

PRATİK VERİ SIZINTISI ANALİZİ



MERT SARICA

CYBER SECURITY RESEARCHER

1



**FİDYE YAZILIMI
İSTATİSTİKLERİ**

2



**İSTİSMAR
VEKTÖRLERİ**

3



**MÜCADELE
YÖNTEMLERİ**

4



**BAŞ
AKTÖRLER**

5



**VERİ SIZINTISI
ANALİZİ**

İÇERİK



MERT SARICA
CYBER SECURITY RESEARCHER

BEN KİMİM?

-  **Güvenlik Araştırmacısı** **180+ Güvenlik Araştırması**
-  **Blog Yazarı** **www.mertsarica.com**
-  **Beyaz Yakalı** **Genel Müdür Yardımcısı / CISO @Intertech**
-  **Sertifika Koleksiyoncusu** **CCISO, CISSP, SSCP, OSCP,
OPST, CREA, CERA**



BU KİM?





Moises Luis Zagala Gonzales

Doğum Yeri: Venezuela

Yaşı: 55

Mesleği: Kardiyolog

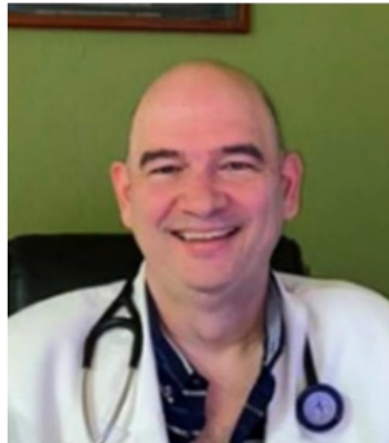
Bildiği Diller: İngilizce, İspanyolca, Fransızca



WANTED BY THE FBI

MOISES LUIS ZAGALA GONZALEZ

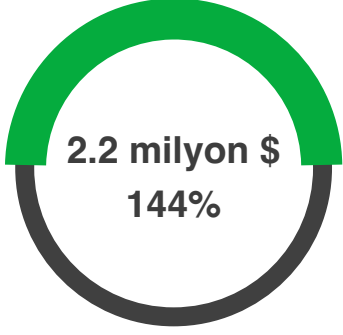
Attempted Computer Intrusions; Conspiracy to Commit Computer Intrusions



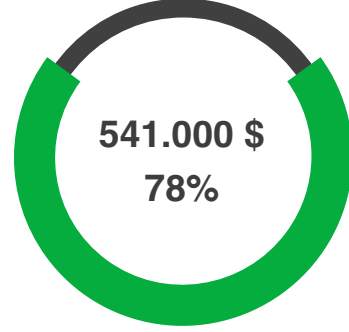
FİDYE YAZILIMI İSTATİSTİKLERİ

2021 yılında;

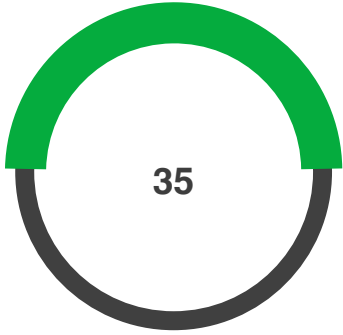
- **2.2 milyon \$ (%144)** ortalama fidye bedeli talep edildi.
- **541.000\$ (%78)** ortalama fidye bedeli ödendi.
- **35** yeni fidye grubu tespit edildi.
- **2566** kurban afişe edildi.



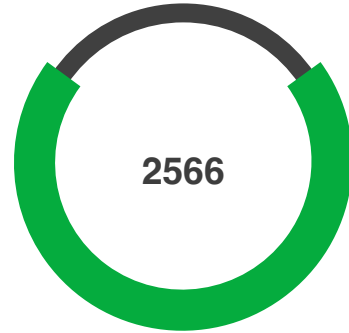
2021



2021



2021



2021

İSTİSMAR VEKTÖRLERİ

9 yıldır aynı tas aynı hamam. (Verizon DBIR)

Baş rolde, Ransomware Deployment Protocol

MERT SARICA
CYBER SECURITY RESEARCHER



İSTİSMAR EDİLEN ZAFİYETLER

Pulse Secure VPN

- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8234
- CVE-2019-11510
- CVE-2019-11510

