Reversing Malware with IDA Pro

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

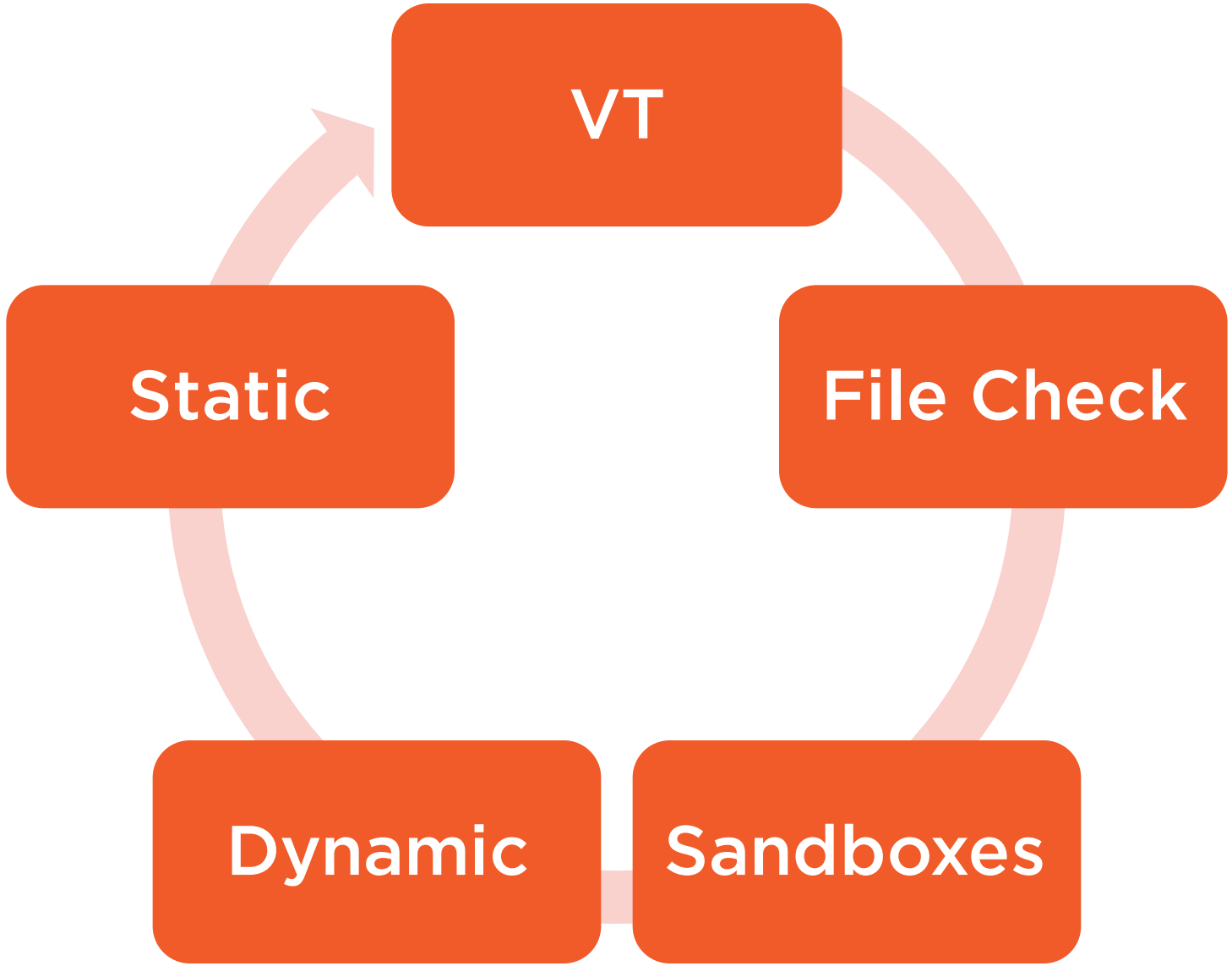
@jareddemott www.vdalabs.com

Overview

- Demo
- Cyclic Analysis
- Goals Recap
- Tools and Techniques
- Task

Demo

Reversing Malware with IDA pro


VT
File Check
Sandboxes
Dynamic
Static

File not found

The file you are looking for is not in our database.

