

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 faydalananı 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 faydalananarak 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 MD5:2abe3cc4bfff46455a945d56c27e9fb45) 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

Matteo Salvalaggio | LinkedIn

Secure | <https://www.linkedin.com/in/matteo-salvalaggio-96635711a/>

in Search

Home My Network Jobs Messaging Notifications Me

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

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 km

Send InMail Connect

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

See less

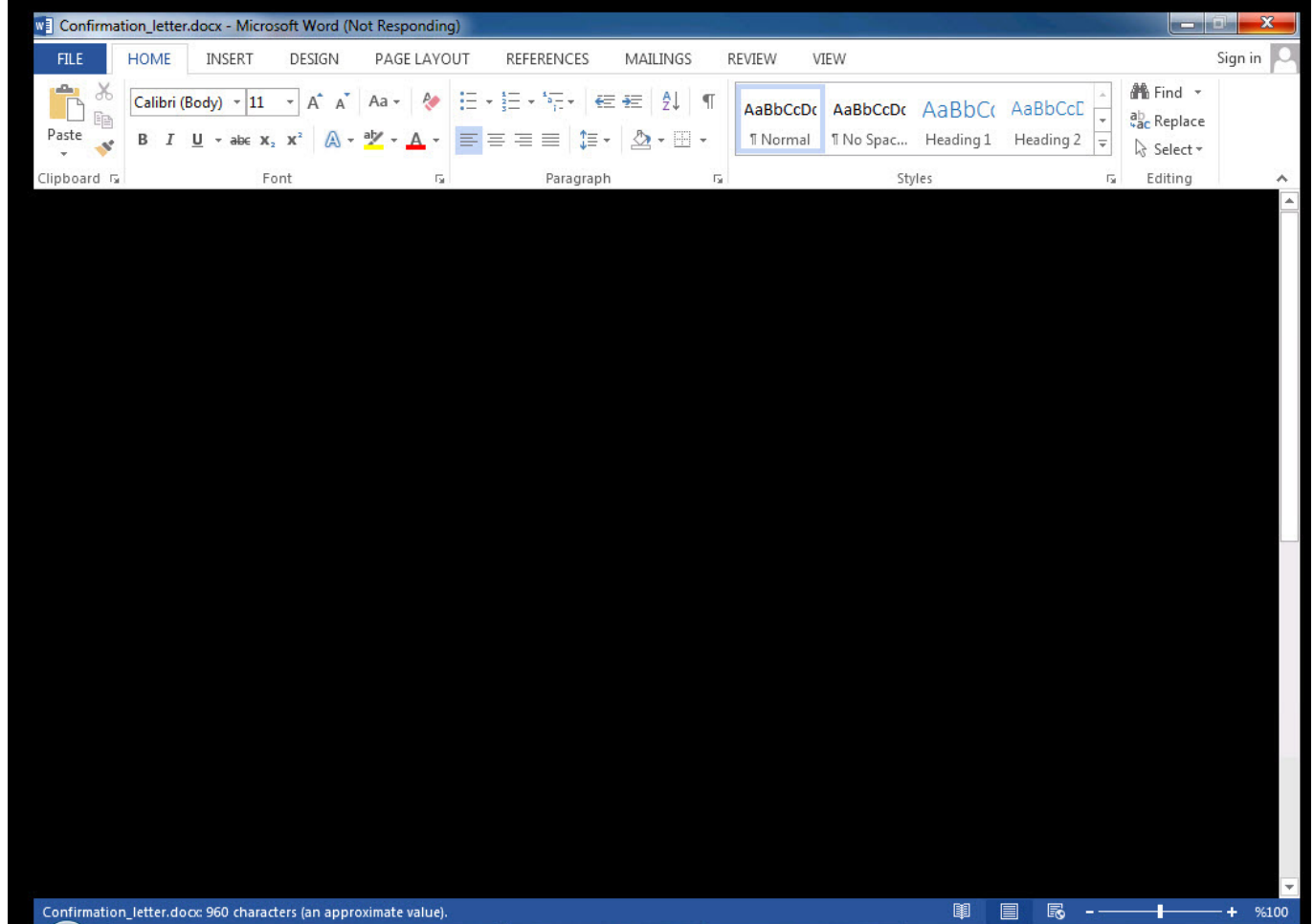
Assegnista borsa di ricerca PON-METRICS

University of Padova

Jun 2016 - Dec 2016 • 7 mos

See description

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.



Confirmation_letter.docx - Word (Not Responding)

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW Sign in

Clipboard Font Paragraph Styles Editing

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,

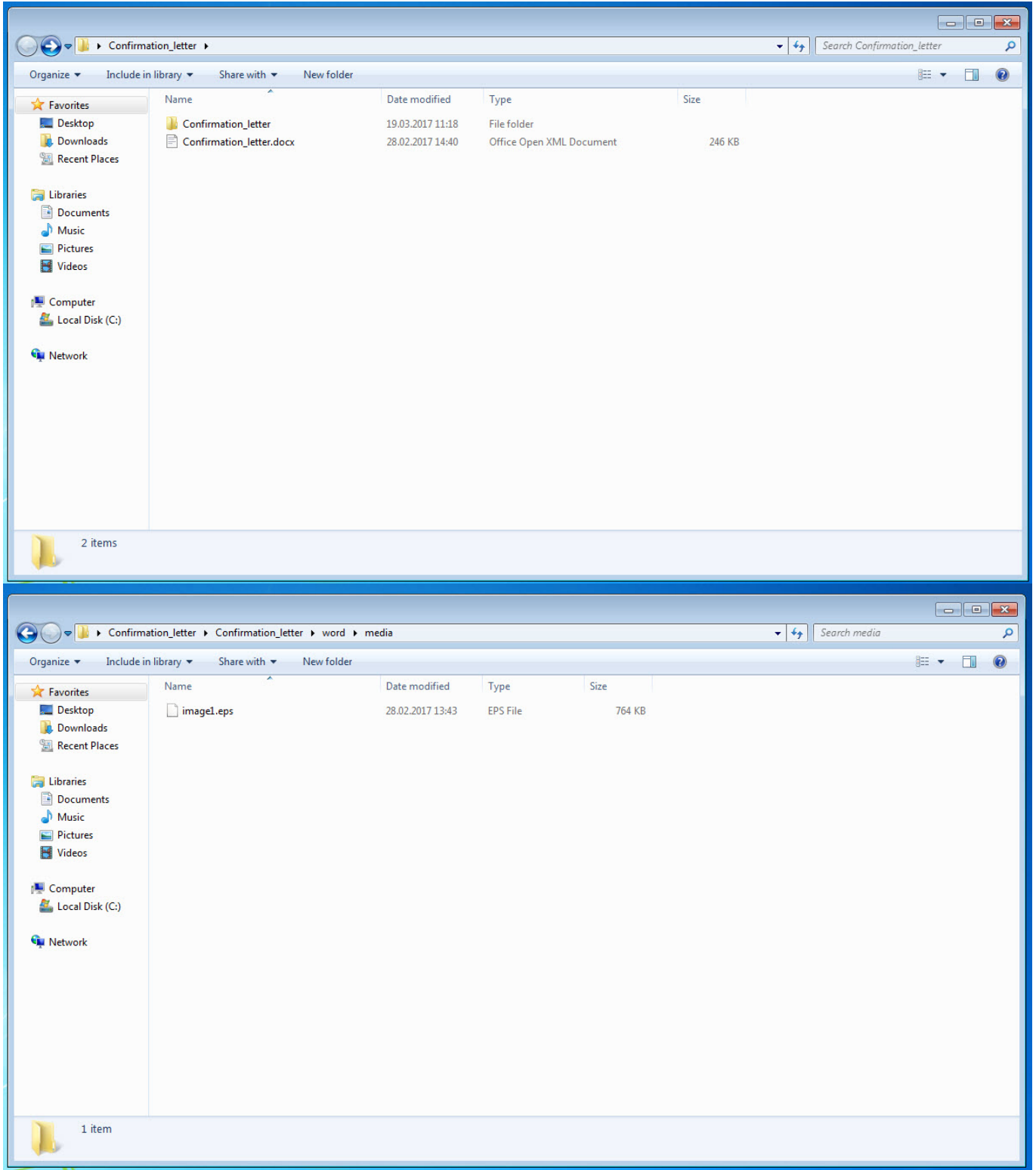
London School of Economics & Political Science, Award Committee

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

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

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.

