Troll Avı

written by Mert SARICA | 1 March 2024
If you are looking for an English version of this article, please visit here.

İÇİNDEKİLER

Başlangıç

Siber tehdit istihbaratının öneminin gün be gün arttığı son yıllarda, kurumlarda bunun için kullanılan ürünlerin, hizmetlerin sayısının da katlanarak arttığını görüyoruz. Öncelikle siber tehdit istihbaratı kurumlara, bulundukları sektörü hedef alan tehdit aktörlerini tanımaları, kullandıkları taktikleri, teknikleri ve prosedürleri öğrenerek kurumlarına karşı gerçekleşebilecek olası siber saldırılara karşı hazırlıklı olmaları adına önemli bir avantaj sağlıyor. Diğer yandan siber saldırıya maruz kaldıklarında ise Siber Olay Müdahale (Incident Response) sürecinde elde edilen verilerin zenginleştirilmesinden tehdit aktörü ile olan bağlantısına kadar olayın aydınlatılmasına ışık tutabiliyor.

Kurumlar kadar teknoloji ile iç içe yaşayan son kullanıcıların, bireylerin yani bizlerin de siber tehdit istihbaratından, platformlarından kimi durumlarda (Misal Troll hesap araştırması) büyük fayda sağlayabileceğimizi unutmamamız gerekiyor.

Troll, Trolleme ve Dezenformasyon Nedir?

Tüm dünyada olduğu gibi ülkemizde de Troll hesaplar tarafından paylaşılan mesajların (Trolleme) sosyal ağlarda, medyalarda mantar gibi türediğine ve kitleleri dezenformasyon yönteminden faydalanarak manipüle etmeye çalıştığına tanıklık ediyoruz. Bazen bu yalan bilgiler kişilerin kendi hesaplarından paylaşıldığı gibi sahte, anonim hesaplar üzerinden de paylaşılabiliyor.

Troll İngilizce’de olta, olta yemi, oltayla balık tutmak anlamına gelen bir kelimedir. Trolleme ise geniş bir kitleyi manipüle etmek için yalan bilgi, asılsız fikir veya yazı yaymak anlamına gelmektedir. (Kaynak: Türk Toplumunda Sosyal Medyaya Eleştirel Bakış Eksikliği: Türk Troller ve Trolleme)

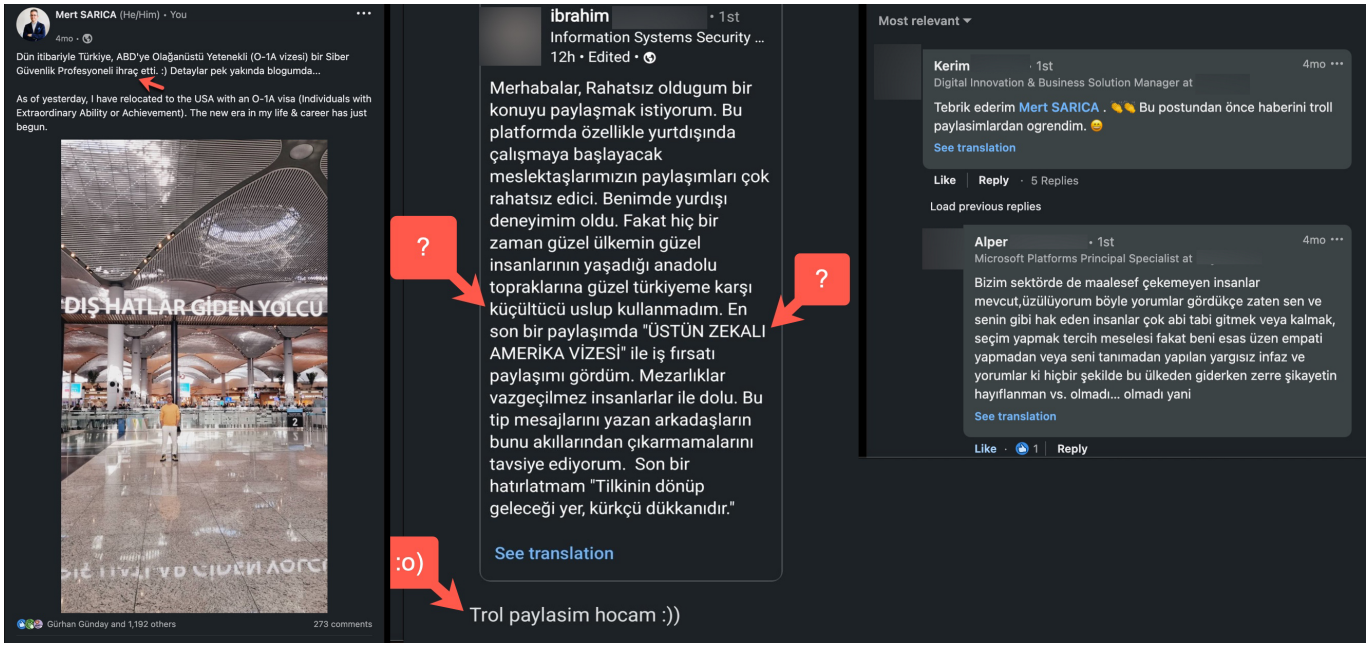
Dezenformasyon, yanlış veya doğruluğu bulunmayan ve kasıtlı olarak yayılan bilgi; bilgi çarpıtma anlamına gelir. Hasmı rencide etmeyi, aşağılayıp küçük düşürmeyi amaçlayan karşı propaganda ile benzerlik taşır. Sahte belge, el yazısı, fotomontaj ve montaj filmler ile fabrikasyon istihbarat ve dedikoduların duyurulması gibi yöntemleri bulunur. Sosyal alanda bireyleri ve toplumları yönlendirmek amacıyla, yanlış bilgi ve haber vermek için kullanılan en önemli araçlardan biridir. Yanlış bilgi üretme ve yayma yoluyla yapılabileceği gibi mevcut bir bilgiyi kötü maksatla kullanma ve çarpıtarak verme yöntemi de uygulanabilir. (Kaynak: Wikipedia)

