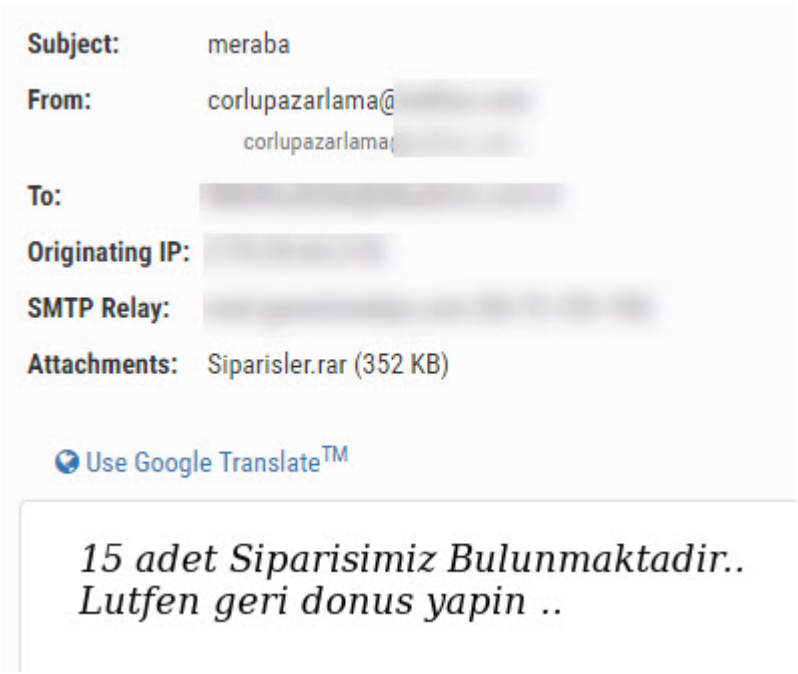
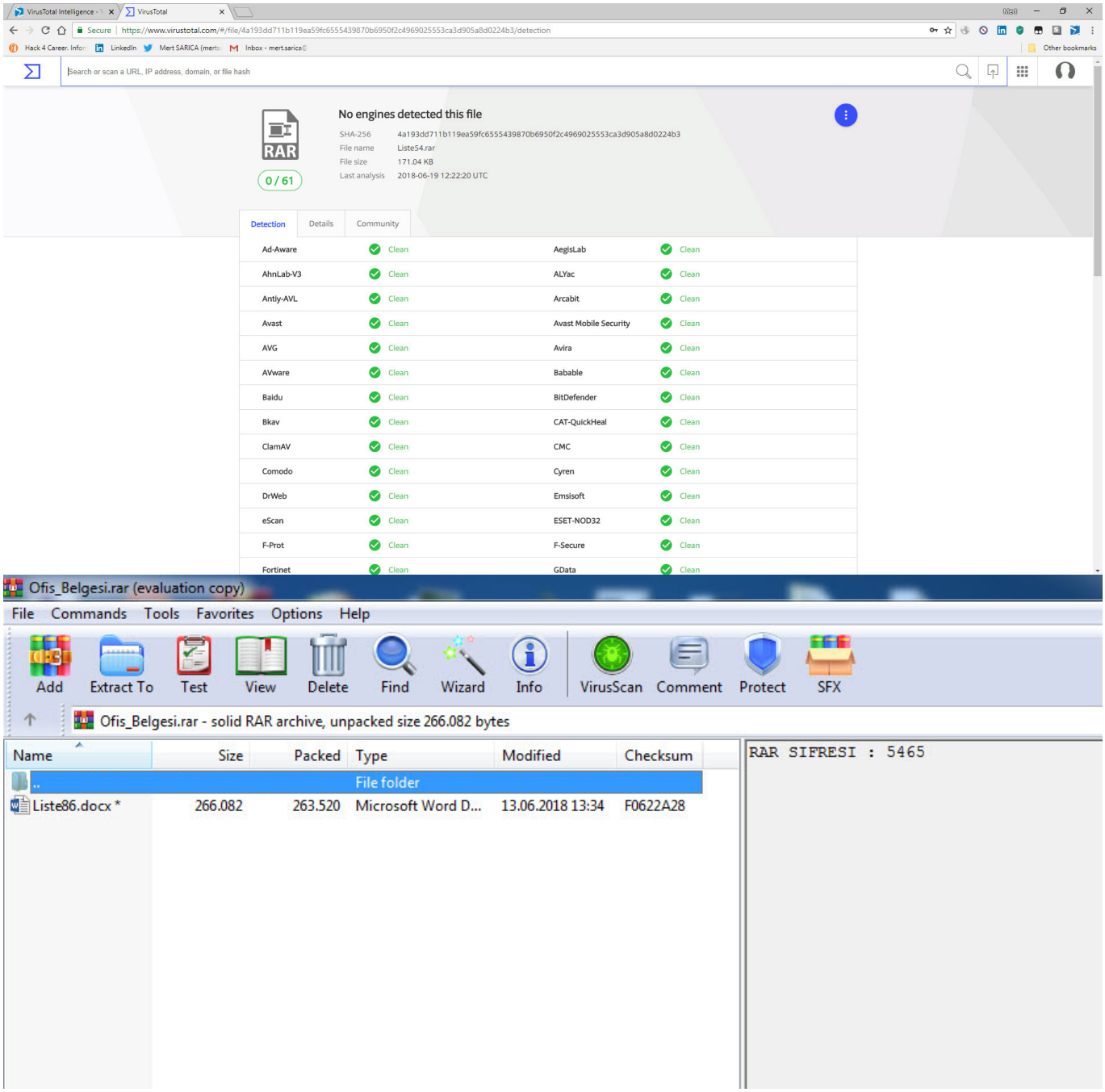
İz Peşinde

