

MetaStrike Operasyonu

written by Mert SARICA | 1 May 2018

21.11.2017 tarihinde saat 16:16'da, Türkiye'de bulunan 19 bankanın toplam 535 çalışanına Anna.Yasko@profix.kiev.ua e-posta adresinden Changes to the terms başlığına sahip, ekinde Swift Changes.rtf dosyası bulunan bir e-posta gönderildi ve çoğu bankanın kullanmış olduğu güvenlik sistemleri tarafından ya silindi ya da karantinaya alındı.

The screenshot shows an email client interface with a ribbon menu at the top. The ribbon has two tabs: 'FILE' and 'MESSAGE'. The 'MESSAGE' tab is active, showing various actions like 'Delete', 'Reply', 'Reply All', 'Forward', 'Meeting', 'More', 'Create New', 'Move', 'Actions', 'Mark Unread', 'Categorize', 'Follow Up', 'Translate', 'Find', 'Related', 'Select', and 'Zoom'. Below the ribbon, the email header shows the sender as 'Yasko Anna <Anna.Yasko@profix.kiev.ua>' with the subject 'Changes to the terms'. The email body contains a list of recipients: '14Petr.Kuznetsov@banksoyuz.ru; 20info@banksoyuz.ru; Aleksey.Chistov@banksoyuz.ru; Aleksey.Kapuskin@banksoyuz.ru; Alla.Dondurey@banksoyuz.ru; Arina.Kuzmina@banksoyuz.ru; BahshyanSG@banksoyuz.ru; Bond@banksoyuz.ru; Dmitriy.Kurkin@banksoyuz.ru; Elena.Sokolova@banksoyuz.ru; Evgeny.Cherednichenko@banksoyuz.ru; Igor.Anokhin@banksoyuz.ru; IsaevaSV@banksoyuz.ru; Kazan@banksoyuz.ru; Kira.Belova@banksoyuz.ru; KrasnikovaMA@banksoyuz.ru; Natalya.Anikina@banksoyuz.ru; Olga.Kogut@banksoyuz.ru; Oxana.Vetrova@banksoyuz.ru; Pavel.Svishchev@banksoyuz.ru; Petr.Kuznetsov@banksoyuz.ru; Research@banksoyuz.ru; Sergey.Potantin@banksoyuz.ru; SpasskinAY@banksoyuz.ru;'. Below the recipients, there is a 'Message' tab and a file icon for 'Swift changes.rtf (31 KB)'. At the bottom of the email, there is a link 'See more about Yasko Anna.' and a row of profile icons.

See more about Yasko Anna.



1 21 Nov 2017 17:16:23 (GMT +03:00) MID: [REDACTED]
SENDER: Anna.Yasko@profix.kiev.ua
RECIPIENT: [REDACTED]
SUBJECT: Changes to the terms
LAST STATE: Message [REDACTED] aborted: Dropped by [REDACTED]
Swift changes.rtf

Message Details	
Envelope and Header Summary	
Received Time:	21 Nov 2017 17:16:23 (GMT +03:00)
MID:	[REDACTED]
Message Size:	98.82 (KB)
Subject:	Changes to the terms
Envelope Sender:	Anna.Yasko@profix.kiev.ua
Envelope Recipients:	[REDACTED]
Attachments:	Swift changes.rtf

Güvenlik sistemlerinde çok sayıda alarma yol açan bu şüpheli e-posta incelendiğinde, başlıkta ve ekindeki dosyada Swift kelimesinin geçmesinin yanısıra, alıcı listesinde (To:) yabancı banka çalışanlarının da dahil olduğu tam 952 kişinin yer alıyor olması ve e-postanın ileti gövdesinde (body) herhangi bir metnin yer almaması şüpheleri fazlasıyla arttırıyordu. E-postanın başlık bilgileri incelendiğinde, gönderen SMTP sunucusunun gerçekten de ProFIX firmasına ait olması ilk olarak bu kurumun hacklenmiş olabileceğine işaret ediyordu. Kim bu ProFIX diye ufak bir araştırma yapıldığında, 29 ülkede 250'den fazla banka ile çalışan, 2013 yılından bu yana ise Belarus, Ermenistan, Gürcistan, Ukrayna ve Moldova'da hizmet veren bir SWIFT iş ortağı olduğu anlaşılıyordu.

Swift Changes.rtf dosyası incelendiğinde ise bu dosyanın içinde Microsoft Office 2007'den 2016'ya kadar tüm sürümlerini etkileyen bir zafiyeti (CVE-2017-11882) istismar eden bir istismar kodu olduğu ortaya çıktı. 14 Kasım'da Microsoft tarafından yaması yayınlanan, GitHub üzerinde ise 20 Kasım'da istismar kodu yayınlanan bir zafiyet, 21 Kasım'da Türkiye'deki 19 bankaya siber saldırı gerçekleştirmek amacıyla, hacklendiği düşünülen ProFIX isimli bir SWIFT iş ortağı üzerinden gerçekleştiriliyordu!

