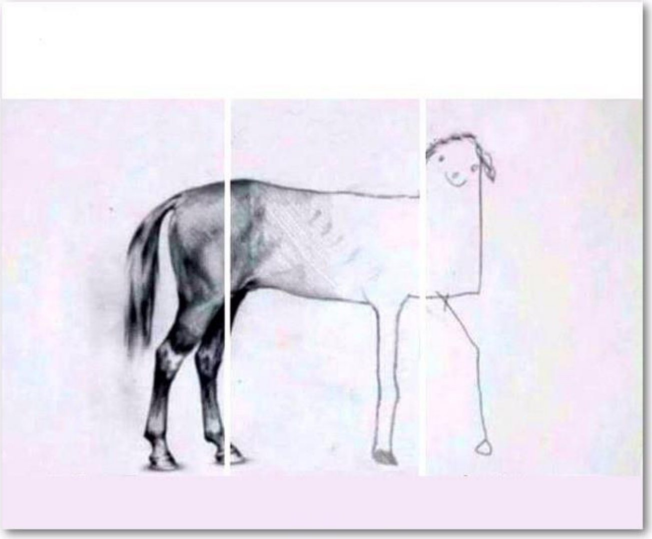


Practical Malware Analysis & Triage

Malware Analysis Report

Remote Access Trojan Malware

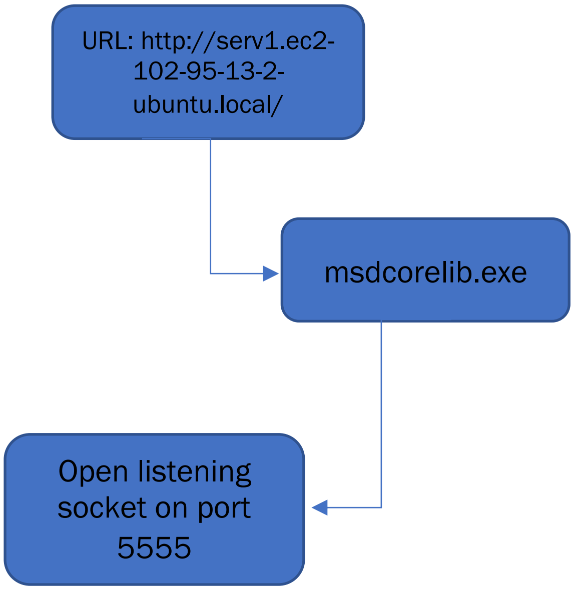
Aug. 2022 | eyyys3c | v1.0

Table of Contents

Executive Summary

SHA256 hash	248d491f89a10ec3289ec4ca448b19384464329c442bac395f680c4f3a345c8c

Remote Access Trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. In this sample, the malware will start to query a specific call back URL to download the initial payload *msdcorelib.exe* which will also open a listening socket on the infected machine.



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

msdcorelib.exe

Open listening socket on port 5555

Remote Access Trojan Malware
Aug 2022
v1.0

Malware Composition

RAT consists of the following components:

File Name	SHA256 Hash
msdcorelib.exe	0a1ae65540bfbe339805376eff97a85fb56660553916c5ada835c543f7a141e3

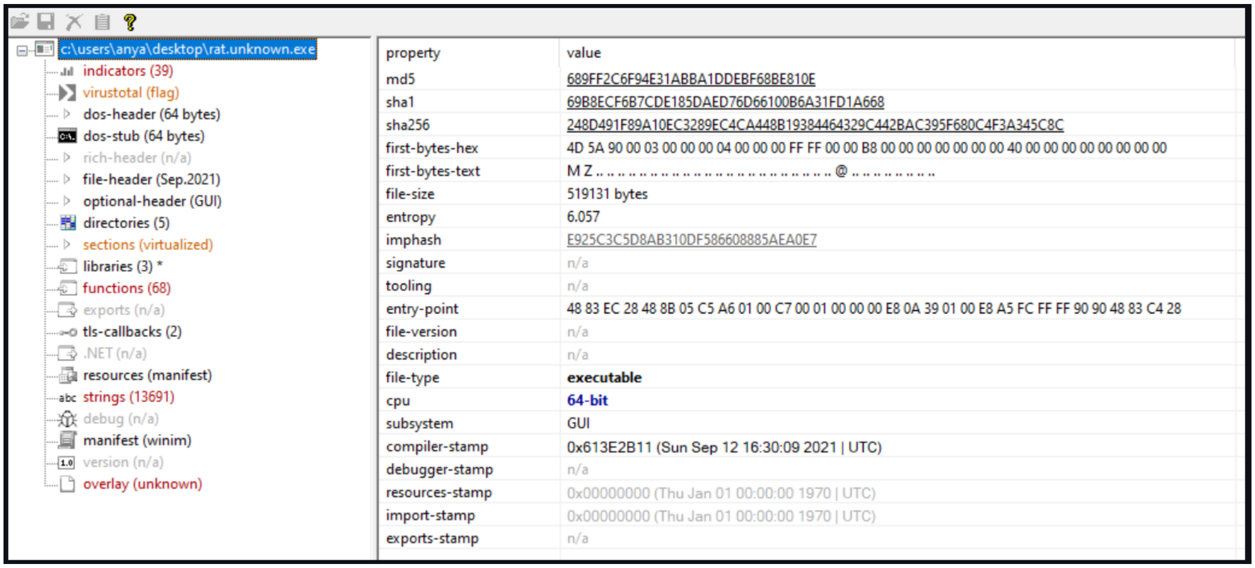
msdcorelib.exe

The executable that runs after a successfully connecting to the callback URL

Basic Static Analysis

Floss/Strings

```
@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
@intrt explr
@http://serv1.ec2-102-95-13-2-ubuntu.local
```