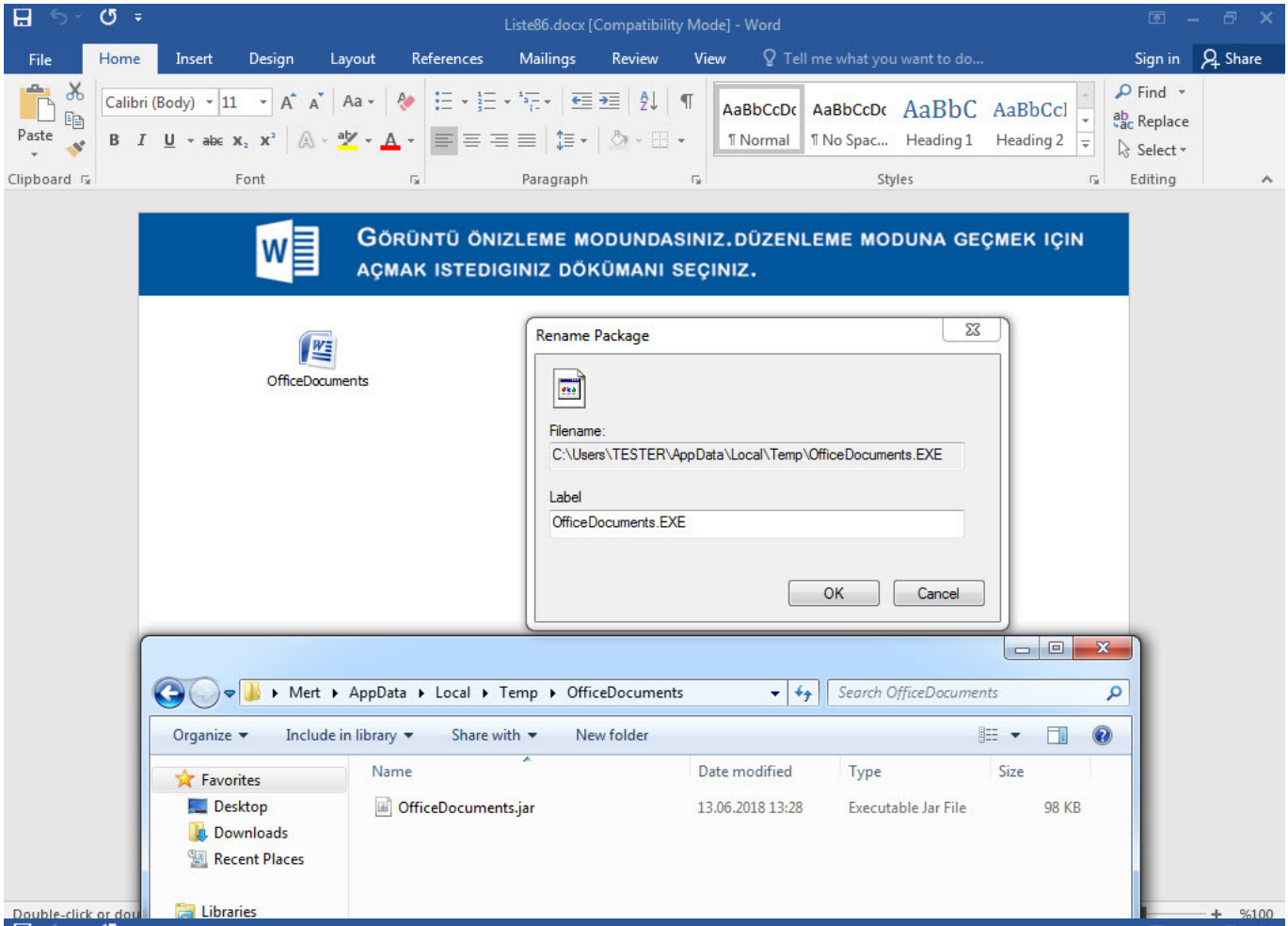
written by Mert SARICA | 1 May 2019

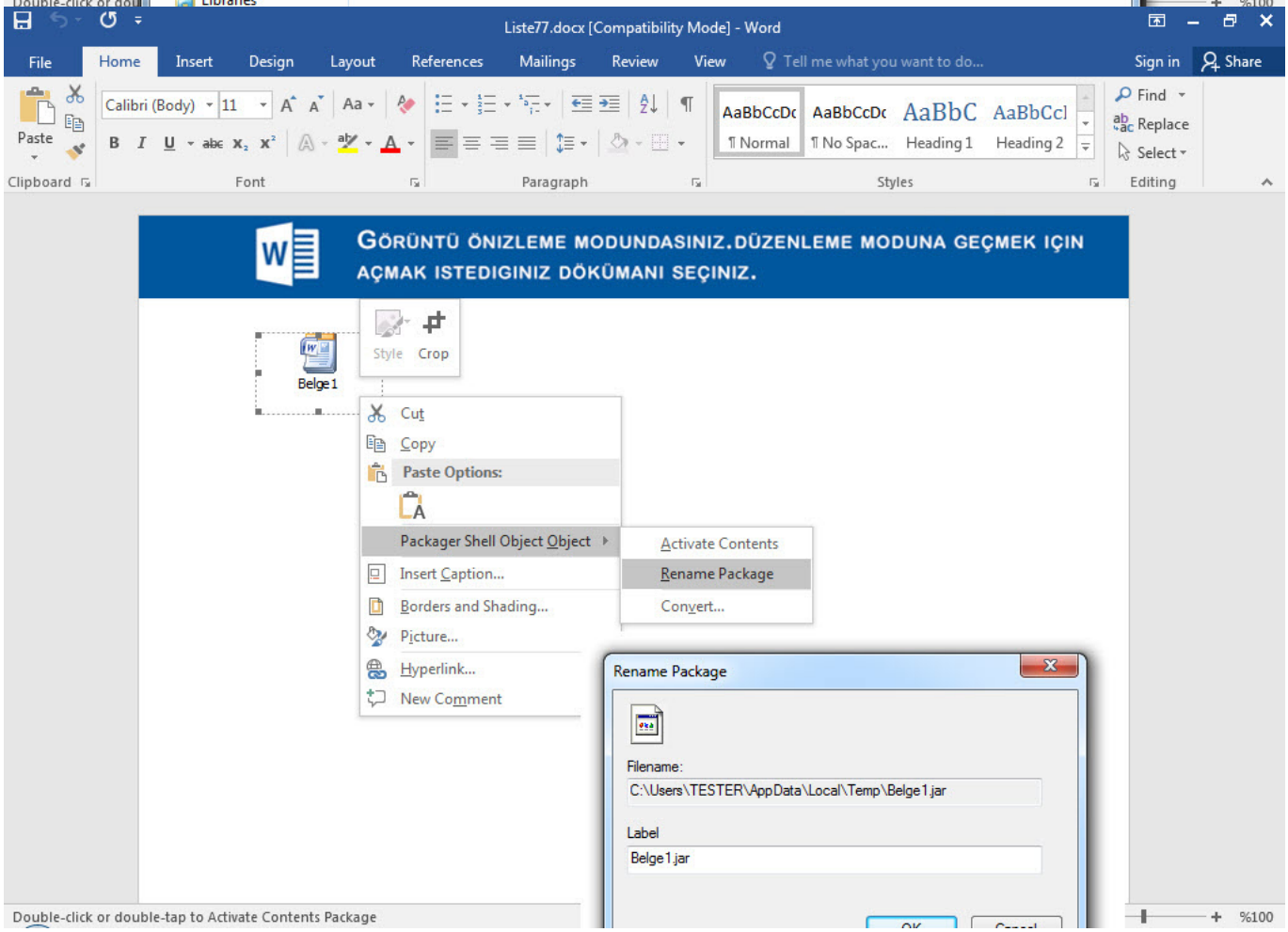
Daha önce başka bir blog yazıma daha konu olup sahte sipariş e-postaları ile hız kesmeden siber operasyonlarına devam edenlerin yıllar içinde taktik, teknik ve prosedürlerini değiştirdiklerini görebiliyoruz. Son aylarda özellikle şifreli RAR dosyaları (Liste54.rar, Ofis_Belgesi.rar, siparis_listesi.doc.rar, Siparisler.rar vb.) ile operasyonlarına devam edenlere karşı dışardan şifreli dosya kabul eden kurumların zor zamanlar yaşadıklarını tahmin etmesi güç değil. Bunun en temel sebebi ise şifreli RAR dosyası içinde yer alan çalıştırılabilir program (exe, jar), ofis dosyası (docx) güvenlik teknolojileri tarafından analiz edilemediği için son kullanıcının e-posta kutusuna iletiliyor ve bilgi güvenliği farkındalığı düşük olan son kullanıcı ve kurum için büyük bir tehdit haline geliyor.




VirusTotal Intelligence
VirusTotal
https://www.virustotal.com/#/file/4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905a8d0224b3/detection