1. 2009 yılından bu zamana dek gerçekleştirmiş olduğum 200‘den fazla siber güvenlik araştırmamı TÜRKÇE olarak blogumda “Bilgi güçtür ve paylaşıldıkça artar!” mottosu ile karşılıksız paylaşmış,
2. 2015 yılından beri düzenlediğim Pi Hediyem Var oyunu ile üniversite öğrencilerine sponsorlarımın desteği ile 15‘ten fazla Raspberry Pi hediye etmiş,
3. 30‘a yakın siber güvenlik etkinliğinde konuşmacı olmuş,
4. Sızma Testi Uzmanlığı / Etik Hacker ve Kariyer başlıklı sunumum ile 40’a yakın üniversitede siber güvenlik alanına meraklı binlerce öğrenciye yol göstermiş,

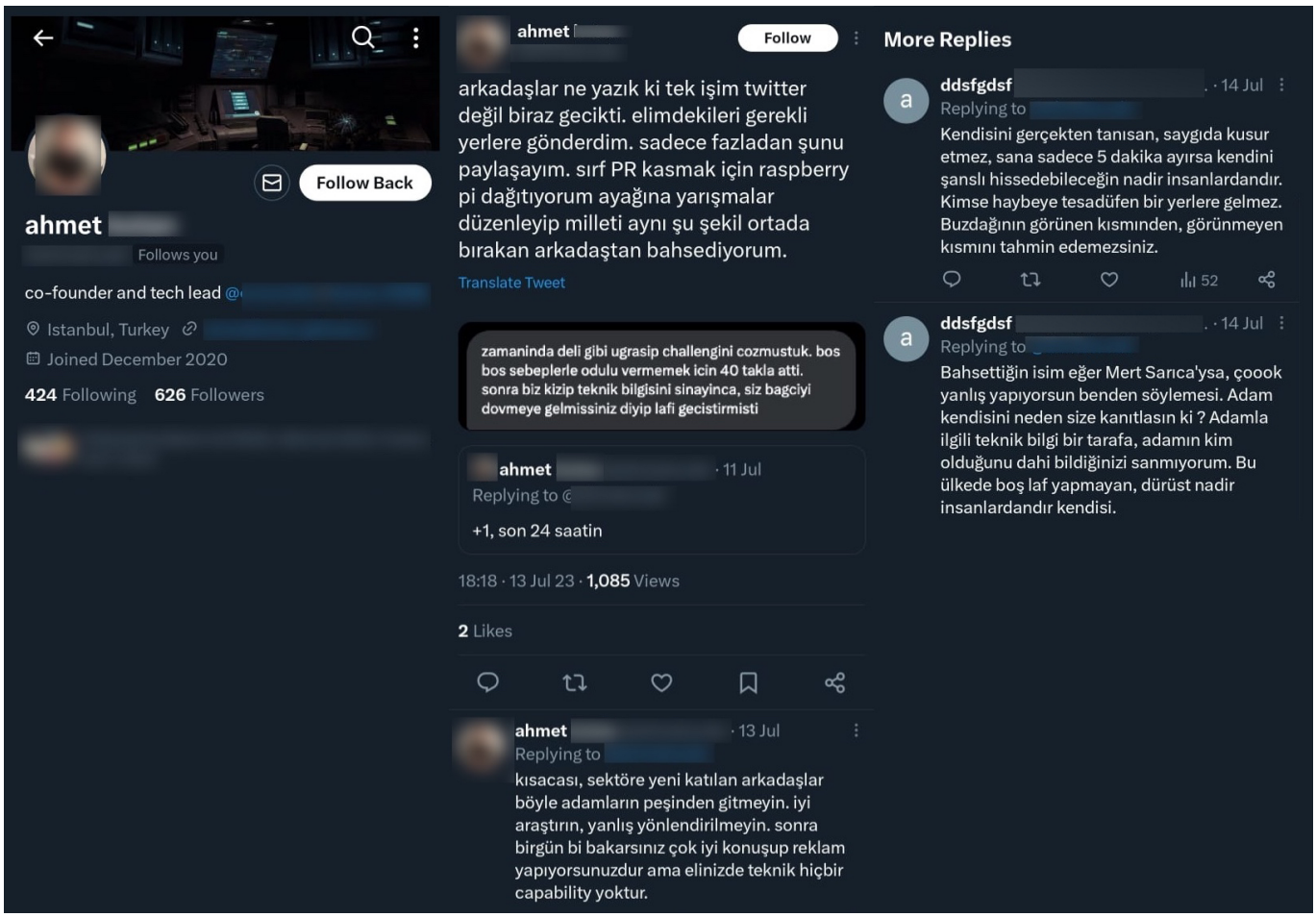
bir siber güvenlik profesyoneli olsam da, nadir de olsa ben de Troll hesapların hedefi haline gelebiliyorum.

Troll ve Trolleme Örnekleri

Çoğu zaman daha ne olduğunu anlayamadan, iyi niyetimden en ufak şüphesi olmayan sevgili takipçilerimin tepkileri, eleştirileri sayesinde Troll hesaplar çoktan ya kapanmış ya mesajlarını silmiş ya da cevaplarını almış oluyorlar. Bu gibi durumlarda siber tehdit istihbaratından, platformlarından faydalanmama pek gerek kalmıyor. Aksi durumlarda ise WhatsApp Dolandırıcıları, Kripto Para Dolandırıcıları başlıklı blog yazılarımda olduğu gibi siber tehdit istihbaratından, platformlarından bireysel olarak oldukça faydalanıyorum.



