Practical Malware Analysis & Triage

Malware Analysis Report

Rat Unknown Malware

Nov 2021 | Ben Whittaker| v1.0

Table of Contents

Executive Summary

SHA256 hash	248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

RAT.Unknown.exe was compiled on Sept 12, 2021 and is a Remote Access Trojan listener that uses port 5555. This trojan requires internet access to site **serv1.ec2-102-95-13-2-ubuntu.local** so that it can download **mscordll.exe** to: C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup making the trojan persistence.

High-Level Technical Summary

The malware trojan RAT.Unknown test if the internet is available. If the internet is available, it downloads **mscordll.exe** from **serv1.ec2-102-95-13-2-ubuntu.local** and saves it to "C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ **mscordll.exe"** (mscordll.exe was not available as this was .local) RAT.Unknown creates a listener on port 5555 which is able to execute commands on the host.

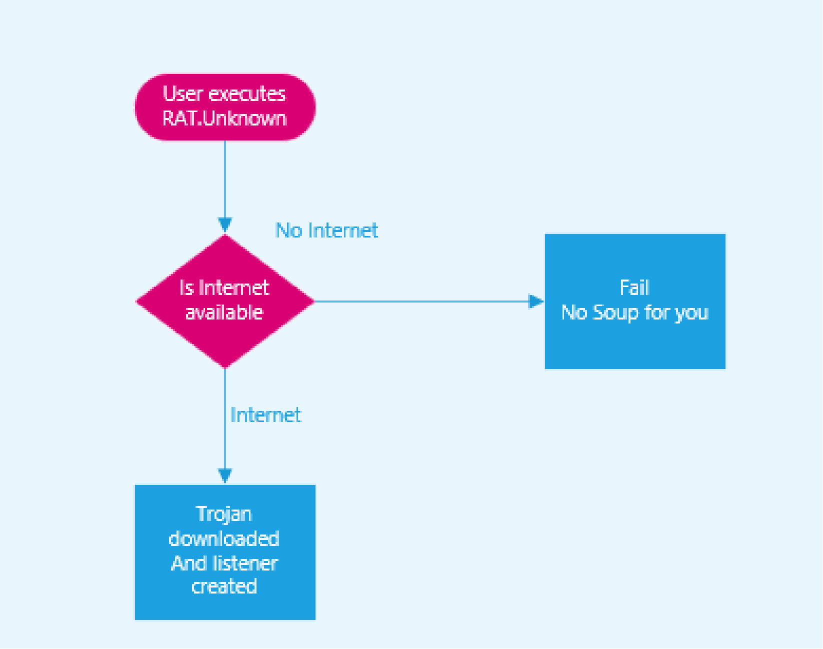

User executes RAT.Unknown
No Internet
Is Internet available
Fail
No Soup for you
Internet
Trojan downloaded And listener created

Figure 1 Basic Flow Diagram

Malware Composition

Rat Unknown consists of the following components:

File Name	SHA256 Hash
RAT.Unknown	248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C
mscordll.exe	Not available

Basic Static Analysis

File hash of RAT.Unknown.exe

Hash Type	Hash
md5	689FF2C6F94E31ABBA1DDEBF68BE810E
sha1	69B8ECF6B7CDE185DAED76D66100B6A31FD1A668
sha256	248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

