

RAT.Reverseshell.EXE

Sunday, July 02, 2023 11:40 AM

Static Analysis

Hashes

md5sum.exe c211704777e168a5151de79dc87ffac7
sha256sum.exe 481eae82ac4cd1a9cfadc026a628b18d7b4c54f50385d28c505fbc3e999b8b0
sha1sum.exe 1f688b4872f8a740872b5cb6d58e2b9c7103143a

Floss/Strings

@cmd.exe /c
@exit
@.local
@iterators.nim(189, 11) `len(a) == L` the length of the seq changed while iterating over it
@kadusus

Dynamic Analysis

Network based Indicators

Creating a dns request

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.102	192.168.56.101	DNS	94	Standard query 0xa32a A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
2	0.006753098	192.168.56.101	192.168.56.102	DNS	110	Standard query response 0xa32a A aaaaaaaaaaaaaaaaaaaaa.kadusus.local A 192.168.56.101
3	0.009949178	192.168.56.102	192.168.56.101	TCP	66	49677 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.009989554	192.168.56.101	192.168.56.102	TCP	66	443 -> 49677 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
5	0.010151118	192.168.56.102	192.168.56.101	TCP	60	49677 -> 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0

Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu-da:08:75 (08:00:27:da:06:75), Dst: PcsCompu_4f:01:13 (08:00:27:4f:01:13)

Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101

User Datagram Protocol, Src Port: 51810, Dst Port: 53

Source Port: 51810

Destination Port: 53

Length: 60

Checksum: 0xca9c [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

[Timestamps]

UDP payload (52 bytes)

Domain Name System (query)

Transaction ID: 0xa32a

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

aaaaaaaaaaaaaaaaaaaa.kadusus.local: type A, class IN

[Response In: 2]

Host Based Indicators

DNS request

Requesting for aaaaaaaaaaaaaaaaaaaaa.kadusus.local

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process

10:53:00 [RAT.L...]

10:53:00 [RAT.L...]

10:53:00 [RAT.L...]

10:53:00 [RAT.L...]

10:53:00 [RAT.L...]

Event Properties

Event Process Stack

Date: 7/6/2023 10:53:08.3078986 PM

Thread: 0

Class: Network

Operation: TCP Reconnect

Result: SUCCESS

Path: aaaaaaaaaaaaaaaaaaaaa.kadusus.local:57335 -> aaaaaaaaaaaaaaaaaaaaa.kadusus.local:https