Citrix

- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-11634
- CVE-2021-22941

Microsoft Exchange

- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Fortinet

- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Sonicwall

- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

F5

- CVE-2021-22986
- CVE-202-5902

QNAP

- CVE-2021-28799
- CVE-2020-36198

Sophos

- CVE-2020-12271

Sharepoint

- CVE-2019-0604

Log4J

- CVE-2021-45046

Microsoft Windows

- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Office

- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444

vCenter

- CVE-2021-2198

Acellion (mostly used by ClOp)

- CVE-2021-2701
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

FileZen

- CVE-2021-20655

Atlassian

- CVE-2021-26084

Zoho Corp

- CVE-2021-40539

Microsoft Azure

- CVE-2021-38647

MÜCADELE YÖNTEMLERİ

Bilgi güvenliği farkındalığı

Şifreleme engelleyen güvenlik çözümleri

Yama yönetimi

Yedekleme

Harici Saldırı Yüzey Yönetimi Platformu
(EASM)



BAŞ AKTÖRLER

MERT SARICA
CYBER SECURITY RESEARCHER

platform.socradar.com/darkweb?tab=ransomware

India 141

Ransomware Group

- Lockbit 2.0 869
- Conti 574
- AlphVM Blackcat 131
- HiveLeaks 127
- Revil 96
- Pysa 93
- Vice Society 80
- Grief 79
- BlackByte 67
- Avaddon 65
- ClOp 58
- LV 57
- Everest 51
- Cuba 48
- Lorenz 44
- Karakurt 42
- Quantum 42
- Midas 40
- BlackMatter 39
- Black Basta 36
- AvosLocker 34
- SpyArea 33
- CoomingProject 33

The New Ransomware Victim of Black Basta: Wenzel Wenzel GmbH

2022-07-06

In the Black Basta ransomware group website monitored by SOCRadar, a new ransomware victim allegedly ...

The New Ransomware Victim of Black Basta: Jakob Becker

2022-07-06

In the Black Basta ransomware group website monitored by SOCRadar, a new ransomware victim allegedly ...

The New Data Breach Victim of Karakurt: Assura Group

2022-07-06

In the Karakurt data breacher group website monitored by SOCRadar, a new data breach victim allegedly ...

The New Ransomware Victim of SpyArea: IDEX

2022-07-06

In the SpyArea ransomware group website monitored by SOCRadar, a new ransomware victim allegedly ann ...

The New Data Breach Victim of Karakurt: V-Soft

Assura Group

19 JUL 2022 / Retail

CONTİ GRUBU

- ✓ 2022 Ocak ayı itibariyle **1000** kurbandan **150 milyon \$** gelir elde ettiler.
- ✓ Amerika Dışışleri Bakanlıđı'ndan kilit üyeleri ihbar edenlere **10 milyon \$** ödöl verileceđi açıkladı.
- ✓ 2022 Mayıs ayı itibariyle operasyonlarını durdurma kararı aldılar.