Take me back to the main page | Try another search

SHA256: bf7875ce708b7d68fbcbf046d3f32dd99144b4ed543bc41a884f441590c0631f

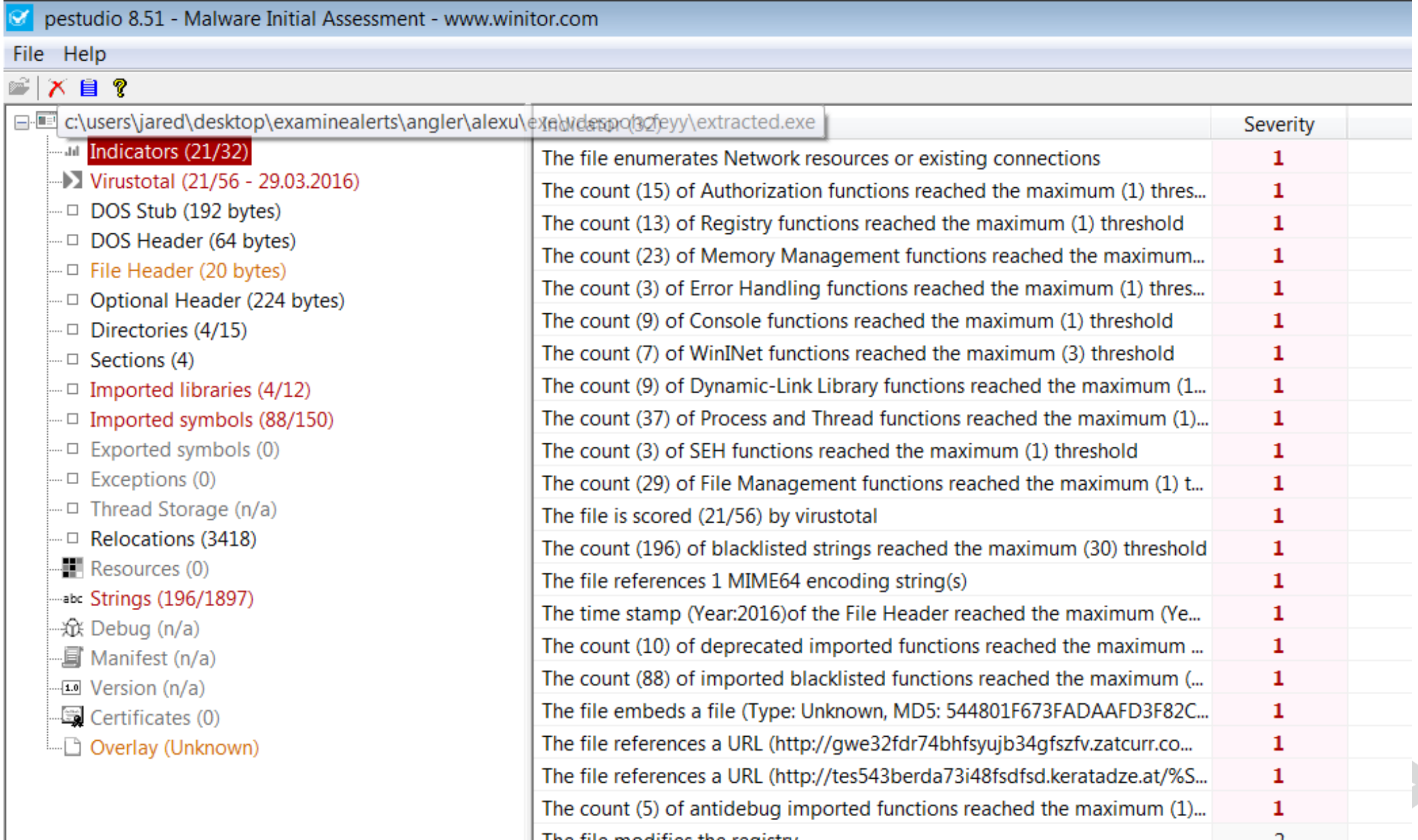
File name: extracted.exe

Detection ratio: 21 / 56

Analysis date: 2016-03-29 14:23:33 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes | Behavioural information

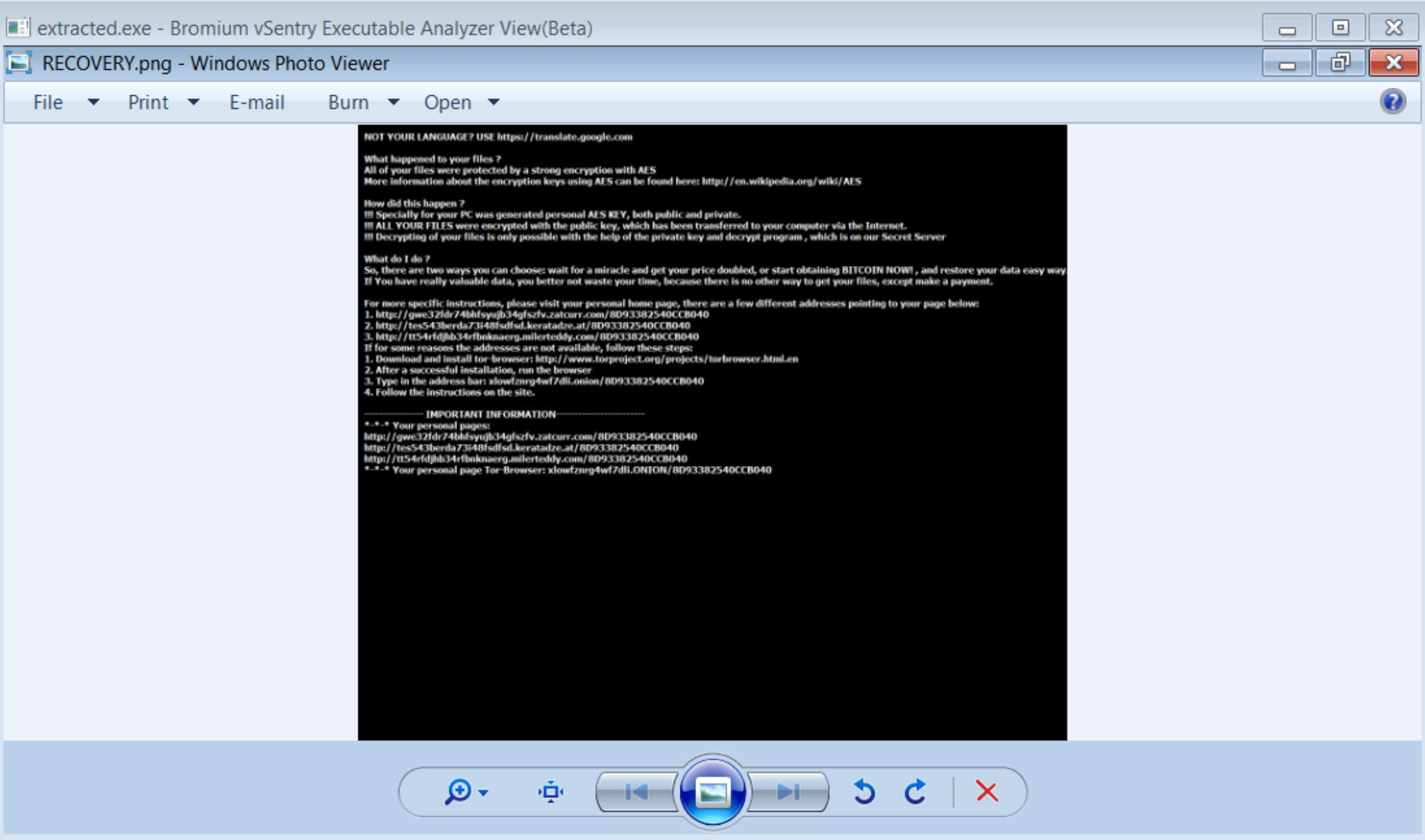
Antivirus	Result	Update
ALYac	Gen:Variant.Zusy.183720	20160329
AVG	Generic_r.HRP	20160329
Ad-Aware	Gen:Variant.Zusy.183720	20160329
Antiy-AVL	Trojan[:HEUR]/Win32.AGeneric	20160329
Arcabit	Trojan.Zusy.D2CDA8	20160329
Avast	Win32:Malware-gen	20160329
Baidu	Win32.Trojan.WisdomEyes.151026.9950.9998	20160329
BitDefender	Gen:Variant.Zusy.183720	20160329
ESET-NOD32	a variant of Win32/Filecoder.TeslaCrypt.I	20160329


pestudio 8.51 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\jared\desktop\examinealerts\angler\alexu\extracted.exe
Indicators (21/32)
Virustotal (21/56 - 29.03.2016)
DOS Stub (192 bytes)
DOS Header (64 bytes)
File Header (20 bytes)
Optional Header (224 bytes)
Directories (4/15)
Sections (4)
Imported libraries (4/12)
Imported symbols (88/150)
Exported symbols (0)
Exceptions (0)
Thread Storage (n/a)
Relocations (3418)
Resources (0)
Strings (196/1897)
Debug (n/a)
Manifest (n/a)
Version (n/a)
Certificates (0)
Overlay (Unknown)
Indicator (32)
Severity
The file enumerates Network resources or existing connections 1
The count (15) of Authorization functions reached the maximum (1) thres... 1
The count (13) of Registry functions reached the maximum (1) threshold 1
The count (23) of Memory Management functions reached the maximum... 1
The count (3) of Error Handling functions reached the maximum (1) thres... 1
The count (9) of Console functions reached the maximum (1) threshold 1
The count (7) of WinINet functions reached the maximum (3) threshold 1
The count (9) of Dynamic-Link Library functions reached the maximum (1... 1
The count (37) of Process and Thread functions reached the maximum (1)... 1
The count (3) of SEH functions reached the maximum (1) threshold 1
The count (29) of File Management functions reached the maximum (1) t... 1
The file is scored (21/56) by virustotal 1
The count (196) of blacklisted strings reached the maximum (30) threshold 1
The file references 1 MIME64 encoding string(s) 1
The time stamp (Year:2016)of the File Header reached the maximum (Ye... 1
The count (10) of deprecated imported functions reached the maximum ... 1
The count (88) of imported blacklisted functions reached the maximum (... 1
The file embeds a file (Type: Unknown, MD5: 544801F673FADAAFD3F82C... 1
The file references a URL (http://gwe32fdr74bhfsyujb34gfszfv.zatcurr.co... 1
The file references a URL (http://tes543berda73i48fsdfsd.keratadze.at/%S... 1
The count (5) of antidebug imported functions reached the maximum (1)... 1

