

Practical Data Leakage Analysis

written by Mert SARICA | 1 June 2023

Conti, a Russian-backed cybercrime group that earned \$180 million in revenue from ransomware attacks in 2021, reached a major turning point in 2022 with Russia's invasion of Ukraine. The group publicly supported the Russian invasion, resulting in a rift among its international members. One member began leaking internal messages from 2020-2021 on a Twitter account (@ContiLeaks), including the source code for the ransomware they used in their cyberattacks. The group was considered one of the most notorious cybercrime groups in the world.

The screenshot shows a Twitter profile for 'conti leaks' (@ContiLeaks). The profile bio includes the text 'fuck ru gov' and 'Şubat 2022 tarihinde katıldı'. The profile has 1 follower and 6,698 followers. The tweets shown are:

- Tweet 1: 'Ukraine will Rise! fresh jabber logs anonfiles.com/zflc33Lbxf/jab...' (2 Mar, 18 replies, 58 retweets, 173 likes)
- Tweet 2: 'anonfiles.com/l3b7n7L6xc/con... - conti source without locker src.' (1 Mar, 15 replies, 80 retweets, 222 likes)

The screenshot shows a Twitter interface with a dark theme. On the left is a navigation sidebar with icons for Home, Discover, Notifications, Messages, Bookmarks, Lists, Profile, and More. At the bottom of the sidebar is a 'Tweetle' button and a user profile for 'Mert SARICA'. The main content area shows a thread from 'conti leaks' (@ContiLeaks) with 28 tweets. The first tweet, dated 1 Mar, contains a list of seven links to anonfiles.com. The second tweet, also dated 1 Mar, contains one link. The third tweet, dated 1 Mar, contains one link. The fourth tweet, dated 27 Şub, contains one link. Each tweet shows engagement metrics like replies, retweets, and likes.

As a cybersecurity researcher, when data from such threat actors is leaked, one of the things that interests me the most is whether the data includes information about hacked organizations in Turkey, as well as non-Russian, English messages. If you ask me why, it's because I can have the opportunity to learn how extensively Turkey is targeted by these threat actors and which nationalities are involved in such internationally organized crime groups. To find out, I decided to conduct cybersecurity research to provide insights to cybersecurity researchers who are also interested in this topic.

First, I downloaded the files that include the Conti group's messages from the sharing area of the vx-underground website. When I extracted all the zip files, more than 11,000 files came out.

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 %

```

After learning that the messages are stored as readable text in JSON files (Example: 185.25.51.173-20220301.json), my first task was to use the following regex-supported GREP command to find and deduplicate all IP addresses in the files. I ended up with a total of 3819 IP addresses that match these two regex patterns, which I saved in a file named "ip.txt."

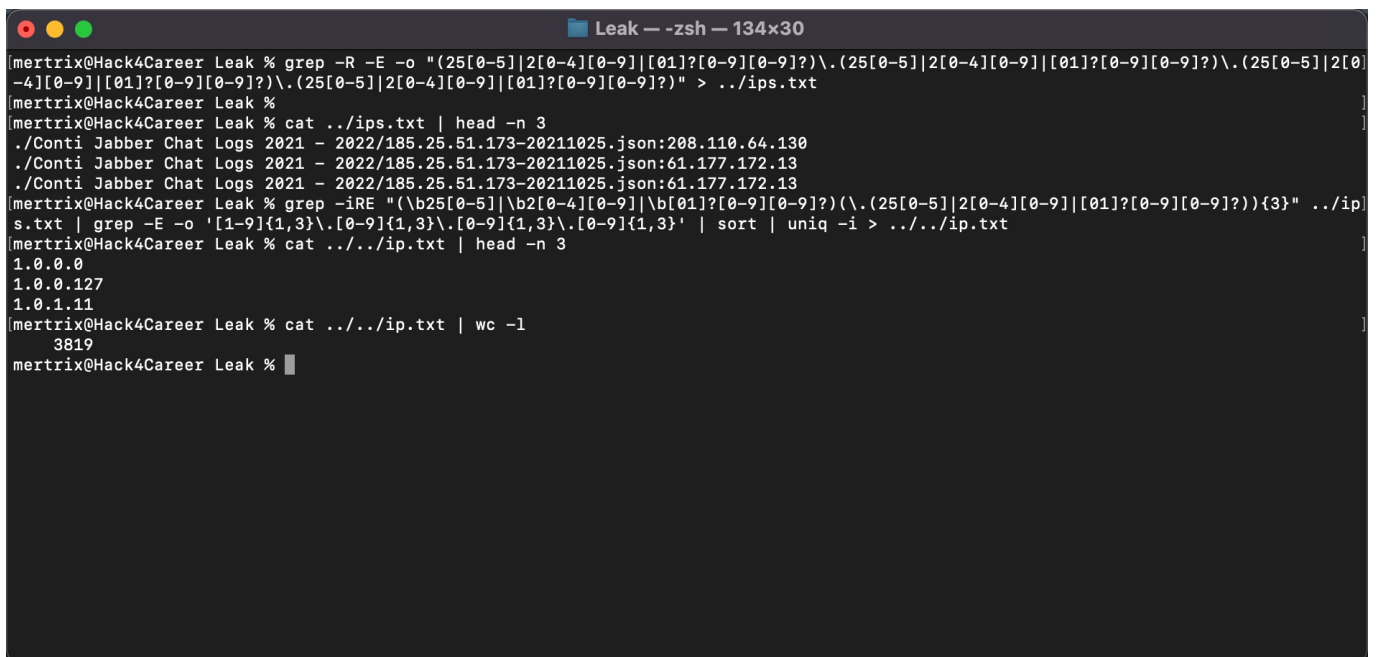
```
grep -R -E -o
```

