

Pratik Veri Sızıntısı Analizi

written by Mert SARICA | 27 May 2023

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

Gerçekleştirdikleri fidye yazılım (ransomware) saldırıları ile 2021 yılında 180 milyon dolar gelir elde etmiş ve dünyanın sayılı siber suç çeteleri arasında yer almayı başarmış Rusya destekli Conti grubu, 2022 yılında Rusya'nın Ukrayna'yı işgal etmesi ile önemli bir dönemece gelmişti. Conti grubunun Rus işgalini desteklediğini açıklaması ile uluslararası grup üyeleri arasında oluşan fikir ayrılıkları neticesinde üyelerden biri @ContiLeaks isimli Twitter hesabından grubun kendi aralarında 2020-2021 yıllarında gerçekleştirdiği yazışmaları sızdırmaya başlamıştı ve sızıntılar, siber saldırılarda kullandıkları fidye yazılımlarının kaynak kodunun da sızdırılması ile devam etmişti.

The screenshot shows a Twitter profile for 'conti leaks' (@ContiLeaks). The profile bio is 'fuck ru gov' and it indicates the user joined in February 2022. There are 1 follower and 6,698 followers. The profile is followed by the user. Two tweets are visible: one from March 2nd about 'Ukraine will Rise! fresh jabber logs' and one from March 1st about 'conti source without locker src.'.

The image shows a screenshot of a Twitter profile page for 'conti leaks'. The profile has 28 tweets. The tweets are as follows:

- Tweet 1:** @ContiLeaks · 1 Mar
anonfiles.com/T6U9caL6x5/Scr...
anonfiles.com/V1Uec2Ldxa/baz...
anonfiles.com/X3U4cdL6x7/baz...
anonfiles.com/ZfU0c0Lex7/Scr...
anonfiles.com/bfV9cfL5xd/Scr...
anonfiles.com/deVdcaLbx6/Scr...
anonfiles.com/f1VfcbLdxe/Scr...
anonfiles.com/lfV7c2L8xa/con...
anonfiles.com/nfVbccL9x7/baz...
16 replies, 104 retweets, 216 likes
- Tweet 2:** @ContiLeaks · 1 Mar
anonfiles.com/f1VfcbLdxe/Scr...
2 replies, 22 retweets, 65 likes
- Tweet 3:** @ContiLeaks · 1 Mar
this is the 2020 chats: anonfiles.com/H8B7b1L4x6/2_t...
3 replies, 27 retweets, 68 likes
- Tweet 4:** @ContiLeaks · 27 Şub
conti jabber leaks anonfiles.com/VeP6K6K5xc/1_t...
18 replies, 146 retweets, 297 likes

The left sidebar shows navigation options: Anasayfa, Keşfet, Bildirimler, Mesajlar, Yer İşaretleri, Listeler, Profil, and Daha fazla. A 'Tweetle' button is visible. The user's profile information at the bottom left shows 'Mert SARICA' (@MertSARICA).

Bir siber güvenlik arařtırmacısı olarak bu gibi tehdit aktörlerine ait veriler sızdıđında en çok merakımı cezbeden konuların bařında bu veriler arasında Türkiye'de hacklenmiř bir sisteme ait bilgilerin ve de Rusça olmayan, özellikle Türkçe yazıřmaların, metinlerin yer alıp, almadığı oluyor. Neden diye soracak olursanız, bu tür sayılı tehdit aktörleri tarafından Türkiye'nin ne kadar geniş çapta hedef alındığını ve de bu tür uluslararası, organize, gruplarda hangi milletlerden üyelerin olduğunu öğrenme şansım olabiliyor.

Bu zamana dek bu merakımı gidermek için diđer güvenlik arařtırmacılarının analiz çalışmalarını ile yetinmeyi tercih etmiş biri olarak buna bir dur demeye, çok daha hızlı bir şekilde bu bilgiye nasıl ulaşabileceğimi öğrenmeye ve benim gibi bu konuya ilgili duyan siber güvenlik arařtırmacılarına fikir vermek için kolları sıvamaya karar verdim.

