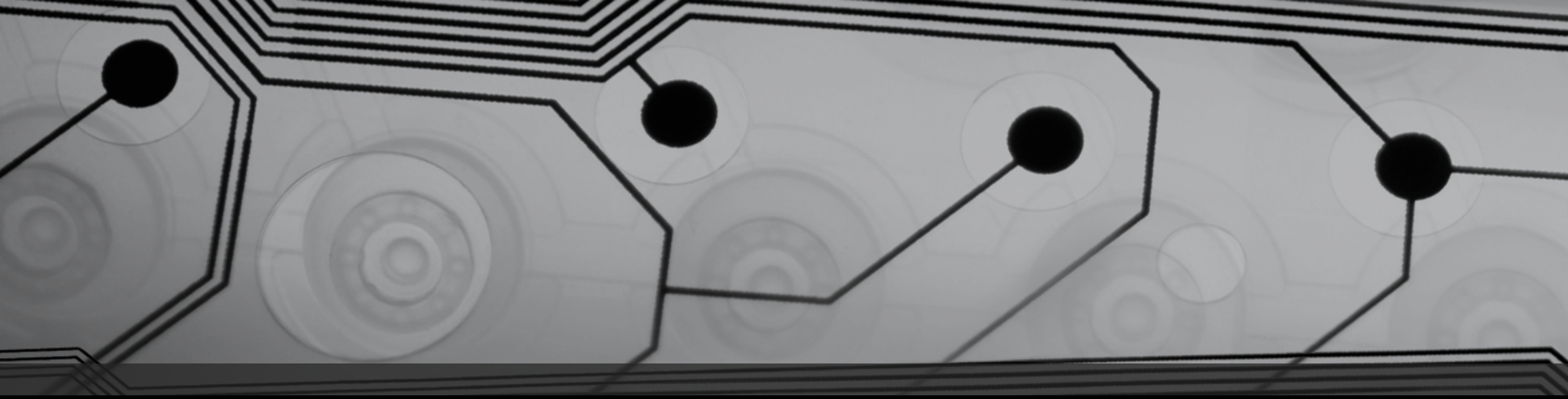


In OPSEC Fails We Trust

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
MULTIDISCIPLINARY WARRIOR BOOTCAMP

arquanum

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 CustomerServiceDefenceIC Oct 28 (5 days ago)

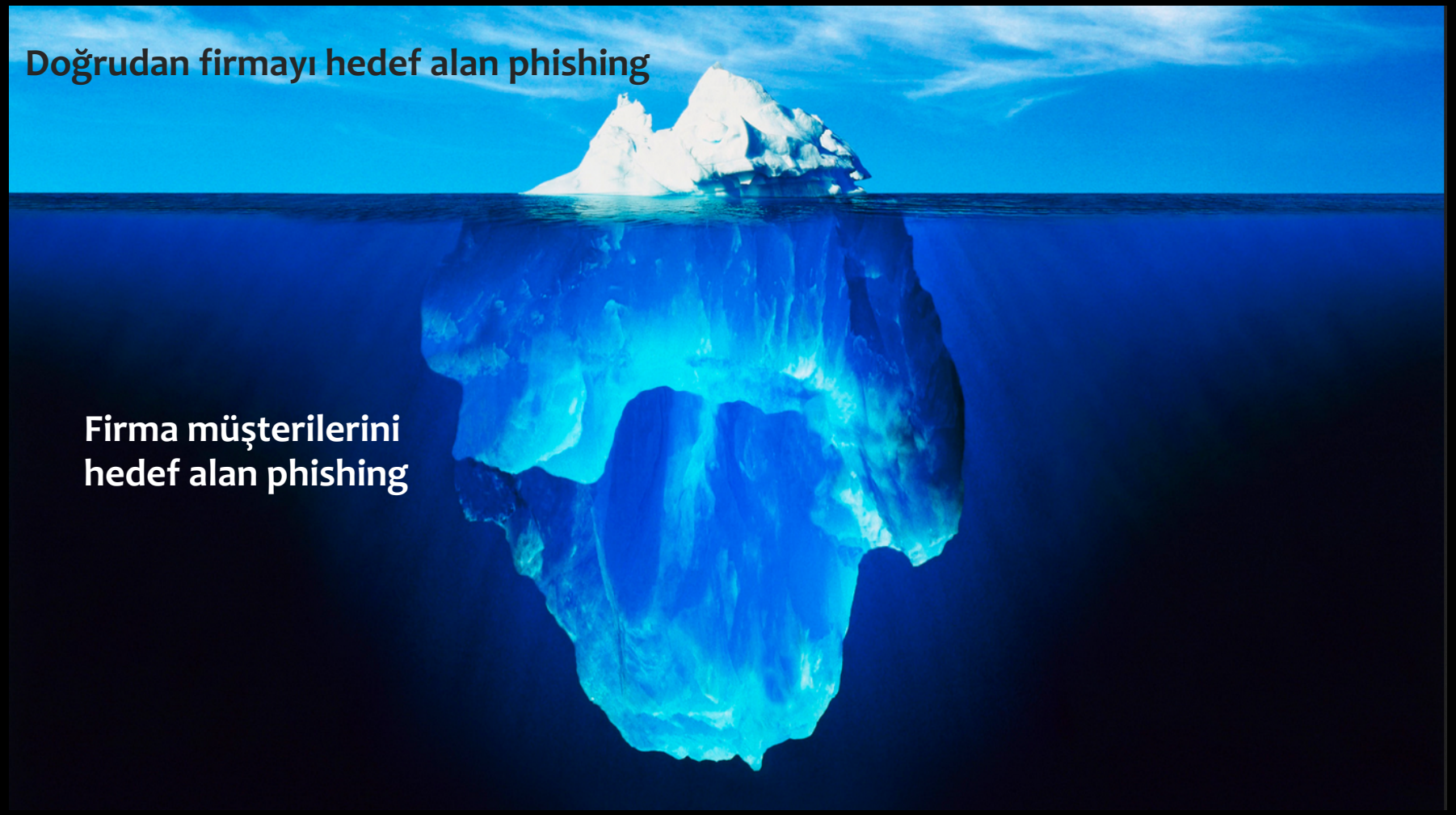
to [redacted]

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.

Programm_Detail...

Dışı Seni İçi Beni



Dışı Seni İçi Beni

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

"İçtihat Metni"

MAHKEMESİ :T

DAVA T

Yargıtay: İnternet hesabından çalınan paradan banka sorumlu

Bilgisayarına virüs gönderilerek 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 bilgisi ve izni dışında hesabından çekilen 2 bin lirayı banka ödeyecek.

...ce verilen Kredi ... Başkanlık Kurulu'nun ... girmiş olmasına ve Yargıtay ...251-27501 sayılı kararı ile dosyanın ...esi Başkanlığına gönderilmesine dair karar ... kaydedildiği anlaşılmakla dosyanın Yargıtay 19. ... Yargıtay Hukuk İş Bölümü İnceleme Kurulu'na ...lığıyle karar verildi.

