BGA
SECURITY

BİLGİ GÜVENLİĞİ AKADEMİSİ

- 2017 -

BGA Bilgi Güvenliği A.Ş

BGA Security Hakkında

Siber güvenlik dünyasına yönelik, yenilikçi profesyonel çözümleri ile katkıda bulunmak amacı ile 2008 yılında kurulan BGA Bilgi Güvenliği A.Ş. stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında büyük ölçekli çok sayıda kuruma hizmet vermektedir.

Gerçekleştirdiği vizyoner danışmanlık projeleri ve nitelikli eğitimleri ile sektörde saygın bir yer kazanan BGA Bilgi Güvenliği, kurulduğu günden bugüne kadar alanında lider finans, enerji, telekom ve kamu kuruluşları ile 1.000'den fazla eğitim ve danışmanlık projelerine imza atmıştır.

SWIFT TEHDİTLERİ

İbrahim AKGÜL

BGA SECURITY

Finansal Zararlılar

Son Kullanıcıyı Hedef Alan

Doğrudan Hırsızlık

- Zeus
- IcelX
- Carberp
- Tinba
- Vawtrak
- Bebloh
- Citadel
- Gameover Zeus
- Shylock
- Bugat
- Gozi
- Torpig

Sırtından Geçinme (CryptoConcurrency)

- Mal/Miner-C (2016 model)

Bankaları Hedef Alan

ATM

- Alice
- Ripper

SWIFT

- Carbanak
- Odinaff
- BangSwift
- Batel

KURUM

- Shamoon


SWIFT
50 EURO

SWIFT Nedir?

Society for Worldwide Inter bank Financial Telecommunication

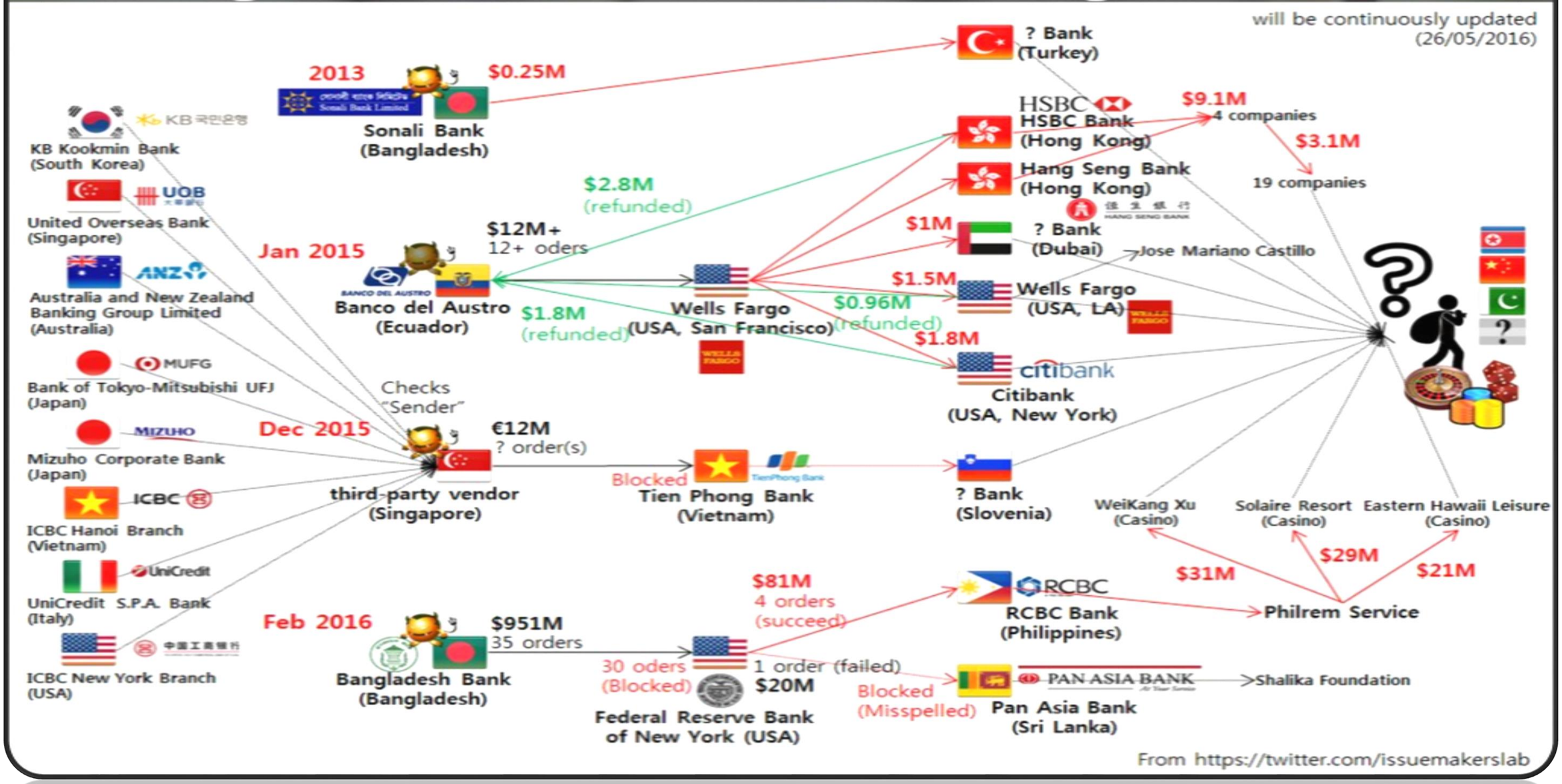
- 1973 de 240 banka ile başladı. Bugün 11.000 kullanıcısı var.
- Çok büyük paraların transfer edildiği bir ödeme sistemi,
- Ülkemiz için yurtdışına para göndermek ve almak istendiğinde öncelikli tercih,
- Her Banka BIC olarak bilinen kendine has bir Swift Code sahibidir. Tüm para transferleri bu kodlara bağlı olarak işlem görür.
- Para gönderiminde herhangi bir üst limit yoktur!
- Tüm iletişim uçtan uca **SSL** aracılığı ile gerçekleştirilir ☺