Goals Recap:

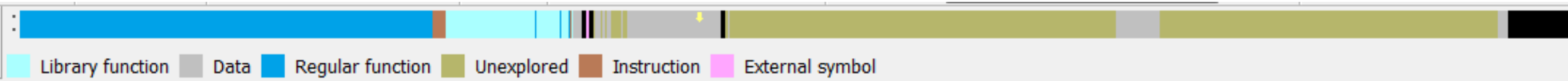
- Yara Sig
- C2 servers
- Networking
- Decode config or DGA
- Server emulator
- Artifacts for detection
- Deep dive for research

Urls found in memory or binary data	
Source: extracted.exe	String found in binary or memory: file:///c:/windows/system32/cmd.exe
Source: fuqximjyderv.exe	String found in binary or memory: file:///c:/windows/system32/wbem/wmic.exe
Source: WMIC.exe	String found in binary or memory: file:///c:/windows/system32/wbem/xsl-mappings.xmlbe
Source: WMIC.exe	String found in binary or memory: file:///c:/windows/system32/wbem/xsl-mappings.xmlg9
Source: WMIC.exe	String found in binary or memory: file:///c:/windows/system32/wbem/xsl-mappings.xmlw9
Source: WMIC.exe	String found in binary or memory: file://c:
Source: fuqximjyderv.exe	String found in binary or memory: http://biocarbon.com.ec/cgi-sys/suspendedpage.cgic
Source: fuqximjyderv.exe	String found in binary or memory: http://biocarbon.com.ec/cgi-sys/suspendedpage.cgipa
Source: fuqximjyderv.exe	String found in binary or memory: http://biocarbon.com.ec/wp-content/uploads/bstr.php
Source: fuqximjyderv.exe	String found in binary or memory: http://biocarbon.com.ec/wp-content/uploads/bstr.phpg
Source: fuqximjyderv.exe, _RECOVERY_+lhvyp.txt97.2912.dr, _RECOVERY_+lhvyp.txt57.2912.dr, _RECOVERY_+lhvyp.txt33.2912.dr, _RECOVERY_+lhvyp.txt3.2912.dr, _RECOVERY_+lhvyp.txt166.2912.dr, _RECOVERY_+lhvyp.txt58.2912.dr, _RECOVERY_+lhvyp.txt68.2912.dr, _RECOVERY_+lhvyp.txt157.2912.dr, _RECOVERY_+lhvyp.txt51.2912.dr, _RECOVERY_+lhvyp.txt121.2912.dr, _RECOVERY_+lhvyp.txt172.2912.dr,	String found in binary or memory: http://en.wikipedia.org/wiki/aes


extracted.exe - Bromium vSentry Executable Analyzer View(Beta)
RECOVERY.png - Windows Photo Viewer
File
Print
E-mail
Burn
Open
NOT YOUR LANGUAGE? USE https://translate.google.com
What happened to your files ?
All of your files were protected by a strong encryption with AES
More information about the encryption keys using AES can be found here: http://en.wikipedia.org/wiki/AES
How did this happen ?
!!! Specially for your PC was generated personal AES KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server
What do I do ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://gwe32fdr74bhfsyujb34gfszfv.zatcurr.com/8D93382540CCB040
2. http://tes543berda73i48fsdfsd.keratadze.at/8D93382540CCB040
3. http://tt54rfdjhb34rfbnknaerg.milerteddy.com/8D93382540CCB040
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser
3. Type in the address bar: xlowfznrg4wf7dli.onion/8D93382540CCB040
4. Follow the instructions on the site.
---------- IMPORTANT INFORMATION----------
--* Your personal pages:
http://gwe32fdr74bhfsyujb34gfszfv.zatcurr.com/8D93382540CCB040
http://tes543berda73i48fsdfsd.keratadze.at/8D93382540CCB040
http://tt54rfdjhb34rfbnknaerg.milerteddy.com/8D93382540CCB040
--* Your personal page Tor-Browser: xlowfznrg4wf7dli.ONION/8D93382540CCB040

```
PROCESS INVOCATIONS
```

13:07:57	extracted.exe	Execute Windows\iiigvgofrses.exe C:\Windows\iiigvgofrses.exe
13:07:57	extracted.exe	Execute Windows\SysWOW64\cmd.exe "C:\Windows\system32\cmd.exe" /c DEL R:\FZ\extracted.exe
13:07:58	iiigvgofrses.exe	Execute Windows\System32\wbem\WMIC.exe "C:\Windows\System32\wbem\WMIC.exe" shadowcopy delete /nointeractive
13:07:58	csrss.exe	Execute Windows\System32\conhost.exe \??\C:\Windows\system32\conhost.exe "460489515-1968229600344248790120764531 7-1089126277-740237141-1491494192-1146763216"
13:07:59	svchost.exe	Execute Windows\System32\wbem\WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
13:08:30	iiigvgofrses.exe	Execute Windows\SysWOW64\notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\bruser1729\Desktop\RECOVERY.TXT
13:08:31	iiigvgofrses.exe	Execute Program Files (x86)\Internet Explorer\iexplore.exe "C:\Program Files (x86)\Internet Explorer\iexplore.exe" -nohome
13:08:31	iexplore.exe	Execute Program Files (x86)\Internet Explorer\iexplore.exe "C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:2440 CREDAT:145409
13:08:31	svchost.exe	Execute Windows\SysWOW64\dllhost.exe C:\Windows\SysWOW64\DllHost.exe /Processid:{76D0CB12-7604-4048-B83C-1005C7DDC503}
13:08:31	iiigvgofrses.exe	Execute Windows\System32\wbem\WMIC.exe "C:\Windows\System32\wbem\WMIC.exe" shadowcopy delete /nointeractive
13:08:31	csrss.exe	Execute Windows\System32\conhost.exe \??\C:\Windows\system32\conhost.exe "-6568675541652306669-226462461156285432338762968 9-1603158033-98631504412009967 75"
13:09:25	iiigvgofrses.exe	Execute Windows\SysWOW64\cmd.exe "C:\Windows\system32\cmd.exe" /c DEL C:\Windows\iiigvgofrses.exe
13:09:25	csrss.exe	Execute Windows\System32\conhost.exe \??\C:\Windows\system32\conhost.exe "-172123015687710696413091334 01-1625877672-525941083-2062840476-377192802-1134920395"