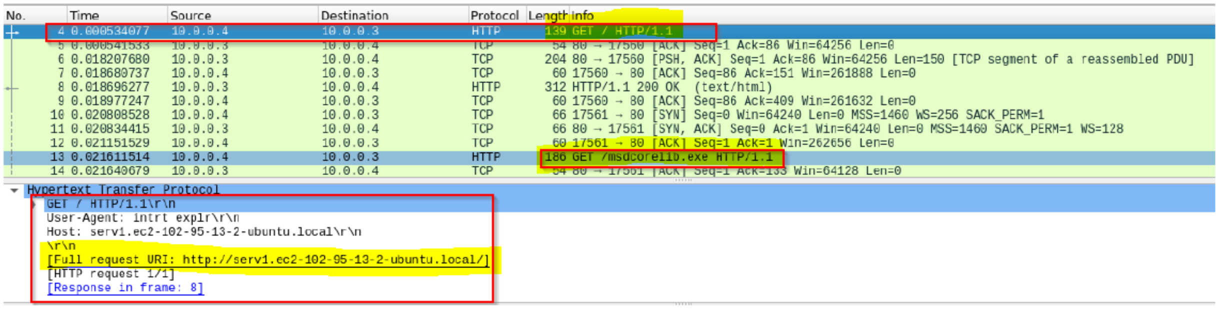


- c:\users\anya\desktop\rat.unknown.exe
  - indicators (39)
  - virustotal (flag)
  - dos-header (64 bytes)
  - dos-stub (64 bytes)
  - rich-header (n/a)
  - file-header (Sep.2021)
  - optional-header (GUI)
  - directories (5)
  - sections (virtualized)
  - libraries (3) *
  - functions (68)
  - exports (n/a)
  - tls-callbacks (2)
  - .NET (n/a)
  - resources (manifest)
  - strings (13691)
  - debug (n/a)
  - manifest (winim)
  - version (n/a)
  - overlay (unknown)

property	value
md5	689FF2C6F94E31ABBA1DDEBF68BE810E
sha1	69B8ECF6B7CDE185DAED76D66100B6A31FD1A668
sha256	248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	519131 bytes
entropy	6.057
imphash	E925C3C5D8AB310DF586608885AEA0E7
signature	n/a
tooling	n/a
entry-point	48 83 EC 28 48 8B 05 C5 A6 01 00 C7 00 01 00 00 00 E8 0A 39 01 00 E8 A5 FC FF FF 90 90 48 83 C4 28
file-version	n/a
description	n/a
file-type	**executable**
cpu	**64-bit**
subsystem	GUI
compiler-stamp	0x613E2B11 (Sun Sep 12 16:30:09 2021 | UTC)
debugger-stamp	n/a
resources-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
import-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
exports-stamp	n/a

Basic Dynamic Analysis

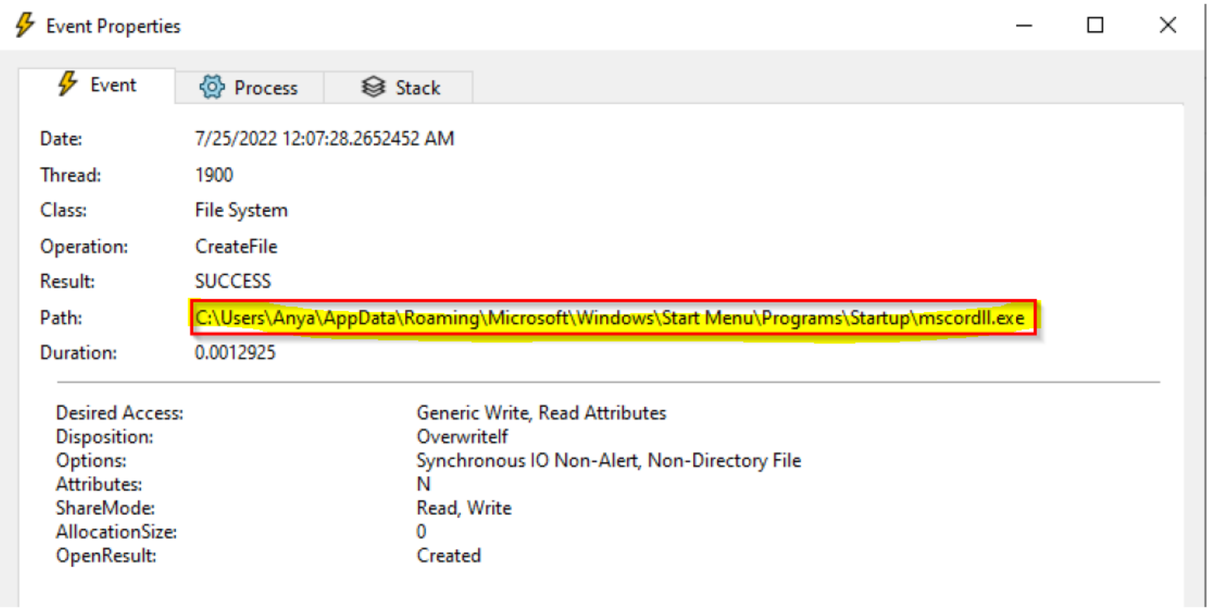
Network-Based Signatures



```
No.   Time          Source      Destination  Protocol Length Info
    4 0.000534077   10.0.0.4    10.0.0.3     HTTP     139 GET / HTTP/1.1
    5 0.000541533   10.0.0.3    10.0.0.4     TCP       54 80 → 17560 [ACK] Seq=1 Ack=86 Win=64256 Len=0
    6 0.018207680   10.0.0.3    10.0.0.4     TCP      204 80 → 17560 [PSH, ACK] Seq=1 Ack=86 Win=64256 Len=150 [TCP segment of a reassembled PDU]
    7 0.018680737   10.0.0.4    10.0.0.3     TCP       60 17560 → 80 [ACK] Seq=86 Ack=151 Win=261888 Len=0
    8 0.018696277   10.0.0.3    10.0.0.4     HTTP     312 HTTP/1.1 200 OK  (text/html)
    9 0.018977247   10.0.0.4    10.0.0.3     TCP       60 17560 → 80 [ACK] Seq=86 Ack=409 Win=261632 Len=0
   10 0.020808528   10.0.0.4    10.0.0.3     TCP       66 17561 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   11 0.020834415   10.0.0.3    10.0.0.4     TCP       66 80 → 17561 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
   12 0.021151529   10.0.0.4    10.0.0.3     TCP       60 17561 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   13 0.021611514   10.0.0.4    10.0.0.3     HTTP     186 GET /msdcorelib.exe HTTP/1.1
   14 0.021640679   10.0.0.3    10.0.0.4     TCP       54 80 → 17561 [ACK] Seq=1 Ack=133 Win=64128 Len=0

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  User-Agent: intrt explr\r\n
  Host: serv1.ec2-102-95-13-2-ubuntu.local\r\n
  \r\n
  [Full request URI: http://serv1.ec2-102-95-13-2-ubuntu.local/]
  [HTTP request 1/1]
  [Response in frame: 8]
```

