PRATİK 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, CEREA

BU KİM?

MERT SARICA

CYBER SECURITY RESEARCHER

Moises Luis Zagala Gonzales

Doğum Yeri: Venezuela

Yaşı: 55

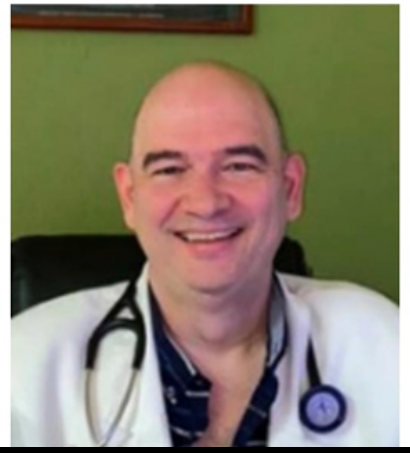
Mesleği: Kardiyolog

Bildiği Diller: İngilizce, İspanyolca, Fransızca

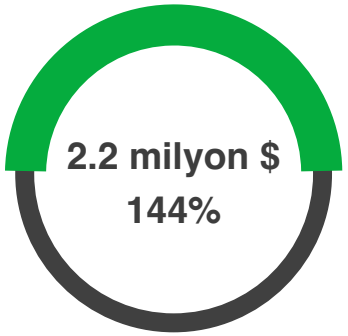
WANTED BY THE FBI

MOISES LUIS ZAGALA GONZALEZ

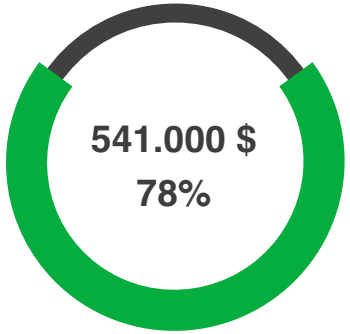
Attempted Computer Intrusions; Conspiracy to Commit Computer Intrusions



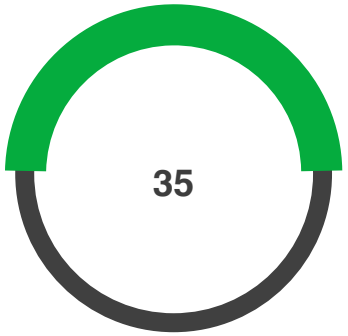
MacBook



2021



2021



2021

2021

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.