Strings

C:\Tools\FLOSS>

FLARE Thu 11/25/2021 13:20:07.79

Interesting Strings

@http://serv1.ec2-102-95-13-2-ubuntu.local - **Interesting URL**

@[+] what command can I run for you - **Interesting**

@[+] online

@NO SOUP FOR YOU - **interesting**

@\mscordll.exe

@Nim httpclient/1.0.6 – **May be a Nim executable**

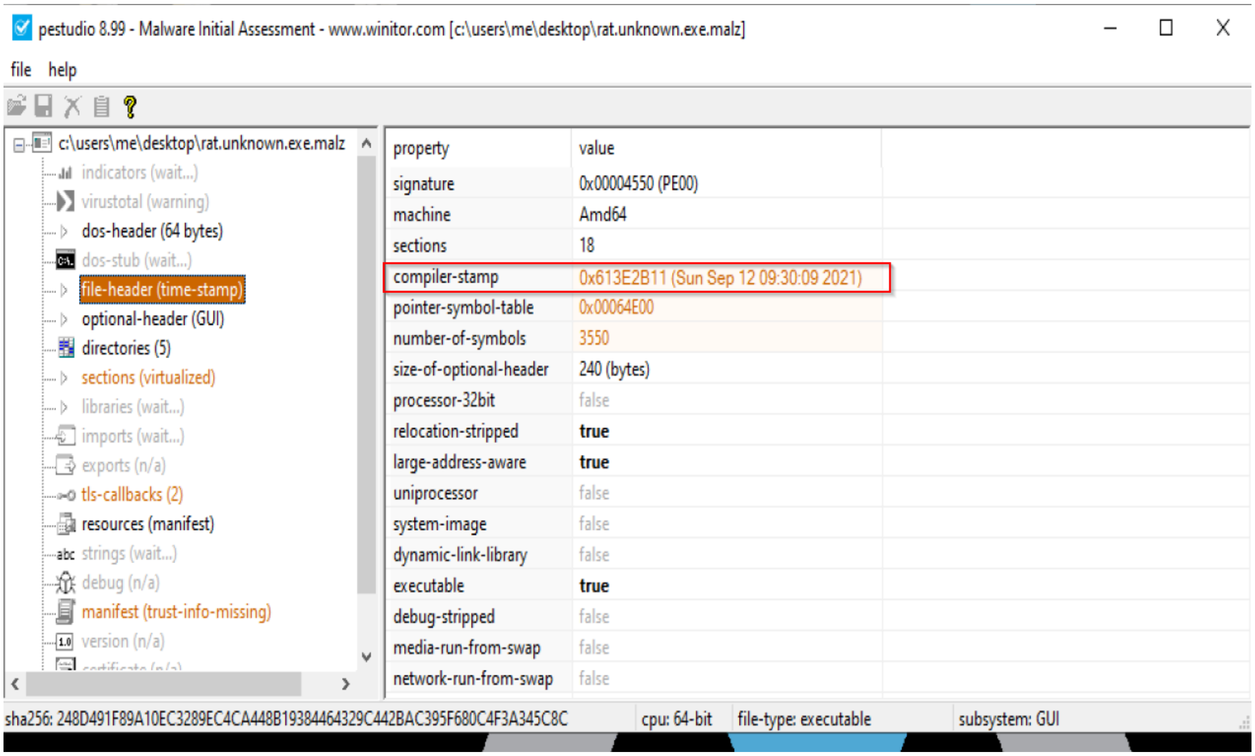
@/msdcorelib.exe

@AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup - **May be a file location**

GNU C99 9.2-win32 20191008 -m64 -mtune=generic -march=x86-64 -g -O2 -std=gnu99 -fno-PIE – **Compile information**

Pestudio output

Pestudio was used to identify possible static artifacts.



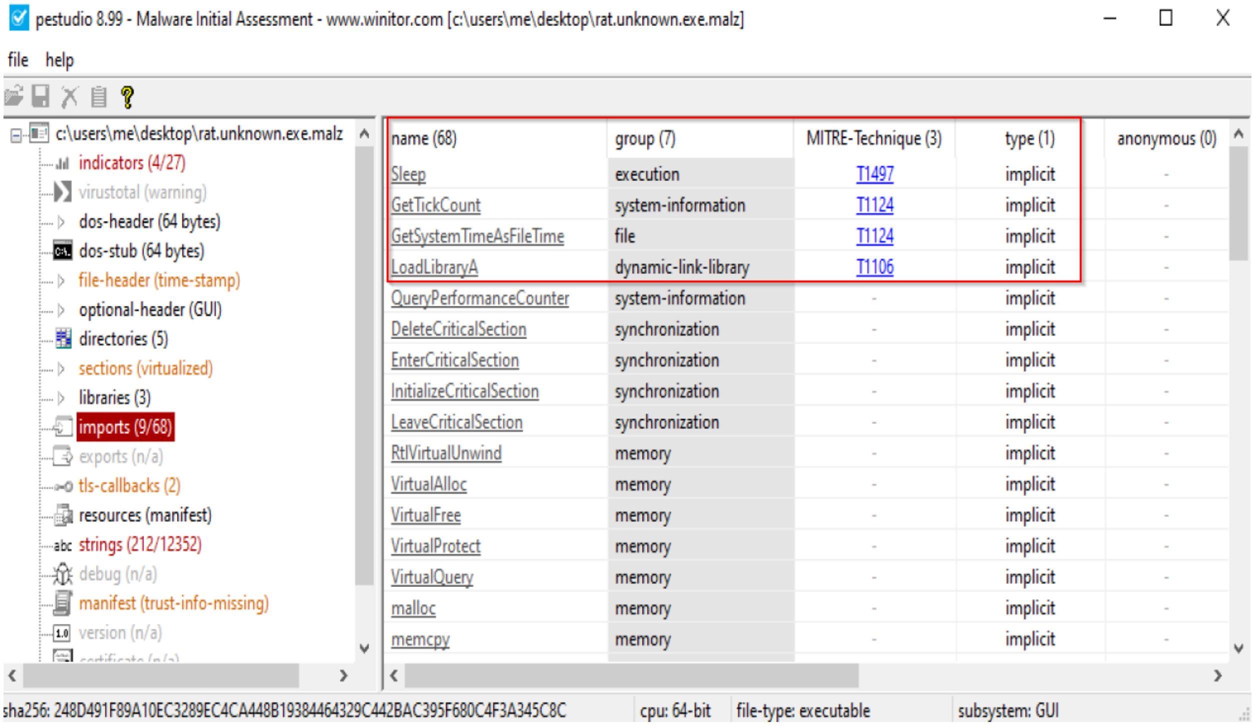
pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\me\desktop\rat.unknown.exe.malz]

property	value
signature	0x00004550 (PE00)
machine	Amd64
sections	18
compiler-stamp	0x613E2B11 (Sun Sep 12 09:30:09 2021)
pointer-symbol-table	0x00064E00
number-of-symbols	3550
size-of-optional-header	240 (bytes)
processor-32bit	false
relocation-stripped	**true**
large-address-aware	**true**
uniprocessor	false
system-image	false
dynamic-link-library	false
executable	**true**
debug-stripped	false
media-run-from-swap	false
network-run-from-swap	false

sha256: 248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C cpu: 64-bit file-type: executable subsystem: GUI

