<table>
<thead>
<tr>
<th>Title</th>
<th>Open social data crime analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Ihsan, Ullah.; Lane, Caoilfhionn; Drury, Brett; Mellotte, Marc; Madden, Michael G.</td>
</tr>
<tr>
<td>Publication Date</td>
<td>2017-07-20</td>
</tr>
<tr>
<td>Publisher</td>
<td>IJCAI 17 Melbourne</td>
</tr>
<tr>
<td>Item record</td>
<td><a href="http://hdl.handle.net/10379/6830">http://hdl.handle.net/10379/6830</a></td>
</tr>
</tbody>
</table>

Some rights reserved. For more information, please see the item record link above.
Open Social Data Crime Analytics

Ihsan Ullah, Caoilfhionn Lane, Brett Drury, Marc Mellotte, and Michael G. Madden
Insight Centre for Data Analytics, National University of Ireland, Galway, Ireland
ihsan.ullah@insight-centre.org

Abstract
Crime is under-reported. Reporting crime requires the victim to complete a number of administrative obligations. These obligations, as well as the nature of the crime, may create an inertia that discourages the reporting of the crime (for example, being defrauded might damage a financial organisation’s reputation). However, there may be information leaks from compromised organizations, via affected customers on social media. A key advantage of using social data is that it is often immediate, and can have indications of the nature of a crime such as (1) named entities, for example, Bitcoin or PayPal; (2) geocoding information; and (3) the affected persons. Our aim in this work is to use social media platforms e.g. Twitter, Reddit, Facebook, etc. to detect signals of cybercrime incidents. Such signaling is arguably a better indicator of the extent and effect of cybercrime than traditional reporting methods.

1 Introduction
Computers and the Internet have become part of daily life for almost all people and organizations. The daily usage of smartphones, phenomena related to the internet of things, and a move to cashless societies etc. have increased the risk of cybercrime. The definition of cybercrime encompasses any crime committed with the help of computers or the Internet. However, the majority of these crimes are under-reported due to many reasons e.g. because of lack of knowledge or due to potential damage to reputation [Levi et al., 2017; Calnan and Denise, 2016].

According to the IBM X-Force threat intelligence index 2017, the five most targeted areas are financial institutions, information and communications, manufacturing, retail, and healthcare [Alvarez et al., 2017]. On 12th May 2017, ransomware WannaCry attack hit around 150 countries and affected about 200K computers [Karla and Adam, 2017]. In January 2015, Facebook & Google confirmed a phishing scam carried out between 2013 and 2015 in which both the companies lost US $100 m. The vendor management team were asked to transfer money based on fake documents. In December 2016, a CEO fraud was perpetrated on Meath County Council, Ireland, in which a cybercriminal impersonated the county council CEO and secured the transfer of €4.3m to an account in Hong Kong.

In a recent survey [Levi et al., 2017], three months of crime-related data, provided by Action Fraud UK (the national centre for reporting fraud and cybercrime) were analyzed. Out of 106,681 reported incidents, 4% of the incidents were related to cybercrime. The banking and credit industries face the highest number of fraud incidents [Levi et al., 2017; Alvarez et al., 2017].

Table 1 shows our analysis of attacks on financial institutions since 2014. When the end customer is affected directly, information may leaks. For example, we reviewed tweets about recent compromise of Tesco Bank. Tesco customers started to complain on Twitter from the 31st July 2016 whereas Tesco only instructed their customers to take extra security precautions on 6th November 2016 (Newspapers reported the breach on 8th November 2016). There are indications that financial institutions do not always report due to potential concerns over reputational damage e.g. SWIFT fraud in Ecuadorian Banco del Austro [Spier, 2016].

2 Indicators of Cybercrime on Social Media and Web Forums
There are a number of sources of social media, social news, and web forums such as Twitter, Facebook, Instagram, Google+, Reddit, IRC, devRant, etc. that potentially contain indicators of cybercrime. One of the most frequently quoted sources in the literature is Twitter (users tweet around 500 million times per day). A number of studies have examined the role of Twitter in relation to criminal acts. The best channels to reach the public during a health crisis are Twitter, Facebook, and Instagram. It is also a good platform for collecting and analyzing data [Burnap and Williams, 2016]. Using Twitter to detect criminal acts is a recent area of study. Tweets have been used to detect both offline and online criminal acts, for example, to predict hit-and-run crimes from traffic alerts[Wang et al., 2012], detect cyber hate [Burnap and Williams, 2016], and to study online rumors in terms of offline harm [Webb et al., 2015]. Social media is also used in research for health surveillance. The research on detection and analysis of phishing, spam, rumour, riot, etc. may be applicable in the detection of cybercrime.
3 Methodologies, Data Sources, Tools, and Supplementary Material

A number of methodologies from other domains can be adopted to detect cybercrime in open social data e.g. Text classification, Spam classification, Rumour/Riot modeling, Pandemic disease detection, Event detection/alignment.

Data Sources: We have identified over 30 general cybercrime related open datasets. The majority of them are related to networks e.g. intrusion detection. The second most common type of dataset was related to reviews for spam detection or opinion fraud. Only four of them were related to social media i.e. Twitter. Currently, there is no suitable dataset available that can be used for our specific objectives.

Tools: Although there is no known dataset that can be directly used for this project, there are tools with the help of which we can collect the required data. e.g. Twitter, Reddit, In-House Insight API, IBM X-Force Exchange. As a starting point, we can take hints from previously committed crimes, search data related to that. And then use it for financial institutions in a single jurisdiction.

Supplementary Material: In addition to social media data, digital currency data may also be a helpful tool in detecting suspicious activities. e.g. in recent ransomware attack, the ransom typically must be paid in Bitcoins, so an increase in Bitcoin purchases relative to the usual baseline number of transactions in a specific jurisdiction should provide an indicator of how many individuals paid the ransom to ransomware attack.

4 Conclusion

Open social data can be helpful in detecting cybercrime in financial institutions. Analyzing digital currency stock may supplement open social data. Existing methodologies for studying riots and rumours, sentiment analysis, or the analysis of pandemic disease etc. can be adopted. Currently, there is no suitable dataset available, but a number of suitable APIs may be used to collect relevant data. There is also the possibility of using a combination of two or more platforms to confirm a cyberattack e.g. any tweet on Twitter asking/discussing a compromised account of a specific bank and any discussion in the same time period on a blog or forum e.g. on Reddit.

Acknowledgment

This project is funded by IBM and Science Foundation Ireland (SFI) under Grant Number SFI/12/RC/2289.

References