engine (58)	positiv (24)	date (dd.mm.yyyy)	age (days)
Sophos	Exp/201711882-A	22.11.2017	1
McAfee	Exploit-FXR18ED2312BF6CD	22.11.2017	1
Ikarus	Exploit.CVE-2017-11882	22.11.2017	1
BitDefender	Exploit.CVE-2017-11882.Gen	22.11.2017	1
Ad-Aware	Exploit.CVE-2017-11882.Gen	22.11.2017	1
GData	Exploit.CVE-2017-11882.Gen	22.11.2017	1
Rising	Exploit.CVE-2017-11882.Gen!1.AED3 (CLASS...	22.11.2017	1
AegisLab	Exploit.Msoffice.Cvelc	22.11.2017	1
Microsoft	Exploit:O97M/CVE-2017-11882	22.11.2017	1
Kaspersky	HEUR:Exploit.MSOoffice.CVE-2017-11882.b	22.11.2017	1
ZoneAlarm	HEUR:Exploit.MSOoffice.CVE-2017-11882.b	22.11.2017	1
Avast	Other:Malware-gen [Trj]	22.11.2017	1
AVG	Other:Malware-gen [Trj]	22.11.2017	1
ViRobot	RTF.S.Exploit.31811	22.11.2017	1
AhnLab-V3	RTF/Cve-2017-11882	22.11.2017	1
TrendMicro-HouseCall	TROJ_RTFCVE201711882.A	22.11.2017	1
TrendMicro	TROJ_RTFCVE201711882.A	22.11.2017	1
DrWeb	Trojan.DownLoader25.57745	22.11.2017	1
Symantec	Trojan.Mdropper	22.11.2017	1
Fortinet	WM/Agent.1416ltr	22.11.2017	1
Baidu	Win32.Exploit.CVE-2017-11882.a	22.11.2017	1
ESET-NOD32	Win32/Exploit.CVE-2017-11882.A	22.11.2017	1
Bkav	clean	21.11.2017	2
MicroWorld-eScan	clean	22.11.2017	1
nProtect	clean	22.11.2017	1
CMC	clean	22.11.2017	1
CAT-QuickHeal	clean	22.11.2017	1
Malwarebytes	clean	22.11.2017	1
Zillya	clean	22.11.2017	1
TheHacker	clean	21.11.2017	2
K7GW	clean	22.11.2017	1
K7AntiVirus	clean	22.11.2017	1
Arcabit	clean	22.11.2017	1

Bulmacının kayıp parçalarını birleştirdiğimizde ortaya zamanlaması muazzam, senaryosu amatörce ((To: kısmında 952 kişinin olması, ileti gövdesinde metin olmaması vs.) kurgulanmış bir siber saldırı girişimi çıktı. 952 e-posta adresinin nereden ve nasıl temin edildiği sorusuna tam olarak yanıt bulunamasa da, sosyal medya üzerinde siber güvenlik uzmanlarından Huzeyfe ÖNAL ve Furkan ÇALIŞKAN'ın tespitlerine göre 25 Eylül tarihinde Pastebin sitesinde yer alan bir liste baz alınmıştı. 952 e-posta adresi ile Pastebin'de yer alan bu liste karşılaştırıldığında e-posta adreslerinin çok büyük bir oranının bu liste ile örtüşüyor olması, güvenlik uzmanlarını doğrular nitelikteydi.



Huzeyfe ÖNAL
@huzeyfeonal

Follow

Rusya Merkez Bankası (CBR) ve Ukraynalı #SWIFT firması Profix'den geliyormuş gibi Türkiye'deki 16 bankaya yönelik #Phishing saldırısı yapıyor. lnkd.in/e953fNb

9:25 PM - 22 Nov 2017

13 Retweets 10 Likes



2

13

10



Huzeyfe ÖNAL @huzeyfeonal - 5h

Replying to @huzeyfeonal

Bu da gönderilen mail ve indirilen .exe'ye ait IP/Domain bilgileri.



