CPSC 458 assignment 2 my work

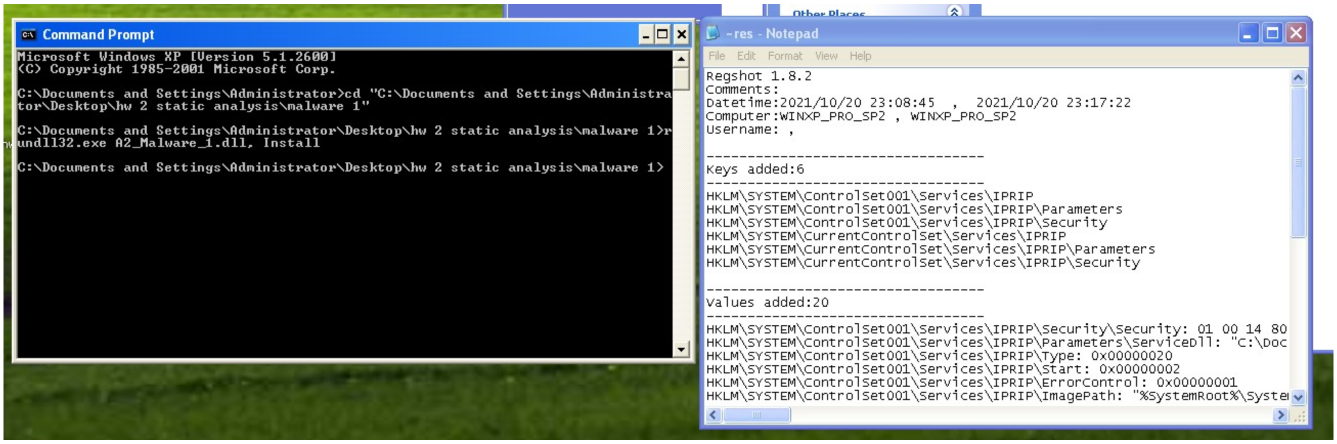
by Carla Jacobsen

Q1: ***For all questions that follow please provide screenshots and descriptions of all your findings. Also, please remember, that we should always do the basic static analysis first when we analyze any malware.***

==

Q2: Analyze the malware found in the file A2_malware_1.dll using basic dynamic analysis tools. ***For all questions that follow please provide screenshots and descriptions of all your findings.***

How can you get this malware to install itself?



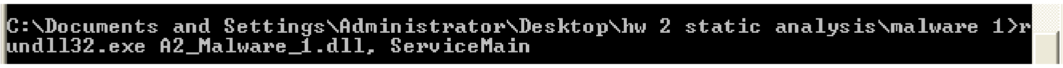
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administra
tor\Desktop\hw 2 static analysis\malware 1"

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, Install

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>
```

```
Regshot 1.8.2
Comments:
Datetime:2021/10/20 23:08:45  ,  2021/10/20 23:17:22
Computer:WINXP_PRO_SP2 , WINXP_PRO_SP2
Username: ,

----------------------------------
Keys added:6
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

----------------------------------
Values added:20
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security: 01 00 14 80
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Doc
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\Syste
```

Rundll32.exe A2_Malware_1.dll, Install

==

Q3: How would you get this malware to run after installation?



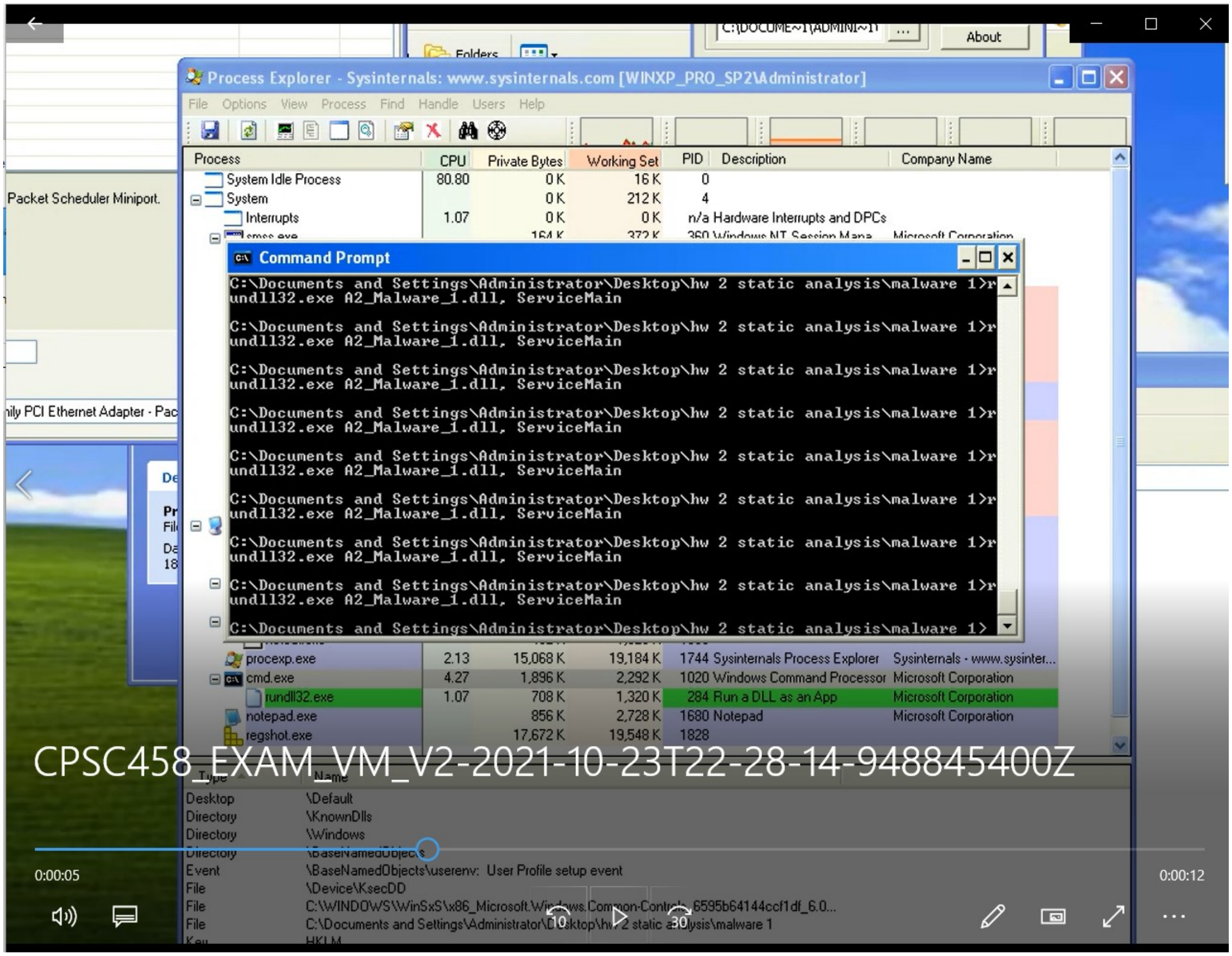
```
C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain
```

Rundll32.exe A2_Malware_1.dll, ServiceMain

More advanced analysis techniques are required to find out what this program truly does.

==

Q4: How can you find the process under which this malware is running?


Process Explorer - Sysinternals: www.sysinternals.com [WINXP_PRO_SP2\Administrator]
File Options View Process Find Handle Users Help
Packet Scheduler Miniport.
ily PCI Ethernet Adapter - Pac
About
Command Prompt
CPSC458_EXAM_VM_V2-2021-10-23T22-28-14-948845400Z
0:00:05
0:00:12

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	80.80	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	1.07	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation
procexp.exe	2.13	15,068 K	19,184 K	1744	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe	4.27	1,896 K	2,292 K	1020	Windows Command Processor	Microsoft Corporation
rundll32.exe	1.07	708 K	1,320 K	284	Run a DLL as an App	Microsoft Corporation
notepad.exe		856 K	2,728 K	1680	Notepad	Microsoft Corporation
regshot.exe		17,672 K	19,548 K	1828		

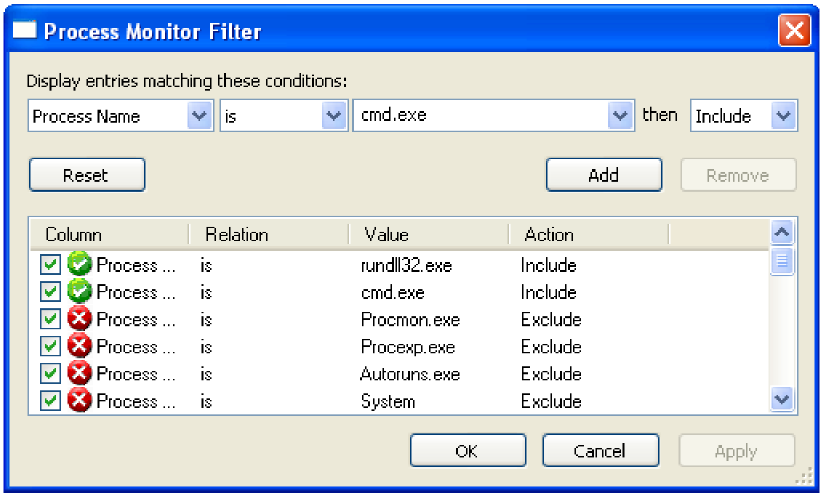
```
C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>
```

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\userenv: User Profile setup event
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1
Key	HKLM

In process explorer look for the rundll32.exe in the command prompt which is being used to run the malware. Use the command rundll32.exe A2_Malware_1.dll, ServiceMain.

===

Q5: Which filters could you set in order to use procmon to glean information?



Display entries matching these conditions:

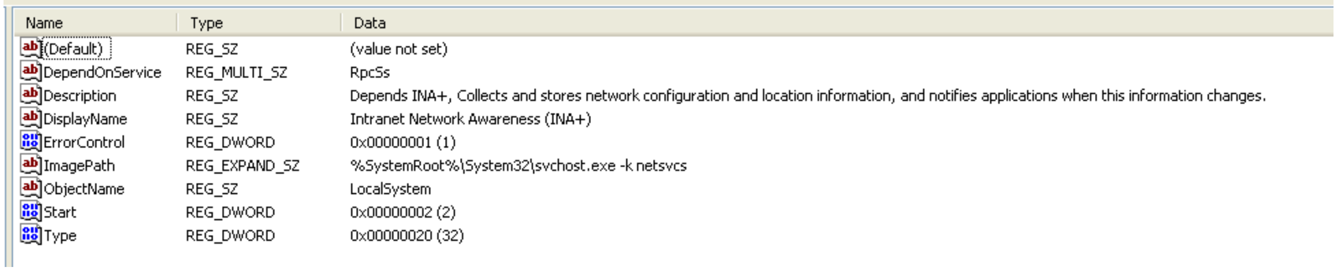
Process Name | is | cmd.exe | then | Include

Column	Relation	Value	Action
☑ ✓ Process ...	is	rundll32.exe	Include
☑ ✓ Process ...	is	cmd.exe	Include
☑ ✗ Process ...	is	Procmon.exe	Exclude
☑ ✗ Process ...	is	Procexp.exe	Exclude
☑ ✗ Process ...	is	Autoruns.exe	Exclude
☑ ✗ Process ...	is	System	Exclude

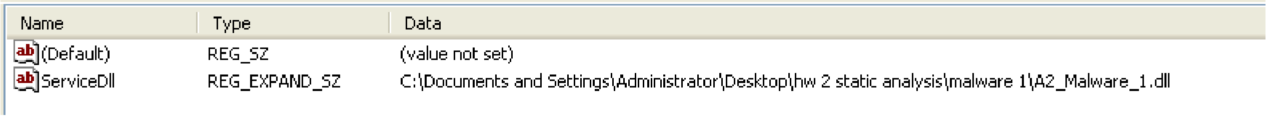
Process name is rundll32.exe and process name is cmd.exe

==

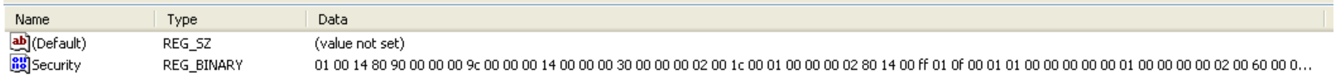
Q6: What are the malware’s host-based indicators?



Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RpcSs
Description	REG_SZ	Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.
DisplayName	REG_SZ	Intranet Network Awareness (INA+)
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k netsvcs
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000020 (32)

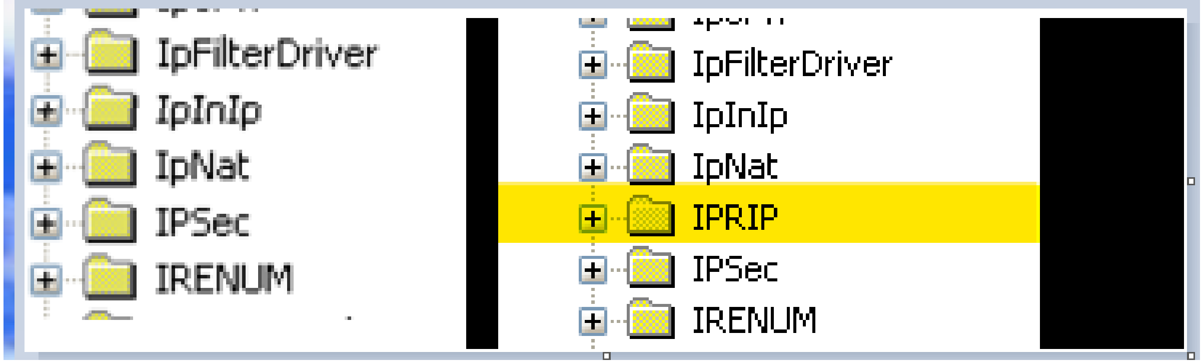


Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1\A2_Malware_1.dll



Name	Type	Data
(Default)	REG_SZ	(value not set)
Security	REG_BINARY	01 00 14 80 90 00 00 00 9c 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 01 00 00 00 02 80 14 00 ff 01 0f 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 0...

Screenshots of the contents of the IPRIP directory



IPRIP is a new directory probably created by the malware through the install function.

- from regshot after running rundll32.exe A2_Malware_1.dll, Install
- HKLM\SYSTEM\ControlSet001\Services\IPRIP
- HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
- HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
- HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
- HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
- HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

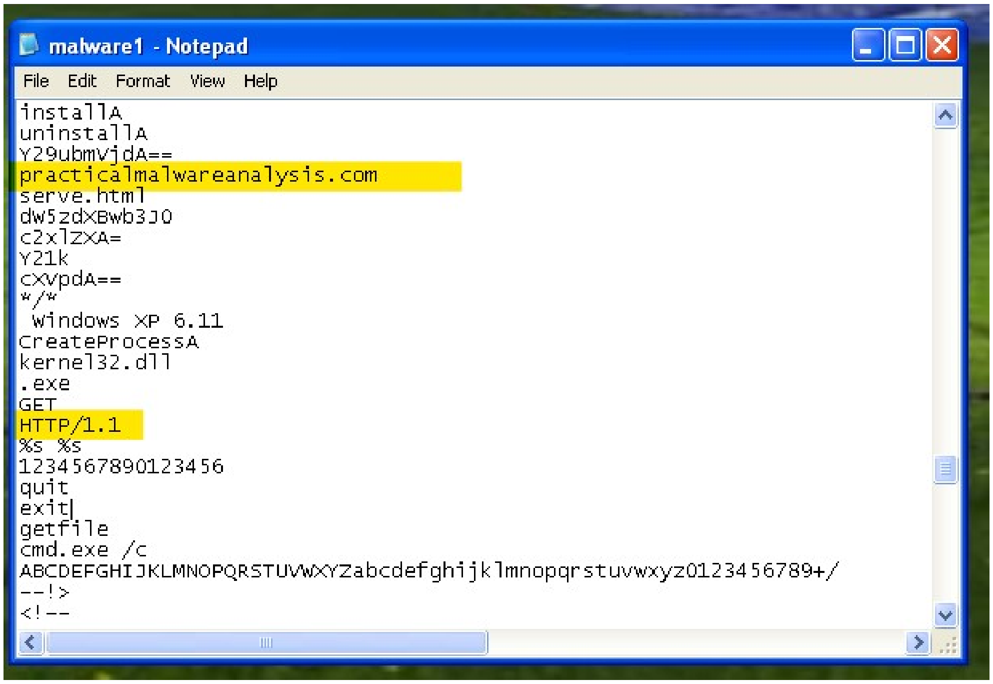
-

===

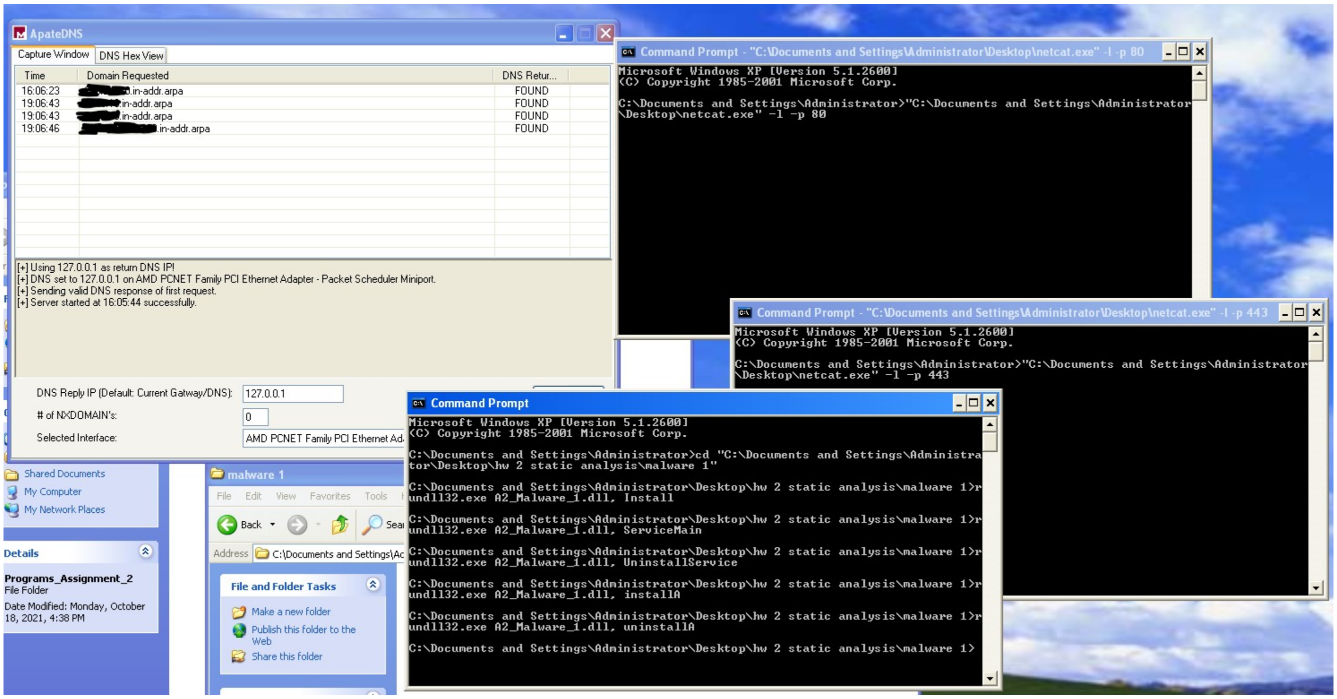
Q7: Are there any useful network-based signatures for this malware?

Network based indicators found through static analysis:

- practicalmalwareanalysis . Com
- HTTP/1.1