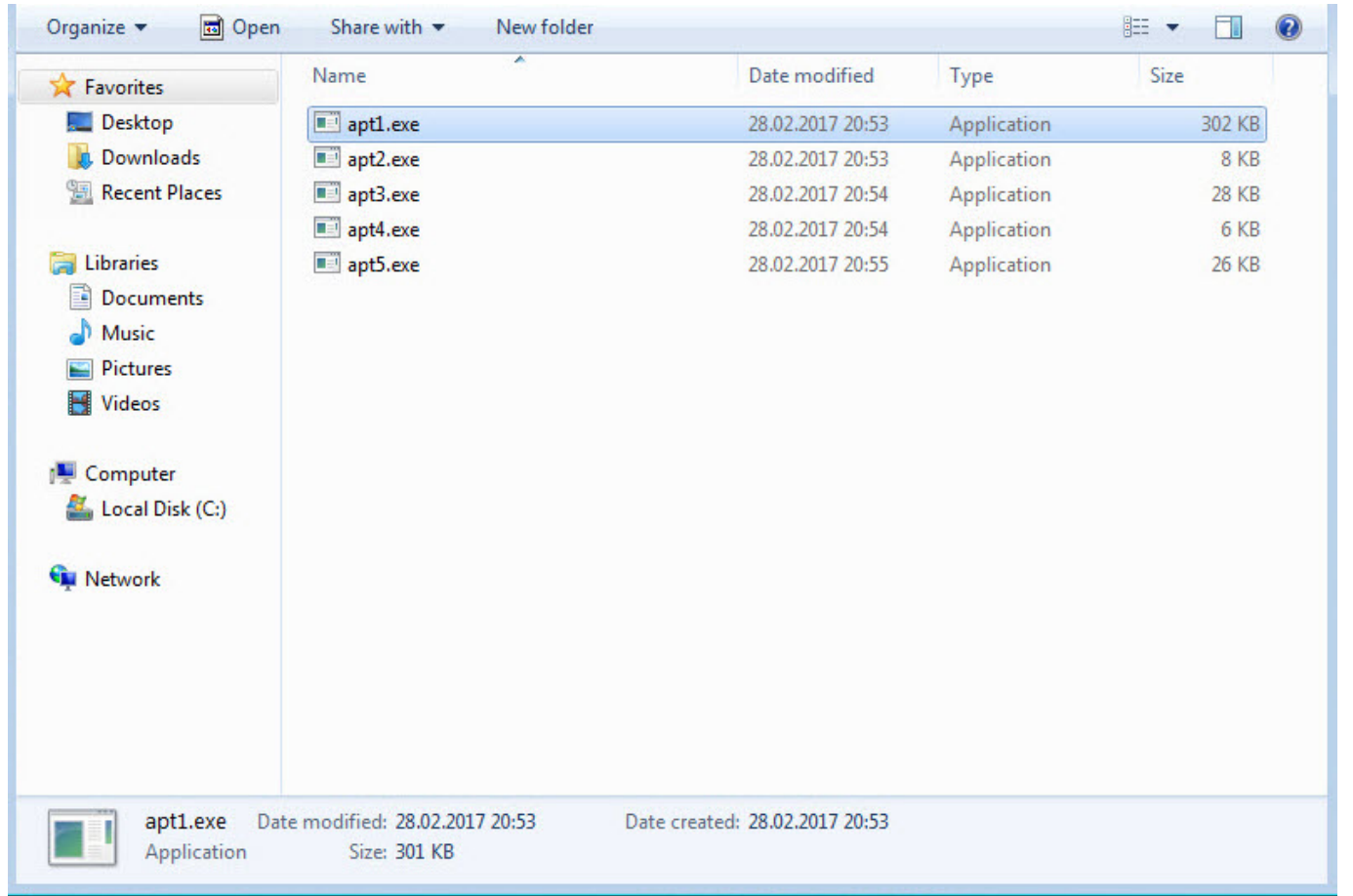


EPS dosyasını Notepad++ aracı ile incelediğimde, istismar kodu içinde yer alan birden fazla yürütülebilir dosya (executable – binary) başlıkları (MZ – 4D5A) hemen dikkatimi çekti. Bu tespit, istismar kodu içinde birden fazla yürütülebilir dosya (executable) olduğunu ve zafiyet başarıyla istismar edildikten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

ediyordu.

[illegible]

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.winator.com					
File Help					
c:\users\mert\Desktop\A3.exe	type	size	location	blacklisted (44)	item (331)
indicators (3/10)	ascii	4	-	-	\\$@H
virustotal (1/58 - 01.03.201)	ascii	4	-	-	\\$HH
dos-stub (160 bytes)	ascii	4	-	-	\\$PH
file-header (20 bytes)	ascii	4	-	-	\\$XH
optional-header (240 byte:	ascii	4	-	-	D\$ P
directories (5)	ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
sections (4)	ascii	22	-	-	A_A^A)A\A[AZAYAX_^]ZY[
libraries (2)	ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
imports (62)	ascii	22	-	-	A_A^A)A\A[AZAYAX_^]ZY[
exports (2)	ascii	14	-	-	Microsoft Word
exceptions (60)	ascii	50	-	-	The document is locked for editing by another user
tls-callbacks (n/a)	ascii	15	-	-	GetLastError = 0x
resources (n/a)	ascii	19	-	-	OpenInputDesktop =
strings (44/331)	ascii	19	-	-	SetThreadDesktop ok
debug (invalid)	ascii	10	-	-	USER32.dll
manifest (n/a)	ascii	23	-	-	Try non-patched Windows
file-version (n/a)	ascii	30	-	-	RCE works, but LPE is patched!
certificate (n/a)	ascii	6	-	-	res =
overlay (n/a)	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.winator.com					
File Help					
c:\users\mert\Desktop\A5.exe	type	size	location	blacklisted (46)	item (283)
indicators (3/11)	ascii	4	-	-	T%0L
virustotal (5/58 - 01.03.201)	ascii	4	-	-	D%4H
dos-stub (152 bytes)	ascii	14	-	-	Microsoft Word
file-header (20 bytes)	ascii	50	-	-	The document is locked for editing by another user
optional-header (224 byte:	ascii	15	-	-	GetLastError = 0x
directories (5)	ascii	19	-	-	OpenInputDesktop =
sections (4)	ascii	19	-	-	SetThreadDesktop ok
libraries (2)	ascii	10	-	-	USER32.dll
imports (63)	ascii	23	-	-	Try non-patched Windows
exports (2)	ascii	30	-	-	RCE works, but LPE is patched!
exceptions (n/a)	ascii	6	-	-	res =
tls-callbacks (n/a)	ascii	12	-	-	LpeExecMutex
resources (n/a)	ascii	16	-	-	0123456789ABCDEF
strings (46/283)	ascii	20	-	-	GetKernelVal error 0
debug (invalid)	ascii	25	-	-	ExploitTagMenuState start
manifest (n/a)	ascii	27	-	-	ExploitTagMenuState error 1
file-version (n/a)	ascii	26	-	-	ExploitTagMenuState end OK
certificate (n/a)	ascii	19	-	-	ExploitThread start
overlay (n/a)	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(0x400000) =
	ascii	41	-	-	EscalateThread VirtualAlloc(0x4000000) =
	ascii	22	-	-	EscalateThread error 2
	ascii	22	-	-	EscalateThread error 3
	ascii	22	-	-	EscalateThread wnd1 =

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

File Help

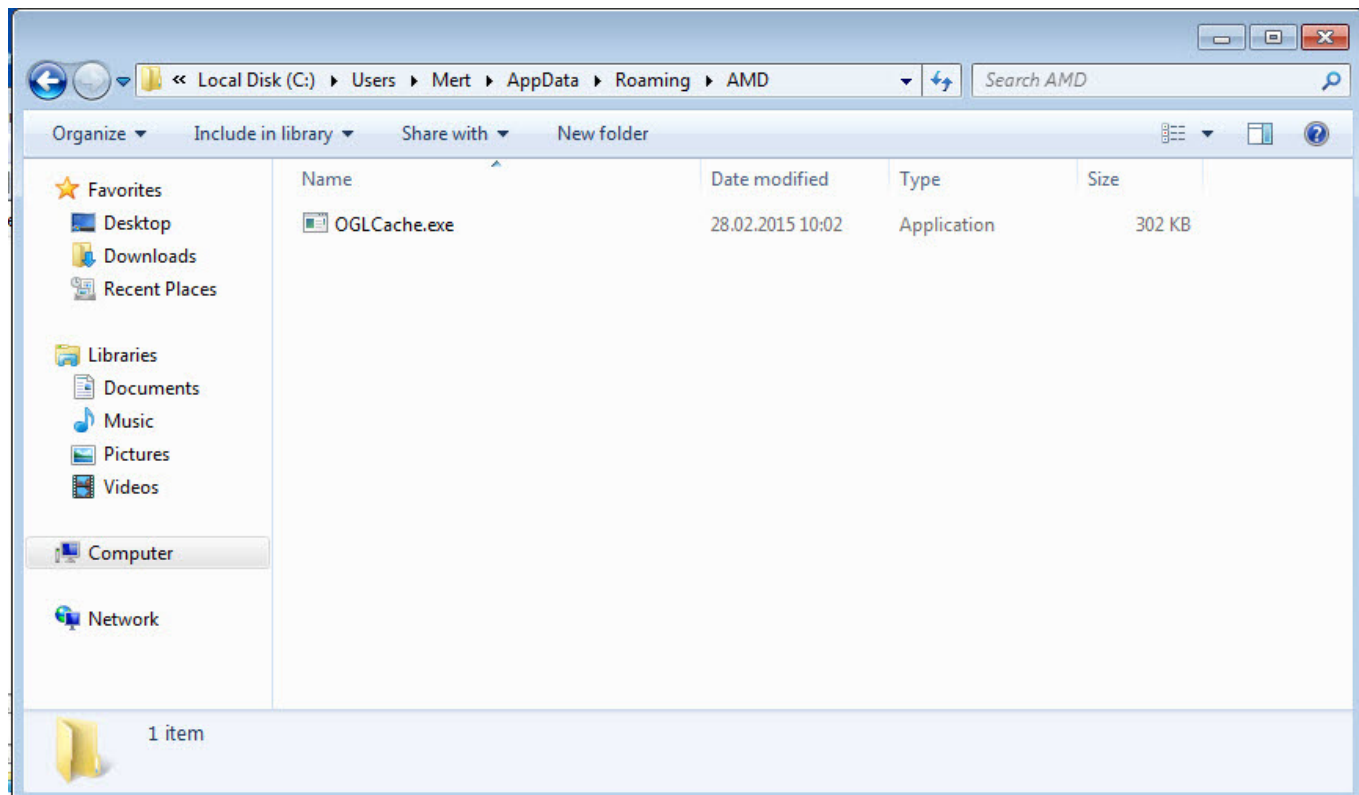
c:\users\mert\desktop\as.exe

- indicators (3/11)
- virustotal (5/58 - 01.03.2017)**
- dos-stub (152 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- 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)

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

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.