Mesaj Silinmiş



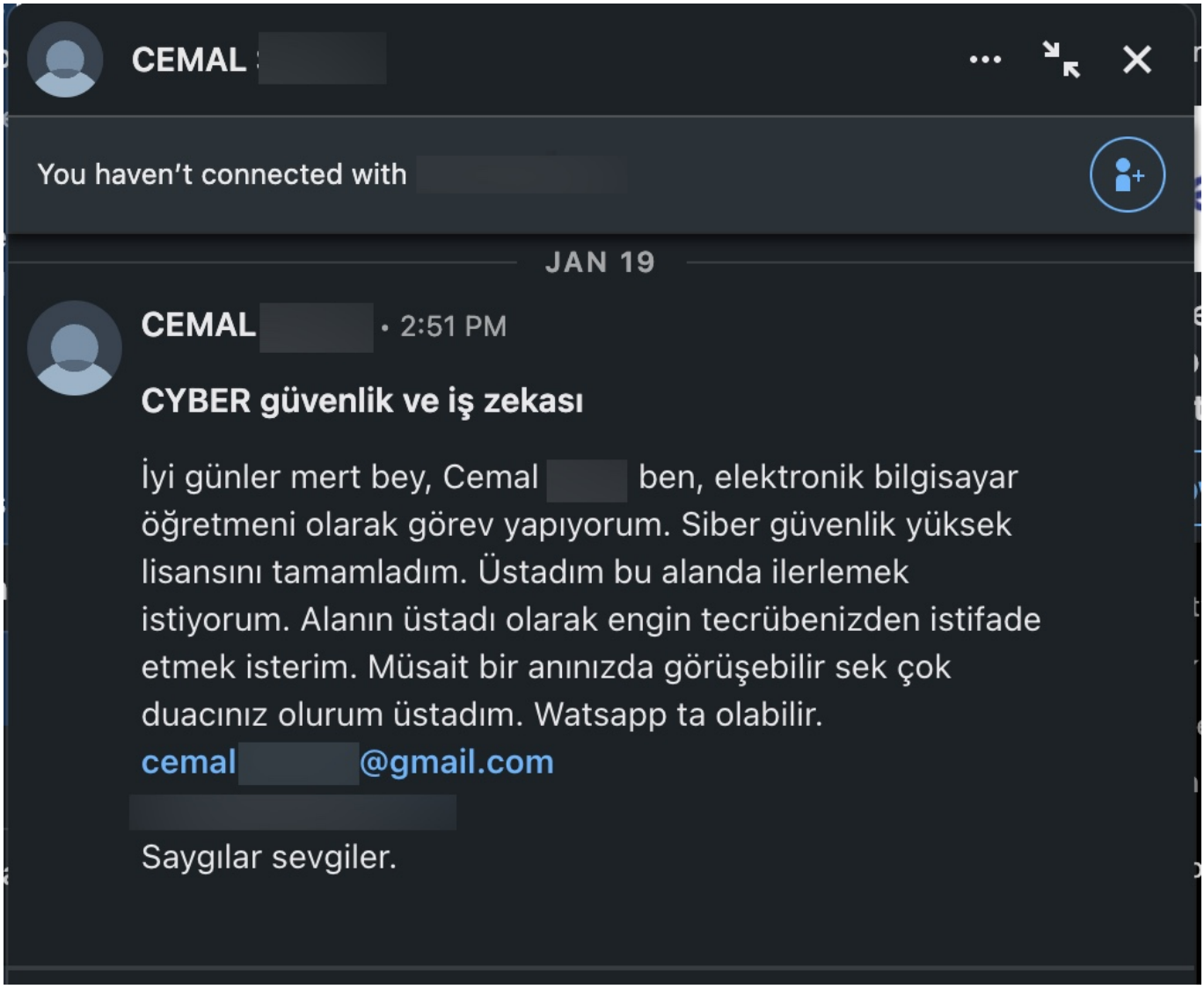
Mesaj Silinmiş

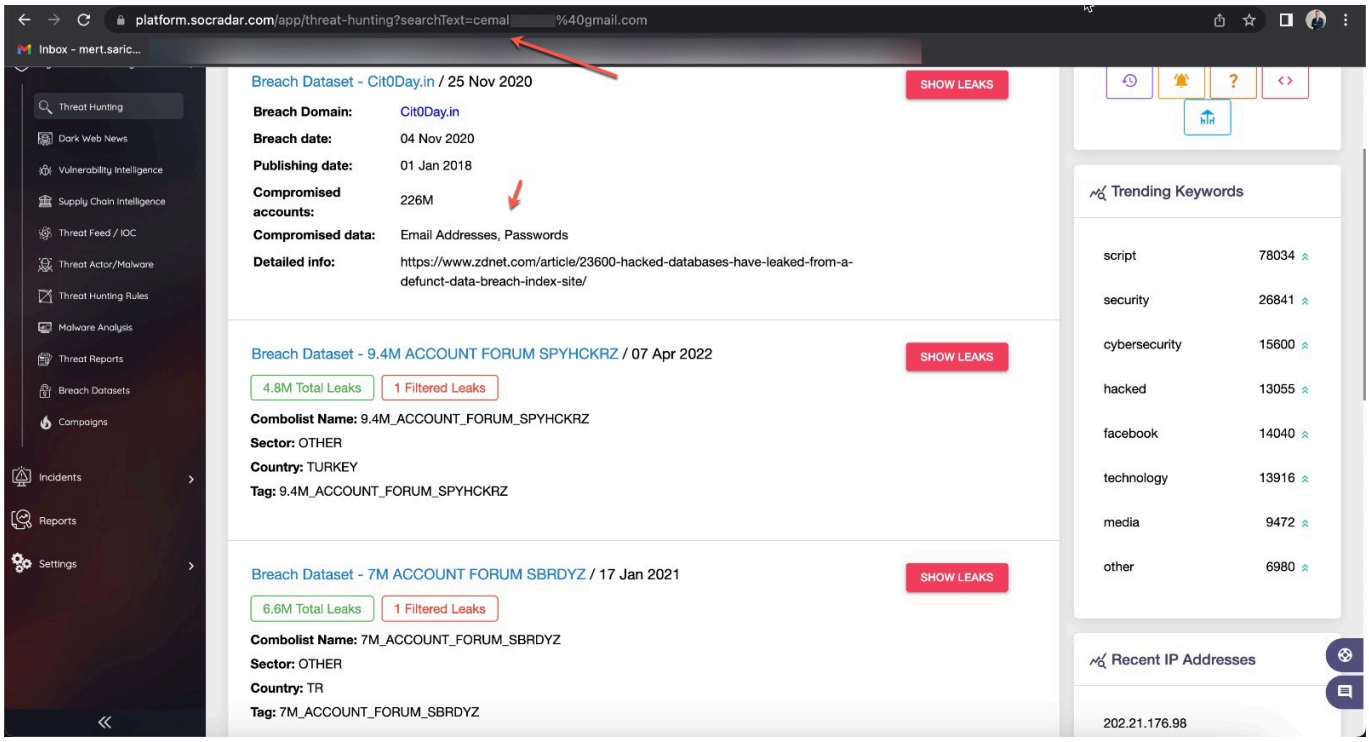
Özellikle sosyal mecralarda bir kişiye direkt veya dolaylı yoldan hakaret ettiğinizde, küfür ettiğinizde, itibar suikastı yaptığınızda, iftira attığınızda, tehdit ettiğinizde, vatanseverliğine dil uzattığınızda, er ya da geç bunun karşınıza çıkacağını, bir nedenden pişman olup mesajınızı silseniz

de, kayıtlardan ve hafızalardan kolay kolay silinmeyeceğini unutmamanız gerekiyor.