```
installA
uninstallA
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
*/*
 Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
```



ApateDNS

Time	Domain Requested	DNS Retur...
16:06:23	[redacted].in-addr.arpa	FOUND
19:06:43	[redacted].in-addr.arpa	FOUND
19:06:43	[redacted].in-addr.arpa	FOUND
19:06:46	[redacted].in-addr.arpa	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 16:05:44 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

# of NXDOMAIN's: 0

Selected Interface: AMD PCNET Family PCI Ethernet Ad

Command Prompt - "C:\Documents and Settings\Administrator\Desktop\netcat.exe" -l -p 80

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator
\Desktop\netcat.exe" -l -p 80
```

Command Prompt - "C:\Documents and Settings\Administrator\Desktop\netcat.exe" -l -p 443

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator
\Desktop\netcat.exe" -l -p 443
```

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administra
tor\Desktop\hw 2 static analysis\malware 1"

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, Install

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, ServiceMain

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, UninstallService

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, installA

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>r
undll32.exe A2_Malware_1.dll, uninstallA

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 1>
```

There were no network based signatures found through dynamic analysis. More advanced analysis techniques are necessary to determine if there is any network activity.

==

==

==

==

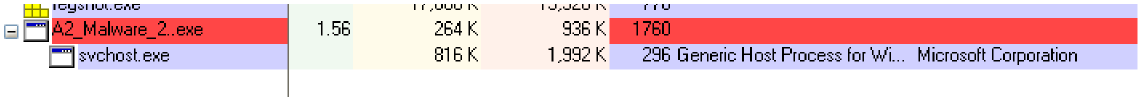
==

==

Q8: Execute the malware found in the file A2_Malware_2.exe while monitoring it using basic dynamic analysis tools in a safe environment.

For all questions that follow please provide supporting screenshots and descriptions. Also, please keep in mind that we should always follow the standard procedure of performing the basic static analysis first.

What do you notice when monitoring this malware with Process Explorer?

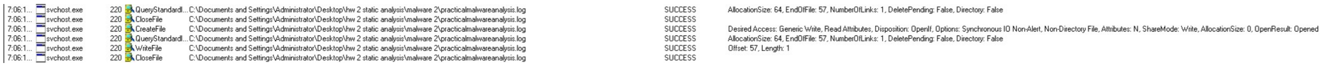


```
  regshot.exe                 17,000 K   13,320 K   770
⊟ A2_Malware_2..exe    1.56      264 K      936 K  1760
    svchost.exe                  816 K    1,992 K   296 Generic Host Process for Wi...  Microsoft Corporation
```

A process named svchost.exe is added.

==

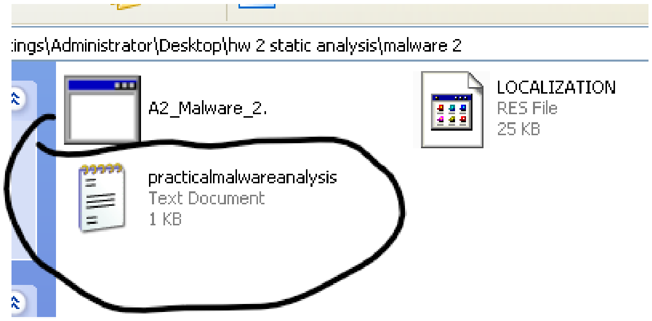
Q9: Can you identify any live memory modifications?

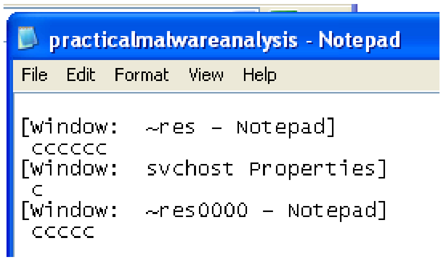


```
7:06:1... svchost.exe  220 QueryStandardI... C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS  AllocationSize: 64, EndOfFile: 57, NumberOfLinks: 1, DeletePending: False, Directory: False
7:06:1... svchost.exe  220 CloseFile         C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS
7:06:1... svchost.exe  220 CreateFile        C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS  Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, OpenResult: Opened
7:06:1... svchost.exe  220 QueryStandardI... C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS  AllocationSize: 64, EndOfFile: 57, NumberOfLinks: 1, DeletePending: False, Directory: False
7:06:1... svchost.exe  220 WriteFile         C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS  Offset: 57, Length: 1
7:06:1... svchost.exe  220 CloseFile         C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 2\practicalmalwareanalysis.log  SUCCESS
```

===

Q10: What are the malware's host-based indicators?

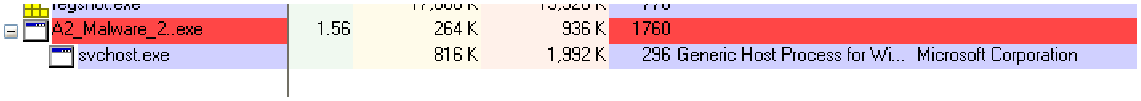




practicalmalwareanalysis - Notepad
File Edit Format View Help

```
[Window:  ~res - Notepad]
 cccccc
[Window:  svchost Properties]
 c
[Window:  ~res0000 - Notepad]
 ccccc
```

The practicalmalwareanalysis text document.