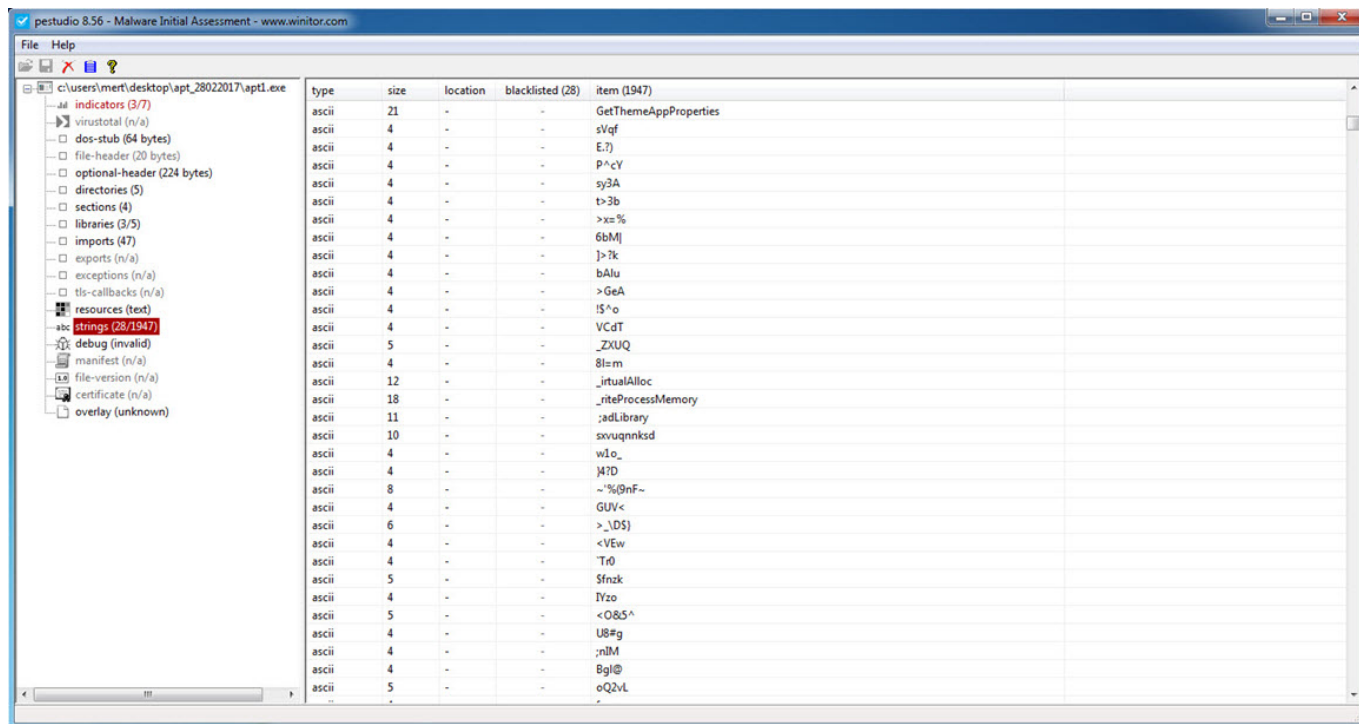


Process Monitor - Sysinternals: www.sysinternals.com

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...	SUCCESS
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...	SUCCESS
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...	SUCCESS
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...	SUCCESS
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 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
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 L
13:50:22.8367323	OGLCache.exe	2460	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale	SUCCESS

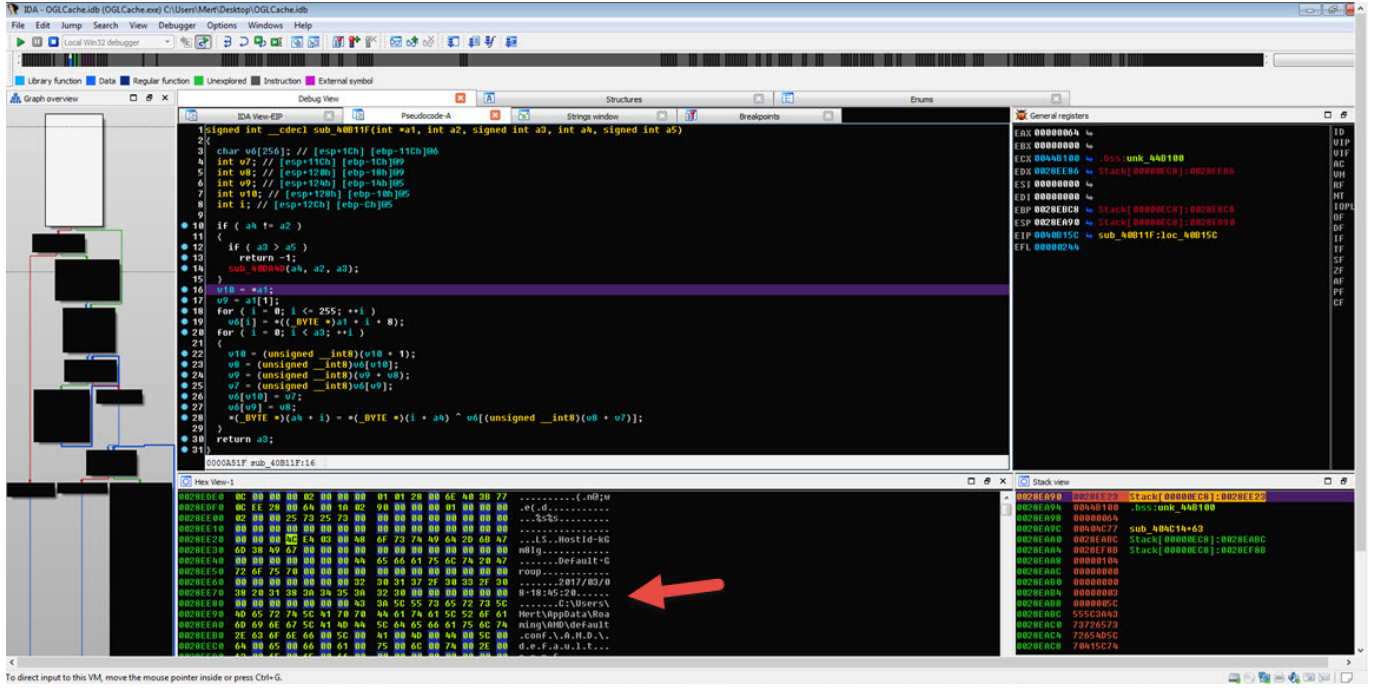
Showing 2.070 of 980.472 events (0.2%) Backed by virtual memory



