"Leadership in Action: How Top Hackers Behave" A Big-Data Approach with Text-Mining and Sentiment Analysis

Baidyanath Biswas
Indian Institute of Management Lucknow, India
fpm15005@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow, India
arunabha@iiml.ac.in

Gaurav Gupta
Indian Institute of Management Calcutta, India
gauravg13@email.iimcal.ac.in

Abstract

This paper examines hacker behavior in dark forums and identifies its significant predictors in the light of "leadership theory" for "communities of practice." We combine techniques from online forum features as well as text-mining and sentiment-analysis of messages. We create a multinomial logistic regression model to achieve role-based hacker classification and validate our model with actual hacker forum data. We identify "total number of messages," "number of threads," "hacker keyword frequency," and "sentiments" as the most significant predictors of expert hacker behavior. We also demonstrate that while disseminating technical knowledge, the hacker community follows Pareto principle. As a recommendation for future research, we build a unique keyword lexicon of the most significant terms derived by tf-idf measure. Such investigation of hacker behavior is particularly relevant for organizations in proactive prevention of cyber-attacks. Foresight on online hacker behavior can help businesses save losses from breaches and additional costs of attack-preventive measures.

1. Introduction and Motivation

Cyber security is a chronic and urgent issue which impacts the whole of society as individuals, industry, and governments. The World Economic Forum considers cyber-risks with top priority equivalent to the fiscal policy economic crisis [1]. News reports concerning cyber criminals stealing consumer data and cybercrime committed against high-profile targets have become everyday occurrences. It is estimated that cybercrime costs the global economy about $445 billion a year, mostly due to theft of intellectual property within developed countries and sale of stolen personal information [2]. Contemporary studies claim that a deep understanding of cyber criminals would greatly benefit the development of future cyber defenses [3]. In 2011, the National Science and Technology Council (NSTC) released a report claiming that *novel methods to model cyber adversaries* still has not been achieved in research.

Often there are instances of hackers and malignant actors who join online social networks (OSNs), build knowledge groups, and share innovative tools and techniques, code-files and impart cyber-crime awareness to other new members. Cyber threat intelligence (CTI), is the *threat intelligence related to computers, networks, and information technology*. Organizations need robust CTI analysis to help them safeguard their cyber-infrastructure from imminent attacks [5], [6], [7]. They are gradually learning to be aware of enhanced CTI analysis comprising of precognitive analysis of dark webs, forum messages and internet relay chat forums. Such activities are highly proactive and beneficial in comparison to traditional post-facto malware and attack analysis.

Dynamic CTI has helped the intelligence unit of U.K. Government Communications Headquarters (GCHQ) to shut down chat rooms of hacktivist groups Anonymous and LulzSec using distributed denial of service (DDoS) attacks [5]. Among many offenders, one hacker had stolen 200,000 PayPal account and credit card data. Another attacker had targeted government websites, and it was possible to thwart future attacks by analyzing chat messages in the Internet relay chat (IRC) forums.

Dark forums and hacker communities provide an easy but simple mechanism for malignant users to share and distribute malicious source codes and files [6], [7]. After the Mirai attack in October 2016, sharing of exploit codes and hacking I-o-T devices, webcams and network devices have become very popular.

Traditionally, studies have explored forum features only – those which are explicitly visible from the forum discussions. Ours is a step ahead, in particular, to examine individual participants' networking and message content, related patterns to understand the cyber criminals better. That is, we can identify what behaviors or features are unique to particular forum participants. Based on the uniquely identified implicit text-mining features and sentiment analysis of forum posts, as well as specific forum features from existing studies, we build our classification model to predict the possible role (or leadership) of a hacker in the participating forum. The resulting hacker-role classification model answers the following research questions, hitherto unanswered by existing literature:

URI: http://hdl.handle.net/10125/50108
ISBN: 978-0-9981331-1-9
(CC BY-NC-ND 4.0)

- What are the significant predictors of hacking behavior in dark forums?
- Top hackers manage technical discussions and knowledge dissemination (Pareto).

Due to lack of an existing dictionary on hacker forum dialect till date, we address:

- Top hacker keywords used in a typical forum.

To encourage analysis of hacker behavior independent of forums and platforms, we expect future studies to use this new hacker lexicon as a ready reference in cyber security analysis.

In the context of recent advances in cybercrime, the need for identification of implicitly formed hacker groups under anonymity is paramount. Further, it renders the more interesting to examine the behavior of top hackers and dark experts in online forums.