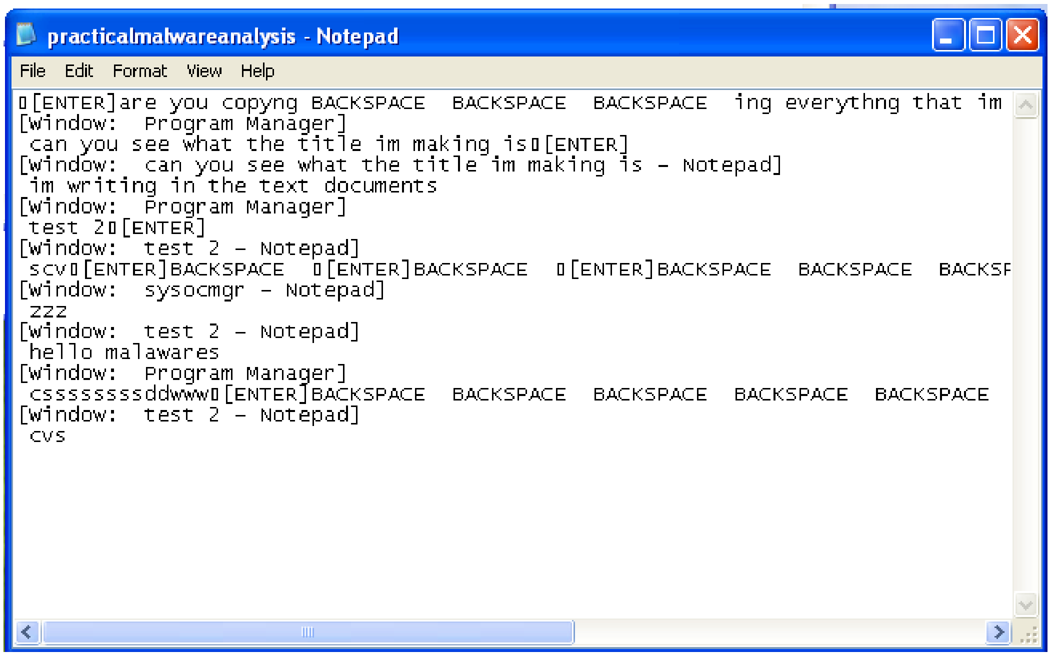


```
regshot.exe
A2_Malware_2..exe   1.56   264 K     936 K   1760
svchost.exe                816 K   1,992 K    296 Generic Host Process for Wi...   Microsoft Corporation
```

The svchost.exe process.

==

Q11: What is the purpose of this program?



practicalmalwareanalysis - Notepad
File Edit Format View Help

```
▯[ENTER]are you copyng BACKSPACE  BACKSPACE  BACKSPACE  ing everythng that im
[Window:  Program Manager]
 can you see what the title im making is▯[ENTER]
[Window:  can you see what the title im making is - Notepad]
 im writing in the text documents
[Window:  Program Manager]
 test 2▯[ENTER]
[Window:  test 2 - Notepad]
 scv▯[ENTER]BACKSPACE  ▯[ENTER]BACKSPACE  ▯[ENTER]BACKSPACE  BACKSPACE  BACKSP
[Window:  sysocmgr - Notepad]
 zzz
[Window:  test 2 - Notepad]
 hello malawares
[Window:  Program Manager]
 cssssssssddwww▯[ENTER]BACKSPACE  BACKSPACE  BACKSPACE  BACKSPACE  BACKSPACE
[Window:  test 2 - Notepad]
 cvs
```

To record keys pressed on the keyboard by the user. It seems to be a keylogger. The keys pressed are listed in the practicalmalwareanalysis text document.

==

==

==

==

==

==

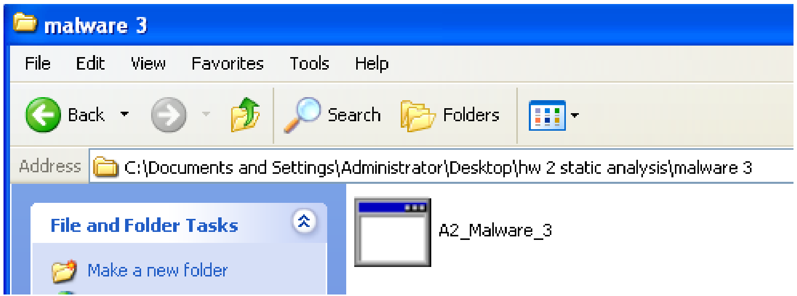
Q12: Analyze the malware found in the file A2_Malware_3.exe using basic dynamic analysis tools.

For all questions that follow please include screenshots and descriptions supporting your answer. Also, please remember to perform the basic static analysis first.

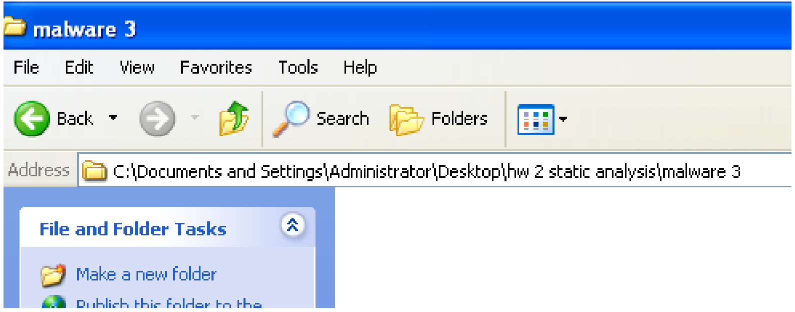
What happens when you run this file?

What is causing the roadblock in dynamic analysis?

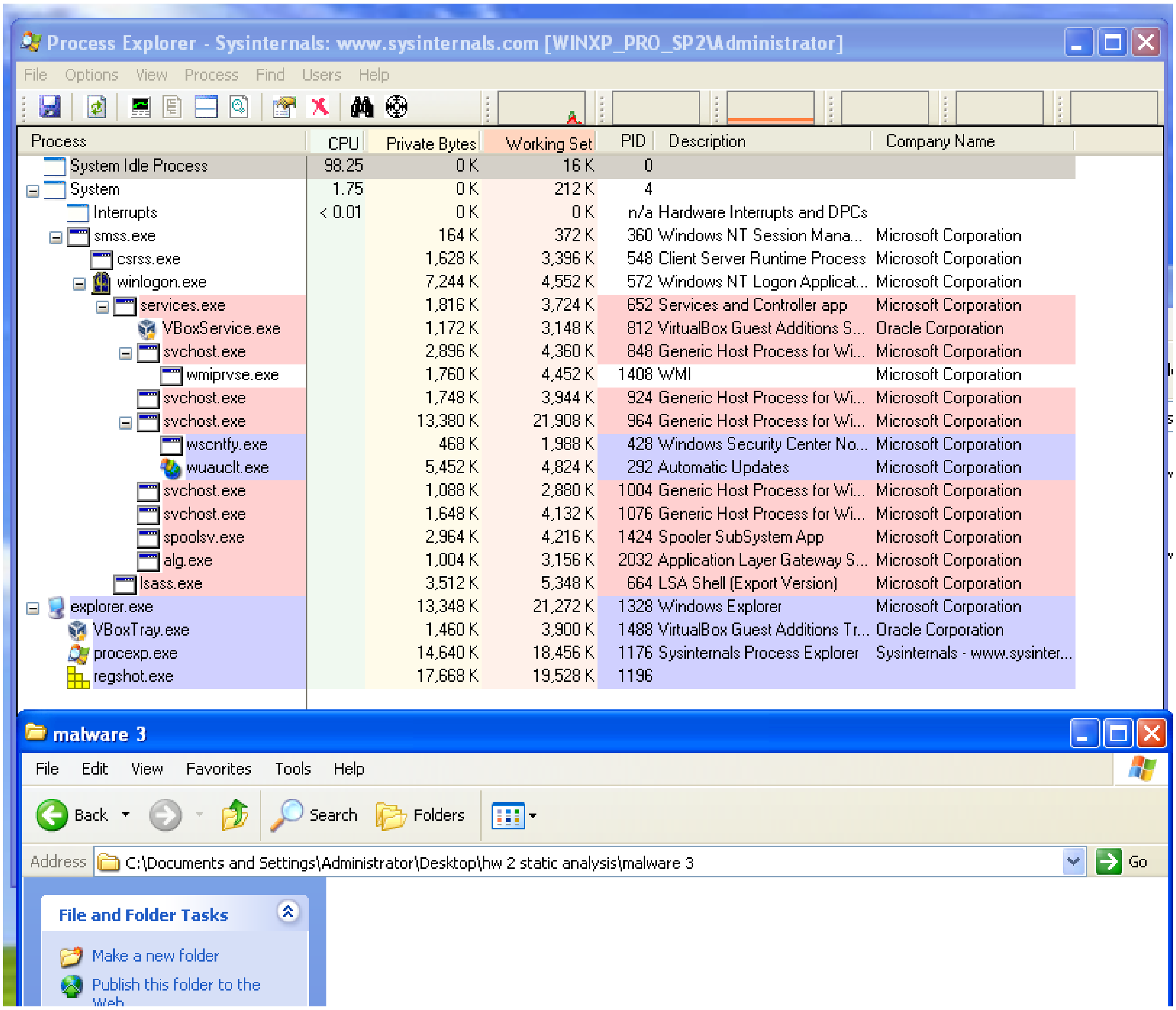
Are there other ways to run this program?



Address C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3



Address C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3

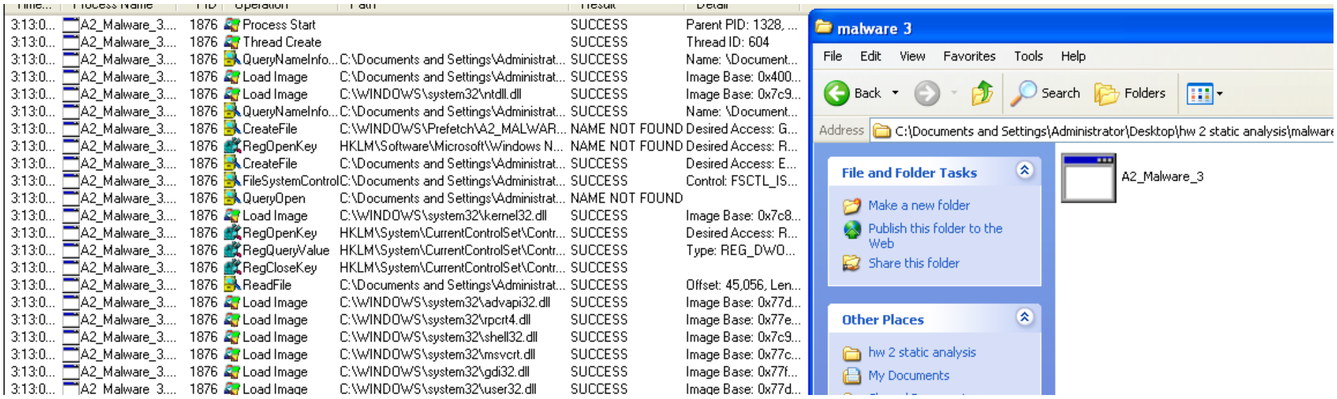


Process Explorer - Sysinternals: www.sysinternals.com [WINXP_PRO_SP2\Administrator]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	98.25	0 K	16 K	0		
System	1.75	0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,628 K	3,396 K	548	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		7,244 K	4,552 K	572	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,816 K	3,724 K	652	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,172 K	3,148 K	812	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,896 K	4,360 K	848	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		1,760 K	4,452 K	1408	WMI	Microsoft Corporation
svchost.exe		1,748 K	3,944 K	924	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,380 K	21,908 K	964	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		468 K	1,988 K	428	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		5,452 K	4,824 K	292	Automatic Updates	Microsoft Corporation
svchost.exe		1,088 K	2,880 K	1004	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,648 K	4,132 K	1076	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2,964 K	4,216 K	1424	Spooler SubSystem App	Microsoft Corporation
alg.exe		1,004 K	3,156 K	2032	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,512 K	5,348 K	664	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		13,348 K	21,272 K	1328	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,460 K	3,900 K	1488	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		14,640 K	18,456 K	1176	Sysinternals Process Explorer	Sysinternals - www.sysinter...
regshot.exe		17,668 K	19,528 K	1196		

