

Exploring Hackers Assets: Topics of Interest as Indicators of Compromise

Mohammad Al-Ramahi
Computing and Cybersecurity
Texas A&M, San Antonio
San Antonio, TX, USA
mrahman1@tamusa.edu

Izzat Alsmadi
Computing and Cybersecurity
Texas A&M, San Antonio
San Antonio, TX, USA
izzat.alsmadi@tamusa.edu

Joshua Davenport
Computing and Cybersecurity
Texas A&M, San Antonio
San Antonio, TX, USA
jdavenport@protonmail.com

ABSTRACT

The need to develop actionable intelligence that is proactive is very critical to current security controls and systems. Hackers and hacking techniques continue to grow and become more sophisticated. As such Security teams start to adopt proactive and offensive approaches within hackers' territories. In this scope, we proposed a systematic approach to automatically extract "topics of interest, ToI" from hackers' websites. Those can eventually be used as inputs to actionable security controls or Indicators of Compromise (IOS) collectors. As a showcase, we selected the hackers' news website "CrackingFire". ToI can be integrated into Indicators of Compromise (IoC) and once correlated with other signs of attacks from those IoC will trigger further cybersecurity offense or defense actions. We also developed our own dark web crawler and evaluate extracting ToIs. We observed the types of challenges in both the crawling and the processing stages.

KEYWORDS

Online Social Networks, Security and privacy, Human and societal aspects of security and privacy

ACM Reference format:

Mohammad Al-Ramahi, Izzat Alsmadi, and Joshua Davenport. 2020. Exploring Hackers Assets: Topics of Interest as Indicators of Compromise. In *Hot Topics in the Science of Security Symposium (HotSoS)*, April 7-8, 2020, Lawrence, KS, USA, ACM, New York, NY, USA, 4 pages. <https://doi.org/10.1145/3384217.3385619>

1 Introduction

With the evolution of the Internet, protection of data should be one of the main priorities for each business. Traditional security mechanisms are able to detect and prevent malicious behaviors, but cannot keep up with the speed and sophistication of cyber criminal

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

HotSoS '20, April 7–8, 2020, Lawrence, KS, USA

© 2020 Association for Computing Machinery.

ACM ISBN 978-1-4503-7561-0/20/04...\$15.00

<https://doi.org/10.1145/3384217.3385619>

tools and tactics. Cyber criminals, also known as hackers, are devoting additional time and resources to prepare more advanced and sophisticated attacks, which conventional security safeguards such as firewalls and malware and intrusion detection and prevention systems often cannot detect and prevent.

Hackers continuously change their tools and methods to surprise defense mechanisms. Their task is easier than the defense team as all what it takes hackers is to discover one vulnerability to eventually exploit and launch their attack or malware. Therefore, more proactive approaches are needed to increase the effectiveness of cyber security systems. One such approach that has recently gained security community attention is called Cyber intelligence. An increasing body of research has started to discover the social dynamics among the hackers [1].

Cyber intelligence gathering may include data collection about hackers, intruders, adversaries, etc. that can help understand their motives, intrusion methods, etc. to ultimately help prevent or deter future attacks. Not only cyber intelligence teams; private or public use the Internet and public resources to learn about threats and vulnerabilities but also hackers and attackers. In the year 2016 alone, 135 high threat zero-day exploits in Adobe, 76 in Microsoft products and 50 in Apple products were discovered, (Zero Day Initiative: <https://www.zerodayinitiative.com>, 2017).

Not even dark web sites, but public websites can be also used as effective hacking or attacking tools. For example, websites such as Shodan: (<https://www.shodan.io/>), Zomeye: (<https://www.zomeye.org>), and <https://www.go4expert.com/> can provide a wealth of information for attackers about candidate targets with very good introduction details to start further investigations and analysis.

While Online Social Intelligence (OSINT) information is available largely for free, however, several challenges exist related to information overload, the collection, and aggregation process. Additionally, transferring such information into actions is not trivial. Several recent security incidents in the US showed that significant information was available before many events. The problems were related to making timely proper actions or synchronizing information from different sources.

In this paper, we adopted a text mining approach, specifically topic modeling, to extract topics of interest from hackers' websites that can be used as inputs to security controls and systems. The rest of the paper is organized as the following: Section 2 summarizes a selection of relevant research contributions, and section 3 presents

our goals and approaches. In section 4, we describe initial experiments on a selected hackers' website to demo the topic modeling approach and paper is concluded in section 5.

