Hocam merhaba,  
  
Sizinle yaptığımız son görüşmemizde belirlemiş olduğumuz kelimelerin (siber saldırı, ddos, hacklendi gibi) Türkçe tweetlerde kullanım sıklığı frekansını belli periyotlarda karşılaştırarak kelimelerin kullanım sıklığının artması ile siber güvenlik olayları arasında bir korelasyon olup olmayacağının araştırılması ile ilgili geliştirdiğim yazılımın demosunu yapmıştım.

Bu ve bu konuya benzer alanlarda daha önce yaptığım bibliyografi çalışmasını bu konu özelinde tekrar yapmamı, çalışma sonuçlarını sizinle paylaşmamı istemiştiniz.

Yapmış olduğum araştırma neticesinde ilgili olabilecek 22 adet yayını inceledim, aralarından 8 tanesinin çalışmalarımızla alakalı olabileceğini, araştırmamız sırasında kullanılabileceğini düşünüyorum. Bu yayınlar aşağıdaki gibi.

Araştırmalarla ilgili kişisel notlarımın daha ayrıntılı haline ekteki pdf dosyasından erişebilirsiniz (Tablolar ve ekran alıntıları eklenmiş hali)

Özellikle incelememi istediğiniz, bu çalışmanın Türkçe tweetler için olan versiyonunu yapabiliriz dediğiniz “Weakly Supervised Extraction of Computer Security Events from Twitter”

## Publications

1. [Weakly Supervised Extraction of Computer Security Events from Twitter] ( https://aritter.github.io/twitter\_security.pdf )

Twitter verilerini kullanarak sabit kategorilere bağımlı kalmadan kullanıcının istediği kategorileri ekleyebileceği ve çıktı olarak bu kategorilerdeki saldırılardan etkilenen kurbanları belirlenmesi üzerine bir çalışma.

Daha sonra bu eventlerden etkilenen mağdur kimse/kurum/programı bulmaya çalışıyorlar.

2. [Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example]( https://kar.kent.ac.uk/66861/7/SMSociety2018.pdf )

Yıldırım Beyazıt Üniversitesinden bir doktora öğrencisi ve bir Profesörün University of Kent Canterbury(UK) de çalışan bir profesörle yaptıkları bir çalışma. Machine learning teknikleri kullanarak Siber güvenlikle alakalı sosyal medya hesaplarının bulunup bulunamayacağını araştırmışlar. Twitterı da örnek sosyal medya hesabı olarak seçmişler.

3. [DDoS Event Forecasting using Twitter Data](https://www.ijcai.org/proceedings/2017/0580.pdf)

Twitter datalarını işleyerek henüz gerçekleşmemiş DDos saldırılarını tahmin etmeye yönelik bir yayın.

Bu bilgiyi 6 popüler “supervised classification model” kullanarak elde etmeye çalışmışlar. Örneğin kullandıkları modellerden biri negative term count.

“Neg-Term-count is the baseline sentiment-based model, we count the negative words from tweets each day, forecasting an attack if the number of negative words is larger than a threshold α, which is the average number of negative words on training data.”

4. [Real Time Prediction of Drive by Download Attacks on Twitter](https://arxiv.org/pdf/1708.05831.pdf)

url kısaltma ile zararlı web sitelerini normal bir web sitesi olarak gösterip twitter’da kısaltılmış url’i paylaşarak zararlı web sitelerinin tıklanmasını önlemeye yönelik ne yapabilirizi araştırmışlar. Honeypot ile cpu ram kullanımı artışından detect etme gibi yöntemler denemişler.

5. [SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream](https://www.researchgate.net/publication/319048233\_SONAR\_Automatic\_Detection\_of\_Cyber\_Security\_Events\_over\_the\_Twitter\_Stream)

Sonar adında otomatik olarak kendi kendine öğrenebilen bir framework geliştirmişler. Siber güvenlikle ilgili olayları twitter verilerini işleyerek yakalayabiliyor. Sisteme takip etmesi gereken bazı keywordleri veriyorlar, system siber güvenlikle ilgili olabilecek diğer keywordleri verdiğimiz keyworlerin yardımıyla bulabiliyor.

Araştırmalarını yapabilmek için birçok big data teknolojisinden de faydalanmışlar.

6. [Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation](https://link.springer.com/article/10.1007/s00500-016-2265-0)

Yayının full-text ine erişemedim. Research gate aracılığıyla erişim izni istedim. Preview den anladığım kadarıyla sosyal media streamlerini işleyerek siber güvenlikle ilgili saldırıları detect edip bu saldırılardan korunmak için otomatik olarak çözümler öneren bir system üzerine araştırma yapmışlar.

7. [Crowdsourcing Cybersecurity: Cyber Attack Detection using Social Media](http://people.cs.vt.edu/naren/papers/case1872-khandpurA.pdf)

Twitter verilerini işleyerek siber güvenlik saldırılarını detect etme üzerine bir çalışma daha. Daha önceki yapılan çalışmalara benzer bir çalışma olduğunu Kabul ediyorlar fakat daha başarılı sonuçlar elde ettiklerini iddia ediyorlar.

8. [Identifying offenders on Twitter: A law enforcement practitioner guide](https://www.researchgate.net/publication/320005848\_Identifying\_offenders\_on\_Twitter\_A\_law\_enforcement\_practitioner\_guide)

Twitter da saldırganları ve yasadışı içerik paylaşanlara karşı twitter streamlerini analiz ederek tespit edilmesine yönelik bir çalışma. Yayının full text ine erişim iznim henüz yok, researchgate üzerinden erişim izni talebinde bulundum.   
  
  
Saygılarımla,  
Özgür Ural