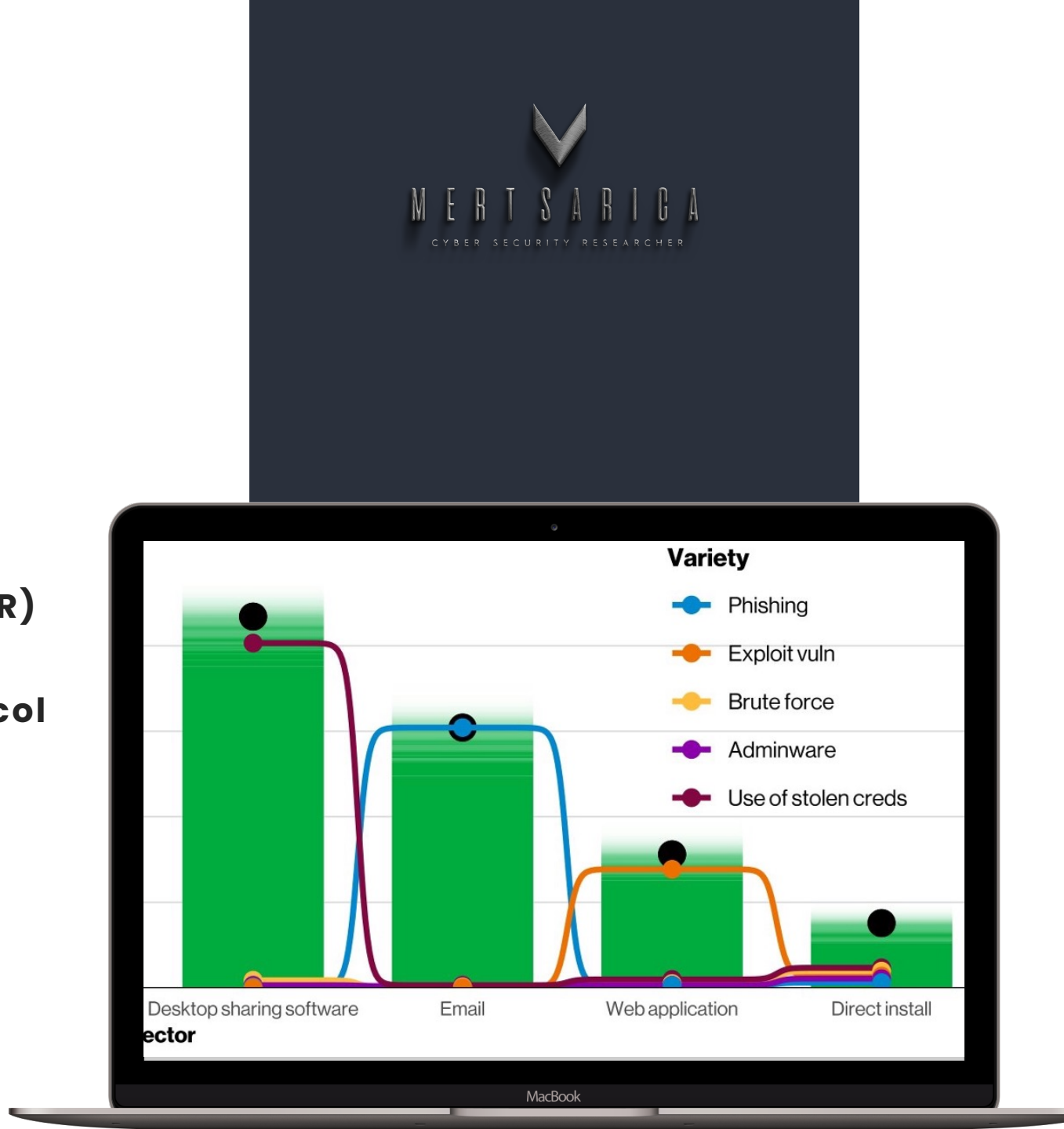
Unit 42 Ransomware Threat Report 2022

MERT SARICA
CYBER SECURITY RESEARCHER

İSTİSMAR VEKTÖRLERİ

9 yıldır aynı tas aynı hamam. (Verizon DBIR)

Baş rolde, Ransomware Deployment Protocol



İSTİSMAR EDİLEN ZAFİYETLER

MÜCADELE YÖNTEMLERİ

Bilgi güvenliği farkındalığı

Şifreleme engelleyen güvenlik çözümleri

Yama yönetimi

Yedekleme

Harici Saldırı Yüzey Yönetimi Platformu (EASM)


MERT SARICA
CYBER SECURITY RESEARCHER
BAŞ
AKTÖRLER
platform.socradar.com/darkweb?tab=ransomware
India 141
See More
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
Cl0p 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
The New Ransomware Victim of Black Basta: Jakob Becker
2022-07-06
The New Data Breach Victim of Karakurt: Assura Group
2022-07-06
The New Ransomware Victim of SpyArea: IDEX
2022-07-06
The New Data Breach Victim of Karakurt: V-Soft
The New Data Breach Victim of Karakurt: Assura Group
2022-07-06
United Kingdom
Real Estate, Rental and Leasing
Karakurt
Assuraplc.com
Assura Group
FILES
0 Bytes / 0 Bytes
Assura Group
19 JUL 2022 / Retail
MacBook

CONTİ GRUBU

- 2022 Ocak ayı itibariyle **1000** kurbandan **150 milyon $** gelir elde ettiler.
- Amerika Dışişleri Bakanlığı'ndan kilit üyeleri ihbar edenlere **10 milyon $** ödül verileceği açıklandı.
- 2022 Mayıs ayı itibariyle operasyonlarını durdurma kararı aldılar.