Functions window

Function name

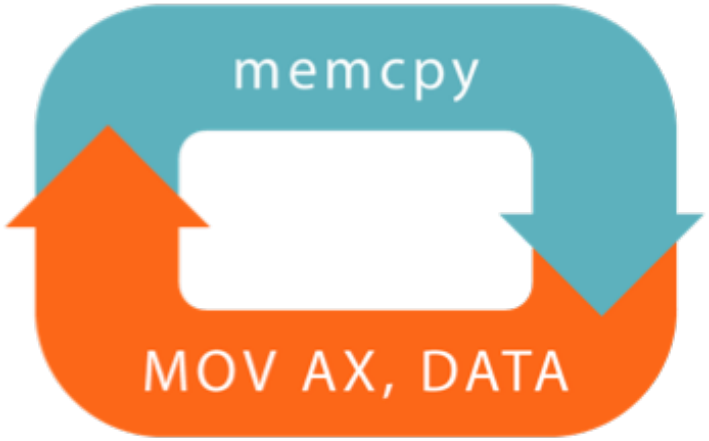
- _abort
- __msize
- __flswbuf
- __chsize_nolock
- __read_nolock
- __lseek_nolock
- __setmode_nolock
- sub_42FDE3
- __towlower_l
- ___initconout
- sub_42FECF
- ___ascii_strnicmp
- __allmul
- RtlUnwind
- _aullshr
- _allshl
- _alldiv
- sub_42FFAC
- ___DestructExceptionObject
- _CallSettingFrame(x,x,x)
- _memcpy_0

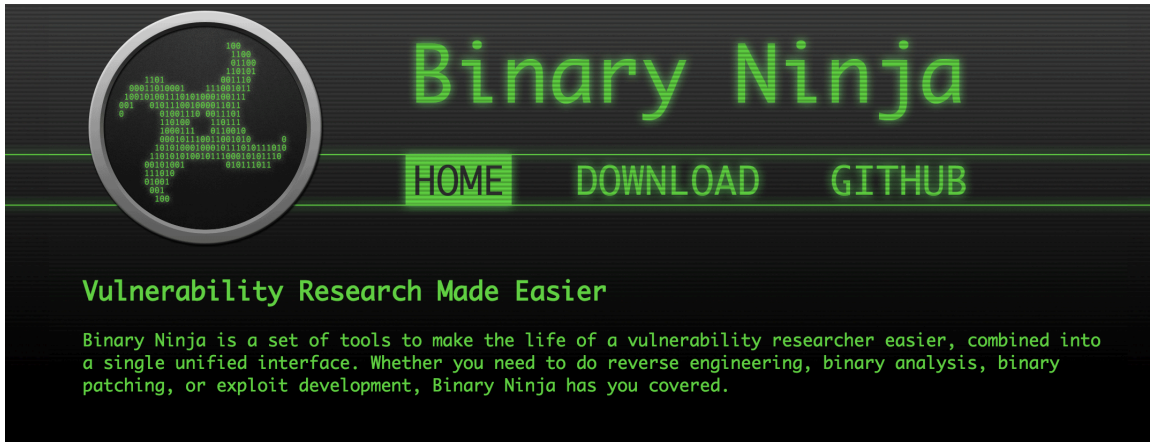
Line 534 of 534

IDA Vi... | simpliFiRE.IDAscope v... | Strings wi... | Hex Vi... | Struc... | En...

```
.rdata:0043A2AD                   align 10h
.rdata:0043A2B0 ; char a_exe[]
.rdata:0043A2B0 a_exe             db '.exe',0             ; DATA XREF: sub_41EAA0+62↑o
.rdata:0043A2B5                   align 4
.rdata:0043A2B8 ; char aShadowcopy[]
.rdata:0043A2B8 aShadowcopy       db ' shadowcopy ',0     ; DATA XREF: sub_41EAA0+8B↑o
.rdata:0043A2C5                   align 4
.rdata:0043A2C8 ; char aDelete[]
.rdata:0043A2C8 aDelete           db ' delete ',0         ; DATA XREF: sub_41EAA0+A1↑o
.rdata:0043A2D1                   align 4
.rdata:0043A2D4 ; char aNoin[]
.rdata:0043A2D4 aNoin             db ' /noin',0           ; DATA XREF: sub_41EAA0+B7↑o
.rdata:0043A2DB                   align 4
.rdata:0043A2DC ; char aTeractive[]
.rdata:0043A2DC aTeractive        db 'teractive ',0       ; DATA XREF: sub_41EAA0+D0↑o
.rdata:0043A2E7                   align 4
.rdata:0043A2E8 aOpen             db 'open',0             ; DATA XREF: sub_41EAA0+10A↑o
.rdata:0043A2ED                   align 10h
.rdata:0043A2F0 aRunas_0          db 'runas',0            ; DATA XREF: sub_41EAA0+116↑o
.rdata:0043A2F6                   align 4
.rdata:0043A2F8 aKasdfgh283       db 'kasdfgh283',0       ; DATA XREF: sub_412930+7C↑o
.rdata:0043A2F8                                           ; sub_412930+9F↑o
.rdata:0043A303                   align 4
.rdata:0043A304 aImagePng:                                ; DATA XREF: sub_4202E0+56↑o
.rdata:0043A304                   unicode 0, <image/png>,0
.rdata:0043A318 ; const WCHAR aShell32_dll_0
.rdata:0043A318 aShell32_dll_0:                           ; DATA XREF: wWinMain(x,x,x,x)+F7↑o
.rdata:0043A318                   unicode 0, <Shell32.dll>,0
.rdata:0043A330 ; const WCHAR ModuleName
.rdata:0043A330 ModuleName:                               ; DATA XREF: wWinMain(x,x,x,x)+12E↑o
.rdata:0043A330                   unicode 0, <KERNEL32>,0
```

00038AB8 0043A2B8: .rdata:aShadowcopy (Synchronized with Hex View-1)