SWIFT Temelleri

- Bu sistemden yararlanmak isteyen her kurum SWIFT Alliance üyesi olmalıdır.
- Kurumlar kendilerine ait tekil bir SWIFT Code (BIC) ile tanımlanır.
- Alliance Access, Alliance Gateway gibi uygulamaları üzerinden Bankalar arası para transferlerini içeren mesajlaşma alt yapısını sunar.
- Para transferlerini de içeren mesajlar Alliance Access uygulaması ile dosya tabanlı in/out klasörleri yolu ile sağlanır (FileAct). (Swift 30 yıllık bu ilkel yapıyı XML tabanlı yeni nesil bir protokolle değiştirmek için kolları sıvadı)
- Ülkemizde çoğu banka Alliance uygulamalarını ortak bir sağlayıcı üzerinden kullanmaktadır!!!


S.W.I.F.T.
HACKED

Hacking the Worldwide Banking System (Using fraudulent SWIFT messages)



Saldırı Vektörleri

Hedefe Macro zararlısı içeren e-mail Gönderilir

Kurban dosyayı çalıştırır ve C&C bağlantısı sağlanmış olur.

Saldırgan girdiği sistemde hedef Swift Alliance Access sunucusuna erişir.

İncelenen altyapıya özel hazırlanan zararlı Alliance Access sunucusuna infecte edilir.

Zararlı önceden belirlenen transaction id lere göre in/out klasörünü denetler.

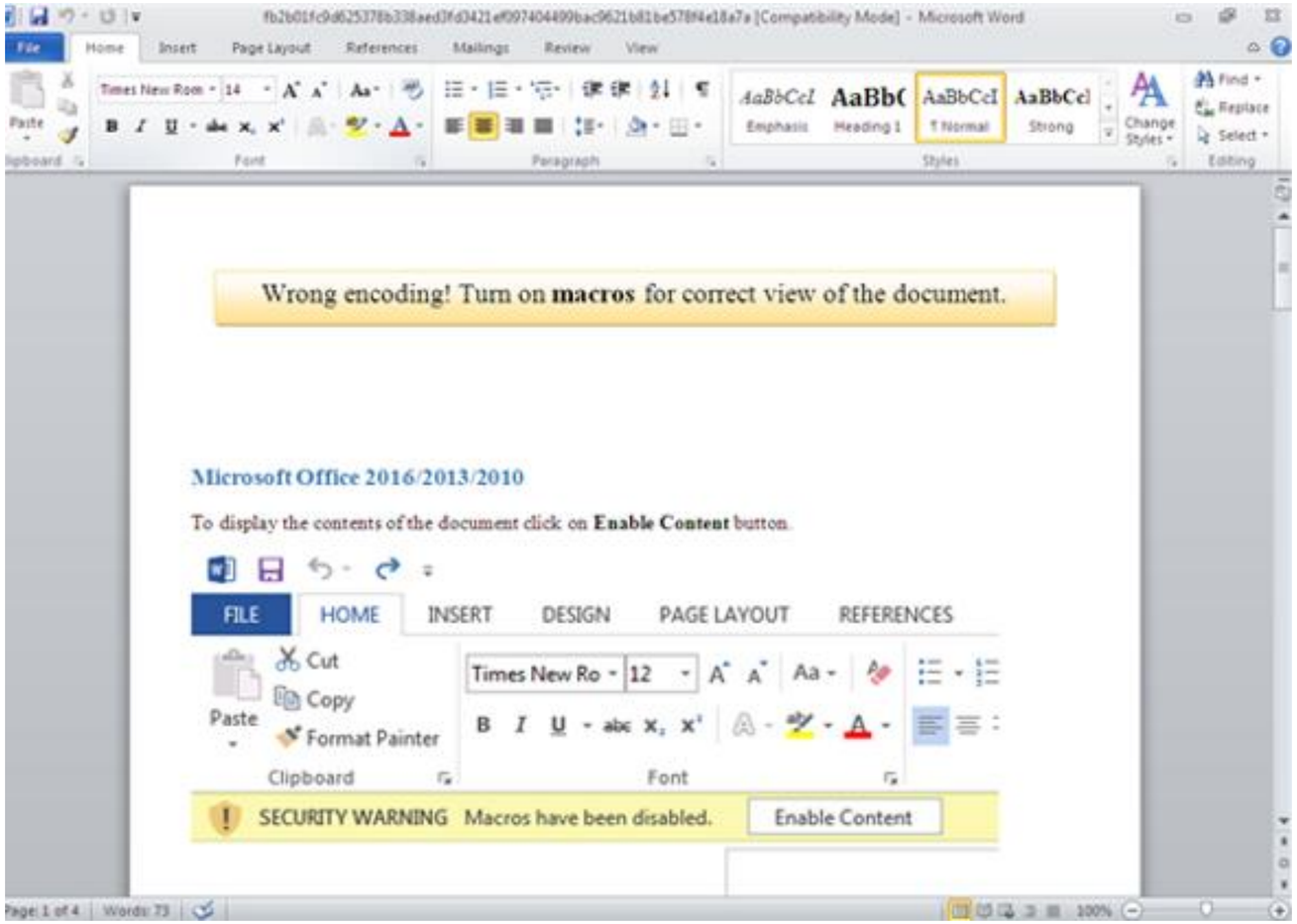
Beklenen işlem gerçekleştiğinde manipülasyon da başlamış olur.