Potential File Download: msdcorelib.exe

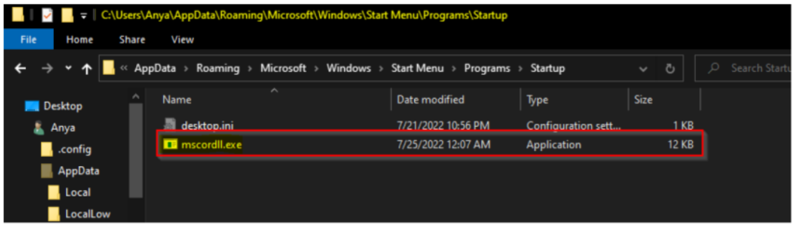
Host-Based Indicator



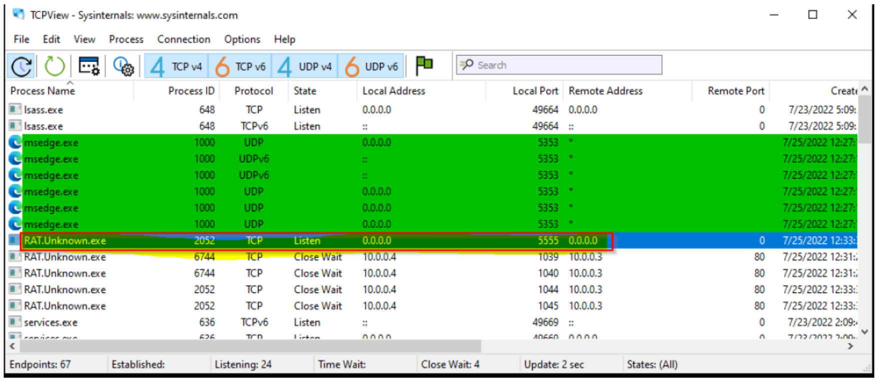
Date: 7/25/2022 12:07:28.2652452 AM
Thread: 1900
Class: File System
Operation: CreateFile
Result: SUCCESS
Path: C:\Users\Anya\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe
Duration: 0.0012925

Desired Access: Generic Write, Read Attributes
Disposition: OverwriteIf
Options: Synchronous IO Non-Alert, Non-Directory File
Attributes: N
ShareMode: Read, Write
AllocationSize: 0
OpenResult: Created

Persistence Binary


C:\Users\Anya\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
File
Home
Share
View
« AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup
Search Startu
Desktop
Anya
.config
AppData
Local
LocalLow

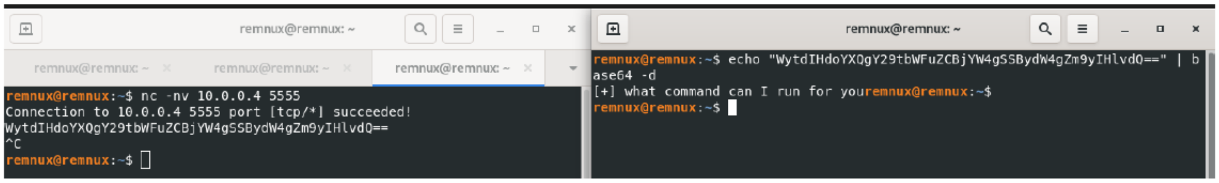
Name	Date modified	Type	Size
desktop.ini	7/21/2022 10:56 PM	Configuration sett...	1 KB
mscordll.exe	7/25/2022 12:07 AM	Application	12 KB


TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
4 TCP v4
6 TCP v6
4 UDP v4
6 UDP v6
Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
lsass.exe	648	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	7/23/2022 5:09:
lsass.exe	648	TCPv6	Listen	::	49664	::	0	7/23/2022 5:09:
msedge.exe	1000	UDP		0.0.0.0	5353	*		7/25/2022 12:27:
msedge.exe	1000	UDPv6		::	5353	*		7/25/2022 12:27:
msedge.exe	1000	UDPv6		::	5353	*		7/25/2022 12:27:
msedge.exe	1000	UDP		0.0.0.0	5353	*		7/25/2022 12:27:
msedge.exe	1000	UDP		0.0.0.0	5353	*		7/25/2022 12:27:
msedge.exe	1000	UDP		0.0.0.0	5353	*		7/25/2022 12:27:
RAT.Unknown.exe	2052	TCP	Listen	0.0.0.0	5555	0.0.0.0	0	7/25/2022 12:33:
RAT.Unknown.exe	6744	TCP	Close Wait	10.0.0.4	1039	10.0.0.3	80	7/25/2022 12:31:
RAT.Unknown.exe	6744	TCP	Close Wait	10.0.0.4	1040	10.0.0.3	80	7/25/2022 12:31:
RAT.Unknown.exe	2052	TCP	Close Wait	10.0.0.4	1044	10.0.0.3	80	7/25/2022 12:33:
RAT.Unknown.exe	2052	TCP	Close Wait	10.0.0.4	1045	10.0.0.3	80	7/25/2022 12:33:
services.exe	636	TCPv6	Listen	::	49669	::	0	7/23/2022 2:09:
services.exe	636	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	7/23/2022 2:09:

Endpoints: 67 | Established: | Listening: 24 | Time Wait: | Close Wait: 4 | Update: 2 sec | States: (All)