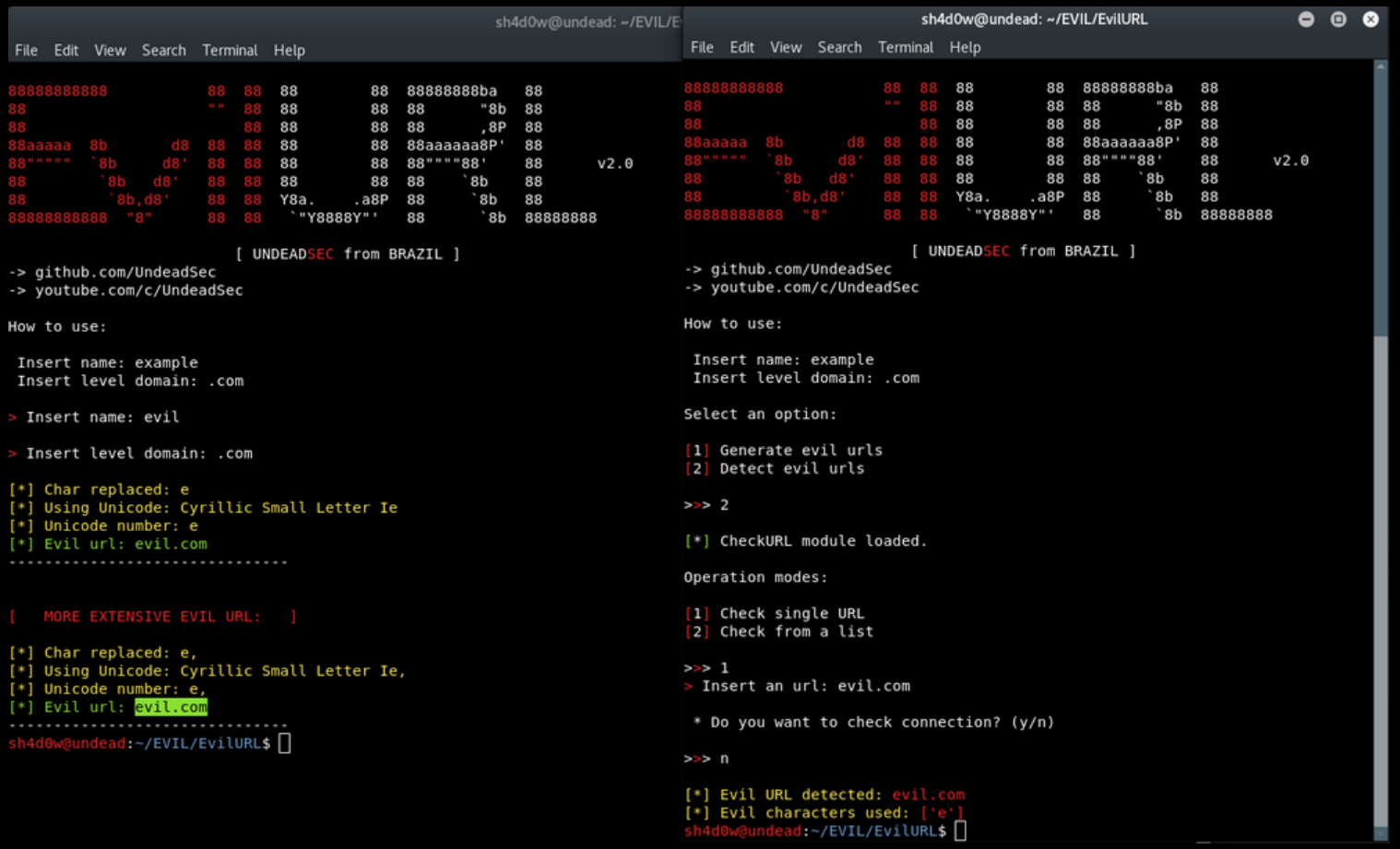
OSINT #1

- 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$
```

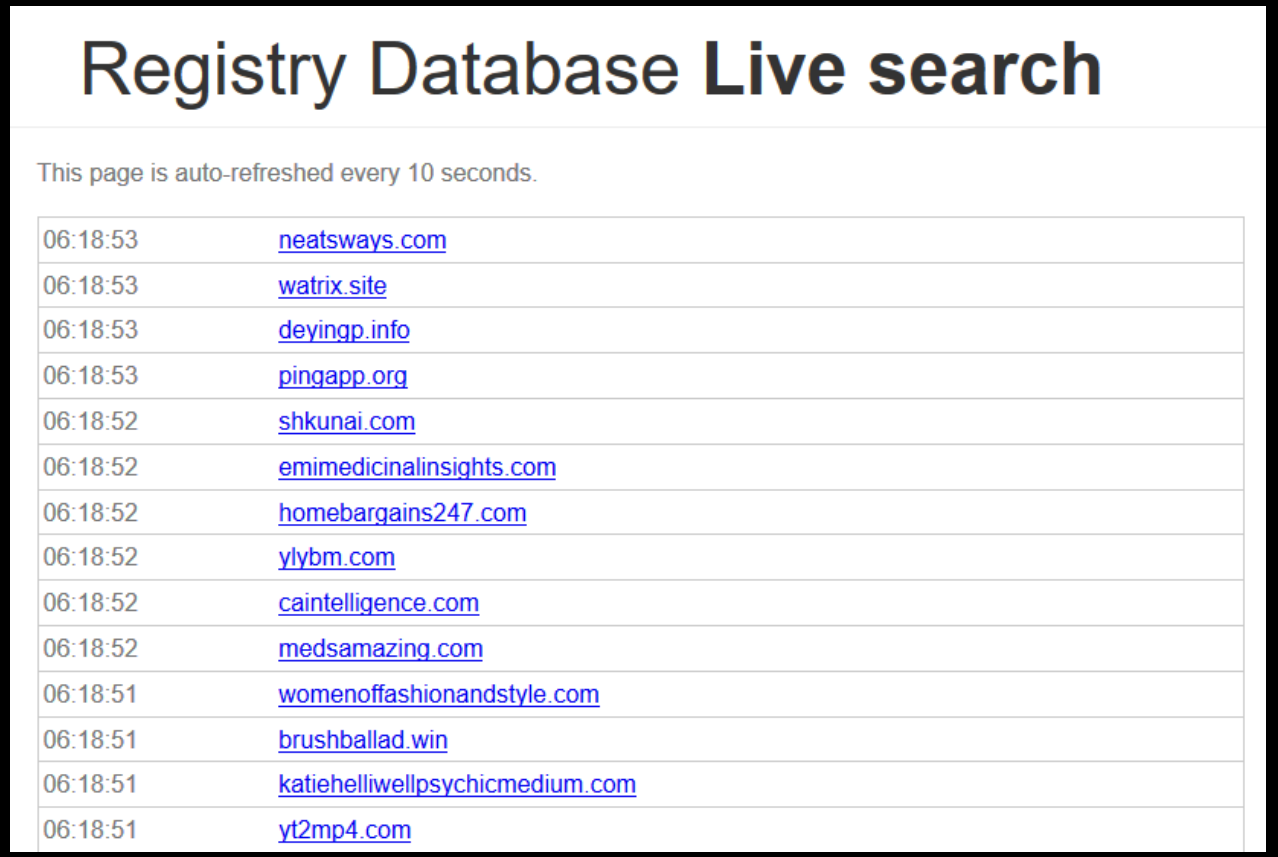
OSINT #1

- Benzer domainleri üret ve aktiflik durumlarını kontrol et



OSINT #2

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



Registry Database **Live search**

This page is auto-refreshed every 10 seconds.

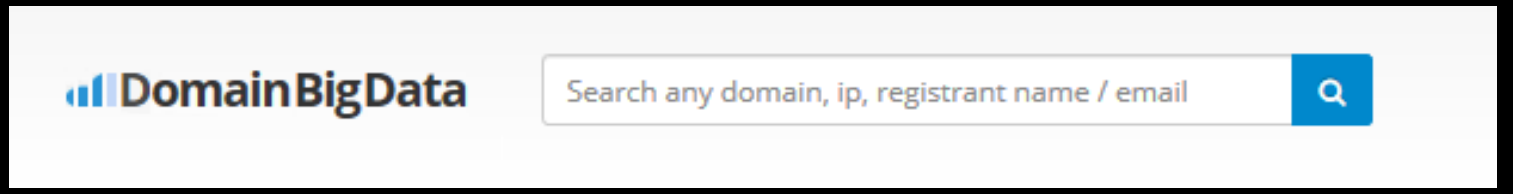
06:18:53	neatsways.com
06:18:53	watrix.site
06:18:53	deyingp.info
06:18:53	pingapp.org
06:18:52	shkunai.com
06:18:52	emimedicinalinsights.com
06:18:52	homebargains247.com
06:18:52	ylybm.com
06:18:52	caintelligence.com