İz bırakmamak ve Yetki kontrollerini bypass etmek için binary patch ve truncate işlemleri gerçekleştirilir.

Belgelenen her olayda, suçlular aynı yöntemi kullanıyor:

- Bankanın yerel güvenlik sistemlerini engellemek ve işlerini otomatize etmek için malware kullandılar.
- SWIFT mesajlaşma ağına eriştiler.
- Büyük bankalardaki hesaplardan nakit para transferlerini başlatmak için sahte mesajlar SWIFT yoluyla gönderildi.

Dolaşımda ki Kavramlar

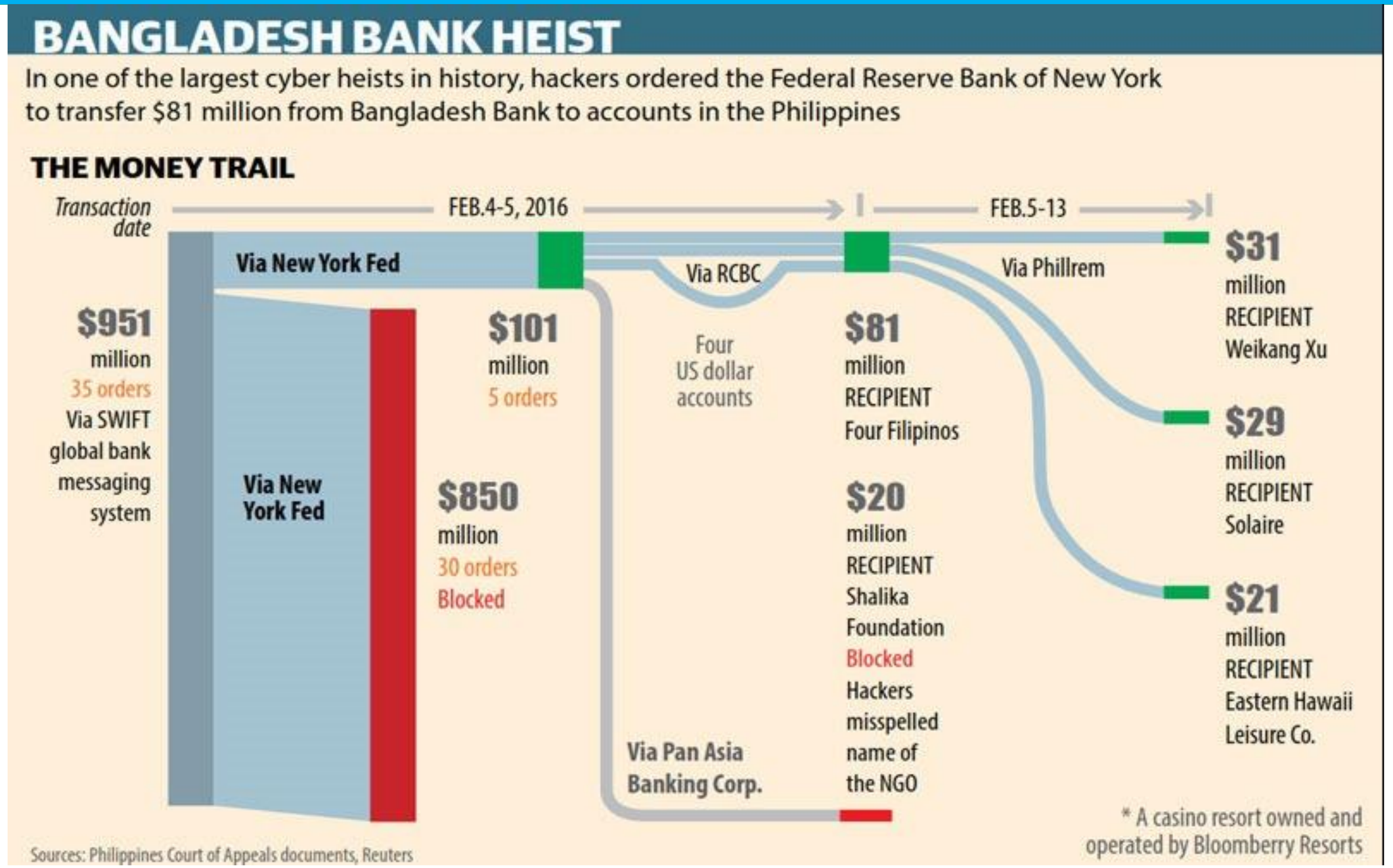


ODINAFF

Backdoor.Batel

Trojan.BanSwift

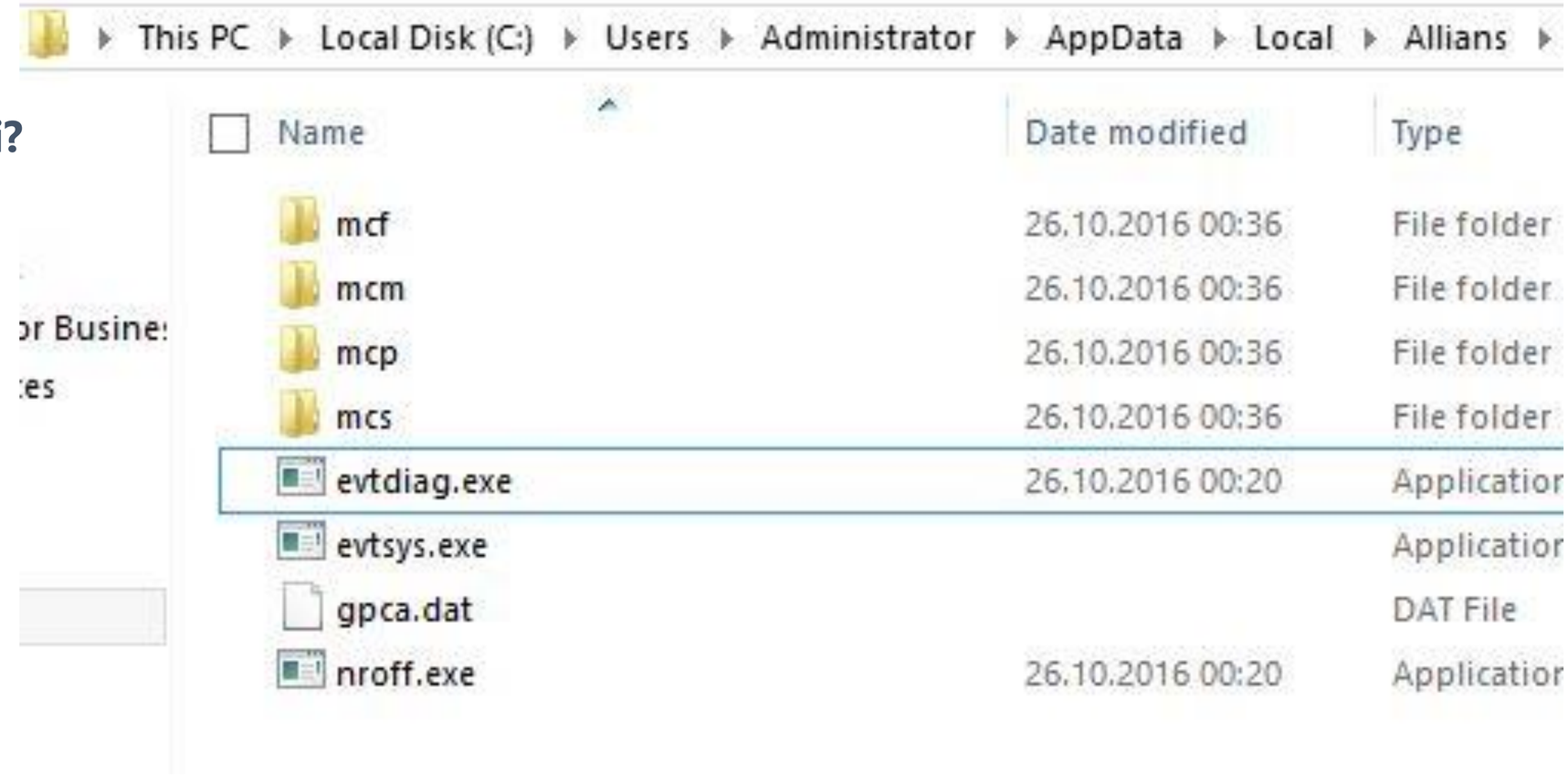
- Bangladeş Soygunu



Nasıl Çalışıyor?

Bu dosyalar buraya nasıl geldi?

- Firewall yok
- Endpoint Security yok
- DLP yok
- IPS yok
- Yetkilendirme yok
- … yok
- … yok



File View Debug Plugins Favourites Options Help Oct 10 2016

CPU | Graph | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Snowman | Handles

```
00408C51    5F                  pop edi
00408C52    5E                  pop esi                                 esi:"e9)"
00408C53    5D                  pop ebp
00408C54    83 C8 FF            or eax,FFFFFFFF
00408C57    5B                  pop ebx
00408C58    81 C4 60 06 00 00   add esp,660
00408C5E    C3                  ret
00408C5F    8B 3D 8C D1 40 00   mov edi,dword ptr ds:[<&fprintf>]
00408C65    68 8C F9 40 00      push evtdiag.40F98C                     40F98C:"set heading off;\r\n"
00408C6A    56                  push esi                                esi:"e9)"
00408C6B    FF D7               call edi                                edi:fprintf
00408C6D    83 C4 08            add esp,8
