

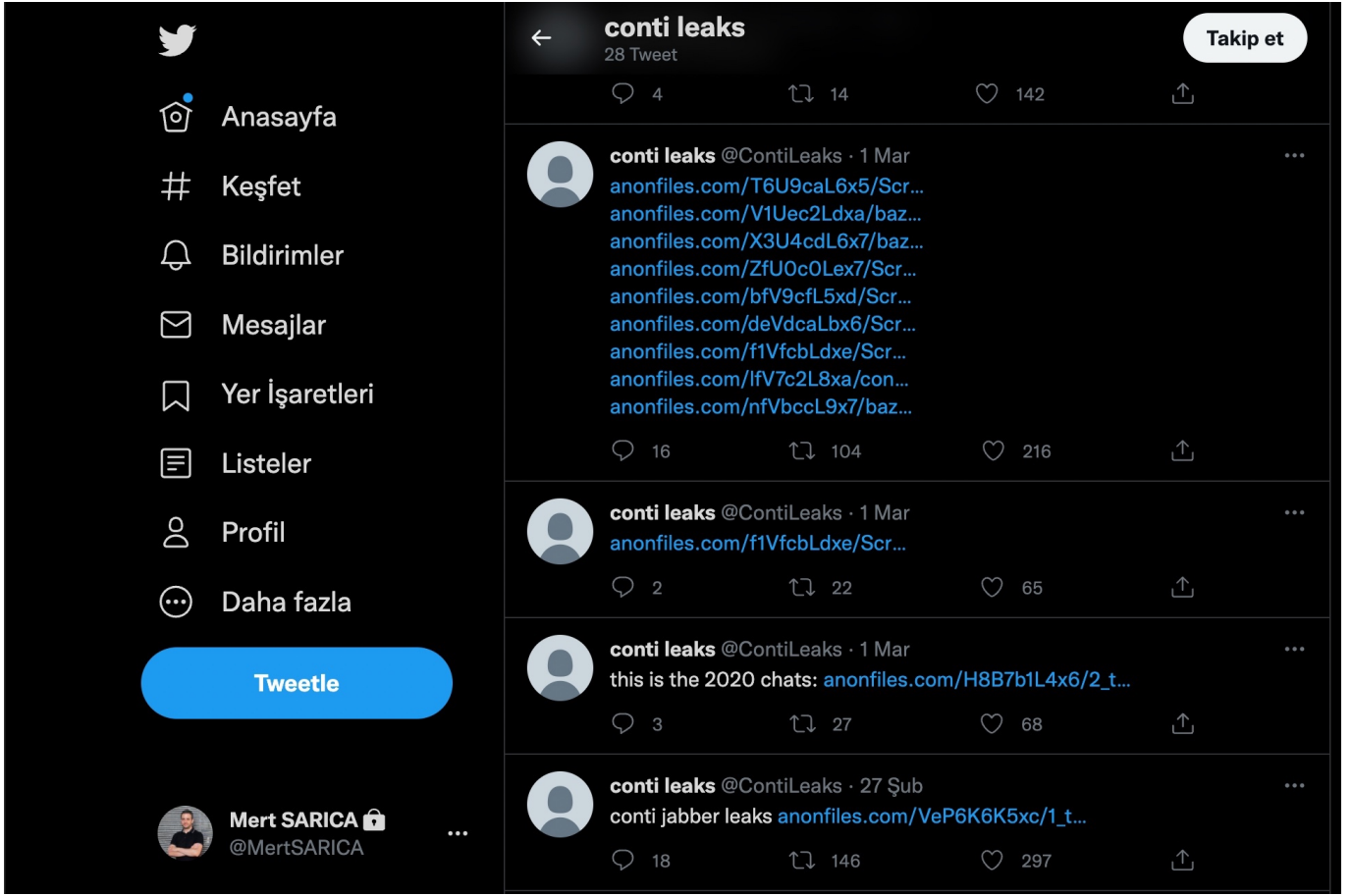
Pratik Veri Sızıntısı Analizi

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 the Twitter profile of @ContiLeaks. The profile bio is "fuck ru gov" and "Şubat 2022 tarihinde katıldı". It has 1 follower and 6,698 followers. The profile picture is a blue circle with a white outline. The header shows "conti leaks" with 28 tweets. The main content area shows two tweets: one from 2 Mar about "Ukraine will Rise! fresh jabber logs" and another from 1 Mar about "conti source without locker src.".



