

Matruşka

written by Mert SARICA | 1 November 2018

If you are looking for an English version of this article, please visit here.

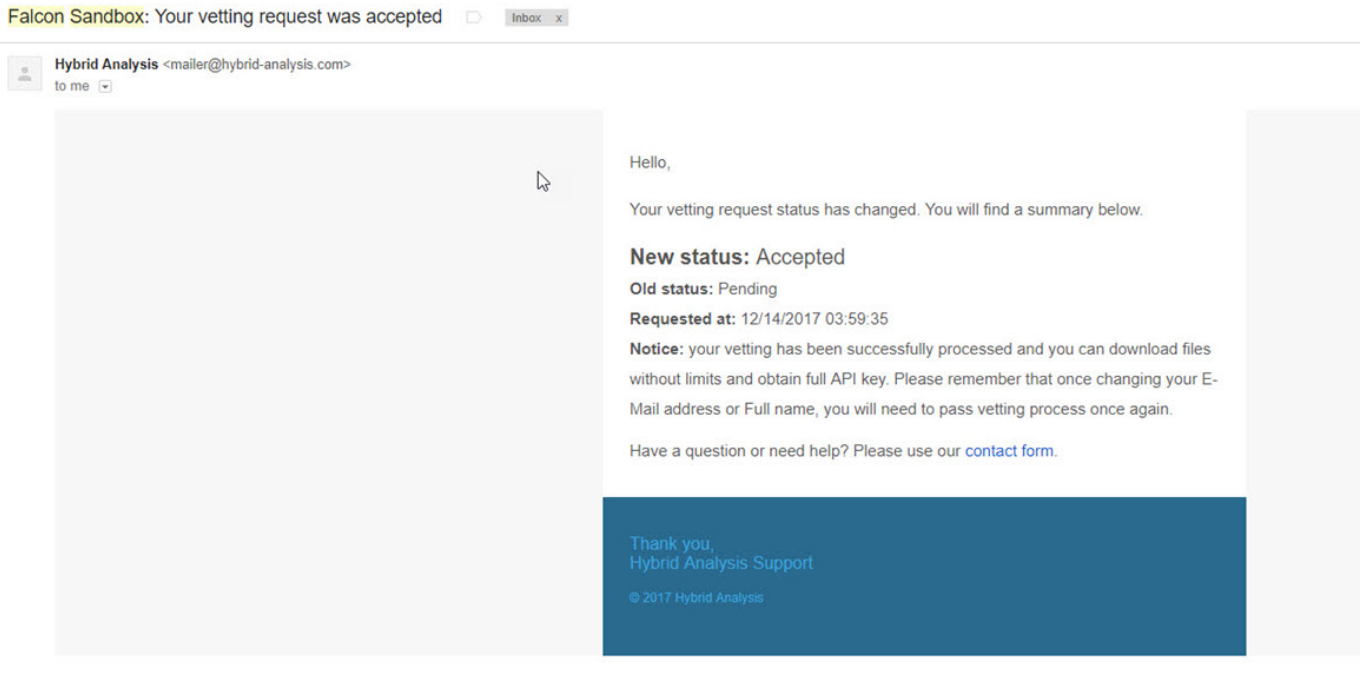
Her daim örümcek hislerinin peşinden koşan bir güvenlik araştırmacısı olarak hislerim uzun zamandan beri beni Gmail hesabımın Spam klasörüne dikkat etmem konusunda uyarıyordu. 2006 yılından bu yana aktif olarak Gmail kullanan biri olarak, 13 yıl içinde e-posta adresimin Nijerya'dan Papua Yeni Gine'ye kadar birçok coğrafyadaki istenmeyen e-posta gönderen niyeti bozuk kişilerin (spammers) e-posta listelerine girdiği konusunda şüphem bulunmuyordu.

Günlerden bir gün yine spam klasörüne göz atışımda kendimi çok yakışıklı bir film yıldızı gibi hissetmemi sağlayan çok sayıda istenmeyen e-posta olduğunu gördüm. :) Bu e-postalardan yola çıkarak zaman içinde Gmail hesabıma gelip spam klasörüne düşen, ekinde zararlı dosyalar bulunan e-postaların sayısı ve bu zararlı dosyaların türü (casus yazılım gibi) hakkında bilgi sahibi olmak için neler yapabileceğimi düşünmeye başladım. Kısa bir süre sonra Python ile spam klasörüne gelen e-postaları izleyen ve e-postaların ekindeki dosyaları bir kum havuzu (sandbox) sistemine yükleyen bir program hazırlamaya karar verdim.

Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)					
<input type="checkbox"/>	<input type="checkbox"/>	<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	1:34 am
<input type="checkbox"/>	<input type="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<input type="checkbox"/>	Lesia	-Hi do You Know Me !! - _Hi, We Need to Talk	Nov 23
<input type="checkbox"/>	<input type="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<input type="checkbox"/>	Lesia	-Hi do You Know Me !! - _Hi, We Need to Talk	Nov 22
<input type="checkbox"/>	<input type="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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="checkbox"/>	<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

Kum havuzu servisi olarak zararlı yazılım analizinde sıklıkla kullandığım ve her daim sonuçlardan memnun kaldığım, arka planda Falcon kum havuzu sistemi bulunan Hybrid Analysis'i kullanmaya karar verdim. Tabii Hybrid-Analysis'in API'sine tespit edilen dosyaları otomatik olarak yükleyebilmek için kısıtlı bulunmayan bir API anahtarı gerekiyordu. Neyse ki güvenlik araştırmacılarına

bunu ücretsiz vermeleri sayesinde API anahtarına kısa bir sürede sahip olabildim.



Python ile Spam Analyzer isimli bir araç hazırlayıp, hayata geçirdikten kısa bir süre sonra bu araç, Spam klasöründe ekinde P0.docx isimli şüpheli bir dosya keşfetti.

```
✓ 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 P0.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

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 : airport@tmtcargo.com : www.tmtcargo.com

Member of. Image result for iata cargo logoRelated imagecid:image004.jpg@01D2BDF8.DA9E4430http://www.alcargoc.com/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](#)



Spam Analyzer aracı, Gmail API üzerinden Gmail hesabınıza client_secret.json dosyasında yer alan bağlantı bilgileri ile (Google API Console'dan da client_secret.json dosyasını indirebilirsiniz) bağlanarak Spam klasöründeki tüm e-postaları okur, ekindeki dosyaları attachments klasörüne kopyalar ve ardından bu dosyaları Hybrid-Analysis sistemine yükler. Yüklediği tüm dosyaların bilgilerini hashes.txt dosyasında saklar. Bu dosyaları Hybrid-Analysis'e yükledikten 1 saat sonra ise ilgili Hybrid-Analysis raporunu ve dosyanın zararlı olup olmadığı bilgisini yine hashes.txt dosyasına yazar.