00408C70    68 74 F9 40 00      push evtdiag.40F974                     40F974:"set linesize 32567;\r\n"
00408C75    56                  push esi                                esi:"e9)"
00408C76    FF D7               call edi                                edi:fprintf
00408C78    83 C4 08            add esp,8
00408C7B    68 60 F9 40 00      push evtdiag.40F960                     40F960:"SET FEEDBACK OFF;\r\n"
00408C80    56                  push esi                                esi:"e9)"
00408C81    FF D7               call edi                                edi:fprintf
00408C83    83 C4 08            add esp,8
00408C86    68 50 F9 40 00      push evtdiag.40F950                     40F950:"SET ECHO OFF;\r\n"
00408C8B    56                  push esi                                esi:"e9)"
00408C8C    FF D7               call edi                                edi:fprintf
00408C8E    83 C4 08            add esp,8
00408C91    68 40 F9 40 00      push evtdiag.40F940                     40F940:"SET FEED OFF;\r\n"
00408C96    56                  push esi                                esi:"e9)"
00408C97    FF D7               call edi                                edi:fprintf
00408C99    83 C4 08            add esp,8
00408C9C    68 2C F9 40 00      push evtdiag.40F92C                     40F92C:"SET VERIFY OFF;\r\n"
00408CA1    56                  push esi                                esi:"e9)"
00408CA2    FF D7               call edi                                edi:fprintf
00408CA4    8B 8C 24 7C 06 00 00 mov ecx,dword ptr ss:[esp+67C]
00408CAB    83 C4 08            add esp,8
00408CAE    51                  push ecx
```