2 Literature Review

A significant contribution in this area comes from AZSecure team (<https://www.azsecure-data.org/home.html>) lead by Arizona State University [e.g., 2, 3, 4]. Similar to our goal, those papers attempted to crawl selected hackers' websites to extract security or cyber intelligence related knowledge. Some of those contributions correlated extracted knowledge from hackers' websites with information from cybersecurity experts collected from Online Social Networks (OSN) such as Twitter.

The commonality of the papers surveyed in the relevant literature is related to (1) the goal; extracting useful knowledge and (2) the target; hackers' websites and forums. Differences are on what type of knowledge to extract and how to approach the extraction and the analysis activities.

Samtani, et al. [5] conducted an analysis on investigating hackers' assets through some well-known hackers' forums. Some of the most commonly used assets are attachments, source-codes, and tutorials. As expected in those forums, the main subjects or themes are related to hacking methods, tools, and zero-day vulnerabilities.

Abbasi, et al. [1] examined hackers' profiles, characteristics, and specialties. Profiles are studied based on three main high-level features: cybercriminal assets, specialty lexicons, and forum involvement. Each one of those features can have one or more direct features that can be extracted from hackers' forums. In the scope of studying hackers' profiles and characteristics, Park, et al. [6] paper studied different categories of behaviors in hackers' profiles related to their technical skills, their social or mental profiles and personalities. Hackers' profiles include extreme personalities such as those who are looking for high publicity and ego-fulfillment. On the other hand, hackers can be much conservative in their publicity and desire to be visible to the public.

Several challenges related to the overall process of extracting knowledge from hackers' websites are discussed in those different papers and others [e.g., 4, 7, 8, 9]. Some of the main challenges are related to hackers' techniques in information hiding and masquerading in addition to their different techniques to block such content from public accessibility.

3 Goals and Approaches

Figure 1 below simplifies our model to extract topics of interest from hackers' websites. Our focus in this paper is on the technical aspects of attacks and malware. We used a popular topic mining algorithm, (LDA algorithm) to extract the best selection of topics as classes.

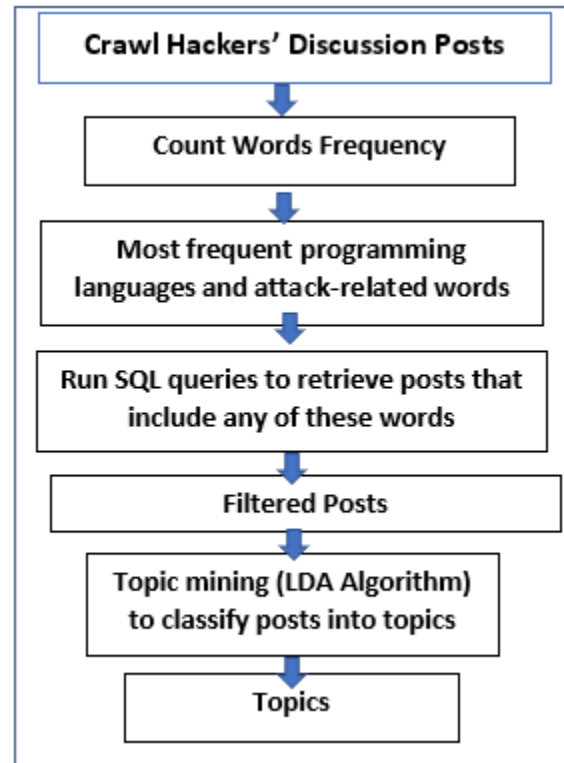


Figure 1: Our Topics of Interest Extraction model

3.1 Data Collection and Preparation

In this study, we used CrackingFire forum public dataset that contains 37,572 forum posts ranging from 4/7/2011 – 2/21/2018 (Available <http://www.azsecure-data.org/> [10]). This dataset facilitates cybersecurity research concerning with analysis of hacker assets and especially source code analysis of these assets. To prepare the dataset, we excluded stop words and used the Term Frequency Inverse Document Frequency (TF-IDF) technique to represent each post [11]. Particularly, the weight of a word i in a user post j is given by

$$F_{ij} * \log(N/DF)$$

Where F_{ij} is the frequency of the word i in the post j , N indicates the number of posts in the data set, and DF is the number of discussion posts that contains word i .

3.2 Topic Modeling: LDA

Topic models are types of statistical algorithms for extracting the main topics in a collection of documents. Latent Dirichlet Allocation (LDA) is one of the common topic modeling algorithms used [12]. The algorithm produces a set of topics with a probability distribution over words in each topic. The algorithm also generates probability distributions over topics for each document [13].

