

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.

Subject: meraba
From: corlupazarlama@
corlupazarlama@
To:
Originating IP:
SMTP Relay:
Attachments: Siparisler.rar (352 KB)

[Use Google Translate™](#)

*15 adet Siparisimiz Bulunmaktadır..
Lutfen geri donus yapin ..*

VirusTotal Intelligence - VirusTotal

Secure | <https://www.virustotal.com/#/file/4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905a8d0224b3/detection>

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

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)

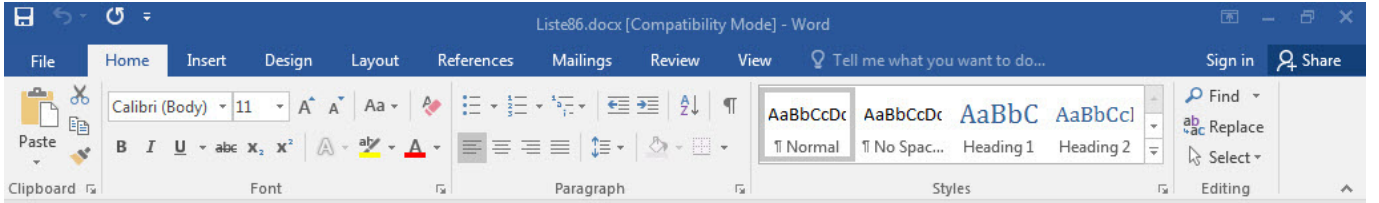
File Commands Tools Favorites Options Help

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

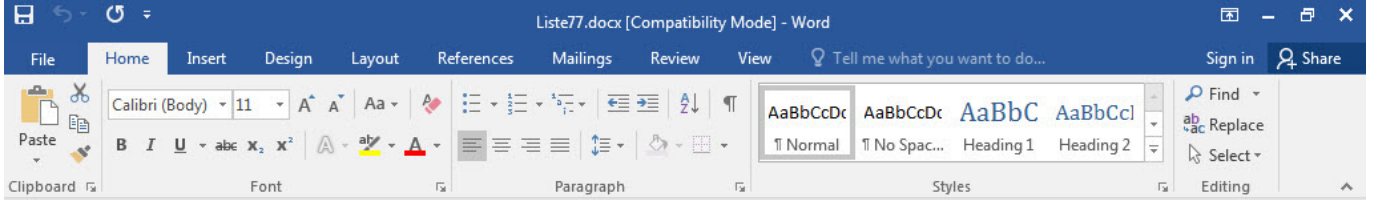
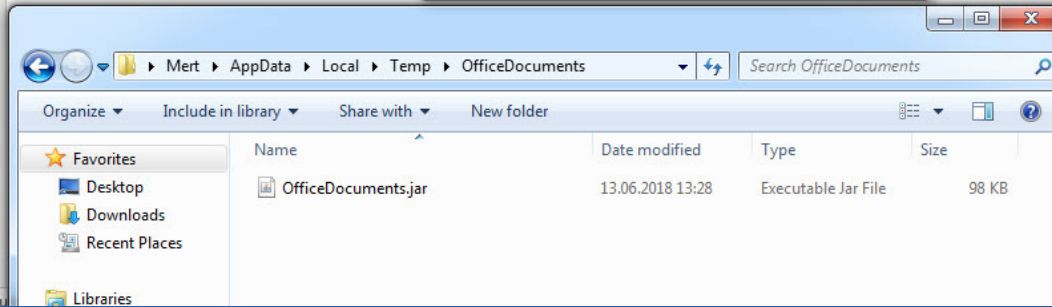
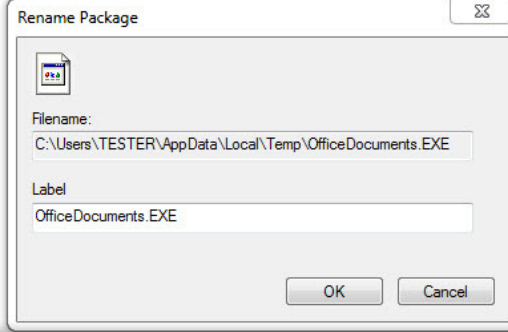
RAR SIFRESİ : 5465