Address C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3

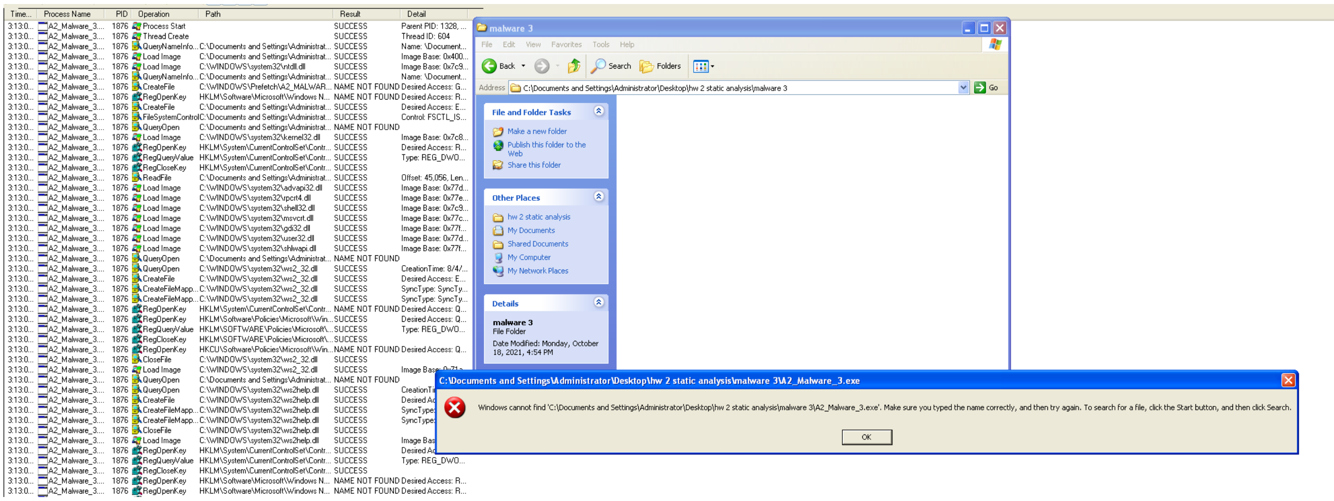
The file seems to disappear when being run while process explorer is open.



```
Time...  Process Name    PID  Operation          Path                                   Result           Detail
3:13:0... A2_Malware_3.... 1876 Process Start                                           SUCCESS          Parent PID: 1328, ...
3:13:0... A2_Malware_3.... 1876 Thread Create                                           SUCCESS          Thread ID: 604
3:13:0... A2_Malware_3.... 1876 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS          Name: \Document...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\Documents and Settings\Administrat... SUCCESS          Image Base: 0x400...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\ntdll.dll          SUCCESS          Image Base: 0x7c9...
3:13:0... A2_Malware_3.... 1876 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS          Name: \Document...
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\WINDOWS\Prefetch\A2_MALWAR...        NAME NOT FOUND Desired Access: G...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\Software\Microsoft\Windows N...    NAME NOT FOUND Desired Access: R...
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\Documents and Settings\Administrat... SUCCESS          Desired Access: E...
3:13:0... A2_Malware_3.... 1876 FileSystemControlC:\Documents and Settings\Administrat... SUCCESS          Control: FSCTL_IS...
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\Documents and Settings\Administrat... NAME NOT FOUND
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\kernel32.dll       SUCCESS          Image Base: 0x7c8...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\System\CurrentControlSet\Contr...  SUCCESS          Desired Access: R...
3:13:0... A2_Malware_3.... 1876 RegQueryValue    HKLM\System\CurrentControlSet\Contr...  SUCCESS          Type: REG_DWO...
3:13:0... A2_Malware_3.... 1876 RegCloseKey      HKLM\System\CurrentControlSet\Contr...  SUCCESS
3:13:0... A2_Malware_3.... 1876 ReadFile         C:\Documents and Settings\Administrat... SUCCESS          Offset: 45,056, Len...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\advapi32.dll       SUCCESS          Image Base: 0x77d...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\rpcrt4.dll         SUCCESS          Image Base: 0x77e...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\shell32.dll        SUCCESS          Image Base: 0x7c9...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\msvcrt.dll         SUCCESS          Image Base: 0x77c...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\gdi32.dll          SUCCESS          Image Base: 0x77f...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\user32.dll         SUCCESS          Image Base: 0x77d...
```

Address C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware

The file does not seem to disappear when being run while procmon is open.



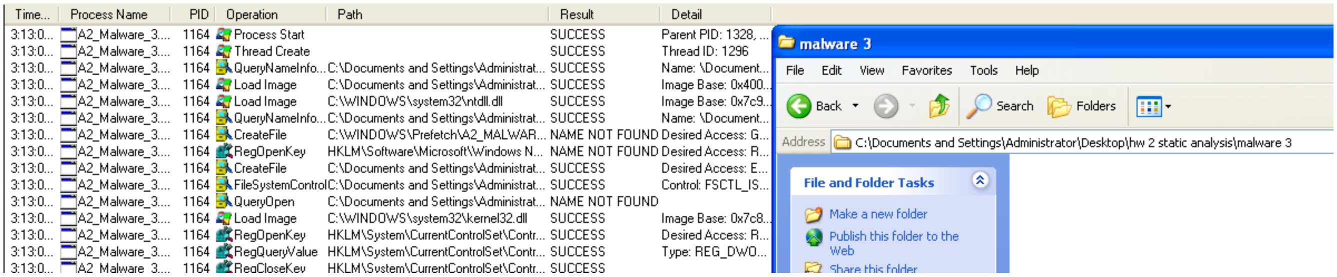
```
Time...   Process Name    PID  Operation         Path                                      Result          Detail
3:13:0... A2_Malware_3.... 1876 Process Start                                               SUCCESS         Parent PID: 1328, ...
3:13:0... A2_Malware_3.... 1876 Thread Create                                               SUCCESS         Thread ID: 604
3:13:0... A2_Malware_3.... 1876 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS         Name: \Document...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\Documents and Settings\Administrat... SUCCESS         Image Base: 0x400...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\ntdll.dll            SUCCESS         Image Base: 0x7c9...
3:13:0... A2_Malware_3.... 1876 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS         Name: \Document...
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\WINDOWS\Prefetch\A2_MALWAR...         NAME NOT FOUND  Desired Access: G...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\Software\Microsoft\Windows N...     NAME NOT FOUND  Desired Access: R...
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\Documents and Settings\Administrat... SUCCESS         Desired Access: E...
3:13:0... A2_Malware_3.... 1876 FileSystemControlC:\Documents and Settings\Administrat... SUCCESS         Control: FSCTL_IS...
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\Documents and Settings\Administrat... NAME NOT FOUND
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\kernel32.dll         SUCCESS         Image Base: 0x7c8...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\System\CurrentControlSet\Contr...   SUCCESS         Desired Access: R...
3:13:0... A2_Malware_3.... 1876 RegQueryValue    HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_DWO...
3:13:0... A2_Malware_3.... 1876 RegCloseKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS
3:13:0... A2_Malware_3.... 1876 ReadFile         C:\Documents and Settings\Administrat... SUCCESS         Offset: 45,056, Len...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\advapi32.dll         SUCCESS         Image Base: 0x77d...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\rpcrt4.dll           SUCCESS         Image Base: 0x77e...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\shell32.dll          SUCCESS         Image Base: 0x7c9...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\msvcrt.dll           SUCCESS         Image Base: 0x77c...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\gdi32.dll            SUCCESS         Image Base: 0x77f...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\user32.dll           SUCCESS         Image Base: 0x77d...
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\shlwapi.dll          SUCCESS         Image Base: 0x77f...
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\Documents and Settings\Administrat... NAME NOT FOUND
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\WINDOWS\system32\ws2_32.dll           SUCCESS         CreationTime: 8/4/...
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\WINDOWS\system32\ws2_32.dll           SUCCESS         Desired Access: E...
3:13:0... A2_Malware_3.... 1876 CreateFileMapp... C:\WINDOWS\system32\ws2_32.dll          SUCCESS         SyncType: SyncTy...
3:13:0... A2_Malware_3.... 1876 CreateFileMapp... C:\WINDOWS\system32\ws2_32.dll          SUCCESS         SyncType: SyncTy...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND  Desired Access: Q...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\Software\Policies\Microsoft\Win...  SUCCESS         Desired Access: Q...
3:13:0... A2_Malware_3.... 1876 RegQueryValue    HKLM\SOFTWARE\Policies\Microsoft\...     SUCCESS         Type: REG_DWO...
3:13:0... A2_Malware_3.... 1876 RegCloseKey      HKLM\SOFTWARE\Policies\Microsoft\...     SUCCESS
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKCU\Software\Policies\Microsoft\Win...  NAME NOT FOUND  Desired Access: Q...
3:13:0... A2_Malware_3.... 1876 CloseFile        C:\WINDOWS\system32\ws2_32.dll           SUCCESS
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\ws2_32.dll           SUCCESS         Image Base: 0x71a
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\Documents and Settings\Administrat... NAME NOT FOUND
3:13:0... A2_Malware_3.... 1876 QueryOpen        C:\WINDOWS\system32\ws2help.dll          SUCCESS         CreationTi
3:13:0... A2_Malware_3.... 1876 CreateFile       C:\WINDOWS\system32\ws2help.dll          SUCCESS         Desired Ac
3:13:0... A2_Malware_3.... 1876 CreateFileMapp... C:\WINDOWS\system32\ws2help.dll         SUCCESS         SyncType
3:13:0... A2_Malware_3.... 1876 CreateFileMapp... C:\WINDOWS\system32\ws2help.dll         SUCCESS         SyncType
3:13:0... A2_Malware_3.... 1876 CloseFile        C:\WINDOWS\system32\ws2help.dll          SUCCESS
3:13:0... A2_Malware_3.... 1876 Load Image       C:\WINDOWS\system32\ws2help.dll          SUCCESS         Image Bas
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\System\CurrentControlSet\Contr...   SUCCESS         Desired Ac
3:13:0... A2_Malware_3.... 1876 RegQueryValue    HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_DWO...
3:13:0... A2_Malware_3.... 1876 RegCloseKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\Software\Microsoft\Windows N...     NAME NOT FOUND  Desired Access: R...
3:13:0... A2_Malware_3.... 1876 RegOpenKey       HKLM\Software\Microsoft\Windows N...     NAME NOT FOUND  Desired Access: R...
```

malware 3
File Folder
Date Modified: Monday, October 18, 2021, 4:54 PM

C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3\A2_Malware_3.exe

Windows cannot find 'C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3\A2_Malware_3.exe'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.

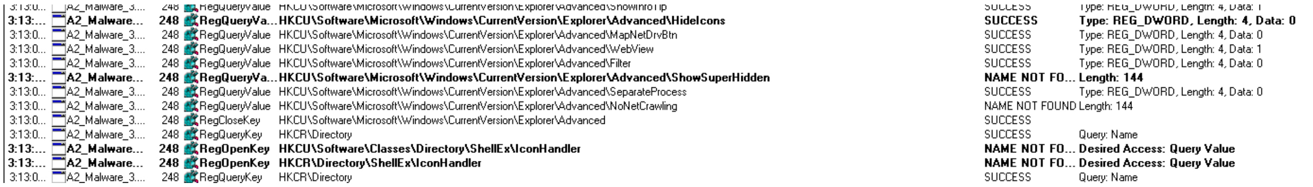
After being ran enough times the program appears to disappear while procmon is open.



```
Time...   Process Name    PID  Operation         Path                                      Result          Detail
3:13:0... A2_Malware_3.... 1164 Process Start                                               SUCCESS         Parent PID: 1328, ...
3:13:0... A2_Malware_3.... 1164 Thread Create                                               SUCCESS         Thread ID: 1296
3:13:0... A2_Malware_3.... 1164 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS         Name: \Document...
3:13:0... A2_Malware_3.... 1164 Load Image       C:\Documents and Settings\Administrat... SUCCESS         Image Base: 0x400...
3:13:0... A2_Malware_3.... 1164 Load Image       C:\WINDOWS\system32\ntdll.dll            SUCCESS         Image Base: 0x7c9...
3:13:0... A2_Malware_3.... 1164 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS         Name: \Document...
3:13:0... A2_Malware_3.... 1164 CreateFile       C:\WINDOWS\Prefetch\A2_MALWAR...         NAME NOT FOUND  Desired Access: G...
3:13:0... A2_Malware_3.... 1164 RegOpenKey       HKLM\Software\Microsoft\Windows N...     NAME NOT FOUND  Desired Access: R...
3:13:0... A2_Malware_3.... 1164 CreateFile       C:\Documents and Settings\Administrat... SUCCESS         Desired Access: E...
3:13:0... A2_Malware_3.... 1164 FileSystemControlC:\Documents and Settings\Administrat... SUCCESS         Control: FSCTL_IS...
3:13:0... A2_Malware_3.... 1164 QueryOpen        C:\Documents and Settings\Administrat... NAME NOT FOUND
3:13:0... A2_Malware_3.... 1164 Load Image       C:\WINDOWS\system32\kernel32.dll         SUCCESS         Image Base: 0x7c8...
3:13:0... A2_Malware_3.... 1164 RegOpenKey       HKLM\System\CurrentControlSet\Contr...   SUCCESS         Desired Access: R...
3:13:0... A2_Malware_3.... 1164 RegQueryValue    HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_DWO...
3:13:0... A2_Malware_3.... 1164 RegCloseKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS
```

malware 3
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder

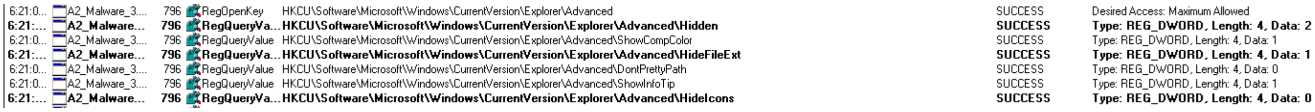
Sometimes when the snapshot is reloaded the program appears to disappear the first time it is ran with procmon running.



```
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip        SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
3:13:... A2_Malware...      248 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons          SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn       SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView            SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter             SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
3:13:... A2_Malware...      248 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden    NAME NOT FO...  Length: 144
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess    SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
3:13:0... A2_Malware_3....  248 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling      NAME NOT FOUND  Length: 144
3:13:0... A2_Malware_3....  248 RegCloseKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced                    SUCCESS
3:13:0... A2_Malware_3....  248 RegQueryKey    HKCR\Directory                                                                       SUCCESS         Query: Name
3:13:... A2_Malware...      248 RegOpenKey     HKCU\Software\Classes\Directory\ShellEx\IconHandler                                  NAME NOT FO...  Desired Access: Query Value
3:13:... A2_Malware...      248 RegOpenKey     HKCR\Directory\ShellEx\IconHandler                                                   NAME NOT FO...  Desired Access: Query Value
3:13:0... A2_Malware_3....  248 RegQueryKey    HKCR\Directory                                                                       SUCCESS         Query: Name
```