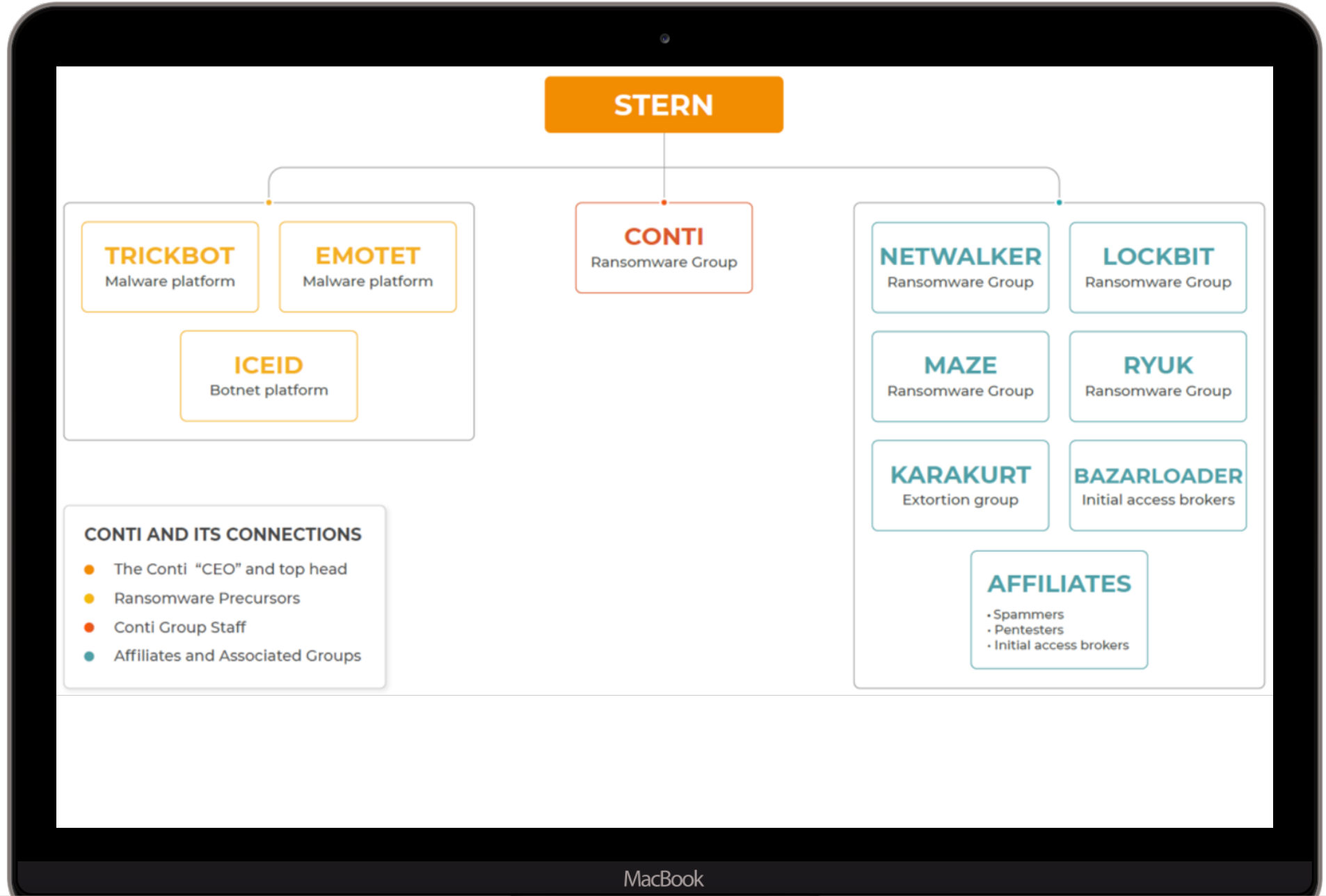


CONTİ VAKASI

- ✓ 2022 Şubat ayında Conti grubu, Rusya'nın Ukrayna işgalini desteklediğini açıkladı.
- ✓ Karşıt görüşlü bir grup üyesi, **@ContiLeaks** Twitter hesabı üzerinden 2020-2021 grup içi yazışmaları paylaşmaya başladı.
- ✓ **60.000**'den fazla yazışmadan çıkan bilgilere göre grubun FSB ile bağlantısı olduğu iddia edildi.



CONTI ORGANİZASYON ŞEMASI





AKLIMDAKİ SORULAR

Türkiye'den hacklenmiş sistemler var mı ?

Üyeler arasında Türkçe konuşan var mı ?



MERTSARICA
CYBER SECURITY RESEARCHER



IP ADRESİ TESPİTİ

11.000 dosya üzerinde çalıştırılan komutlar;

- `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]?)\\b){3}"` `../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`

IP ADRESİNDEN ÜLKE TESPİTİ



API (**IPinfo** - <https://ipinfo.io/>)