To explain the outputs of LDA, assume $D=\{d_1, d_2, \dots, d_n\}$ the set of documents in a collection, $T=\{t_1, t_2, \dots, t_m\}$ the set of generated topics, and $W=\{w_1, w_2, \dots, w_k\}$ the words in each topic. The first output is an $D \times T$ matrix with $n \times m$ size, where the weight

$w_{i,j}$ is the association between a document d_i and a topic t_j . In our study, the documents are discussion posts for hackers' forum CrackingFire. The second result is an $T \times W$ matrix with $m \times k$ size, where the weight $w_{i,j}$ is the association between the topic t_i and a word w_j . The corresponding reproductive process is shown below [14, 15]:

- (1) For each topic $t \in \{1, \dots, m\}$,
 - (a) generate a probability distribution over words
 $\beta_t \sim \text{Dirichlet}(\eta)$.
- (2) For each document d ,
 - (a) generate a vector of the topic probability distribution
 $\theta_d \sim \text{Dirichlet}(\alpha)$.
 - (b) For each word w_i in document d ,
 - (i) generate a topic assignment
 $z_i \sim \text{Multinomial}(\theta_d)$;
 - (ii) generate a word $w_i \sim \text{Multinomial}(\beta_{z_i})$.

β_t is the word distribution for topic t , and θ_d is the topic distribution for document d . The notations η and α are model parameters.

4 Experiment and Analysis

4.1 Extracting ToI from CrackingFire

We selected one hackers' forum or website, CrackingFire, to evaluate our model. However, our model is generic and can be expanded to other websites. The LDA identified 10 topics and within each topic showed the top-10 words and their relative weight (i.e. probability). The naming of topics was based on the logical connection between these 10 most frequent words for a topic.

Table 1 shows the Topics of Interest "ToIs" related to SQL Injection and their most relevant terms.

ToI	Key Terms
Sql injection	Sql, injection, hacking, attack, lesson, mirror, htc, ddos, theme, id
The Structured Query Language injection (SQLI)	Php, crackingfire, Ramadan, analyzer, Brazilian, sqli, com, expiration, army, asp'
SQLi Dumper	Sqli, dumper, MediaFire, pass, hacknho, link, hq, com, private, cyberakline'

Table 2 shows other examples of ToI and their most significant terms.

ToI	Key Terms
Google dork	Inurl, php, upload, dork, members, usd, com, login, id, proxy'
List of proxies and spoiltertarget	Proxies, anonymous, com, http, shell, spoiler, spoiltertarget, php, list, www
Bots	Apk, nm, kent, tab, wow, bots, tried, script, wp
Silent Exploit FUD	Com, cyber, https, http, renew, Brazilian, army, fud, exploits

Hackers tactics and websites	Navigon, euq, hackers, vip, nav, com, sites, coins, gmail, igraal
CyberGhost VPN crack	Vpn, http, com, cyberghost, crack, id, php, www, premium, hidden"
Hidden contents	Hidden, file, rar, content, http, net, click, download, data, use

Our findings based on previous experiments:

We have several incidents of False Positive (FP) terms, where our model suggests they are key terms to the ToI and they were not (either discovered manually or through the prediction algorithms). This can be caused by several factors such as:

- Accuracy in most topic analysis cases is size-dependent where larger datasets from the subject can show more insights and hence better results. Given the large content of the website, our dataset is an early small attempt that needs more collection, analysis and tuning.
- Attacks usually have contexts and tools that judge content purely based on individual words may miss such context. This may make some irrelevant words, relevant or vice versa.
- Users on OSNs in general and hackers in particular use slang and unstructured language and terms part of their discussions.
- Hackers may also use "hacking conventions" as their own way of encrypting their discussions.
- Spams exist in hacking forums and can impact the accuracy of ToI extractions, without implementing proper spam reduction or elimination methods.

4.2 Extracting ToI from Torum

In the second experiment, we selected a website that has its own hacking/malware related categories (see Figure 2). This can help us compare the algorithmic classification of posts in the different categories with those predefined by the website.

The data we extracted from Torum included the following main columns (see Figure 3 for a sample of data extracted):

1. The forum and topic under which the post is located.
2. Metadata about the user, who wrote the post, date/time of the post, etc.
3. The content of the post

We extracted thousands of posts from this website. We observed the following after the analysis and ToI extraction process.

1. The dark web is an open market for all types of "illegal contents" not only malware or hacking subjects. For example, it contains content related to identity theft, drugs, pornography, etc. Hence, we should have in future two stages of classification; The first one on whether the post is hacking/malware related post or not. Then, the second one for those related to malware/hacking, we can conduct

further classification for the type/nature of hacking or malware subject.