Search or scan a URL, IP address, domain, or file hash
No engines detected this file
SHA-256 4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905a8d0224b3
File name Liste54.rar
File size 171.04 KB
Last analysis 2018-06-19 12:22:20 UTC
0 / 61
Detection
Details
Community
Ad-Aware Clean
AegisLab Clean
AhnLab-V3 Clean
ALYac Clean
Antiy-AVL Clean
Arcabit Clean
Avast Clean
Avast Mobile Security Clean
AVG Clean
Avira Clean
AVware Clean
Babable Clean
Baidu Clean
BitDefender Clean
Bkav Clean
CAT-QuickHeal Clean
ClamAV Clean
CMC Clean
Comodo Clean
Cyren Clean
DrWeb Clean
Emsisoft Clean
eScan Clean
ESET-NOD32 Clean
F-Prot Clean
F-Secure Clean
Fortinet Clean
GData Clean

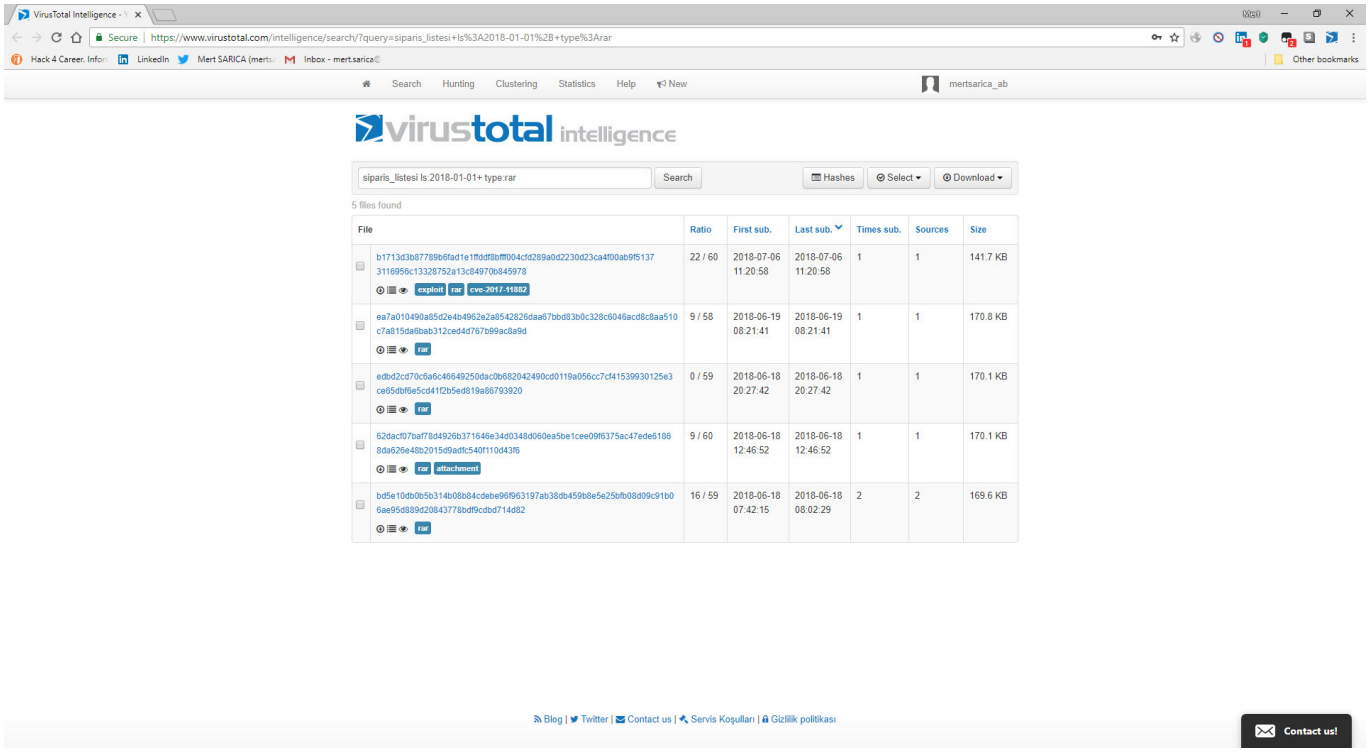
Ofis_Belgesi.rar (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
Protect
SFX
Ofis_Belgesi.rar - solid RAR archive, unpacked size 266.082 bytes
Name Size Packed Type Modified Checksum
.. File folder
Liste86.docx * 266.082 263.520 Microsoft Word D... 13.06.2018 13:34 F0622A28
RAR SIFRESI : 5465