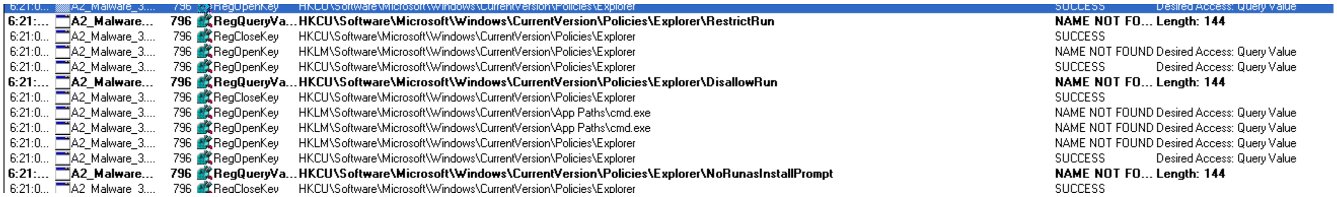
3:13:03.5988810 PM A2_Malware_3.exe 248 RegQueryValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons SUCCESS Type: REG_DWORD, Length: 4, Data: 0

It is possible that the malware is using this directory to hide itself



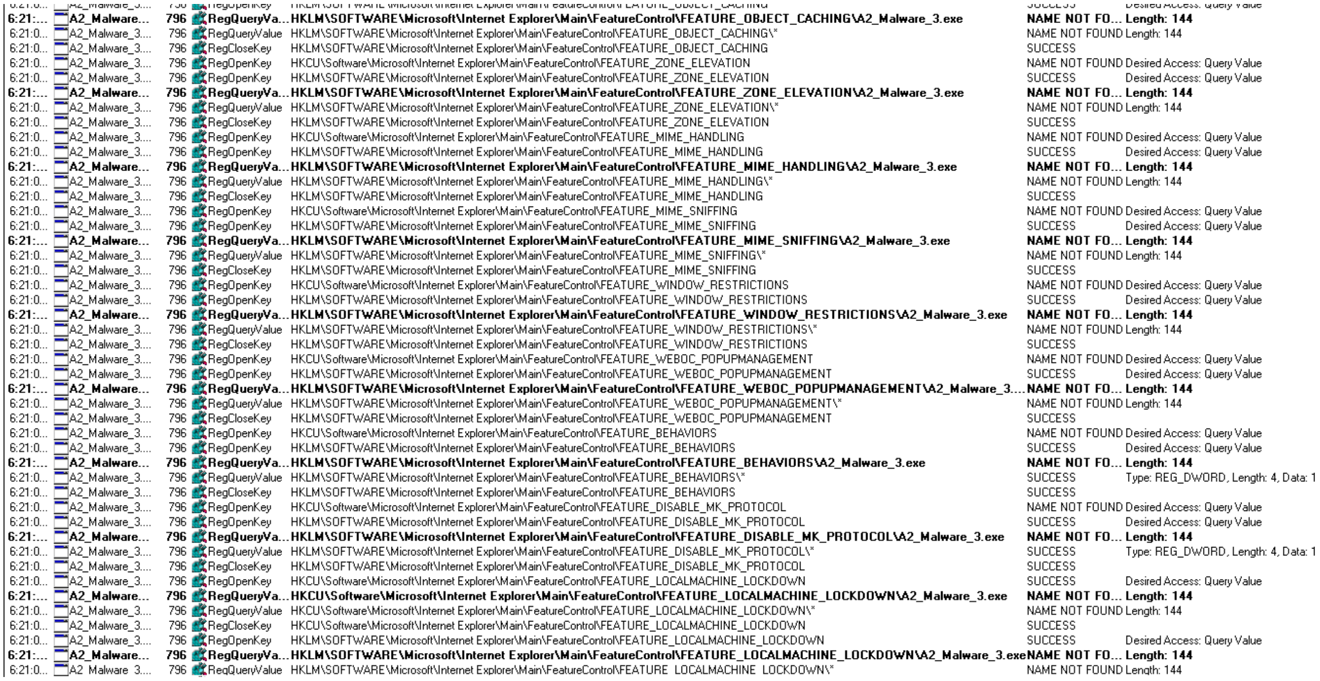
```
6:21:0... A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced                SUCCESS  Desired Access: Maximum Allowed
6:21:... A2_Malware...      796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden         SUCCESS  Type: REG_DWORD, Length: 4, Data: 2
6:21:0... A2_Malware_3....  796 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor  SUCCESS  Type: REG_DWORD, Length: 4, Data: 1
6:21:... A2_Malware...      796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt    SUCCESS  Type: REG_DWORD, Length: 4, Data: 1
6:21:0... A2_Malware_3....  796 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath SUCCESS  Type: REG_DWORD, Length: 4, Data: 0
6:21:0... A2_Malware_3....  796 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip    SUCCESS  Type: REG_DWORD, Length: 4, Data: 1
6:21:... A2_Malware...      796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons      SUCCESS  Type: REG_DWORD, Length: 4, Data: 0
```

More indicators of possible file hiding



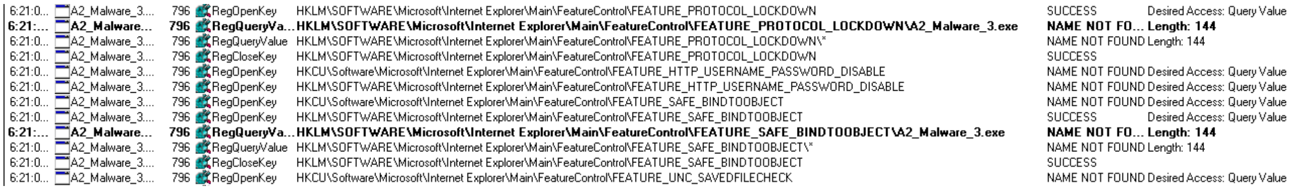
```
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun                    NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun                    NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\cmd.exe                                NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\cmd.exe                                NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRunasInstallPrompt           NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer                                SUCCESS
```

RestrictRun, might be preventing itself from being run



```
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                                SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\A2_Malware_3.exe              NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\*                             NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                                SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                                NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                                SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\A2_Malware_3.exe              NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\*                             NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                                SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                 NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                 SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\A2_Malware_3.exe               NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\*                              NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                 SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                 NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                 SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\A2_Malware_3.exe               NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\*                              NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                 SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                           NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                           SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\A2_Malware_3.exe         NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\*                        NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                           SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                         NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                         SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\A2_Malware_3....       NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\*                      NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                         SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                     NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                     SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\A2_Malware_3.exe                   NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\*                                  SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                     SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                           NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                           SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\A2_Malware_3.exe         NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\*                        SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                           SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                         SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malware_3.exe       NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                      NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                         SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                         SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malware_3.exeNAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                      NAME NOT FOUND   Length: 144
```

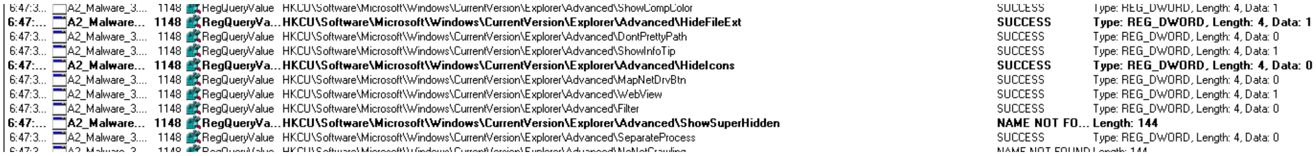
the malware seems to be performing these actions upon itself maybe this hides it?



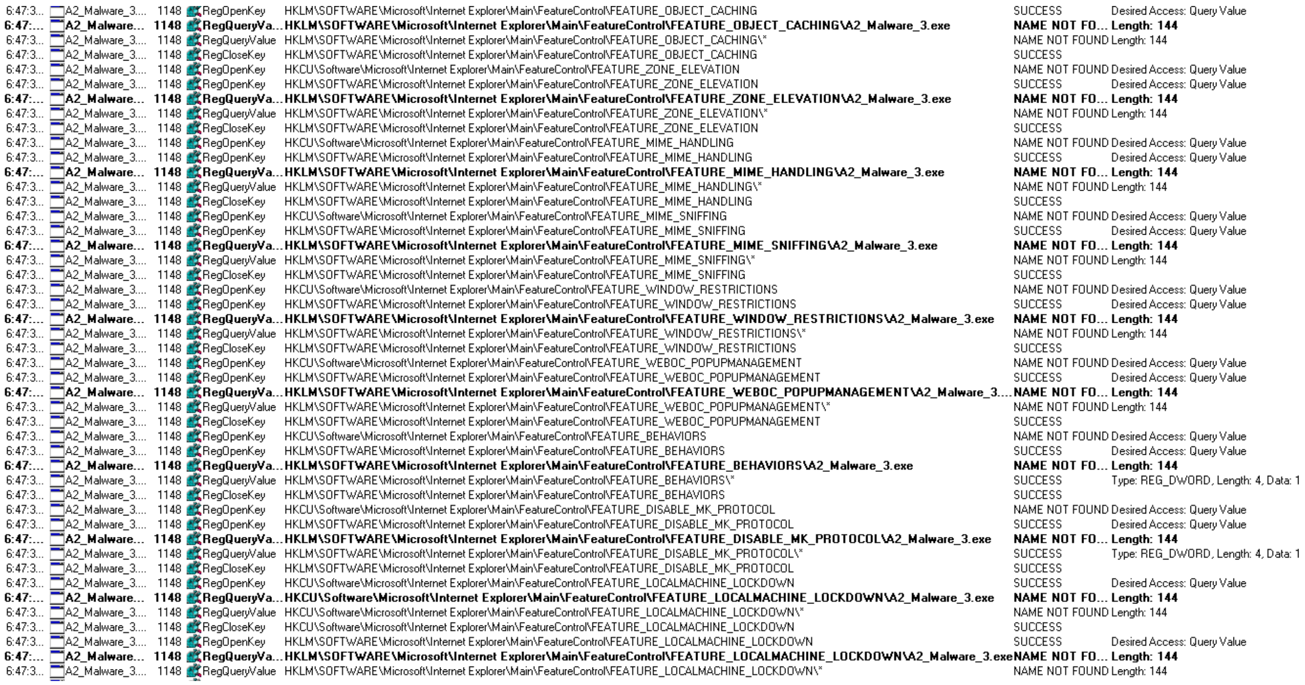
```
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN                       SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\A2_Malware_3.exe     NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\*                    NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN                       SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE          NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE          NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                       NAME NOT FOUND   Desired Access: Query Value
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                       SUCCESS          Desired Access: Query Value
6:21:...   A2_Malware...     796 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT\A2_Malware_3.exe     NAME NOT FO...   Length: 144
6:21:0...  A2_Malware_3....  796 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT\*                    NAME NOT FOUND   Length: 144
6:21:0...  A2_Malware_3....  796 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                       SUCCESS
6:21:0...  A2_Malware_3....  796 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_UNC_SAVEDFILECHECK                      NAME NOT FOUND   Desired Access: Query Value
```