MERT SARICA
CYBER SECURITY RESEARCHER

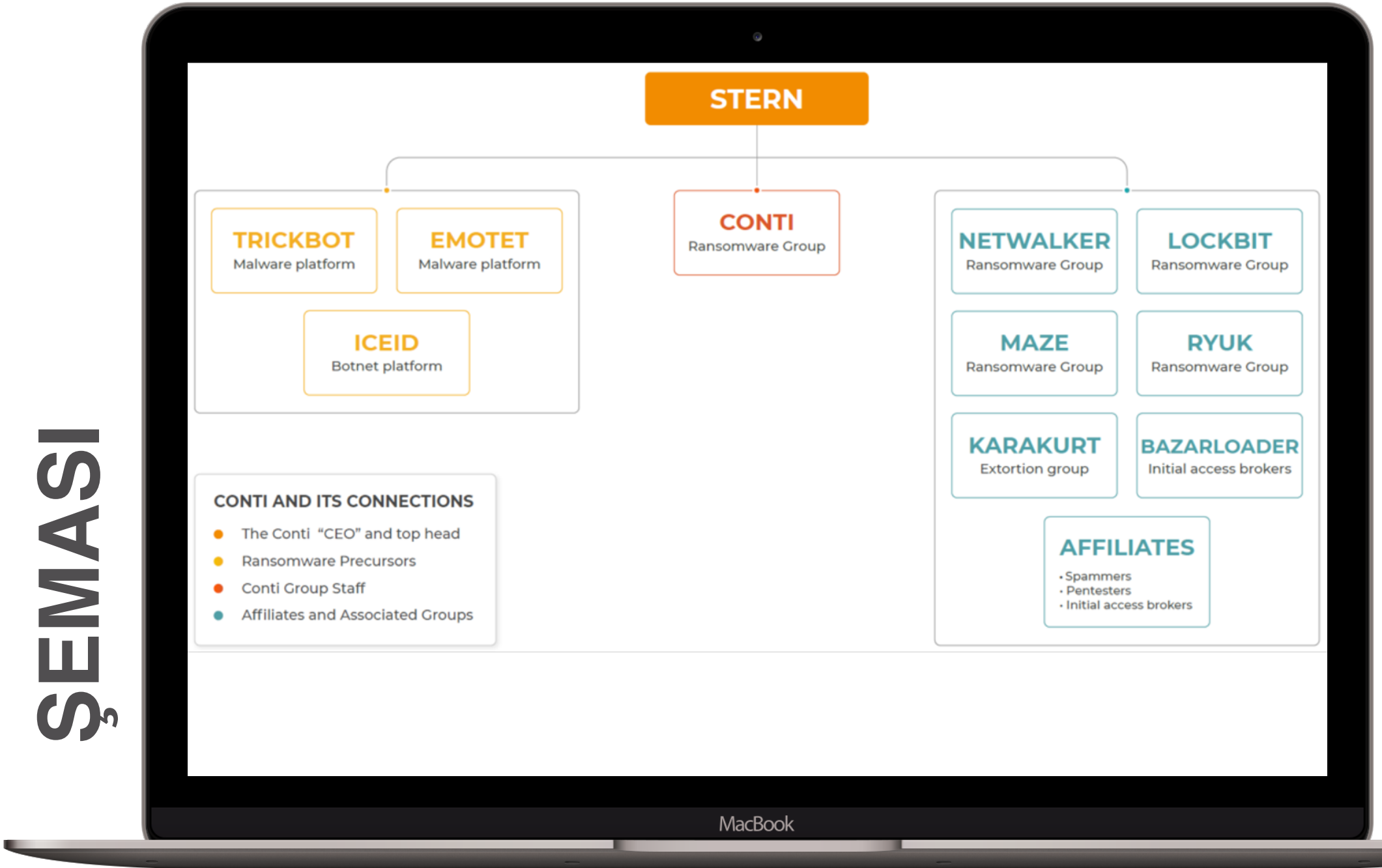
MERT SARICA

CYBER SECURITY RESEARCHER

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.

CONTİ ORGANİZASYON ŞEMASI



AKLIMDAKİ SORULAR

Türkiye’den hacklenmiş sistemler var mı ?

Üyeler arasında Türkçe konuşan var mı ?

