An Empirical Study of Malicious Threads in Security Forums

Joobin Gharibshah
jghar002@ucr.edu
University of California Riverside
Riverside, California

Zhabiz Gharibshah
zgharibshah2017@fau.edu
Florida Atlantic University
Boca Raton, Florida

Evangelos E. Papalexakis
epapalex@cs.ucr.edu
University of California Riverside
Riverside, California

Michalis Faloutsos
michalis@cs.ucr.edu
University of California Riverside
Riverside, California

ABSTRACT

How useful is the information that a security analyst can extract from a security forum? We focus on threads of interest, which we define as: (i) alerts of worrisome events, such as attacks, (ii) offering of malicious services and products, (iii) hacking information to perform malicious acts, and (iv) useful security-related experiences. The analysis of security forums is in its infancy despite several promising recent works. Here, we leverage our earlier work in thread analysis, and ask the question: what kind of information do these malicious threads provide. Specifically, we analyze threads in three dimensions: (a) temporal characteristics, (b) user-centric characteristics (c) content-centric properties. We study threads pulled from three security forums spanning the period 2012-2016. First, we show that 53% of the users asking/selling malicious *Services* on average has 3 posts and initiate 1 thread and 1 day lifetime. Second, we argue that careful analysis can help to identify emerging threats reported in security forums through *Services* and *Alerts* threads and potentially help security analysts prevent attacks. We see this study as a first attempt to argue for the wealth and type of information that can be extracted from security forums.

KEYWORDS

Security forums, Malicious threads, Profiling

ACM Reference Format:
Joobin Gharibshah, Zhabiz Gharibshah, Evangelos E. Papalexakis, and Michalis Faloutsos. 2019. An Empirical Study of Malicious Threads in Security Forums. In *Companion Proceedings of the 2019 World Wide Web Conference (WWW '19 Companion), May 13–17, 2019, San Francisco, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3308560.3316501

1 INTRODUCTION

Security forums hide a wealth of information, but mining it requires novel methods and tools. The problem is driven by practical forces: there is useful information that could help to improve security, but the volume of the data requires an automated method. The challenge is that there is a lot of "noise", there is lack of structure, and an abundance of informal and hastily written text. At the same time, security analysts need to receive focused and categorized information, which can help their task of shifting through it further. We define the problem more specifically below.

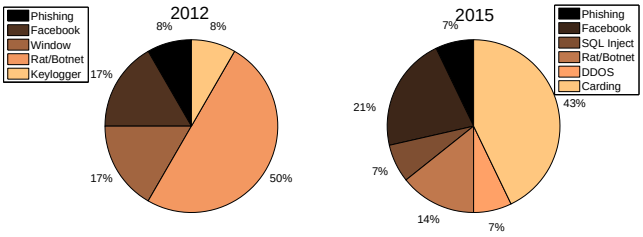


Figure 1: The percentage change of the number of threads discussing different malicious activities in OffensiveCommunity between 2012 and 2015.

Given a security forum, we want to study tempo-behavioral characteristics of **malicious threads**, which we define loosely as threads that a security analyst will want to monitor. We group them in four major categories:

a. *Alerts*: These are threads where users are reporting about being attacked by a hackers or notifying about exploits and vulnerabilities.

b. *Services*: These are threads where users are offering or requesting malicious hacking services or products.

c. *Hacks*: These are threads where users post detailed instructions for performing malicious activities. The difference with the above category is that the information is offered for free here.

d. *Experiences*: These are threads where users share their experience related to general security topics. Often users provide a personal story, a review or an article on a cyber-security concept or event.

There are relatively limited studies on extracting information from security forums, and even less work on using systematic approaches to study the extracted information. We can group prior work in the following categories. First, there is a set of work that focuses on identifying and classifying malicious IP address in security forums.[9–11] Second, there is a group of work that analyzes security forums to identify malicious activity [16, 21]. Third, there are several efforts to detect malicious users [13, 14]. Last but not least, there are some interesting work focusing on emerging threats

WWW '19 Companion, May 13–17, 2019, San Francisco, CA, USA

ACM ISBN 978-1-4503-6675-5/19/05.
https://doi.org/10.1145/3308560.3316501

on forums and other social networks [18, 19]. We discuss related work in more detail in our related work section.