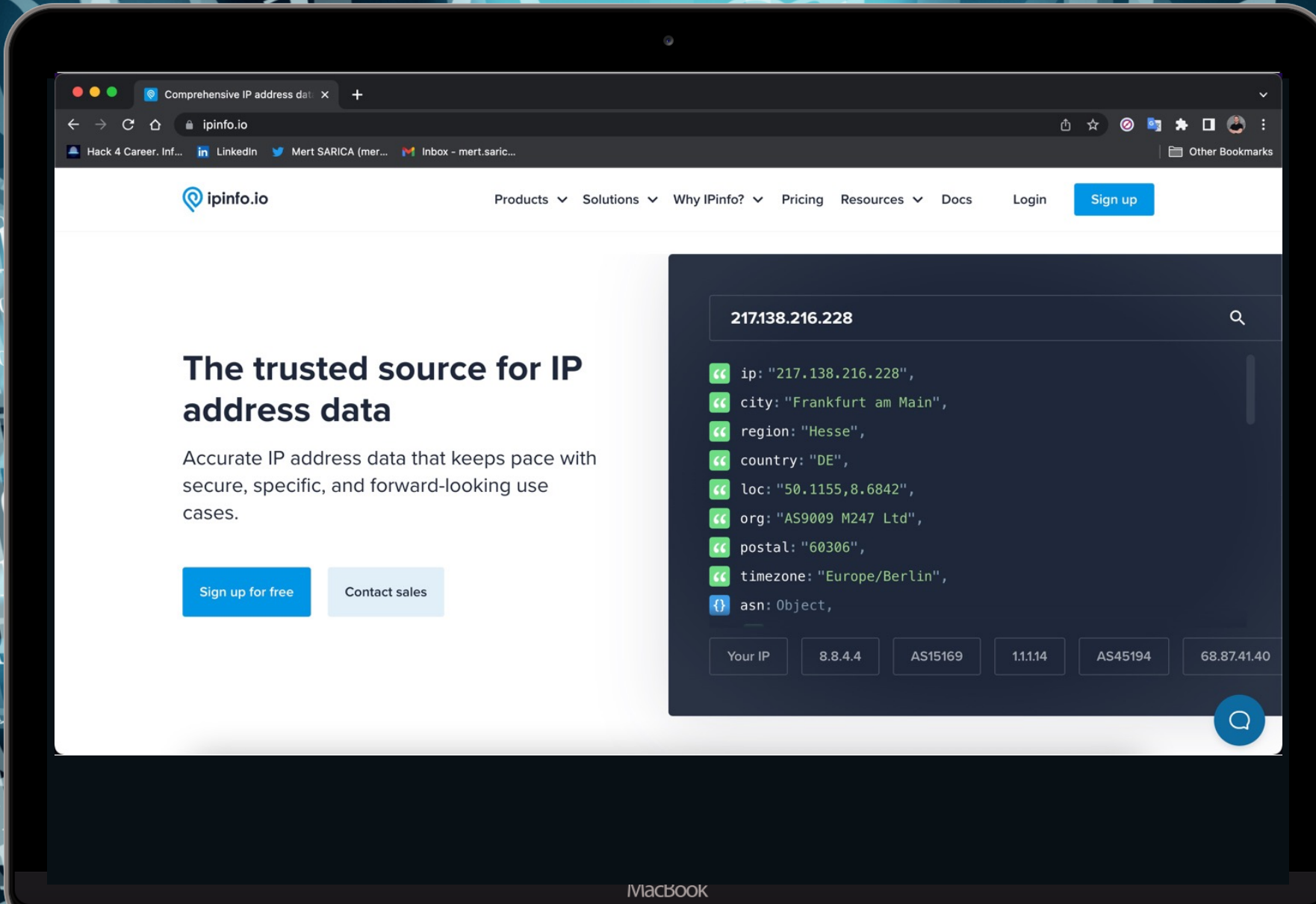


Python kütüphanesi
IPinfo - <https://github.com/ipinfo/python>)



Python aracı
(**IP2Geo Tool v2** - https://github.com/mertsarica/hack4career/blob/master/codes/ip2geo_v2.py)







MERT SARICA
CYBER SECURITY RESEARCHER

TÜRKİYE'DEN HACKLENMİŞ SİSTEMLER

```
=====
IP2Geo Tool v2 [https://www.mertsarica.com]
=====
```