06:18:52	medsamazing.com
06:18:51	womenoffashionandstyle.com
06:18:51	brushballad.win
06:18:51	katiehelliwellpsychicmedium.com
06:18:51	yt2mp4.com

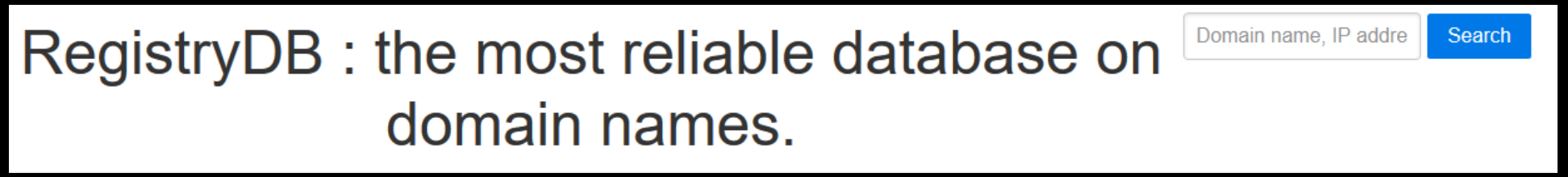
OSINT #3

- CTL Monitoring (certstream)

OSINT #4

- Whois arşivleri üzerinden çapraz sorgulama (DEMO)



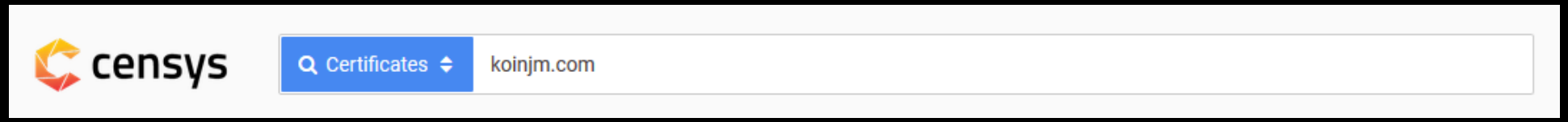


OSINT #5

- Just Google It ☺

OSINT #6

- Censys.io certificate search

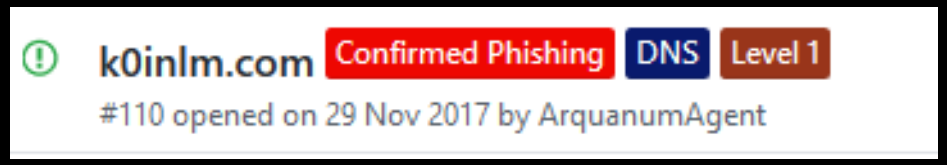


aileronarts.com
aoron.net
astridfinnell0ei5y.ga
benmi.store
bestroadster.win
bpbil.loan
brentfordminicabs.co.uk
bthxf.loan
ccxpn.loan
cvttyz.loan
dfvfv.loan
directbykgxt.ml
etsss.loan
expertsinstress.com