MERT SARICA

CYBER SECURITY RESEARCHER

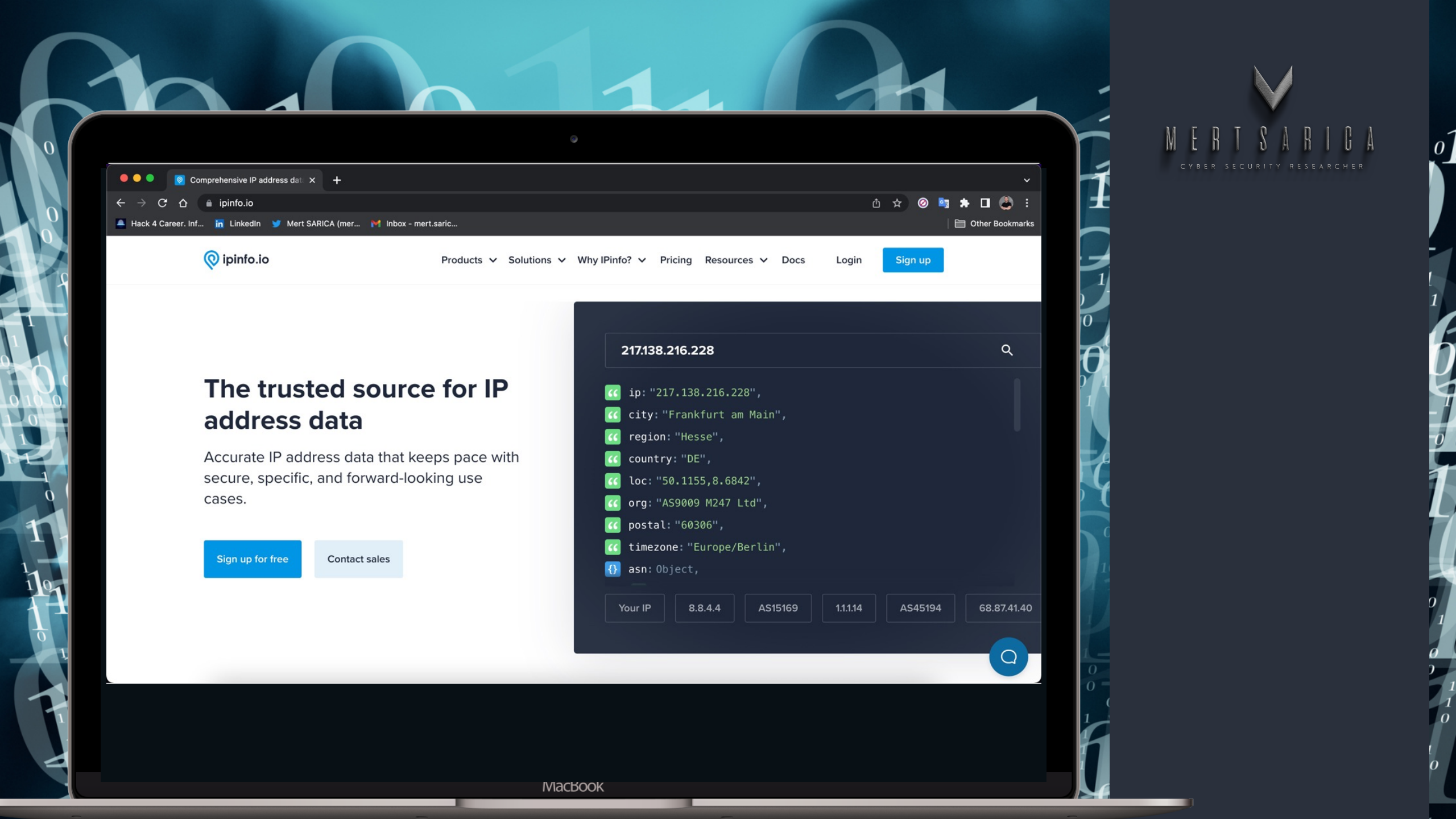

MERT SARICA
CYBER SECURITY RESEARCHER
IP ADRESİ TESPİTİ
11.000 dosya üzerinde çalıştırılan komutlar;
• grep -R -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" > ../ips.txt
• grep -iRE "(\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]?)){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
MacBook

IP ADRESİNDEN ÜLKE TESPİTİ

API (**IPinfo – https://ipinfo.io/**)

Python kütüphanesi
IPinfo – https://github.com/ipinfo/python)