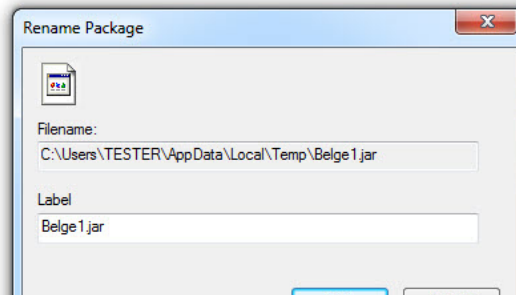
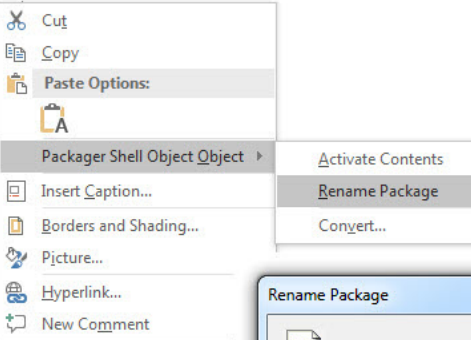
GÖRÜNTÜ ÖNİZLEME MODUNDASINIZ.DÜZENLEME MODUNA GEÇMEK İÇİN
AÇMAK İSTEDİĞİNİZ DÖKÜMANI SEÇİNİZ.



OfficeDocuments



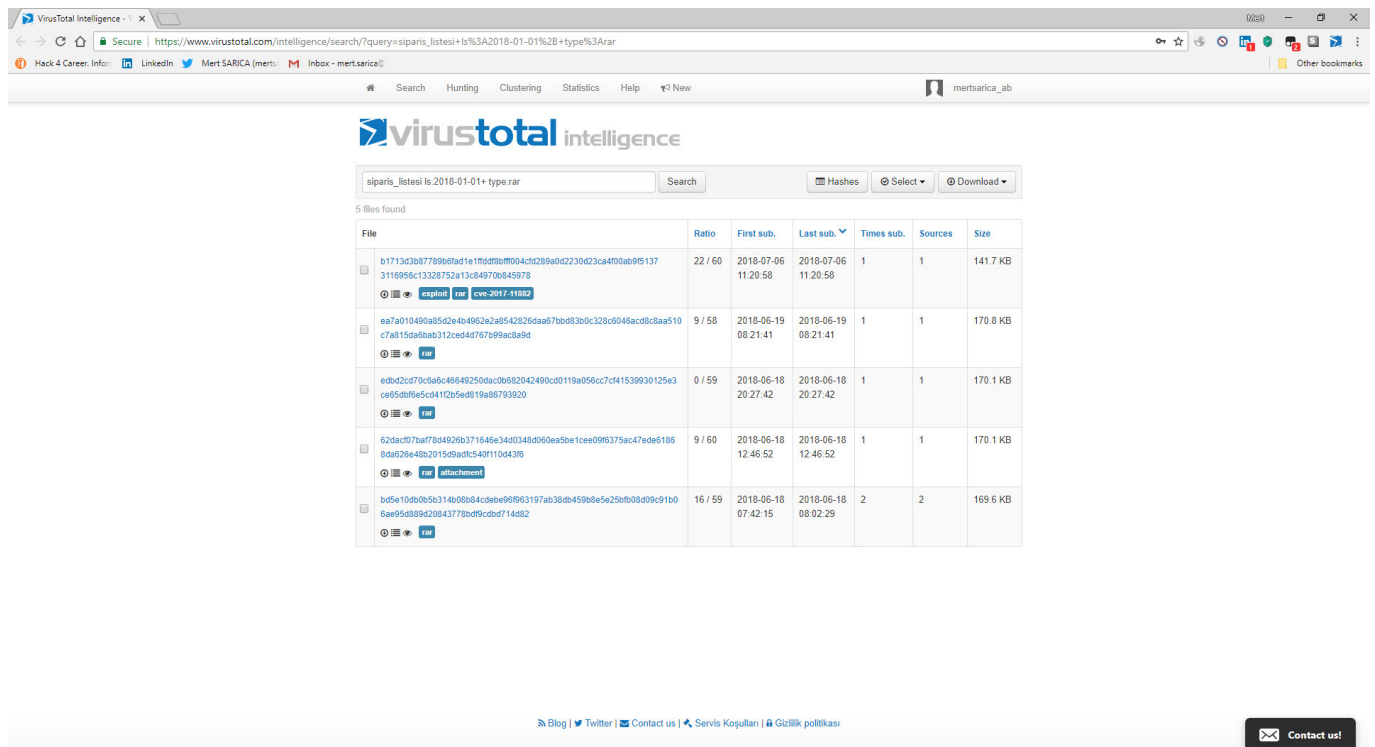
GÖRÜNTÜ ÖNİZLEME MODUNDASINIZ.DÜZENLEME MODUNA GEÇMEK İÇİN
AÇMAK İSTEDİĞİNİZ DÖKÜMANI SEÇİNİZ.



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.