```
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|9750f81d3b1fbbee8f0f1fb7aac1482|c9e4badba591f852f35ffecf6b296e8a5e557b665ac9ae964885ba163a4bfff|environmentId=100|clean
04-03-2018 15:45:43|AbeI 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
```

P0.docx dosyasını ilk olarak pestudio aracı ile analiz etmeye başladığımda ZoneAlarm dışında herhangi bir güvenlik yazılımının bunu şüpheli olarak tespit edemediğini gördüm. Dosyayı yaması güncel olmayan Microsoft Office 2010 ile açıp Fiddler aracı ile izlediğimde öncelikle winword.exe tarafından kısaltılmış hali [http://urlz\[.\]fr/6uQM](http://urlz[.]fr/6uQM), uzun hali [http://23\[.\]249\[.\]161\[.\]109/ace/](http://23[.]249[.]161[.]109/ace/) olan web adresinden svch.doc dosyasının indirilip çalıştırıldığını ardından da svch.exe tarafından [http://jopittex\[.\]zapro\[.\]org/windows/](http://jopittex[.]zapro[.]org/windows/) adresinden svchost32.vbs dosyasının indirilmeye çalışıldığını gördüm.

pestudio 8.71 - Malware Initial Assessment - www.winator.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

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]	

P0.docx dosyasını Notepad++ ve rtfDump.py araçları ile analiz etmeye devam ettiğimde, Microsoft Word'un frameset özelliğinin kötüye kullanılarak (sızma testlerinde de kullanılmaktadır) CVE-2017-8570 zafiyetinin istismar edildiğini gördüm.

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

RDG Packer Detector v0.7.6 Vx Edition 2017

C:\Users\Mert\Desktop\profile\profile.exe x32 Open

DLL Scanner

Detected: ASProtect v2.4 Build 02.26 Beta

Possible:

Contact:

Last Update: January 12 2017

x64dbg hata ayıklama aracı ile svchost.exe (profile.exe) programını analiz ettiğimde ise ana zararlı yazılım olan Remcos RAT zararlı yazılımı Matruşka bebeği gibi nihayet ortaya çıkmış oldu.

The top part of the image shows the x32dbg interface. The 'Strings' window is open, displaying a list of strings extracted from the profile.exe module. The disassembly window shows instructions like 'push profile.4140A8' and 'mov dword ptr ss:[ebp-240],profile.4141A8'. The string 'Remcos v1.9.9 Pro' is highlighted in green. Below the debugger, a browser window shows the Remcos website with a navigation menu and a main banner for 'Remcos Remote Control'.

Address	Disassembly	String
0040EF5D	push profile.4140A8	"remscripexecd"
0040EFA2	push profile.414094	"remscripsuccess"
0040EFBA	push profile.414084	"remscriperr"
0040F05C	push profile.4140C0	"exec"
0040F0DA	push profile.4140D4	"NtUnmapViewOfSection"
0040F0DF	push profile.4140C8	"ntdll.dll"
0040F330	push profile.4140F8	"GetCursorInfo"
0040F335	push profile.4140E0	"user32.dll"
0040F3CA	push profile.414108	"DISPLAY"
0040F81E	push profile.413C1C	"shlwapi.dll"
0040F88B	push profile.414130	"errscrcap"
0040F8E6	push profile.414118	"image/jpeg"
0040FA15	push profile.413F48	"initializescrcap"
0040FAAE	push profile.414110	"scrshot"
0040FCF9	push profile.414160	"png"
0040FD3B	push profile.413C1C	"shlwapi.dll"
0040FD7A	push profile.41414C	"image/png"
0040FE3C	push profile.414144	"dat"
0040FFE3	mov dword ptr ss:[ebp-240],profile.4141A8	"wnd_%04i%02i%02i_%02i%02i%02i"
0040FFEF	mov dword ptr ss:[ebp-240],profile.414168	"time_%04i%02i%02i_%02i%02i%02i"
00410004	mov dword ptr ss:[ebp-240],profile.4141A8	"wnd_%04i%02i%02i_%02i%02i%02i"
00410252	push profile.4141E4	"GetLastInputInfo"
00410257	push profile.4140EC	"user32.dll"
00410285	push profile.4141F8	"%02i;%02i;%02i;%03i "
0041036F	push profile.414214	"\\\""
00410424	push profile.414220	"http://shell\\open\\command"
0041043F	push profile.413B68	".exe"
004105D7	mov esi,profile.414250	"abcdefghijklmnopqrstuvwxy"
00410677	push profile.41426C	"user"
0041081F	push profile.41427C	"cmd.exe"
00410831	push profile.414278	"c:\\\""
0041096C	mov edi,profile.414274	"cd \""
00410A50	push profile.412908	". \""
00411143	push profile.412AF4	" \""
00411187	push profile.413EBC	" \""
004118E8	push profile.414290	"GetConsoleWindow"
004118ED	push profile.413808	"kernel32.dll"
00411963	push dword ptr ds:[418134]	"&Remcos"
004119D0	mov esi,profile.4142A4	"MsgWindowClass"
00411B18	push profile.4142B4	"close"
00411B60	push profile.4142E4	"CONOUT\$"
00411B93	mov edi,profile.4142D8	"# REMCOS v"
00411BC2	mov edi,profile.413C9C	"1.9.9 Pro"
00411BEE	mov edi,profile.4142BC	"\n # Breaking-Security.Net\n\n"
004142C8	sub eax,01e32.75636553	"vwj"

Matruška, Rus yapımı bir oyuncak bebek türüdür. Ahşap el yapımı olan bebekler ortasından açıldığında başka bir bebek çıkar, onu açtığınızda yine başka bir bebek çıkar. Tek anne figürünün içerisinde iç içe yerleştirilmiş beş veya yedi bebekten oluşur.

Bir sonraki yazıda grşmek dileęiyle herkese güvenli gnler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediye Var #13 oyununun zm yolunu da iermektedir.