In this work, we study malicious threads and users in real forums along three dimensions: (a) temporal, where we analyze the intensity and the evolution of the threads, (b) user-centric, where we characterize user behavior using five features, and (c) content-centric properties. where we analyze the content of the threads by using dominant keywords.

The key contribution of our work is a three-dimensional study of the properties of threads using real data from three security forums: OffensiveCommunity [4], HackThisSite [2] , EthicalHackers [1]. Our data consists of 163k posts and 21k unique threads spanning 2012-2016 across these three forums. Note that we identify the malicious threads by using a method that we developed earlier to: (i) identify malicious threads and, (ii) classify them into these four groups. The development of this method is not part of the contributions of this paper[1] , but we describe it in section 2 for completeness.

We summarize our key findings below.

(a) *Services* providers make short-lived appearances. We find that more than 50% of sellers of malicious services usually make one thread and typically appear in the platform only briefly[2].

(b) Authors of *Hacks* are fairly active users. We find that most of the authors of *Hacks* usually initiate a number of threads and stay active for more than 60 days in the forums which is significantly larger than the average user who posts in malicious threads.

(c) Thread activity has predictive value. We find an indication that analyzing forums carefully can help us anticipate malicious behaviors and even attacks. We found that a *Hacks* on compromising Facebook accounts seemed to have led to an attack reported by *Alerts* thread that discussed a widespread Facebook accounts hacking in 2015, which referred back to the "how to" thread.

(d) The type of malicious activity varies by forum. We find that the type of malicious activity varies by the forum. For example, 45% of malicious threads in OffensiveCommunity are *Hacks*, which is much higher than other forums, while 54% of malicious threads in HackThisSite are *Services*, which exhibits the highest relative activity in this class.

(e) The content of the threads captures interesting trends. We find that the threads in the forum can mirror the trends and concerns of the security community. For example, in 2012, the majority of the discussions focused on malware, including buying and selling and how to exploit botnet and RAT malware, while in the same forum in 2015, the focus was on buying and selling credit card numbers as shown in Figure 1 which is aligned with independently observed trends [3]

2 OVERVIEW OF OUR PRIOR METHOD

In our earlier work, we proposed an approach that identifies and classifies threads of interest from a forum based on one or more sets of keywords that the user provides. We present a high-level description of our approach for completeness, but we do not consider this as part of the contributions of this work.

[1]Currently under submission.

[2]We use the login name of a user to distinguish users. Clearly, the same seller can appear in the platform under different names, which is something that we will investigate in the future.

The approach consists of the following two parts: (a) a similarity-based approach with thread embedding to extract relevant threads of interest, and b) a classification approach based on weighted-embedding method to group relevant threads into user-defined classes.

2.1 Relevant thread extraction

Here we select relevant threads starting from sets of keywords provided by the user. The approach consists of the following phases: (a) a keyword matching step, where we use the user-defined keywords to identify relevant threads that contain these keywords, and (b) a similarity-based phase, where we identify threads that are "similar" to the ones identified above. The similarity is established at the word embedding space.

a. Keyword matching phase. Given a set or sets of keywords, we identify the threads where these keywords appear. A simple text matching approach can distinguish all occurrence of such keywords in the forum threads.

b. Similarity-based phase. Our approach consists of three steps which gets forums, a set of keywords, and set of relevant threads as the input and identify threads of interest as follows:

Step 1. Determining the embedding space. We project every word as a point in a m-dimensional space using a word embedding approach (e.g. Word2Vec). In this way, every word is represented by a vector of m dimensions.

Step 2. Projecting threads. We project all the threads in a multi-dimensional space: both the relevant threads selected from the output of the keyword matching phase and the non-selected ones. The thread projection is a function of the vectors of its words and captures both the average and the maximum values of the vectors of its words[20].