Hide FPU

```
EAX   000000B4      ''
EBX   00000000
ECX   750D2CF6      msvcrt.750D2CF6
EDX   75179C00      msvcrt.75179C00
EBP   0018FDE4
ESP   0018F644      &"e9)"
ESI   75179C68      "e9)"
EDI   750D2C10      <msvcrt.fprintf>

EIP   00408CB7      evtdiag.00408CB7

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError 000000B7 (ERROR_ALREADY_EXISTS)

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

x87r0 00000000000000000000 ST0 Empty 0.000000000000000000
x87r1 00000000000000000000 ST1 Empty 0.000000000000000000
x87r2 00000000000000000000 ST2 Empty 0.000000000000000000
x87r3 00000000000000000000 ST3 Empty 0.000000000000000000
x87r4 00000000000000000000 ST4 Empty 0.000000000000000000
```

```
esi=75179C68 "e9)"

.text:00408CB7 evtdiag.exe:$8CB7 #8CB7
```

Default (stdcall) 5 Unlocked

```
1: [esp+4] 0040F924 "%s\r\n"
2: [esp+8] 0018FCE0 "SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, J
3: [esp+C] 0018FEE8
4: [esp+10] 00292788 &"C:\\Users\\Analyzer\\Desktop\\evtdiag.ex
```

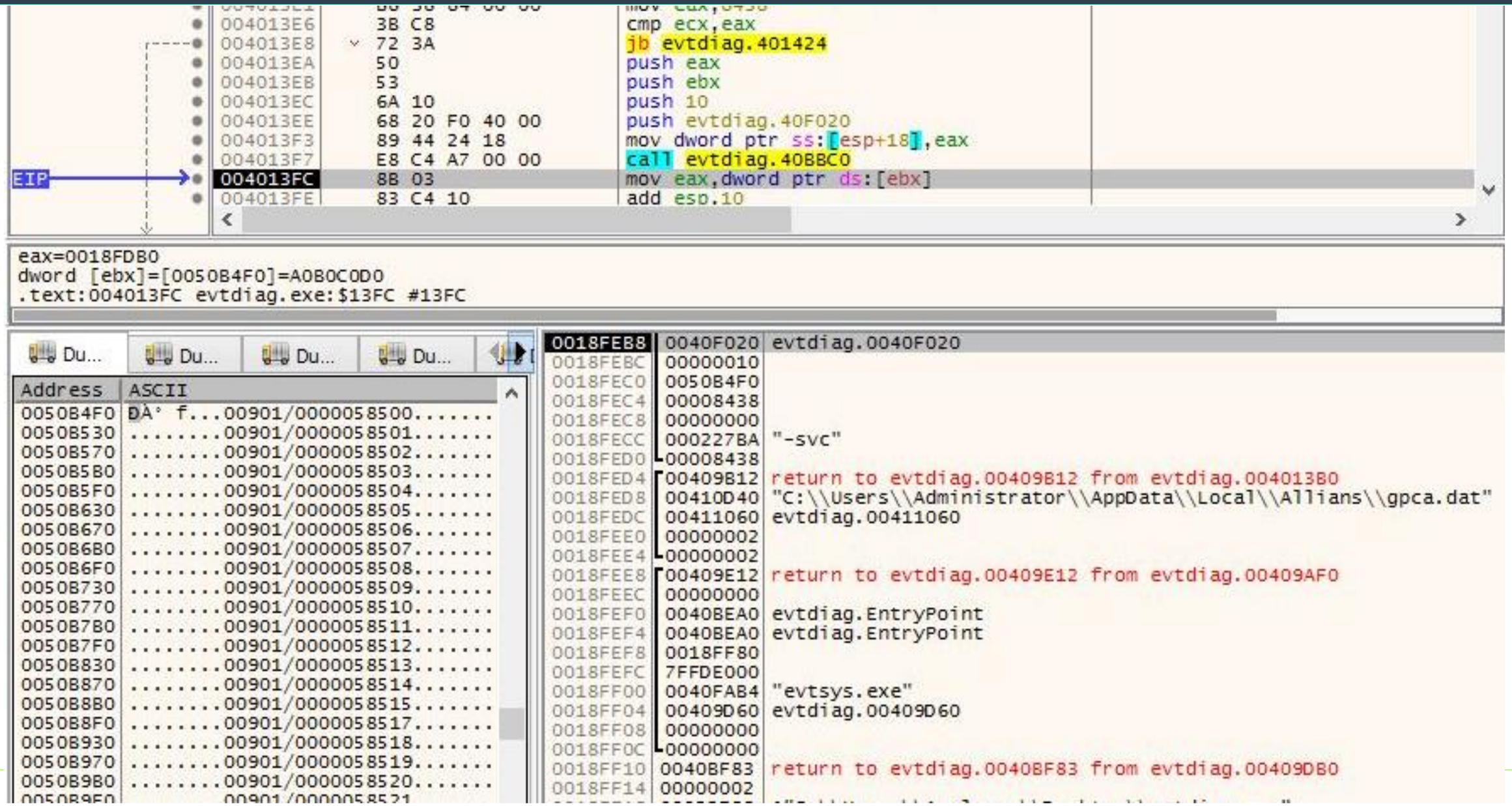
Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1