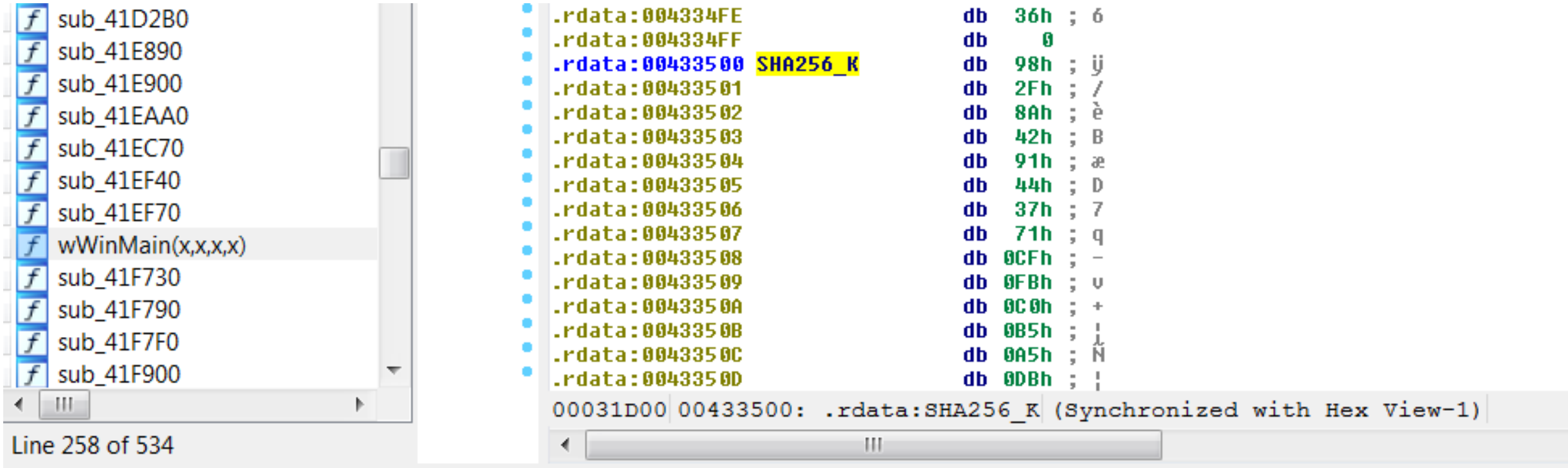

memcpy
MOV AX, DATA


Binary Ninja
HOME
DOWNLOAD
GITHUB
Vulnerability Research Made Easier
Binary Ninja is a set of tools to make the life of a vulnerability researcher easier, combined into a single unified interface. Whether you need to do reverse engineering, binary analysis, binary patching, or exploit development, Binary Ninja has you covered.

Anti-Analysis

- Debugger Detection
- Inline Obfuscation

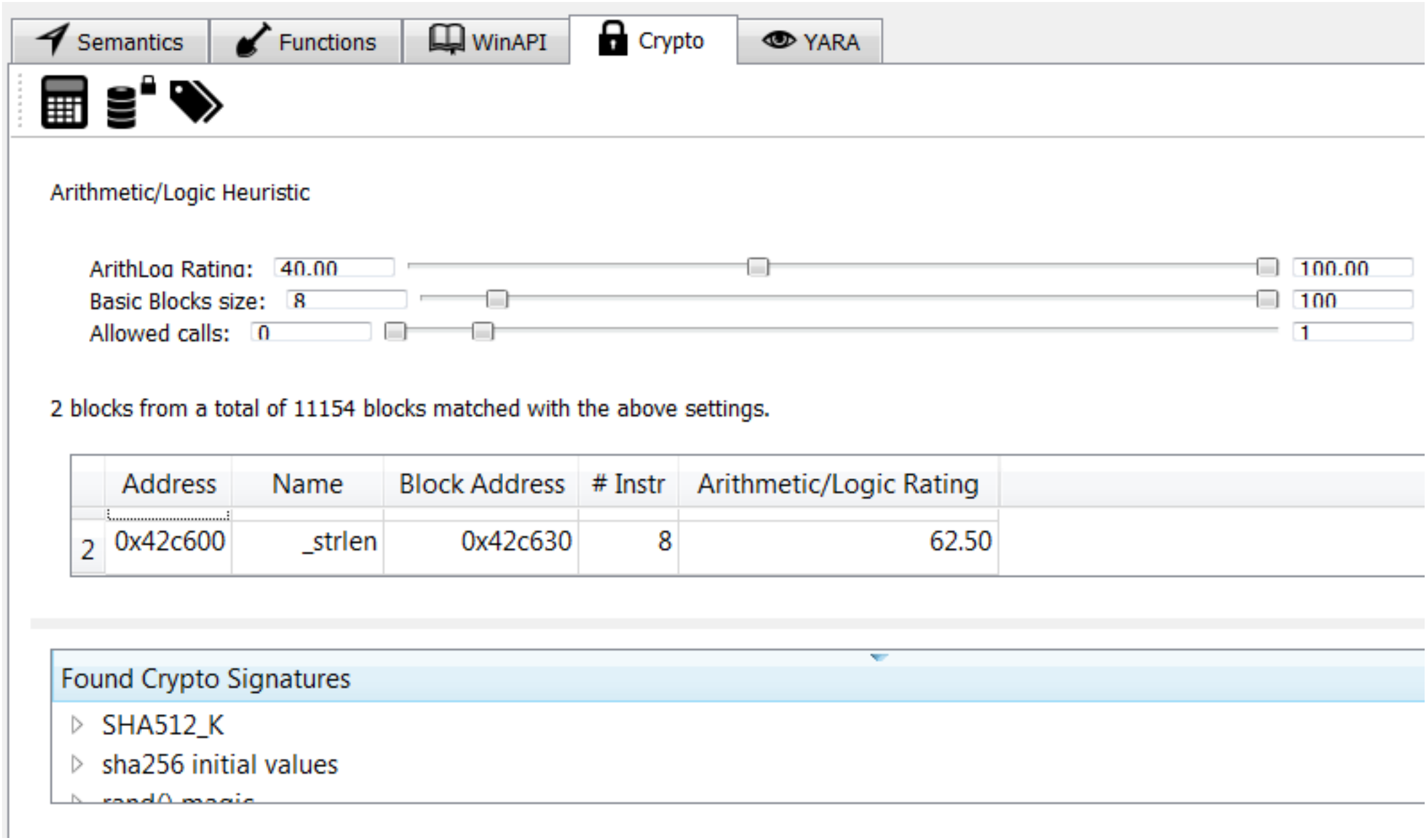
```
v9 = -134758405;
while ( v10 != a1 + 4 * a2 )
{
  v3 = -2084904757 * v7;
  *(_DWORD *)v10 = v8;
  v4 = __ROR4__(v8, 1);
  HIWORD(v8) = HIWORD(v4);
  BYTE1(v8) = v4 + BYTE1(v4);
  v9 |= 0x7550E9ADu;
  LOBYTE(v8) = v4 + BYTE1(v4) + v4;
  v5 = (v3 + v3 - 2066108466) & 0x7B265032 ^ v3 ^
  v7 = v5 & 0x2F0000;
```



Output window

```
[|] loading WinApiWidget
[|] loading CryptoIdentificationWidget
[|] loading YaraScannerWidget
[\] this took 0.16 seconds.

Caching 'Imports'... ok
  [/] CryptoIdentifier: Starting aritlog heuristic analysis.
  [\] Analysis took 1.22 seconds.
4018AE: found sparse constants for SHA-1
41B2C9: found sparse constants for SHA-1
433278: found const array SHA512_K (used in SHA512)
433500: found const array SHA256_K (used in SHA256)
Found 4 known constant arrays in total.
```


Semantics
Functions
WinAPI
Crypto
YARA
Arithmetic/Logic Heuristic
ArithLog Rating: 40.00 100.00
Basic Blocks size: 8 100
Allowed calls: 0 1
2 blocks from a total of 11154 blocks matched with the above settings.
Address Name Block Address # Instr Arithmetic/Logic Rating
2 0x42c600 _strlen 0x42c630 8 62.50
Found Crypto Signatures
SHA512_K
sha256 initial values

aaronportnoy / toolbag

Watch 45 Star 206 Fork 51

Code Issues 1 Pull requests 0 Wiki Pulse Graphs

The IDA Toolbag is a plugin providing supplemental functionality to Hex-Rays IDA Pro disassembler.