Bazı zamanlarda e-posta, sosyal medya veya ağ üzerinden aldığınız şüpheli bir mesajın arkasındaki kişinin niyetini, kim olduğunu anlamak amacıyla da siber tehdit istihbaratı platformlarından faydalanabiliyorsunuz.

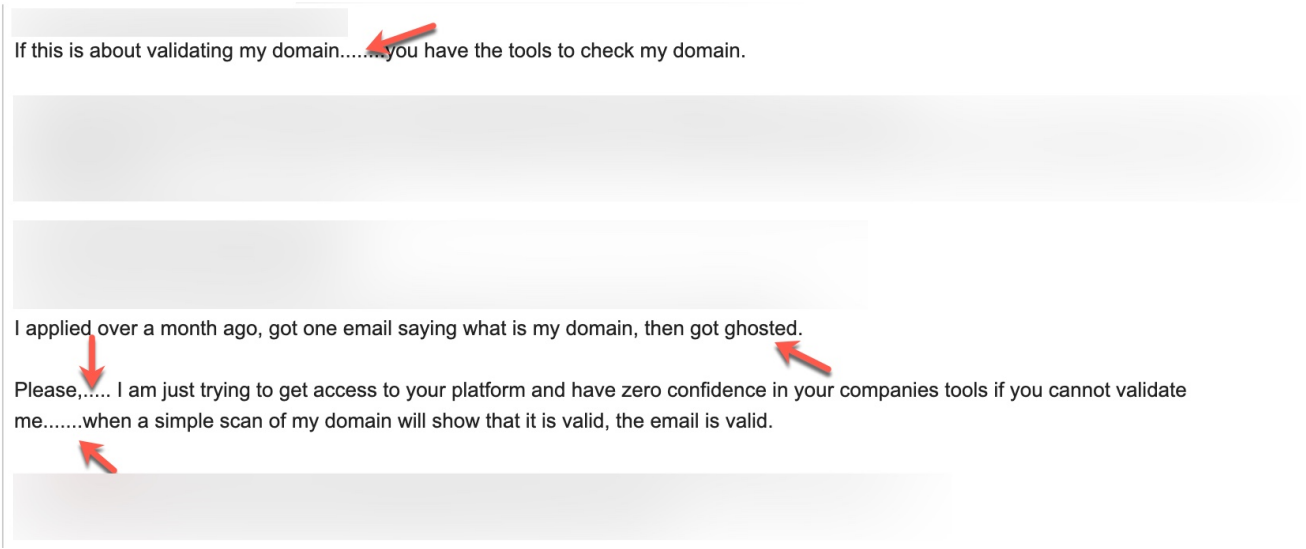
Bu örnekte bir Troll'ün web sitem üzerinden önce hakaret ettiğini, muhattap alınmadıktan 1 ay sonra ise bu defa farklı bir yaklaşımla sosyal ağ üzerinden iletişime geçmeye çalıştığını görüyorsunuz. E-posta adresini SOCRadar Siber Tehdit İstihbaratı Platformu'nda arattığınızda şahsın yıllardır hacker forumlarında gezindiğini öğrenerek niyeti ve motivasyonu hakkında kolaylıkla bilgi ve fikir sahibi olabiliyorsunuz.