Bir siber güvenlik araştırmacısı olarak bu gibi tehdit aktörlerine ait veriler sızdığında en çok merakımı cezbeden konuların başında bu veriler arasında Türkiye’de hacklenmiş bir sisteme ait bilgilerin ve de Rusça olmayan, özellikle Türkçe yazışmaların, 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 diğer güvenlik araştırmacılarının analiz çalışmaları 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 araştırmacılarına fikir vermek için kolları sıvamaya karar verdim.

İlk iş olarak Conti grubuna ait yazışmaların 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]?)" > ../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]?)" > ../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]?)" > ../ip
s.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 % 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 yetiştii. 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.

```
Desktop — Python ip2geo.py — 134x30
=====
IP2Geo Tool v2 [https://www.mertsarica.com]
=====
1.0.0.0 AU Brisbane
1.0.0.127 AU Brisbane
1.0.1.11 CN Beijing
1.1.0.1 CN Beijing
1.1.1.1 US Los Angeles
1.13.2.28 CN Shenzhen
1.2.0.17 CN Beijing
1.2.1.0 CN Beijing
1.2.3.0 AU Brisbane
1.2.3.255 AU Brisbane
1.2.3.4 AU Brisbane
1.21.2.1 JP Osaka
1.3.0.0 CN Beijing
1.3.135.29 CN Beijing
1.3.35.45 CN Beijing
1.33.23.183 JP Tokyo
1.35.17.221 TW Taipei
1.4.29.0 CN Beijing
1.48.76.146 CN Guizhou

Desktop — -zsh — 80x24
[mertrix@Hack4Career Desktop % grep ":TR:" location.txt
31.210.111.142:TR:Istanbul
5.188.168.190:TR:Bahçelievler

Conti — -zsh — 87x40
mertrix@Hack4Career Conti % grep 5.188.168.190 ips.txt
/Conti Chat Logs 2020/185.25.51.173-20200625.json:5.188.168.190
/Conti Chat Logs 2020/185.25.51.173-20200625.json:5.188.168.190
/Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20210513.json:31.210.111.142
mertrix@Hack4Career Conti %

Leak — nano Conti Chat Logs 2020/185.25.51.173-20200625.json — 96x23
GNU nano 2.0.6 File: Conti Chat Logs 2020/185.25.51.173-20200625.json
{
  "ts": "2020-06-25T18:44:47.513880",
  "from": "prico@q3mcco35auwcstmt.onion",
  "to": "target@q3mcco35auwcstmt.onion",
  "body": "с женой детьми, животными встречусь"
}
{
  "ts": "2020-06-25T18:48:12.975279",
  "from": "kagas@q3mcco35auwcstmt.onion",
  "to": "defender@q3mcco35auwcstmt.onion",
  "body": "5.188.168.190 [Turkey\\n\\n186.216.125.178 system OkwKcEc8qJP22\\n1$
}
{
  "ts": "2020-06-25T18:48:31.813975",
  "from": "kagas@q3mcco35auwcstmt.onion",
  "to": "green@q3mcco35auwcstmt.onion",
  "body": "\\nroot 185.172.129.178 8m0086EzS53d [United States\\nroot 81.177.141.219 XUVmh$
}
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^N Next Page ^U UnCut Text ^T To Spell

Conti Jabber Chat Logs 2021 - 2022 — nano 185.25.51.173-20210513.json — 99x24
GNU nano 2.0.6 File: 185.25.51.173-20210513.json Modified
{
  "ts": "2021-05-13T16:40:48.630631",
  "from": "bentley@q3mcco35auwcstmt.onion",
  "to": "netwalker@q3mcco35auwcstmt.onion",
  "body": "10437177 \\tBZQKXOFVINZLSH_W629200.F43FE097769B17A28BBAE29198866EDD \\tnet16 \\t2021-05-1$
}
{
  "ts": "2021-05-13T16:40:55.167472",
  "from": "bentley@q3mcco35auwcstmt.onion",
  "to": "netwalker@q3mcco35auwcstmt.onion",
  "body": "windows 7 x64 SP1 \\t31.210.111.142\\tTR \\t22\\n10439894 \\tDESKTOP-D019GDM_W10018363.B770F85F7E69D33$
}
{
  "ts": "2021-05-13T16:41:11.997127",
  "from": "netwalker@q3mcco35auwcstmt.onion",
  "to": "bentley@q3mcco35auwcstmt.onion",
  "body": "я встаете вижу да"
}
{
  "ts": "2021-05-13T16:41:18.756743",