The remainder of this paper is organized as follows. In the next section, we present an overview of existing studies on hacker communities, key players, and social network approaches. We identify relevant research gaps and outline the current state of knowledge. Further, we present the theoretical premises of our study, drawn from leadership theory and control theory. In the next section, we build our model and develop the hypotheses. Subsequently, we describe the data, and the methodology adopted. Then we execute the model, present the estimates and discuss the implications of the results. Finally, we conclude this study and highlight the future scope of expansion of this study.

2. Related Work

The *community of practice* describes *a group of people who share a mutual concern* - a set of problems or passion about a topic, and who want deepen their knowledge and expertise by interacting on an ongoing basis [8]. Willful association of such individuals who intend to sharpen their skills in a cooperative mode belong to communities of practice. Additionally, the members can also improve their combined capabilities, which then act as foundations of value creation in knowledge-based economies. In contrast, hacker forums thrive mostly in the underground economy of society.

2.1 Hacker Communities

Hackers and malignant users make significant use of online forums [8] [10] [11]. A study by [11] delineates research themes on hacker community into three major strands – (i) *qualitative analysis to understand and describe hacker activities* [12] [13]; (ii) *analysis of carding communities and underground economy* [10] [13] [14], and, (iii) *analysis and identification of key participants in hacker communities* [15]. We identify another set of studies on hacker forums in literature : (iv) *analysis of physical hacker assets and source codes through forum analysis* [15], [16] and [17], (v) *analysis and identification of top hacker keywords and lexicons to examine hacker behavior* [11], and (vi) *analysis of social networks present in hacker forums* [18] [19] [20]. This study contributes to all of these strands of literature except (ii).

2.2 Key Actors in Online Communities

Often online community participants accumulate necessary resources, skills, and assets to form homophile groups to accomplish the intended query task [3]. In software development groups, such as the iOS and Android Developer forums, as also in hacker communities, the relatively inexperienced users strive for assistance from advanced users and experts [4] [9] [10]. Extant studies have analyzed the behavior of top hackers in communities but ignore the examination of forum features and text analytics-based models [10] [17] [18] [19] [20].

2.3. Social Network Approach

While the common perception is that hackers are loners and prefer to be anti-socials, community behavior is reported in studies using social network analysis [18] [19] [20]. Successful hackers in dark communities consist of a variety of skillsets: starting from top hackers with high technical skills to newbies and beginners with no relevant skills [18] [19]. Eventually, it becomes the onus of the selective few to disseminate the knowledge. Hackers may exhibit social network behavior through the formation of monopartite and bipartite linkages in those forums [20]. Subsequently, they attempt to locate the top hackers in the forums.

2.4. Research Gaps

Following are the research gaps identified. First, extant literature [10] [11] [17] have discussed forum features only as the principal factors of hacker reputation and expertise. In fact, few studies to date have attempted to classify hacker communities based on their roles and responsibilities, separately for each hacker group. In [17], authors sought to explain hacker reputation by the forum features. Second, there is a significant lack of connectivity between the forum features and the message content of the forum posts. No universal hacker lexicon exists which can analyze their behavior. Both of these are responsible for the observed hacker community behavioral factor(s) [10] [11] [17] and already pointed out by [11] [16] [20]. Ours is the first study to connect all the six themes mentioned in Section 2.1. Further, we present that no other study in the past been able to explain top hacker behavior applying the theoretical strands of Leadership in Communities of Practice.

3. Theoretical Foundation

We draw the theoretical foundations of our study from the Leadership Theory especially (i) Leadership in Communities of Practice, and (ii) Control Theory and Leadership in Criminal Networks.

3.1 Communities of Practice

In a community of practice, the development depends on its internal dynamics as well as the capability of the leader(s) [23] [24]. Such a group is informally bound, and demonstrates the following features: (a) solve problems quickly, (b) develop professional skills, (c) transfer best practices among the community members, (d) commonly deliver a product or service. Interesting, it may seem, hacker communities perfectly fit such a definition of *knowledge communities of practice*.

Often able leaders resolve conflicts among their members or clarify problems faced by a community. This sort of leadership behavior is resplendent of fast changing environments, such as online hacker forums. However, leader hackers differentiate from members in other communities who can play multiple roles – *browsers*, who only come to the forum for reading and self-clarification [25]; *coordinators*, who are responsible for task coordination within the community [26]; and *gatekeepers*, who regulate community interactions with its external environment [27]. Often members can juggle between each of these roles.