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\\234\\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\\2548j\\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\\316a\\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`\\
```



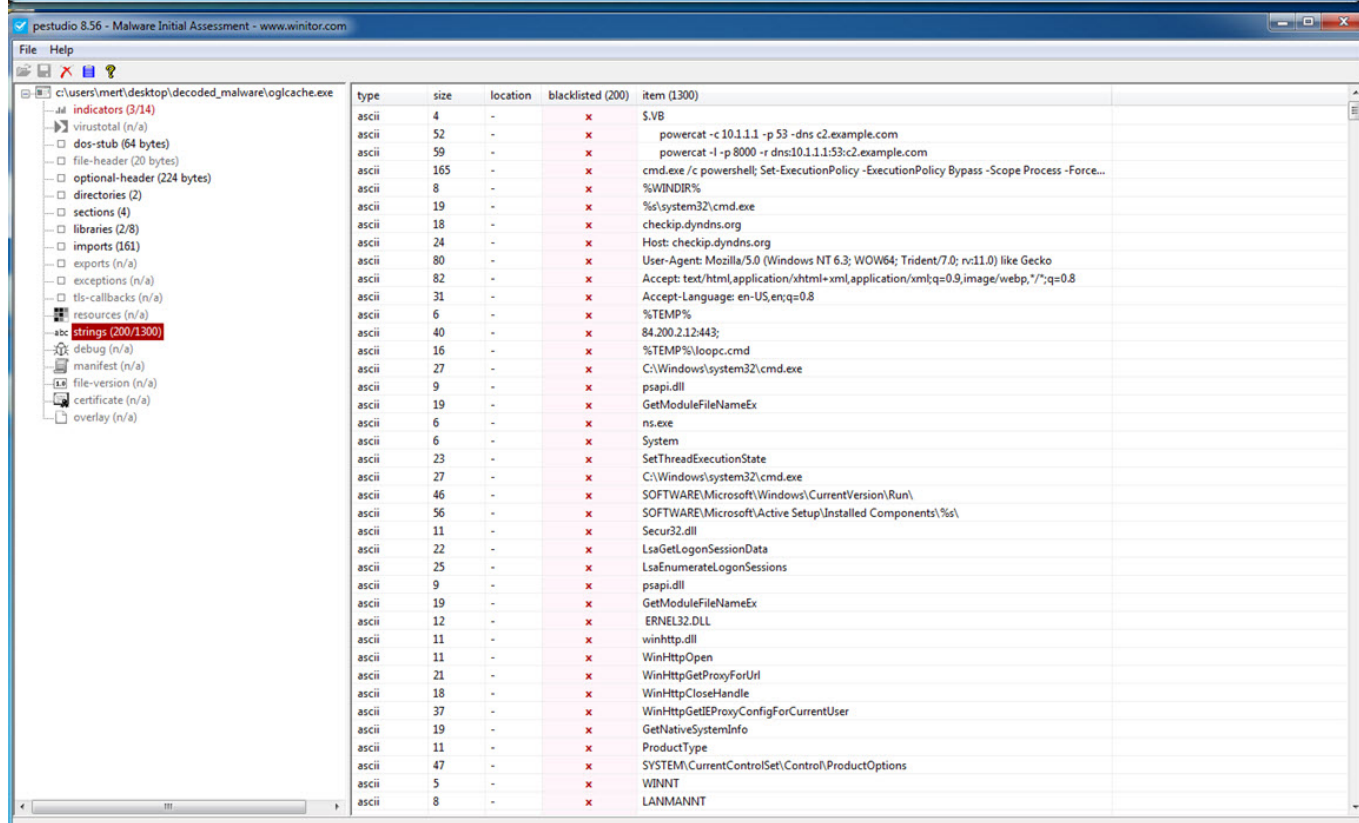
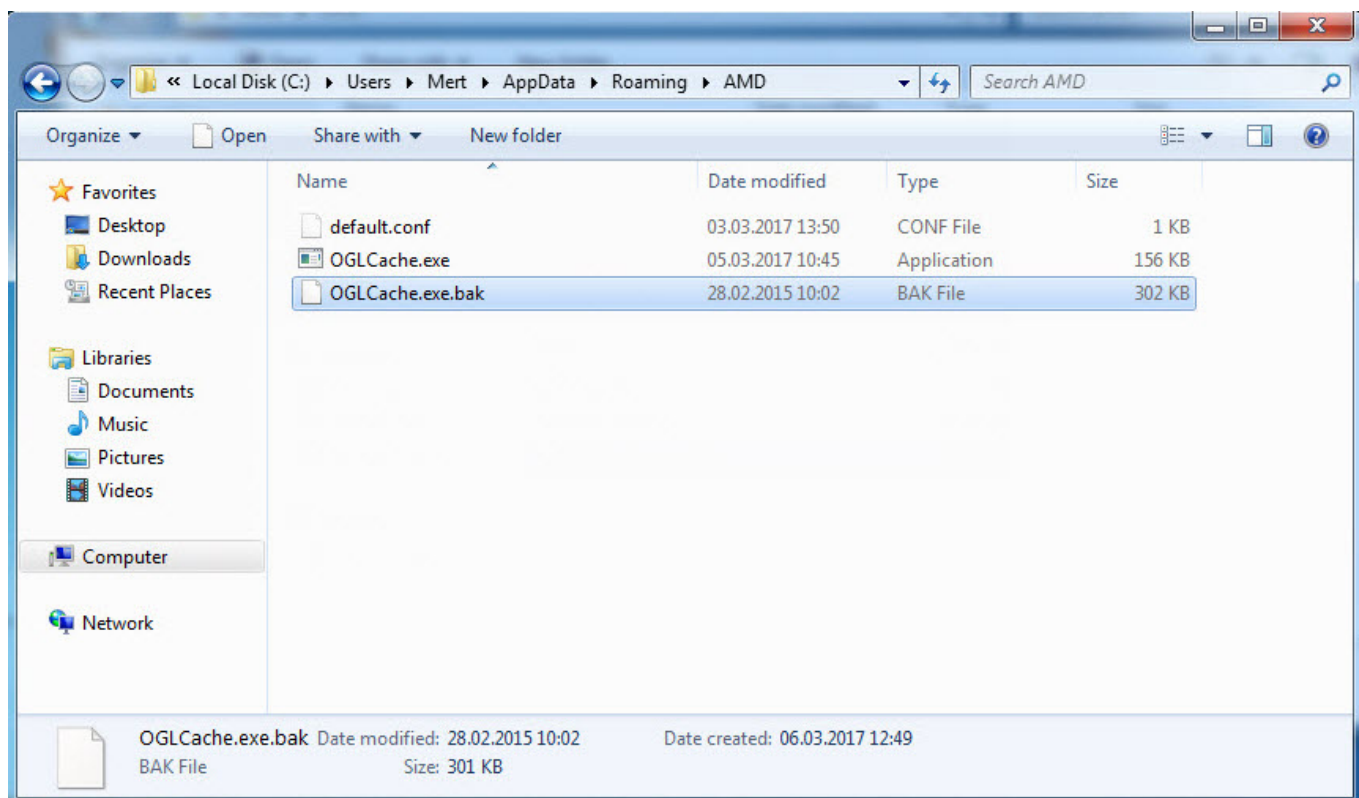
Daha sonra statik analizden WriteProcessMemory fonksiyonunu _riteProcessMemory değiştirerek kendini gizlemeye çalışıp, sistem üzerinde çalıştırıldıktan sonra GetLongPathNameA fonksiyonunu çok defa çağırarak dinamik kod analizini zorlaştırmaya çalışan bir paketleyici (packet) ile paketlenmiş olan OGLCache.exe 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.

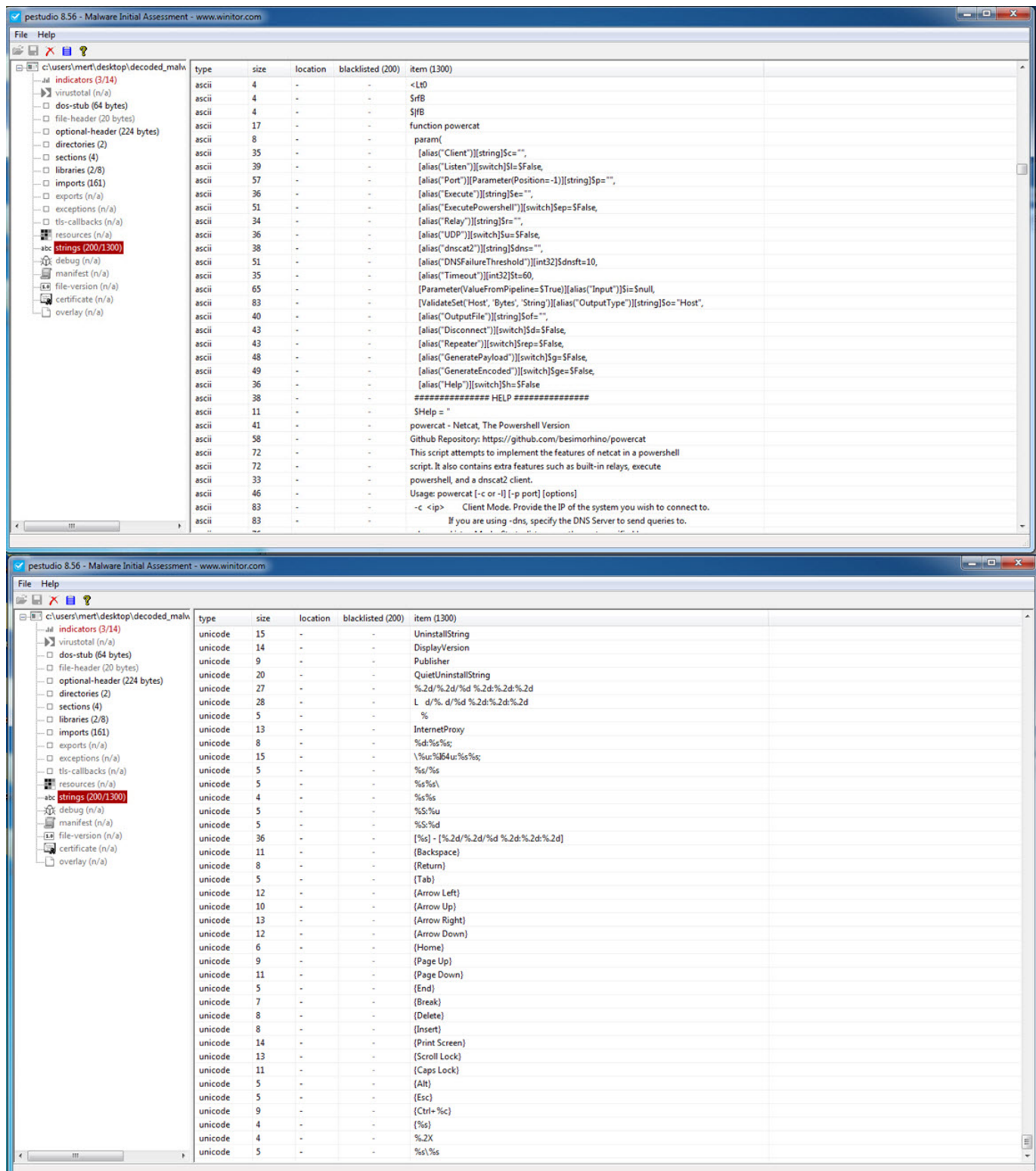
x32dbg - File: apt1.exe - PID: 96C - Module: apt1.exe - Thread: Main Thread 730

File View Debug Plugins Favourites Options Help Feb 28 2017

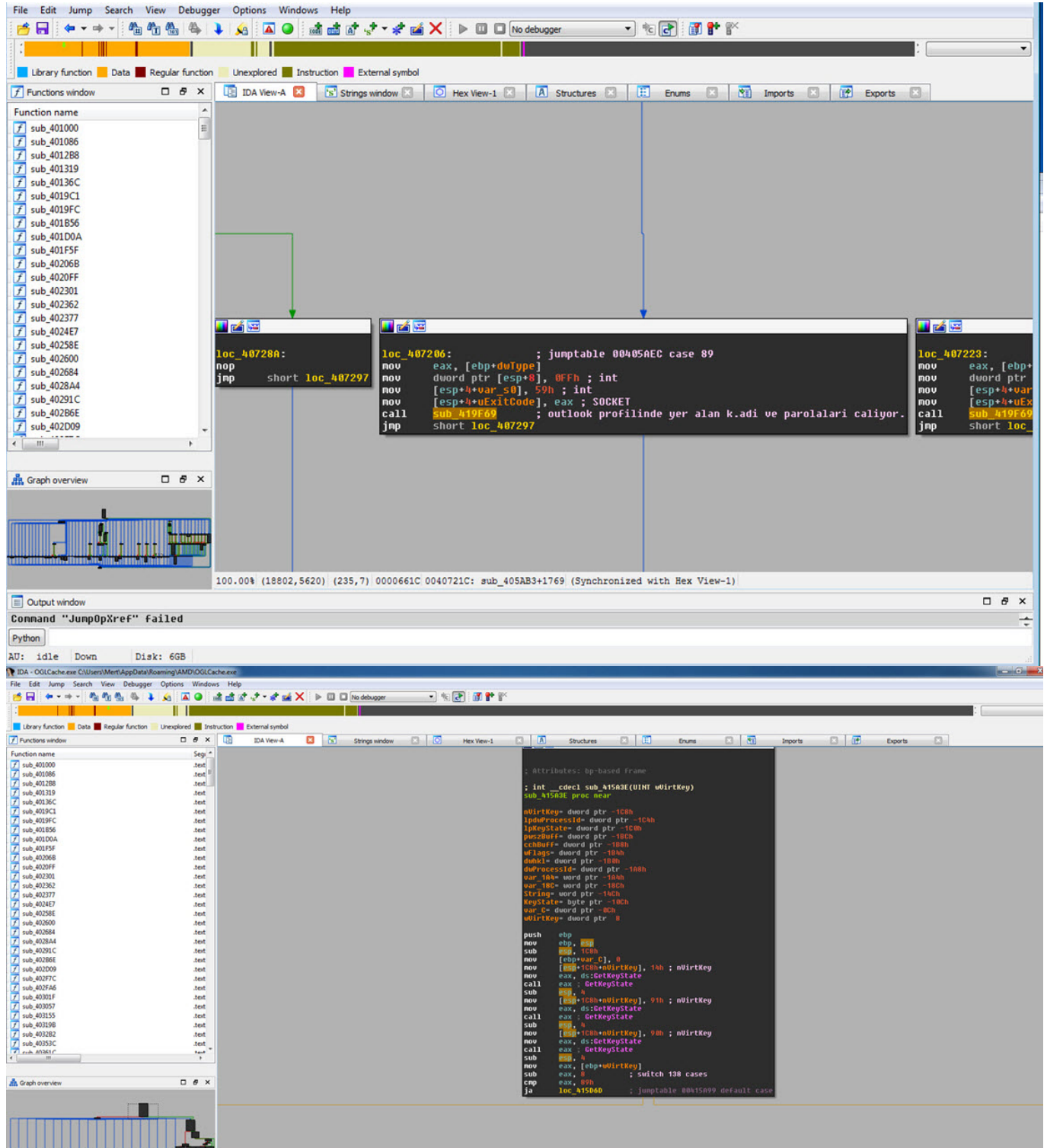
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Thread

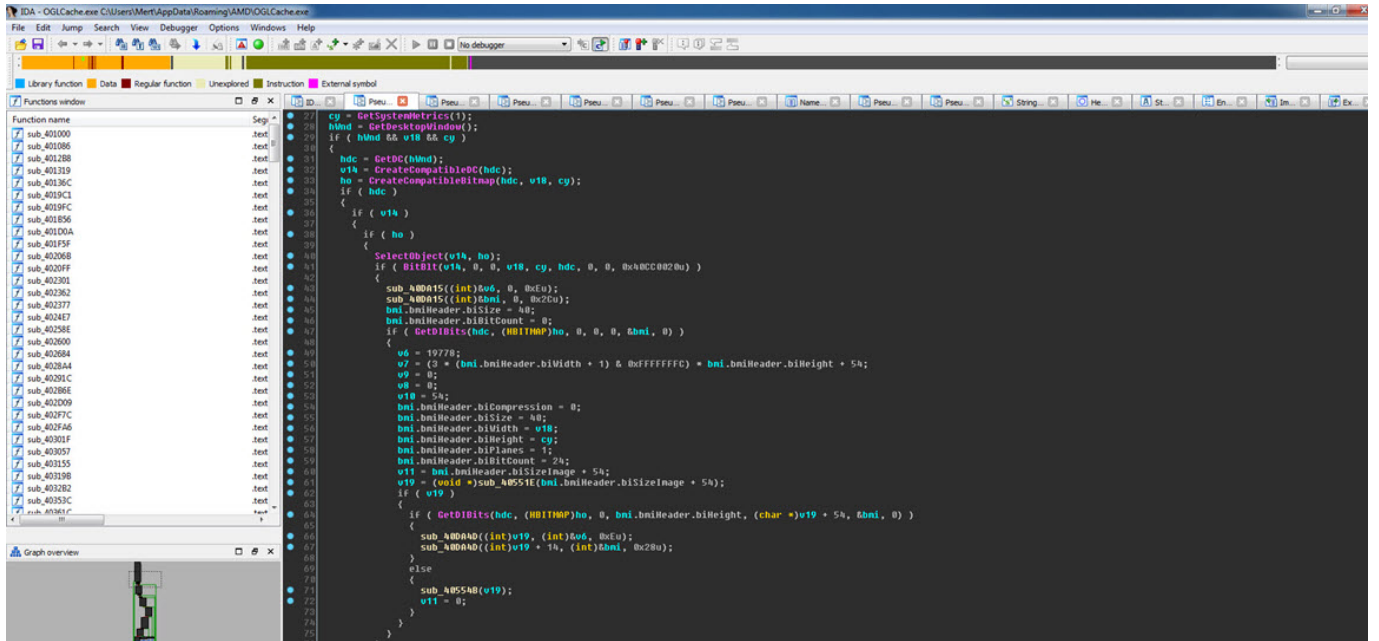
00402666 test eax, eax
00402667 jne apt1.40614E
00402668 lea ebx, dword ptr ds:[425E78]
00402669 push ebx
0040266A mov word ptr ds:[ebx], 725F
0040266B push dword ptr ds:[425E56]
0040266C call dword ptr ds:[&GetProcAddress]
0040266D push 0
0040266E push 8
0040266F push dword ptr ds:[425E4A]
00402670 push apt1.425E4A
00402671 push FFFFFFFF
00402672 push apt1.402690
00402673 push eax
00402674 ret
00402675 push apt1.425EAC
00402676 push E
00402677 push apt1.425EA1
00402678 call dword ptr ds:[&GetLongPathNameA]
00402679 cmp eax, 0
0040267A jne apt1.40614E
0040267B lea ecx, dword ptr ds:[425E4E]
0040267C cmp dword ptr ds:[ecx], FFF
0040267D j3 apt1.40614E
0040267E cmp dword ptr ds:[425E4E], 50000
0040267F j3 apt1.40614E
00402680 sbb dword ptr ds:[ecx], 300
00402681 j3 apt1.404095
00402682 add dword ptr ds:[425E8F], apt1.40614E
00402683 call dword ptr ds:[425E8F]
00402684 add byte ptr ds:[eax], 1
00402685 add byte ptr ds:[eax], 1
00402686 push apt1.425EAC
00402687
00402688
00402689
0040268A
0040268B
0040268C
0040268D
0040268E
0040268F
00402690
00402691
00402692
00402693
00402694
00402695
00402696
00402697
00402698
00402699
0040269A
0040269B
0040269C
0040269D
0040269E
0040269F
004026A0
004026A1
004026A2
004026A3
004026A4
004026A5
004026A6
004026A7
004026A8
004026A9
004026AA
004026AB
004026AC
004026AD
004026AE
004026AF
004026B0
004026B1
004026B2
004026B3
004026B4
004026B5
004026B6
004026B7
004026B8
004026B9
004026BA
004026BB
004026BC
004026BD
004026BE
004026BF
004026C0
004026C1
004026C2
004026C3
004026C4
004026C5
004026C6
004026C7
004026C8
004026C9
004026CA
004026CB
004026CC
004026CD
004026CE
004026CF
004026D0
004026D1
004026D2
004026D3
004026D4
004026D5
004026D6
004026D7
004026D8
004026D9
004026DA
004026DB
004026DC
004026DD
004026DE
004026DF
004026E0
004026E1
004026E2
004026E3
004026E4
004026E5
004026E6
004026E7
004026E8
004026E9
004026EA
004026EB
004026EC
004026ED
004026EE
004026EF
004026F0
004026F1
004026F2
004026F3
004026F4
004026F5
004026F6
004026F7
004026F8
004026F9
004026FA
004026FB
004026FC
004026FD
004026FE
004026FF
00402700
00402701
00402702
00402703
00402704
00402705
00402706
00402707
00402708
00402709
0040270A
0040270B
0040270C
0040270D
0040270E
0040270F
00402710
00402711
00402712
00402713
00402714
00402715
00402716
00402717
00402718
00402719
0040271A
0040271B
0040271C
0040271D
0040271E
0040271F
00402720
00402721
00402722
00402723
00402724
00402725
00402726
00402727
00402728
00402729
0040272A
0040272B
0040272C
0040272D
0040272E
0040272F
00402730
00402731
00402732
00402733
00402734
00402735
00402736
00402737
00402738
00402739
0040273A
0040273B
0040273C
0040273D
0040273E
0040273F
00402740
00402741
00402742
00402743
00402744
00402745
00402746
00402747
00402748
00402749
0040274A
0040274B
0040274C
0040274D
0040274E
0040274F
00402750
00402751
00402752
00402753
00402754
00402755
00402756
00402757
00402758
00402759
0040275A
0040275B
0040275C
0040275D
0040275E
0040275F
00402760
00402761
00402762
00402763
00402764
00402765
00402766
00402767
00402768
00402769
0040276A
0040276B
0040276C
0040276D
0040276E
0040276F
00402770
00402771
00402772
00402773
00402774
00402775
00402776
00402777
00402778
00402779
0040277A
0040277B
0040277C
0040277D
0040277E
0040277F
00402780
00402781
00402782
00402783
00402784
00402785
00402786
00402787
00402788
00402789
0040278A
0040278B
0040278C
