.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Whoami

Procmon reading when command is sent from remote host

After analysis of all the process, Indicator and connection we can say this RAT has command injection utility us a potential persistence file

Summary:

The analysis reveals the presence of a Remote Access Trojan (RAT) with command injection capabilities. The RAT is associated w  
MD5: 689FF2C6F94E31ABBA1DDEBF68BE810E  
SHA1: 69B8ECF6B7CDE185DAED76D66100B6A31FD1A668  
SHA256: 248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C  
The provided VirusTotal scan link (<https://www.virustotal.com/gui/file/248d491f89a10ec3289ec4ca448b19384464329c442bac395f68>) of the file.

Static analysis indicates the presence of various API calls and strings related to network operations, such as InternetOpenW, Inter MessageBoxW, and more. Additionally, there are references to file paths and URIs.

Dynamic analysis with an internet connection shows an error message related to the absence of a "soup" and network indicators c reveals communication between local IP addresses and a remote IP address, including DNS queries and HTTP requests.

Further analysis suggests the potential download of a file named msdcorelib.exe from a fake HTTP server hosted on serv1.ec2-102

Host-based indicators indicate the creation of a file in the startup folder for persistence.

A TCP connection is established on port 5555, with the remote address being 0.0.0.0. Base64-encoded information is observed cor

The RAT exhibits command injection utility, allowing execution of commands such as ipconfig and whoami.

Process Monitor (Procmon) readings indicate the execution of commands sent from a remote host.

In summary, the analysis suggests the presence of a RAT with command injection capabilities. It establishes a TCP connection, dc (msdcorelib.exe), and can execute commands remotely. Further investigation and mitigation steps are recommended to address th