ffqsh.loan
garantihesabim.com
irocky.com
it-consultis.net
klrca.org.my

koinimy.com
koinjm.com
komot.online
kxypp.loan
lequ.loan
louettamanrique1d3qc.cf
mdbyy.loan
mentem.ru
moldumobel.es
nanetteleaguekhzkeh.tk
newergcnmrf.ga
ozbooker.ml
paisa.science
qmltt.loan

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 ☺

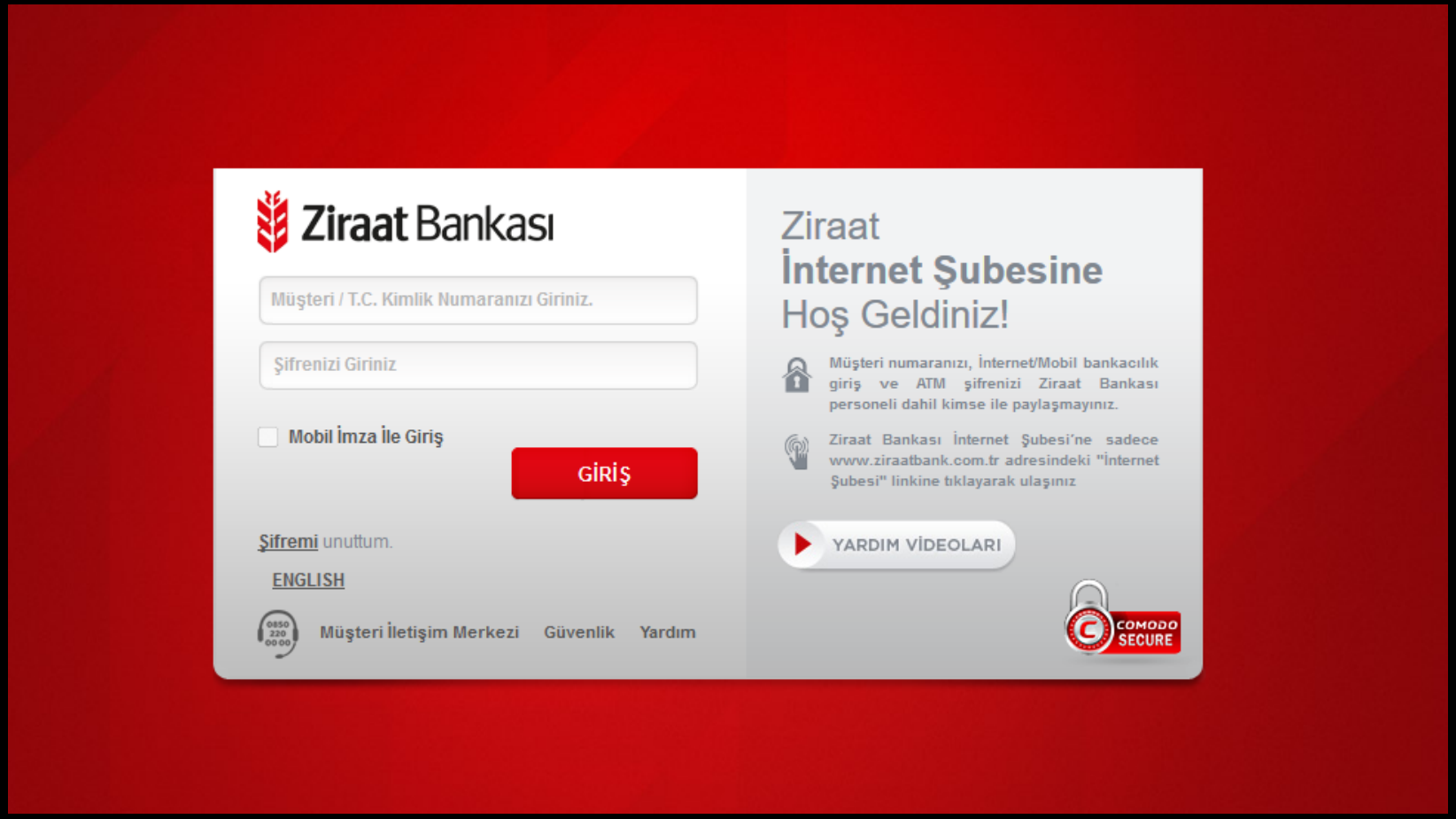
Cloudflare Bypass

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

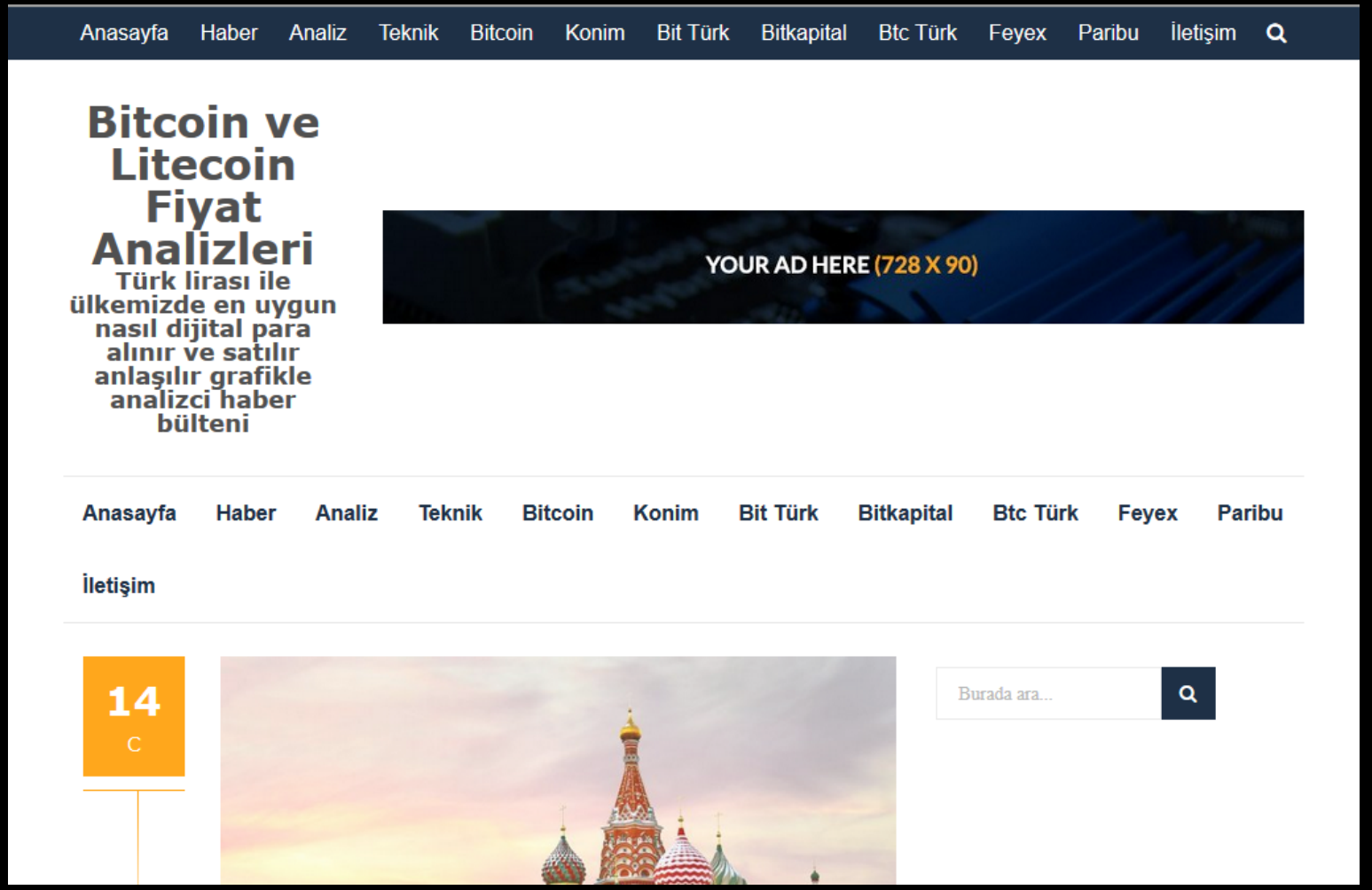
Kış Uykusu

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

Örnek Faal Site



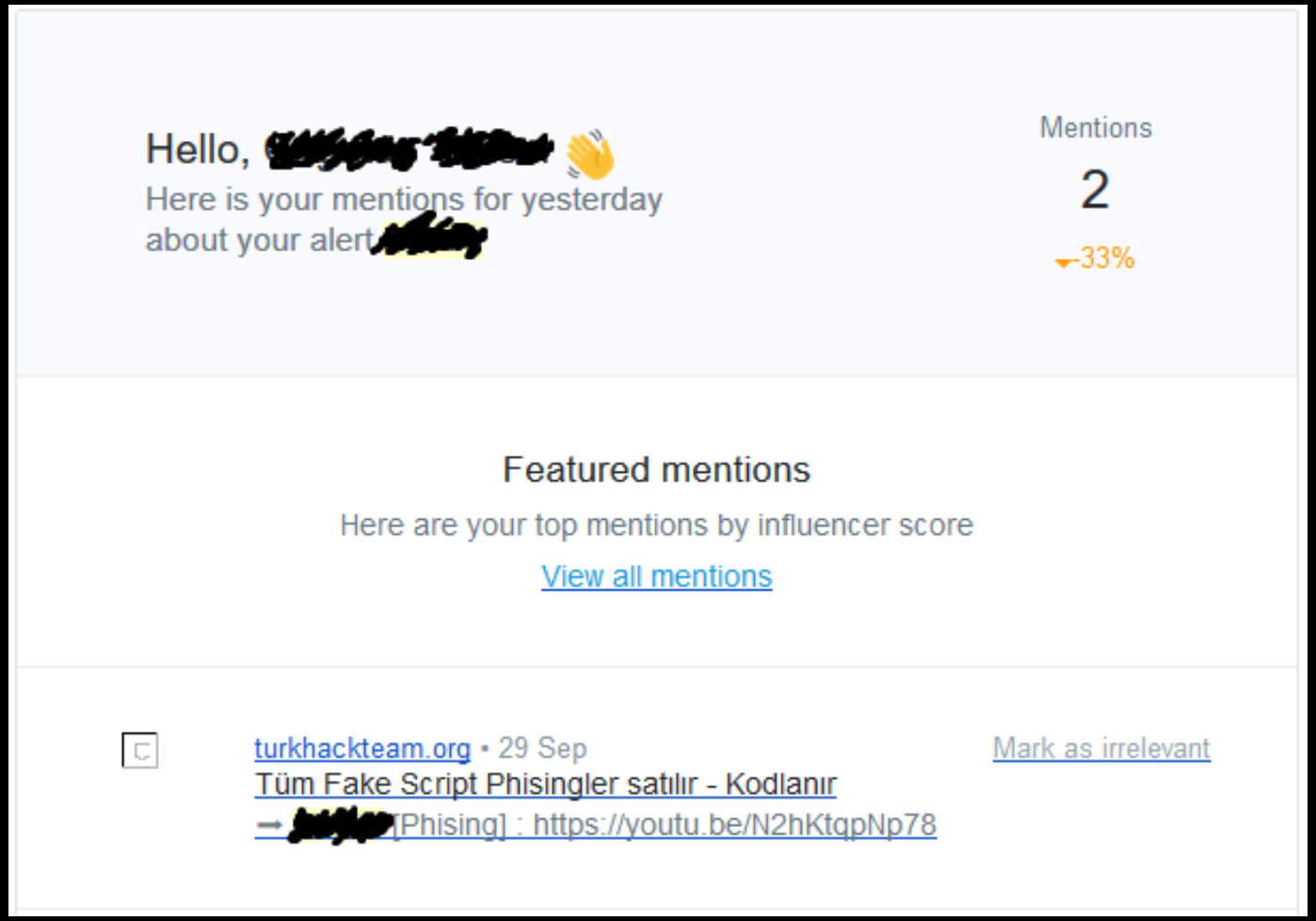
Örnek Kış Uykusunda Site



