

In OPSEC Fails We Trust

Siber Suçla Mücadelede Yaşanan Zorluklar ve Multidisipliner Yaklaşım

Ben Kimim?

- Robin Dimyanoglu
- Eğitmen – Cyber Struggle
- Case Officer– Arquanum Cyber Security and Intelligence
- Red Teaming, Exploit Geliştirme, Tersine Mühendislik, Zararlı Yazılım Analizi
-  /1ce7ea



Cyber Struggle

- Multidisipliner «Siber Mücadele» Sertifikasyon Programı
- Gayrinizami harp
- Mental mukavemet
- Yoğun stres ortamı
- Belirsizlik doktrini



Arquanum

- Siber mücadele uzmanlarından oluşan bir ekip
- Incident Management
- Intelligence
- Red Teaming
- Profiling
- Anti-Surveillance



Phishing



Phishing

THE 3 TYPES OF PHISHING EMAILS



CLONE PHISHING

CLONE PHISHING IS WHERE A LEGITIMATE, AND PREVIOUSLY DELIVERED, BIT OF ONLINE CORRESPONDENCE IS USED TO CREATE AN ALMOST IDENTICAL OR "CLONE" EMAIL.



SPEAR PHISHING

SPEAR PHISHING IS A PHISHING ATTEMPT DIRECTED AT A PARTICULAR INDIVIDUAL OR COMPANY.



WHALING

WHALING IS A PHISHING ATTEMPT DIRECTED SPECIFICALLY AT A SENIOR EXECUTIVE OR ANOTHER HIGH-PROFILE TARGET WITHIN A BUSINESS.

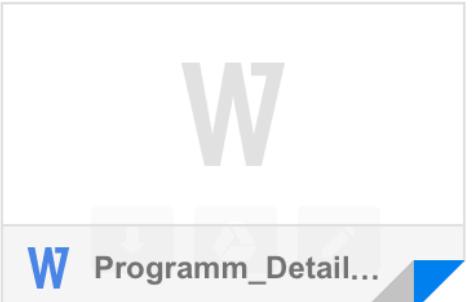
Neden Phishing?

 **Defence iQ CustomerService** DefenceIQ
to [REDACTED] 

We are pleased to offer you to visit our Cyber Threat Intelligence and Incident Response conference in November.

Defence IQ, a division of IQPC
2016 All rights reserved.

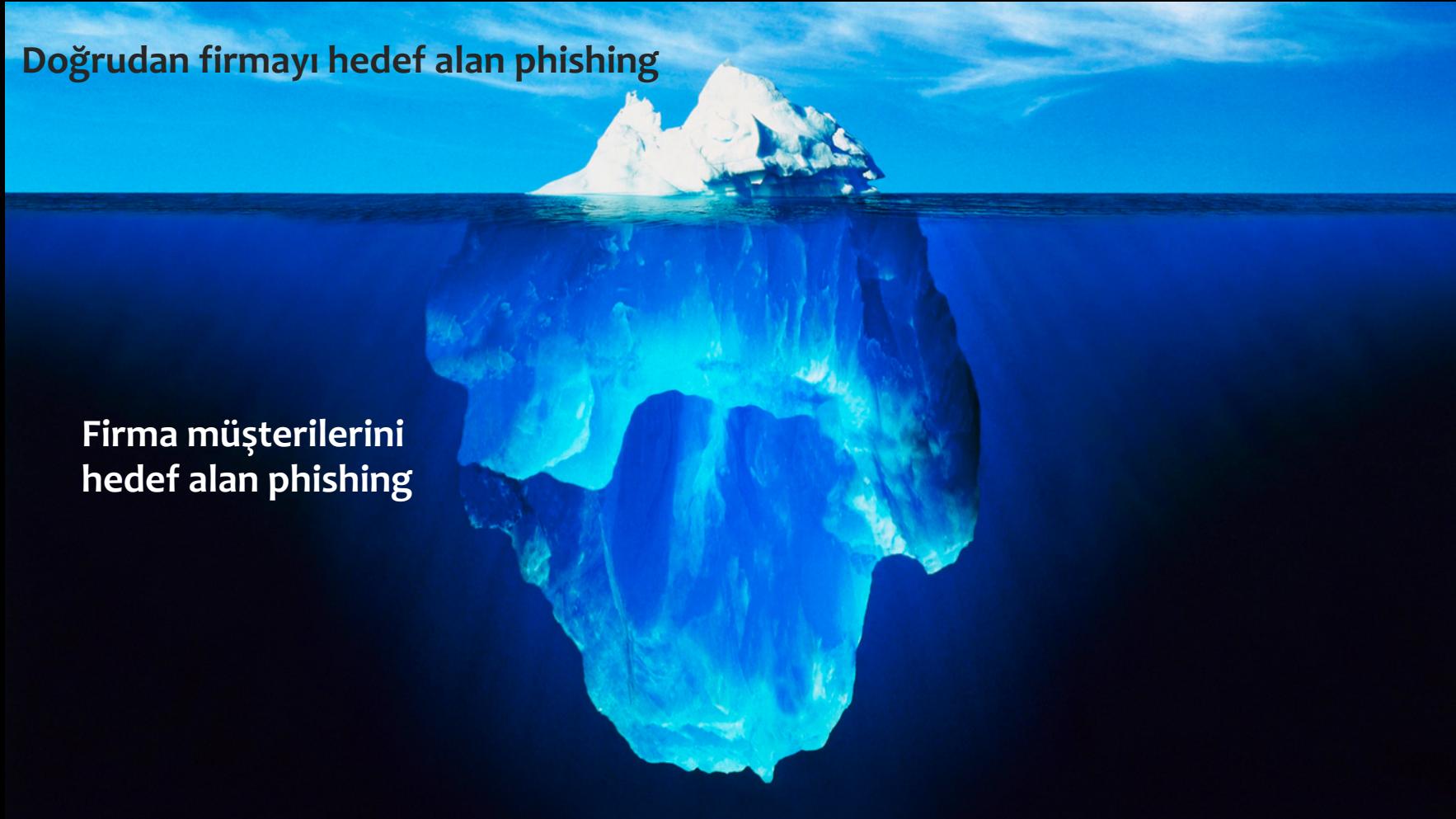
.....