0040278D
0040278E
0040278F
00402790
00402791
00402792
00402793
00402794
00402795
00402796
00402797
00402798
00402799
0040279A
0040279B
0040279C
0040279D
0040279E
0040279F
004027A0
004027A1
004027A2
004027A3
004027A4
004027A5
004027A6
004027A7
004027A8
004027A9
004027AA
004027AB
004027AC
004027AD
004027AE
004027AF
004027B0
004027B1
004027B2
004027B3
004027B4
004027B5
004027B6
004027B7
004027B8
004027B9
004027BA
004027BB
004027BC
004027BD
004027BE
004027BF
004027C0
004027C1
004027C2
004027C3
004027C4
004027C5
004027C6
004027C7
004027C8
004027C9
004027CA
004027CB
004027CC
004027CD
004027CE
004027CF
004027D0
004027D1
004027D2
004027D3
004027D4
004027D5
004027D6
004027D7
004027D8
004027D9
004027DA
004027DB
004027DC
004027DD
004027DE
004027DF
004027E0
004027E1
004027E2
004027E3
004027E4
004027E5
004027E6
004027E7
004027E8
004027E9
004027EA
004027EB
004027EC
004027ED
004027EE
004027EF
004027F0
004027F1
004027F2
004027F3
004027F4
004027F5
004027F6
004027F7
004027F8
004027F9
004027FA
004027FB
004027FC
004027FD
004027FE
004027FF
00402800
00402801
00402802
00402803
00402804
00402805
00402806
00402807
00402808
00402809
0040280A
0040280B
0040280C
0040280D
0040280E
0040280F
00402810
00402811
00402812
00402813
00402814
00402815
00402816
00402817
00402818
00402819
0040281A
0040281B
0040281C
0040281D
0040281E
0040281F
00402820
00402821
00402822
00402823
00402824
00402825
00402826
00402827
00402828
00402829
0040282A
0040282B
0040282C
0040282D
0040282E
0040282F
00402830
00402831
00402832
00402833
00402834
00402835
00402836
00402837
00402838
00402839
0040283A
0040283B
0040283C
0040283D
0040283E
0040283F
00402840
00402841
00402842
00402843
00402844
00402845
00402846
00402847
00402848
00402849
0040284A
0040284B
0040284C
0040284D
0040284E
0040284F
00402850
00402851
00402852
00402853
00402854
00402855
00402856
00402857
00402858
00402859
0040285A
0040285B
0040285C
0040285D
0040285E
0040285F
00402860
00402861
00402862
00402863
00402864
00402865
00402866
00402867
00402868
00402869
0040286A
0040286B
0040286C
0040286D
0040286E
0040286F
00402870
00402871
00402872
00402873
00402874
00402875
00402876
00402877
00402878
00402879
0040287A
0040287B
0040287C
0040287D
0040287E
0040287F
00402880
00402881
00402882
00402883
00402884
00402885
00402886
00402887
00402888
00402889
0040288A
0040288B
0040288C
0040288D
0040288E
0040288F
00402890
00402891
00402892
00402893
00402894
00402895
00402896
00402897
00402898
00402899
0040289A
0040289B
0040289C
0040289D
0040289E
0040289F
004028A0
004028A1
004028A2
004028A3
004028A4
004028A5
004028A6
004028A7
004028A8
004028A9
004028AA
004028AB
004028AC
004028AD
004028AE
004028AF
004028B0
004028B1
004028B2
004028B3
004028B4
004028B5
004028B6
004028B7
004028B8
004028B9
004028BA
004028BB
004028BC
004028BD
004028BE
004028BF
004028C0
004028C1
004028C2
004028C3
004028C4
004028C5
004028C6
004028C7
004028C8
004028C9
004028CA
004028CB
004028CC
004028CD
004028CE
004028CF
004028D0
004028D1
004028D2
004028D3
004028D4
004028D5
004028D6
004028D7
004028D8
004028D9
004028DA
004028DB
004028DC
004028DD
004028DE
004028DF
004028E0
004028E1
004028E2
004028E3
004028E4
004028E5
004028E6
004028E7
004028E8
004028E9
004028EA
004028EB
004028EC
004028ED
004028EE
004028EF
004028F0
004028F1
004028F2
004028F3
004028F4
004028F5
004028F6
004028F7
004028F8
004028F9
004028FA
004028FB
004028FC
004028FD
004028FE
004028FF
00402900
00402901
00402902
00402903
00402904
00402905
00402906
00402907
00402908
00402909
0040290A
0040290B
0040290C
0040290D
0040290E
0040290F
00402910
00402911
00402912
00402913
00402914
00402915
00402916
00402917
00402918
00402919
0040291A
0040291B
0040291C
0040291D
0040291E
0040291F
00402920
00402921
00402922
00402923
00402924
00402925
00402926
00402927
00402928
00402929
0040292A
0040292B
0040292C
0040292D
0040292E
0040292F
00402930
00402931
00402932
00402933
00402934
00402935
00402936
00402937
00402938
00402939
0040293A
0040293B
0040293C
0040293D
0040293E
0040293F
00402940
00402941
00402942
00402943
00402944
00402945
00402946
00402947
00402948
00402949
0040294A
0040294B
0040294C
0040294D
0040294E
0040294F
00402950
00402951
00402952
00402953
00402954
00402955
00402956
00402957
00402958
00402959
0040295A
0040295B
0040295C
0040295D
0040295E
0040295F
00402960
00402961
00402962
00402963
00402964
00402965
00402966
00402967
00402968
00402969
0040296A
0040296B
0040296C
0040296D
0040296E