The screenshot shows the VirusTotal Intelligence search results for a Yara rule. The search query is "siparis_listesi is 2018-01-01+ type rar". The results show 5 files found. The table below summarizes the data:

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
b713d3b87789b6fed1e1f0d9b0f004c3d289a0d2230d23ca4f00ab0951373118956c13328752a13c84970a845978	22 / 60	2018-07-06 11:20:58	2018-07-06 11:20:58	1	1	141.7 KB
ea7a010490a85d2e4b4962a2a8542826daa67bbd83b0c328c6046acd8baa510c7a815da60ab312ced4d767b99ac8a9d	9 / 58	2018-06-19 08:21:41	2018-06-19 08:21:41	1	1	170.8 KB
edbd2cd70c8a6c46649250da0b682042490cd0119a056cc7cd41539930125a3ce65dbf6e5cd412b5e8d19a88793920	0 / 59	2018-06-18 20:27:42	2018-06-18 20:27:42	1	1	170.1 KB
62dac07ba778d492b371645a340348d050ea5be1cee096375ac47ede61868da626e48b2015d9acfc540f11043b6	9 / 60	2018-06-18 12:46:52	2018-06-18 12:46:52	1	1	170.1 KB
bd5e19db0e5b314b08884c4bae86963197ab38db459b8e5e25bfb08d09c91b06ae95d89ac20843778bdf9cdd714d82	16 / 59	2018-06-18 07:42:15	2018-06-18 08:02:29	2	2	169.6 KB

VirusTotal Intelligence

Search Hunting Clustering Statistics Help

mertsarica_ab

File information

Identification Content Analyses Submissions ITW Comments

Hexview Strings

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	52	61	72	21	1A	07	01	00	C0	55	DE	76	11	01	05	0d	Raz!.....U.v....
00000010	0c	0c	01	03	9c	b7	88	80	00	a4	c0	88	80	00	0e	3b	
00000020	4f	dd	13	03	02	93	00	04	93	00	00	da	3a	f5	0a	80	
00000030	00	00	03	43	4d	54	52	41	52	20	53	49	46	52	45	53	RAR SIFRESI
00000040	49	20	3a	20	35	34	32	30	00	fa	fd	6c	5a	e6	02	03	... 5420...12f..
00000050	3c	e0	bd	08	04	bc	d2	08	20	2e	11	b6	c0	80	1d	00	<.....
00000060	17	53	49	50	41	52	49	53	5f	4c	49	53	54	45	53	49	SIPARIS SIFRESI
00000070	5f	38	34	2e	64	6f	63	78	30	01	00	03	0f	63	5b	3b	84.docx0....c()
00000080	6e	40	43	90	c9	f6	f6	f9	20	4e	92	16	41	85	26	e4	"C.....O.A.s.
00000090	da	48	6e	1c	71	6a	3a	a0	d1	4c	c3	e9	ea	7b	9d	b2	..h.ej.....()
000000a0	df	5b	f1	b4	f8	2b	0e	0c	e2	0a	03	02	51	76	d9	6d	.[...+.....QV.m
000000b0	e3	06	d4	01	a4	aa	93	49	e7	a4	fc	da	fa	17	1d	c0	2.....
000000c0	ec	a0	b7	de	5e	e9	af	01	35	73	18	78	2c	34	51	b6	5a.w.QQ.
000000d0	8a	24	ee	8b	0a	89	96	fb	af	cd	ac	e7	e9	f8	f6	f9	.8.....
000000e0	81	4b	a3	c3	76	e0	9a	bd	9b	0c	e9	50	6f	9b	84	6b	.R.v.....Po.k
000000f0	7e	25	3f	64	5a	d9	ef	90	52	ff	f5	35	dc	4a	17	0c	..7d2....R..S.J..
00000100	bb	4d	44	25	ed	7d	91	b6	5f	c6	b0	da	e2	22	6f	e6	.Jd2....."o.

Download file Re-scan file Close

Blog Twitter Contact us Servis Koşulları Gizlilik politikası

Contact us!

VirusTotal Intelligence

Rulesets Notifications Scan file Retrohunt

5 jobs remaining this month

```
1 /* Paste your rules here. Malware Hunting-specific features won't work. Use pure YARA rules only. */
2 rule rar_sifresi : RAR
3 {
4   meta:
5     author = "Mert SARICA (mert.sarica@gmail.com)"
6     version = "0.1"
7     weight = 5
8
9   strings:
10     $magic = { 52 61 72 21 }
11
12     $a = "RAR SIFRESI : "
13     condition:
14       $magic at 0 and all of ($a*)
15 }
```

☒ When job finishes send an email to

Launch Retrohunt job

Blog Twitter Contact us Servis Koşulları Gizlilik politikası

Contact us!