Figure 2 Pestudio

Pestudio – Sorted on MITRE Technique



pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\me\desktop\rat.unknown.exe.malz]

name (68)	group (7)	MITRE-Technique (3)	type (1)	anonymous (0)
Sleep	execution	T1497	implicit	-
GetTickCount	system-information	T1124	implicit	-
GetSystemTimeAsFileTime	file	T1124	implicit	-
LoadLibraryA	dynamic-link-library	T1106	implicit	-
QueryPerformanceCounter	system-information	-	implicit	-
DeleteCriticalSection	synchronization	-	implicit	-
EnterCriticalSection	synchronization	-	implicit	-
InitializeCriticalSection	synchronization	-	implicit	-
LeaveCriticalSection	synchronization	-	implicit	-
RtlVirtualUnwind	memory	-	implicit	-
VirtualAlloc	memory	-	implicit	-
VirtualFree	memory	-	implicit	-
VirtualProtect	memory	-	implicit	-
VirtualQuery	memory	-	implicit	-
malloc	memory	-	implicit	-
memcpy	memory	-	implicit	-

sha256: 248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C | cpu: 64-bit | file-type: executable | subsystem: GUI

Figure 3 mscordll.exe

MITRE ATT&CK [1]is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The following methods are tag within pestudio MITRE T1106 [2], T1124[3] and T1497[4]

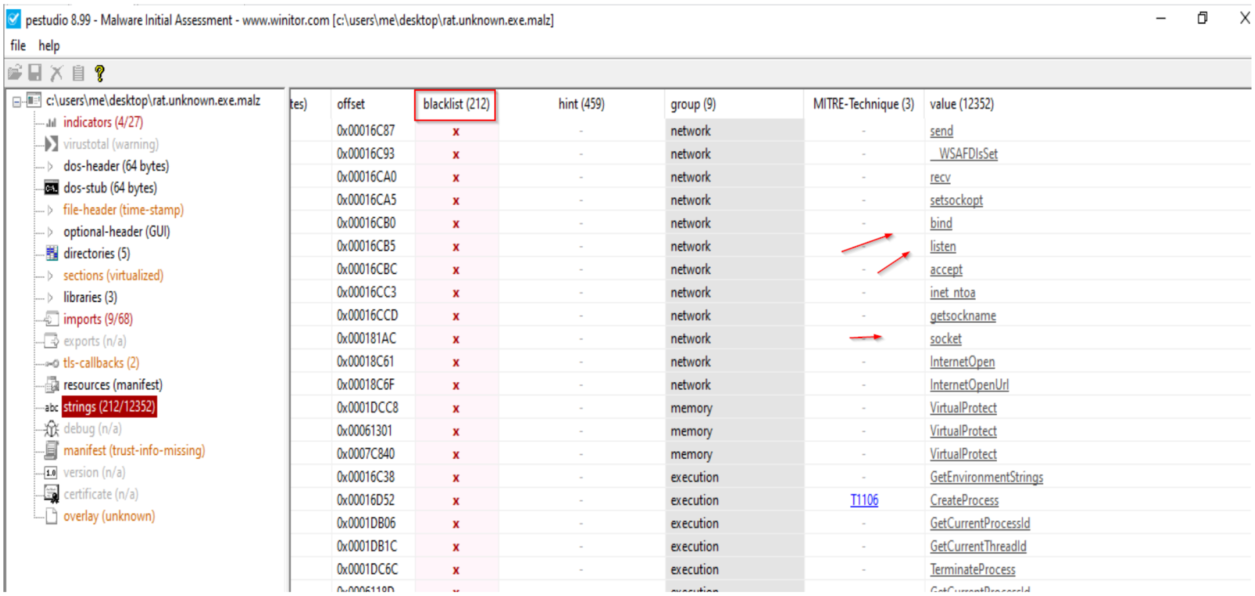
[1] https://attack.mitre.org/

[2] https://attack.mitre.org/techniques/T1106/

[3] https://attack.mitre.org/techniques/T1124/

[4] https://attack.mitre.org/techniques/T1497/

Pestudio – Sorted on blacklist


pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\me\desktop\rat.unknown.exe.malz]

tes)	offset	blacklist (212)	hint (459)	group (9)	MITRE-Technique (3)	value (12352)
	0x00016C87	x	-	network	-	send
	0x00016C93	x	-	network	-	__WSAFDIsSet
	0x00016CA0	x	-	network	-	recv
	0x00016CA5	x	-	network	-	setsockopt
	0x00016CB0	x	-	network	-	bind
	0x00016CB5	x	-	network	-	listen
	0x00016CBC	x	-	network	-	accept
	0x00016CC3	x	-	network	-	inet_ntoa
	0x00016CCD	x	-	network	-	getsockname
	0x000181AC	x	-	network	-	socket
	0x00018C61	x	-	network	-	InternetOpen
	0x00018C6F	x	-	network	-	InternetOpenUrl
	0x0001DCC8	x	-	memory	-	VirtualProtect
	0x00061301	x	-	memory	-	VirtualProtect
	0x0007C840	x	-	memory	-	VirtualProtect
	0x00016C38	x	-	execution	-	GetEnvironmentStrings
	0x00016D52	x	-	execution	T1106	CreateProcess
	0x0001DB06	x	-	execution	-	GetCurrentProcessId
	0x0001DB1C	x	-	execution	-	GetCurrentThreadId
	0x0001DC6C	x	-	execution	-	TerminateProcess