İlk iş olarak Conti grubuna ait yazıřmaların da yer aldığı dosyaları vx-underground isimli web sitesinin paylaşım alanından indirdim. Tüm dosyaları teker teker açtığımda içinden 11000'den fazla dosya çıktı.

Directory: Conti/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	2022-03-02 13:10:39
Conti Locker Leak.7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Conti Trickbot Leaks.7z	955850	2022-03-01 06:52:40
Training Material Leak	0	1969-12-31 18:00:00

```
mertrix@Hack4Career Leak % ls -al
total 0
drwxr-xr-x  14 mertrix  staff   448 Apr 10 20:33 .
drwxr-xr-x@  48 mertrix  staff  1536 Apr 10 20:10 ..
drwx----- 150 mertrix  staff  4800 Mar  1 11:34 Conti Chat Logs 2020
drwx-----  3 mertrix  staff   96 Mar  1 14:29 Conti Documentation Leak
drwx-----  14 mertrix  staff   448 Mar  1 11:56 Conti Internal Software Leak
drwx----- 398 mertrix  staff 12736 Mar  2 22:10 Conti Jabber Chat Logs 2021 - 2022
drwx-----  3 mertrix  staff   96 Mar  1 11:48 Conti Pony Leak 2016
drwx----- 10 mertrix  staff   320 Mar  1 11:47 Conti Rocket Chat Leaks
drwx-----  7 mertrix  staff   224 Mar  1 11:35 Conti Screenshots December 2021
drwx-----  4 mertrix  staff   128 Mar  1 11:39 Conti Toolkit Leak
drwx----- 55 mertrix  staff  1760 Mar  1 11:50 Conti Trickbot Forum Leak
drwx-----  4 mertrix  staff   128 Mar  1 15:52 Conti Trickbot Leaks
drwx-----  9 mertrix  staff   288 Apr 10 20:31 conti_locker
drwx-----  4 mertrix  staff   128 Apr 10 20:31 jabber_logs
mertrix@Hack4Career Leak % find . | wc -l
11289
mertrix@Hack4Career Leak %
```

Yazışmaların okunabilir metin olarak JSON uzantılı dosyalarda saklandığını (Örnek: 185.25.51.173-20220301.json) öğrendikten sonra ilk iş olarak tüm dosyalardaki IP adreslerini aşağıdaki regex destekli GREP komutu ile bulup, tekilleştirip ip.txt isimli bir dosyaya kaydettiğimde elimde toplamda bu 2 regex paternine uyan 3819 tane IP adresi oldu.