Dışı Seni İçi Beni

Doğrudan firmayı hedef alan phishing

Firma müşterilerini
hedef alan phishing



Dışı Seni İçi Beni

Yargıtay: Internet hesabından çalınan paradan banka sorumlu

16. Hukuk Dairesi 2016/9538 E. , 2016/7014 K.

•

"İçtihat Metni"

MAHKEMESİ :^{TÜRK}
DAVA TÜRK



Bilgisayarına virus göndererek şifresi ele geçirilen vatandaşın hesabından 2 bin lira üçüncü bir kişinin hesabına aktarıldı. Yargıtay, şifre ve parolanın davacının kusuru ile üçüncü kişilerce ele geçirildiğini ispatlayamayan bankanın sorumlu olduğuna hükmetti. Kararla birlikte, vatandaşın internet bankacılığı şifresi kullanılarak bilgiyi ve izni dışında hesabından çekilen 2 bin lirayı banka ödeyecek. ... ve verilen Kredi ... Başkanlık Kurulu'nun ... girmiş olmasına ve Yargıtay ... 251-27501 sayılı kararı ile dosyanın ... kaydedildiği anlaşılmakla dosyanın Yargıtay 19. ... Yargıtay Hukuk İş Bölümü İnceleme Kurulu'na ...larıyla karar verildi.

OSINT #1

- Benzer domainleri üret ve aktiflik durumlarını kontrol et

```
dnstwist 1.02b by <marcin@ulikowski.pl>

usage: ./dnstwist.py [OPTION]... DOMAIN

Find similar-looking domain names that adversaries can use to attack you. Can
detect typosquatters, phishing attacks, fraud and corporate espionage. Useful
as an additional source of targeted threat intelligence.

positional arguments:
  domain            domain name or URL to check

optional arguments:
  -h, --help          show this help message and exit
  -c, --csv           print output in CSV format
  -j, --json          print output in JSON format
  -r, --registered    show only registered domain names
  -w, --whois         perform lookup for WHOIS creation/update time (slow)
  -g, --geoip         perform lookup for GeoIP location
  -b, --banners       determine HTTP and SMTP service banners
  -s, --ssdeep        fetch web pages and compare their fuzzy hashes to
                      evaluate similarity
  -m, --mxcheck       check if MX host can be used to intercept e-mails
  -d FILE, --dictionary FILE
                      generate additional domains using dictionary FILE
  -t NUMBER, --threads NUMBER
                      start specified NUMBER of threads (default: 10)
elceef@osiris:~/dnstwist$
```

OSINT #1

- Benzer domainleri üret ve aktiflik durumlarını kontrol et

The screenshot shows two terminal windows side-by-side, both titled "sh4d0w@undead: ~/EVIL/EvilURL".

Terminal 1 (Left):

```
sh4d0w@undead: ~/EVIL/EvilURL
File Edit View Search Terminal Help
[ UNDEADSEC from BRAZIL ]
-> github.com/UndeadSec
-> youtube.com/c/UndeadSec

How to use:
Insert name: example
Insert level domain: .com

> Insert name: evil
> Insert level domain: .com
[*] Char replaced: e
[*] Using Unicode: Cyrillic Small Letter Ie
[*] Unicode number: e
[*] Evil url: evil.com
-----
[ MORE EXTENSIVE EVIL URL: ]
[*] Char replaced: e,
[*] Using Unicode: Cyrillic Small Letter Ie,
[*] Unicode number: e,
[*] Evil url: evil.com
-----
sh4d0w@undead:~/EVIL/EvilURL$
```

Terminal 2 (Right):

```
sh4d0w@undead: ~/EVIL/EvilURL
File Edit View Search Terminal Help
[ UNDEADSEC from BRAZIL ]
-> github.com/UndeadSec
-> youtube.com/c/UndeadSec

How to use:
Insert name: example
Insert level domain: .com

Select an option:
[1] Generate evil urls
[2] Detect evil urls
>>> 2
[*] CheckURL module loaded.

Operation modes:
[1] Check single URL
[2] Check from a list
>>> 1
> Insert an url: evil.com
* Do you want to check connection? (y/n)
>>> n
[*] Evil URL detected: evil.com
[*] Evil characters used: ['e']
sh4d0w@undead:~/EVIL/EvilURL$
```

OSINT #2

- <https://registrydb.com/live.html>

Registry Database Live search	
This page is auto-refreshed every 10 seconds.	
06:18:53	neatsways.com
06:18:53	watrix.site
06:18:53	deyingp.info
06:18:53	pingapp.org
06:18:52	shkunai.com
06:18:52	emimedicalinsights.com
06:18:52	homebargains247.com
06:18:52	ylybm.com
06:18:52	caintelligence.com
06:18:52	medsamazing.com
06:18:51	womenoffashionandstyle.com
06:18:51	brushballad.win
06:18:51	katiehelliwellpsychicmedium.com
06:18:51	yt2mp4.com

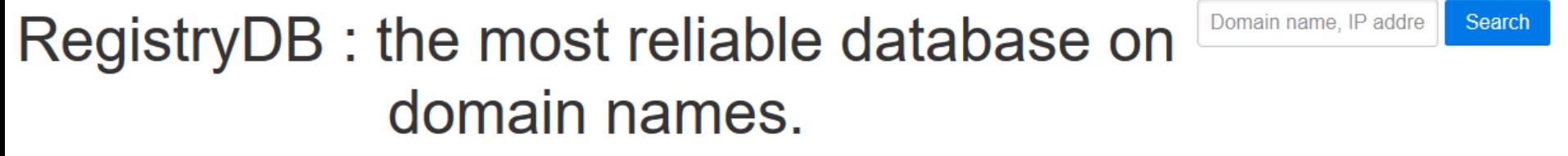
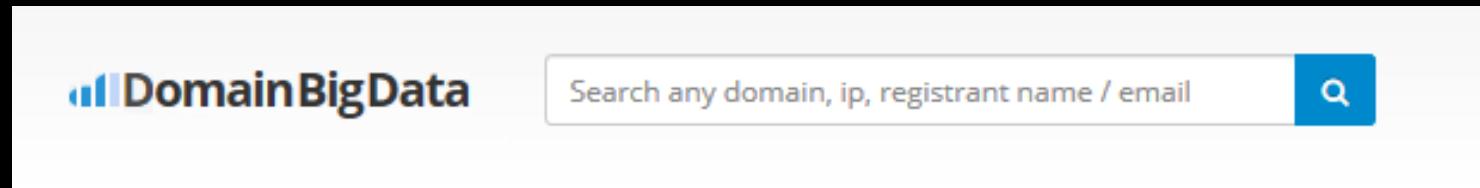
OSINT #3