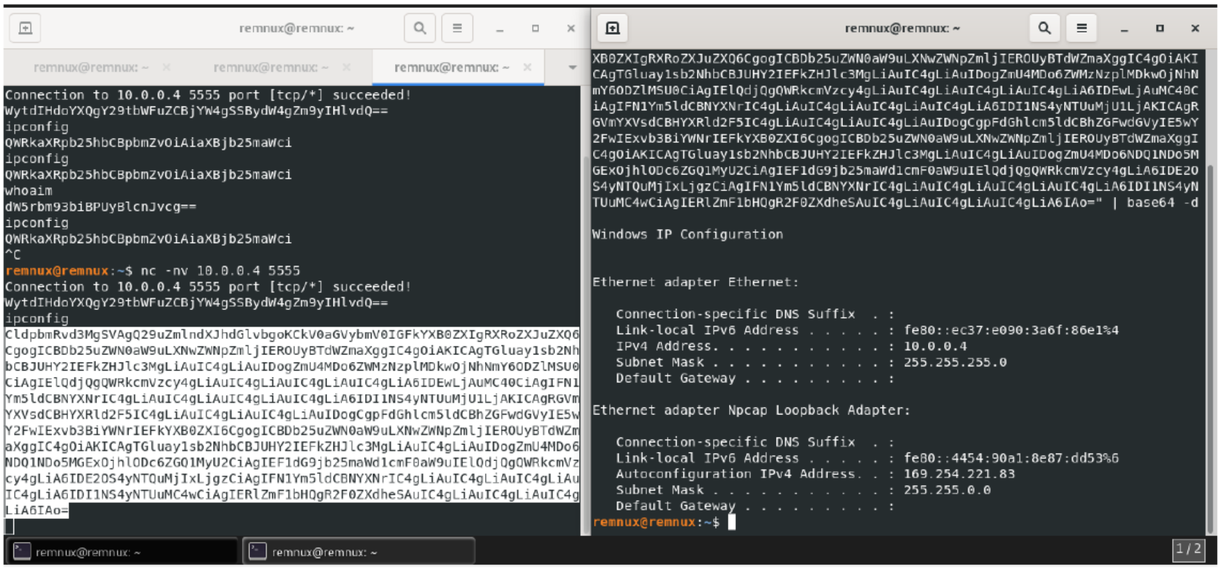
encoded base64 from port 5555



```
remnux@remnux:~$ nc -nv 10.0.0.4 5555
Connection to 10.0.0.4 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
^C
remnux@remnux:~$ 
```

```
remnux@remnux:~$ echo "WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==" | b
ase64 -d
[+] what command can I run for youremnux@remnux:~$
remnux@remnux:~$ 
```

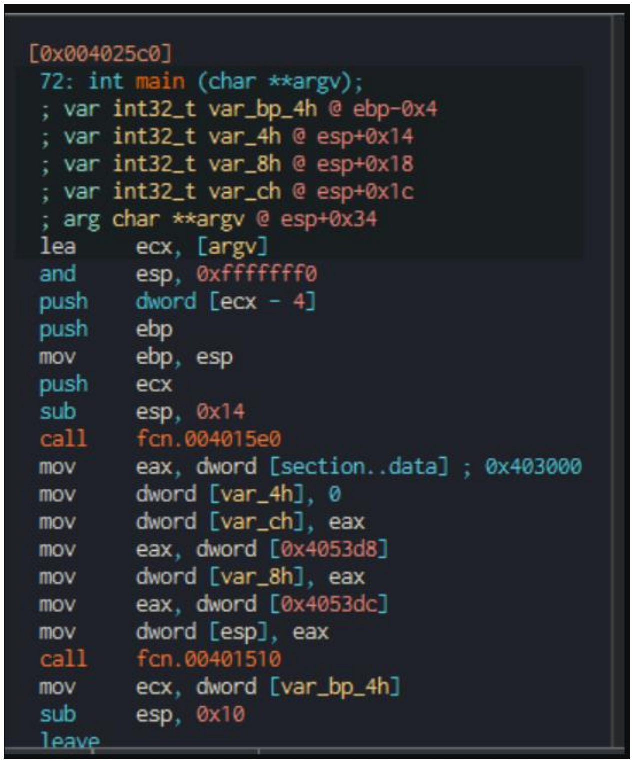
Command Injection Capability:



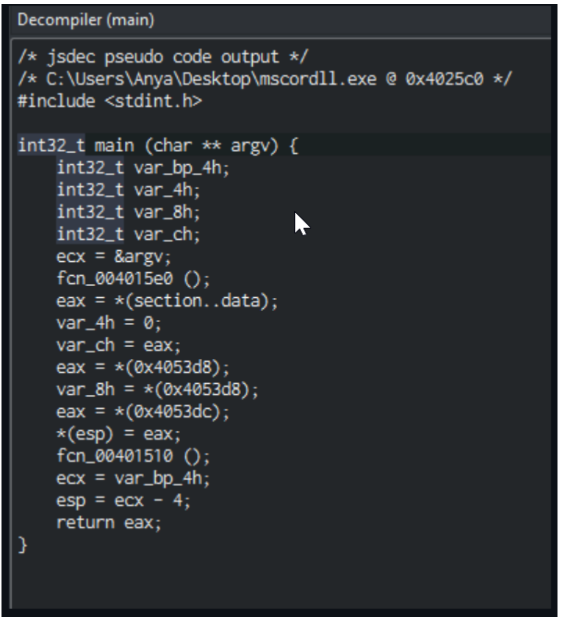
```
Connection to 10.0.0.4 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
ipconfig
QWRkaXRpb25hbCBpbmZvOiAiaXBjb25maWci
ipconfig
QWRkaXRpb25hbCBpbmZvOiAiaXBjb25maWci
whoaim
dW5rbm93biBPUyBlcnJvcg==
ipconfig
QWRkaXRpb25hbCBpbmZvOiAiaXBjb25maWci
^C
remnux@remnux:~$ nc -nv 10.0.0.4 5555
Connection to 10.0.0.4 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
ipconfig
CldpbmRvd3MgSVAgQ29uZmlndXJhdGlvbgoKCkV0aGVybmV0IGFkYXB0ZXIgRXRoZXJuZXQ6
CgogICBDb25uZWN0aW9uLXNwZWNpZmljIEROUyBTdWZmaXggIC4gOiAKICAgTGluay1sb2Nh
bCBJUHY2IEFkZHJlc3MgLiAuIC4gLiAuIDogZmU4MDo6ZWMzNzplMDkwOjNhNmY6ODZlMSU0
CiAgIElQdjQgQWRkcmVzcy4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IDEwLjAuMC40CiAgIFN1
Ym5ldCBNYXNrIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IDI1NS4yNTUuMjU1LjAKICAgRGVm
YXVsdCBHYXRld2F5IC4gLiAuIC4gLiAuIC4gLiAuIDogCgpFdGhlcm5ldCBhZGFwdGVyIE5w
Y2FwIExvb3BiYWNrIEFkYXB0ZXI6CgogICBDb25uZWN0aW9uLXNwZWNpZmljIEROUyBTdWZm
aXggIC4gOiAKICAgTGluay1sb2NhbCBJUHY2IEFkZHJlc3MgLiAuIC4gLiAuIDogZmU4MDo6
NDQ1NDo5MGExOjhlODc6ZGQ1MyU2CiAgIEF1dG9jb25maWd1cmF0aW9uIElQdjQgQWRkcmVz
cy4gLiA6IDE2OS4yNTQuMjIxLjgzCiAgIFN1Ym5ldCBNYXNrIC4gLiAuIC4gLiAuIC4gLiAu
IC4gLiA6IDI1NS4yNTUuMC4wCiAgIERlZmF1bHQgR2F0ZXdheSAuIC4gLiAuIC4gLiAuIC4g
LiA6IAo=
```

```
XB0ZXIgRXRoZXJuZXQ6CgogICBDb25uZWN0aW9uLXNwZWNpZmljIEROUyBTdWZmaXggIC4gOiAKI
CAgTGluay1sb2NhbCBJUHY2IEFkZHJlc3MgLiAuIC4gLiAuIDogZmU4MDo6ZWMzNzplMDkwOjNhN
mY6ODZlMSU0CiAgIElQdjQgQWRkcmVzcy4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IDEwLjAuMC40C
iAgIFN1Ym5ldCBNYXNrIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IDI1NS4yNTUuMjU1LjAKICAgR
GVmYXVsdCBHYXRld2F5IC4gLiAuIC4gLiAuIC4gLiAuIDogCgpFdGhlcm5ldCBhZGFwdGVyIE5wY
2FwIExvb3BiYWNrIEFkYXB0ZXI6CgogICBDb25uZWN0aW9uLXNwZWNpZmljIEROUyBTdWZmaXggI
C4gOiAKICAgTGluay1sb2NhbCBJUHY2IEFkZHJlc3MgLiAuIC4gLiAuIDogZmU4MDo6NDQ1NDo5M
GExOjhlODc6ZGQ1MyU2CiAgIEF1dG9jb25maWd1cmF0aW9uIElQdjQgQWRkcmVzcy4gLiA6IDE2O
S4yNTQuMjIxLjgzCiAgIFN1Ym5ldCBNYXNrIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IDI1NS4yN
TUuMC4wCiAgIERlZmF1bHQgR2F0ZXdheSAuIC4gLiAuIC4gLiAuIC4gLiA6IAo=" | base64 -d

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ec37:e090:3a6f:86e1%4
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4454:90a1:8e87:dd53%6
   Autoconfiguration IPv4 Address. . : 169.254.221.83
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
remnux@remnux:~$ 
```