58 commits 1 branch 0 releases 5 contributors

Branch: master New pull request New file Upload files Find file HTTPS https://github.com/aaronp Download ZIP

aaronportnoy Revert "removed timers that were causing UI delays on large idbs. add… Latest commit 2d39457 on Jan 30, 2015

app	Initial import	4 years ago
base	Fixed pathfinder	4 years ago
docs	added wget mirror of docs page (by request)	2 years ago
rsrc	Added Function Analysis	4 years ago
toolbag	Revert "removed timers that were causing UI delays on large idbs. add…	a year ago
user/bin	Add alt switch jump finder	2 years ago
.gitignore	added the ability to display local comments/repeatable comments inste…	2 years ago

Function name

- wmic_delete_shadow
- set_string_pointers
- sub_41EF40
- sub_41EF70
- wWinMain(x,x,x,x)
- File_sub_41F730
- File_sub_41F790
- sub_41F7F0
- copy_create_process

ine 258 of 534

Graph overview

```
loc_41F549:
call    nullsub_1
xor     edi, edi
cmp     dword_43FC1C, 1
jnz     short loc_41F57D
```

```
push    6FB89AF0h
push    1
push    ebx
mov     dword_460778, ebx
call    resolve_lib_funcs
add     esp, 0Ch
push    ebx
push    ebx
push    ebx
push    offset Http_Str_WINet_sub_41B440
push    ebx
push    ebx
call    eax
mov     edi, eax
```

```
loc_41F57D:             ; lpThreadId
push    ebx
```

Hex Blog

State-of-the-art code analysis

TEAM

- Arnaud Diederen
- Igor Skochinsky
- Ilfak Guilfanov

THE IDA PRO BOOK (2ND ED)

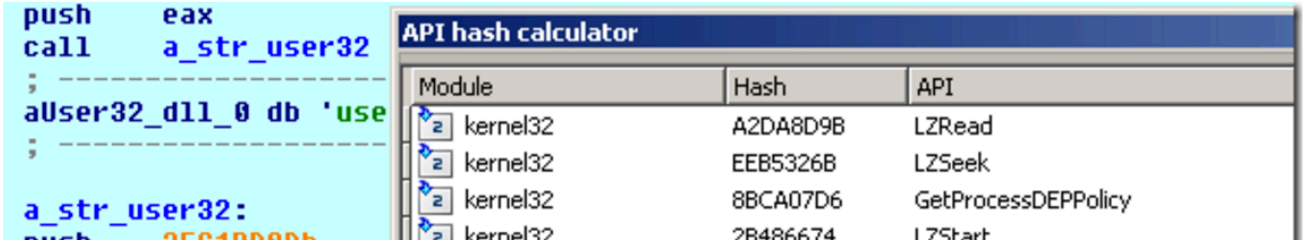
RECENT POSTS

IDA 6.9, Mac OS X, 'random'

Calculating API hashes with IDA Pro

Many times when debugging malware you discover that the malware does not import any function, replaces API names by hashes and tries to resolve the addresses by looking up which API name has the desired hash!

In this blog post we are going to demonstrate how to use IDA Pro to solve this problem and uncover all API hashes.