Step 3. Identifying relevant threads. We identify more relevant threads among the non-selected threads that are "sufficiently-close" in terms of similarity to the relevant threads in the thread embedding space.

2.2 Thread Classification

In this part, we classify threads into classes, which are defined by the user. We assume that each class k is defined by a group of words that we denote as $WordClass_k$. In practice these sets of words will be provided by the user and they are inputs to our algorithm.

Our approach can be described as following steps:

Step 1. We create a projection of every class k into the word embedding space by using the words that define the class, $WordClass_k$.

Step 2. We calculate the similarity of every word in the forum v_i for each class k.

Step 3. For each class, we create a weighted embedding by using the similarity to adjust the embedding projection of each word v_i for each class.

Step 4. We use weighted embedding to train an ensemble classifier using supervised learning.

Using the classifier. Given a thread, we calculate its projection in the embedding space, and then we pass it to the classifier to determine its class.

Table 1: The basic statistics of our forums

	OffensiveCommunity	HackThisSite	EthicalHackers
Posts	25538	84125	54176
Threads	3542	8504	8745
Users	5549	5904	2970

3 EXPERIMENTAL RESULTS

We present our experimental results and evaluation of our approach in analyzing extracted malicious threads.

3.1 Our security forums

We use the three forums (OffensiveCommunity, HackThisSite, EthicalHackers) that presented in Table 1. We briefly describe our three forums below.

a. OffensiveCommunity (OC): This forum seems to be on the fringes of legality. As the name suggests, the forum focuses on "offensive security", namely, breaking into systems. Indeed, many posts provide step by step instructions on how to compromise systems, and advertise hacking tools and services.

b. HackThisSite (HT): As the name suggests, this forum has also an attacking orientation. There are threads that describe how to break into websites and systems, but there are also more general discussions about the users' experiences in cyber-security.

c. EthicalHackers (EH): This forum seems to consist mostly of "white hat" hackers, as its name suggests. Many threads are about making systems more secure. However, it contains more *Alerts* and *Experiences* threads than others forums.

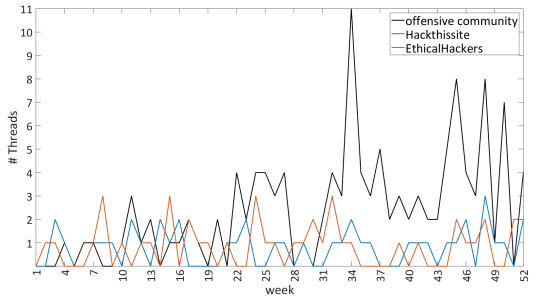


Figure 2: Thread of interest appearing in each week of year 2015 for three forums OffensiveCommunity, HackThisSite, EthicalHackers

Establishing the Groundtruth.

For validating our method, we need groundtruth. To construct the groundtruth, we randomly selected 450 among the relevant threads from each forum as selected by the identification part. The labelling involved three manual evaluations based on the definitions and examples of the four classes, which we listed above. We then combine the "votes", and assign the class selected by the majority. With this process, we labelled 1350 posts in three forums and we show present our labeled data in Table 4.

3.2 Temporal analysis

We study the temporal characteristics of malicious threads. Our goal is to explore forums by looking into information regarding sequence of data over time.

a. The focus of malicious threads varies from year to year. We see in Figure 1 that over two different years the topics of the discussions varied. For example, a topic like "Botnet and Rat" is 50% of the discussions in 2012 but it lost its' popularity in 2015 and possesses only 7% of the discussions. Another topic like "carding" in which users trade stolen credit cards became a major topic in 2015 with about 43% of the discussions of malicious threads in OffensiveCommunity.

b. The malicious activity increased. We find that OffensiveCommunity seems to dominate the other two forums in terms of the absolute number of malicious threads. In 2015 OffensiveCommunity reported malicious threads 2 times more than HackThisSite and EthicalHackers. We can see that during the last five months of 2015 in OffensiveCommunity more malicious threads appear in the forum. In table 2, we see a sample of the discussions happened at week 34 in OffensiveCommunity forums in year 2015.