Advanced Static Analysis

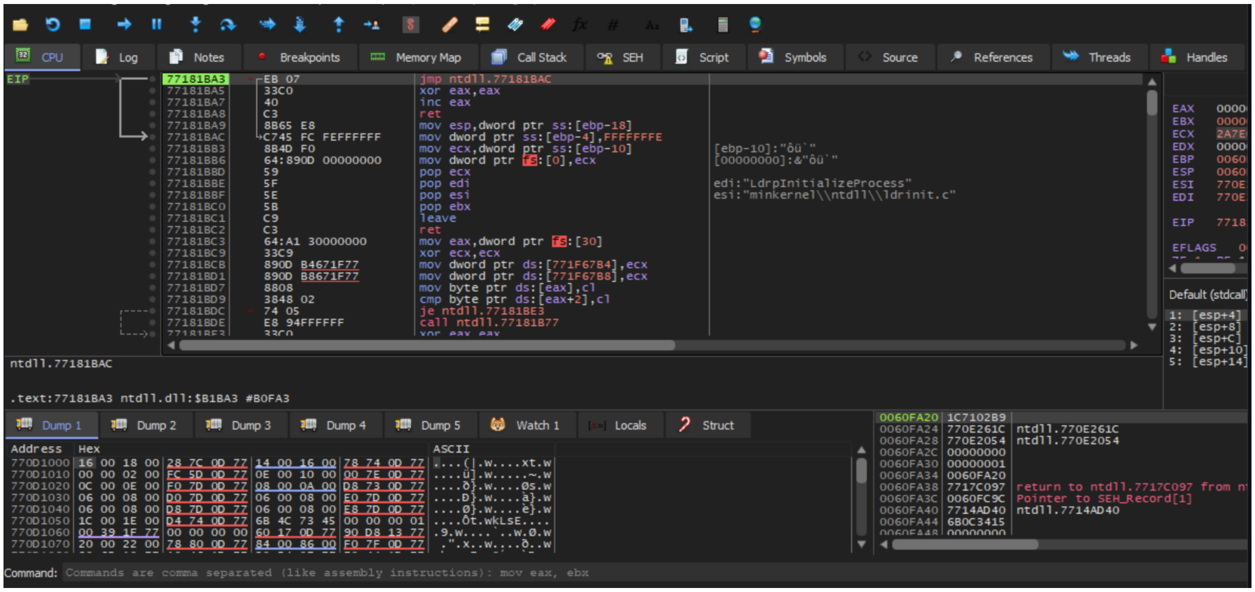


```
[0x004025c0]
 72: int main (char **argv);
 ; var int32_t var_bp_4h @ ebp-0x4
 ; var int32_t var_4h @ esp+0x14
 ; var int32_t var_8h @ esp+0x18
 ; var int32_t var_ch @ esp+0x1c
 ; arg char **argv @ esp+0x34
 lea     ecx, [argv]
 and     esp, 0xfffffff0
 push    dword [ecx - 4]
 push    ebp
 mov     ebp, esp
 push    ecx
 sub     esp, 0x14
 call    fcn.004015e0
 mov     eax, dword [section..data] ; 0x403000
 mov     dword [var_4h], 0
 mov     dword [var_ch], eax
 mov     eax, dword [0x4053d8]
 mov     dword [var_8h], eax
 mov     eax, dword [0x4053dc]
 mov     dword [esp], eax
 call    fcn.00401510
 mov     ecx, dword [var_bp_4h]
 sub     esp, 0x10
 leave
```



```
/* jsdec pseudo code output */
/* C:\Users\Anya\Desktop\mscordll.exe @ 0x4025c0 */
#include <stdint.h>

int32_t main (char ** argv) {
    int32_t var_bp_4h;
    int32_t var_4h;
    int32_t var_8h;
    int32_t var_ch;
    ecx = &argv;
    fcn_004015e0 ();
    eax = *(section..data);
    var_4h = 0;
    var_ch = eax;
    eax = *(0x4053d8);
    var_8h = *(0x4053d8);
    eax = *(0x4053dc);
    *(esp) = eax;
    fcn_00401510 ();
    ecx = var_bp_4h;
    esp = ecx - 4;
    return eax;
}
```