```
"(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]?)" ..../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]?)" ..../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 % 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 %
```

When it came to finding out which of these IP addresses belong to Turkey, I found help in the IPinfo API and its Python library. By using this library with the IP2Geo Tool v2 that I developed, I queried all the IP addresses in my possession (ip.txt), and I learned that two of these IP addresses (31.210.111.142, 5.188.168.19) are located in Turkey.

```
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

3.92.208.96:US:Union City
3.92.208.97:US:Union City
3.92.208.98:US:Union City
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
4.1
4.1
4.1
4.5
4.0.
4.0.
4.0.
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 % █

Conti — -zsh — 87x40
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
3.9
4.1
4.1
4.1
4.5
4.0.
4.0.
4.0.
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@q3mcco35awcstmt.onion",
"to": "target@q3mcco35awcstmt.onion",
"body": "с женой детьми, животными встречусь"
}
{
"ts": "2020-06-25T18:48:12.975279",
"from": "kagas@q3mcco35awcstmt.onion",
"to": "defender@q3mcco35awcstmt.onion",
"body": "\nroot 5.188.168.190 30t36SBP2z0w |Turkey\n\n186.216.125.178 system OkwKcEcsqJP2Z\n\n1$
}
}
{
"ts": "2020-06-25T18:48:31.813975",
"from": "kagas@q3mcco35awcstmt.onion",
"to": "green@q3mcco35awcstmt.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@q3mcco35awcstmt.onion",
"to": "netwalker@q3mcco35awcstmt.onion",
"body": "10437177 \tBZQEKOXFVINZLSH_W629200.F43FE097769B17A28BBAE29198866EDD \ttnet16 \t2021-05-1$
}
}
{
"ts": "2021-05-13T16:40:55.167472",
"from": "bentley@q3mcco35awcstmt.onion",
"to": "netwalker@q3mcco35awcstmt.onion",
"body": "indows 7 x64 SP1 \t31.210.111.142_\tTR \t22\n10439894 \tDESKTOP-D0196DM_W10018363.B770FB5F7E69D33$
}
}
{
"ts": "2021-05-13T16:41:11.997127",
"from": "netwalker@q3mcco35awcstmt.onion",
"to": "bentley@q3mcco35awcstmt.onion",
"body": "я встаете вижу да"
}
}
{
"ts": "2021-05-13T16:41:18.755743",
}
}
^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
```

To validate the results I obtained, I took a look at SOCRadar, Extended Cyber Threat Intelligence Platform that provides real-time notifications to organizations regarding data breaches. I found that the results aligned with what I discovered earlier, thus clarifying my initial curiosity. :)

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.

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 30t365BP2z0W | Turkey \ n \ n186.216.125.178 system 0kwKcECs8qJP2Z \ n177.190.69.162
admin @l0ctyQh243063uD \ n45.235.6.161 system 0kwKcECs8qJP2Z \ n191.241.180.55 admin @l0ctyQh24306
3uD \ n170.84.78.86 system 0kwKcECs8qJP2Z \ n170.247.15.165 system 0kwKcECs8qJP2Z \ ...
```