```

Elde etmiş olduğum sonucu doğrulamak için ise veri sızıntılarını analiz ederek kurumları anlık olarak haberdar eden Siber Tehdit İstihbarat Platformu SOCRadar'a göz attığımda, sonuçların örtüştüğünü görmüş ve merak ettiğim ilk konuyu açıklığa kavuşturmuş oldum. :)

The screenshot displays the Socradar platform interface. The top navigation bar includes links for 'Hack 4 Career. Inf...', 'LinkedIn', 'Mert SARICA (mer...', and 'Inbox - mert.saric...'. The left sidebar lists various security tools and services: Digital Risk Protection, Cyber Threat Intelligence, ThreatHose, ThreatShare, Vulnerability Intelligence, Threat Feed / IOC, Phishing Radar, Threat Actors, Combolist, Malware Analysis, Threat Reports, Breach Datasets, Incidents, Reports, Settings, and Stats & Status.

The main content area shows the 'IP INTEL CARD' for the IP address 5.188.168.190. The card includes a risk score of 1000/1000, a high risk status, and a 'Go to All Events' link. A semi-circular gauge shows the risk score. Below the gauge, a table lists the following information:

Risk Score	1000/1000
IP Address	5.188.168.190
Network	5.188.168.0/23
Country/City	Turkey/Istanbul
Penalty Reasons	1 Threatose (100%)

A map of Turkey is shown on the right side of the card. Below the table, a note states: '© 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 closing to 0 indicates of very low risk.'

The bottom section shows search results for public code repositories. The search criteria are: All Records, Attack Type, Country, Malicious Software, Operating System, Product, and Region. The results are filtered for the date range 07 Mar 2022 to 10 Apr 2022. Two results are shown:

- Result 1: <https://share.vx-underground.org/Conti/c...> (13 Mar 2022). Tag: #Angular #Armenia #Asns #Backdoor. See More. The snippet shows: `5.188.168.190 30t365BP2z0W | Turkey \ n \ n186.216.125.178 system 0kwKcCs8qJP2Z \ n177.190.69.162 admin 0l0ctyQh243063u0 \ n45.235.6.161 system 0kwKcCs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh243063u0 \ n170.84.78.86 system 0kwKcCs8qJP2Z \ n170.247.15.165 system 0kwKcCs8qJP2Z \ ...`
- Result 2: <https://share.vx-underground.org/Conti/c...> (13 Mar 2022). Tag: #Accommodation & food services #Android #Backdoor #Bitcoin addresses. See More. The snippet shows: `5.188.168.190 30t365BP2z0W | Turkey \ n \ n186.216.125.178 system 0kwKcCs8qJP2Z \ n177.190.69.162 admin 0l0ctyQh243063u0 \ n45.235.6.161 system 0kwKcCs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh243063u0 \ n170.84.78.86 system 0kwKcCs8qJP2Z \ n170.247.15.165 system 0kwKcCs8qJP2Z \ ...`

The bottom section also shows a result for <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 düşünürken üçünden de faydalanan bir araç geliştirmeye ve kullanan kişinin ihtiyacına, tercihine 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.