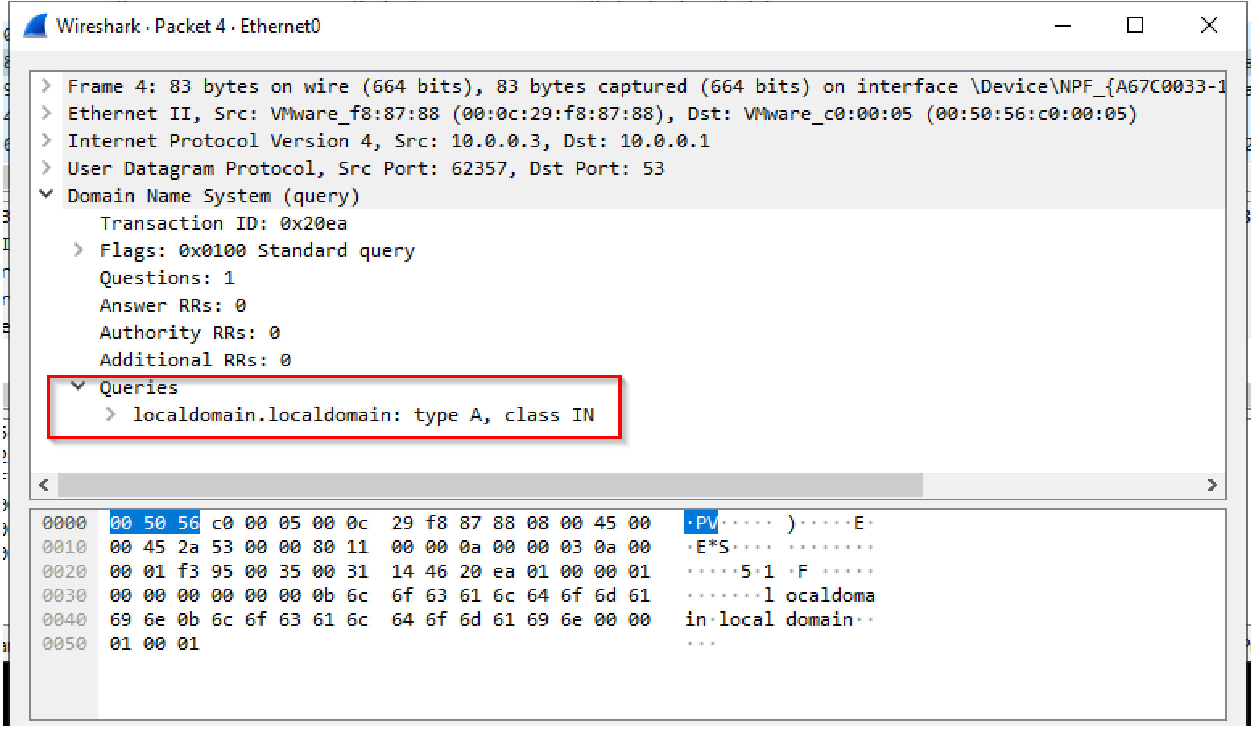
Figure 4 Pestudio – Sorted on blacklist

Seeing items like socket, bind and listen could be an indicator of network activity.

Basic Dynamic Analysis

No Internet

Started out without having inetsim running.



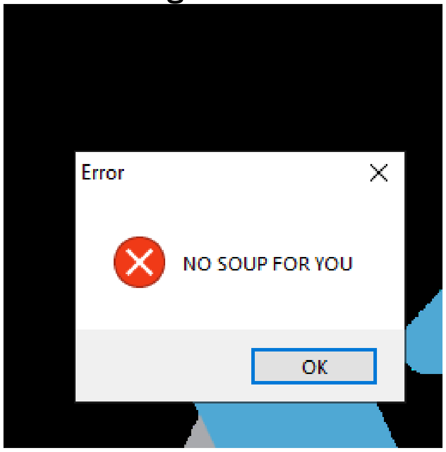
Wireshark · Packet 4 · Ethernet0

```
> Frame 4: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{A67C0033-1
> Ethernet II, Src: VMware_f8:87:88 (00:0c:29:f8:87:88), Dst: VMware_c0:00:05 (00:50:56:c0:00:05)
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 62357, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x20ea
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > localdomain.localdomain: type A, class IN

0000  00 50 56 c0 00 05 00 0c  29 f8 87 88 08 00 45 00   ·PV····· )·····E·
0010  00 45 2a 53 00 00 80 11  00 00 0a 00 00 03 0a 00   ·E*S···· ········
0020  00 01 f3 95 00 35 00 31  14 46 20 ea 01 00 00 01   ·····5·1 ·F ·····
0030  00 00 00 00 00 00 0b 6c  6f 63 61 6c 64 6f 6d 61   ·······l ocaldoma
0040  69 6e 0b 6c 6f 63 61 6c  64 6f 6d 61 69 6e 00 00   in·local domain··
0050  01 00 01                                           ···
```

Figure 5 Wireshark no internet

Did a query for localdomain.localdomain.