0040296F
00402970
00402971
00402972
00402973
00402974
00402975
00402976
00402977
00402978
00402979
0040297A
0040297B
0040297C
0040297D
0040297E
0040297F
00402980
00402981
00402982
00402983
00402984
00402985
00402986
00402987
00402988
00402989
0040298A
0040298B
0040298C
0040298D
0040298E
0040298F
00402990
00402991
00402992
00402993
00402994
00402995
00402996
00402997
00402998
00402999
0040299A
0040299B
0040299C
0040299D
0040299E
0040299F
004029A0
004029A1
004029A2
004029A3
004029A4
004029A5
004029A6
004029A7
004029A8
004029A9
004029AA
004029AB
004029AC
004029AD
004029AE
004029AF
004029B0
004029B1
004029B2
004029B3
004029B4
004029B5
004029B6
004029B7
004029B8
004029B9
004029BA
004029BB
004029BC
004029BD
004029BE
004029BF
004029C0
004029C1
004029C2
004029C3
004029C4
004029C5
004029C6
004029C7
004029C8
004029C9
004029CA
004029CB
004029CC
004029CD
004029CE
004029CF
004029D0
004029D1
004029D2
004029D3
004029D4
004029D5
004029D6
004029D7
004029D8
004029D9
004029DA
004029DB
004029DC
004029DD
004029DE
004029DF
004029E0
004029E1
004029E2
004029E3
004029E4
004029E5
004029E6
004029E7
004029E8
004029E9
004029EA
004029EB
004029EC
004029ED
004029EE
004029EF
004029F0
004029F1
004029F2
004029F3
004029F4
004029F5
004029F6
004029F7
004029F8
004029F9
004029FA
004029FB
004029FC
004029FD
004029FE
004029FF
00402A00
00402A01
00402A02
00402A03
00402A04
00402A05
00402A06
00402A07
00402A08
00402A09
00402A0A
00402A0B
00402A0C
00402A0D
00402A0E
00402A0F
00402A10
00402A11
00402A12
00402A13
00402A14
00402A15
00402A16
00402A17
00402A18
00402A19
00402A1A
00402A1B
00402A1C
00402A1D
00402A1E
00402A1F
00402A20
00402A21
00402A22
00402A23
00402A24
00402A25
00402A26
00402A27
00402A28
00402A29
00402A2A
00402A2B
00402A2C
00402A2D
00402A2E
00402A2F
00402A30
00402A31
00402A32
00402A33
00402A34
00402A35
00402A36
00402A37
00402A38
00402A39
00402A3A
00402A3B
00402A3C
00402A3D
00402A3E
00402A3F
00402A40
00402A41
00402A42
00402A43
00402A44
00402A45
00402A46
00402A47
00402A48
00402A49
00402A4A
00402A4B
00402A4C
00402A4D
00402A4E
00402A4F
00402A50
00402A51
00402A52
00402A53
00402A54
00402A55
00402A56
00402A57
00402A58
00402A59
00402A5A
00402A5B
00402A5C
00402A5D
00402A5E
00402A5F
00402A60
00402A61
00402A62
00402A63
00402A64
00402A65
00402A66
00402A67
00402A68
00402A69
00402A6A
00402A6B
00402A6C
00402A6D
00402A6E
00402A6F
00402A70
00402A71
00402A72
00402A73
00402A74
00402A75
00402A76
00402A77
00402A78
00402A79
00402A7A
00402A7B
00402A7C
00402A7D
00402A7E
00402A7F
00402A80
00402A81
00402A82
00402A83
00402A84
00402A85
00402A86
00402A87
00402A88
00402A89
00402A8A
00402A8B
00402A8C
00402A8D
00402A8E
00402A8F
00402A90
00402A91
00402A92
00402A93
00402A94
00402A95
00402A96
00402A97
00402A98
00402A99
00402A9A
00402A9B
00402A9C
00402A9D
00402A9E
00402A9F
00402AA0
00402AA1
00402AA2
00402AA3
00402AA4
00402AA5
00402AA6
00402AA7
00402AA8
00402AA9
00402AAA
00402AAB
00402AAC
00402AAD
00402AAE
00402AAF
00402AB0
00402AB1
00402AB2
00402AB3
00402AB4
00402AB5
00402AB6
00402AB7
00402AB8
00402AB9
00402ABA
00402ABB
00402ABC
00402ABD
00402ABE
00402ABF
00402AC0
00402AC1
00402AC2
00402AC3
00402AC4
00402AC5
00402AC6
00402AC7
00402AC8
00402AC9
00402ACA
00402ACB
00402ACC
00402ACD
00402ACE
00402ACF
00402AD0
00402AD1
00402AD2
00402AD3
00402AD4
00402AD5
00402AD6
00402AD7
00402AD8
00402AD9
00402ADA
00402ADB
00402ADC
00402ADD
00402ADE
00402ADF
00402AE0
00402AE1
00402AE2
00402AE3
00402AE4
00402AE5
00402AE6
00402AE7
00402AE8
00402AE9
00402AEA
00402AEB
00402AEC
00402AED
00402AEE
00402AEF
00402AF0
00402AF1
00402AF2
00402AF3
00402AF4
00402AF5
00402AF6
00402AF7
00402AF8
00402AF9
00402afa
00402afb
00402afc
00402afd
00402afe
00402aff
00402b00
00402b01
00402b02
00402b03
00402b04
00402b05
00402b06
00402b07
00402b08
00402b09
00402b0a
00402b0b
00402b0c
00402b0d
00402b0e
00402b0f
00402b10
00402b11
00402b12
00402b13
00402b14
00402b15
00402b16
00402b17
00402b18
00402b19
00402b1a
00402b1b
00402b1c
00402b1d
00402b1e
00402b1f
00402b20
00402b21
00402b22
00402b23
00402b24
00402b25
00402b26
00402b27
00402b28
00402b29
00402b2a
00402b2b
00402b2c





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.





stackoverflow

Questions Jobs Documentation Tags Users

Search...

Log In Sign Up

1

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 surprise but would still greatly appreciate any explanations.

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