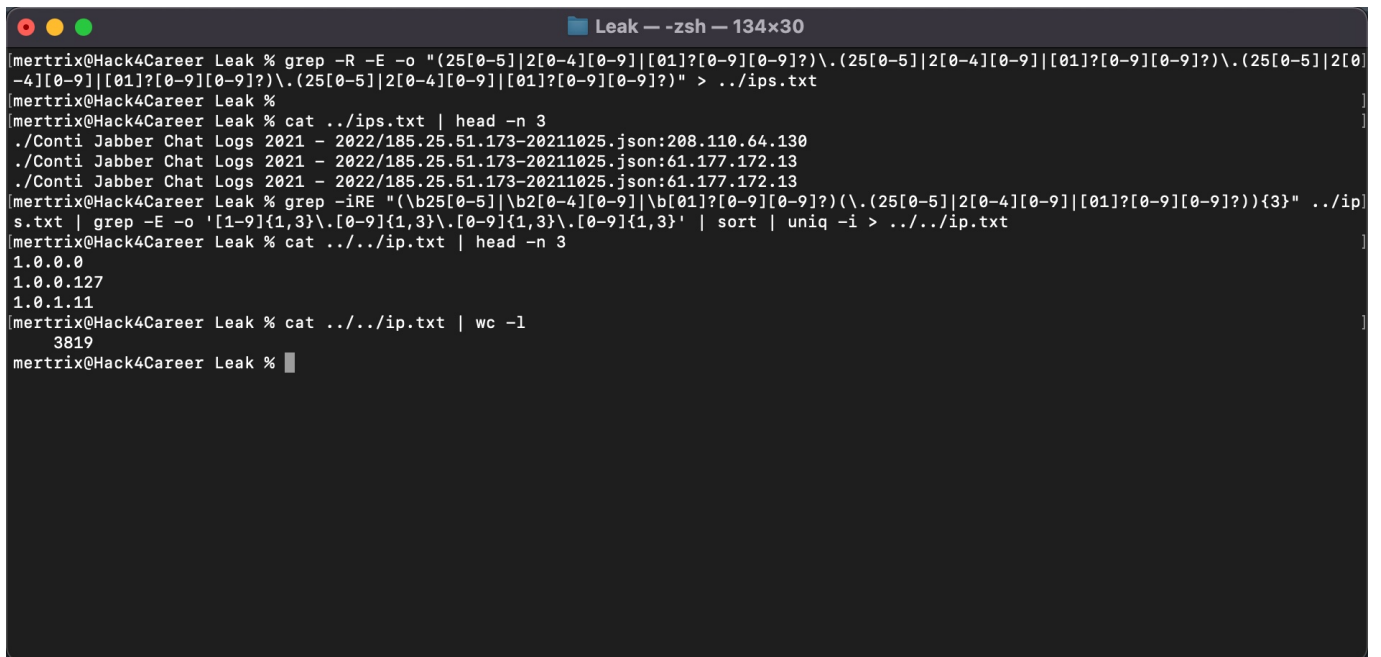
```
grep -R -E -o
```

```
"(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" > ../ips.txt
```

```
grep -iRE
```

```
"(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" ..../ips.txt | grep -E -o
```

```
'[1-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | sort | uniq -i > ..../ip.txt
```



```
mertrix@Hack4Career Leak % grep -R -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" > ../ips.txt
mertrix@Hack4Career Leak %
mertrix@Hack4Career Leak % cat ../ips.txt | head -n 3
./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20211025.json:208.110.64.130
./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20211025.json:61.177.172.13
./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20211025.json:61.177.172.13
mertrix@Hack4Career Leak % grep -iRE "(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" ..../ips.txt
mertrix@Hack4Career Leak % cat ..../ip.txt | head -n 3
1.0.0.0
1.0.0.127
1.0.1.11
mertrix@Hack4Career Leak % cat ..../ip.txt | wc -l
3819
mertrix@Hack4Career Leak %
```

Sıra bu IP adreslerinden hangilerinin Türkiye'ye ait olduğunu bulmaya geldiğinde imdadıma IPinfo API'si ve Python kütüphanesi yetiştirdi. Elimdeki tüm IP adreslerini (ip.txt) bu kütüphaneden faydalanarak geliştirdiğim IP2Geo Tool v2 isimli araç ile sorguladığımda, bu IP adreslerinden 2 tanesinin (31.210.111.142, 5.188.168.19) Türkiye'de bulunduğunu öğrenmiş oldum.

platform.socradar.com/threathose?query=5.188.168.190

5.188.168.190

Stealer Logs Public Repos Public Buckets Reputation Data

IP INTEL CARD

5.188.168.190
High Risk
Go to All Events

1000/1000

Risk Score	1000/1000
IP Address	5.188.168.190
Network	5.188.168.0/23
Country/City	Turkey/Istanbul
Penalty Reasons	Threathose (100%)

© Socradar evaluates many factors to determine likelihood of ip addresses being used in malicious and unwanted activities and assigns a risk score, from 0-1000, to rate the IP address activity. Score close to 0 indicates of very low risk.

platform.socradar.com/threathose?query=5.188.168.190

Search Result Public Code Repositories 2698

All Records Attack Type Country Malicious Software Operating System Product Region

Results are searched from 07 Mar 2022 to 10 Apr 2022 (You can select date range to see results between specified dates)