More actions upon itself

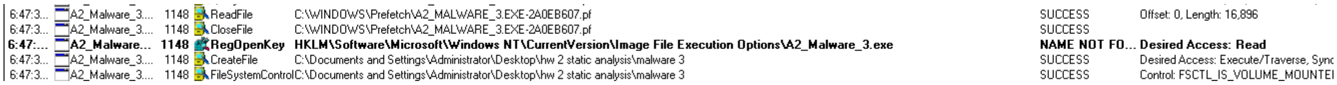
after the malware appears to have successfully hidden itself



```
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor        SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:...   A2_Malware...     1148 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt          SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath       SUCCESS          Type: REG_DWORD, Length: 4, Data: 0
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip          SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:...   A2_Malware...     1148 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons            SUCCESS          Type: REG_DWORD, Length: 4, Data: 0
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn         SUCCESS          Type: REG_DWORD, Length: 4, Data: 0
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView              SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter               SUCCESS          Type: REG_DWORD, Length: 4, Data: 0
6:47:...   A2_Malware...     1148 RegQueryVa...  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden      NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess      SUCCESS          Type: REG_DWORD, Length: 4, Data: 0
6:47:3...  A2_Malware_3....  1148 RegQueryValue  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling        NAME NOT FOUND   Length: 144
```



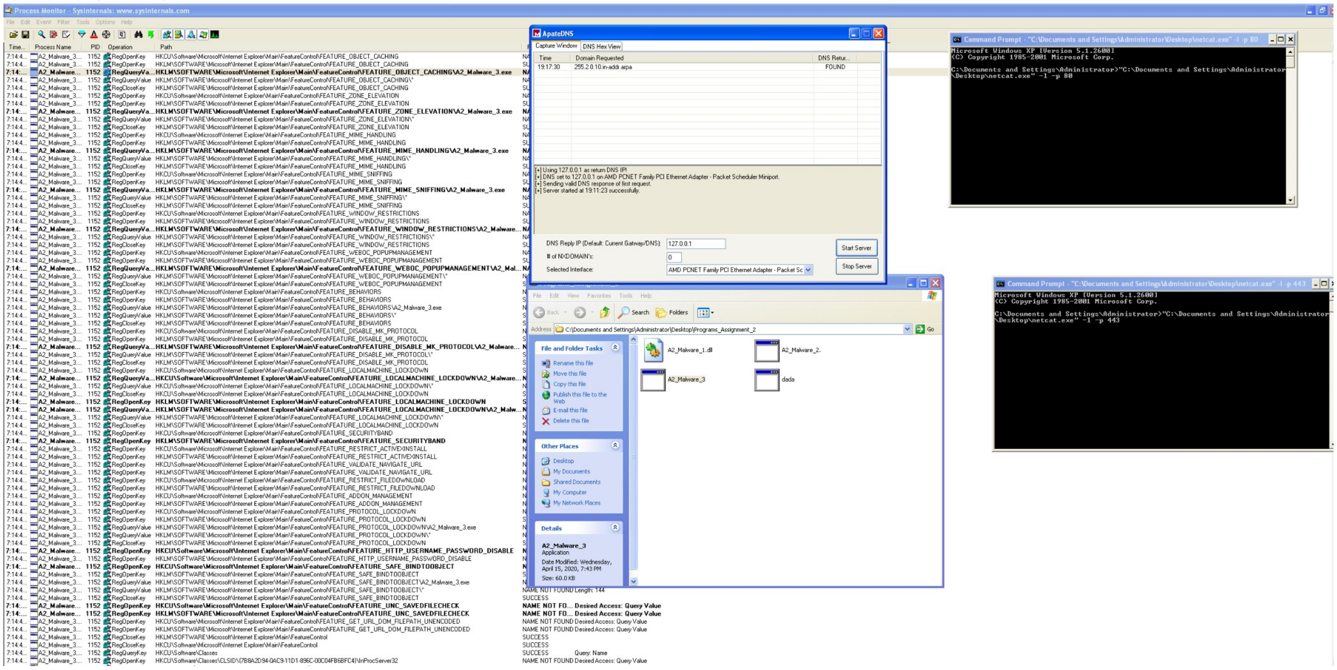
```
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                              SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\A2_Malware_3.exe             NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\*                            NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                              SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\A2_Malware_3.exe             NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\*                            NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\A2_Malware_3.exe               NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\*                              NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                                SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\A2_Malware_3.exe               NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\*                              NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                                SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                          NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                          SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\A2_Malware_3.exe         NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\*                        NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                          SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                        NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                        SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\A2_Malware_3....    NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\*                      NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                        SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                    NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                    SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\A2_Malware_3.exe                   NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\*                                  SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                    SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                          NAME NOT FOUND   Desired Access: Query Value
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                          SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\A2_Malware_3.exe         NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\*                        SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                          SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                        SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malware_3.exe       NAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                      NAME NOT FOUND   Length: 144
6:47:3...  A2_Malware_3....  1148  RegCloseKey    HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                        SUCCESS
6:47:3...  A2_Malware_3....  1148  RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                        SUCCESS          Desired Access: Query Value
6:47:...   A2_Malware...     1148  RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malware_3.exeNAME NOT FO...   Length: 144
6:47:3...  A2_Malware_3....  1148  RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                      NAME NOT FOUND   Length: 144
```



```
6:47:3...  A2_Malware_3....  1148  ReadFile           C:\WINDOWS\Prefetch\A2_MALWARE_3.EXE-2A0EB607.pf                                                          SUCCESS          Offset: 0, Length: 16,896
6:47:3...  A2_Malware_3....  1148  CloseFile          C:\WINDOWS\Prefetch\A2_MALWARE_3.EXE-2A0EB607.pf                                                          SUCCESS
6:47:...   A2_Malware...     1148  RegOpenKey         HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\A2_Malware_3.exe           NAME NOT FO...   Desired Access: Read
6:47:3...  A2_Malware_3....  1148  CreateFile         C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3                            SUCCESS          Desired Access: Execute/Traverse, Sync
6:47:3...  A2_Malware_3....  1148  FileSystemControlC:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3                            SUCCESS          Control: FSCTL_IS_VOLUME_MOUNTEI
```

The procmon outputs seem very similar to how they were when the malware was not hidden

there appears to be no network activity despite some network based indicators being found in the procmon



Process Monitor - Sysinternals: www.sysinternals.com

```
Time...  Process Name     PID   Operation      Path
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                              NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                              SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\A2_Malware_3.exe        NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING\*                            NA
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING                              SU
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\A2_Malware_3.exe        NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION\*                            NA
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION                              SU
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                               NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                               SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\A2_Malware_3.exe         NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\*                             NA
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING                               SU
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                               NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                               SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\A2_Malware_3.exe         NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\*                             NA
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING                               SU
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                         NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                         SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\A2_Malware...        NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS\*                       NA
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS                         SU
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                       NA
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                       SU
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\A2_Mal...        NA
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT\*                     N
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT                       S
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                   N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                   S
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\A2_Malware_3.exe             N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS\*                                 S
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS                                   S
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                         N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                         S
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\A2_Malware...        N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL\*                       S
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL                         S
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                       S
7:14:...  A2_Malware...    1152 RegQueryVa...  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malware...      N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                     N
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                       S
7:14:...  A2_Malware...    1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                       S
7:14:...  A2_Malware...    1152 RegQueryVa...  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\A2_Malw...        N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\*                     N
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN                       S
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SECURITYBAND                                N
7:14:...  A2_Malware...    1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SECURITYBAND                                N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL                     N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL                     N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_VALIDATE_NAVIGATE_URL                       N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_VALIDATE_NAVIGATE_URL                       N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD                       N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD                       N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT                            N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT                            N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN                           N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN                           S
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\A2_Malware_3.exe     N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN\*                         N
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN                           S
7:14:...  A2_Malware...    1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE              N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE              N
7:14:...  A2_Malware...    1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                           N
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                           S
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT\A2_Malware_3.exe     N
7:14:4... A2_Malware_3.... 1152 RegQueryValue  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT\*                         NAME NOT FOUND Length: 144
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT                           SUCCESS
7:14:...  A2_Malware...    1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_UNC_SAVEDFILECHECK                          NAME NOT FO... Desired Access: Query Value
7:14:...  A2_Malware...    1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_UNC_SAVEDFILECHECK                          NAME NOT FO... Desired Access: Query Value
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_GET_URL_DOM_FILEPATH_UNENCODED              NAME NOT FOUND Desired Access: Query Value
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_GET_URL_DOM_FILEPATH_UNENCODED              NAME NOT FOUND Desired Access: Query Value
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl                                                     SUCCESS
7:14:4... A2_Malware_3.... 1152 RegCloseKey    HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl                                                     SUCCESS
7:14:4... A2_Malware_3.... 1152 RegQueryKey    HKCU\Software\Classes                                                                                             SUCCESS        Query: Name
7:14:4... A2_Malware_3.... 1152 RegOpenKey     HKCU\Software\Classes\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\InProcServer32                                NAME NOT FOUND Desired Access: Query Value
```

ApateDNS

Time	Domain Requested	DNS Retur...
19:17:30	255.2.0.10.in-addr.arpa	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 19:11:23 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

# of NXDOMAIN's: 0

Selected Interface: AMD PCNET Family PCI Ethernet Adapter - Packet Sc

Command Prompt - "C:\Documents and Settings\Administrator\Desktop\netcat.exe" -l -p 80

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator
\Desktop\netcat.exe" -l -p 80
```

Command Prompt - "C:\Documents and Settings\Administrator\Desktop\netcat.exe" -l -p 443

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator
\Desktop\netcat.exe" -l -p 443
```

Address: C:\Documents and Settings\Administrator\Desktop\Programs_Assignment_2

A2_Malware_3
Application
Date Modified: Wednesday, April 15, 2020, 7:43 PM
Size: 60.0 KB

There seems to be attempts to access file paths associated with internet explorer however no network activity was detected in the apate and netcat

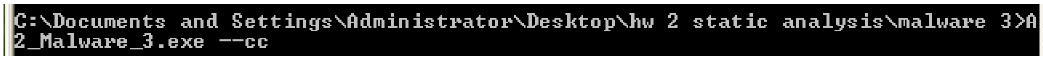
Perhaps the malware knows that apate and netcat are running and thus hides its network behaviors

The malware also seems to hide itself when process explorer is running but does not do so as often if procmon is the software running

Perhaps the malware changes its behaviors based on certain softwares being present

This makes the analysis difficult because it can be hard to determine what the true purpose of this malware is

more advanced analysis techniques are needed to determine the true nature of this malware



```
C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3>A
2_Malware_3.exe --cc
```

ran using the argument --cc

Regshot 1.8.2
Comments:
Datetime:2021/10/29 23:41:21 , 2021/10/29 23:41:38
Computer:WINXP_PRO_SP2 , WINXP_PRO_SP2
Username: ,

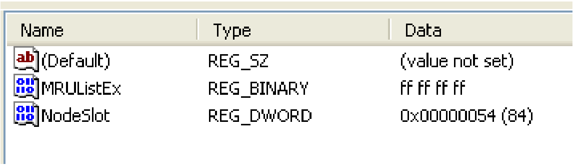
Keys added:3

```
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\21
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell

----------------------------------
Values added:27
----------------------------------
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\21: 40 00 31 00 00 00 00 00 5D 53 D8 BC 10 00 42 41 43 4B 55 50 7E 31 00 00 28 00 03 00
04 00 EF BE 5D 53 D8 BC 5D 53 D8 BC 14 00 00 00 62 00 61 00 63 00 6B 00 75 00 70 00 20 00 31
00 00 00 18 00 00 00
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\21\NodeSlot: 0x00000054
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\21\MRUListEx: FF FF FF FF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\MinPos2560x1320(1).x: 0xFFFF8300
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\MinPos2560x1320(1).y: 0xFFFF8300
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\MaxPos2560x1320(1).x: 0xFFFFFFFF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\MaxPos2560x1320(1).y: 0xFFFFFFFF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\WinPos2560x1320(1).left: 0x0000006E
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\WinPos2560x1320(1).top: 0x00000091
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\WinPos2560x1320(1).right: 0x0000038E
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\WinPos2560x1320(1).bottom: 0x000002E9
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Rev: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\WFlags: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\ShowCmd: 0x00000001
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\FFlags: 0x00000001
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\HotKey: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Buttons: 0xFFFFFFFF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Links: 0x00000000
```

```
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Address: 0xFFFFFFFF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Mode: 0x00000006
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\ScrollPos2560x1320(1).x: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\ScrollPos2560x1320(1).y: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Sort: 0x00000000
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\SortDir: 0x00000001
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\Col: 0xFFFFFFFF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
Bags\84\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FD DF DF FD 0F 00 06 00
28 00 10 00 34 00 48 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 B4
00 60 00 78 00 78 00 B4 00 B4 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 FF FF FF FF 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00

----------------------------------
Values modified:5
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 85 E0 8A C9 96 34 9C 86 CC BC 61 2C 10
BC 8C D4 10 49 43 58 3F 76 E2 88 62 65 4E 7E E2 87 88 67 00 68 DF 7A C5 20 B3 71 F1 5B 1F 7E
46 E3 56 43 C8 65 2F 97 74 D0 27 09 BD 6F 7B E6 09 B1 1E C2 2A 36 8F 82 17 23 C9 C7 84 C9 61
E4 02 8B A7 8B
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: B8 DE 31 50 A3 9D B2 3C C2 F2 E8 9D
A6 D9 D3 84 B8 89 6F 38 8B 6F F6 F8 14 8D 00 82 DE 7F 82 F4 CC 9E D2 86 68 12 10 49 EA 6C 38
E2 CE 5F F1 1F EC A0 C7 78 9E 93 72 48 AD 85 E5 E2 71 47 A4 35 C6 8C F5 40 C4 BF 13 39 28 76
A0 4F D5 98 42 AE
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_PGYFRFFVBA: BC 2A BE 0E 0B 00 00 00
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_PGYFRFFVBA: F3 68 BE 0E 0C 00 00 00
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_HVFPHG: 08 00 00 00 72 00 00 00 50 6F 56 43 1E CD D7 01
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_HVFPHG: 08 00 00 00 73 00 00 00 80 ED BA 7B 1E CD D7 01
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
```