Advanced Dynamic Analysis



```
77181BA3   EB 07                jmp ntdll.77181BAC
77181BA5   33C0                 xor eax,eax
77181BA7   40                   inc eax
77181BA8   C3                   ret
77181BA9   8B65 E8              mov esp,dword ptr ss:[ebp-18]
77181BAC   C745 FC FEFFFFFF     mov dword ptr ss:[ebp-4],FFFFFFFE
77181BB3   8B4D F0              mov ecx,dword ptr ss:[ebp-10]        [ebp-10]:"ôü`"
77181BB6   64:890D 00000000     mov dword ptr fs:[0],ecx             [00000000]:&"ôü`"
77181BBD   59                   pop ecx
77181BBE   5F                   pop edi                              edi:"LdrpInitializeProcess"
77181BBF   5E                   pop esi                              esi:"minkernel\\ntdll\\ldrinit.c"
77181BC0   5B                   pop ebx
77181BC1   C9                   leave
77181BC2   C3                   ret
77181BC3   64:A1 30000000       mov eax,dword ptr fs:[30]
77181BC9   33C9                 xor ecx,ecx
77181BCB   890D B4671F77        mov dword ptr ds:[771F67B4],ecx
77181BD1   890D B8671F77        mov dword ptr ds:[771F67B8],ecx
77181BD7   8808                 mov byte ptr ds:[eax],cl
77181BD9   3848 02              cmp byte ptr ds:[eax+2],cl
77181BDC   74 05                je ntdll.77181BE3
77181BDE   E8 94FFFFFF          call ntdll.77181B77
77181BE3   33C0                 xor eax,eax

ntdll.77181BAC

.text:77181BA3 ntdll.dll:$B1BA3 #B0FA3
```

```
EAX    0000
EBX    0000
ECX    2A7E
EDX    0000
EBP    0060
ESP    0060
ESI    770E
EDI    770E

EIP    7718

EFLAGS    0

1:  [esp+4]
2:  [esp+8]
3:  [esp+C]
4:  [esp+10]
5:  [esp+14]
```

```
Address   Hex                                              ASCII
770D1000  16 00 18 00 28 7C 0D 77 14 00 16 00 78 74 0D 77  ....(|.w....xt.w
770D1010  00 00 02 00 FC 5D 0D 77 0E 00 10 00 00 7E 0D 77  ....ü].w.....~.w
770D1020  0C 00 0E 00 F0 7D 0D 77 08 00 0A 00 D8 73 0D 77  ....ð}.w....Øs.w
770D1030  06 00 08 00 D0 7D 0D 77 06 00 08 00 E0 7D 0D 77  ....Ð}.w....à}.w
770D1040  06 00 08 00 D8 7D 0D 77 06 00 08 00 E8 7D 0D 77  ....Ø}.w....è}.w
770D1050  1C 00 1E 00 D4 74 0D 77 6B 4C 73 45 00 00 00 01  ....Ôt.wkLsE....
770D1060  00 39 1F 77 00 00 00 00 60 17 0D 77 90 D8 13 77  .9.w....`..w.Ø.w
770D1070  20 00 22 00 78 80 0D 77 84 00 86 00 F0 7F 0D 77   .".x..w....ð..w
```

```
0060FA20  1C7102B9
0060FA24  770E261C  ntdll.770E261C
0060FA28  770E2054  ntdll.770E2054
0060FA2C  00000000
0060FA30  00000001
0060FA34  0060FA20
0060FA38  7717C097  return to ntdll.7717C097 from nt
0060FA3C  0060FC9C  Pointer to SEH_Record[1]
0060FA40  7714AD40  ntdll.7714AD40
0060FA44  6B0C3415
0060FA48  00000000
```

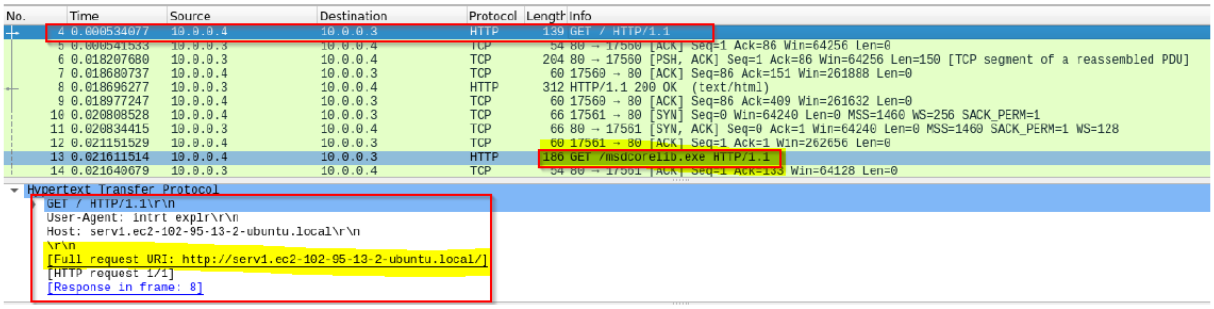
Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Remote Access Trojan Malware
Aug 2022
v1.0