Error message



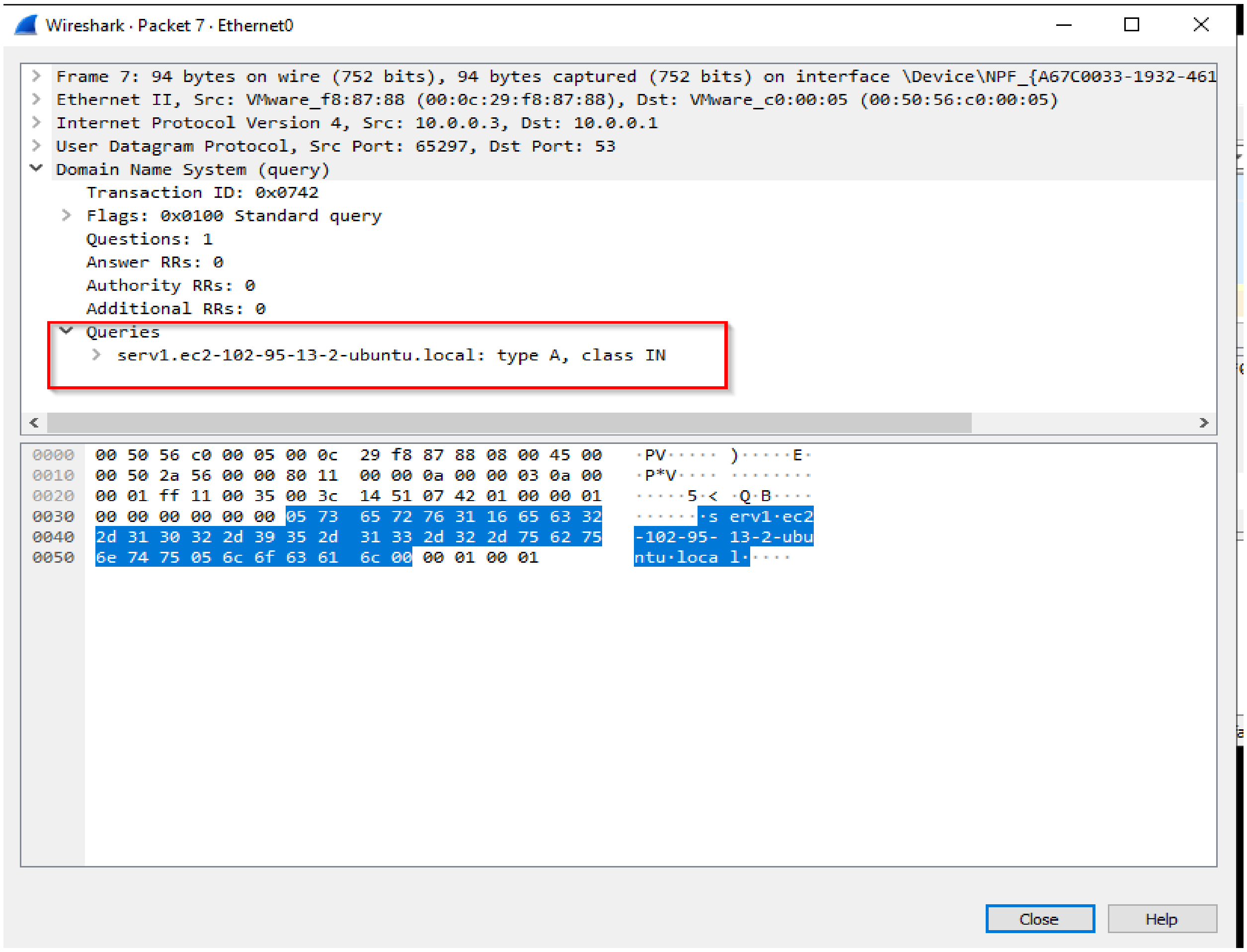
Error

NO SOUP FOR YOU

Figure 6 Error Message "NO SOUP FOR YOU"

With INETSIM running

Internet simulation with Inetsim



```
> Frame 7: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{A67C0033-1932-461
> Ethernet II, Src: VMware_f8:87:88 (00:0c:29:f8:87:88), Dst: VMware_c0:00:05 (00:50:56:c0:00:05)
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 65297, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x0742
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   v Queries
      > serv1.ec2-102-95-13-2-ubuntu.local: type A, class IN
```