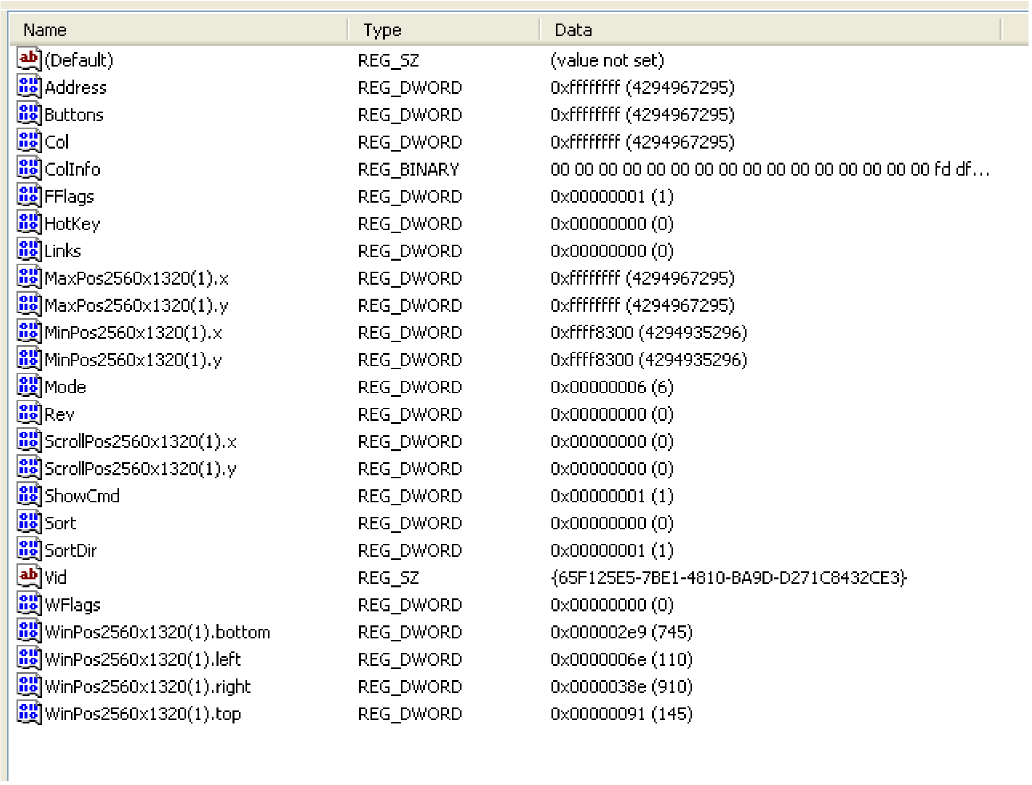
```
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\MRUListEx: 11 00 00 00 00 00 00 00 0A 00 00 00 14 00 00 00 0C 00 00 00 13 00 00 00 10
00 00 00 12 00 00 00 0F 00 00 00 0E 00 00 00 0D 00 00 00 06 00 00 00 03 00 00 00 0B 00 00 00 01
00 00 00 09 00 00 00 08 00 00 00 05 00 00 00 07 00 00 00 04 00 00 00 02 00 00 00 FF FF FF FF
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\
BagMRU\MRUListEx: 11 00 00 00 15 00 00 00 00 00 00 00 0A 00 00 00 14 00 00 00 0C 00 00 00 13
00 00 00 10 00 00 00 12 00 00 00 0F 00 00 00 0E 00 00 00 0D 00 00 00 06 00 00 00 03 00 00 00 0B
00 00 00 01 00 00 00 09 00 00 00 08 00 00 00 05 00 00 00 07 00 00 00 04 00 00 00 02 00 00 00 FF FF
FF FF

----------------------------------
Total changes:35
----------------------------------
```

HKEY_USERS\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\21



Name	Type	Data
(Default)	REG_SZ	(value not set)
MRUListEx	REG_BINARY	ff ff ff ff
NodeSlot	REG_DWORD	0x00000054 (84)

HKEY_USERS\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\84\Shell



Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0xffffffff (4294967295)
Buttons	REG_DWORD	0xffffffff (4294967295)
Col	REG_DWORD	0xffffffff (4294967295)
ColInfo	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd df…
FFlags	REG_DWORD	0x00000001 (1)
HotKey	REG_DWORD	0x00000000 (0)
Links	REG_DWORD	0x00000000 (0)
MaxPos2560x1320(1).x	REG_DWORD	0xffffffff (4294967295)
MaxPos2560x1320(1).y	REG_DWORD	0xffffffff (4294967295)
MinPos2560x1320(1).x	REG_DWORD	0xffff8300 (4294935296)
MinPos2560x1320(1).y	REG_DWORD	0xffff8300 (4294935296)
Mode	REG_DWORD	0x00000006 (6)
Rev	REG_DWORD	0x00000000 (0)
ScrollPos2560x1320(1).x	REG_DWORD	0x00000000 (0)
ScrollPos2560x1320(1).y	REG_DWORD	0x00000000 (0)
ShowCmd	REG_DWORD	0x00000001 (1)
Sort	REG_DWORD	0x00000000 (0)
SortDir	REG_DWORD	0x00000001 (1)
Vid	REG_SZ	{65F125E5-7BE1-4810-BA9D-D271C8432CE3}
WFlags	REG_DWORD	0x00000000 (0)
WinPos2560x1320(1).bottom	REG_DWORD	0x000002e9 (745)
WinPos2560x1320(1).left	REG_DWORD	0x0000006e (110)
WinPos2560x1320(1).right	REG_DWORD	0x0000038e (910)
WinPos2560x1320(1).top	REG_DWORD	0x00000091 (145)

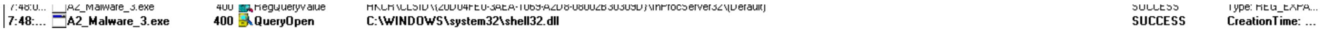
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\21
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\84
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\84\Shell

S-1-5-21-682003330-2147343463-725345543-500 appears to be a security identifier
there is a different security identifier for each user
(https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers)

http://www.thinworld.net/blog/2009/06/explanation-of-shellnoroam-registry.html
“This registry area is used to store information on window position/size and view settings.
Windows allow for each folder to have unique view settings (eg. Details view) and this information is stored under the BAGS and BAGSMRU Keys. ”

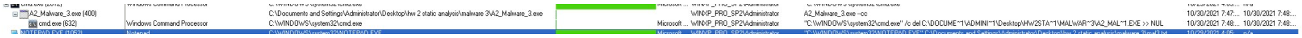
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\21
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\84
HKU\S-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\84\Shell

the view settings should be in these keys

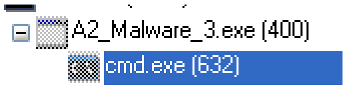


```
7:48:0...  A2_Malware_3.exe  400  RegQueryValue  HKCR\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\InProcServer32\(Default)  SUCCESS  Type: REG_EXPA...
7:48:...   A2_Malware_3.exe  400  QueryOpen      C:\WINDOWS\system32\shell32.dll                                           SUCCESS  CreationTime: ...
```

the shell is shell32.dll



```
A2_Malware_3.exe (400)                        C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\malware 3\A2_Malware_3.exe               WINXP_PRO_SP2\Administrator  A2_Malware_3.exe --cc                                                                              10/30/2021 7:47:...  10/30/2021 7:48:...
  cmd.exe (632)   Windows Command Processor   C:\WINDOWS\system32\cmd.exe                                                                      Microsoft ...  WINXP_PRO_SP2\Administrator  "C:\WINDOWS\system32\cmd.exe" /c del C:\DOCUME~1\ADMINI~1\Desktop\HW2STA~1\MALWAR~3\A2_MAL~1.EXE >> NUL  10/30/2021 7:48:...  10/30/2021 7:48:...
```



```
A2_Malware_3.exe (400)
  cmd.exe (632)
```

There is a process associated with the malware called cmd.exe

==

Q13: You are working as a security administrator. Your company was recently struck by a malware infection.

Here is what the regular users report:

User 1: "A strange black window, I think you nerds called it a terminal. I do not remember installing that"

User 2: "Some of my shareware applications stopped working"

User 3: "This is annoying..."

1. You were able to capture dada.exe and have a reason to believe that it is the culprit.
2. 1. Perform basic static analysis on this binary. What were able to learn?
3. 2. Perform basic dynamic analysis on this binary. What were you able to learn?
4. 3. Using the results from static and dynamic analysis write up your conclusion about what this malware does and support your results with screenshots. Please be sure to first describe the conclusion in crisply terms accessible to your bosses (who are non-technical individuals) and then provide a technical description suitable for the senior IT experts. An example of a real-world model malware analysis report can be found here. (Links to an external site.)

==

==

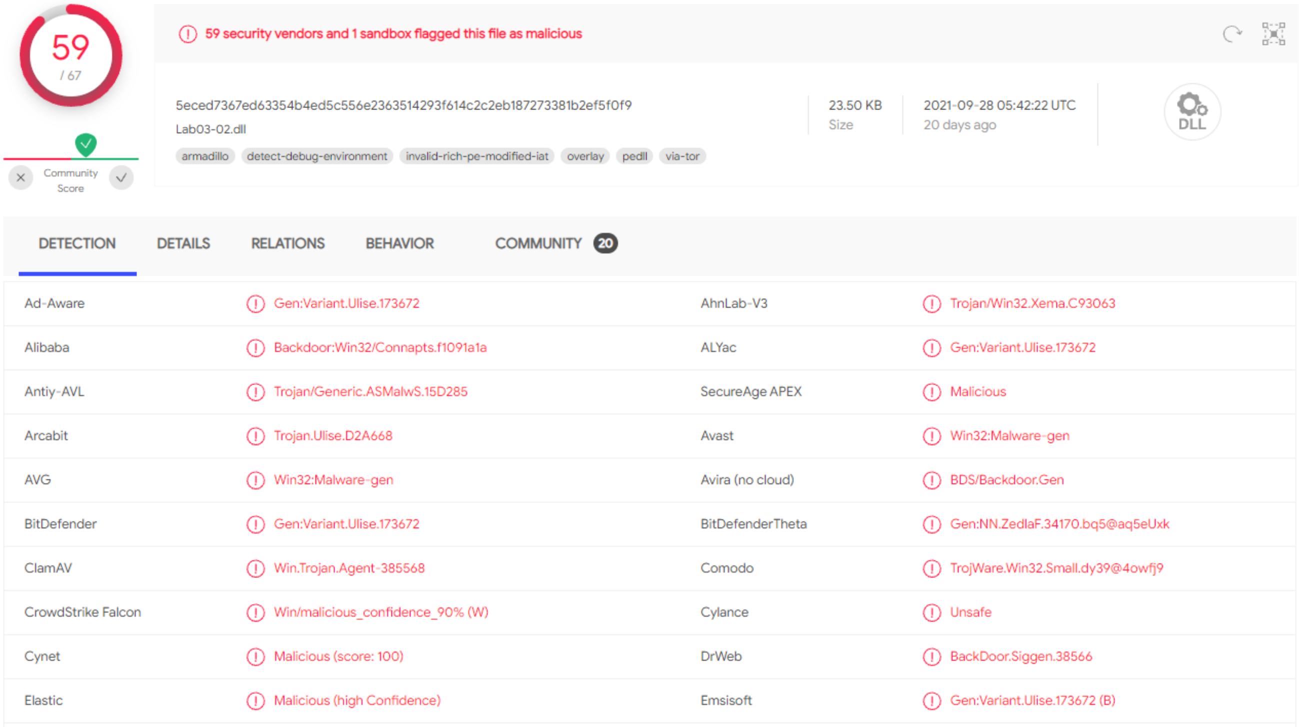
==

==

==

A2_malware_1.dll static analysis

Virus total: https://www.virustotal.com/gui/file/5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9