5

3



Furkan ÇALIŞKAN @caliskanfurkan_ - 6h

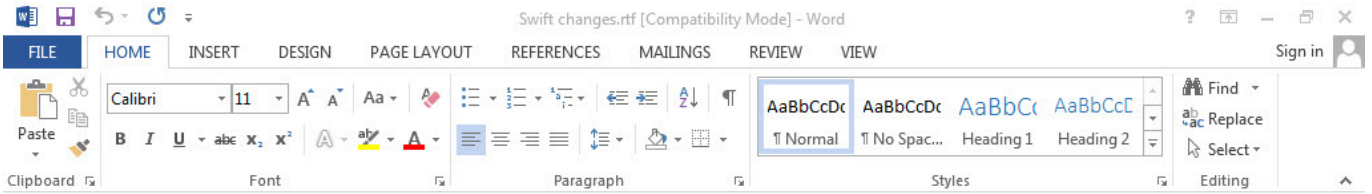
Replying to @huzeyfeonal

Hedefler şuradan seçilmiş gibic

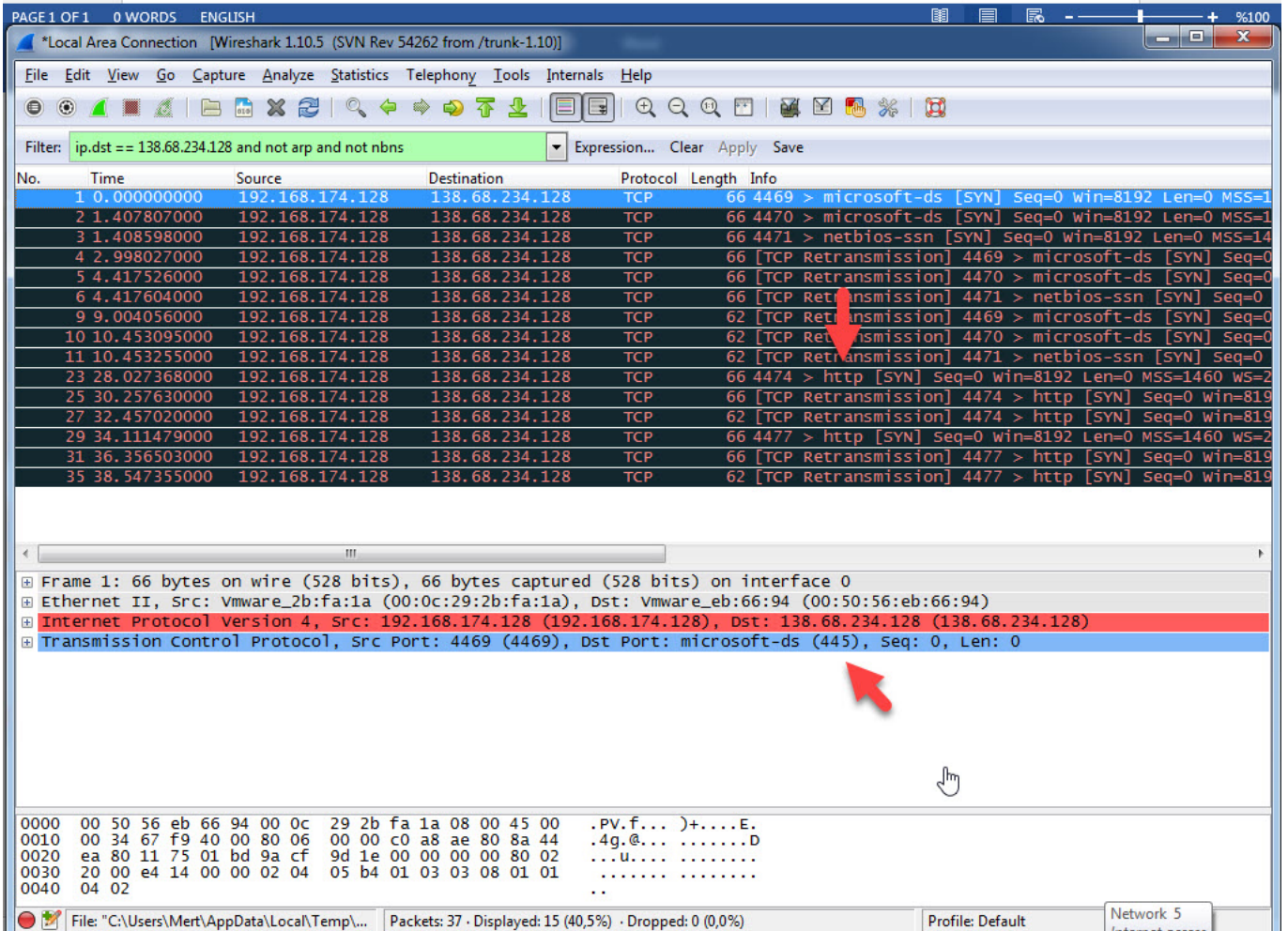
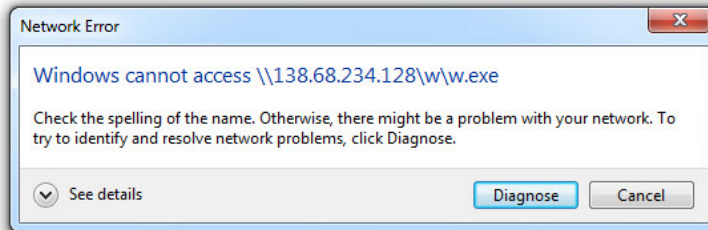


22 Kasım tarihinde Carbon Black firmasının blog sayfasında bu siber saldırının özet teknik detaylarına IOCLeri ile birlikte yer verildi. 30 Kasım tarihli FireEye iSight istihbarat raporuna bakıldığında bu grubun 2016 yılından bu yana 19 ülkedeki finansal kurumları Cobalt Strike sızma testi yazılımı ile hedef alan Cobalt grubu (diğer bir adıyla MetaStrike) olduğu anlaşılıyordu. 8 Aralık tarihinde ise Palo Alto Networks firmasının blog sayfasında bu defa istismar kodunun teknik detaylarına yer verildi.