- CTL Monitoring (certstream)

```
user@debian:~/Work/phishing_catcher$ ./catch_phishing.py
certificate_update: 0cert [00:00, ?cert/s][INFO;root] 2017-11-07 11:46:23,822 - Connection established to CertStrea
m! Listening for events...
certificate_update: 2289cert [00:29, 390.89cert/s]
```

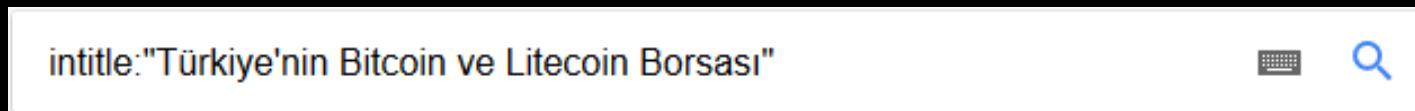
OSINT #4

- Whois arşivleri üzerinden çapraz sorgulama (DEMO)



OSINT #5

- Just Google It ☺



The image shows a search results page with two entries:

- Koinim | Türkiye'nin Bitcoin ve Litecoin Borsası**
<https://koinimx.com/>
7 Ağu 2017 - Bitcoin eşler-arası bir dijital ödeme sistemidir ve birçok özelliğe sahip olması nedeniyle de ilk ve benzersizdir. 2009 yılında ortaya çıktığı andan itibaren önemi ve değeri giderek artmaktadır. Bitcoin'in geleneksel ödeme sistemlerine (banka havalesi, EFT, kredi kartı vs.) göre bir çok avantajı bulunmaktadır ve ...
- Bitcoin – Türkiye'nin Bitcoin ve Litecoin Borsası**
koinim.com/category/bitcoin
Amerika Birleşik Devletleri'nde oluşturulan ve kısa sürede tüm dünyada tanınan Bitcoin, sanal para birimi olarak kullanılıyor. Yaygın bir şekilde kullanımına başlayan Bitcoin, beraberinde pek çok soruya da gündeme getiriyor. 1. Bitcoin Ne İşe Yarar? Online finansal ağ olarak tanımlanabilen Bitcoin, sanal para olmasına ...

OSINT #6

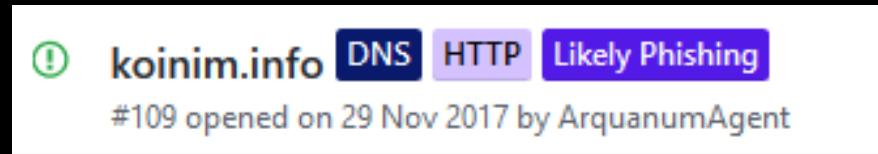
- Censys.io certificate search

The screenshot shows a search results page from Censys.io. The search bar at the top contains the query "koinjm.com". The results are listed in two columns. In the left column, the domain "garantihesabim.com" is highlighted with a red box. In the right column, the domains "koinimy.com" and "koinjm.com" are both highlighted with red boxes.

Results (Left Column)	Results (Right Column)
aileronarts.com	koinimy.com
aaron.net	koinjm.com
astridfinnell0ei5y.ga	komot.online
benmi.store	kxypp.loan
bestroadster.win	lequ.loan
bpbil.loan	louettamanrique1d3qc.cf
brentfordminicabs.co.uk	mdbyy.loan
bthxf.loan	mentem.ru
ccxpn.loan	moldumobel.es
cvttyz.loan	nanetteleaguekhzkeh.tk
dfvfv.loan	newergcnmrf.ga
directbykgxt.ml	ozbooker.ml
etsss.loan	paisa.science
expertsinstress.com	qmltt.loan
ffqsh.loan	
garantihesabim.com	
irocky.com	
it-consultis.net	
klrca.org.my	

Ev Yapımı Phishing Monitoring Sistemi

- OSINT Tekniklerini otomatize et
- + Github entegrasyonu (Phishing domaini bulunca otomatik issue aç)



In OPSEC We Trust

- Whois Privacy
- Cloudflare
- Kış Uykusu
- Bukalemun

Whois Privacy

- Domain sahibinin kimlik bilgilerini gizlemeye yarayan bir hizmet

Whois Privacy

- Domain sahibinin kimlik bilgilerini gizlemeye yarayan bir hizmet
- Whois arşivlerinde gerçek bilgiler kaydedilmiş olabilir!

Cloudflare

- DDoS saldırılarını önlemek maksadıyla geliştirilmiş bir hizmet
- Trafik cloudflare sunucuları üzerinden yönlendirilir

Cloudflare

- DDoS saldırılarını önlemek maksadıyla geliştirilmiş bir hizmet
- Trafik cloudflare sunucuları üzerinden yönlendirilir
- Uygulama sunucusunun IP adresi gizlenmiş olur
- + Bedava SSL Sertifikası ☺

Cloudflare Bypass

- Whois arşivlerinde eski IP adresi yer alıyor olabilir
- DNS History
- Crimeflare
- Subdomain enumeration
- Shodan.io
- Censys.io

Kış Uykusu

- Kısa süre periyodunda Phishing eylemini gerçekleştir (3 gün)
- Uzun bir müddet siteyi kapalı tut (+1 ay)
- Adım 1'e dön

Örnek Faal Site

The screenshot shows the login page of Ziraat Bankası'ın Internet Subesi. The background is red. On the left, there's a white login form with the bank's logo at the top. It has two input fields: 'Müşteri / T.C. Kimlik Numaranızı Giriniz.' and 'Şifrenizi Giriniz'. Below these is a checkbox for 'Mobil İmza İle Giriş' and a large red 'GİRİŞ' button. At the bottom of the form, there are links for 'Şifremi unuttum.' and 'ENGLISH'. On the right, a grey sidebar contains the text 'Ziraat Internet Şubesine Hoş Geldiniz!', a lock icon with a note about security, a hand icon with information about the website, and a 'YARDIM VİDEOLARI' button. A Comodo Secure logo is also present.