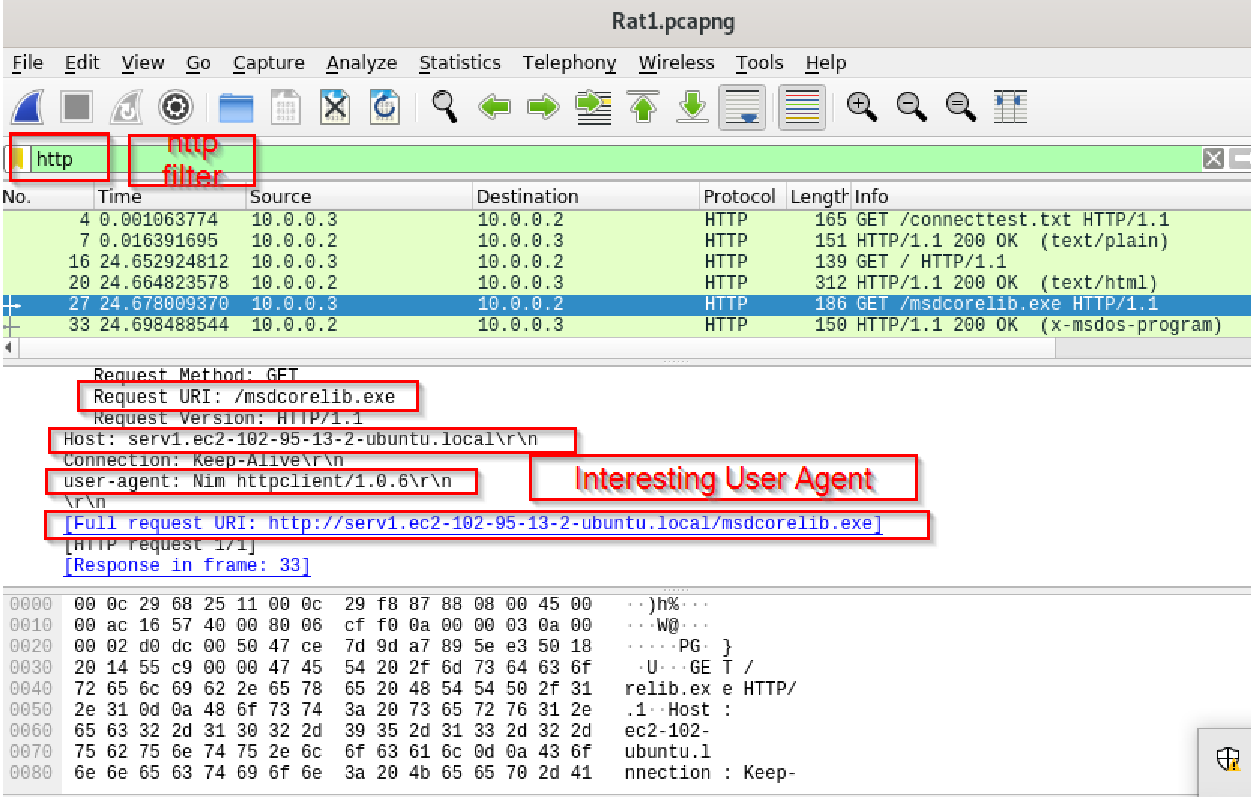
```
0000  00 50 56 c0 00 05 00 0c  29 f8 87 88 08 00 45 00   ·PV····· )·····E·
0010  00 50 2a 56 00 00 80 11  00 00 0a 00 00 03 0a 00   ·P*V···· ········
0020  00 01 ff 11 00 35 00 3c  14 51 07 42 01 00 00 01   ·····5·< ·Q·B····
0030  00 00 00 00 00 00 05 73  65 72 76 31 16 65 63 32   ·······s erv1·ec2
0040  2d 31 30 32 2d 39 35 2d  31 33 2d 32 2d 75 62 75   -102-95- 13-2-ubu
0050  6e 74 75 05 6c 6f 63 61  6c 00 00 01 00 01         ntu·loca l·····
```

Figure 7 Wireshark with INETSIM

Data from INETSIM

[2021-11-25 16:52:18] [1603] [dns_53_tcp_udp 1607] [10.0.0.3] recv: Query Type A, Class IN, **Name serv1.ec2-102-95-13-2-ubuntu.local**
[2021-11-25 16:52:18] [1603] [dns_53_tcp_udp 1607] [10.0.0.3] **send: serv1.ec2-102-95-13-2-ubuntu.local 3600 IN A 10.0.0.3**

Using Wireshark and a filter of http we find a request for msdcorelib.exe.


Rat1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

http filter

```
No.   Time           Source      Destination  Protocol Length Info
    4 0.001063774    10.0.0.3    10.0.0.2     HTTP     165 GET /connecttest.txt HTTP/1.1
    7 0.016391695    10.0.0.2    10.0.0.3     HTTP     151 HTTP/1.1 200 OK  (text/plain)
   16 24.652924812   10.0.0.3    10.0.0.2     HTTP     139 GET / HTTP/1.1
   20 24.664823578   10.0.0.2    10.0.0.3     HTTP     312 HTTP/1.1 200 OK  (text/html)
   27 24.678009370   10.0.0.3    10.0.0.2     HTTP     186 GET /msdcorelib.exe HTTP/1.1
   33 24.698488544   10.0.0.2    10.0.0.3     HTTP     150 HTTP/1.1 200 OK  (x-msdos-program)
```

```
        Request Method: GET
        Request URI: /msdcorelib.exe
        Request Version: HTTP/1.1
    Host: serv1.ec2-102-95-13-2-ubuntu.local\r\n
    Connection: Keep-Alive\r\n
    user-agent: Nim httpclient/1.0.6\r\n
    \r\n
    [Full request URI: http://serv1.ec2-102-95-13-2-ubuntu.local/msdcorelib.exe]
    [HTTP request 1/1]
    [Response in frame: 33]
```