fireeye / flare-ida

Watch 101 | Star 330 | Fork 116

Code | Issues 8 | Pull requests 1 | Wiki | Pulse | Graphs

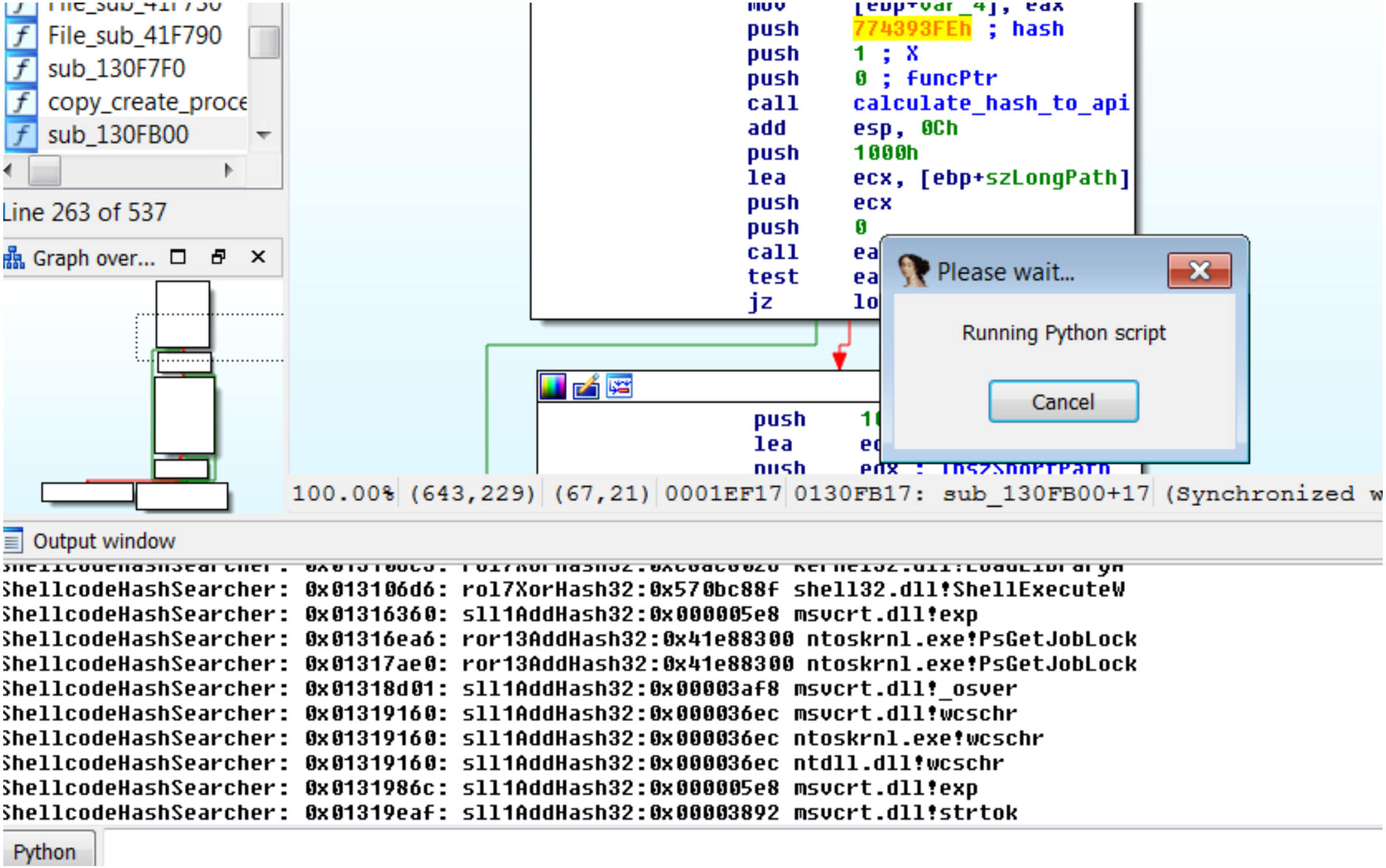
IDA Pro utilities from FLARE team

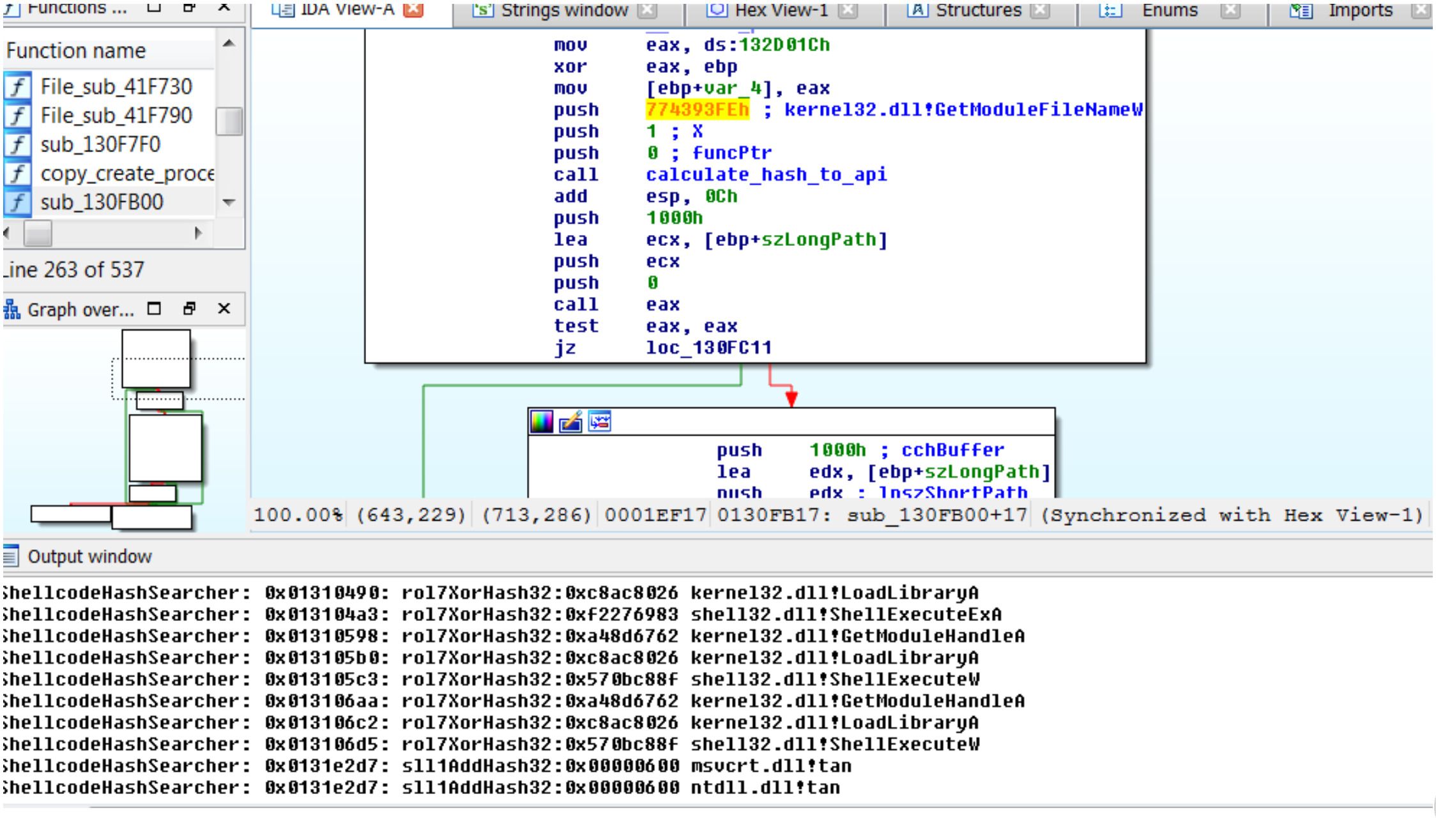
71 commits | 1 branch | 0 releases | 7 contributors

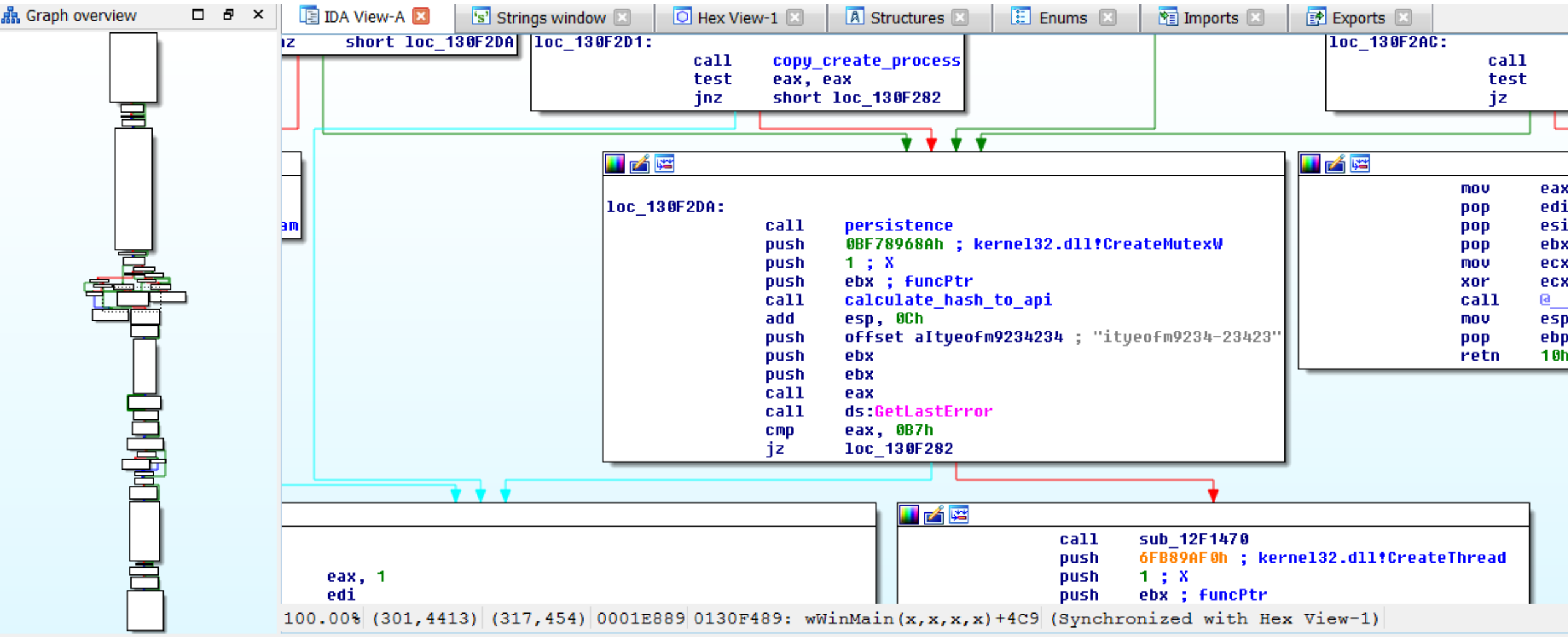
Branch: master | New pull request | New file | Upload files | Find file | HTTPS | https://github.com/fireey | Download ZIP