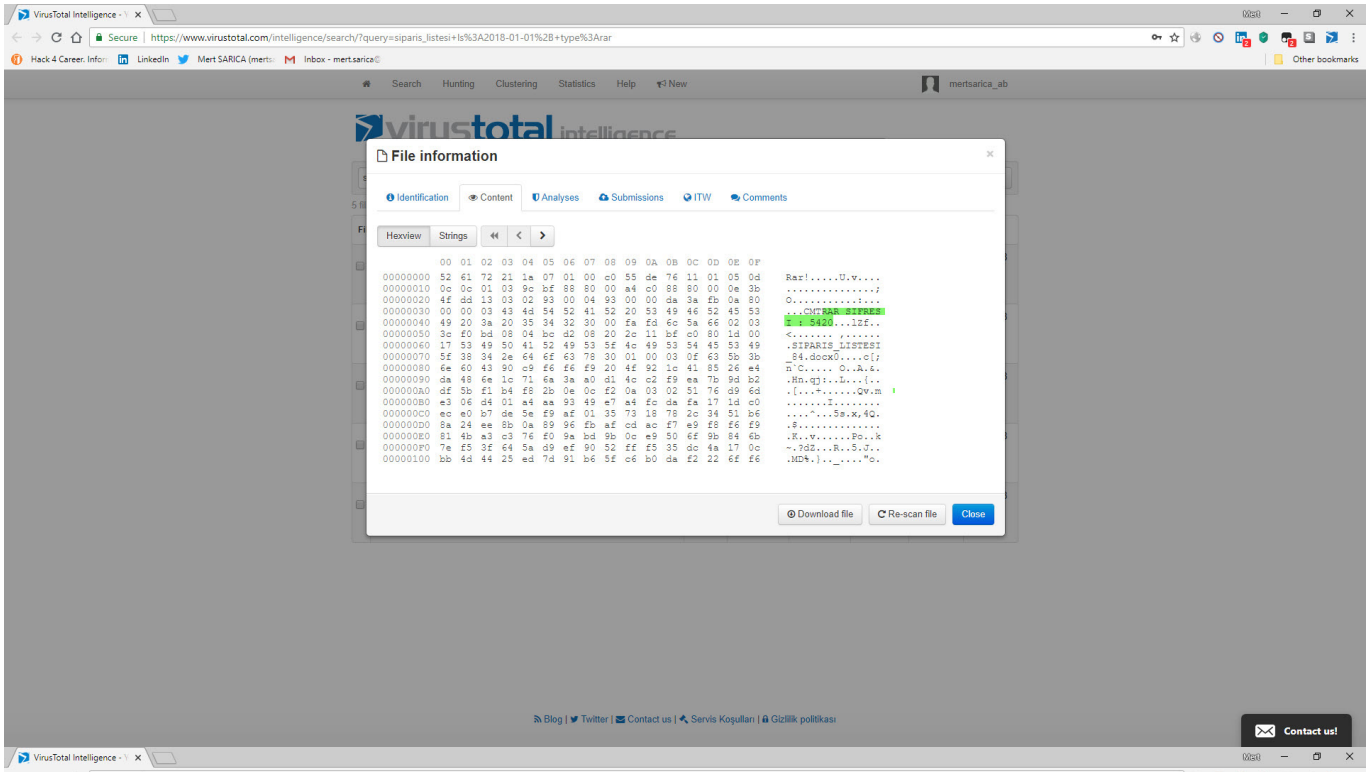

Liste86.docx [Compatibility Mode] - Word
GÖRÜNTÜ ÖNIZLEME MODUNDASINIZ.DÜZENLEME MODUNA GEÇMEK IÇIN AÇMAK ISTEDIGINIZ DÖKÜMANI SEÇINIZ.
OfficeDocuments
Rename Package
Filename:
C:\Users\TESTER\AppData\Local\Temp\OfficeDocuments.EXE
Label
OfficeDocuments.EXE
OK
Cancel
Mert ▸ AppData ▸ Local ▸ Temp ▸ OfficeDocuments
Search OfficeDocuments
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Name
Date modified
Type
Size
OfficeDocuments.jar
13.06.2018 13:28
Executable Jar File
98 KB