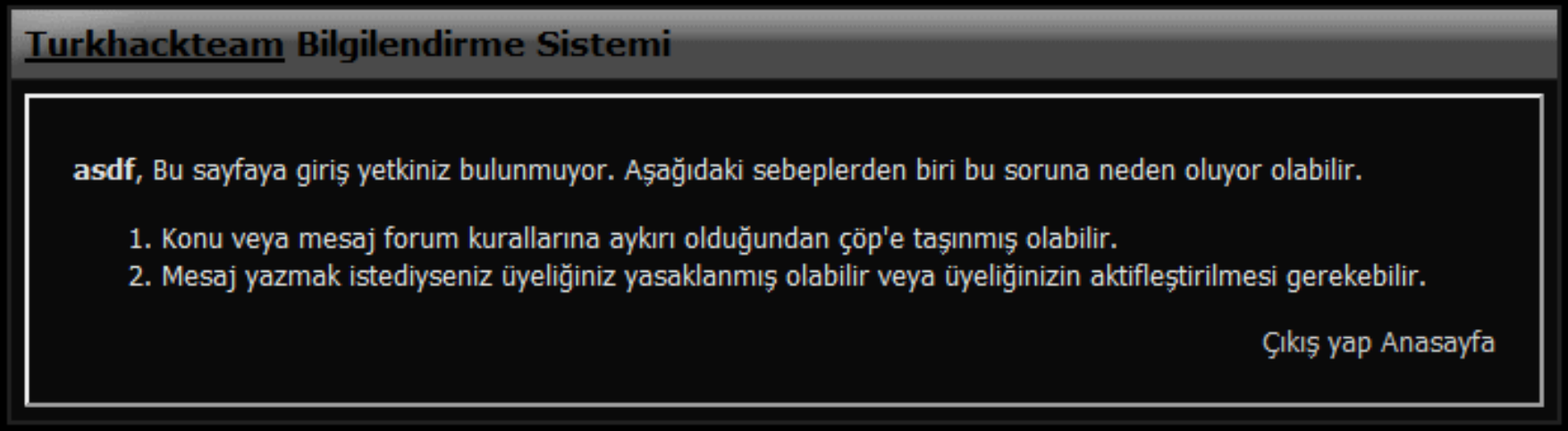
Bukalemun

- 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

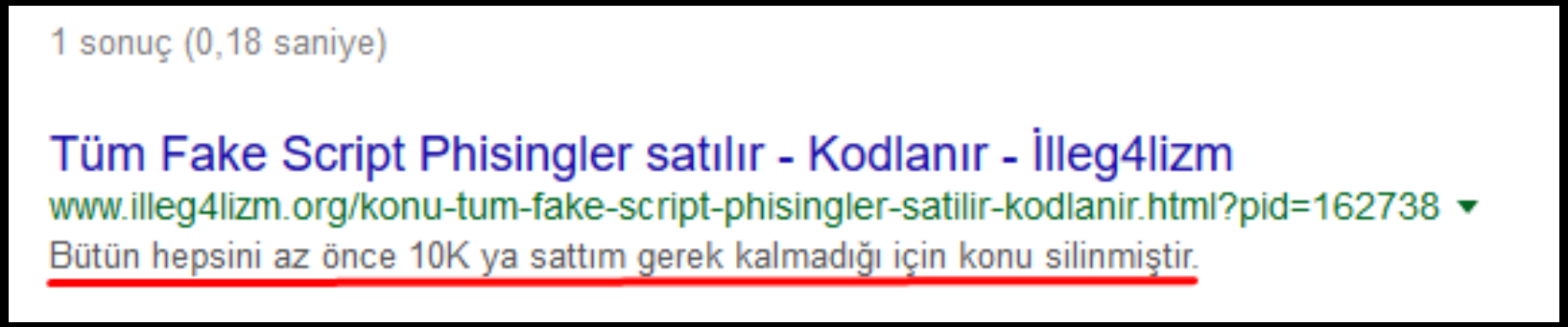
In OPSEC Fails We Trust :(



In OPSEC Fails We Trust :(



In OPSEC Fails We Trust :(



In OPSEC Fails We Trust :(

Tüm Fake Script Phisingler satılır - Kodlanır

beratttacasd123
Yararlı Üye
illegal Üye

0

Rütbe: illegal Üye
Üye Offline
Konu Sayısı: 18
Mesaj Sayısı: 113

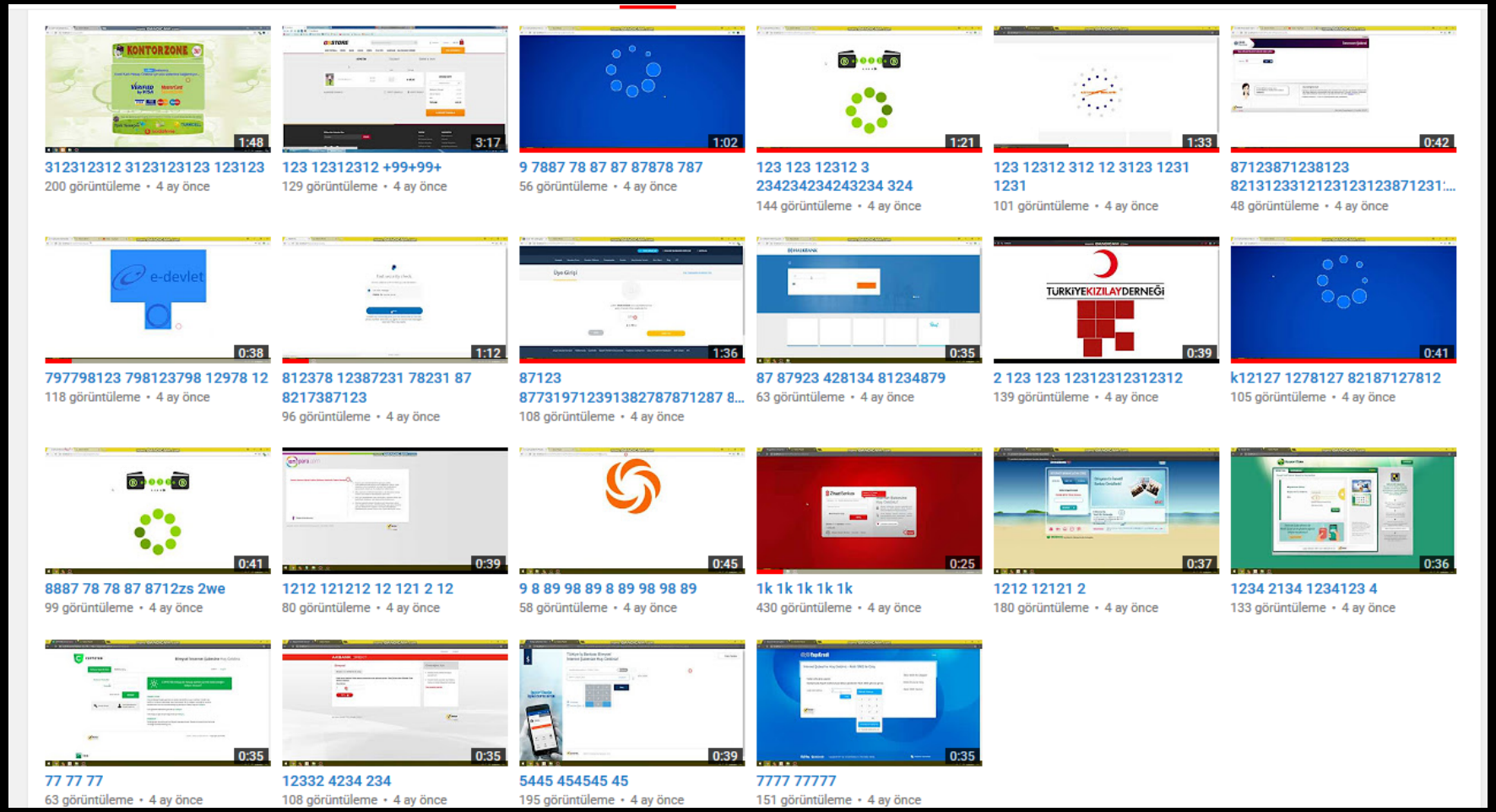
Para: 347TL

Üye No: 20531
Üyelik: 14.05.2017

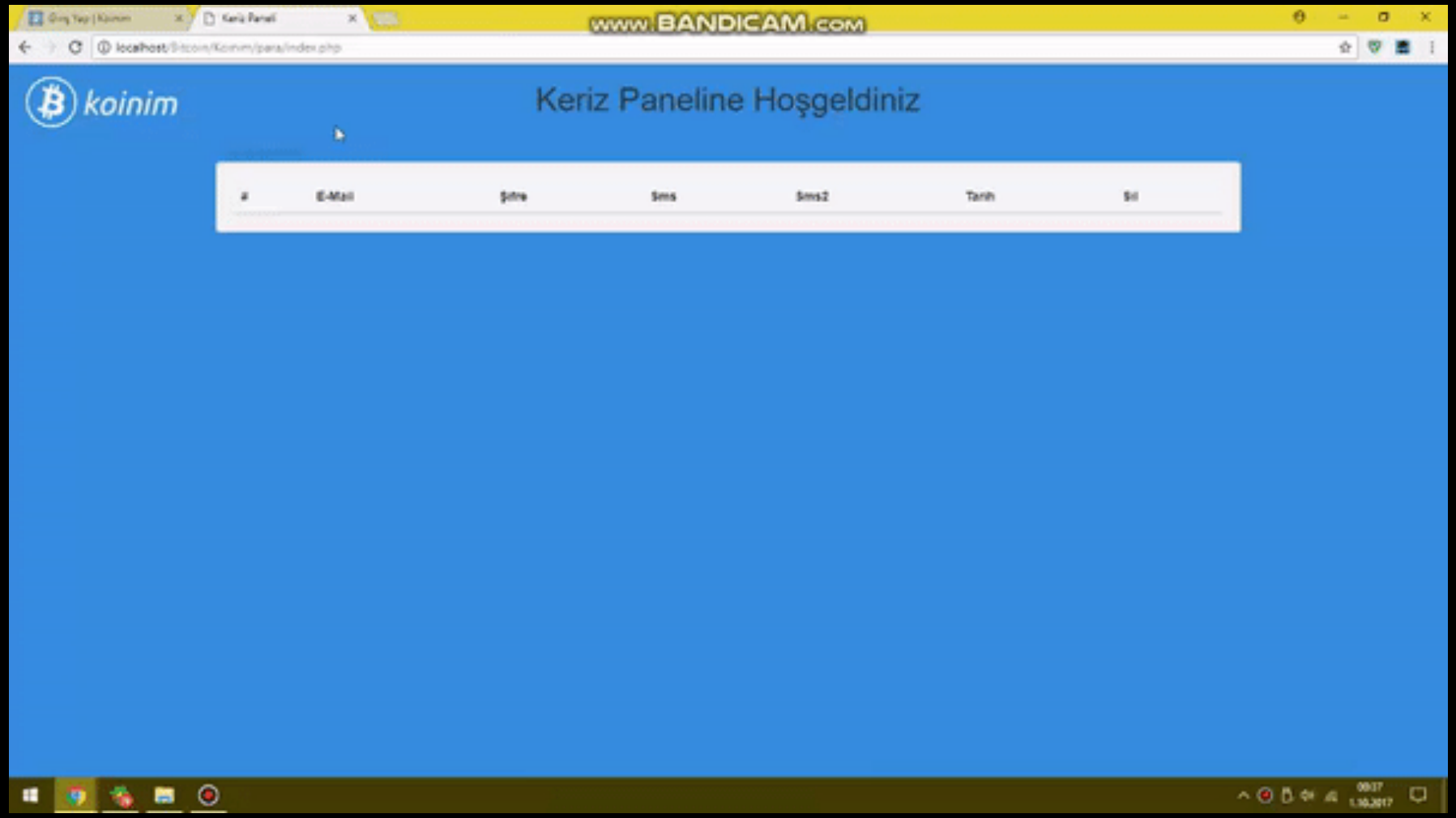
Konu : **Tüm Fake Script Phisingler satılır - Kodlanır** - 29.09.2017, 23:30
Mesaj: #1
Merhaba sayın ziyaretçimiz.