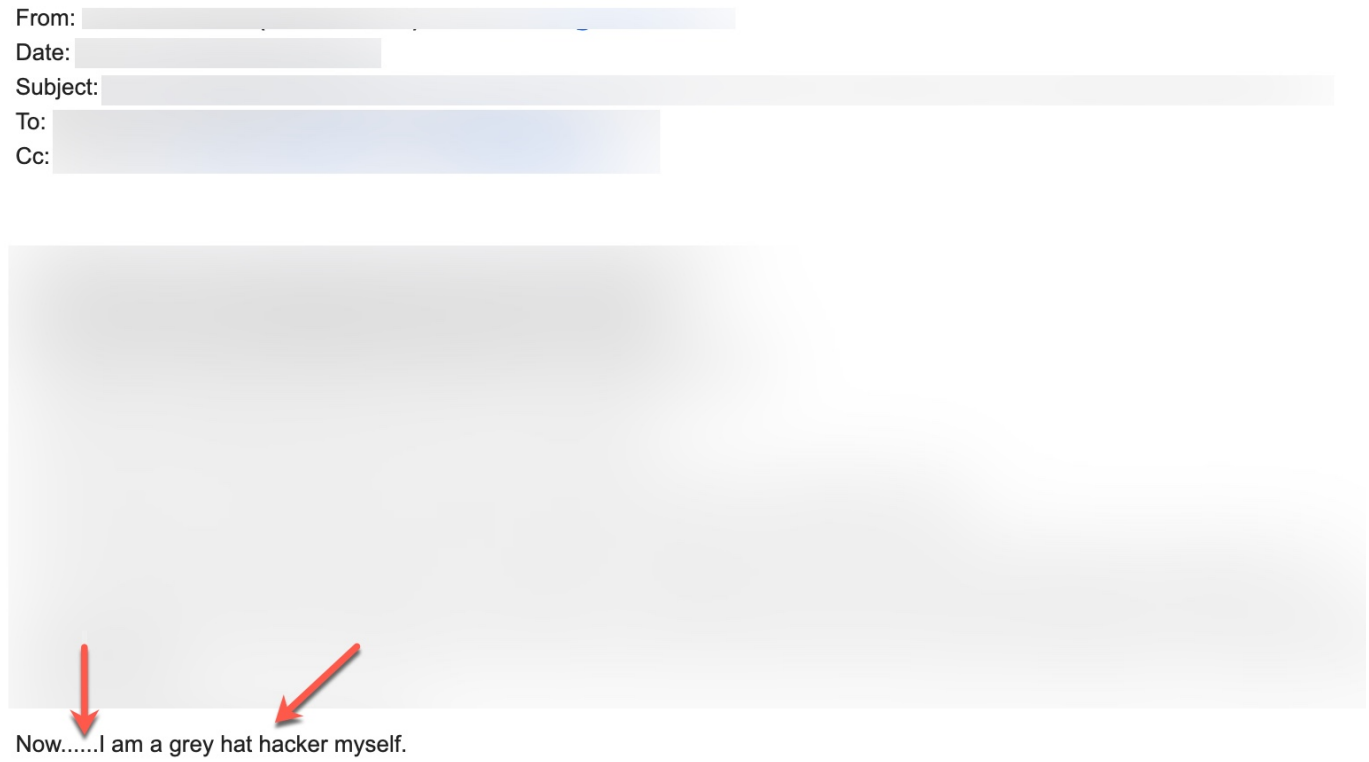

CEMAL
You haven't connected with
JAN 19
CEMAL • 2:51 PM
CYBER güvenlik ve iş zekası
İyi günler mert bey, Cemal ben, elektronik bilgisayar öğretmeni olarak görev yapıyorum. Siber güvenlik yüksek lisansını tamamladım. Üstadım bu alanda ilerlemek istiyorum. Alanın üstadı olarak engin tecrübenizden istifade etmek isterim. Müsait bir anınızda görüşebilir sek çok duacınız olurum üstadım. Watsapp ta olabilir.
cemal @gmail.com
Saygılar sevgiler.