3.2.1 Case-study: Hacks *activity as an early indication of an attack.* We argue that mining the forums could actually provide information about real events. Here we provide a case where threads of the *Hacks* class were "early indications" of an attack that happened later. Specifically, we identify a link between malicious *Hacks* posted on OffensiveCommunity to hack Facebook accounts in March 2015 to a reported attack by posts of *Alerts* class regarding a widespread Facebook account hacking.

We conducted the following analysis. We plot the time-series of the number of malicious threads in OffensiveCommunity in 2015. We show the time-series in Figure 2. We observe some spikes on these time-series, which we further analyze. One of the spikes was in March 2015, and there is a *Hacks* tutorial thread to break into Facebook accounts with this title "How to Hack Facebook Account with Reconnect Tool". Subsequently, we found other threads in August 2015, in which it was reported that many Facebook's accounts got hacked and the posts argue that attackers used the same techniques as discussed in the earlier threads. The *Alerts* made in a thread with this title: "Hacking Facebook Pages 2015"

We argue that this case-study points to additional layers of functionality that can be built upon our method, that can provide a semi-automated way to extract richer information beyond just reporting malicious threads.

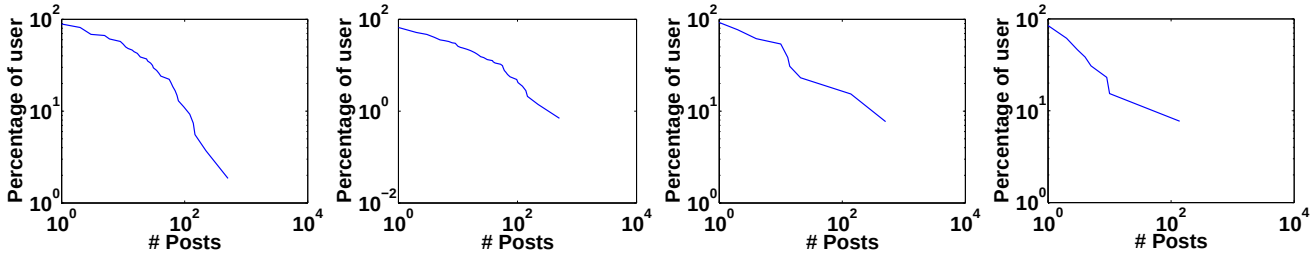
3.3 User-centric analysis

In Figures 3,4,5,6,7, we present the cumulative complementary distribution function of the number of posts per user, the number of threads per user, the number of initiated threads per user, the average length of the posts per users, and the active life time per users for each of the four groups of malicious threads respectively. We focus on the OffensiveCommunity as a forum with indicative behavior in this regard.

(a) *Services* providers make short-lived appearances. We show that more than 50% sellers and buyer of malicious services usually make one thread and they do not post more than 3 times in the thread, also they typically appear in the platform only briefly

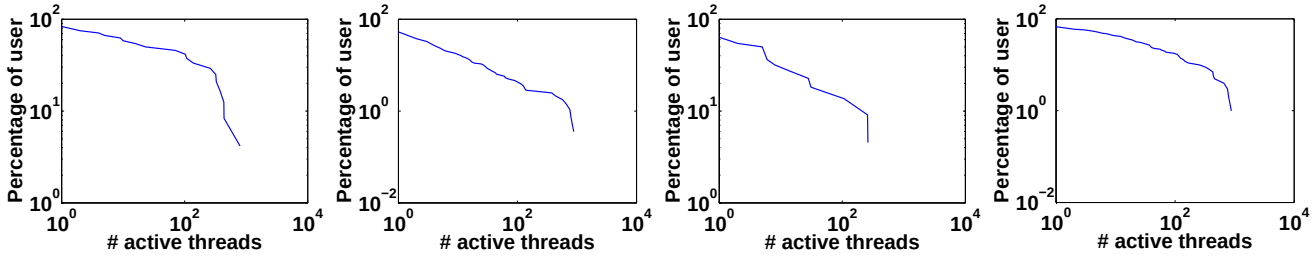
Table 2: Threads of interest in OffensiveCommunity in week 34 in year 2015