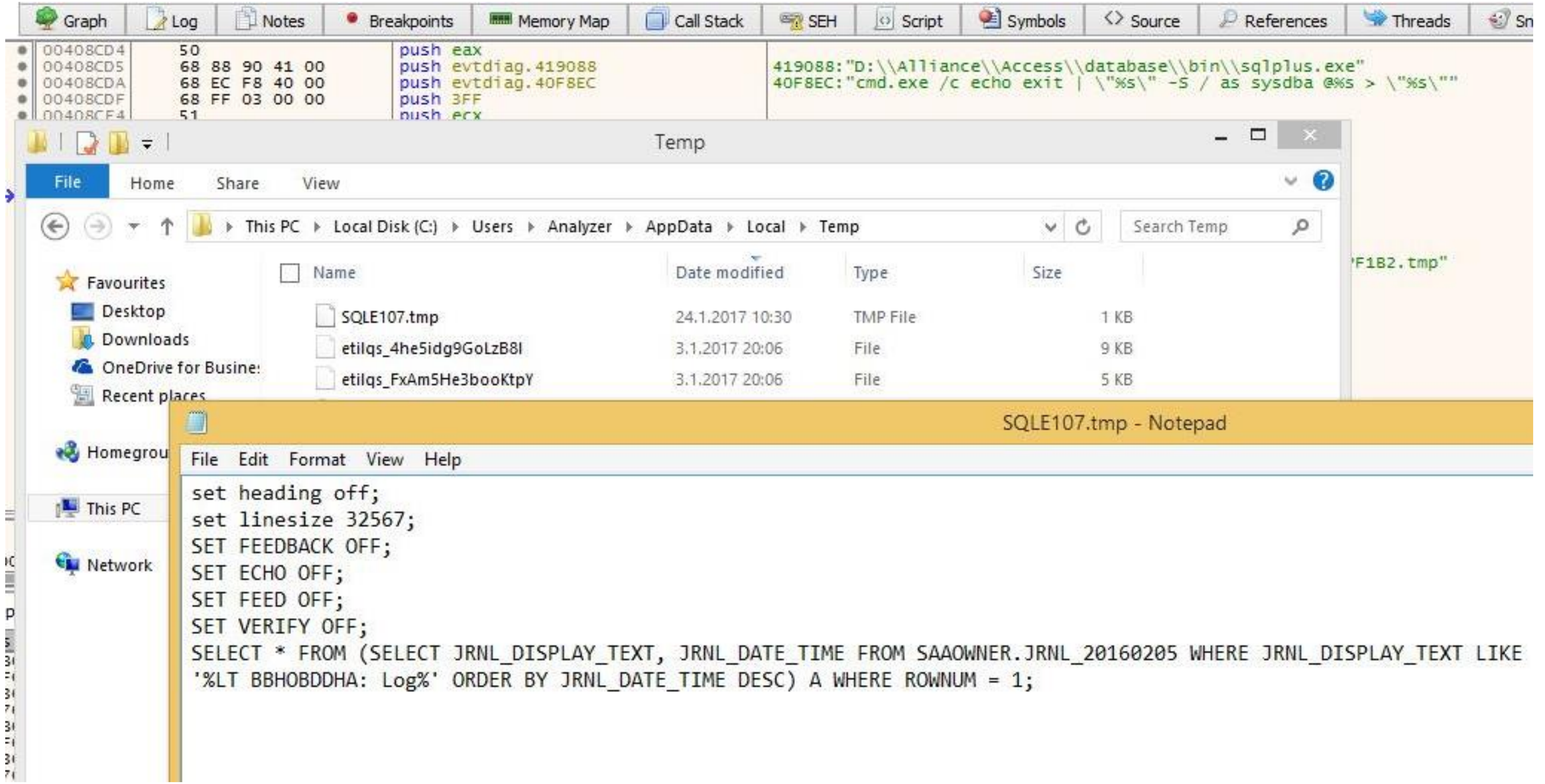
Address	Hex	ASCII
0018F644	68 9C 17 75 24 F9 40 00 E0 FC 18 00 E8 FE 18 00	h..u$ù@.àü..èþ..
0018F654	88 27 29 00 03 00 00 00 00 00 00 00 00 00 00 00	.').....
0018F664	7D 9E 6A 5D 02 F8 FF FF 50 E1 08 00 00 00 00 00	}.j].øÿÿPá.....
0018F674	B0 E4 08 00 00 00 00 00 00 00 00 00 00 00 00 00	°ä.....
0018F684	78 DC 08 00 00 00 00 00 50 E1 08 00 00 00 00 00	xÜ.....Pá.....
0018F694	00 00 00 00 34 FD FF FF 34 04 00 00 34 FD FF FF	....4ýÿÿ4...4ýÿÿ
0018F6A4	CC 02 00 00 28 00 00 00 40 01 00 00 00 00 00 00	Ì...(...@.....
0018F6B4	A0 96 C1 30 43 3A 5C 55 73 65 72 73 5C 41 6E 61	.ÁOC:\Users\Ana
0018F6C4	6C 79 7A 65 72 5C 41 70 70 44 61 74 61 5C 4C 6F	lyzer\AppData\Lo
0018F6D4	63 61 6C 5C 54 65 6D 70 5C 54 4D 50 43 37 46 32	cal\Temp\TMPC7F2
0018F6E4	2E 74 6D 70 00 00 00 00 00 00 00 00 00 00 00 00	.tmp.....
0018F6F4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F704	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F714	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F724	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F734	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F744	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F754	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F764	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018F774	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

```
0018F644  75179C68  "e9)"
0018F648  0040F924  "%s\r\n"
0018F64C  0018FCE0  "SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM SAAOWNER
0018F650  0018FEE8
0018F654  00292788  &"C:\\Users\\Analyzer\\Desktop\\evtdiag.exe"
0018F658  00000003
0018F65C  00000000
0018F660  00000000
0018F664  5D6A9E7D
0018F668  FFFFF802
0018F66C  0008E150
0018F670  00000000
0018F674  0008E4B0
0018F678  00000000
0018F67C  00000000
0018F680  00000000
0018F684  0008DC78
0018F688  00000000
0018F68C  0008E150
0018F690  00000000
0018F694  00000000
0018F698  FFFFFD34
```