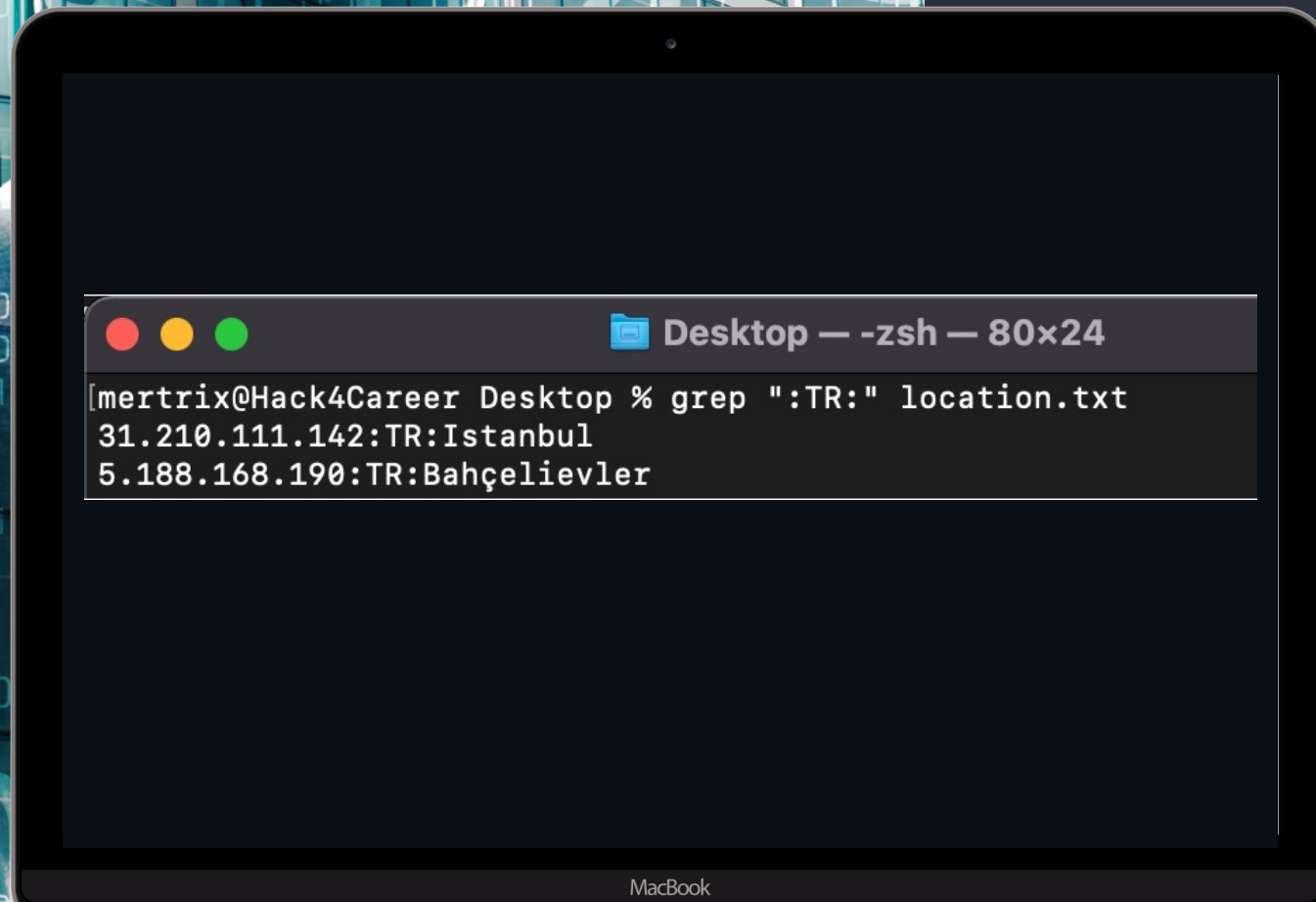
```
1.0.0.0 AU Brisbane
1.0.0.127 AU Brisbane
1.0.1.11 CN Beijing
1.1.0.1 CN Beijing
1.1.1.1 US Los Angeles
1.13.2.28 CN Shenzhen
1.2.0.17 CN Beijing
1.2.1.0 CN Beijing
1.2.3.0 AU Brisbane
1.2.3.255 AU Brisbane
1.2.3.4 AU Brisbane
1.21.2.1 JP Osaka
1.3.0.0 CN Beijing
1.3.135.29 CN Beijing
1.3.35.45 CN 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
```