Ziraat Bankası

Müşteri / T.C. Kimlik Numaranızı Giriniz.

Şifrenizi Giriniz

Mobil İmza İle Giriş

GİRİŞ

Şifremi unuttum.

ENGLISH

0850 220 00 00

Müşteri İletişim Merkezi Güvenlik Yardım

Ziraat Internet Şubesine Hoş Geldiniz!

Müşteri numaranızı, İnternet/Mobil bankacılık giriş ve ATM şifrenizi Ziraat Bankası personeli dahil kimse ile paylaşmayın.

Ziraat Bankası Internet Şubesi'ne sadece www.ziraatbank.com.tr adresindeki "Internet Şubesi" linkine tıklayarak ulaşınız

YARDIM VİDEOLARI

COMODO SECURE

Örnek Kış Uykusunda Site

Anasayfa Haber Analiz Teknik Bitcoin Konim Bit Türk Bitkapital Btc Türk Feyex Paribu İletişim 

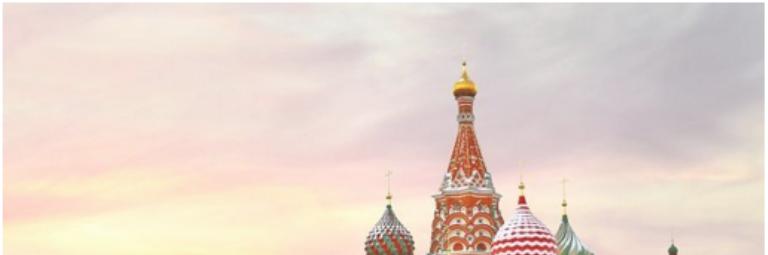
Bitcoin ve Litecoin Fiyat Analizleri
Türk lirası ile ülkemizde en uygun nasıl dijital para alınır ve satılır anlaşılır grafikle analizci haber bülteni



Anasayfa Haber Analiz Teknik Bitcoin Konim Bit Türk Bitkapital Btc Türk Feyex Paribu

[İletişim](#)

14
C



Burada ara... 

Bukalemun

- Domain uykudayken siteye «masum» içerikler koy
 - Blog, haber sitesi v.b
- Mümkünse uyku süresince gelecek ziyaretçileri uzaklaştır
 - Yabancı dilde içerik (Japonca, çince, ibranice)
 - Hata mesajları

In OPSEC Fails We Trust :(

Hello, [REDACTED] 🙋

Here is your mentions for yesterday about your alert [REDACTED]

Mentions 2
-33%

Featured mentions

Here are your top mentions by influencer score

[View all mentions](#)

[REDACTED] [turkhackteam.org](#) • 29 Sep [Mark as irrelevant](#)

Tüm Fake Script Phisingler satılır - Kodlanır

→ [REDACTED] [Phising] : <https://youtu.be/N2hKtqpNp78>

In OPSEC Fails We Trust :(

Turkhackteam Bilgilendirme Sistemi

asdf, Bu sayfaya giriş yetkiniz bulunmuyor. Aşağıdaki sebeplerden biri bu soruna neden oluyor olabilir.

1. Konu veya mesaj forum kurallarına aykırı olduğundan çöp'e taşınmış olabilir.
2. Mesaj yazmak istediyiniz üyeliğiniz yasaklanmış olabilir veya üyeliğinizin aktifleştirilmesi gerekebilir.

[Çıkış yap](#) [Anasayfa](#)

In OPSEC Fails We Trust :(

1 sonuç (0,18 saniye)

Tüm Fake Script Phisingler satılır - Kodlanır - İleg4lizm

www.illeg4lizm.org/konu-tum-fake-script-phisingler-satilir-kodlanir.html?pid=162738 ▾

Bütün hepsini az önce 10K ya sattım gerek kalmadığı için konu silinmiştir.