Duration: 0.0000000

Length: 0

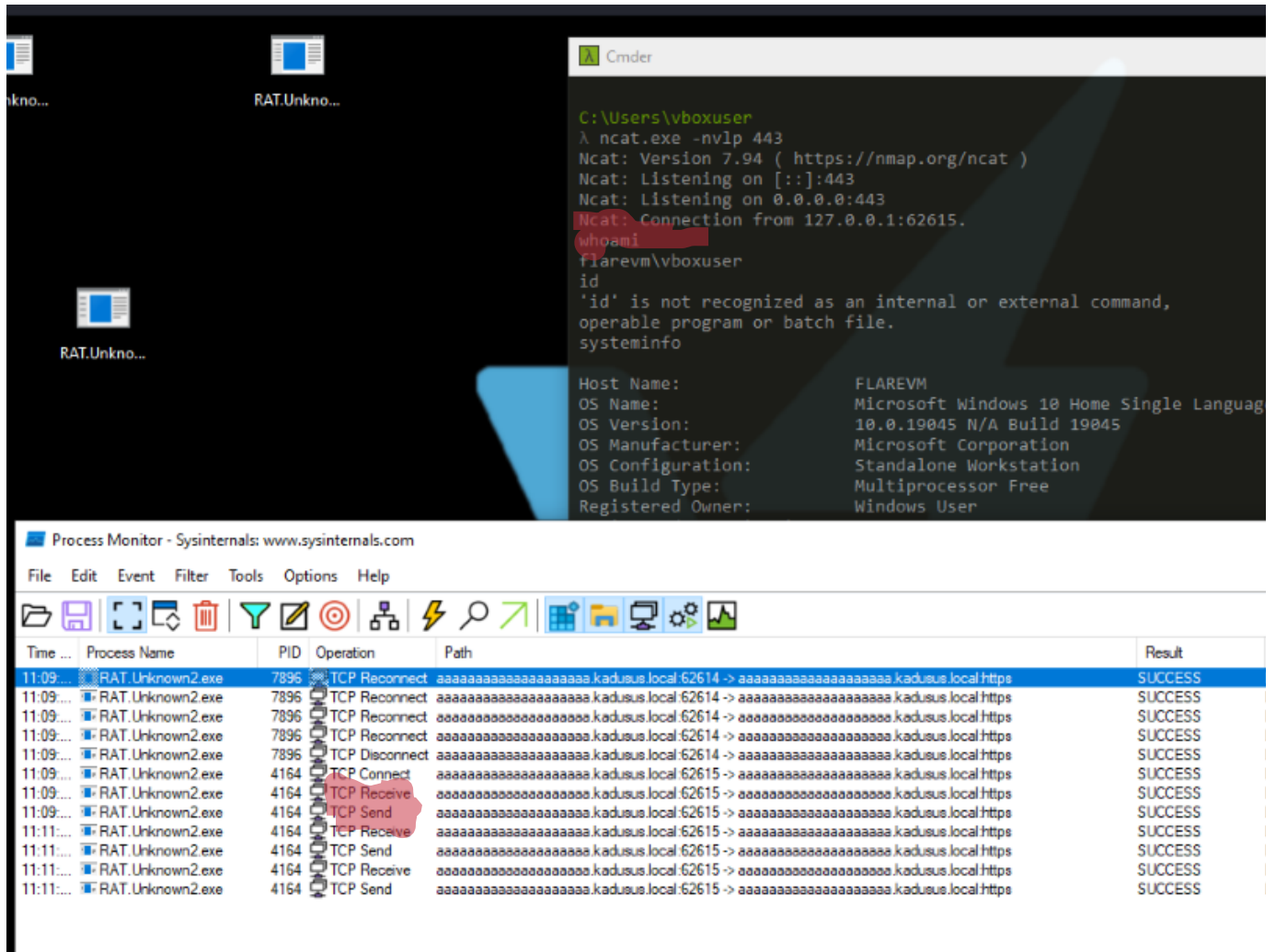
seqnum: 0

connid: 0

Result	Dt
SUCCESS	Ler
SUCCESS	Ler
SUCCESS	Ler
SUCCESS	Ler

Reverse Shell capability

At port 443



Process tree

Have cmd.exe as child of this malware

csrss.exe (344)	Client Server Runtime Process	C:\Windows\system32\csrss.exe	Microsoft Corporation
Explorer.EXE (2740)	Windows Explorer	C:\Windows\Explorer.EXE	Microsoft Corporation
runonce.exe (4128)	Run Once Wrapper	C:\Windows\system32\runonce.exe	Microsoft Corporation
BGAUpsell.EXE (4432)	BGAUpsell	C:\Windows\Temp\MBUSTemp\BGAUpsell.EXE	Microsoft Corporation
SecurityHealthSystray.exe (580)	Windows Security notification icon	C:\Windows\System32\SecurityHealthSystray.exe	Microsoft Corporation
VBoxTray.exe (5980)	VirtualBox Guest Additions Tray Application	C:\Windows\System32\VBoxTray.exe	Oracle and/or its affiliates
Procmon.exe (9156)	Process Monitor	C:\Tools\sysinternals\Procmon.exe	Sysinternals - www.sysinternals.com
Procmon64.exe (8924)	Process Monitor	C:\Users\vbouser\AppData\Local\Temp\Procmon64.exe	Sysinternals - www.sysinternals.com
7zFM.exe (5392)	7-Zip File Manager	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov
RAT.Unknown2.exe (7896)		C:\Users\vbouser\Desktop\RAT.Unknown2.exe	
RAT.Unknown2.exe (4164)		C:\Users\vbouser\Desktop\RAT.Unknown2.exe	
cmd.exe (6780)	Windows Command Processor	C:\Windows\SYSTEM32\cmd.exe	Microsoft Corporation
Conhost.exe (1728)	Console Window Host	C:\Windows\System32\Conhost.exe	Microsoft Corporation
whoami.exe (7396)	whoami - displays logged on user information	C:\Windows\system32\whoami.exe	Microsoft Corporation
cmd.exe (8956)	Windows Command Processor	C:\Windows\SYSTEM32\cmd.exe	Microsoft Corporation
Conhost.exe (2940)	Console Window Host	C:\Windows\System32\Conhost.exe	Microsoft Corporation
cmd.exe (2260)	Windows Command Processor	C:\Windows\SYSTEM32\cmd.exe	Microsoft Corporation
Conhost.exe (1516)	Console Window Host	C:\Windows\System32\Conhost.exe	Microsoft Corporation
systeminfo.exe (2904)	Displays system information	C:\Windows\system32\systeminfo.exe	Microsoft Corporation
cmd.exe (7264)	Windows Command Processor	C:\Windows\SYSTEM32\cmd.exe	Microsoft Corporation
Conhost.exe (3508)	Console Window Host	C:\Windows\System32\Conhost.exe	Microsoft Corporation
cmd.exe (3328)	Windows Command Processor	C:\Windows\SYSTEM32\cmd.exe	Microsoft Corporation
Conhost.exe (7824)	Console Window Host	C:\Windows\System32\Conhost.exe	Microsoft Corporation
whoami.exe (7784)	whoami - displays logged on user information	C:\Windows\system32\whoami.exe	Microsoft Corporation

In last we can say that this EXE have capability of revershell connection and command injection at port 443