Command: Default

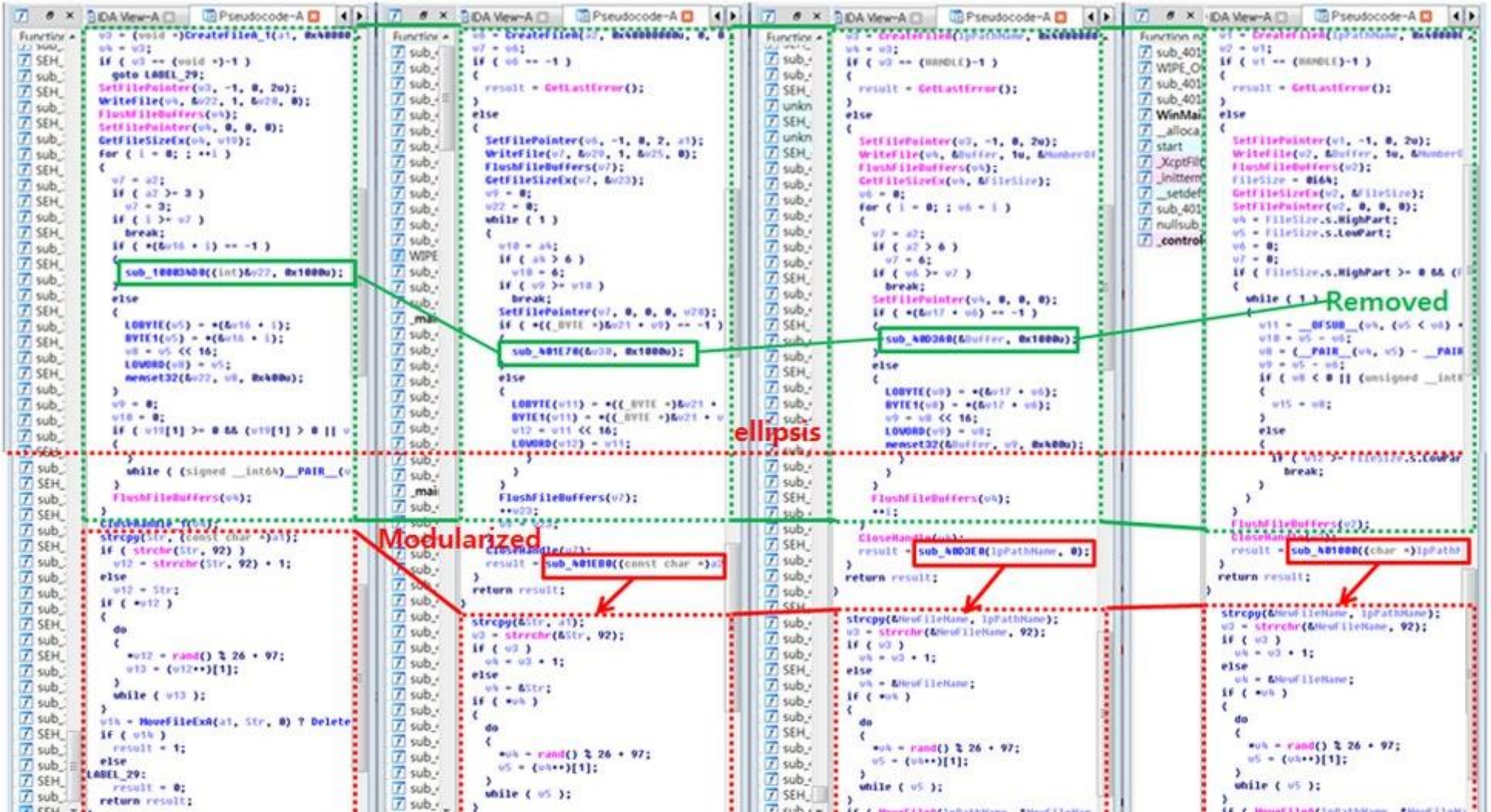
Configten müdahale edilecek Transaction id ler alınıyor