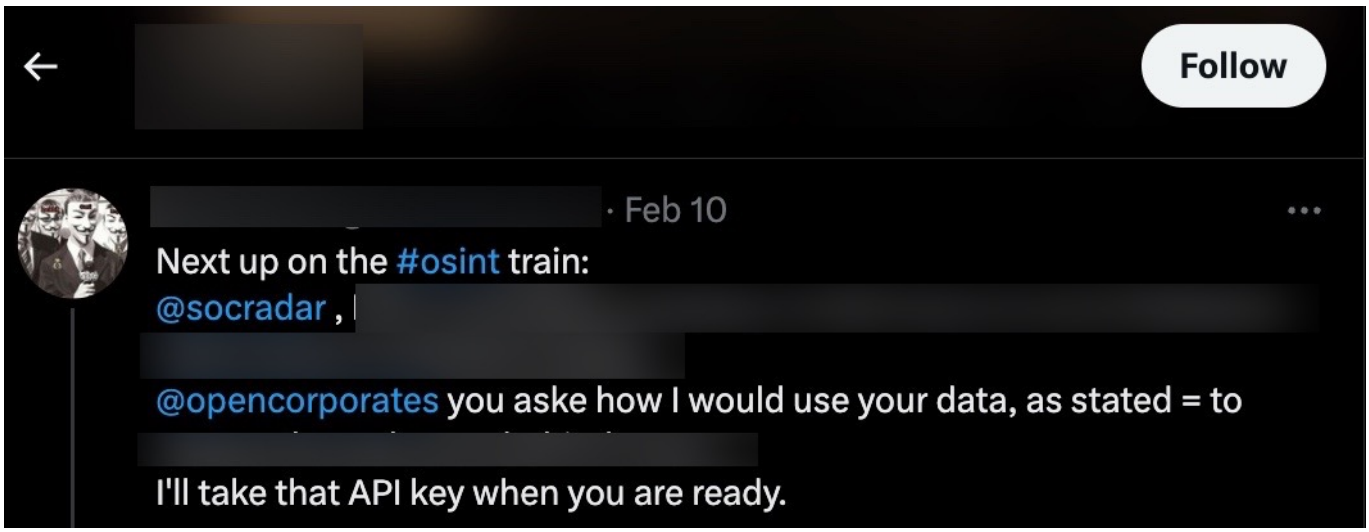

platform.socradar.com/app/threat-hunting?searchText=cemal%40gmail.com
Inbox - mert.saric...
Threat Hunting
Dark Web News
Vulnerability Intelligence
Supply Chain Intelligence
Threat Feed / IOC
Threat Actor/Malware
Threat Hunting Rules
Malware Analysis
Threat Reports
Breach Datasets
Campaigns
Incidents
Reports
Settings
Breach Dataset - Cit0Day.in / 25 Nov 2020
SHOW LEAKS
Breach Domain: Cit0Day.in
Breach date: 04 Nov 2020
Publishing date: 01 Jan 2018
Compromised accounts: 226M
Compromised data: Email Addresses, Passwords
Detailed info: https://www.zdnet.com/article/23600-hacked-databases-have-leaked-from-a-defunct-data-breach-index-site/
Breach Dataset - 9.4M ACCOUNT FORUM SPYHCKRZ / 07 Apr 2022
SHOW LEAKS
4.8M Total Leaks
1 Filtered Leaks
Combolist Name: 9.4M_ACCOUNT_FORUM_SPYHCKRZ
Sector: OTHER
Country: TURKEY
Tag: 9.4M_ACCOUNT_FORUM_SPYHCKRZ
Breach Dataset - 7M ACCOUNT FORUM SBRDYZ / 17 Jan 2021
SHOW LEAKS
6.6M Total Leaks
1 Filtered Leaks
Combolist Name: 7M_ACCOUNT_FORUM_SBRDYZ
Sector: OTHER
Country: TR
Tag: 7M_ACCOUNT_FORUM_SBRDYZ
Trending Keywords
script 78034
security 26841
cybersecurity 15600
hacked 13055
facebook 14040
technology 13916
media 9472
other 6980
Recent IP Addresses
202.21.176.98

Özellikle tehdit aktörlerinin, siber suçluların, dolandıcıların izini süren, operasyonlarını ortaya çıkaran ve bununla ilgili istihbarat paylaşan bir siber tehdit istihbaratı firmasında çalışıyorsanız kimi zaman sosyal medyada anonim hesaplar üzerinden kurumunuzu hedef alan tehditvari mesajlarla da karşılaşabiliyorsunuz. Bu gibi durumlarda da kendi platformunuzdan faydalanabildiğiniz gibi daha farklı yöntemler de izleyebiliyorsunuz.

Bu örnekte güvenlik kontrolünden geçemediği için siber tehdit istihbaratı platformuna kayıt olmasına izin verilmeyen bir şahsın önce tehditvari e-posta gönderdiğini akabinde ise Twitter'da anonim bir hesap üzerinden trolleme yapmaya başladığını görüyorsunuz.







Hesap Silinmiş

Peki gerçek kimliği ile e-posta gönderen bir kişi ile Guy Fawkes maskesi ardına gizlenen anonim bir Twitter hesabı üzerinden mesaj paylaşan bir kişinin yüksek olasılıkla aynı kişi olduğunu nasıl kanaat getirebiliriz?

Elimizde şüphelendiğimiz kişiye ait örnek e-postalar ve anonim Twitter hesabından paylaşılan mesajlar olduğu için bunlar üzerinde yazarı tespit etmeye yönelik stilometrik yöntemlerden (Noktalama, yazım yanlışları, vurgu,

yabancı sözcük, argo ve jargon, bağlaç, kısaltmalar, sayılar, konu etiketleri, şekil ve işaretler) faydalanabiliyoruz.

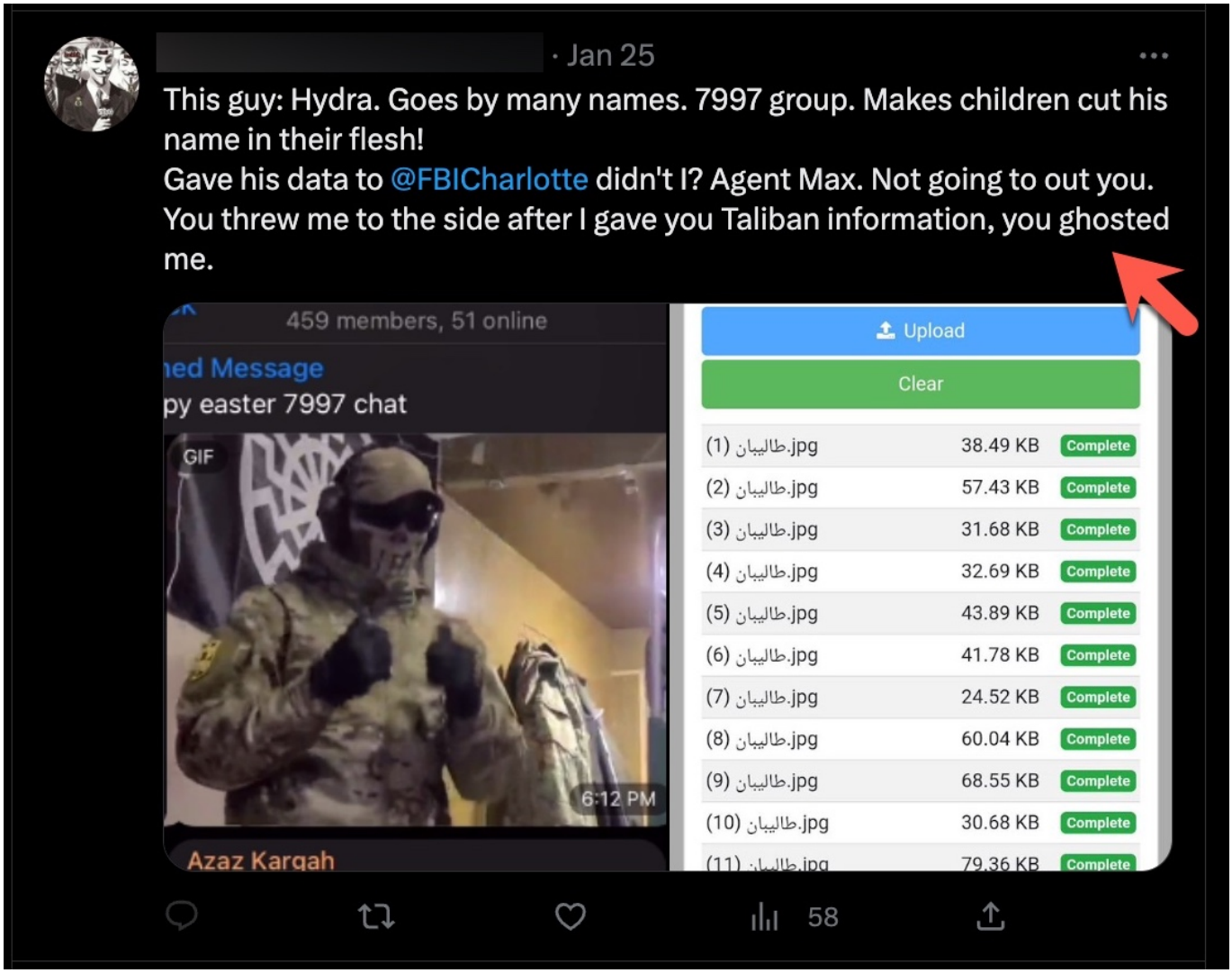
Stilometri Nedir?