In OPSEC Fails We Trust :(

Tüm Fake Script Phisingler satılır - Kodlanır

beratttacasd123

Yararlı Üye

illegal Üye

Rütbe: illegal Üye

Üye Offline

Konu Sayısı: 18

Mesaj Sayısı: 113

Üye No: 20531

Üyelik: 14.05.2017

0

Para: 347TL

Konu : Tüm Fake Script Phisingler satılır - Kodlanır - 29.09.2017, 23:30

Mesaj: #1

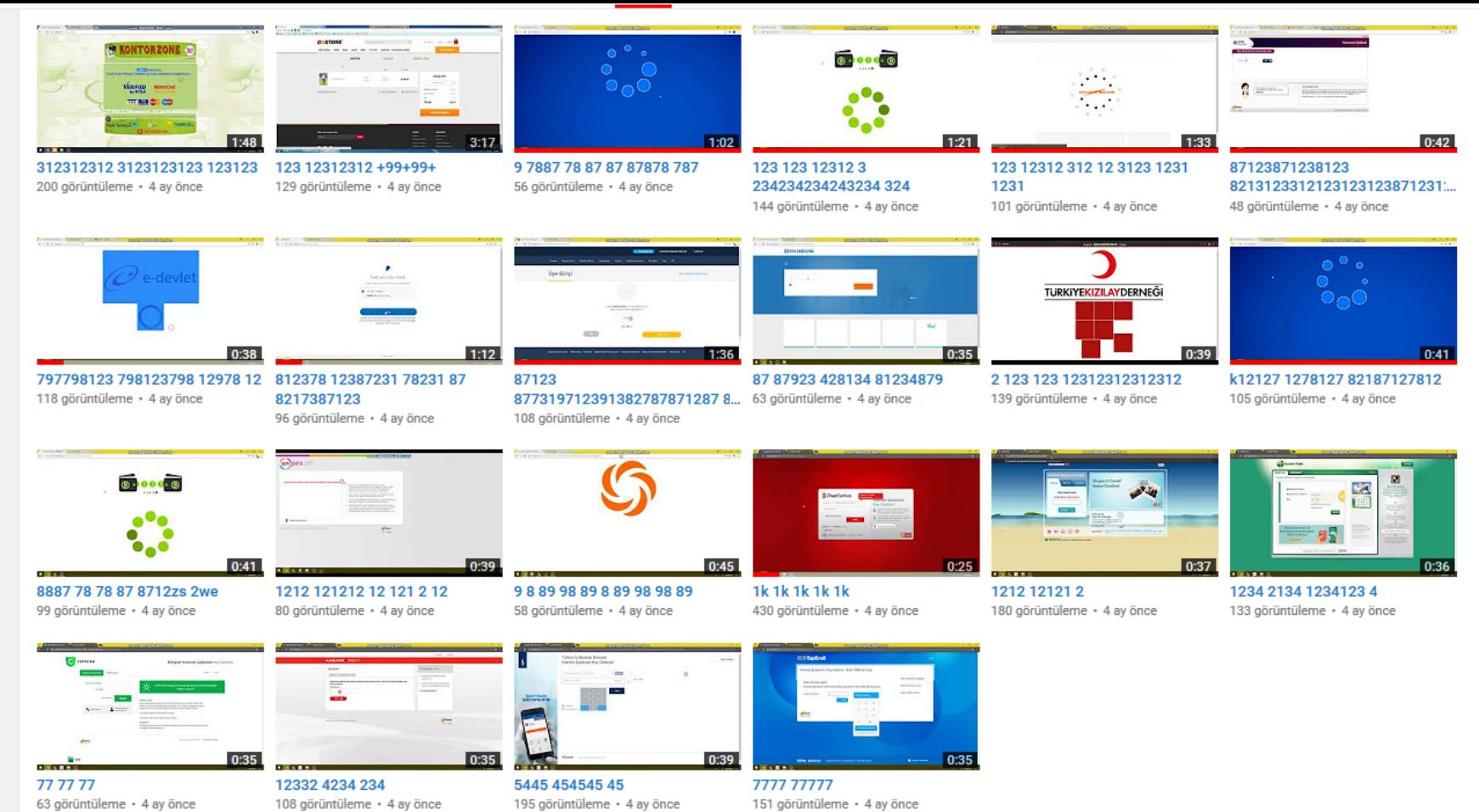
Merhaba sayın ziyaretçimiz.

Sitemize kayıtlı değilseniz mesajın içeriğini görebilmeniz için [üye ol](#) bağlantısını kullanarak sitemize üye olmanız gerekmektedir. Eğer zaten kayıtlı kullanıcı iseniz, lütfen kullanıcı adınız ve şifreniz ile [giriş](#) yapınız. (Sitemize üyelik ücretsizdir).

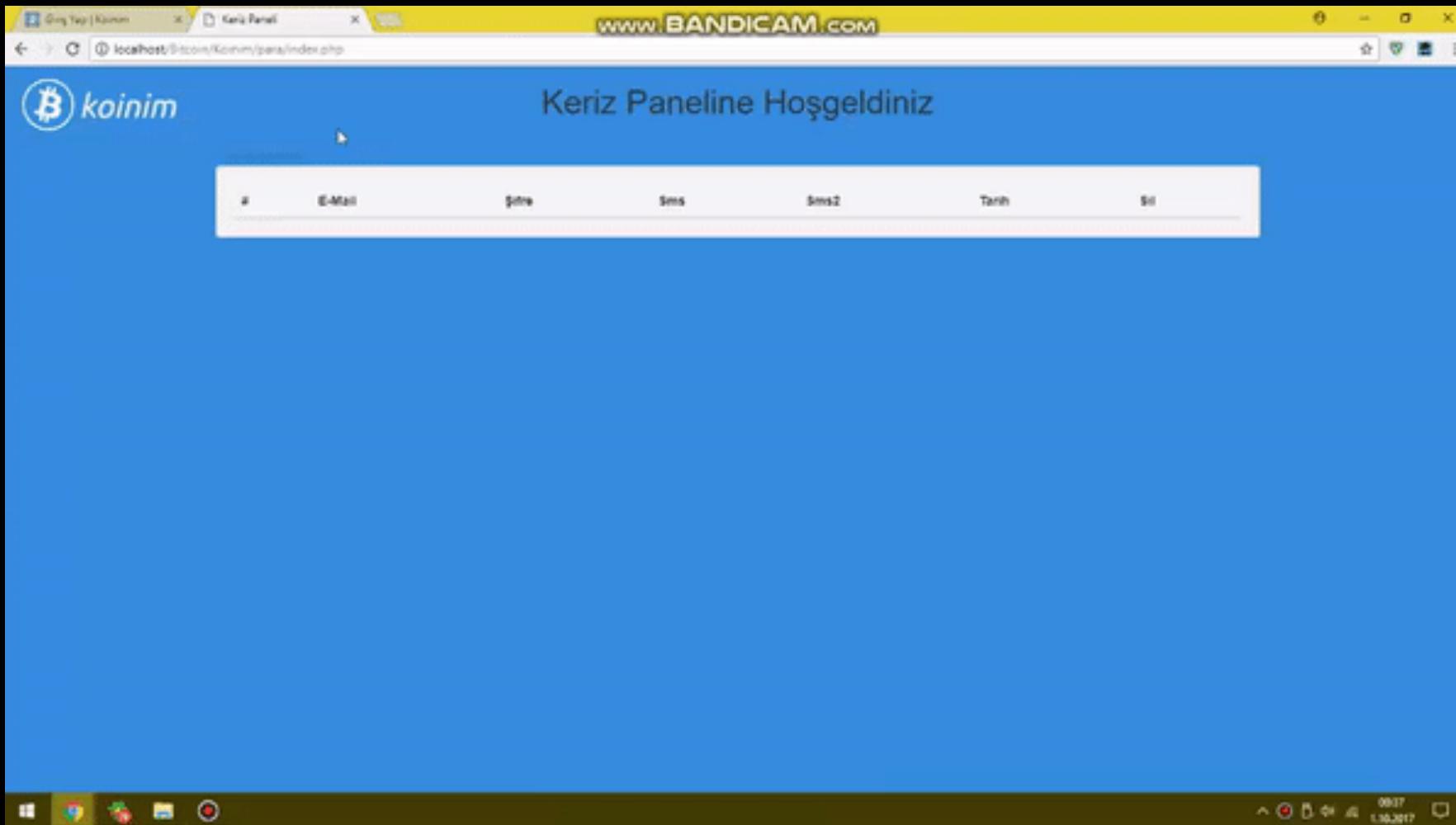
beratttacasd123, üyesi illegalizm | Private illegal Topluluk - Hack forum, Warez Scriptler forumlarına 14.05.2017 tarihinde katılmıştır.