- Users who post on those websites may not necessarily observe the predefined categories and may post content in the wrong categories. Most of those websites do not reject such content and only expect users to adhere to posting content in the most relevant category.
- The preprocessing of posts from the dark web should take into consideration the nature of the special languages, symbols or icons used for slangs, shortcuts, etc. Standard dictionary-based algorithms may fail to detect or identify such content.



Figure 2: Torum predefined categories, a sample

Forum	Topic	UserData	Comment		
General d	Bitcoin Mixer	Postby tyl	If you have monero you can use sei		
General d	Bitcoin Mixer	Postby h3 tyler100 wrote: A	*01 Dec 2018If yo		
General d	Black hat or white	Postby Fr	I am in a dilemma whether I want t		
General d	Black hat or white	Postby sp	I am not a hacker i just have a bit of		
General d	Black hat or white	Postby cle	i just recently decided to transition		
General d	Black hat or white	Postby ch	I am no hacker but if i was i would j		
General d	Why is IE down	Postby Or	The intel exchange forum went do		
General d	Why is IE down	Postby au	From what I hear the admin team h		
General d	Why is IE down	Postby Or	Yeah the admins werent active and		
General d	Private section	Postby po	Hello guys im new here. I want to k		

Figure 3: Extracted data from Torum, a sample

5 Conclusion

In this paper, our goal is to extract relevant cyber intelligence knowledge from hackers' websites. Ultimately, such systems can be deployed as agents throughout the Internet and act as early warning agents for possible security attacks or malwares. Using a publicly available dataset collected from CrackingFire website, we utilized topic mining to analyze the contents of the posts and identify "Topics of Interest, ToI". The extracted ToI represent known attacks or popular attack tools.

In the second experiment, we built our own Darkweb crawler. We tested the crawler using Torum website as it has predefined malware/hacking related categories. We observed several challenges related to the process of crawling from the dark web as well as extracting relevant ToIs.

Our next call is to integrate such ToI as a new category of IoC that can be eventually fed as actionable IOCs to security controls and systems.

REFERENCES

- [1] A. Abbasi, W. Li, V. Benjamin, S. Hu, and H. Chen, "Descriptive analytics: Examining expert hackers in web forums," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 56-63: IEEE.
- [2] J. Hansen, "The study of keyword search in open source search engines and digital forensics tools with respect to the needs of cyber crime investigations," NTNU, 2017.
- [3] A. J. Park, B. Beck, D. Fletche, P. Lam, and H. H. Tsang, "Temporal analysis of radical dark web forum users," in *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2016, pp. 880-883: IEEE.
- [4] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 1845-1854.
- [5] S. Samtani, R. Chinn, and H. Chen, "Exploring hacker assets in underground forums," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2015, pp. 31-36: IEEE.
- [6] C. H. Park, I. U. Song, M. J. Kim, E. H. Chang, J. Heo, and H. T. Kim, "Prediction Model for Deviant Hacking Behavior and Hacking Type in Hackers Based on Psychological Variable," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 41, no. 4, pp. 489-498, 2016.
- [7] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017, pp. 3648-3656: IEEE.
- [8] A. Roy, C. A. Kamhoua, and P. Mohapatra, "Game theoretic characterization of collusive behavior among attackers," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, 2018, pp. 2078-2086: IEEE.
- [9] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman, and E. Ferrara, "Early warnings of cyber threats in online discussions," in *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, 2017, pp. 667-674: IEEE.
- [10] N. Zhang and M. Ebrahimi, "Hacker Web Forum Collection: Hackhound Forum Dataset," in *University of Arizona Artificial Intelligence Lab*, ed. AZSecure-data, 2018.
- [11] E. Haddi, X. Liu, and Y. Shi, "The role of text pre-processing in sentiment analysis," *Procedia Computer Science*, vol. 17, pp. 26-32, 2013.
- [12] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent dirichlet allocation," *Journal of machine Learning research*, vol. 3, no. Jan, pp. 993-1022, 2003.
- [13] Y. Bao and A. Datta, "Simultaneously discovering and quantifying risk types from textual risk disclosures," *Management Science*, vol. 60, no. 6, pp. 1371-1391, 2014.
- [14] M. A. Al-Ramahi, J. Liu, and O. F. El-Gayar, "Discovering Design Principles for Health Behavioral Change Support Systems: A Text Mining Approach," *ACM Transactions on Management Information Systems (TMIS)*, vol. 8, no. 2-3, p. Article No. 5, 2017.
- [15] M. Al-Ramahi and C. Noteboom, "A Systematic Analysis of Patient Portals Adoption, Acceptance and Usage: The Trajectory for Triple Aim?," 2018.