59
/ 67

Community Score

59 security vendors and 1 sandbox flagged this file as malicious

5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9
Lab03-02.dll

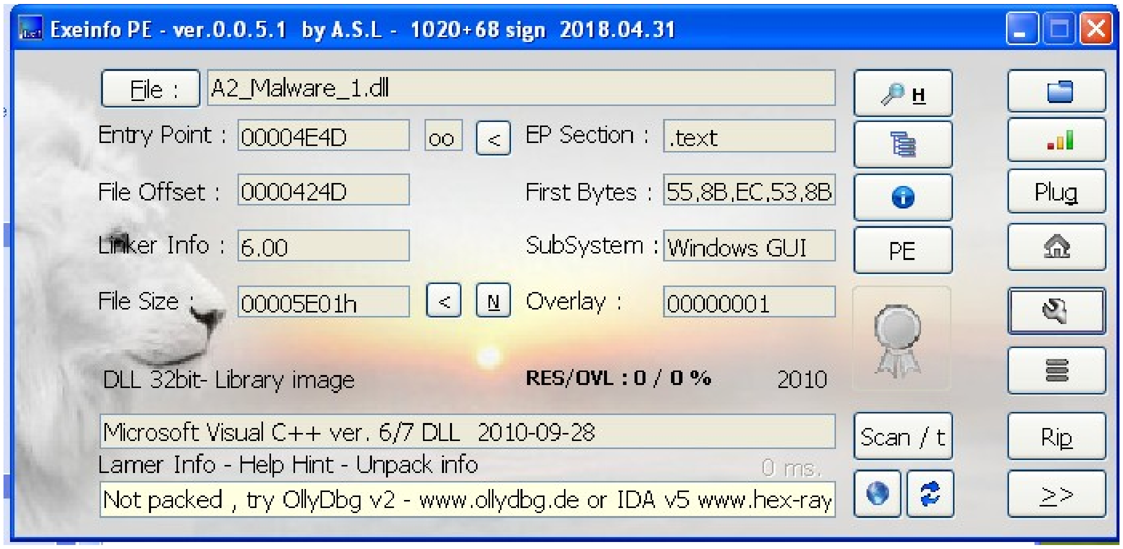
armadillo detect-debug-environment invalid-rich-pe-modified-iat overlay pedll via-tor

23.50 KB
Size

2021-09-28 05:42:22 UTC
20 days ago

Ad-Aware	Gen:Variant.Ulise.173672	AhnLab-V3	Trojan/Win32.Xema.C93063
Alibaba	Backdoor:Win32/Connapts.f1091a1a	ALYac	Gen:Variant.Ulise.173672
Antiy-AVL	Trojan/Generic.ASMalwS.15D285	SecureAge APEX	Malicious
Arcabit	Trojan.Ulise.D2A668	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	BDS/Backdoor.Gen
BitDefender	Gen:Variant.Ulise.173672	BitDefenderTheta	Gen:NN.ZedlaF.34170.bq5@aq5eUxk
ClamAV	Win.Trojan.Agent-385568	Comodo	TrojWare.Win32.Small.dy39@4owfj9
CrowdStrike Falcon	Win/malicious_confidence_90% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	BackDoor.Siggen.38566
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ulise.173672 (B)

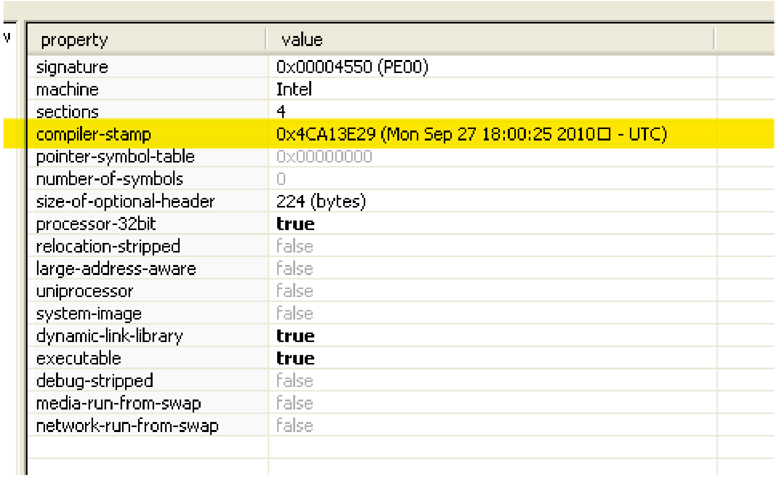
Ad-Aware says Ulise
AhnLab-V3 says Xema and trojan
Alibaba says backdoor and Connapts
DrWeb says Siggen



Exeinfo PE - ver.0.0.5.1 by A.S.L - 1020+68 sign 2018.04.31

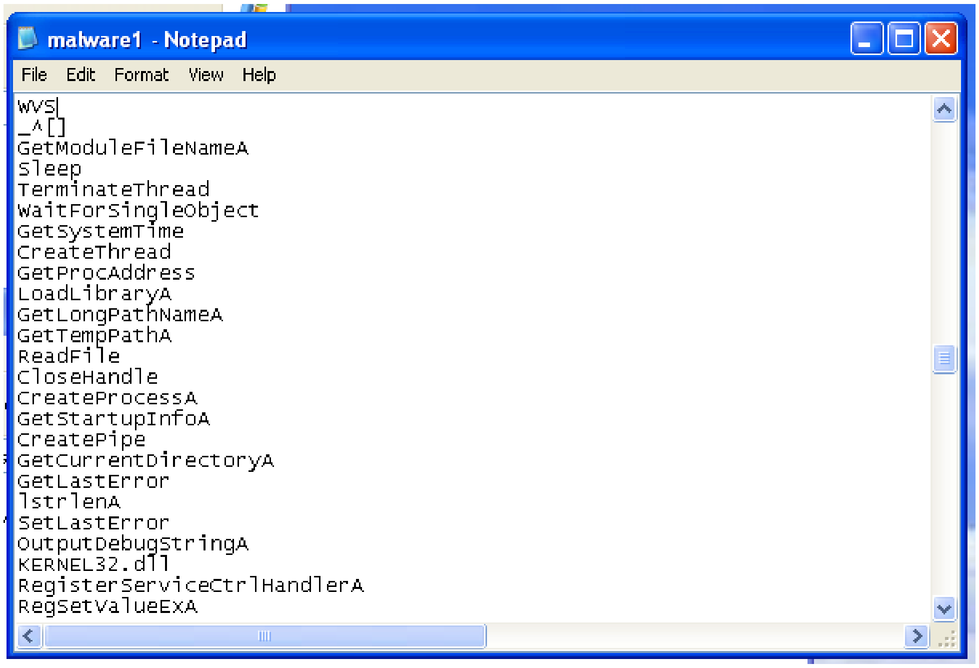
File : A2_Malware_1.dll
Entry Point : 00004E4D
EP Section : .text
File Offset : 0000424D
First Bytes : 55,8B,EC,53,8B
Linker Info : 6.00
SubSystem : Windows GUI
File Size : 00005E01h
Overlay : 00000001
DLL 32bit- Library image
RES/OVL : 0 / 0 % 2010
Microsoft Visual C++ ver. 6/7 DLL 2010-09-28
Lamer Info - Help Hint - Unpack info
0 ms.
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

The malware does not appear to be packed.
The malware appears to be compiled with Microsoft Visual C++ and on 2010-09-28.
There might be a GUI.



property	value
signature	0x00004550 (PE00)
machine	Intel
sections	4
compiler-stamp	0x4CA13E29 (Mon Sep 27 18:00:25 2010□ - UTC)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)
processor-32bit	**true**
relocation-stripped	false
large-address-aware	false
uniprocessor	false
system-image	false
dynamic-link-library	**true**
executable	**true**
debug-stripped	false
media-run-from-swap	false
network-run-from-swap	false

The compiler stamp appears to be Monday September 27 18:00:25 2010 UTC.



```
WVS
_^[]
GetModuleFileNameA
Sleep
TerminateThread
WaitForSingleObject
GetSystemTime
CreateThread
GetProcAddress
LoadLibraryA
GetLongPathNameA
GetTempPathA
ReadFile
CloseHandle
CreateProcessA
GetStartupInfoA
CreatePipe
GetCurrentDirectoryA
GetLastError
lstrlenA
SetLastError
OutputDebugStringA
KERNEL32.dll
RegisterServiceCtrlHandlerA
RegSetValueExA
```

Misc. Suspicious strings:

- “Windows XP 6.11”
- “Description
- Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.”
- “Intranet Network Awareness (INA+)”
- “You specify service name not in Svchost//netsvcs, must be one of following:”
- “uninstall success”
- “uninstall is starting”

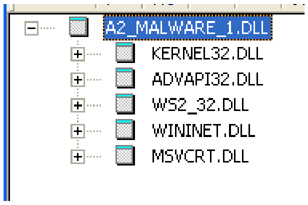
Host based indicators:

- Lab03-02.dll
- serve.html
- .exe

- cmd.exe
- %SystemRoot%\System32\svchost.exe
- SYSTEM\CurrentControlSet\Services\
- %SystemRoot%\System32\svchost.exe
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

Network based indicators:

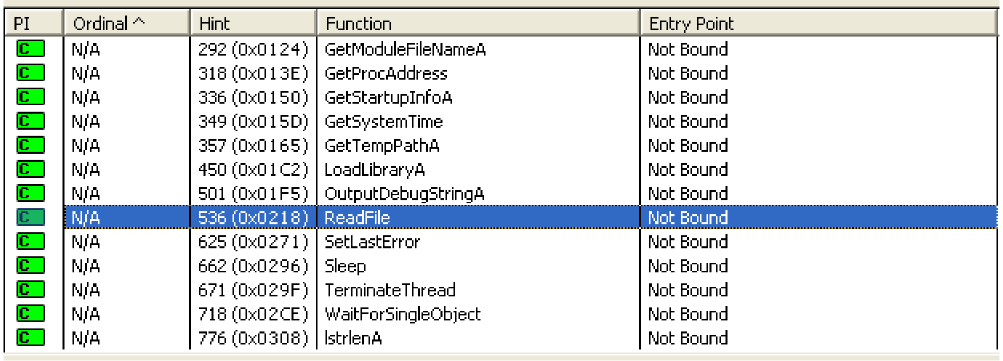
- practicalmalwareanalysis . Com
- HTTP/1.1
-



```
A2_MALWARE_1.DLL
    KERNEL32.DLL
    ADVAPI32.DLL
    WS2_32.DLL
    WININET.DLL
    MSVCRT.DLL
```

Suspicious imports:

- KERNEL32.dll (from lecture, might have access to memory, files, and hardware)
- advapi32.dll: (https://www.file.net/process/advapi32.dll.html can shutdown or restart the machine, has access to the windows registry, has access to user accounts, can start and stop windows services)
- WS2_32.DLL: (from lecture, might connect to a network and might have network related features)
- WININET.DLL: (from lecture, might use protocols like HTTP)
- MSVCRT (https://docs.python.org/3/library/msvcrt.html used in some windows services, there might be a service involved)



PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	292 (0x0124)	GetModuleFileNameA	Not Bound
C	N/A	318 (0x013E)	GetProcAddress	Not Bound
C	N/A	336 (0x0150)	GetStartupInfoA	Not Bound
C	N/A	349 (0x015D)	GetSystemTime	Not Bound
C	N/A	357 (0x0165)	GetTempPathA	Not Bound
C	N/A	450 (0x01C2)	LoadLibraryA	Not Bound
C	N/A	501 (0x01F5)	OutputDebugStringA	Not Bound
C	N/A	536 (0x0218)	ReadFile	Not Bound
C	N/A	625 (0x0271)	SetLastError	Not Bound
C	N/A	662 (0x0296)	Sleep	Not Bound
C	N/A	671 (0x029F)	TerminateThread	Not Bound
C	N/A	718 (0x02CE)	WaitForSingleObject	Not Bound
C	N/A	776 (0x0308)	lstrlenA	Not Bound

Suspicious imports continued:

- ReadFile (might read a file)
- GetSystemTime (https://docs.microsoft.com/en-us/windows/win32/api/sysinfoapi/nf-sysinfoapi-getsystemtime , might look at the system time and use that information to do something)
- GetCurrentDirectoryA (https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getcurrentdirectory , looks at the directory a process is in, might use this to keep track of process location)

- CreateServiceA: (https://docs.microsoft.com/en-us/windows/win32/api/winsvc/nf-winsvc-createservicea starts a service and puts it into a database, might create a service as part of its behaviors, might be a host based indicator)
- HttpOpenRequestA (https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-httpopenrequesta , might create a HTTP request, might be a network based indicator, might work with HTTP functions)
- InternetConnectA (https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetconnecta , might connect to the internet with HTTP)
- InternetReadFile (https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetreadfile , might read information from the internet)

==
==
==
==
==

==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==
==

```
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================

========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
========================================================================
```