(Son Düzenleme: 01.10.2017, 21:38, Düzenleyen: beratttacasd123.)

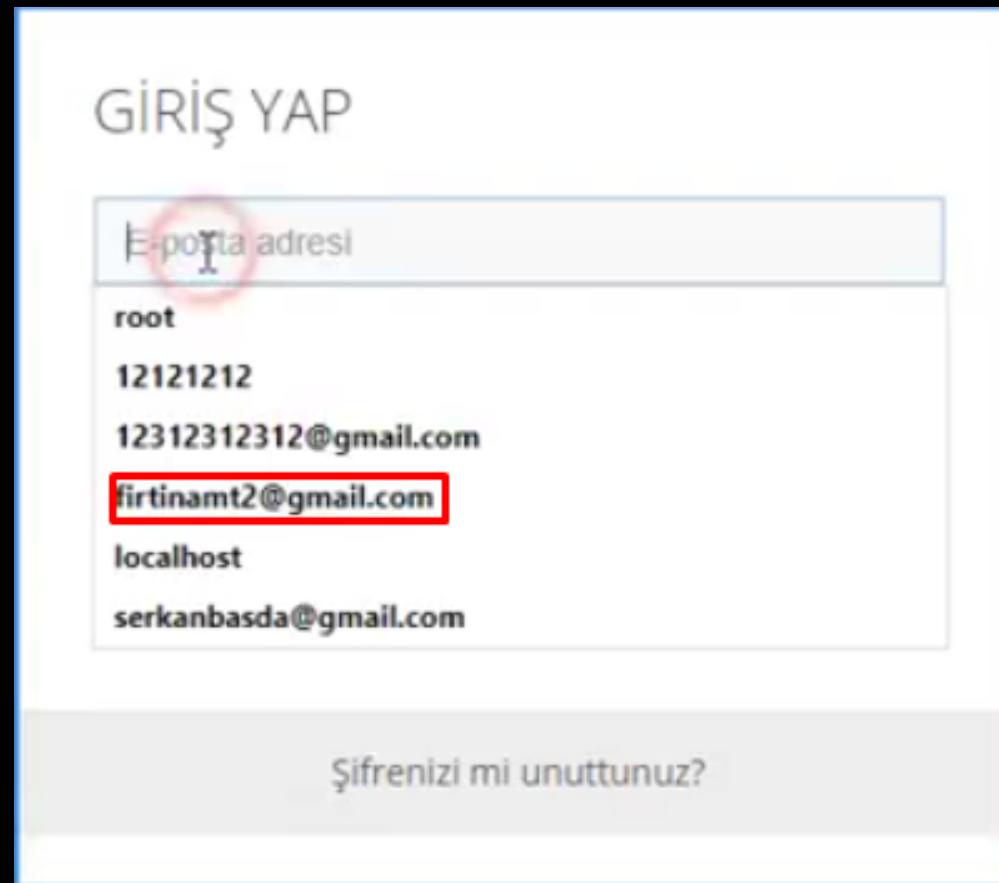
In OPSEC Fails We Trust :(



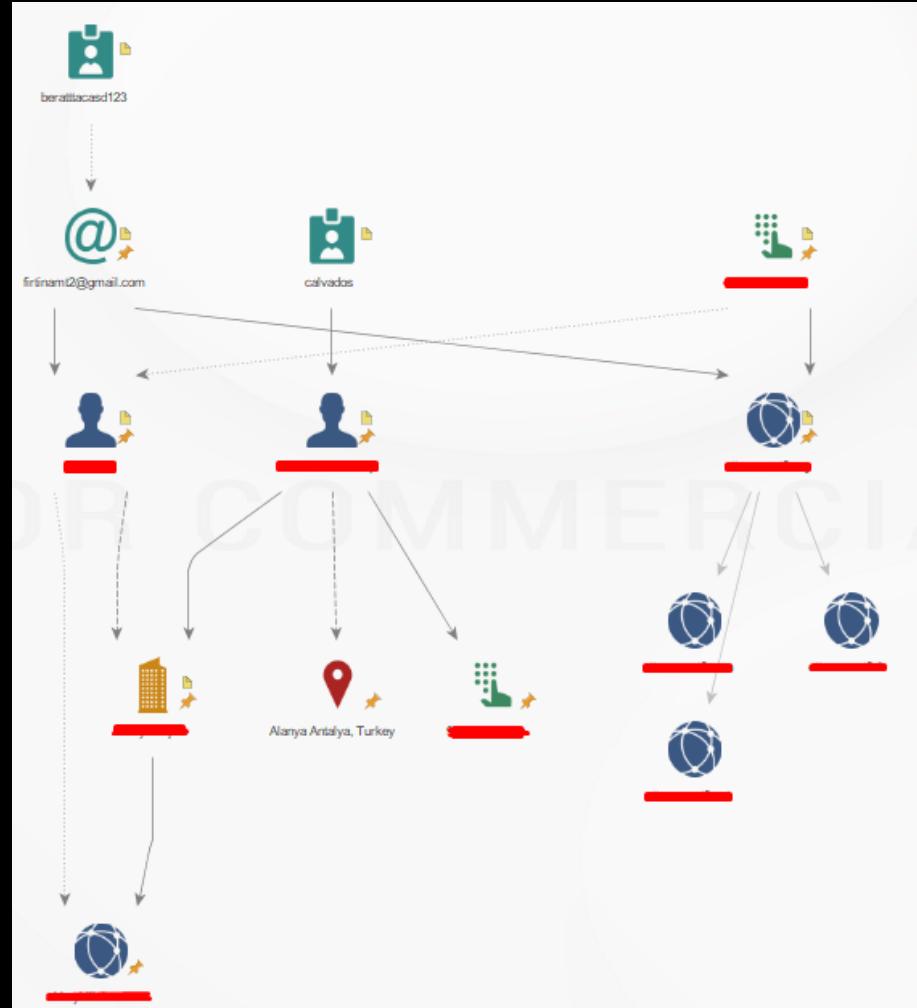
In OPSEC Fails We Trust :(



In OPSEC Fails We Trust :)



In OPSEC Fails We Trust :):)



Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme

Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme
- Cezaevi Etkisi

Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme
- Cezaevi Etkisi
- Adli Farkındalık

Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme
- Cezaevi Etkisi
- Adli Farkındalık
- Erişilebilirlik

Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme
- Cezaevi Etkisi
- Adli Farkındalık
- Erişilebilirlik
- Anonimlik (kısmen)

Kinetik Suç vs Siber Suç

- Duygusal Deneyimleme
- Cezaevi Etkisi

FAQ Detail

What is the probability of conviction for felony defendants?

<https://www.bjs.gov/index.cfm?ty=qajid=403>

Among felony defendants whose cases were adjudicated within the one-year tracking period (89% of cases), 68% were convicted. This includes a 59% felony conviction rate with the remainder receiving misdemeanor convictions. Felony conviction rates were highest for defendants originally charged with motor vehicle theft (74%), a driving-related offense (73%), murder (70%), burglary (69%), or drug trafficking (67%). They were lowest for defendants originally charged with assault (45%).