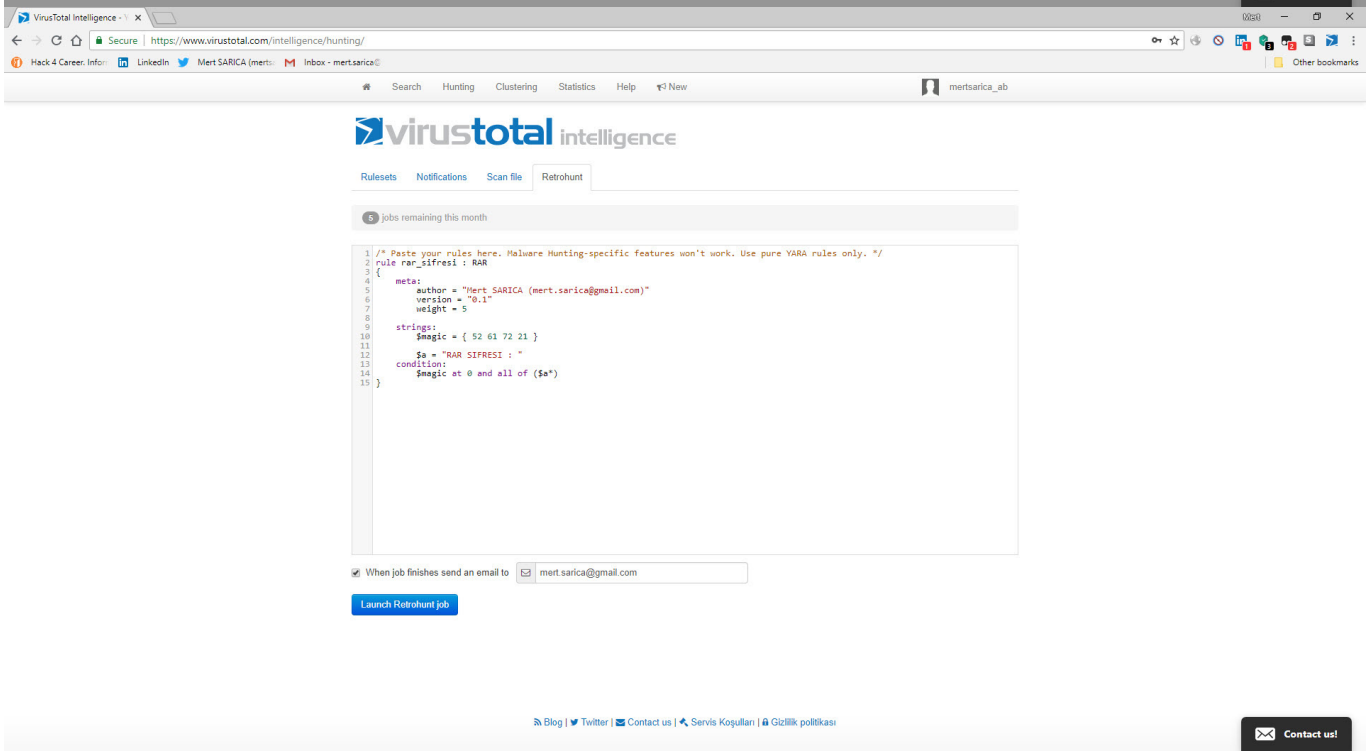

Liste77.docx [Compatibility Mode] - Word
GÖRÜNTÜ ÖNIZLEME MODUNDASINIZ.DÜZENLEME MODUNA GEÇMEK IÇIN AÇMAK ISTEDIGINIZ DÖKÜMANI SEÇINIZ.
Belge1
Style
Crop
Cut
Copy
Paste Options:
Packager Shell Object Object
Activate Contents
Rename Package
Convert...
Insert Caption...
Borders and Shading...
Picture...
Hyperlink...
New Comment
Rename Package
Filename:
C:\Users\TESTER\AppData\Local\Temp\Belge1.jar
Label
Belge1.jar
Double-click or double-tap to Activate Contents Package

Bu gibi tehditlerle mücadele edebilme adına Yara ile Tehdit Avı başlıklı blog yazımda olduğu gibi Yara aracından ve kurallarından faydalanabilirsiniz. Kendi yazdığınız bir Yara kuralını, kullandığınız herhangi bir güvenlik teknolojisinde devreye almadan önce hatalı tespite (false-positive) karşı olabildiğince fazla örnek üzerinde çalıştırmanızda, örneklerin her birini ayrı ayrı analiz etmenizde fayda olacaktır. Bunun için de VirusTotal'ın ücretli (premium) servislerinden faydalanabilirsiniz.

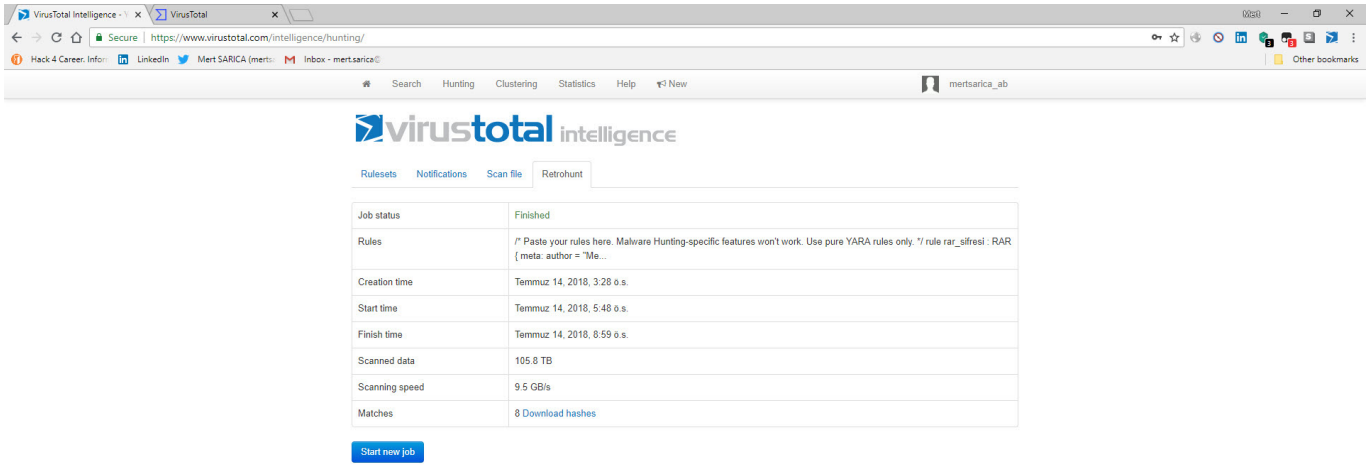
Hem örneklere ulaşmak hem de Yara kuralınızı test etmek için VirusTotal'ın Retrohunt ve Intelligence servislerini kullanabilirsiniz. Retrohunt ile hazırladığınız bir Yara kuralını terabaytlarca büyük veri setleri üzerinde çalıştırarak örneklere ulaşmak için kullanabiliyorsunuz. Örneğin şifreli RAR olarak gönderilen bir, iki örneğini ele alacak olursak, şifreyi çözmek için kullanılması gereken parolanın yine bu şifreli RAR dosyasının içinde yer aldığını VirusTotal Intelligence üzerinde yaptığımız bir arama görebiliyoruz. Bu bilgiden yola çıkarak hazırladığımız basit bir Yara kuralını Retrohunt sayesinde 100+ TB veri seti üzerinde, 9.5 GB/s hızla çalıştırarak, yaklaşık 3 saat içinde örneklere ulaşabiliyoruz.