Sitemize kayıtlı değilseniz mesajın içeriğini görebilmeniz için üye ol bağlantısını kullanarak sitemize üye olmanız gerekmektedir. Eğer zaten kayıtlı kullanıcı iseniz, lütfen kullanıcı adınız 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.)

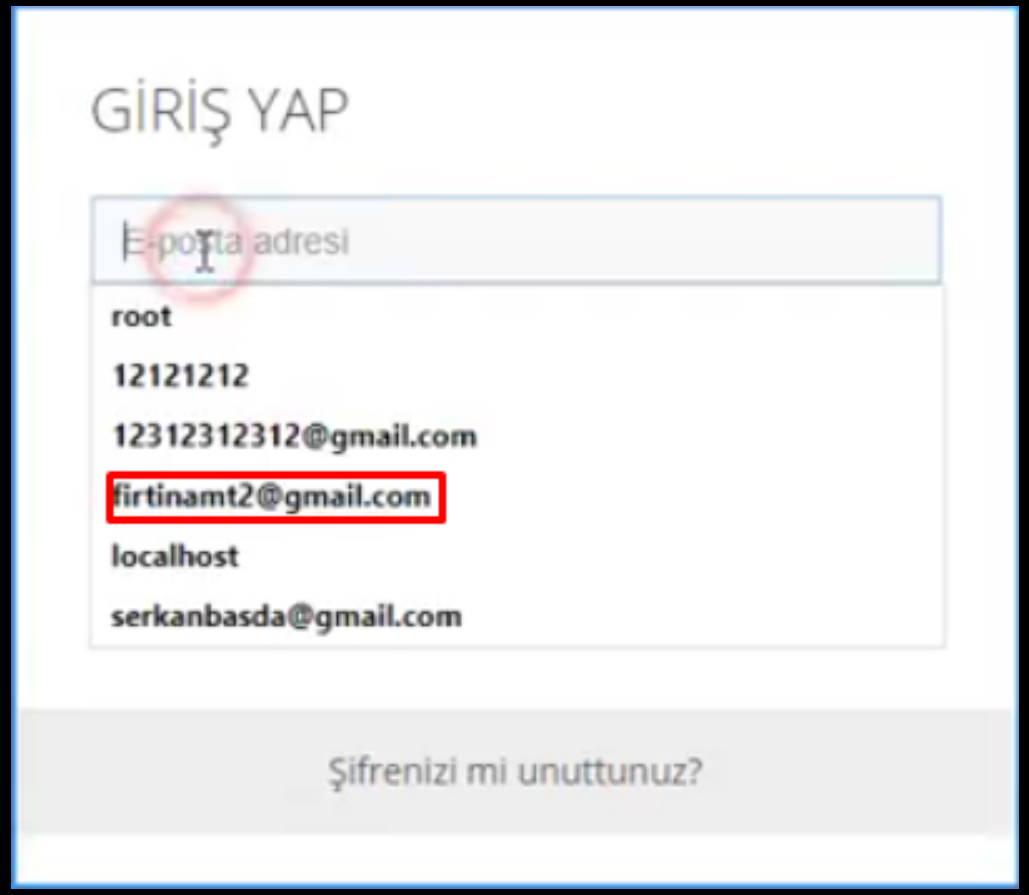
In OPSEC Fails We Trust :(



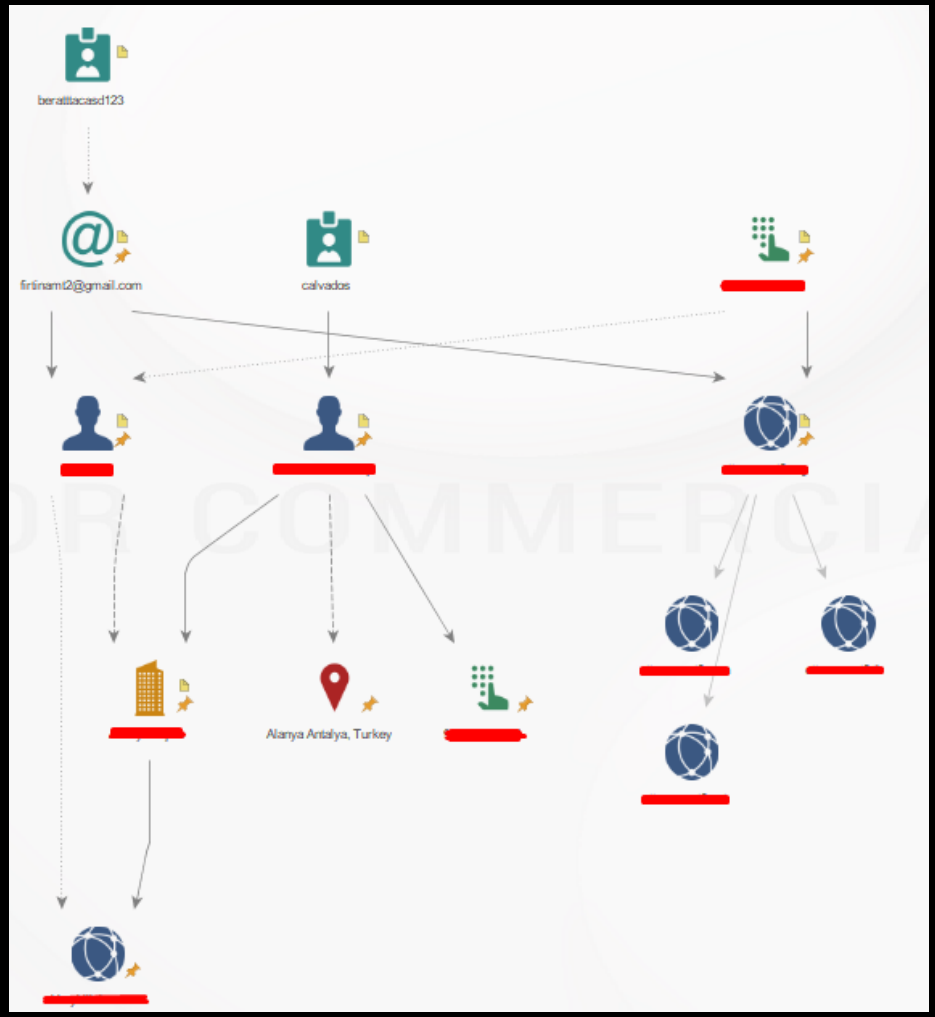
In OPSEC Fails We Trust :(



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=qa&iid=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.csoonline.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
- Karakteristikler
- Lokasyon
- Yordama

Asset analizi