```

#define _CRT_SECURE_NO_DEPRECATED
#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);
    //Save the captured bitmap to a file. //Place holder - Put your code here to save the file
    ReleaseDC(hDesktopDC, hDesktopDC);
    DeleteDC(hCaptureDC);
    DeleteObject(hCaptureBitmap);
}

```

c++ windows screenshot bitmap hdc

share improve this question

edited Jul 28 '15 at 21:59

asked Jul 28 '15 at 21:31

Corbin

6 +2

2

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 GitHub

Want a python job?

Project Lead - Small Team of Experts - 100% Remote, Flexible Hours

Analytics Firm - 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?

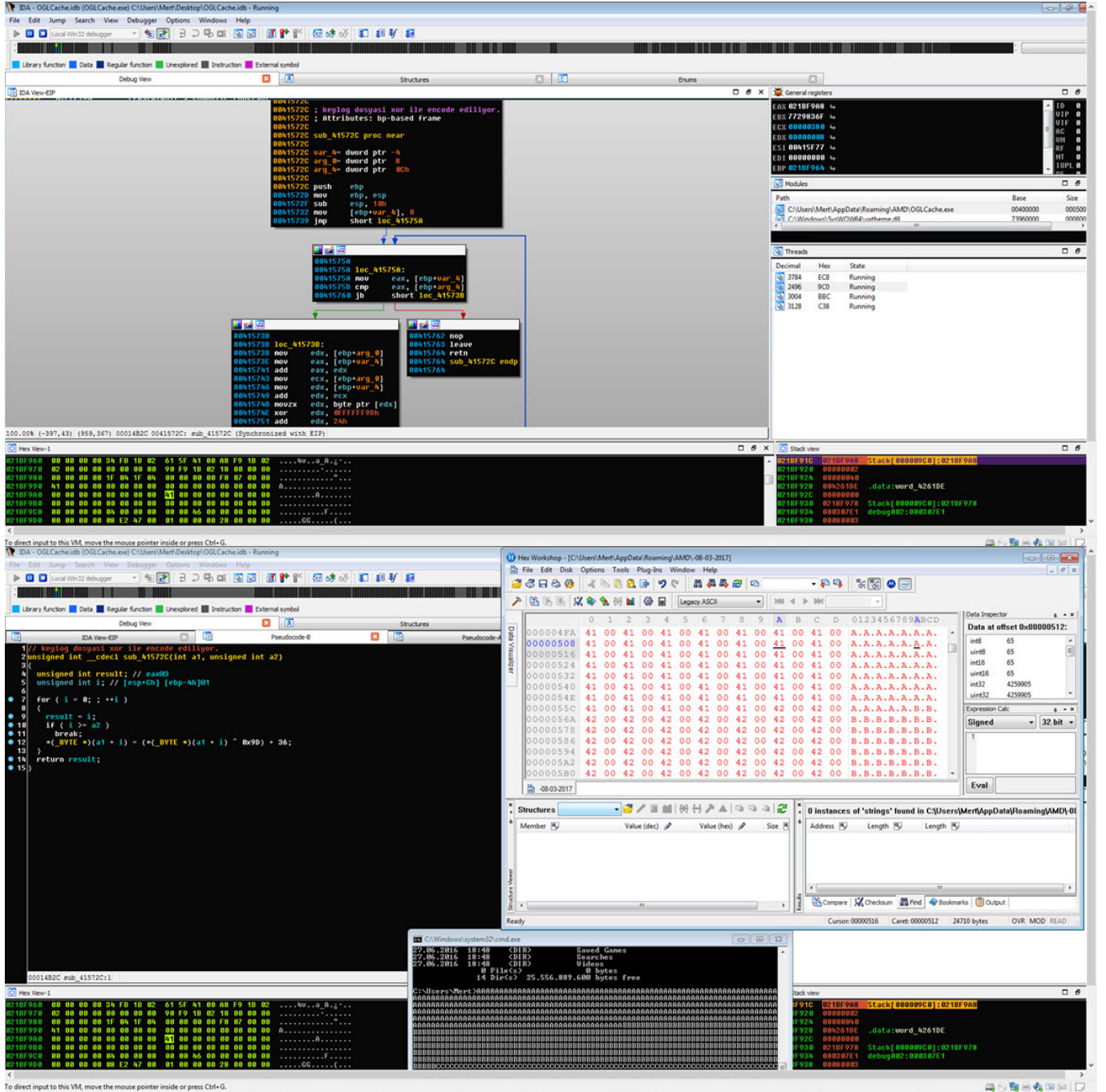
1

Are there any bitblt alternatives without the slowness?

0

How to get the screen capture of other full screen games using DXGI?

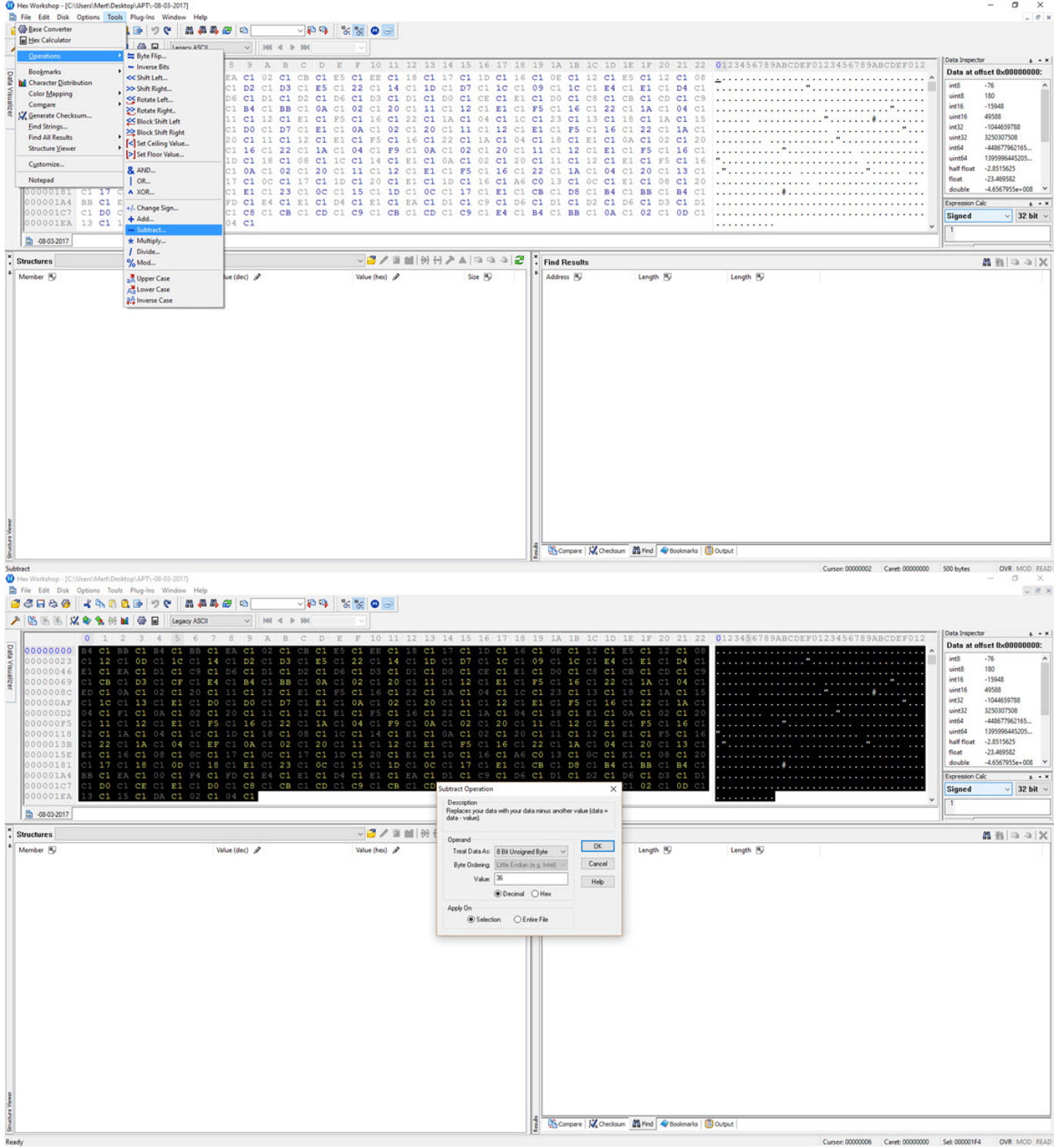
Analizimi tamamlamadan önce zararlı yazılımda yer alan fakat analizim süresince devreye girmeyen tuş kaydından sorumlu olan fonksiyonu bulup, hızlıca göz atmaya karar verdim. 0041572C adresinde yer alan tuş kaydından sorumlu olan fonksiyonu tespit ettikten sonra programın akışını değiştirerek, akışın 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 ($-36 \wedge 9D$) yaptığımda ise okunaklı olmayan bastığım tuş bilgilerini okunaklı hale çevirebildim.

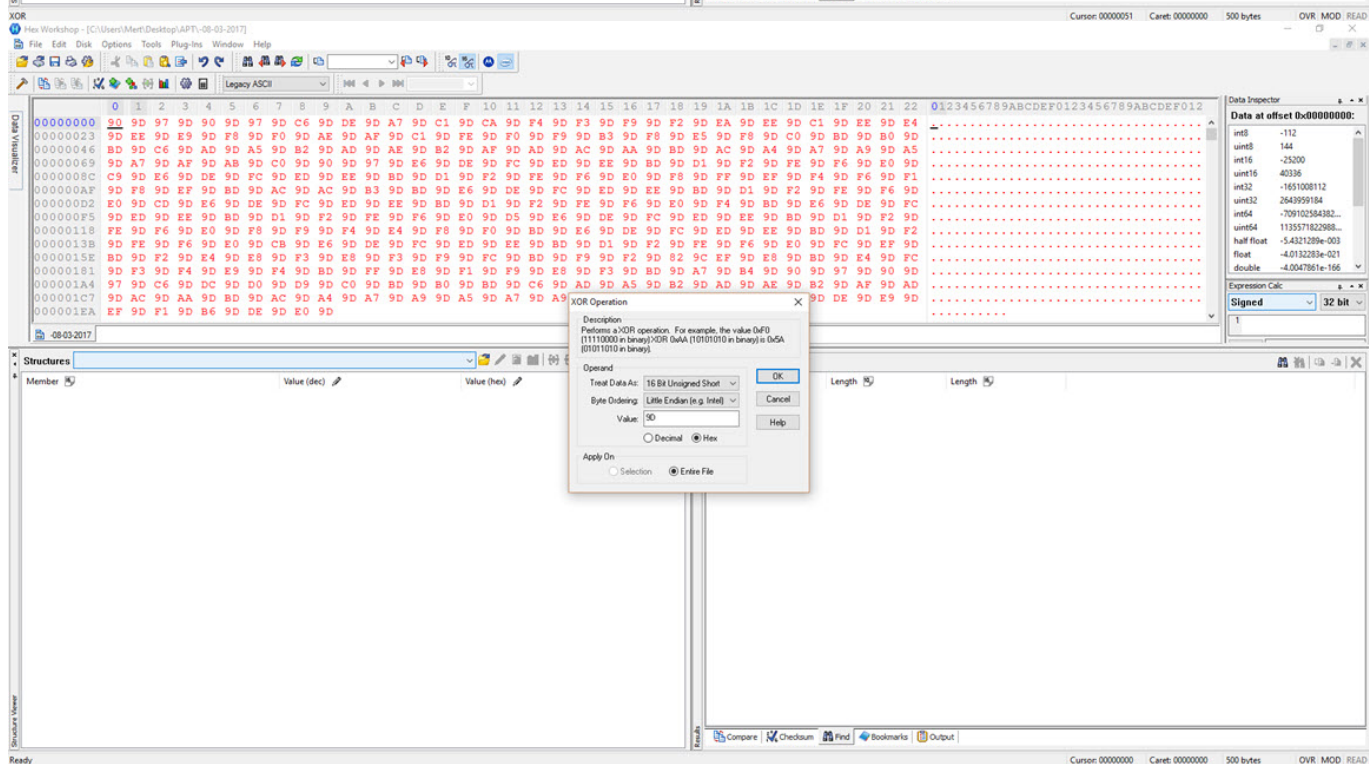
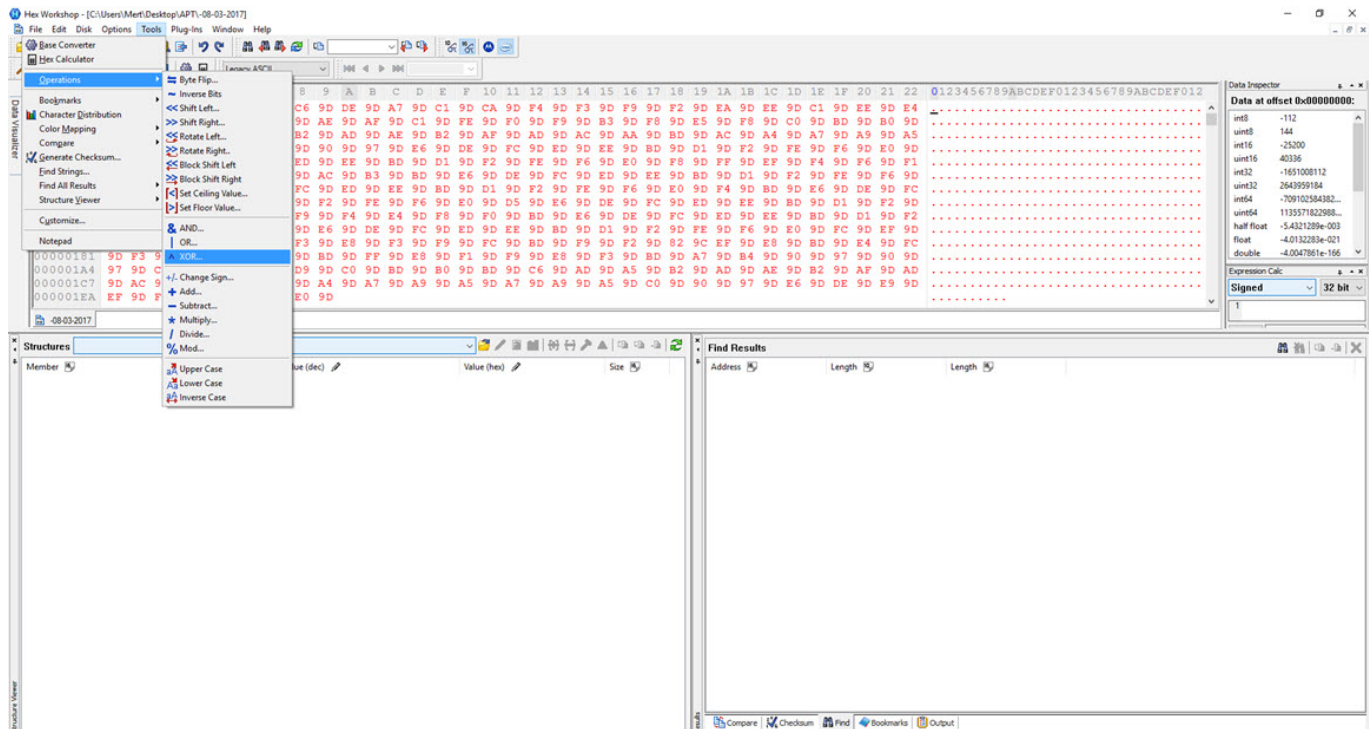


Sonuç itibariyle organize siber suç çetelerinin hedef aldıkları kurumlara saldırırken devlet destekli (nation state) siber saldırganlardan çok da geri kalmadıklarını görebiliyoruz. Çıta'yı her daim yükseltelen siber saldırganlarla mücadele adına FireEye (Mandiant)'ın da raporunda yer verdiği üzere özellikle 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 Hediye Var #11 oyununun çözüm yolunu da içermektedir.