Title	Post
Professional Booter/DDoS service OverLoadLab	Hello, welcome to OverLoadLab . We are proud to offer probably the best service for the implementation of DDoS attacks in the world.....
àÿ£ Hacker Wanted MAKE 1000s àÿ£	Digitalmafia is a group of Blackhat hackers from all over the world! Organized Digital Crime Syndicate - ODCS. We are decentralized and can only be contacted through .onion market sites
how to hack facebook account using brute force	What is Brute Force And How to Work Brute force definition Brute force also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such
PM RIPPER ALERT!!!	Seller with the following IDs - Yahoo ID : XXX - EMail: ... Is a real ripper, i sent him PM and he disappear into thin air... if you love your PM please do not send to this guy. He is here to rip off. Be warned!!!



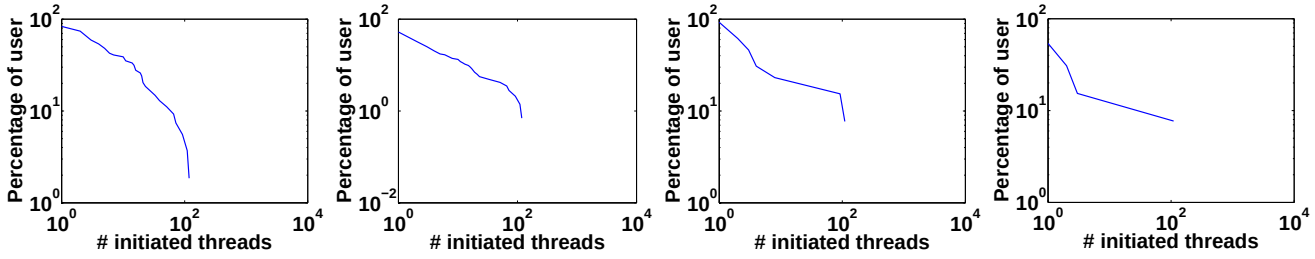
(a) *Hacks* (b) *Services* (c) *Alerts* (d) *Experiences*

Figure 3: CCDF of the number of posts per user who posted malicious threads (log-log scale) in OffensiveCommunity. More than 54% of the users who write in *Services* has less than 3 posts in the forum.



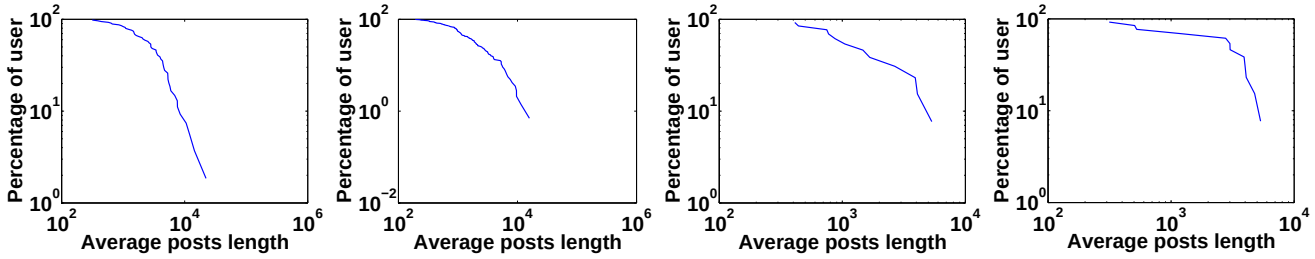
(a) *Hacks* (b) *Services* (c) *Alerts* (c) *Experiences*

Figure 4: CCDF of the number of active threads per user who posted malicious threads (log-log scale) in OffensiveCommunity. More than 63% of the users who write in *Services* were active in only one or two threads.