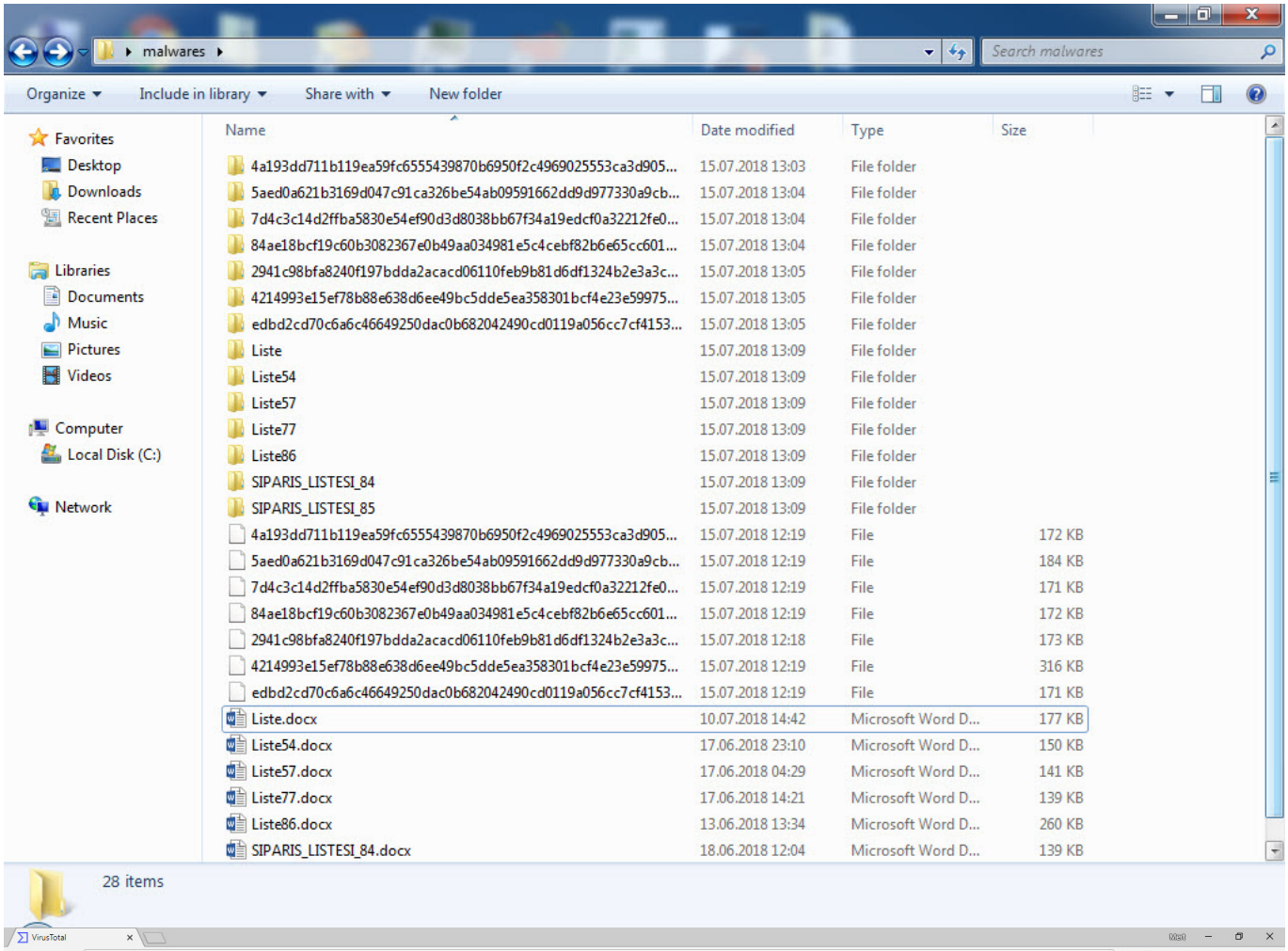


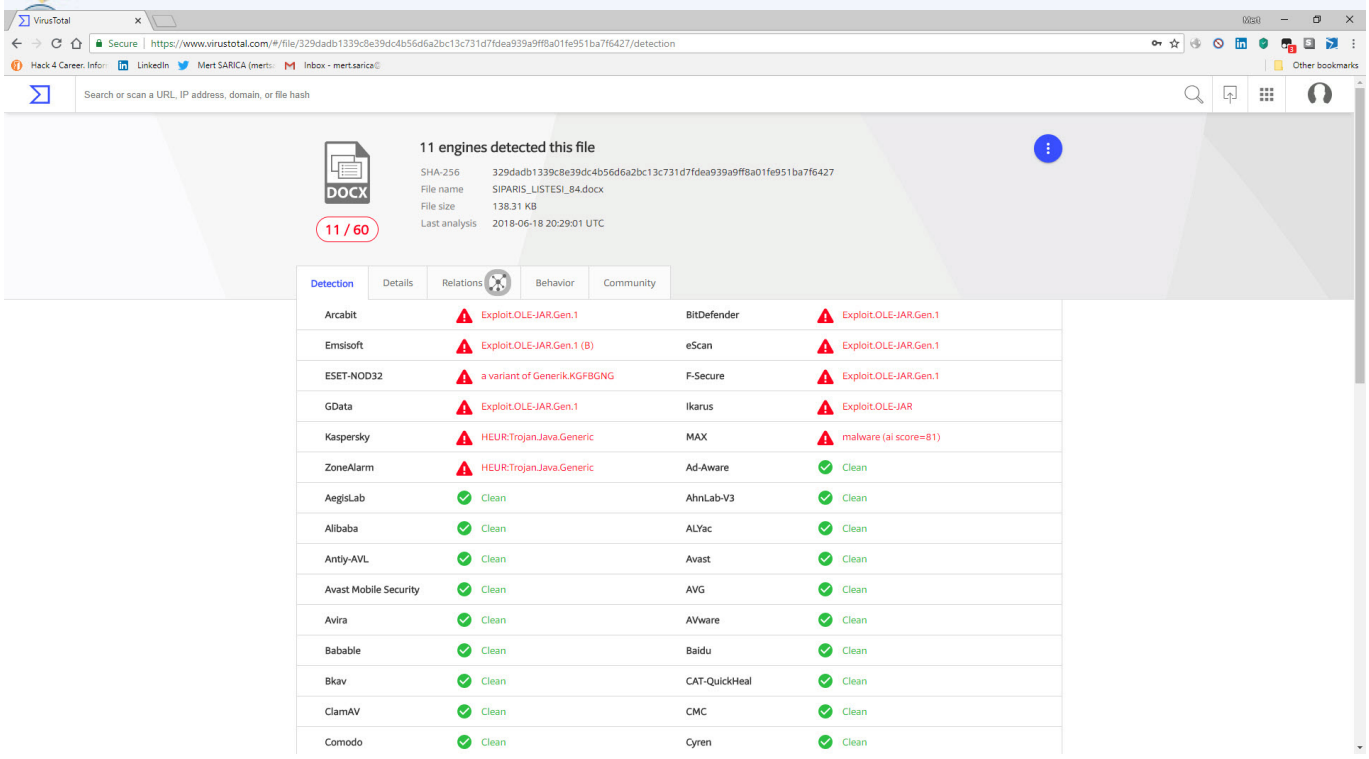


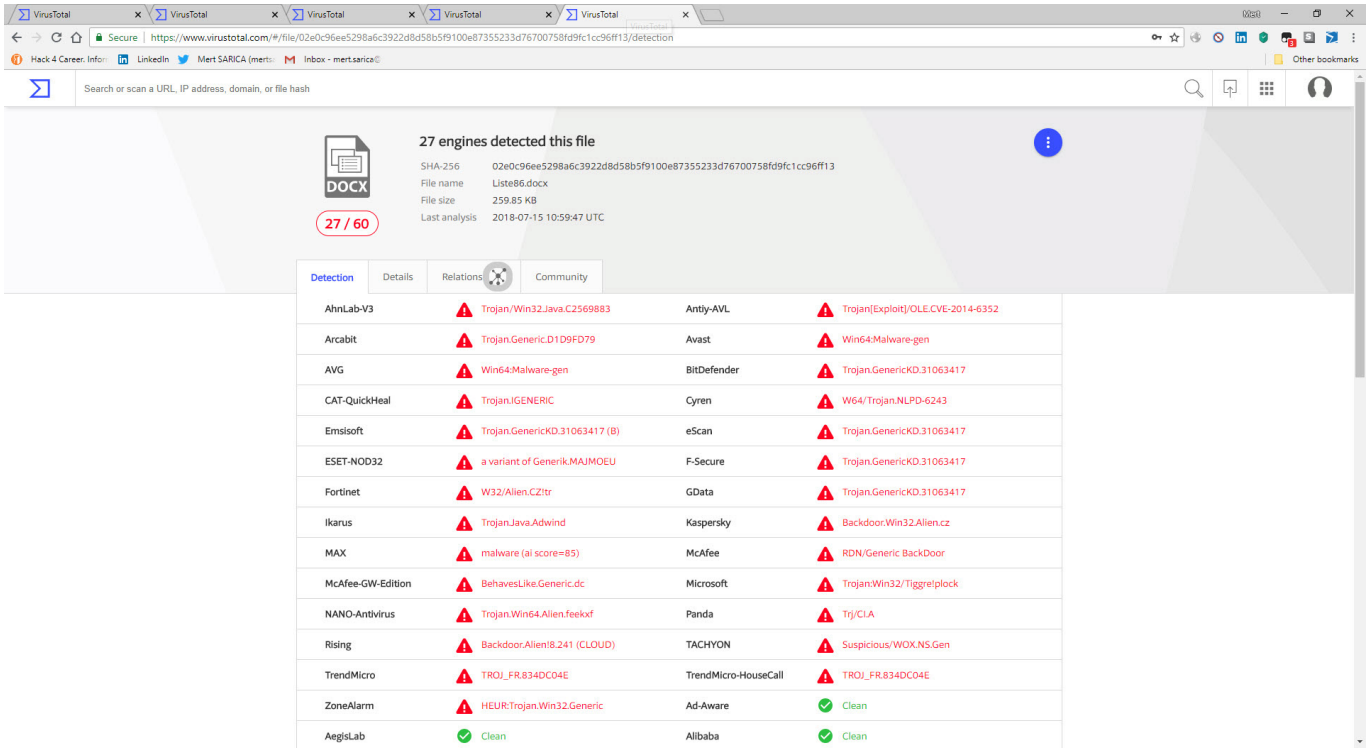

```
/* Paste your rules here. Malware Hunting-specific features won't work. Use pure YARA rules only. */
rule rar_sifresi : RAR
{
    meta:
        author = "Mert SARICA (mert.sarica@gmail.com)"
        version = "0.1"
        weight = 5

    strings:
        $magic = { 52 61 72 21 }

        $a = "RAR SIFRESI : "
    condition:
        $magic at 0 and all of ($a*)
}
```