Interesting User Agent

```
0000  00 0c 29 68 25 11 00 0c  29 f8 87 88 08 00 45 00   ··)h%···
0010  00 ac 16 57 40 00 80 06  cf f0 0a 00 00 03 0a 00   ···W@···
0020  00 02 d0 dc 00 50 47 ce  7d 9d a7 89 5e e3 50 18   ·····PG· }
0030  20 14 55 c9 00 00 47 45  54 20 2f 6d 73 64 63 6f    ·U···GE T /
0040  72 65 6c 69 62 2e 65 78  65 20 48 54 54 50 2f 31   relib.ex e HTTP/
0050  2e 31 0d 0a 48 6f 73 74  3a 20 73 65 72 76 31 2e   .1··Host :
0060  65 63 32 2d 31 30 32 2d  39 35 2d 31 33 2d 32 2d   ec2-102-
0070  75 62 75 6e 74 75 2e 6c  6f 63 61 6c 0d 0a 43 6f   ubuntu.l
0080  6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70 2d 41   nnection : Keep-
```

Figure 8 Wireshark http filter

```
[2021-11-26 07:53:30] [1441] [http_80_tcp 2693] [10.0.0.3:53747] stat: 1 method=GET url=http://serv1.ec2-102-95-13-2-ubuntu.local/msdcorelib.exe sent=/var/lib/inetsim/http/fakefiles/sample_gui.exe postdata=
```

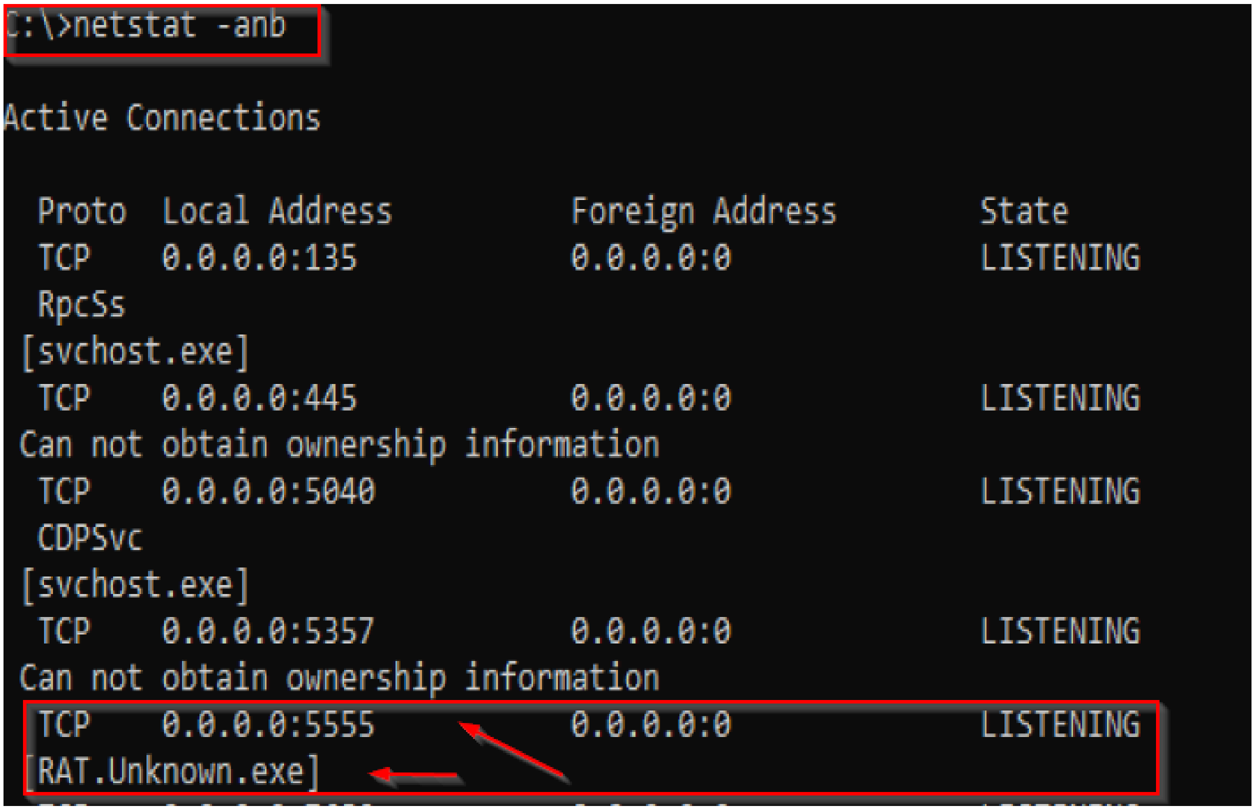
Checked for C:\Users\Me\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ mscordll.exe

```
C:\Users\Me\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>md5sum mscordll.exe
1af0ac17b51334de97e162b4a19b989b *mscordll.exe
```

Which matches the sample_gui.exe from Inetsim

```
emnux@remnux:/usr/share/inetsim/data/http/fakefiles$ md5sum sample_gui.exe
1af0ac17b51334de97e162b4a19b989b  sample_gui.exe
FLARE Fri 11/26/2021  3:45:20.30
C:\Users\Me\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup>md5sum mscordll.exe
1af0ac17b51334de97e162b4a19b989b *mscordll.exe
```