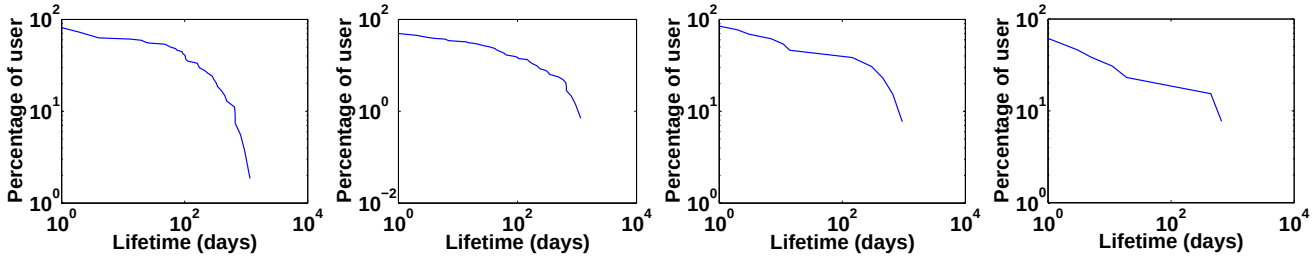
(a) *Hacks* (b) *Services* (c) *Alerts* (d) *Experiences*

Figure 5: CCDF of the number of threads initiated per user who posted malicious threads (log-log scale) in OffensiveCommunity. More than 68% of the users who write in *Services* initiated less than 2 threads.



(a) *Hacks* (b) *Services* (c) *Alerts* (d) *Experiences*

Figure 6: CCDF of the average posts length per user who posted malicious threads (log-log scale) in OffensiveCommunity. More than 50% of the users write posts with average length of 870 characters in *Alerts* threads, while in *Hacks* threads the average post length is less than 4100 characters.



(a) *Hacks* (b) *Services* (c) *Alerts* (d) *Experiences*

Figure 7: CCDF of the average lifetime length per user who posted malicious threads (log-log scale) in OffensiveCommunity. More than 50% of the users who start *Services* threads appear only for one day in the forum.

for at most one day (at least with a given login name). Moreover compared to the users who posting in other categories, here they write shorter posts with an average of 870 characters. This behavior is different than what have seen in other social trading networks where people only do trading. [6].

(b) *Hacks* providers are mostly active users. We find that most of the *Hacks* providers usually initiate larger number of threads and stay active more than 60 days in the forums, which is significantly larger than other users posting in the malicious threads. These users on average use longer posts length compared to users in other categories with more than 4100 characters.

Moreover, we see in all the cases the distributions are skewed, that is, most of the users contribute few posts in the forums and engage with few threads. In OffensiveCommunity, 85% of users who post malicious threads have less than 10 posts in the forum, while 3.8% of such users post more than 50 posts. We find that more than 60% of the users have the lifetime less than 13 days in the forums. It means that for such users the difference between their first and the last post in the forums is less than 13 days. This skewed behavior is typical for online users and communities [7].

3.4 Content-centric analysis

Here, we study the content of malicious threads in forums, although we have done some of that already in our temporal analysis.

a. The type of malicious activity variation by forum. We find that the type of malicious activity varies by the forum. Usually in all forums the *Services* threads have the highest activity. However, in other categories we can see that 45% of malicious threads in OffensiveCommunity is in *Hacks* which is more than other forums. EthicalHackers has the most number of *Alerts* threads compared to other forums. HackThisSite with 54% of the threads in *Services* has the highest activity in this class among other forums. We show more details in Table 4.

Table 3: *WordClass*, the set of words which "define" each class.

Hacks	*Services*	*Alerts*	*Experiences*
tutorial	tool	announced	article
guide	price	reported	story
steps	pay	hacker	challenge

Table 4: The breakdown of the data per class in forums.