The screenshot shows a code editor with two tabs: 'lang_id.py' and 'logs.txt'. The 'logs.txt' tab is active, displaying a JSON log file with several entries. The entries are chat messages from 'driver@q3mcco35auwcstmt.onion' to 'hofeq3mcco35auwcstmt.onion' and 'defender@q3mcco35auwcstmt.onion'. The messages are encrypted, and the log file contains error messages indicating that the messages cannot be decrypted. The 'lang_id.py' tab is also visible, showing a script that identifies the language of the text. The script is titled 'Conti - Python lang_id.py logs.txt TR High - 115x31'. The script output shows the language identification results for the text 'Selam merhaba nasilsin ? (test için eklenmiştir)'. The results are: Language Code:TR, Confidence Level:High, Text:Sosyal medyayı oldukça etkin kullanan bir güvenlik araştırmacısı olarak bu zamana dek sosyal ağlar, e-postalar üzerinden aldığım mesajları güvenlik araştırmalarına ve ardından blog yazıları, sunumlara çevirdiğimi biliyorsunuzdur. Çıkış noktası diğerleri ile aynı olan bu hikayede ise müşteri güvenliğini sağlamak amacıyla sosyal ağ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz. (test için eklenmiştir).

```
1 ./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20210823.json
2 {
3   "ts": "2021-08-23T06:17:46.326321",
4   "from": "driver@q3mcco35auwcstmt.onion",
5   "to": "hofeq3mcco35auwcstmt.onion",
6   "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
7 }
8 {
9   "ts": "2021-08-23T06:21:29.401324",
10  "from": "driver@q3mcco35auwcstmt.onion",
11  "to": "defender@q3mcco35auwcstmt.onion",
12  "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
13 }
14 {
15  "ts": "2021-08-23T06:43:20.480030",
16  "from": "driver@q3mcco35auwcstmt.onion",
17  "to": "hofeq3mcco35auwcstmt.onion",
18  "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
19 }
20 Selam merhaba nasilsin ? (test için eklenmiştir)
21 Sosyal medyayı oldukça etkin kullanan bir güvenlik araştırmacısı olarak bu zamana dek sosyal ağlar, e-postalar üzerinden aldığım mesajları güvenlik araştırmalarına ve ardından blog yazıları, sunumlara çevirdiğimi biliyorsunuzdur. Çıkış noktası diğerleri ile aynı olan bu hikayede ise müşteri güvenliğini sağlamak amacıyla sosyal ağ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz. (test için eklenmiştir)
22 {
23   "ts": "2021-08-23T06:43:46.773096",
24   "from": "hofeq3mcco35auwcstmt.onion",
25   "to": "driver@q3mcco35auwcstmt.onion",
26   "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
27 }
28 {
29   "ts": "2021-08-23T06:44:22.941040",
30   "from": "driver@q3mcco35auwcstmt.onion",
31   "to": "hofeq3mcco35auwcstmt.onion",
32   "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
33 }
34 {
35   "ts": "2021-08-23T06:45:20.386289",
36   "from": "hofeq3mcco35auwcstmt.onion",
37   "to": "driver@q3mcco35auwcstmt.onion",
38   "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
39 }
40 {
41   "ts": "2021-08-23T08:00:32.458165",
42   "from": "bentley@q3mcco35auwcstmt.onion",
43   "to": "many@q3mcco35auwcstmt.onion",
44   "body": "Привет, бро. Криптанем длл?"
```

```
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:Sosyal medyayı oldukça etkin kullanan bir güvenlik araştırmacısı olarak bu zamana dek sosyal ağlar, e-postalar üzerinden aldığım mesajları güvenlik araştırmalarına ve ardından blog yazıları, sunumlara çevirdiğimi biliyorsunuzdur. Çıkış noktası diğerleri ile aynı olan bu hikayede ise müşteri güvenliğini sağlamak amacıyla sosyal ağ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz. (test için eklenmiştir)
```

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.