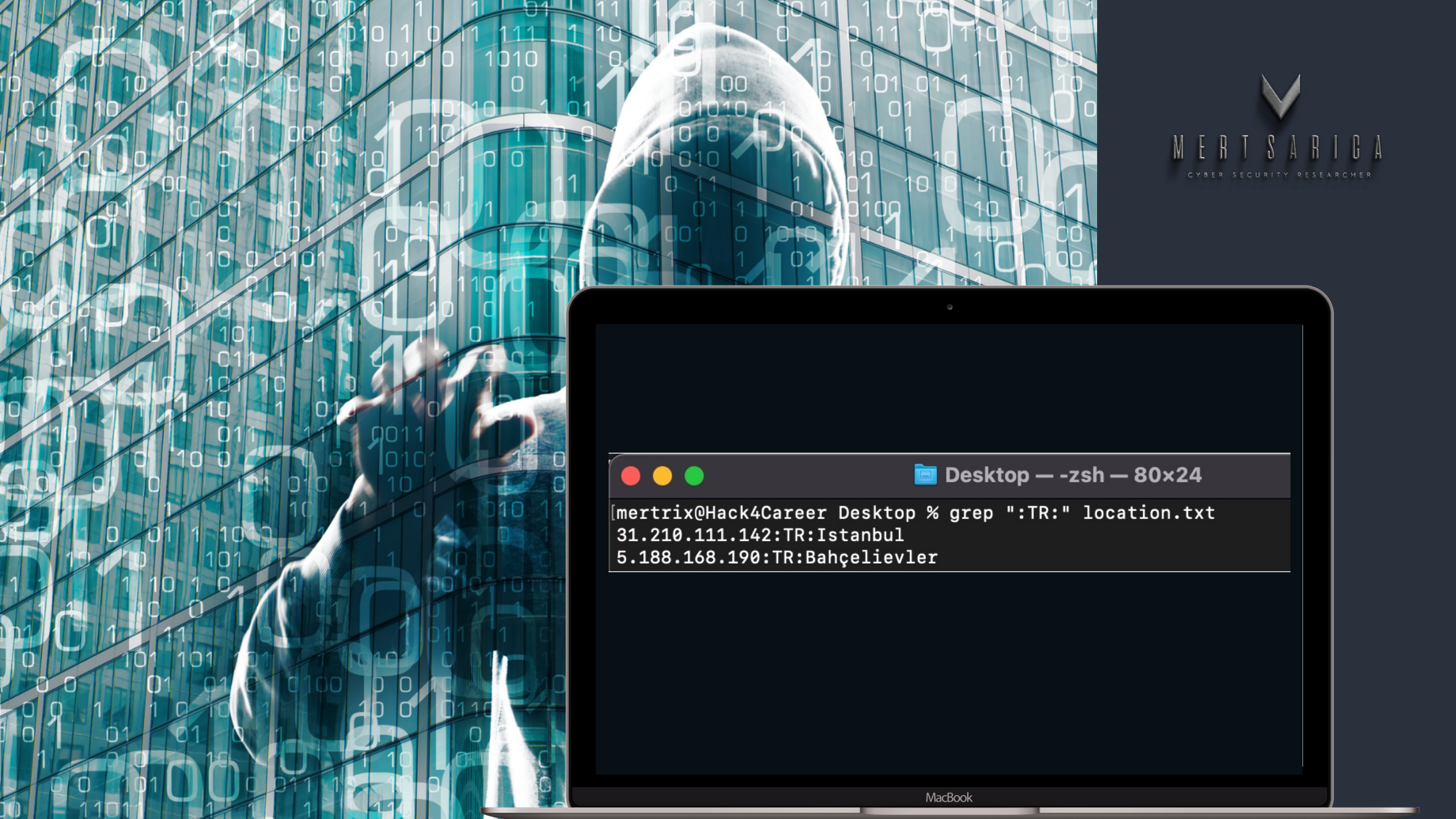
Python aracı
(**IP2Geo Tool v2 – https://github.com/mertsarica/hack4career/blob/master/codes/ip2geo_v2.py**)