<https://share.vx-underground.org/Conti/c...>
Tag: #Angular #Armenia #Asns #Backdoor See More 13 Mar 2022

5.188.168.190 30t36SBP2z0W | Turkey \ n \ n186.216.125.178 system OkwKcECs8qJP2Z \ n177.190.69.162 admin 0l0ctyQh243063uD \ n45.235.6.161 system OkwKcECs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh243063uD \ n170.84.78.86 system OkwKcECs8qJP2Z \ n170.247.15.165 system OkwKcECs8qJP2Z \ ...
Showing only first 300 characters, see full details

<https://share.vx-underground.org/Conti/c...>
Tag: #Accommodation & food services #Android #Backdoor #Bitcoin addresses See More 13 Mar 2022

5.188.168.190 30t36SBP2z0W | Turkey \ n \ n186.216.125.178 system OkwKcECs8qJP2Z \ n177.190.69.162 admin 0l0ctyQh243063uD \ n45.235.6.161 system OkwKcECs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh243063uD \ n170.84.78.86 system OkwKcECs8qJP2Z \ n170.247.15.165 system OkwKcECs8qJP2Z \ ...
Showing only first 300 characters, see full details

Results are searched from 13 Mar 2021 to 10 Apr 2022 (You can select date range to see results between specified dates)

<https://www.ipvvoid.com>

Sıra merak ettiğim diğer konuya geldiğinde metinden dil tespiti yapabilen Python kütüphanelerine göz atmaya karar verdim. Kısa bir araştırma yaptıktan sonra karşıma bu alanda öne çıkan fastText, langdetect, langid kütüphaneleri çıktı.

Kütüphaneleri teker teker Conti'nin sızan verilerindeki metinler üzerinde test ederken kütüphanelerin kimi metinler için doğru kimi metinler için hatalı dil tespiti yaptığını gördüm. Hangisini kullanacağım konusunda kara kara düşünürken üçünden de faydalanan bir araç geliştirmeye ve kullanan kişinin ihtiyacına, tercihi göre güvenilirlik seviyesi (confidence level)

parametresi ile bu aracı kullanmasının daha doğru bir yol olacağına karar kıldım.

```
find . -type f -print -exec cat {} \; > ../logs.txt
```

komutu ile Conti'nin sızan verilerini tek bir dosyada birleştirdikten sonra geliştirdiğim Language Identification aracı ile logs.txt dosyasındaki her bir satırın Türkçe dil tespitine yönelik olarak üç kütüphane tarafından (güven seviyesi olarak High parametresini belirttim) kontrol ettim.

Language Identification aracını kullanmak için ilk parametre olarak öncelikle satır satır analiz edilmesini istediğiniz metin dosyasını belirtmeniz gerekmektedir. İkinci parametre olarak ise hangi dile dair tespit gerçekleştirmesini istiyorsanız o dilin kodunu (Türkçe ise TR, İngilizce ise EN gibi) belirtmeniz gerekmektedir. Opsiyonel parametre olan 3. parametre ise güven seviyesini belirlemektedir. Bu seviyeyi High olarak belirlerseniz üç kütüphanenin de belirttiğiniz dil kodunu tespit etmesi durumunda bunu ekranda belirtecektir.