Graph
Log
Notes
Breakpoints
Memory Map
Call Stack
SEH
Script
Symbols
Source
References
Threads
00408CD4 50 push eax
00408CD5 68 88 90 41 00 push evtdiag.419088
00408CDA 68 EC F8 40 00 push evtdiag.40F8EC
00408CDF 68 FF 03 00 00 push 3FF
00408CE4 51 push ecx
419088:"D:\\Alliance\\Access\\database\\bin\\sqlplus.exe"
40F8EC:"cmd.exe /c echo exit | \"%s\" -S / as sysdba @%s > \"%s\""
Temp
File
Home
Share
View
This PC
Local Disk (C:)
Users
Analyzer
AppData
Local
Temp
Search Temp
Favourites
Desktop
Downloads
OneDrive for Busine:
Recent places
Homegrou
This PC
Network
Name
Date modified
Type
Size
SQLE107.tmp
24.1.2017 10:30
TMP File
1 KB
etilqs_4he5idg9GoLzB8l
3.1.2017 20:06
File
9 KB
etilqs_FxAm5He3booKtpY
3.1.2017 20:06
File
5 KB
F1B2.tmp"
SQLE107.tmp - Notepad
File Edit Format View Help
set heading off;
set linesize 32567;
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM SAAOWNER.JRNL_20160205 WHERE JRNL_DISPLAY_TEXT LIKE
'%LT BBHOBDDHA: Log%' ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;

```
004023F2 push evtdiag.40F19C   "SeDebugPrivilege"
004024A2 push evtdiag.40F18C   "liboradb.dll"
004024C7 push evtdiag.40F18C   "liboradb.dll"
00402507 push evtdiag.40F184   "OK : %s"
00402528 push evtdiag.40F178   "FAIL : %s"
0040283C push evtdiag.40F220   "SELECT C.TEXT_S_UMID FROM (SELECT A.TEXT_S_UMID, A.TEXT_DATA_BLOCK FROM SAAOWNER.TEXT_%s A,
00402887 push evtdiag.40F1E8   "DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';"
0040288E push evtdiag.40F1B0   "DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';"
00402971 push evtdiag.40F348   "SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS LIKE '%%%s%%' AND M
004029BC push evtdiag.40F1E8   "DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';"
004029F3 push evtdiag.40F1B0   "DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';"
00402B16 push evtdiag.40F484   "SELECT MESG_FIN_CCY_AMOUNT FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';"
00402BDD push evtdiag.40F47C   "%s%19s"
00402BFE push evtdiag.40F428   "UPDATE SAAOWNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID = '%s';"
00402C39 push evtdiag.40F3C0   "UPDATE SAAOWNER.TEXT_%s SET TEXT_DATA_BLOCK = UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UM
00402CEB push evtdiag.40F220   "SELECT C.TEXT_S_UMID FROM (SELECT A.TEXT_S_UMID, A.TEXT_DATA_BLOCK FROM SAAOWNER.TEXT_%s A,
00402E07 push evtdiag.40F4D0   "SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS LIKE '%%%s%%' AND M
00402ED3 mov al,byte ptr ds:[4 "196.202.103.174"
00402FFB push evtdiag.40F550   "%s"
0040302E mov al,byte ptr ds:[4 "196.202.103.174"
00403203 push evtdiag.40F554   "%04d"
00403256 push evtdiag.40F568   "prt"
0040325B push evtdiag.40F55C   "????????"
0040376C push evtdiag.40F580   "%s \"%s\" \"%s\" 2 -1"
0040378D push evtdiag.40F574   "%s \"%s\" %s"
004037D2 push evtdiag.40F56C   "%s.bak"
004038CF mov edi,evtdiag.40F6B ".\\\"\n"
004038F7 mov esi,evtdiag.40F6B ".\\\"\n"
004038FE mov edi,evtdiag.40F6A ".\n"
0040392C mov esi,evtdiag.40F6A ".\n"
0040394C mov edi,evtdiag.40F67 ".\\\" Definition of the Page Header for the first message\n"
00403974 mov esi,evtdiag.40F67 ".\\\" Definition of the Page Header for the first message\n"
0040399B mov edi,evtdiag.40F63 ".\\\" Redefinition of the Page Header for every next message\n"
004039C9 mov esi,evtdiag.40F63 ".\\\" Redefinition of the Page Header for every next message\n"
00403A87 push evtdiag.40F614   "%02d/%02d/%02d-%02d:%02d:%02d"
00403A9E push evtdiag.40F554   "%04d"
00403AB6 push evtdiag.40F60C   "%06d"
00403B53 mov edi,evtdiag.40F5C ".wh 0 PH\t\\\" Trap at line 0 (top of each page). Print the page header\n"
00403B77 mov esi,evtdiag.40F5C ".wh 0 PH\t\\\" Trap at line 0 (top of each page). Print the page header\n"
00403B7E mov edi,evtdiag.40F59 ".bp\t\\\" Every next message starts at a new page\n"
00403BA2 mov esi,evtdiag.40F59 ".bp\t\\\" Every next message starts at a new page\n"
00403F3F mov edi,evtdiag.41918 "D:\\MESSAGE_PARTNER"
00403F71 mov edi,evtdiag.41000 "C:\\Users\\Administrator\\AppData\\Local\\Allians\\mcf"
00404114 push evtdiag.40F0DC   ".."
00404158 push evtdiag.40F6B8   "????????.prt"
```

Sanırım bu dump zararlının kısa bir özeti olabilir


South Korea's Media Hack
(Jun 2013) by North Korea
Sony Pictures Hack
(Nov 2014) by North Korea
Vietnam Bank Hack
(Dec 2015) by ?
Bangladesh Bank Hack
(Feb 2016) by ?
Removed
ellipsis
Modularized

Peki Bangladesh bankası diğer sıradan güvenlik yatırımları yapan Bankalar gibi olsaydı durum farklı mı olacaktı?

BGA
SECURITY

-Teşekkürler-

bgasecurity.com | @bgasecurity