Willi Ballenthin manually merge idb2pat — Latest commit 2f0a449 on Feb 4

MSDN_crawler	Adding MSDN crawler	2 years ago
examples	Fixed names for argtracker examples	5 months ago
plugins	Updates to apply callee	a year ago
python/flare	manually merge idb2pat	2 months ago
shellcode_hashes	New rol7AddXor2Hash32 shellcode hash	4 months ago
.gitignore	Initial commit	2 years ago
LICENSE	Added readme & license file	2 years ago


File_sub_41F790
sub_130F7F0
copy_create_proce
sub_130FB00
Line 263 of 537
Graph over...
push 774393FEh ; hash
push 1 ; X
push 0 ; funcPtr
call calculate_hash_to_api
add esp, 0Ch
push 1000h
lea ecx, [ebp+szLongPath]
push ecx
push 0
test
jz
Please wait...
Running Python script
Cancel
100.00% (643,229) (67,21) 0001EF17 0130FB17: sub_130FB00+17 (Synchronized w
Output window
ShellcodeHashSearcher: 0x013106d6: rol7XorHash32:0x570bc88f shell32.dll!ShellExecuteW
ShellcodeHashSearcher: 0x01316360: sll1AddHash32:0x000005e8 msvcrt.dll!exp
ShellcodeHashSearcher: 0x01316ea6: ror13AddHash32:0x41e88300 ntoskrnl.exe!PsGetJobLock
ShellcodeHashSearcher: 0x01317ae0: ror13AddHash32:0x41e88300 ntoskrnl.exe!PsGetJobLock
ShellcodeHashSearcher: 0x01318d01: sll1AddHash32:0x00003af8 msvcrt.dll!_osver
ShellcodeHashSearcher: 0x01319160: sll1AddHash32:0x000036ec msvcrt.dll!wcschr
ShellcodeHashSearcher: 0x01319160: sll1AddHash32:0x000036ec ntoskrnl.exe!wcschr
ShellcodeHashSearcher: 0x01319160: sll1AddHash32:0x000036ec ntdll.dll!wcschr
ShellcodeHashSearcher: 0x0131986c: sll1AddHash32:0x000005e8 msvcrt.dll!exp
ShellcodeHashSearcher: 0x01319eaf: sll1AddHash32:0x00003892 msvcrt.dll!strtok
Python


Functions ...
Function name
File_sub_41F730
File_sub_41F790
sub_130F7F0
copy_create_proce
sub_130FB00
Line 263 of 537
Graph over...
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
mov eax, ds:132D01Ch
xor eax, ebp
mov [ebp+var_4], eax
push 774393FEh ; kernel32.dll!GetModuleFileNameW
push 1 ; X
push 0 ; funcPtr
call calculate_hash_to_api
add esp, 0Ch
push 1000h
lea ecx, [ebp+szLongPath]
push ecx
push 0
call eax
test eax, eax
jz loc_130FC11
push 1000h ; cchBuffer
lea edx, [ebp+szLongPath]
100.00% (643,229) (713,286) 0001EF17 0130FB17: sub_130FB00+17 (Synchronized with Hex View-1)
Output window
ShellcodeHashSearcher: 0x01310490: rol7XorHash32:0xc8ac8026 kernel32.dll!LoadLibraryA
ShellcodeHashSearcher: 0x013104a3: rol7XorHash32:0xf2276983 shell32.dll!ShellExecuteExA
ShellcodeHashSearcher: 0x01310598: rol7XorHash32:0xa48d6762 kernel32.dll!GetModuleHandleA
ShellcodeHashSearcher: 0x013105b0: rol7XorHash32:0xc8ac8026 kernel32.dll!LoadLibraryA
ShellcodeHashSearcher: 0x013105c3: rol7XorHash32:0x570bc88f shell32.dll!ShellExecuteW
ShellcodeHashSearcher: 0x013106aa: rol7XorHash32:0xa48d6762 kernel32.dll!GetModuleHandleA
ShellcodeHashSearcher: 0x013106c2: rol7XorHash32:0xc8ac8026 kernel32.dll!LoadLibraryA
ShellcodeHashSearcher: 0x013106d5: rol7XorHash32:0x570bc88f shell32.dll!ShellExecuteW
ShellcodeHashSearcher: 0x0131e2d7: sll1AddHash32:0x00000600 msvcrt.dll!tan
ShellcodeHashSearcher: 0x0131e2d7: sll1AddHash32:0x00000600 ntdll.dll!tan


Graph overview
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
Exports
short loc_130F2DA
loc_130F2D1:
call copy_create_process
test eax, eax
jnz short loc_130F282
loc_130F2AC:
call
test
jz
loc_130F2DA:
call persistence
push 0BF78968Ah ; kernel32.dll!CreateMutexW
push 1 ; X
push ebx ; funcPtr
call calculate_hash_to_api
add esp, 0Ch
push offset aItyeofm9234234 ; "ityeofm9234-23423"
push ebx
push ebx
call eax
call ds:GetLastError
cmp eax, 0B7h
jz loc_130F282
mov eax
pop edi
pop esi
pop ebx
mov ecx
xor ecx
call
mov esp
pop ebp
retn 10h
eax, 1
edi
call sub_12F1470
push 6FB89AF0h ; kernel32.dll!CreateThread
push 1 ; X
push ebx ; funcPtr
100.00% (301,4413) (317,454) 0001E889 0130F489: wWinMain(x,x,x,x)+4C9 (Synchronized with Hex View-1)

www.hacoder.com/2016/02/how-to-decrypt-or-restore-encrypted-files-teslacrypt-ransomware-removal/

Let's decrypt the files!

Note: Before decrypting the files, please backup the encrypted files.

STEP 1: Download Talos TeslaCrypt Decryption Tool.

Windows binary:

http://labs.snort.org/files/TeslaDecrypt_exe.zip

Python script:

https://labs.snort.org/files/TeslaDecrypt_python.zip

Source code to Windows binary:

https://labs.snort.org/files/TeslaDecrypt_cpp.zip

Summary

Static analysis

Multiple Techniques

Lab