MacE





MERT SARICA
CYBER SECURITY RESEARCHER



```
3.92.208.96:US:Union City
3.92.208.97:US:Union City
3.92.208.98:US:Union City
```

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 Chat Logs 2020/185.25.51.173-20200626.json:5.188.168.190
mertrix@Hack4Career Conti % grep 31.210.111.142 ips.txt
./Conti Jabber Chat Logs 2021 - 2022/185.25.51.173-20210513.json:31.210.111.142
mertrix@Hack4Career Conti %
```

```
.135.129.250:US:Hilliard
.135.193.147:US:Hilliard
.135.216.86:US:Hilliard
.137.174.178:US:Hilliard
.137.180.197:US:Hilliard
```

```
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": "price@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",
$ \nroot 5.188.168.190 30t36SBP2z0W |Turkey\n\n186.216.125.178 system OkwKcECs8qJP2Z\nn1$
}
{
"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 ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V 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 \tBZQEKOXFVINZLSH_W629200.F43FE097769B17A28BBAE29198866EDD \tnet16 \t2021-05-1$
}
{
"ts": "2021-05-13T16:40:55.167472",
"from": "bentley@q3mcco35auwcstmt.onion",
"to": "netwalker@q3mcco35auwcstmt.onion",
$ indows 7 x64 SP1 \t31.210.111.142 \tTR \t22\n10439894 \tDESKTOP-D019GDM_W10018363.B770FB5F7E69D33$
}
{
"ts": "2021-05-13T16:41:11.997127",
"from": "netwalker@q3mcco35auwcstmt.onion",
"to": "bentley@q3mcco35auwcstmt.onion",
"body": "я встате вижу да"
}
}
{
"ts": "2021-05-13T16:41:18.755743",
}
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

- Digital Risk Protection RiskPrime
- Cyber Threat Intelligence ThreatFusion
- ThreatHose
- ThreatShare
- Vulnerability Intelligence
- Threat Feed / IOC
- Phishing Radar
- Threat Actors
- Combolist
- Malware Analysis
- Threat Reports
- Breach Datasets
- Incidents
- Reports
- Settings
- Stats & Status

85.237.217.157

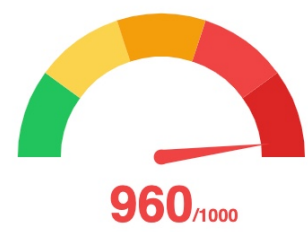
- Stealer Logs
- Public Repos
- Public Buckets
- Reputation Data

IP INTEL CARD

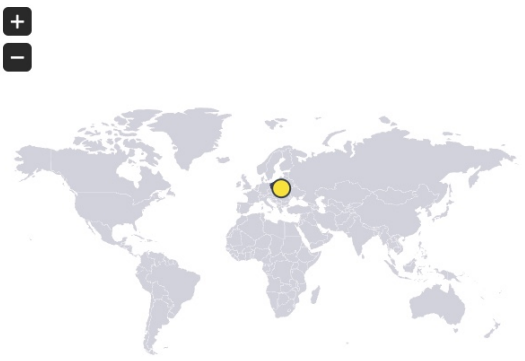
85.237.217.157

High Risk

[Go to All Events](#)



Risk Score	960/1000
IP Address	85.237.217.157
Network	85.237.217.0/24
Country/City	Poland/Lublin
Penalty Reasons	! Github (96%)



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.

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...

https://share.vx-underground.org/Conti/conti-leaks-en-translated

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...

https://share.vx-underground.org/Conti/conti-leaks-en-translated

Tag: #Accommodation & food services #Android #Backdoor #Bitcoin addresses See More

