

Rat.Unknown2.exe

Dynamic Analysis

There are nothing important strings or binaries in the malware but while it's network packet is traced in wireshark when executed it try's to connect to some weird dns i.e

aaaaaaaaaaaaaaaaaaaaa.kadusus.local

udp.stream eq 1						
No.	Time	Source	Destination	Protocol	Length	Info
7	6.043843201	192.168.28.128	192.168.28.130	DNS	96	Standard query 0xf6b1 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
8	6.043872524	192.168.28.130	192.168.28.128	ICMP	124	Destination unreachable (Port unreachable)
9	6.048848779	192.168.28.128	192.168.28.130	DNS	96	Standard query 0xf6b1 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
10	6.048871159	192.168.28.130	192.168.28.128	ICMP	124	Destination unreachable (Port unreachable)
11	6.049843257	192.168.28.128	192.168.28.130	DNS	96	Standard query 0xf6b1 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
12	6.049853442	192.168.28.130	192.168.28.128	ICMP	124	Destination unreachable (Port unreachable)
13	6.050145453	192.168.28.128	192.168.28.130	DNS	96	Standard query 0xf6b1 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
14	6.050153354	192.168.28.130	192.168.28.128	ICMP	124	Destination unreachable (Port unreachable)
15	6.050385021	192.168.28.128	192.168.28.130	DNS	96	Standard query 0xf6b1 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
16	6.050392750	192.168.28.130	192.168.28.128	ICMP	124	Destination unreachable (Port unreachable)

Transaction ID: 0xf6b1

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- aaaaaaaaaaaaaaaaaaaaa.kadusus.local: type A, class IN
 - Name: aaaaaaaaaaaaaaaaaaaaa.kadusus.local
 - [Name Length: 24]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

0000	00 00 00 01 00 06 00 0c	29 32 ac 20 00 00 08 00)2.
0010	45 00 00 50 b0 da 00 00	80 11 cf 6f c0 a8 1c 80	E..P....	..o....
0020	c0 a8 1c 82 da 7a 00 35	00 3c 9e c6 f6 b1 01 00z.5	<.....
0030	00 01 00 00 00 00 00 00	14 61 61 61 61 61 61 61	aaaaaaa
0040	61 61 61 61 61 61 61 61	61 61 61 61 61 07 6b 61	aaaaaaa	aaaaa-ka
0050	64 75 73 75 73 05 6c 6f	63 61 6c 00 00 01 00 01	dusus-lo	cal.....

Further looking in procmon it shows the domain and port number it's trying to query to

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result
1:01:2...	RAT.Unknown...	5884	TCP Reconnect	aaaaaaaaaaaaaaaa katusus.local:49764 -> aaaaaaaaaaaaaaaaa katusus.local:https	SUCCESS

1:01:2...
1:01:2...
1:01:2...
1:01:2...
1:01:2...
1:01:2...
1:01:2...
1:01:2...
1:01:2...

Event Properties

Event

Process

Stack

Date:

6/22/2024 1:01:25.4967729 PM

Thread:

0

Class:

Network

Operation:

TCP Reconnect

Result:

SUCCESS

Path:

aaaaaaaaaaaaaaaa.katusus.local:49764 -> aaaaaaaaaaaaaaaaa.katusus.local:https

Duration:

0.0000000

Length:

0

seqnum:

0

connid:

0

↑

↓

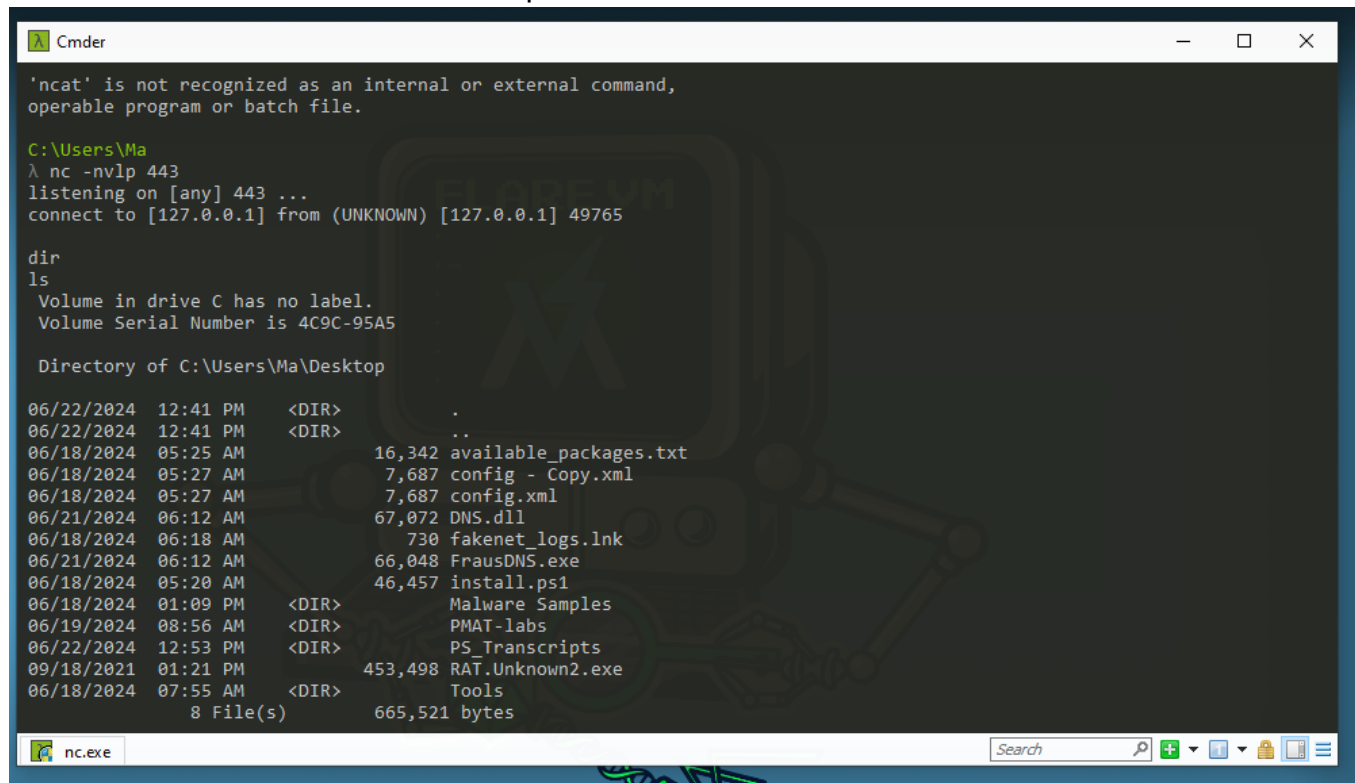
☐ Next Highlighted

Copy All

Close

when we run `nc -nvlp 443` it catches a reverse shell that has command injection vulnerability
when we add any commands in terminal it starts windows cmd.exe and runs the command then

terminate the cmd.exe & hows the output of the command



```
'ncat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Ma
λ nc -nvlp 443
listening on [any] 443 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 49765

dir
ls
Volume in drive C has no label.
Volume Serial Number is 4C9C-95A5

Directory of C:\Users\Ma\Desktop

06/22/2024  12:41 PM    <DIR>          .
06/22/2024  12:41 PM    <DIR>          ..
06/18/2024  05:25 AM             16,342 available_packages.txt
06/18/2024  05:27 AM             7,687 config - Copy.xml
06/18/2024  05:27 AM             7,687 config.xml
06/21/2024  06:12 AM            67,072 DNS.dll
06/18/2024  06:18 AM             730 fakenet_logs.lnk
06/21/2024  06:12 AM            66,048 FrausDNS.exe
06/18/2024  05:20 AM            46,457 install.ps1
06/18/2024  01:09 PM    <DIR>          Malware Samples
06/19/2024  08:56 AM    <DIR>          PMAT-labs
06/22/2024  12:53 PM    <DIR>          PS_Transcripts
09/18/2021  01:21 PM    453,498 RAT.Unknown2.exe
06/18/2024  07:55 AM    <DIR>          Tools
                        8 File(s)          665,521 bytes
```

nc.exe