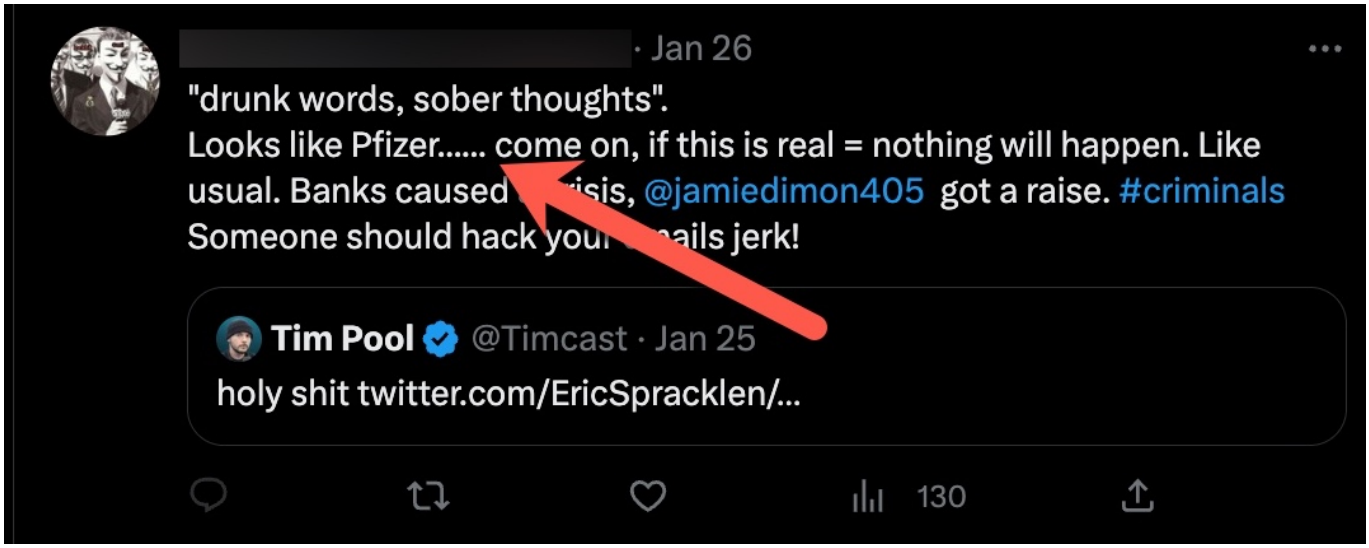
Stilometri, öncelikle yazılı edebiyat alanında olmak üzere, resim ve müzik gibi sanat dallarında, tarih, din ve hukuk alanında ve adli bilimlerde kullanılan bir üslup belirleme çalışmasıdır. Stilometri analizi ise, üslup belirteçlerinin (syle markers) değişken olarak alınıp bu değişkenlerin istatistiksel ve bilişimsel metotlar incelenmesine dayanan bir yöntemdir.

Stilometri, yaklaşık iki yüz yıldır yazarların edebi üslubunun karşılaştırılması ve özellikle eser sahipliği (authorship attribution) problemlerinde çeşitli istatistiksel metotlar kullanılarak uygulanmıştır. Kullanılan metotlar, temel istatistiksel hesaplamalardan ve testlerden yapay sinir ağlarına kadar geniş bir aralıkta yer almaktadır. Dini metinlerden tarihi metinlere, bilimsel çalışmalardaki intihalden edebi eserlerin ve yazarların üslubunun incelenmesine kadar pek çok konuda stilometrik çalışma yapılmıştır. (Kaynak: İstatistik’ten Edebiyat’a Bir Köprü: Stilometri Analizi – Ayşe İŞİ, Fatih ÇEMREK, Zeki YILDIZ)

Troll Avı

Bu aşamada geniş kapsamlı bir Stilometri analizi yapmak yerine anonim Twitter hesabındaki 109 tane mesaja kabaca göz atıp, e-postalarla örtüşen ortak kelimelere, noktalama işaretlerine odaklanmaya karar verdim. Aldığım notlar doğrultusunda dikkatimi çeken mesajlarında bol bol ….. noktalama işaretine yer vermesi ve İngilizce yazışmalarda pek sık rastlamadığım ghosted kelimesi oldu. Bunlara yönelik olarak şüphelendiğim kişiden gelen e-postalara baktığımda tespitlerim ile fazlasıyla örtüştüğünü görerek iki kişi arasındaki benzerlik olasılığını fazlasıyla arttırmış oldum.