Network stats show Rat.Unknown is listening on port 5555

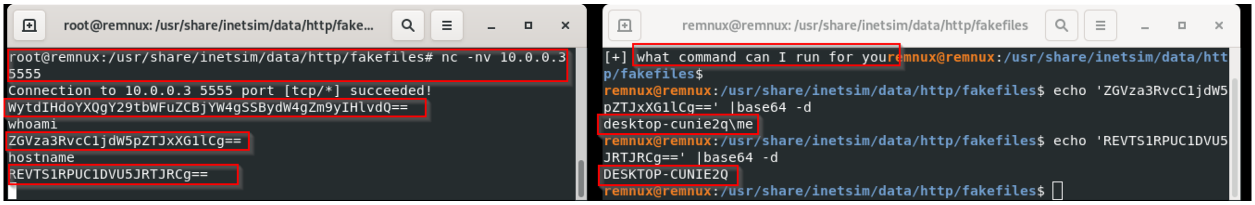


```
:\>netstat -anb

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5555           0.0.0.0:0              LISTENING
 [RAT.Unknown.exe]
```

Figure 9 netstat -anb output

Knowing that RAT.Unknown is listening on port 5555, netcat was used on remnux to connect on port 5555.

This screenshot shows netcat connection on the left along with the commands whoami and hostname. On the right is the base64 decoded output.


root@remnux: /usr/share/inetsim/data/http/fake...
remnux@remnux: /usr/share/inetsim/data/http/fakefiles

```
root@remnux:/usr/share/inetsim/data/http/fakefiles# nc -nv 10.0.0.3
5555
Connection to 10.0.0.3 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
whoami
ZGVza3RvcC1jdW5pZTJxXG1lCg==
hostname
REVTS1RPUC1DVU5JRTJRCg==
```

```
[+] what command can I run for youremnux@remnux:/usr/share/inetsim/data/htt
p/fakefiles$
remnux@remnux:/usr/share/inetsim/data/http/fakefiles$ echo 'ZGVza3RvcC1jdW5
pZTJxXG1lCg==' |base64 -d
desktop-cunie2q\me
remnux@remnux:/usr/share/inetsim/data/http/fakefiles$ echo 'REVTS1RPUC1DVU5
JRTJRCg==' |base64 -d
DESKTOP-CUNIE2Q
remnux@remnux:/usr/share/inetsim/data/http/fakefiles$
```

Figure 10 Netcat

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

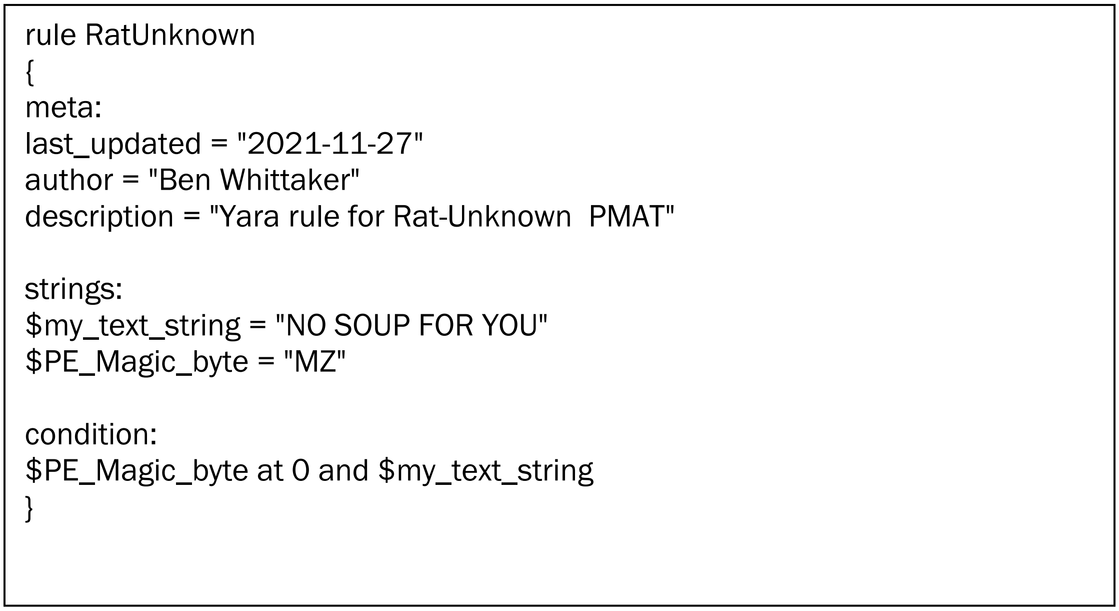
Network Indicators

Domain	Port
Localdomain.localdomain	53
serv1.ec2-102-95-13-2-ubuntu.local	53
http://serv1.ec2-102-95-13-2-ubuntu.local/msdcorelib.exe	80
Reverse shell listener	5555

Host-based Indicators

Indicator	Type
C:\Users\Me\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>md5sum **mscordll.exe**	File
RAT.Unknown.exe	Evidence of Execution

Rules & Signatures



```
rule RatUnknown
{
meta:
last_updated = "2021-11-27"
author = "Ben Whittaker"
description = "Yara rule for Rat-Unknown  PMAT"

strings:
$my_text_string = "NO SOUP FOR YOU"
$PE_Magic_byte = "MZ"

condition:
$PE_Magic_byte at 0 and $my_text_string
}
```

Figure 11 Yara Rule

Test of Yara Rule rat-yara.yara

```
C:\Users\Me\Desktop>yara32  rat-yara.yara RAT.Unknown.exe
RatUnknown RAT.Unknown.exe
```

Attack Mitigation

Blocking connections to port 5555 could prevent this attack.