	OffensComm.		HackThisSite		EthicalHackers	
Total	450		450		450	
	#	%	#	%	#	%
Hacks	202	45%	49	11%	42	9%
Services	204	45%	242	54%	166	37%
Alerts	27	6%	37	8%	78	17%
Experiences	17	4%	128	28%	164	36%

b. Identifying surprising keywords. We extract the dominant keywords in each class of the malicious threads, and we see words that we did not expect. In more detail, we consider the frequency

(a) *Services* (b) *Hacks* (c) *Alerts* (d) *Experiences*

Figure 8: Word cloud for the different classes of malicious threads for OffensiveCommunity.

of the keywords in each class of malicious threads. We show the results for OffensiveCommunity.

First, interestingly, we found that less than 40% of $WordClass_k$, which we introduced in section 2 and depicted in Table 3 appear as the most dominant keywords in malicious threads classes as we show in Figure 8. For example, the most frequent words in class *Alerts* in OffensiveCommunity forums are: “hacker", “Indian", “Pakistan", “hacked". Note that among these words, we only used the word “hacked" to define class *Alerts* previously. Similarly in *Hacks* class the words “tutorial", “code", “file" dominate in terms of frequency. Among these words, only the word “tutorial" was used to define this class.

Second, we find some surprising frequent words. For example, it is quite surprising that the words “Indian" and "Pakistan" emerge as popular words. For exmaple there is an *Alerts* thread with title “Pakistan Under Big Cyber Attack By Indians - 15 August” with discuss about a cyber-was between two countries of Pakistan and India.

The importance of such analysis is that even though we extracted the malicious threads with an initial set of keywords (Table 3), our analysis can point to interested related concepts that were not anticipating ahead of time. In fact, we intend to create an iterative approach, where we start with an initial set of keywords, and in each iteration we can refine the keywords of interest in order to explore naturally occurring themes.

4 RELATED WORK

We summarize related work in extracting and classifying entities from security forums.

a. Identifying IP addresses in security forums. There is a group of efforts that study IP addresses in security forums to identify and classify malicious IP addresses in such forums [9, 10]. They have proposed transfer learning based approach that can use training information on one forum to develop sufficient training data for a new forum [11]. In another work [8], they focus on the spatiotemporal properties of Canadian IP addresses in forums without employing any identification and classification methods.

b. Identifying entities of interest. A few recent studies identify malicious services and products in security forums by focusing on their availability and price [6, 15, 16] Another interesting work [21] uses a word embedding technique focusing identifying vulnerabilities and exploits.

c. Identifying malicious users. there are several efforts to study the users of security forums, group them into different classes, and identify their roles and social interactions [5, 12–14, 22].

d. Identifying malicious events. Another work [18] identifies emerging threats by monitoring the behavior of malicious users and correlating it with information from security experts on Twitter. Moreover, there is a comprehensive study on the vulnerability reported on twitter. [17] Another study [19] detects emerging security concerns by monitoring the keywords used in forums and other online platforms, such as blogs.

5 CONCLUSION

There is a wealth of information in security forums, but still, the analysis of security forums is in its infancy, despite several promising recent works.

The goal of our work is provide empirical, but concrete indication, of useful information from threads that have been identified as threads of interest. We consider three dimensions of properties: (a) temporal, (b) user-centric, (c) content-centric properties. Using real data from security forums, we show that we can find interesting and often actionable pieces of information from these forums.

In the future, we plan to extend our work in two different dimensions. First, we want to develop automated methods to extract useful and actionable information from such threads in a form that can be readily used by a security analyst. Second, we want to develop visualization techniques and metrics that can easily highlight properties and phenomena of interst.

6 ACKNOWLEDGMENT

This material is based upon work supported by DHS ST Cyber Security (DDoSD) HSHQDC-14-R-B00017 grant. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the funding institutions.