Hedef Seçimi **Teknik Taktik Prosedür**

İmzalar

Motivasyon **Strateji**

Kriminal Profilleme

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

Kriminal Profilleme

- İlişkilendirme
- Belirginlik
- Karakteristikler -> Nasıl tanıyabiliriz?
- Lokasyon
- Yordama

Kabiliyet analizi

Finansal fonlama

Kişisel özellikler?

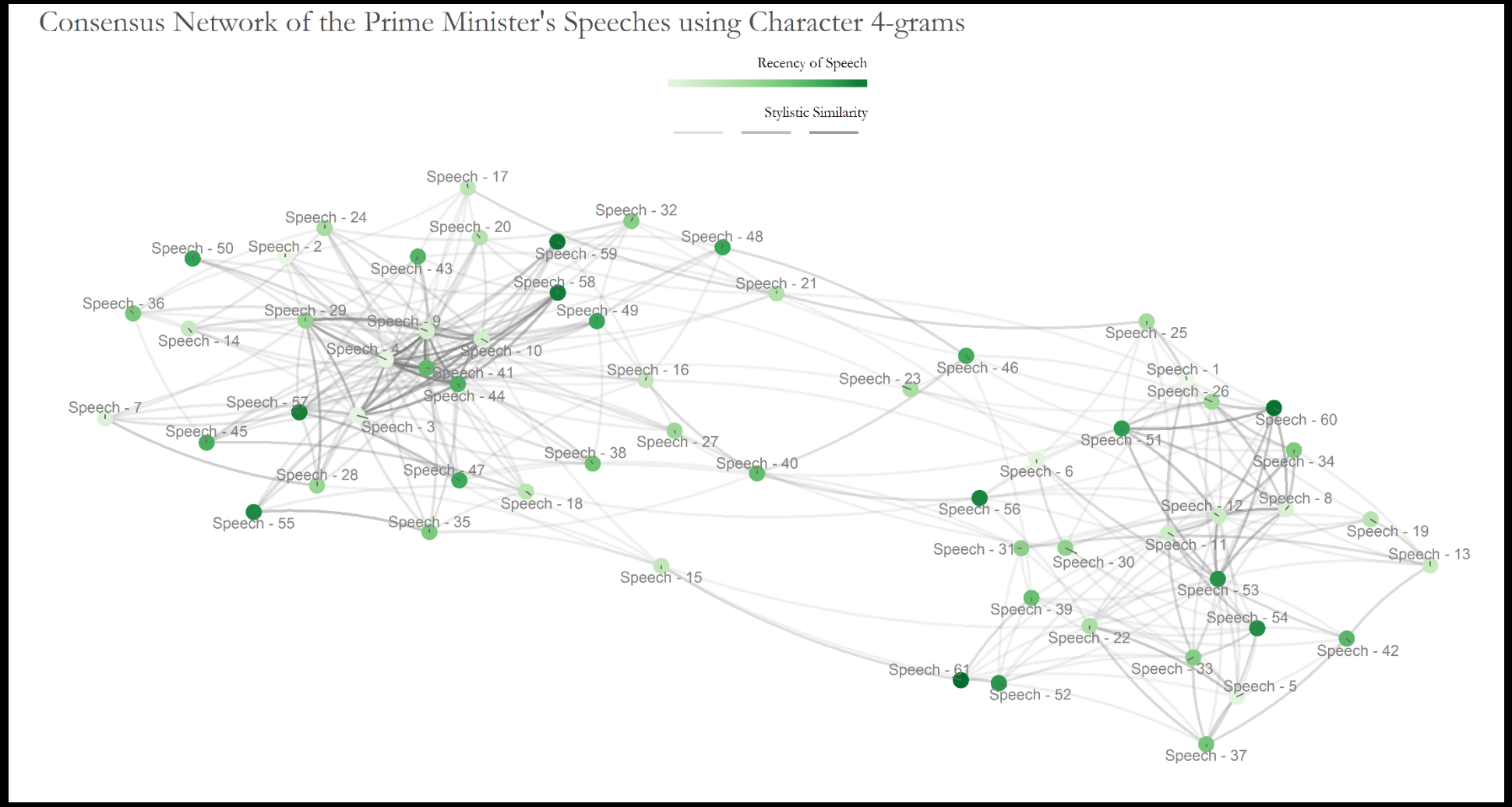
Kriminal Profilleme

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

Kriminal Profilleme

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

Adli Dilbilimi - Stilometri



Adli Dilbilimi - Stilometri

- Fidye notları

Adli Dilbilimi - Stilometri

- Fidye notları
