

# RAT.Uknown.Malware2

RAT.Uknown.Malware2

## Hashes

md5==>

c211704777e168a5151de79dc87ffac7 RAT.Uknown2.exe.malz

SHA256==>

c522e0f1f9edb7e03c0a770e4c52a93db72dce21e7247322f4bbd5b053b967aab5240ce90d6aa65a79e3  
a3068f227346bf0190f9ca762fb8e8d076a58490d7a1 RAT.Uknown2.exe.malz

## Dynamic Analysis

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::800:27ff:fe00...	ff02::2	ICMPv6	70	Router Solicitation from 0a:00:27:00:00:01
2	40.745992327	10.0.0.4	10.0.0.3	DNS	94	Standard query 0xda13 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local
3	40.750626111	10.0.0.3	10.0.0.4	DNS	110	Standard query response 0xda13 A aaaaaaaaaaaaaaaaaaaaa.kadusus.local A 10.0.0.3
4	40.753705280	10.0.0.4	10.0.0.3	TCP	66	49708 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	40.753720993	10.0.0.3	10.0.0.4	TCP	66	443 -> 49708 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
6	40.753935389	10.0.0.4	10.0.0.3	TCP	60	49708 -> 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
7	45.911281074	PcsCompu_2a:37:f3	PcsCompu_63:8a:26	ARP	42	Who has 10.0.0.4? Tell 10.0.0.3
8	45.911867588	PcsCompu_63:8a:26	PcsCompu_2a:37:f3	ARP	60	10.0.0.4 is at 08:00:27:63:8a:26
9	75.898729801	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10	76.906900781	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
11	77.925253079	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	78.937986403	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13	112.212180571	10.0.0.3	10.0.0.2	DHCP	332	DHCP Request - Transaction ID 0x12bf792f
14	112.227851796	10.0.0.2	10.0.0.3	DHCP	590	DHCP ACK - Transaction ID 0x12bf792f
15	117.334851332	PcsCompu_2a:37:f3	PcsCompu_81:4e:21	ARP	42	Who has 10.0.0.2? Tell 10.0.0.3
16	117.335069773	PcsCompu_81:4e:21	PcsCompu_2a:37:f3	ARP	60	10.0.0.2 is at 08:00:27:81:4e:21
17	195.915240681	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18	196.925210137	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	197.925617448	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	198.941043665	10.0.0.4	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 2: 94 bytes on wire (752 bits), 94 bytes captured (752 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

User Datagram Protocol, Src Port: 60365, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xda13

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: 3]

tried DNS: aaaaaaaaaaaaaaaaaaaaa.kadusus.local

potential call out to specific DNS Record on HTTPS port(443)

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
10:35:...	RAT.Uknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa.kadusus.local:1037 -> aaaaaaaaaaaaaaaaaaaaa.kadusus.local/https	SUCCESS	Length: 0, seqnum: 0, connid: 0
10:35:...	RAT.Uknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa.kadusus.local:1037 -> aaaaaaaaaaaaaaaaaaaaa.kadusus.local/https	SUCCESS	Length: 0, seqnum: 0, connid: 0
10:35:...	RAT.Uknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa.kadusus.local:1037 -> aaaaaaaaaaaaaaaaaaaaa.kadusus.local/https	SUCCESS	Length: 0, seqnum: 0, connid: 0
10:35:...	RAT.Uknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa.kadusus.local:1037 -> aaaaaaaaaaaaaaaaaaaaa.kadusus.local/https	SUCCESS	Length: 0, seqnum: 0, connid: 0

# Reverse Shell Capability

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:39:16.6957325 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:26.4559410 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:29.8344464 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:36.9852027 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:40.3195897 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:35.9643205 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:36.4643538 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:36.9796894 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:37.4951083 PM	RAT.Unknown...	840	TCP Reconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:37.4951937 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:37.4951937 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	
10:39:37.4951937 PM	RAT.Unknown...	840	TCP Disconnect	aaaaaaaaaaaaaaaaaaaa katusus local:1037 -> aaaaaaaaaaaaaaaaaaaaa katusus local:https	SUCCESS	

Showing 12 of 441,956 events (0.0027%) Backed by virtual memory

Cmder

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

C:\Users\toxin
λ ncat
Ncat: You must specify a host to connect to. QUITTING.

C:\Users\toxin
λ ncat -nlvp 443
Ncat: Version 5.598BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 127.0.0.1:1038.
ls
FLARE.lnk
Google Chrome.lnk
PMAT-labs-main
PS_Transcripts
RAT.Unknown2.exe
README.txt
analysis
fakenet_logs.lnk
install.ps1
whoami
desktop-tnkuaph\toxin
pwd
C:\Users\toxin\Desktop
```

ncat.exe

## Conclusion

It's a **REVERSE SHELL** injection malware using DNS