Swift Changes.rtf dosyası çalıştırılır çalıştırılmaz Microsoft Office'in Microsoft Equation Editor bileşenindeki yığın tabanlı bellek taşması (stack buffer overflow) zafiyetini istismar ederek \\138.68.234.12\w\w.exe paylaşım adresi üzerinden w.exe dosyasını çalıştırıyordu. Şayet Windows, SMB protokolü üzerinden ilgili adrese bağlanamıyor ise ve işletim sistemi üzerinde WebClient servisi çalışır durumda ise bu durumda WebDAV protokolü üzerinden tanımlı vekil sunucu (proxy) ayarlarını da dikkate alarak bağlanmaya çalışmaktaydı. Bu durum da istismar edilen hedef sistemin ilgili adrese erişip zararlı kodu çalıştırma ihtimalini fazlasıyla arttırıyordu!



111111111111



Son zamanlarda gerekleřtirilen siber saldırılarda zararlı RTF dosyalarının sıklıkla kullanılıyor olması sebebiyle bu yazı ile řüphede duyułan bir RTF dosyasının hızlı bir řekilde nasıl analiz edilebileceđine, Swift Changes.rtf dosyası özelinde yer vermek istedim. Zararlı RTF dosyalarının kötü emellerini gerekleřtirebilmeleri için OLE nesnelereinden faydalandıklarını bildiđimiz için Didier Stevens tarafından geliřtirilen RTFDump aracı ile kısa bir sürede zararlı koda ulařmak mümkün olabiliyor.

rtfdump aracına -aE parametresi vererek RTF içeriđini ASCII olarak görüntülediđimde ilgili OLE nesnelereini bulmak samanlıkla iđne aramaktan farksız olduđu için -f 0 parametresi ile sadece OLE nesnelereini listeledim. Ardından 7, 13, 19 ve 25 dizilerine tek tek -s ve -H (hex ıktısı) parametreleri ile baktıđımda 7. dizide istismar kodu içine gömülü olan ip adresine ve Palo Alto Networks'un yazısına da konu olan WinExec fonksiyonunun adresine (0x430c12) statik olarak ulařtım.

Swift changes.rtf

Acrobat Reader DC

CCleaner

Google Chrome

Hex Workshop ...