MERT SARICA
CYBER SECURITY RESEARCHER
Comprehensive IP address dat
ipinfo.io
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks
ipinfo.io
Products
Solutions
Why IPinfo?
Pricing
Resources
Docs
Login
Sign up
The trusted source for IP address data
Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.
Sign up for free
Contact sales
217.138.216.228
ip: "217.138.216.228",
city: "Frankfurt am Main",
region: "Hesse",
country: "DE",
loc: "50.1155,8.6842",
org: "AS9009 M247 Ltd",
postal: "60306",
timezone: "Europe/Berlin",
asn: Object,
Your IP
8.8.4.4
AS15169
1.1.1.14
AS45194
68.87.41.40
MacBook

MERT SARICA

CYBER SECURITY RESEARCHER

TÜRKİYE'DEN HACKLENMİŞ SİSTEMLER


MERT SARICA
CYBER SECURITY RESEARCHER
Desktop — -zsh — 80×24
[mertrix@Hack4Career Desktop % grep ":TR:" location.txt
31.210.111.142:TR:Istanbul
5.188.168.190:TR:Bahçelievler
MacBook

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

Conti — -zsh — 87×40

```
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 %
```

.135.193.147: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 — 96×23

```
 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",
$\nroot 5.188.168.190 30t36SBP2z0W          |Turkey\n\n186.216.125.178 system OkwKcECs8qJP2Z\n1$
}
{
  "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   ^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 — 99×24