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 30t365BP2z0W | Turkey \ n \ n186.216.125.178 system 0kwKcECs8qJP2Z \ n177.190.69.162
admin @l0ctyQh243063uD \ n45.235.6.161 system 0kwKcECs8qJP2Z \ n191.241.180.55 admin @l0ctyQh24306
3uD \ n170.84.78.86 system 0kwKcECs8qJP2Z \ n170.247.15.165 system 0kwKcECs8qJP2Z \ ...
```

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.ipvoid.com>

When it came to my curiosity about the other topic, I decided to explore Python libraries capable of language detection from text. After a brief research, I came across several prominent libraries in this field, including fastText, langdetect and langid

While testing the libraries individually on the text from the leaked Conti data, I observed that each library made accurate language detections for some texts but produced incorrect results for others. As I pondered over which library to use, I decided to develop a tool that combines all three libraries and allows users to specify the confidence level parameter according to their

needs and preferences. This approach would provide a more reliable way to determine the language in a customizable manner.

After merging the leaked Conti data into a single file using the command `find . -type f -print -exec cat {} \; > ../logs.txt`, I used the Language Identification tool I developed to check each line in the “logs.txt” file for Turkish language detection using the three libraries (with the confidence level set to “High”).

To use the Language Identification tool, you need to provide the following parameters.

1. The first parameter is the text file you want to analyze, specifying it line by line.
2. The second parameter is the language code for the language you want to detect (e.g., “TR” for Turkish, “EN” for English).
3. The optional third parameter determines the confidence level. If you set it to “High,” when all three libraries detect the language code you specified, it will indicate it on the screen.

Here’s an example command using the tool:

```
python3 lang_id.py logs.txt TR High
```

This command will analyze each line in the “logs.txt” file for Turkish language detection with a high confidence level.

Since there were no Turkish words or sentences used in the text files, there was no language detection indicating the usage of Turkish language by any of the three libraries. However, to test the tool’s functionality, I added three fake Turkish texts to the “logs.txt” file. As a result, I successfully observed that the program detected them correctly. Through this analysis, I learned from the leaked Conti data that there was no Turkish conversation among the group members, thereby clarifying my final curiosity.

```
lang_id.py logs.txt
./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 medyay\u0131 olduk\u00e7a etkin kullanan bir g\u00fcvenlik ara\u015ft\u0131rmac\u0131s\u0131 olarak bu z
ardından blog yaz\u0131larına, sunumlara \u00e7evirdi\u011fimi biliyorsunuzdur. \u00c7\u0131k\u0131\u015f nokt
\u00fczerinden gelen bir siber tehdit istihbaratından nas\u0131l faydaland\u0131\u011fimi g\u00f6rebil
22 {
23   "ts": "2021-08-23T06:43:46.773096",
24   "from": "hof@q3mcco35auwcstmt.onion",
25   "to": "driver@q3mcco35auwcstmt.onion",
26   "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.]"}
27 }
28 }
29 {"ts": "2021-08-23T06:44:22.941040",
30 "from": "driver@q3mcco35auwcstmt.onion",
31 "to": "hofeq3mcco35auwcstmt.onion",
32 "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.]"}
33 }
34 }
35 {"ts": "2021-08-23T06:45:20.386289",
36 "from": "hof@q3mcco35auwcstmt.onion",
37 "to": "driver@q3mcco35auwcstmt.onion",
38 "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.]"}
39 }
40 }
41 {"ts": "2021-08-23T08:00:32.458165",
42 "from": "bentley@q3mcco35auwcstmt.onion",
43 "to": "many@q3mcco35auwcstmt.onion",
44 "body": "\u041f\u0440\u0438\u0432\u0435\u0442, \u0431\u0440\u043e. \u041a\u0440\u0438\u043f\u0442\u0430\u043d\u0435\u043c \u0434\u043b\u0430?"
}
```

```
Conti - Python lang_id.py logs.txt TR High - 115x31
=====
Language Identification v1.0 [https://www.mertzarica.com]
=====
Language Code:TR Confidence Level:High Text:Selam merhaba nasilsin ? (test i\u00e7in eklenmi\u015ftir)
Language Code:TR Confidence Level:High Text:Sosyal medyay\u0131 olduk\u00e7a etkin kullanan bir g\u00fcvenlik ara\u015ft\u0131rmac\u0131s\u0131 olarak
bu zamana dek sosyal a\u011flar, e-postalar \u00fczerinden ald\u0131\u011f\u0131m mesajlar\u0131 g\u00fcvenlik ara\u015ft\u0131rmalar\u0131na ve ard\u0131ndan blog yaz\u0131l
ar\u0131na, sunumlara \u00e7evirdi\u011fimi biliyorsunuzdur. \u00c7\u0131k\u0131\u015f nokt\u0131s\u0131 de\u011ferleri ile aynı olan bu hikayede ise m\u00fc\u015fteri g\u00fcvenli
\u011fini sa\u011flamak amacıyla sosyal a\u011f \u00fczerinden gelen bir siber tehdit istihbaratından nas\u0131l faydaland\u0131\u011f\u0131m\u0131 g\u00f6rebilirsin
iz. (test i\u00e7in eklenmi\u015ftir)
```

I hope this method I have followed and the two tools I have developed will be beneficial for security researchers and experts in data leakage analysis. Hope to see you in the following articles.