Immunity Debugger

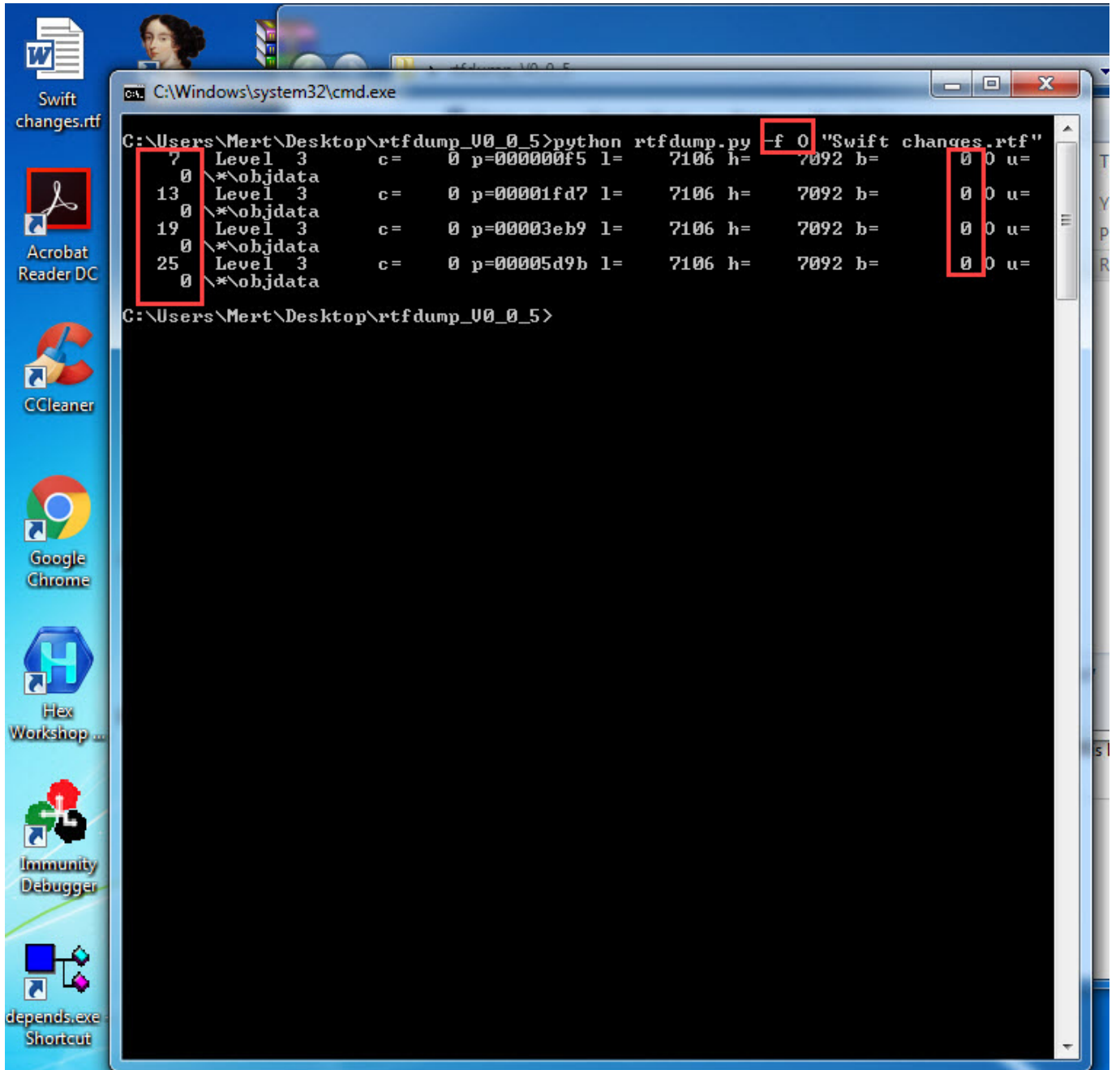
depends.exe Shortcut

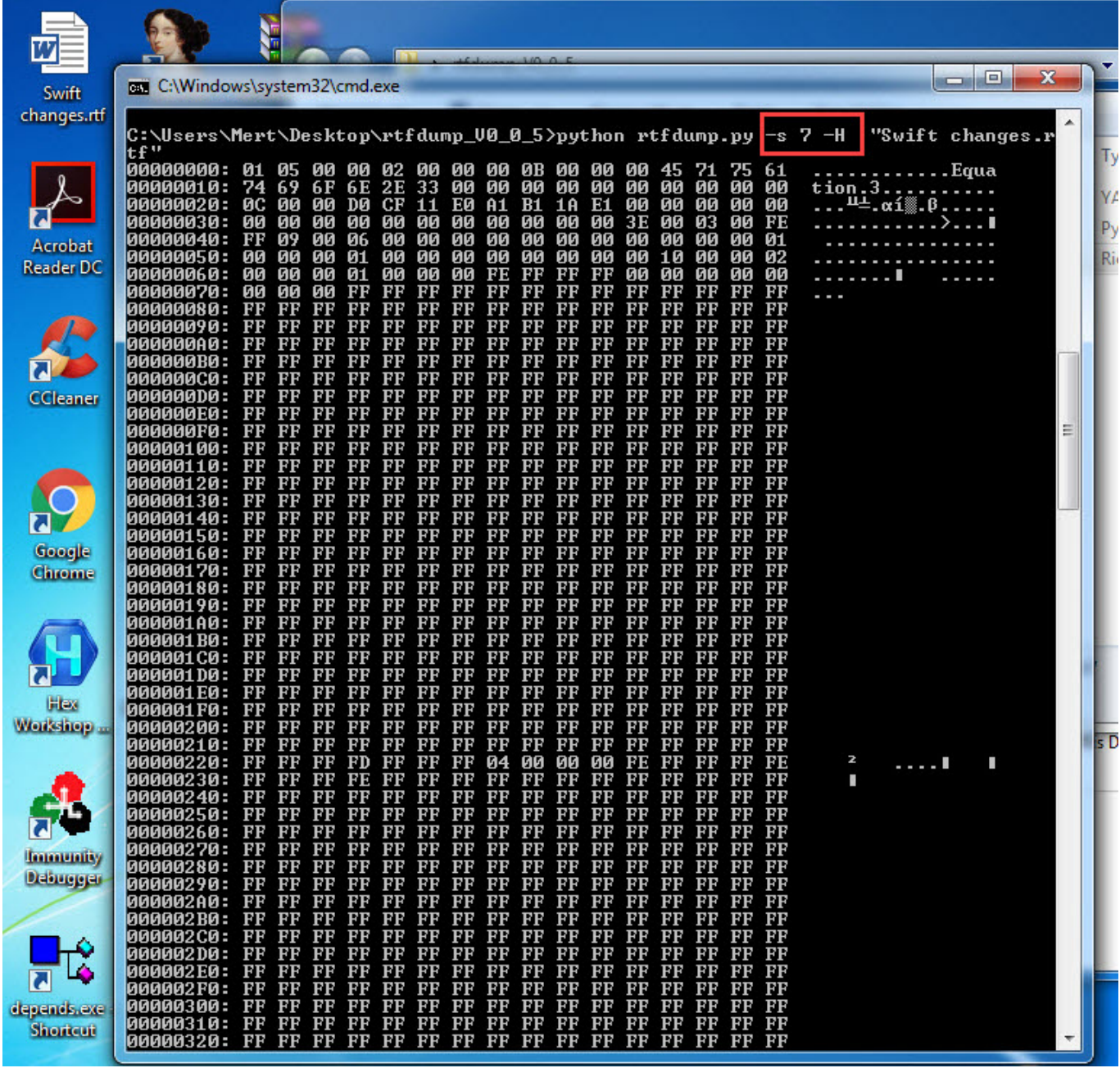
C:\Windows\system32\cmd.exe

```

C:\Users\Mert\Desktop>python rtfdump.py -aE "Swift changes.rtf"
1 Level 1 c= 6 p=00000000 l= 31808 h= 30922 b= 0 u=
38 \rtf1
2 Level 2 c= 1 p=00000034 l= 38 h= 3 b= 0 u=
5 \fonttbl
3 Level 3 c= 0 p=0000003d l= 28 h= 3 b= 0 u=
5 \f0
4 Level 2 c= 0 p=0000005d l= 31 h= 11 b= 0 u=
5 \*generator
5 Level 2 c= 3 p=000000b4 l= 7903 h= 7727 b= 0 u=
7 \object
6 Level 3 c= 0 p=000000cd l= 23 h= 3 b= 0 u=
7 \*objclass Equation.3
7 Level 3 c= 0 p=000000f5 l= 7106 h= 7092 b= 0 0 u=
0 \*objdata
8 Level 3 c= 1 p=00001cb8 l= 730 h= 632 b= 0 u=
0 \result
9 Level 4 c= 1 p=00001cc0 l= 721 h= 632 b= 0 u=
0 \pict
10 Level 5 c= 0 p=00001cc6 l= 11 h= 0 b= 0 u=
0 \*picprop
11 Level 2 c= 3 p=00001f96 l= 7903 h= 7727 b= 0 u=
7 \object
12 Level 3 c= 0 p=00001faf l= 23 h= 3 b= 0 u=