REFERENCES

[1] 2018. Ethical hacker Forums. https://www.ethicalhacker.net/forums/
[2] 2018. Hack This Site Forums. https://www.hackthissite.org/forums/
[3] 2018. Nasdaq. https://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388
[4] 2018. Offensive Community Forums. http://www.offensivecommunity.net
[5] A. Abbasi, W. Li, V. Benjamin, S. Hu, and H. Chen. 2014. Descriptive Analytics: Examining Expert Hackers in Web Forums. In *2014 IEEE Joint Intelligence and Security Informatics Conference*. 56–63. https://doi.org/10.1109/JISIC.2014.18

[6] Luca Allodi. 2017. Economic factors of vulnerability trade and exploitation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1483–1499.

[7] P. Devineni, D. Koutra, M. Faloutsos, and C. Faloutsos. 2015. If walls could talk: Patterns and anomalies in Facebook wallposts. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. 367–374. https://doi.org/10.1145/2808797.2808880

[8] R. Frank et al. 2016. Location, Location, Location: Mapping Potential Canadian Targets in Online Hacker Discussion Forums *(EISIC '16)*.

[9] Joobin Gharibshah et al. 2018. Mining actionable information from security forums: the case of malicious IP addresses. *CoRR* abs/1804.04800 (2018). arXiv:1804.04800

[10] Joobin Gharibshah, Tai Ching Li, Maria Solanas Vanrell, Andre Castro, Konstantinos Pelechrinis, Evangelos E. Papalexakis, and Michalis Faloutsos. 2017. InferIP: Extracting Actionable Information from Security Discussion Forums. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (ASONAM '17)*. ACM, New York, NY, USA, 301–304. https://doi.org/10.1145/3110025.3110055

[11] Joobin Gharibshah, Evangelos E. Papalexakis, and Michalis Faloutsos. 2018. RIPEx: Extracting Malicious IP Addresses from Security Forums Using Cross-Forum Learning. In *Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD'18)*. Springer International Publishing, Cham, 517–529.

[12] Thomas J Holt, Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012. Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology* 6 (01 2012), 891–903.

[13] W. Li and H. Chen. 2014. Identifying Top Sellers In Underground Economy Using Deep Learning-Based Sentiment Analysis. In *2014 IEEE Joint Intelligence and Security Informatics Conference*. 64–67.

[14] E. Marin, J. Shakarian, and P. Shakarian. 2018. Mining Key-Hackers on Darkweb Forums. In *2018 1st International Conference on Data Intelligence and Security (ICDIS)*. 73–80.

[15] Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. An Analysis of Underground Forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC '11)*. ACM, New York, NY, USA, 71–80.

[16] Rebecca S. Portnoff, Sadia Afroz, Greg Durrett, Jonathan K. Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko, and Vern Paxson. 2017. Tools for Automated Analysis of Cybercriminal Markets. In *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 657–666.

[17] Carl Sabottke, Octavian Suciu, and Tudor Dumitras. 2015. Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C., 1041–1056.

[18] Anna Sapienza, Alessandro Bessi, Saranya Damodaran, Paulo Shakarian, Kristina Lerman, and Emilio Ferrara. 2017. Early warnings of cyber threats in online discussions. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*. IEEE, 667–674.

[19] Anna Sapienza, Sindhu Kiranmai Ernala, Alessandro Bessi, Kristina Lerman, and Emilio Ferrara. 2018. DISCOVER: Mining Online Chatter for Emerging Cyber Threats. In *Companion Proceedings of the The Web Conference 2018 (WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 983–990. https://doi.org/10.1145/3184558.3191528

[20] Dinghan Shen et al. 2018. Baseline Needs More Love: On Simple Word-Embedding-Based Models and Associated Pooling Mechanisms. In *ACL 2018*.

[21] Nazgol Tavabi, Palash Goyal, Mohammed Almukaynizi, Paulo Shakarian, and Kristina Lerman. 2018. DarkEmbed: Exploit Prediction With Neural Language Models. In *IAAI2018*.

[22] Xiong Zhang, Alex Tsang, Wei T. Yue, and Michael Chau. 2015. The Classification of Hackers by Knowledge Exchange Behaviors. *Information Systems Frontiers* 17, 6 (Dec. 2015), 1239–1251.