```
 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

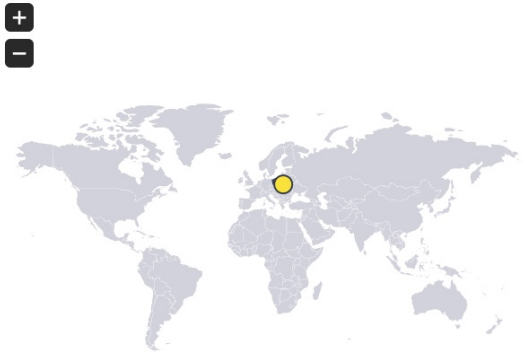
IP INTEL CARD

85.237.217.157

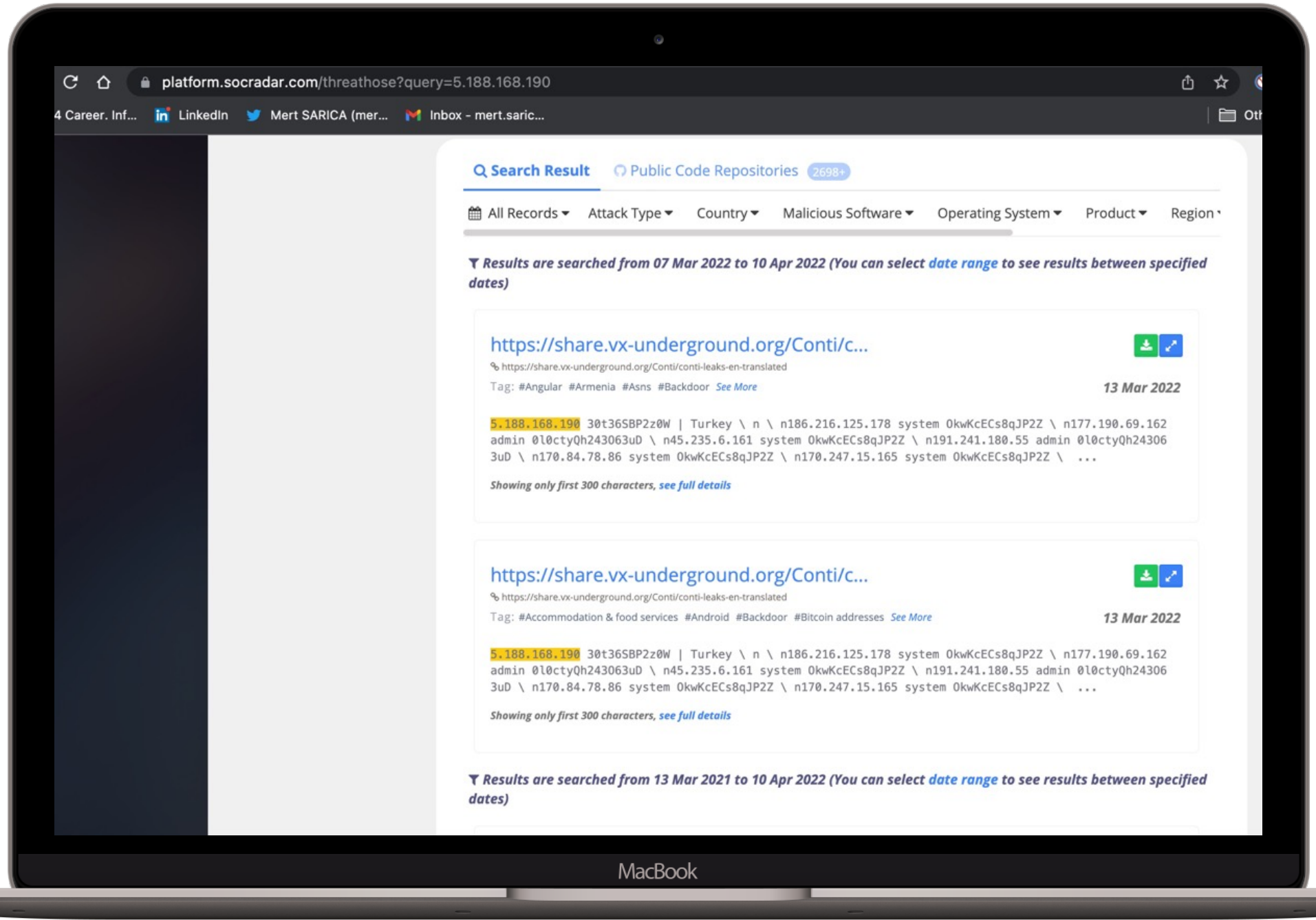
High Risk

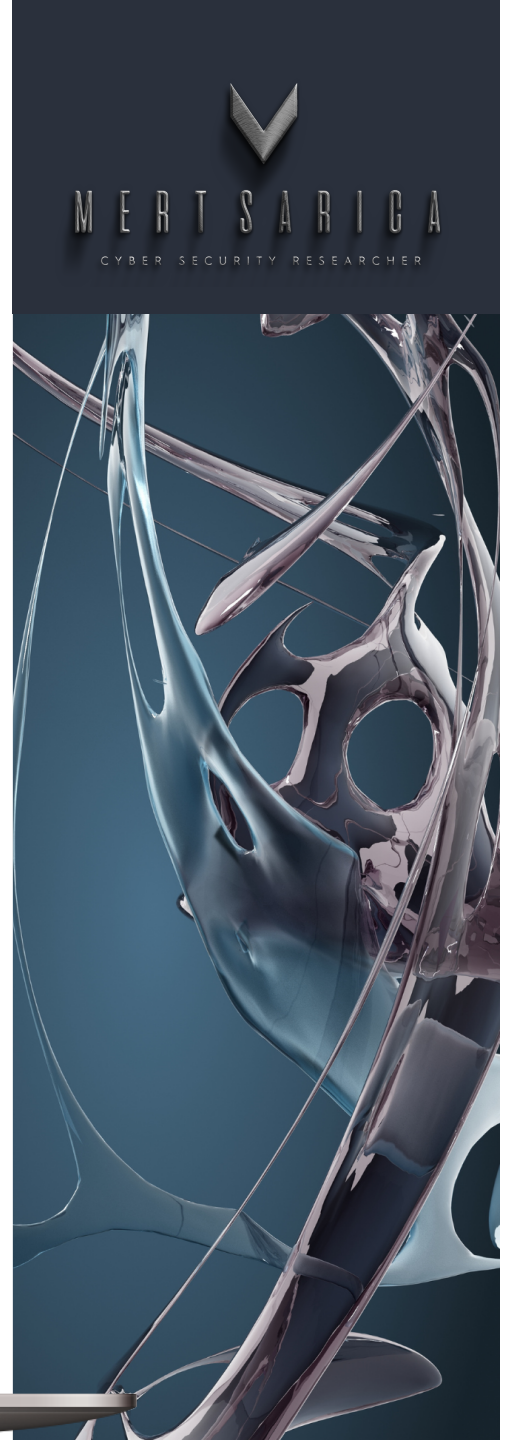
Go to All Events

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.