7 \*objclass Equation.3
13 Level 3 c= 0 p=00001fd7 l= 7106 h= 7092 b= 0 0 u=
0 \*objdata
14 Level 3 c= 1 p=00003b9a l= 730 h= 632 b= 0 u=
0 \result
15 Level 4 c= 1 p=00003ba2 l= 721 h= 632 b= 0 u=
0 \pict
16 Level 5 c= 0 p=00003ba8 l= 11 h= 0 b= 0 u=
0 \*picprop
17 Level 2 c= 3 p=00003e78 l= 7903 h= 7727 b= 0 u=
7 \object
18 Level 3 c= 0 p=00003e91 l= 23 h= 3 b= 0 u=
7 \*objclass Equation.3
19 Level 3 c= 0 p=00003eb9 l= 7106 h= 7092 b= 0 0 u=
0 \*objdata
20 Level 3 c= 1 p=00005a7c l= 730 h= 632 b= 0 u=
0 \result
21 Level 4 c= 1 p=00005a84 l= 721 h= 632 b= 0 u=
0 \pict
22 Level 5 c= 0 p=00005a8a l= 11 h= 0 b= 0 u=
0 \*picprop
23 Level 2 c= 3 p=00005d5a l= 7903 h= 7727 b= 0 u=
7 \object
24 Level 3 c= 0 p=00005d73 l= 23 h= 3 b= 0 u=
7 \*objclass Equation.3
25 Level 3 c= 0 p=00005d9b l= 7106 h= 7092 b= 0 0 u=
0 \*objdata
26 Level 3 c= 1 p=0000795e l= 730 h= 632 b= 0 u=
0 \result
27 Level 4 c= 1 p=00007966 l= 721 h= 632 b= 0 u=