Indicators of Compromise

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

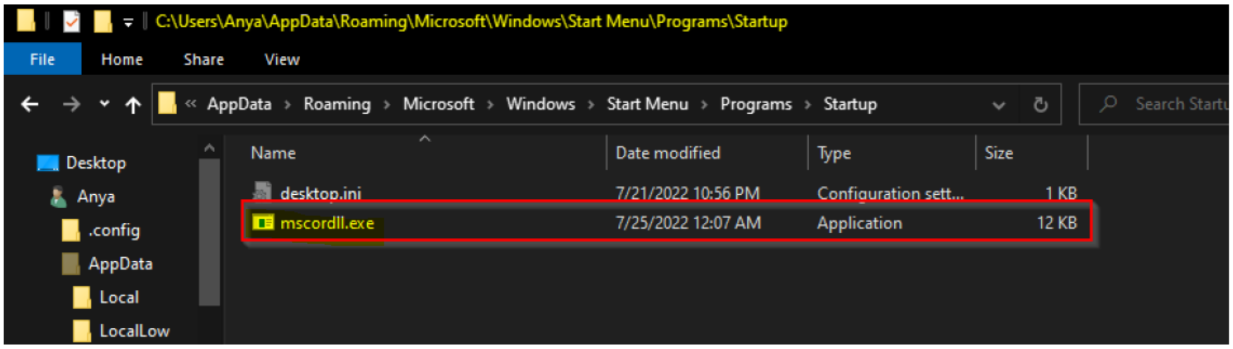
Network Indicators



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000534077	10.0.0.4	10.0.0.3	HTTP	139	GET / HTTP/1.1
5	0.000541533	10.0.0.3	10.0.0.4	TCP	54	80 → 17560 [ACK] Seq=1 Ack=86 Win=64256 Len=0
6	0.018207680	10.0.0.3	10.0.0.4	TCP	204	80 → 17560 [PSH, ACK] Seq=1 Ack=86 Win=64256 Len=150 [TCP segment of a reassembled PDU]
7	0.018680737	10.0.0.4	10.0.0.3	TCP	60	17560 → 80 [ACK] Seq=86 Ack=151 Win=261888 Len=0
8	0.018696277	10.0.0.3	10.0.0.4	HTTP	312	HTTP/1.1 200 OK (text/html)
9	0.018977247	10.0.0.4	10.0.0.3	TCP	60	17560 → 80 [ACK] Seq=86 Ack=409 Win=261632 Len=0
10	0.020808528	10.0.0.4	10.0.0.3	TCP	66	17561 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	0.020834415	10.0.0.3	10.0.0.4	TCP	66	80 → 17561 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
12	0.021151529	10.0.0.4	10.0.0.3	TCP	60	17561 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
13	0.021611514	10.0.0.4	10.0.0.3	HTTP	186	GET /msdcorelib.exe HTTP/1.1
14	0.021640679	10.0.0.3	10.0.0.4	TCP	54	80 → 17561 [ACK] Seq=1 Ack=133 Win=64128 Len=0

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  User-Agent: intrt explr\r\n
  Host: serv1.ec2-102-95-13-2-ubuntu.local\r\n
  \r\n
  [Full request URI: http://serv1.ec2-102-95-13-2-ubuntu.local/]
  [HTTP request 1/1]
  [Response in frame: 8]
```

Host-based Indicators



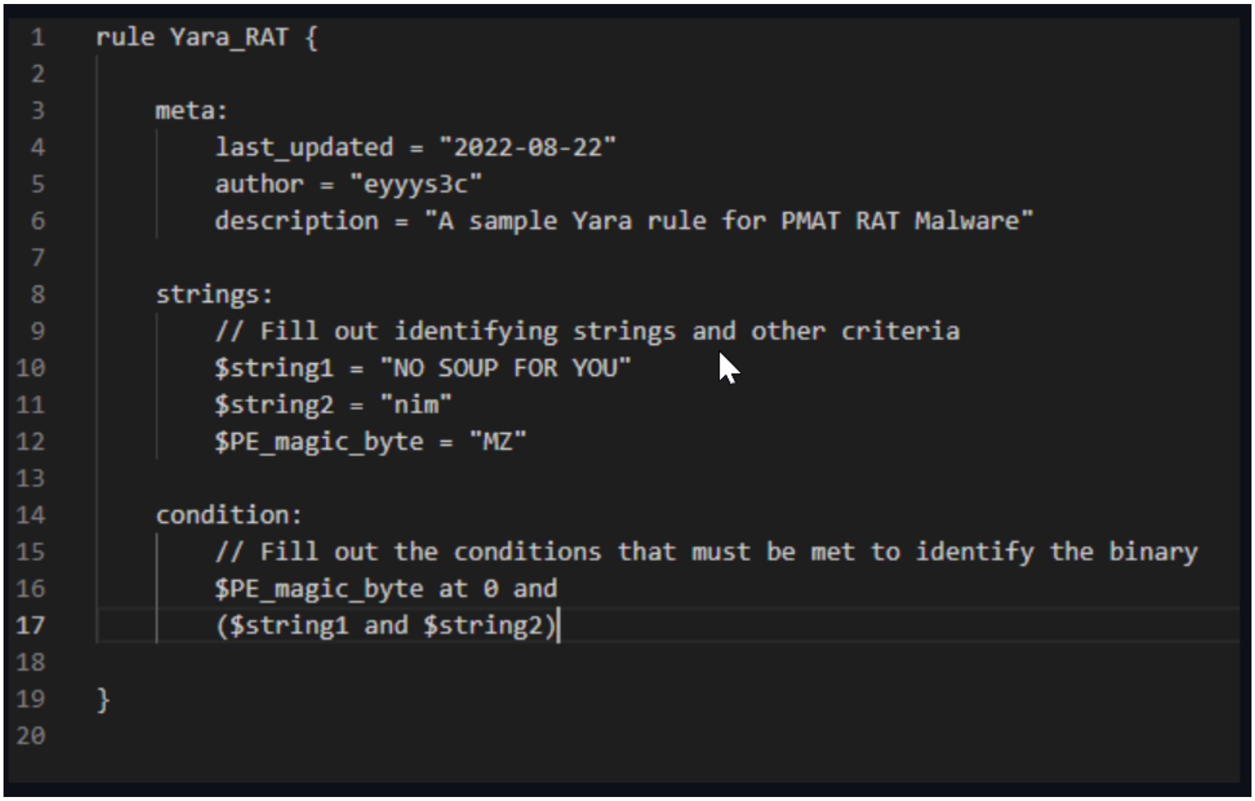
C:\Users\Anya\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

File
Home
Share
View
AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup
Search Startu
Desktop
Anya
.config
AppData
Local
LocalLow

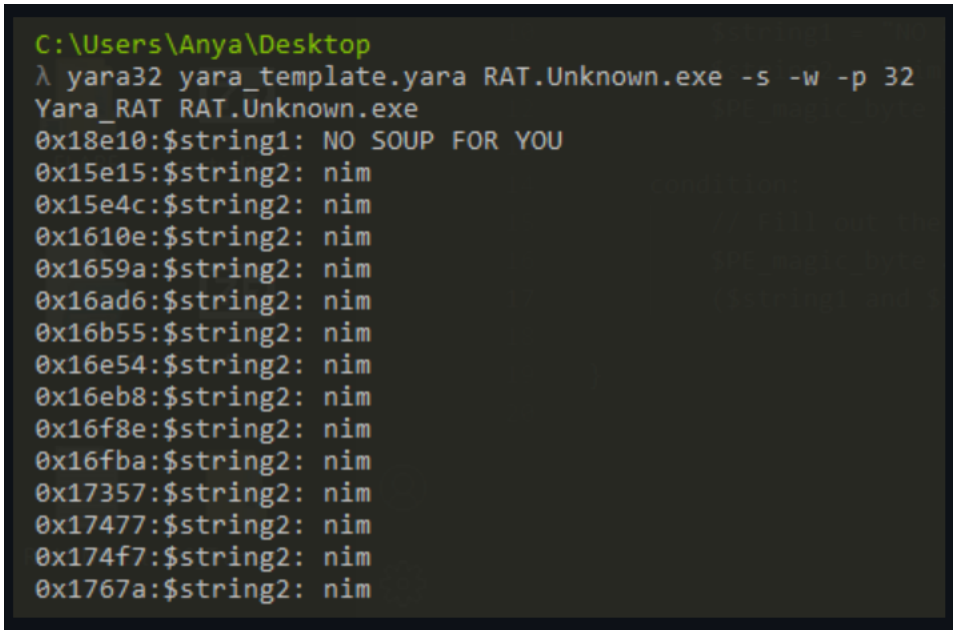
Name	Date modified	Type	Size
desktop.ini	7/21/2022 10:56 PM	Configuration sett...	1 KB
mscordll.exe	7/25/2022 12:07 AM	Application	12 KB

Rules & Signatures

A full set of YARA rules is included in Appendix A.



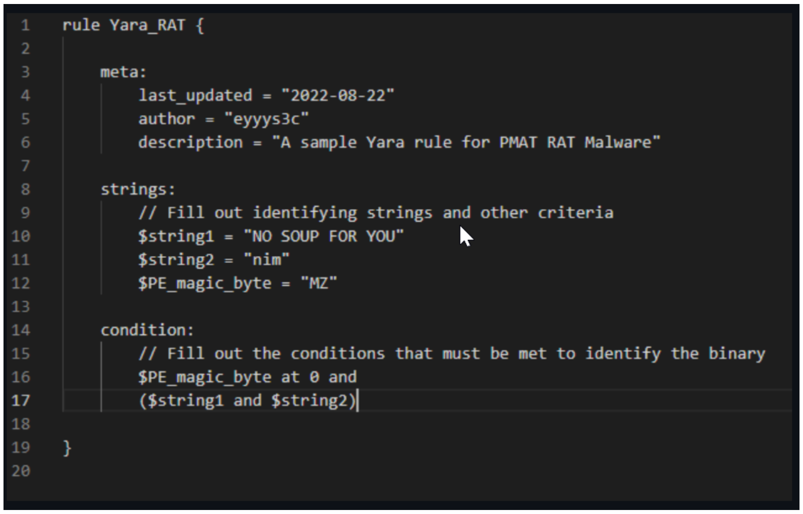
```
rule Yara_RAT {