Hex Workshop - [C:\Users\Merf\Desktop\APTI-08-03-2017]

File Edit Disk Options Tools Plug-ins Window Help

Legacy ASCII

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
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
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
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 68 00 7D 00
0000008C 54 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 68 00 7D 00 65 00 62 00 72 00 69 00 6B 00 6C
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 68 00
000000D2 7D 00 50 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00 63 00 68 00 7D 00 69 00 20 00 7B 00 43 00 61
000000F5 00 70 00 73 00 20 00 4C 00 6F 00 63 00 68 00 7D 00 48 00 7B 00 43 00 61 00 70 00 73 00 20 00 4C 00 6F 00
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 00
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 68 00 7D 00 61 00 72 00
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
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
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
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
000001EA 72 00 6C 00 2B 00 43 00 7D 00

08-03-2017

Structures

Member Value (dec) Value (hex) Size

Find Results

Address Length Length

Ready

Cursor: 0000008B Caret: 00000000 500 bytes OVR MOD READ

Data Inspector

Data at offset 0x00000000:

int8 13
uint8 13
int16 13
uint16 13
int32 655373
uint32 655373
int64 2814805602336...
uint64 2814805602336...
half float 7.7486036e-007
float 8.1837338e-040
double 1.3904987e-308

Expression Calc

Signed 32 bit

1