```





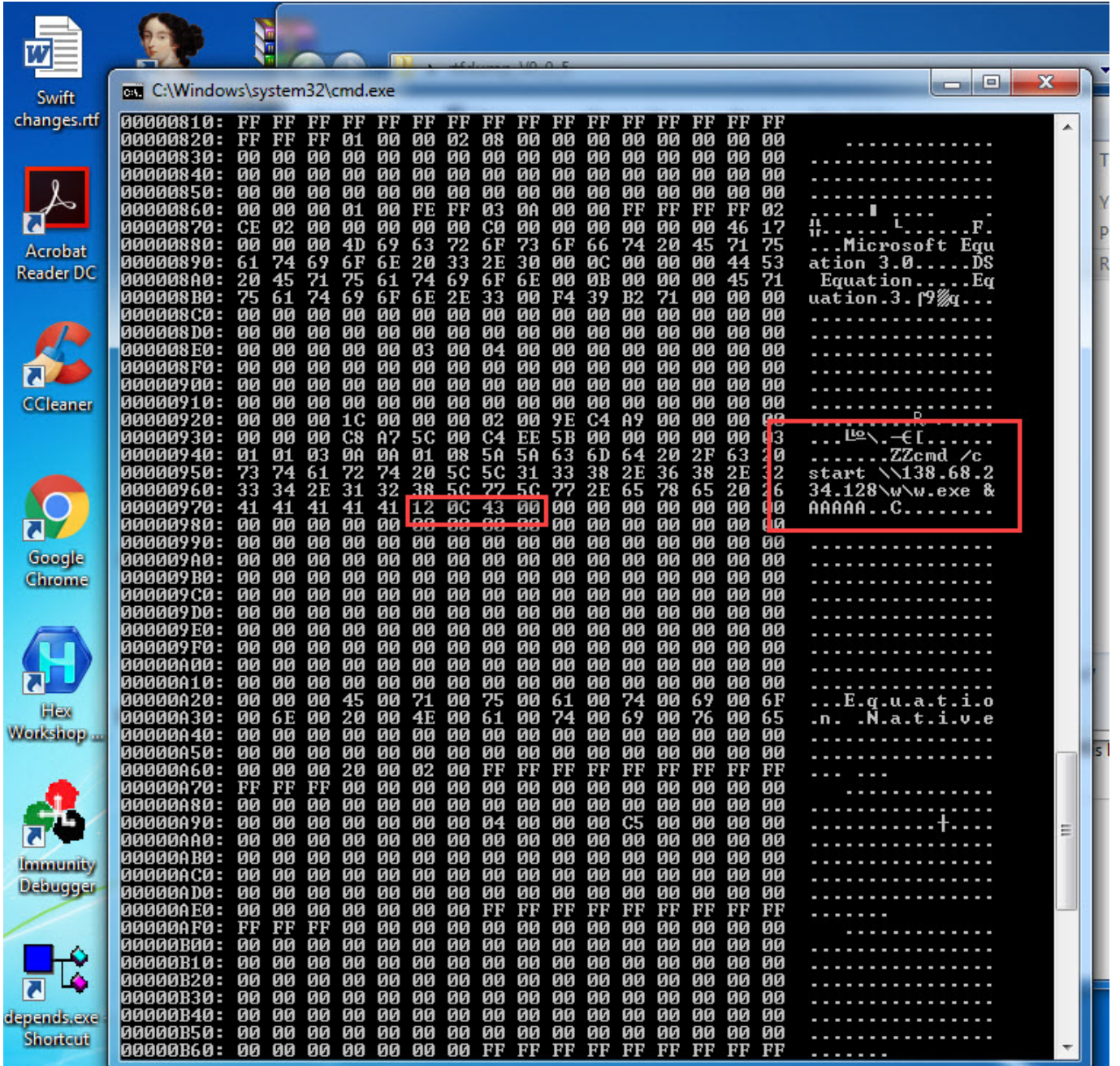
C:\Windows\system32\cmd.exe

C:\Users\Mert\Desktop>python rtfdump.py -s 7 -H "Swift changes.rtf"

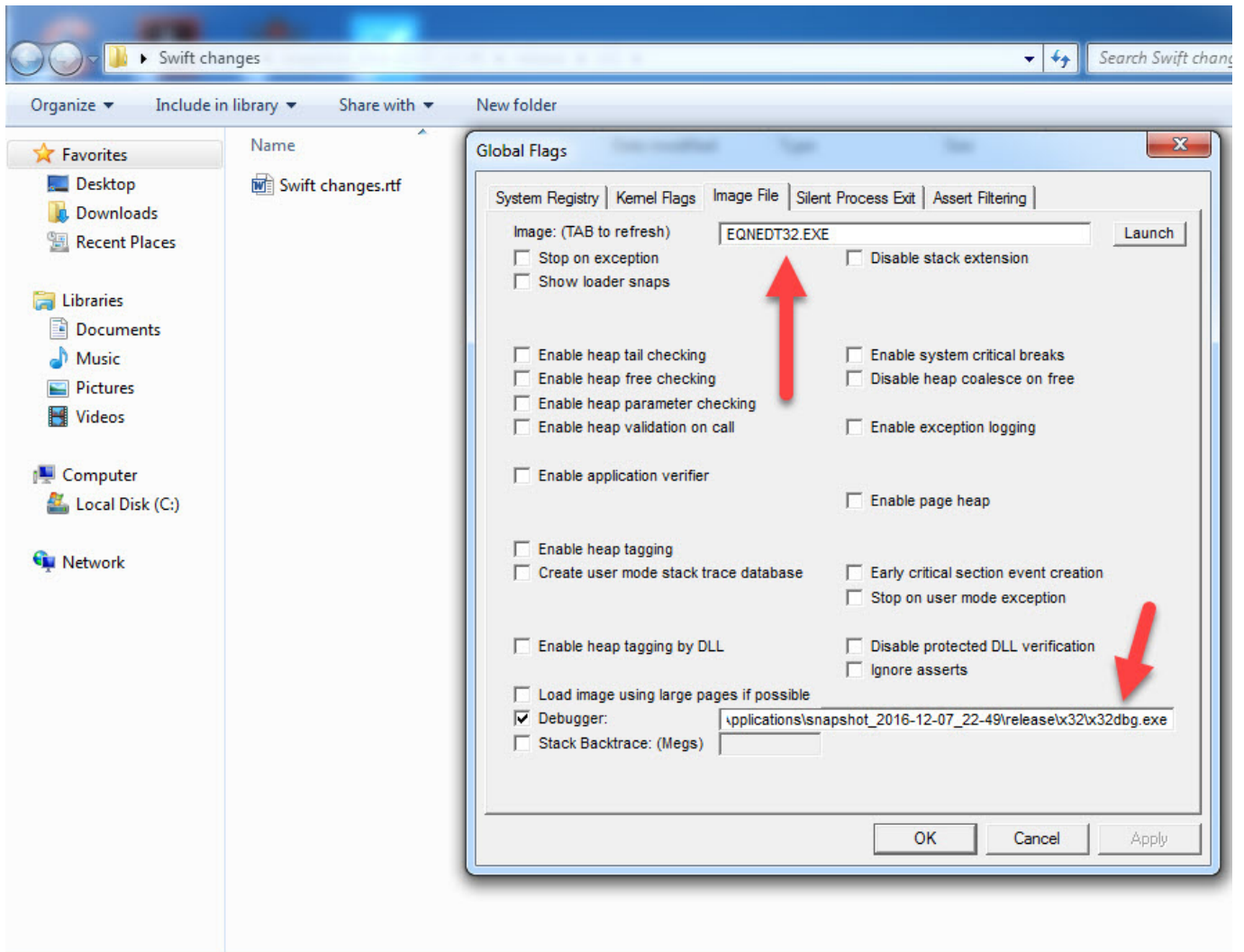
```

00000000: 01 05 00 00 02 00 00 00 0B 00 00 00 45 71 75 61 .....Equa
00000010: 74 69 6F 6E 2E 33 00 00 00 00 00 00 00 00 00 00 .....tion.3
00000020: 0C 00 00 00 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 .....u1.alpha
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 3E 00 03 00 .....>
00000040: FF 09 00 06 00 00 00 00 00 00 00 00 00 00 00 01 .....
00000050: 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 .....
00000060: 00 00 00 01 00 00 00 FE FF FF FF 00 00 00 00 00 .....
00000070: 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000000F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000001F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000200: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000210: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000220: FF FF FF FD FF FF FF 04 00 00 00 FE FF FF FF FF .....
00000230: FF FF FF FE FF FF FF FF FF FF FF FF FF FF FF FF .....
00000240: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000250: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000260: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000270: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000280: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000290: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
000002F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000300: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000310: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000320: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....

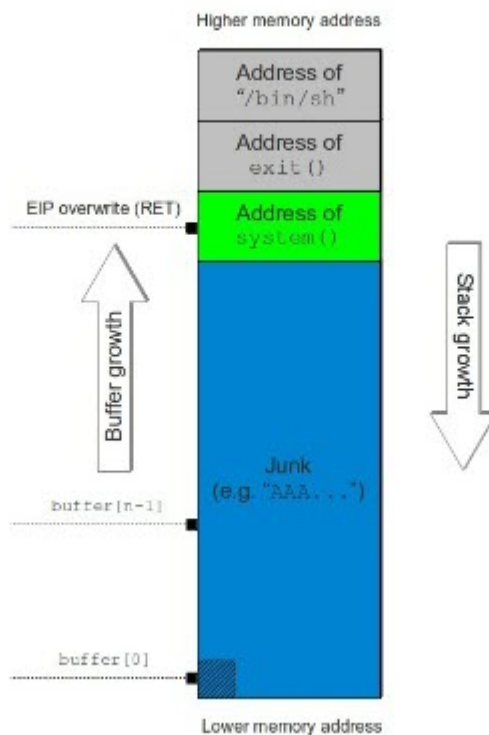
```