- Kazanç / Risk

The conviction rate in 2010 was even worse. According to [FBI's 2010 Internet Crime Report](#), from 303,809 complaints, 1,420 prepared criminal cases resulted in a mere six convictions. That's one jailed cyber criminal for every 50,635 victims, and these are just the cases significant enough to be reported to the FBI.

<https://www.csionline.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html>

Multidisipliner Yaklaşım

- Kriminal Profilleme
- Adli Dilbilimi
- İstihbarat
- Psikolojik Harekat
- Uluslararası İlişkiler

Kriminal Profilleme

- İlişkilendirme
- Belirginlik
- Karakteristikler
- Lokasyon
- Yordama

Kriminal Profilleme

- İlişkilendirme -> Hangi suçlar aynı fail tarafından işlenmiştir?

- Belirginlik

Asset analizi

- Karakteristikler

Hedef Seçimi

Teknik Taktik Prosedür

- Lokasyon

İmzalar

- Yordama

Motivasyon

Strateji

Kriminal Profilleme

- İlişkilendirme
- Belirginlik -> Ayırt edici davranış ve özellikler
- Karakteristikler
- Lokasyon
- Yordama

Kriminal Profilleme

- İlişkilendirme
 - Belirginlik
 - Karakteristikler -> Nasıl tanıyalabiliriz?
 - Lokasyon
 - Yordama
- Kabiliyet analizi**
- Finansal fonlama**
- Kişisel özellikler?**

Kriminal Profilleme

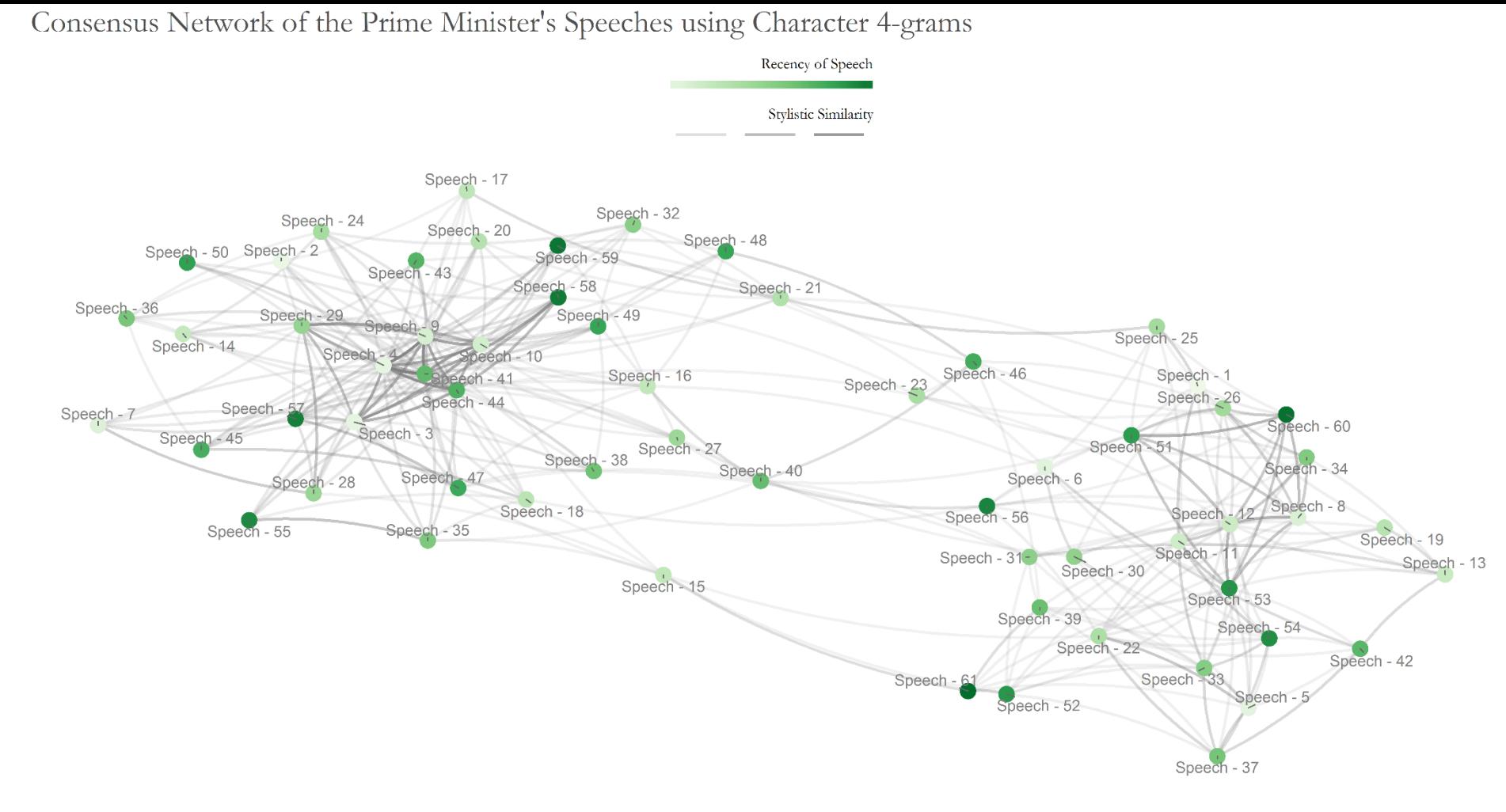
- İlişkilendirme
- Belirginlik
- Karakteristikler
- Lokasyon - nerede
- Yordama