Peki bu anonim Twitter hesabından paylaşılan mesaj sayısı 109 değil de 10009 olsaydı o zaman ne yapardım diye düşünmeye başladığımda veri bilimin yardımına başvurmaya karar verdim.

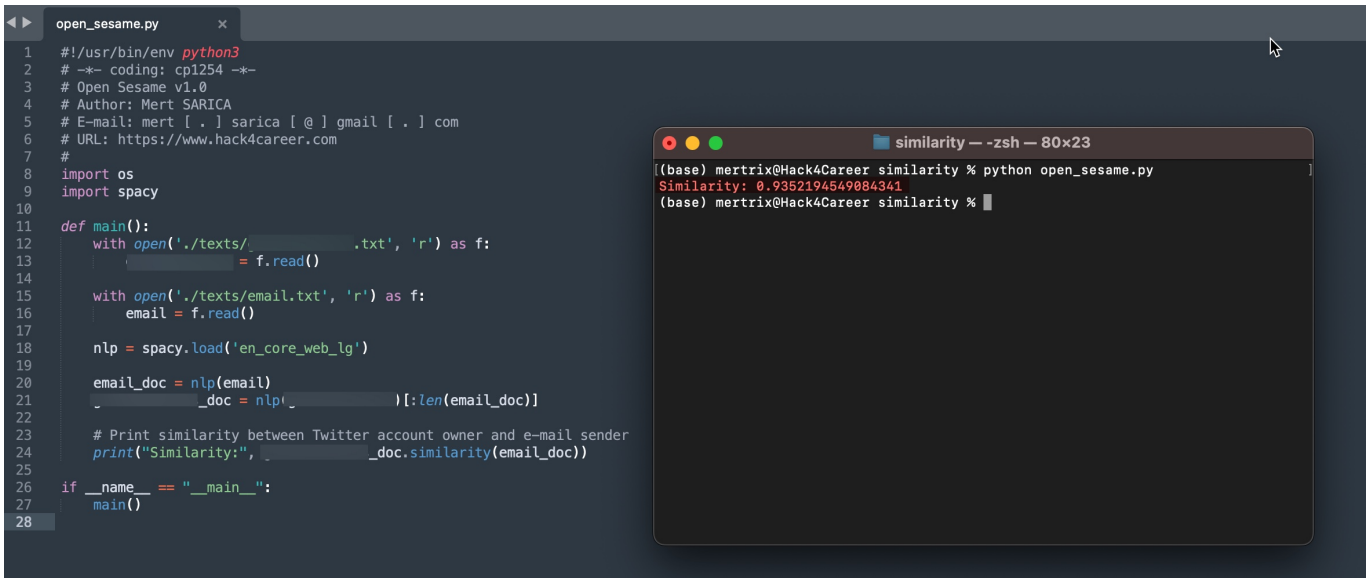
Veri bilimi, iş için anlamlı öngörüler ayıklamak amacıyla veriler üzerinde

gerçekleştirilen çalışmaların adıdır. Büyük miktardaki verileri analiz etmek için matematik, istatistik, yapay zeka ve bilgisayar mühendisliği alanlarının ilke ve uygulamalarını bir araya getiren, disiplinler arası bir yaklaşımdır. Bu analiz, veri bilimcilerinin ne olduğu, neden olduğu, ne olacağı ve sonuçlarla neler yapılabileceğini sormalarına ve bu soruları cevaplamalarına yardımcı olur.

Biraz araştırma yaptıktan sonra SpaCy isimli Doğal Dil İşleme (NLP) kütüphanesinde metinler arasındaki benzerliği ölçmeye yarayan ve Kosinüs Benzerliği'ni kullanan similarity metodundan faydalanabileceğimi öğrendim.

Kosinüs Benzerliği, metinler arasındaki benzerliği vektörel olarak ölçmektedir. Metinlerde geçen kelimelerin metinde kaç kez geçtiği hesaplanır. Daha sonra her metin içerdiği kelimelerle 1 ve 0 şeklinde vektörel olarak ifade edilir. Her metin üç boyutlu uzayda vektörel olarak yerleştirildiğinde aralarındaki kosinüs açısı ne kadar küçük ise metinler birbirlerine o kadar yakındır. Tamamen birbiri ile ilişkisiz olan vektörler için ise kosinüs değeri 0 olurken tamamen birbirini zıddı olan dokümanlar için kosinüs değeri -1 olacaktır. (Kaynak: Netflix verileri üzerinde TF-IDF algoritması ve Kosinüs benzerliği ile bir İçerik Öneri Sistemi Uygulaması – Özlem GELEMET Hakan AYDIN Ali ÇETİNKAYA)

Python ile ufak bir kod yazıp şüphelendiğim kişiden gelen e-postalar ile Twitter mesajları arasındaki benzerliğe baktığımda SpaCy kütüphanesi sayesinde bunların çok yüksek ihtimalle aynı kişi tarafından gönderildiğine kanaat getirerek kendimi ikna etmiş ve mutlu sona ulaşmış oldum. :)



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Stilometrinin kullanımına yönelik daha fazla bilgi edinmek isteyenlerin Real-World Python: A Hacker’s Guide to Solving Problems with Code kitabının ücretsiz olarak sunulan bölümünü okumalarını tavsiye edebilirim.