- Clearnet platformlar – kimlik biliniyor

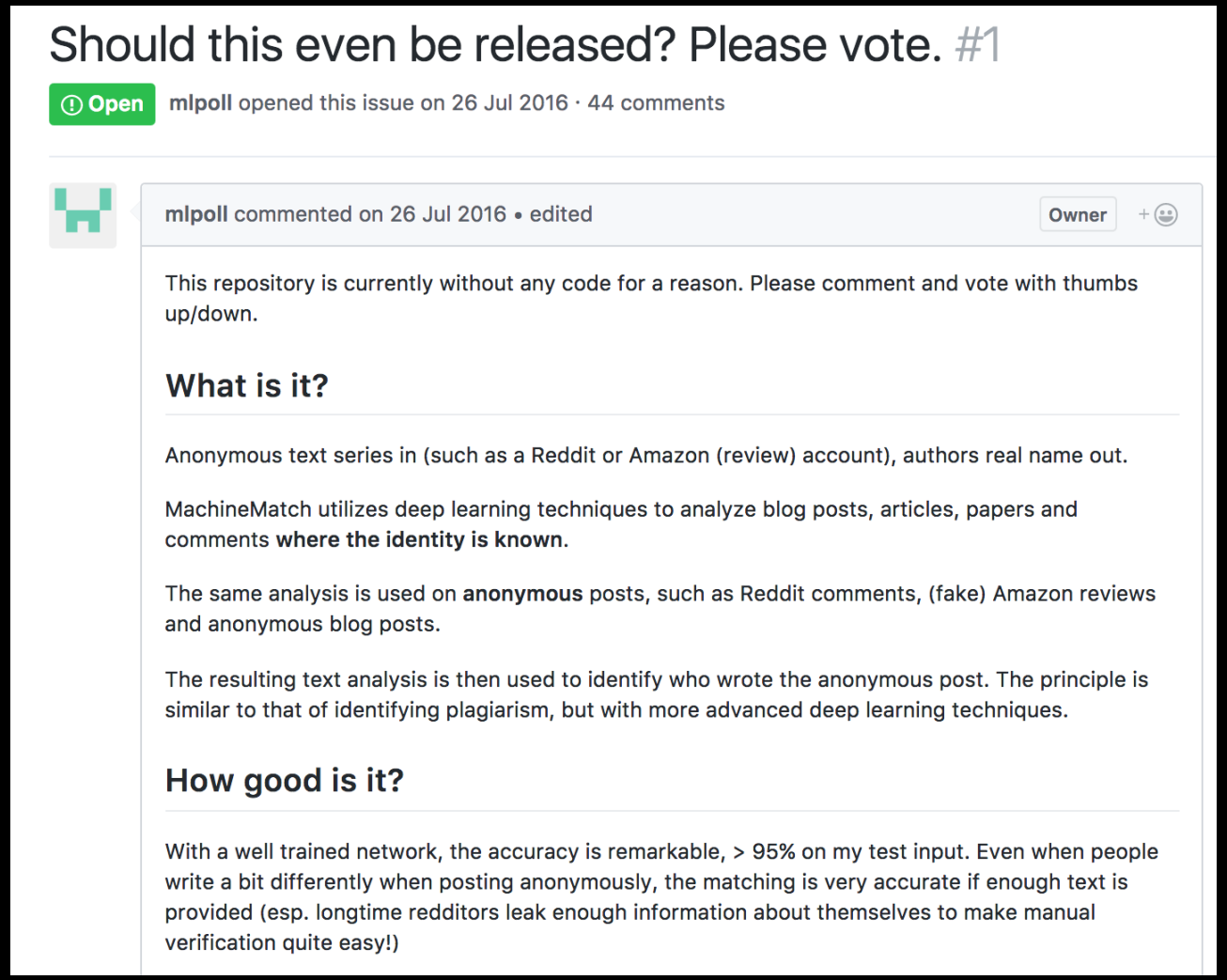
Adli Dilbilimi - Stilometri

- 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 Dilbilimi - Stilometri



Should this even be released? Please vote. #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**.

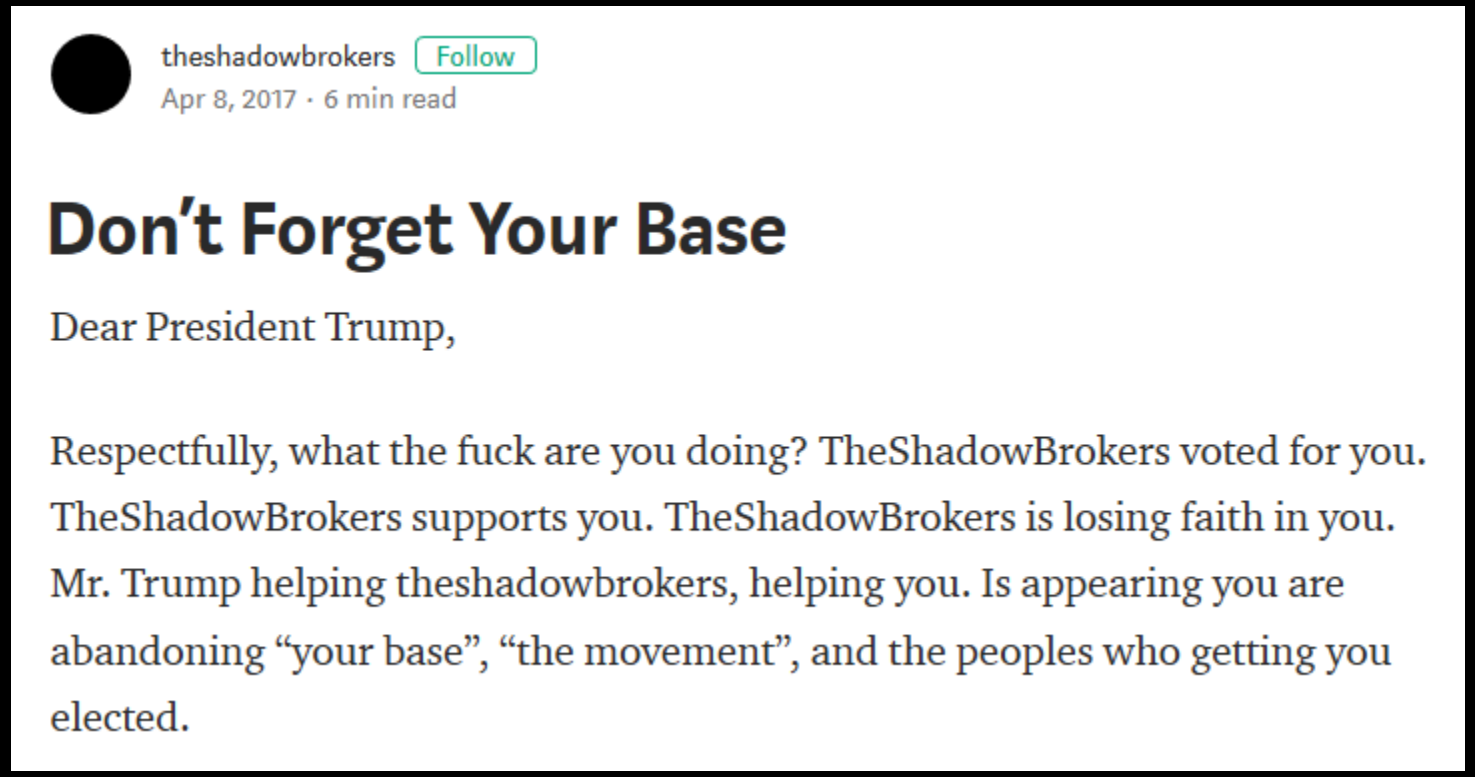
The same analysis is used on **anonymous** posts, such as Reddit comments, (fake) Amazon reviews and anonymous blog posts.

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 Dilbilimi - 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

Uluslararası İlişkiler

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?