Kriminal Profilleme

- İlişkilendirme
- Belirginlik
- Karakteristikler
- Lokasyon
- Yordama -> Bir sonraki adımı ne olacak?

Adli Dilbili - Stilometri

Consensus Network of the Prime Minister's Speeches using Character 4-grams



Adli Dilbilimi - Stilometri

- Fidye notları

Adli Dilbilimi - Stilometri

- Fidye notları
- Clearnet platformlar – kimlik biliniyor

Adli Dilbilimi - Stilometri

- Fidye notları
- Clearnet platformlar – kimlik biliniyor
- Underground platformlar – kimlik bilinmiyor

Adli Dilbilimi - Stilometri

- Fidye notları
- Clearnet platformlar – **kimlik biliniyor**
- Underground platformlar – **kimlik bilinmiyor**
- Deep learning?

Adli Dilbili mi - Stilometri

Should this even be released? Please vote. #1

① Open mlpoll opened this issue on 26 Jul 2016 · 44 comments

 mlpoll commented on 26 Jul 2016 • edited Owner + 

This repository is currently without any code for a reason. Please comment and vote with thumbs up/down.

What is it?

Anonymous text series in (such as a Reddit or Amazon (review) account), authors real name out.

MachineMatch utilizes deep learning techniques to analyze blog posts, articles, papers and comments **where the identity is known**.

The same analysis is used on **anonymous** posts, such as Reddit comments, (fake) Amazon reviews and anonymous blog posts.

The resulting text analysis is then used to identify who wrote the anonymous post. The principle is similar to that of identifying plagiarism, but with more advanced deep learning techniques.

How good is it?

With a well trained network, the accuracy is remarkable, > 95% on my test input. Even when people write a bit differently when posting anonymously, the matching is very accurate if enough text is provided (esp. longtime redditors leak enough information about themselves to make manual verification quite easy!)

Adli Dilbili mi - Stilometri



theshadowbrokers [Follow](#)

Apr 8, 2017 · 6 min read

Don't Forget Your Base

Dear President Trump,

Respectfully, what the fuck are you doing? TheShadowBrokers voted for you. TheShadowBrokers supports you. TheShadowBrokers is losing faith in you. Mr. Trump helping theshadowbrokers, helping you. Is appearing you are abandoning “your base”, “the movement”, and the peoples who getting you elected.

İstihbarat

- HUMINT
- Underground platformlarda yapılacak angajman ve elemanlama çalışmaları

İstihbarat

- HUMINT
- Underground platformlarda yapılacak angajman ve elemanlama çalışmaları
- IOC != Intelligence !!!

Psikolojik Harekat

The image displays two side-by-side screenshots of seized dark web marketplaces, both featuring a dark blue background with a network-like pattern.

Hansa Market (Left):

- Notice:** THIS HIDDEN SITE HAS BEEN SEIZED and controlled since June 20
- by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hesse (Germany).
- Logo:** A stylized orange and red logo resembling a flame or a rising sun.
- Text:** The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted user information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at politiepol422eu.onion.
- Logos:** Hansa, AlphaBay Market, OPENBAAR MINISTERIE, POLITIE, and EUROPOL.

AlphaBay Market (Right):

- Notice:** THIS HIDDEN SITE HAS BEEN SEIZED Since July 4, 2017
- as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol
- In accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.
- Logo:** A large orange letter 'a' inside a white circle.
- Logos:** HANSA, AlphaBay Market, POLITIE, EUROPOL, NCA, and several other law enforcement agency logos.

Uluslararası İlişkiler

Theories of International Relations



Realism



Idealism/Liberalism



Neo-Realism



Constructivism



Post Structural Theory



Marxist Theories



Feminist Approach



Postcolonial Theories

Kaynakça

- <http://www.hukukmedeniyeti.org/haber/18440/yargitay-internet-hesabindan-calinan-paradan-banka/>
- <https://emsal.yargitay.gov.tr/>
- http://aliarsalankazmi.github.io/blog_DA/posts/r/2016/11/18/authorial_analysis_pm.html
- <https://medium.com/@FaustDeGoethe/on-the-shadow-brokers-poor-grammar-acdc1c27ad84>
- <https://thenextweb.com/insider/2017/07/20/police-fbi-drug-dark-web-market/>

Sorular?