platform.socradar.com/threathose?query=5.188.168.190
4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
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 0l0ctyQh243O63uD \ n45.235.6.161 system OkwKcECs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh24306 3uD \ 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 0l0ctyQh243O63uD \ n45.235.6.161 system OkwKcECs8qJP2Z \ n191.241.180.55 admin 0l0ctyQh24306 3uD \ 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)
MacBook

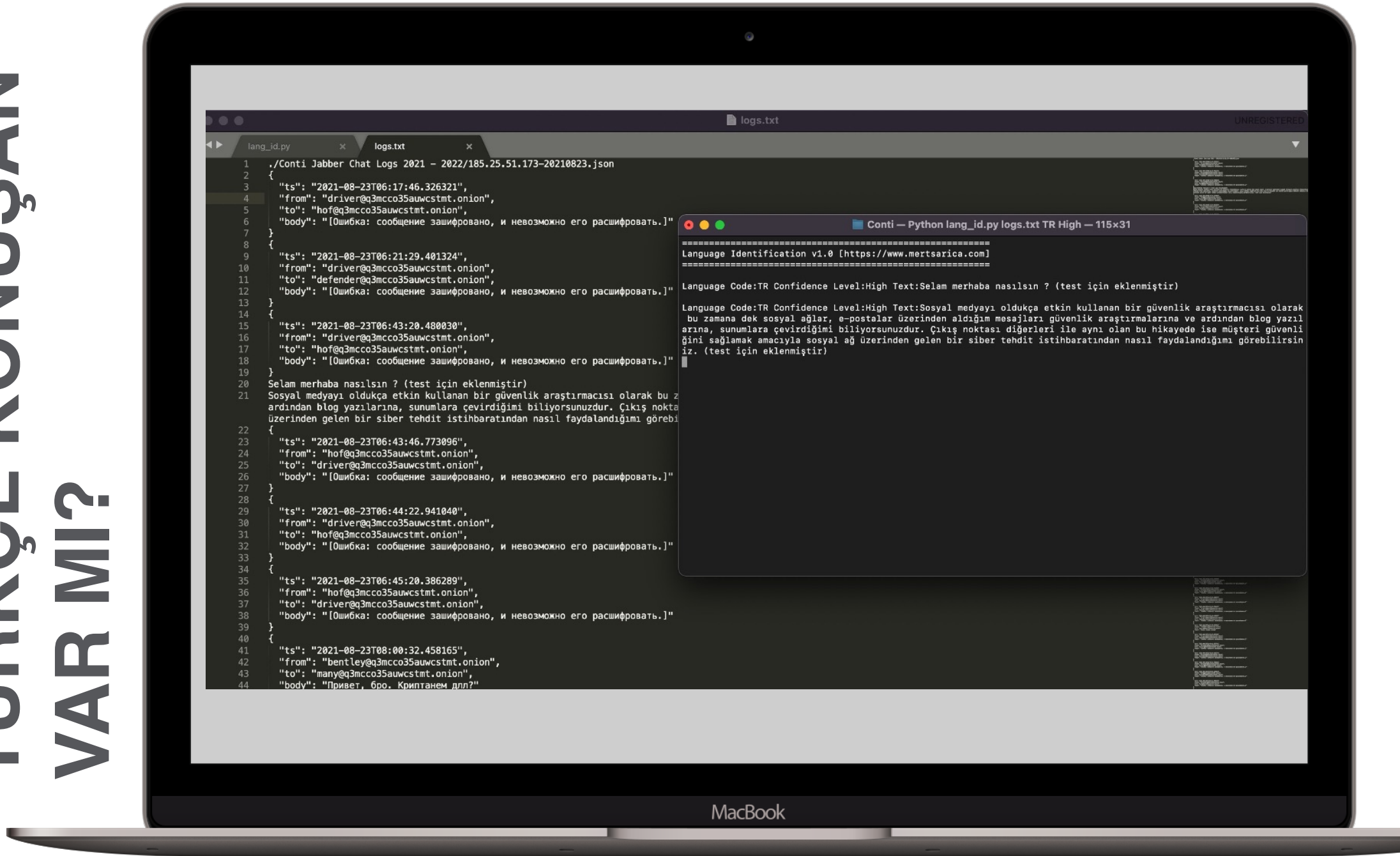

MERT SARICA
CYBER SECURITY RESEARCHER

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?



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