    meta:
        last_updated = "2022-08-22"
        author = "eyyys3c"
        description = "A sample Yara rule for PMAT RAT Malware"

    strings:
        // Fill out identifying strings and other criteria
        $string1 = "NO SOUP FOR YOU"
        $string2 = "nim"
        $PE_magic_byte = "MZ"

    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_magic_byte at 0 and
        ($string1 and $string2)

}
```



```
C:\Users\Anya\Desktop
λ yara32 yara_template.yara RAT.Unknown.exe -s -w -p 32
Yara_RAT RAT.Unknown.exe
0x18e10:$string1: NO SOUP FOR YOU
0x15e15:$string2: nim
0x15e4c:$string2: nim
0x1610e:$string2: nim
0x1659a:$string2: nim
0x16ad6:$string2: nim
0x16b55:$string2: nim
0x16e54:$string2: nim
0x16eb8:$string2: nim
0x16f8e:$string2: nim
0x16fba:$string2: nim
0x17357:$string2: nim
0x17477:$string2: nim
0x174f7:$string2: nim
0x1767a:$string2: nim
```

Appendices

A. Yara Rules

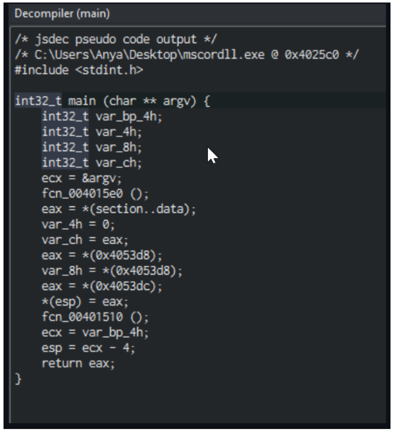


```
rule Yara_RAT {

    meta:
        last_updated = "2022-08-22"
        author = "eyyys3c"
        description = "A sample Yara rule for PMAT RAT Malware"

    strings:
        // Fill out identifying strings and other criteria
        $string1 = "NO SOUP FOR YOU"
        $string2 = "nim"
        $PE_magic_byte = "MZ"

    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_magic_byte at 0 and
        ($string1 and $string2)

}
```

B. Callback URLs

Domain	Port
hxxp://serv1.ec2-102-95-13-2-ubuntu.local/	80

C. Decompiled Code Snippets



```
/* jsdec pseudo code output */
/* C:\Users\Anya\Desktop\mscordll.exe @ 0x4025c0 */
#include <stdint.h>

int32_t main (char ** argv) {
    int32_t var_bp_4h;
    int32_t var_4h;
    int32_t var_8h;
    int32_t var_ch;
    ecx = &argv;
    fcn_004015e0 ();
    eax = *(section..data);
    var_4h = 0;
    var_ch = eax;
    eax = *(0x4053d8);
    var_8h = *(0x4053d8);
    eax = *(0x4053dc);
    *(esp) = eax;
    fcn_00401510 ();
    ecx = var_bp_4h;
    esp = ecx - 4;
    return eax;
}
```