Örnekleri teker teker indirip, şifresiz olarak VirusTotal'a geri yüklediğimizde çoğu antivirüs yazılımının bu örnekleri başarıyla tespit edebildiğini görebiliyoruz ancak zararlı yazılımlar şifreli olarak gönderildiği sürece güvenlik teknolojilerinde Yara kuralı kullanarak bunları engellemek veya şifreli dosyaların e-posta sunucusu üzerinde yasaklanmasını sağlamak kurumlar için en etkili çözümlerden biri haline geliyor.


malwares
Search malwares
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905... 15.07.2018 13:03 File folder
5aed0a621b3169d047c91ca326be54ab09591662dd9d977330a9cb... 15.07.2018 13:04 File folder
7d4c3c14d2ffba5830e54ef90d3d8038bb67f34a19edcf0a32212fe0... 15.07.2018 13:04 File folder
84ae18bcf19c60b3082367e0b49aa034981e5c4cebf82b6e65cc601... 15.07.2018 13:04 File folder
2941c98bfa8240f197bdda2acacd06110feb9b81d6df1324b2e3a3c... 15.07.2018 13:05 File folder
4214993e15ef78b88e638d6ee49bc5dde5ea358301bcf4e23e59975... 15.07.2018 13:05 File folder
edbd2cd70c6a6c46649250dac0b682042490cd0119a056cc7cf4153... 15.07.2018 13:05 File folder
Liste 15.07.2018 13:09 File folder
Liste54 15.07.2018 13:09 File folder
Liste57 15.07.2018 13:09 File folder
Liste77 15.07.2018 13:09 File folder
Liste86 15.07.2018 13:09 File folder
SIPARIS_LISTESI_84 15.07.2018 13:09 File folder
SIPARIS_LISTESI_85 15.07.2018 13:09 File folder
4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905... 15.07.2018 12:19 File 172 KB
5aed0a621b3169d047c91ca326be54ab09591662dd9d977330a9cb... 15.07.2018 12:19 File 184 KB
7d4c3c14d2ffba5830e54ef90d3d8038bb67f34a19edcf0a32212fe0... 15.07.2018 12:19 File 171 KB
84ae18bcf19c60b3082367e0b49aa034981e5c4cebf82b6e65cc601... 15.07.2018 12:19 File 172 KB
2941c98bfa8240f197bdda2acacd06110feb9b81d6df1324b2e3a3c... 15.07.2018 12:18 File 173 KB
4214993e15ef78b88e638d6ee49bc5dde5ea358301bcf4e23e59975... 15.07.2018 12:19 File 316 KB
edbd2cd70c6a6c46649250dac0b682042490cd0119a056cc7cf4153... 15.07.2018 12:19 File 171 KB
Liste.docx 10.07.2018 14:42 Microsoft Word D... 177 KB
Liste54.docx 17.06.2018 23:10 Microsoft Word D... 150 KB
Liste57.docx 17.06.2018 04:29 Microsoft Word D... 141 KB
Liste77.docx 17.06.2018 14:21 Microsoft Word D... 139 KB
Liste86.docx 13.06.2018 13:34 Microsoft Word D... 260 KB
SIPARIS_LISTESI_84.docx 18.06.2018 12:04 Microsoft Word D... 139 KB
28 items


VirusTotal
Search or scan a URL, IP address, domain, or file hash
DOCX
11 / 60
11 engines detected this file
SHA-256 329dadb1339c8e39dc4b56d6a2bc13c731d7fdea939a9ff8a01fe951ba7f6427
File name SIPARIS_LISTESI_84.docx
File size 138.31 KB
Last analysis 2018-06-18 20:29:01 UTC
Detection
Details
Relations
Behavior
Community
Arcabit Exploit.OLE-JAR.Gen.1
BitDefender Exploit.OLE-JAR.Gen.1
Emsisoft Exploit.OLE-JAR.Gen.1 (B)
eScan Exploit.OLE-JAR.Gen.1
ESET-NOD32 a variant of Generik.KGFBGNG
F-Secure Exploit.OLE-JAR.Gen.1
GData Exploit.OLE-JAR.Gen.1
Ikarus Exploit.OLE-JAR
Kaspersky HEUR:Trojan.Java.Generic
MAX malware (ai score=81)
ZoneAlarm HEUR:Trojan.Java.Generic
Ad-Aware Clean
AegisLab Clean
AhnLab-V3 Clean
Alibaba Clean
ALYac Clean
Antiy-AVL Clean
Avast Clean
Avast Mobile Security Clean
AVG Clean
Avira Clean
AVware Clean
Babable Clean
Baidu Clean
Bkav Clean
CAT-QuickHeal Clean
ClamAV Clean
CMC Clean
Comodo Clean
Cyren Clean



Sadede gelecek olursam, kimi zaman kurumunuz için yaptığınız binlerce dolarlık güvenlik teknolojileri yatırımları, tehditleri tespit etmekte yetersiz kalabilmektedir. Bu gibi durumlarda özellikle bünyelerinde Siber Güvenlik Merkezi, SOC barındıran kurumların, VirusTotal'ın ücretli hizmetlerinden faydalanmaları, Yara kuralı yazabilecek yetkinliğe sahip olmaları bu gibi basit ama etkili saldırılarla mücadelede önemli bir rol oynayacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.