Dinamik kod analizi ile de doğrulamak için ise öncelikle Windows Debugging Tools ile gelen Global Flags Editor üzerinde bir ayarlama yapmam gerekti. Swift Changes.rtf dosyası Microsoft Office Word ile açıldıktan sonra Microsoft Equation Editor bileşenine ait eqnedt32.exe programını istismar ettiği için eqnedt32.exe programı açılır açılmaz x64dbg hata ayıklayıcısının devreye gireceği şekilde ayarladım. Winexec fonksiyonun adresine kesme noktası koyup adım adım geriye gidip fonksiyon çıkışlarına da kesme noktası koyarak kısa sürede ret2libc yönteminden faydalanan istismar koduna ulaşmış oldum.



ret2libc (visual)



Sonuç olarak siber saldırı girişimi, hazırlanan e-postanın tahminimce aceleye gelmesi (To: kısmında 952 kişinin olması, ileti gövdesinde metin olmaması vs.) ve sıfırınca gün zafiyeti yerine genele duyurulan bir istismar kodunun (bu sayede güvenlik üreticileri imzalarını hızlıca güncelleyebildiler.) kullanılması sayesinde bildiğim kadarıyla Türkiye'deki herhangi bir bankada başarıya ulaşamadı. İstismar kodunun genele açık olarak yayınlanmasından 1 gün sonra bankalarımıza gerçekleştirilen bu siber saldırı bankalarımızı, finans kurumlarımızı hedef alan grupların ne kadar hızlı bir şekilde organize olup, hareket etmesi gelecekte benzer girişimlere, dikkat edilmesi gereken hususlara dair önemli ipuçları veriyor. Yazıma son noktayı koymadan önce bu ve benzeri siber saldırı girişimlerinin başarıya ulaşmasını zorlaştırma adına finans kurumlarının, iç ağıdan internete doğru WebDAV kullanımını engellemelerinde fayda olacağına inanıyorum.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Kurum içinden internete doğru WebDAV bağlantısını kontrol etmek için Explorer üzerinden \\live.sysinternals.com adresine gitmeyi deneyebilirsiniz.