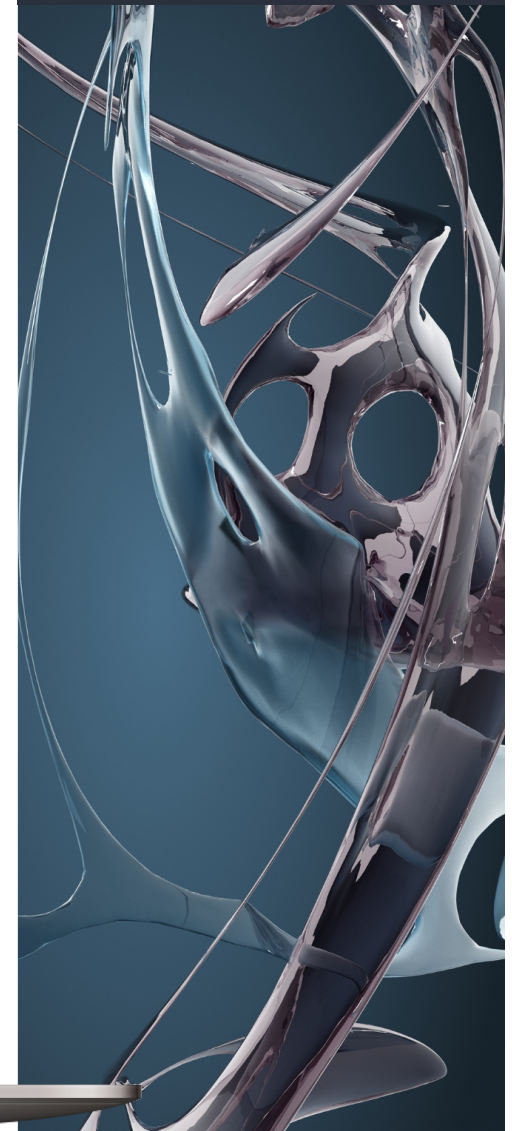


13 Mar 2022

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)



DİL TESPİTİ

- ✓ 3 adet dil tespiti yapan Python kütüphanesi

fastText - <https://fasttext.cc/>

langdetect - <https://github.com/Mimino666/langdetect>

langid - <https://github.com/saffsd/langid.py>

- ✓ Python aracı

Language Identification - https://github.com/mertsarica/hack4career/blob/master/codes/lang_id.py



ÜYELER ARASI TÜRKÇE KONUŞAN VAR MI?

```
logs.txt
UNREGISTERED

lang_id.py logs.txt
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": "hof@q3mcco35auwcstmt.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": "hof@q3mcco35auwcstmt.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 arařtırmacısı olarak bu z
ardından blog yazılarına, sunumlara çevirdiđimi biliyorsunuzdur. Çıkıř nokta
üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandıđımı görebil
22 {
23   "ts": "2021-08-23T06:43:46.773096",
24   "from": "hof@q3mcco35auwcstmt.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": "hof@q3mcco35auwcstmt.onion",
32   "body": "[Ошибка: сообщение зашифровано, и невозможно его расшифровать.]"
33 }
34 {
35   "ts": "2021-08-23T06:45:20.386289",
36   "from": "hof@q3mcco35auwcstmt.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": "manu@q3mcco35auwcstmt.onion",
44   "body": "Привет, бро. Криптанем длл?"
45 }

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 için eklenmiştir)

Language Code:TR Confidence Level:High Text:Sosyal medyayı oldukça etkin kullanan bir güvenlik arařtırmacısı olarak
bu zamana dek sosyal ađlar, e-postalar üzerinden aldıđım mesajları güvenlik arařtırmalarına ve ardından blog yazıl
arına, sunumlara çevirdiđimi biliyorsunuzdur. Çıkıř noktası diđerleri ile aynı olan bu hikayede ise müřteri güvenli
đini sađlamak amacıyla sosyal ađ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandıđımı görebilirsin
iz. (test için eklenmiştir)
```



Fidye yazılımları, organize siber suç örgütlerinin göz bebeği olmaya devam ediyor.

Conti veri sızıntısında;

- Türkiye'den hacklenmiş sistemler bulunuyor.
- Türkçe yazışmalar tespit edilmedi.

SOCRadar, Randori, RiskIQ gibi Harici Saldırı Yüzey Yönetimi Platformları (EASM) ile buna benzer bilgilere çok kısa sürede erişmeniz, alarm almanız mümkün!



MERT SARICA
CYBER SECURITY RESEARCHER



mert.sarica@gmail.com



@MertSARICA



MertSARICA



MERT SARICA

CYBER SECURITY RESEARCHER