VirusTotal Intelligence

Rulesets Notifications Scan file Retrohunt

Job status	Finished
Rules	/ Paste your rules here. Malware Hunting-specific features won't work. Use pure YARA rules only. / rule rar_sifresi : RAR { meta: author = "Me..."
Creation time	Temmuz 14, 2018, 3:28 ö.s.
Start time	Temmuz 14, 2018, 5:48 ö.s.
Finish time	Temmuz 14, 2018, 8:59 ö.s.
Scanned data	105.8 TB
Scanning speed	9.5 GB/s
Matches	8 Download hashes

Start new job

Blog | Twitter | Contact us | Servis Koşulları | Gizlilik politikası

Contact us!

retrohunt_results

```
1 rar_sifresi:8f907054bbebaaa9ad052895bad6a2fa5b13445c99ac4b494ee4b91ee9addb81/subfile
2 rar_sifresi:5aed0a621b3169d047c91ca326be54ab09591662dd9d977330a9cbdb7b796834
3 rar_sifresi:4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905a8d0224b3
4 rar_sifresi:edbd2cd70c6a6c46649250dac0b682042490cd0119a056cc7cf41539930125e3
5 rar_sifresi:4214993e15ef78b88e638d6ee49bc5dde5ea358301bcf4e23e59975a21cd2c2e
6 rar_sifresi:7d4c3c14d2ffba5830e54ef90d3d8038bb67f34a19edcf0a32212fe04256c227
7 rar_sifresi:84ae18bcf19c60b3082367e0b49aa034981e5c4cebf82b6e65cc601eb722067a
8 rar_sifresi:2941c98bfa8240f197bdda2acacd06110feb9b81d6df1324b2e3a3c6365445e6
```

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					
Organize Include in library Share with New folder					
	Name	Date modified	Type	Size	
Favorites Desktop Downloads Recent Places Libraries Documents Music Pictures Videos Computer Local Disk (C:) Network	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					
Secure https://www.virustotal.com/#/file/329dad1339c8e39dc4b56d6a2bc13c731d7fdea939a9ff8a01fe951ba7f6427/detection					
Hack 4 Career, Info LinkedIn Mert SARICA (mert) Inbox - mertsarica@					
Search or scan a URL, IP address, domain, or file hash					
 11 engines detected this file 11 / 60 SHA-256 329dad1339c8e39dc4b56d6a2bc13c731d7fdea939a9ff8a01fe951ba7f6427 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 Generic.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	

VirusTotal

Secure | <https://www.virustotal.com/#/file/02e0c96ee5298a6c3922d8d58b5f9100e87355233d76700758fd9fc1cc96ff13/detection>

Search or scan a URL, IP address, domain, or file hash

27 engines detected this file

SHA-256: 02e0c96ee5298a6c3922d8d58b5f9100e87355233d76700758fd9fc1cc96ff13
File name: Liste86.docx
File size: 259.85 KB
Last analysis: 2018-07-15 10:59:47 UTC

27 / 60

Detection Details Relations Community

AhnLab-V3	Trojan.Win32.Java.C2569883	Antiy-AVL	Trojan[Exploit]/OLE.CVE-2014-6352
Arcabit	Trojan.Generic.D1D9FD79	Avast	Win64:Malware-gen
AVG	Win64:Malware-gen	BitDefender	Trojan.GenericKD.31063417
CAT-QuickHeal	Trojan.IGENERIC	Cyren	W64/Trojan.NLPD-6243
Emsisoft	Trojan.GenericKD.31063417 (B)	eScan	Trojan.GenericKD.31063417
ESET-NOD32	a variant of Generic.MAJMOEU	F-Secure	Trojan.GenericKD.31063417
Fortinet	W32/Allen.C2/tr	GData	Trojan.GenericKD.31063417
Ikarus	Trojan.Java.Adwind	Kaspersky	Backdoor.Win32.Allen.cz
MAX	malware (ai score=85)	McAfee	RDN/Generic BackDoor
McAfee-GW-Edition	BehavesLike.Generic.dc	Microsoft	Trojan.Win32/Tiggrelplock
NANO-Antivirus	Trojan.Win64.Allen.feekxf	Panda	Trj/CIA
Rising	Backdoor.Allen8.241 (CLOUD)	TACHYON	Suspicious/WOX.NS.Gen
TrendMicro	TROJ_FR.834DC04E	TrendMicro-HouseCall	TROJ_FR.834DC04E
ZoneAlarm	HEUR:Trojan.Win32.Generic	Ad-Aware	Clean
AegisLab	Clean	Alibaba	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.