Örnek kullanım: `python3 lang_id.py logs.txt TR High`

Metin dosyalarında herhangi bir Türkçe kelime, cümle kullanılmadığı için üç kütüphane tarafından Türkçe dil kullanımına dair herhangi bir tespit olmadı. Aracın düzgün çalıştığını test etmek için ise logs.txt dosyasına Türkçe sahte 3 metin eklediğimde ise programın başarıyla bunları tespit ettiğini görmüş oldum. Bu analiz sayesinde Conti'nin sızan verilerine göre grup üyeleri arasında Türkçe konuşulmadığını öğrenmiş ve merak ettiğim son konuyu da netleştirmiş oldum.

```
lang_id.py logs.txt UNREGISTERED
./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20210823.json
1 {
2   "ts": "2021-08-23T06:17:46.326321",
3 }
4 "from": "driver@q3mcco35auwcstmt.onion",
5 "to": "hofeq3mcco35auwcstmt.onion",
6 "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
7 }
8 {
9   "ts": "2021-08-23T06:21:29.401324",
10  "from": "driver@q3mcco35auwcstmt.onion",
11  "to": "defender@q3mcco35auwcstmt.onion",
12  "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
13 }
14 {
15   "ts": "2021-08-23T06:43:20.480030",
16   "from": "driver@q3mcco35auwcstmt.onion",
17   "to": "hofeq3mcco35auwcstmt.onion",
18   "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
19 }
20 Selam merhaba nasilsin ? (test i\u00e7in eklenmi\u015ftir)
21 Sosyal medyayı olduk\u00e7a etkin kullanan bir g\u00fcvenlik ara\u015ft\u0438rmacısı olarak bu z
22 arından blog yazılarına, sunumlara \u00e7evirdi\u011fimi biliyorsunuzdur. \u00c7ıkış noktası
23 \u00fczerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı g\u00f6rebil
24 {
25   "ts": "2021-08-23T06:43:46.773096",
26   "from": "hofeq3mcco35auwcstmt.onion",
27   "to": "driver@q3mcco35auwcstmt.onion",
28   "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
29 }
30 {
31   "ts": "2021-08-23T06:44:22.941040",
32   "from": "driver@q3mcco35auwcstmt.onion",
33   "to": "hofeq3mcco35auwcstmt.onion",
34   "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
35 }
36 {
37   "ts": "2021-08-23T06:45:20.386289",
38   "from": "hofeq3mcco35auwcstmt.onion",
39   "to": "driver@q3mcco35auwcstmt.onion",
40   "body": "[\u041e\u0448\u0438\u0431\u043a\u0430: \u0441\u043e\u043e\u0431\u0449\u0435\u043d\u0438\u0435 \u0437\u0430\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u043d\u043e, \u0438 \u043d\u0435\u0432\u043e\u0437\u043c\u043e\u0436\u043d\u043e \u0435\u0433\u043e \u0440\u0430\u0441\u0448\u0438\u0444\u0440\u043e\u0432\u0430\u0442\u044c.]"
41 }
42 {
43   "ts": "2021-08-23T08:00:32.458165",
44   "from": "bentley@q3mcco35auwcstmt.onion",
45   "to": "many@q3mcco35auwcstmt.onion",
46   "body": "\u041f\u0440\u0438\u0432\u0435\u0442, \u0431\u0440\u043e. \u041a\u0440\u0438\u043f\u0442\u0430\u043d\u0435\u043c \u0434\u043b\u043c?"
47 }

```

```
Conti - Python lang_id.py logs.txt TR High - 115x31
=====
Language Identification v1.0 [https://www.mertsarica.com]
=====
Language Code:TR Confidence Level:High Text:Selam merhaba nasilsin ? (test i\u00e7in eklenmi\u015ftir)
Language Code:TR Confidence Level:High Text:Sosyal medyayı olduk\u00e7a etkin kullanan bir g\u00fcvenlik ara\u015ft\u0438rmacısı olarak
bu zamana dek sosyal a\u011flar, e-postalar \u00fczerinden ald\u0131\u011fım mesajları g\u00fcvenlik ara\u015ft\u0438rmalarına ve ardından blog yazı
larına, sunumlara \u00e7evirdi\u011fimi biliyorsunuzdur. \u00c7ıkış noktası di\u011ferleri ile aynı olan bu hikayede ise m\u00fc\u015fteri g\u00fcvenli
ğini sa\u011flamak amacıyla sosyal a\u011f \u00fczerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı g\u00f6rebilirsin
iz. (test i\u00e7in eklenmi\u015ftir)
```

İzlediğim bu yöntemin ve geliştirmiş olduğum iki aracın bu gibi veri sızıntılarında güvenlik araştırmacıları, uzmanları için fayda sağlayacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.