3.2 Control Theory and Criminal Networks

Control theories of physical systems state that a user can govern the entire system of bodies if he can identify and manipulate the existing drivers of the systems, or determine the controls [28]. Further through social media analytics, one can easily observe that particular nodes are the high influential nodes [29]. While control theory aims for commanding the criminal leaders in a network [30], in reality, it is not easy to identify such leaders – and in particular, factors to determine such leaders. Nevertheless, the control theory applied to criminal leadership [29] [30], strives for a criminal network system's controllability by tweaking the highly influential nodes only similar to the manner a hacker forum works.

4. Research model and hypothesis development

We analyze and identify the factors responsible for detecting principal actors in a hacker forum. With the increasing need to examine the textual content of posts and messages in such hacker forums, we also utilize (i) text mining, and (ii) sentiment analysis to investigate our research questions [16] [17] [22]. Each forum message is linked to a thread of discussion and is posted by a user. We transform the individual message and the categorizing factors into text corpora for each user from our dark forum dataset. Based on past studies, we define the following forum based measures: *number of threads involved*, *average message length*, the *number of total messages*, *duration* [11] [16] [17]. Next, through text-mining, we create a hacker dialect lexicon and measure the *correlation of message content* of each corpus with it. Next, we extract the *sentiment content* of the forum message and apply it to generate role-based hacker classification. Each of these features (attributes) corresponds to a hypothesis in building our model.

4.1 Expertise based on Forum Features

An individual's cognitive capital consists of expertise, experience with using the knowledge, and mastery of the application of that skill that increases over time as they interact with others [31]. It also improves on sharing knowledge and norms of the group to which the member belongs. To say further, the tenure in a shared community of practice serves as a measure of cognitive capital [31] [32]. Examination of OSNs often reveals that the visible status of a user is proportionate to the demonstrated online proficiency [32]. If a community member has stayed for longer duration, the mutual trust demonstrated by fellow colleagues, assignment of duties, and their status improves [25]. Such behavior is also visible in community question-answering (CQA) forums [52] [53]. An earlier study defines the duration feature for forum analysis, merely with the help of the date of the first message posted [17]. However, we determine duration as the time spent by each hacker member in the forum. Consequently, we hypothesize:

H1. Time spent in an online forum will intensify the expertise of a hacker.

Leaders are largely subject to moderate to high levels of credibility, because it signals highly dynamic community behavior [27] [51] [53]. A good amount of contribution indicates increased community activity and helps to build trust and reputation among other community members. Similarly, in a hacker forum, the experts and advanced users are the ones whom the beginners and newbies would flock to clarify their doubts. We often notice that super users in forums, OSNs, and CQAs can discourse over a range of diverse themes [32]. They post messages in different threads across a spectrum of sub-forums to express their opinions and share their knowledge [33]. Thus, users of high expertise and technical abilities continue to contribute actively and in the

process, encourage and guide the entire community to a higher level. Consequently, we hypothesize:
H2. The spectrum of threads across which hackers post messages is directly related to their expertise.

Members of a *community of practice* enjoy long and frequent interactions among themselves, because of a simple binding based on interests. They cooperate on joint exercises, exchange ideas and pertinent information. Experts and advanced members often preside over steady, enduring and enriching member-interactions [34]. Hacker communities enjoy similar behavioral traits, and expert hackers exchange large volumes of messages. Similar traits of message handling can be observed in CQA sites such as StackOverflow [51] [52]. Therefore, we can posit:
H3. Messages posted by hackers in the forum are directly related to their expertise.

Homophily is a pervasive feature of social networks [35] and has been shown to be empirically important in online social network data [36] [37]. Advanced hackers and dark forum experts respond to questions posted by newbies and beginners, in an attempt to reinforce their position and reputation in the dark community. Therefore, we can posit:
H4. Replies posted by hackers in each thread are directly related to their expertise.

Top hackers and experts contribute to the overall intellectual progress of the dark forum by sharing attachment. Often these attachments contain botnets, executable malware codes, payloads, and corrupt setup files to poison IPs, machines, and networks. Hence, we can posit:
H5. Total executables and attachments shared by hackers are directly related to their expertise.

4.2 Expertise based on Text-mining Features

Extant studies confirm that the number of characters spent to deliver a message strongly influence the content produced by the user [15] [16] [17]. Often average message length for each message is used as a covariate [17] [38]. We find that relatively lengthy messages deliver more cognitive value and are far more important to the larger audience of the community – be it a hacker forum or an CQA such as StackOverflow [10] [52] [53]. Word counts and message lengths increase significantly across all types of information levels with rising depth of the messages in an online learning platform [39]. Studies also confirm that users in traditional OSNs such as Facebook experience more views and replies for longer messages [40]. Similar results are observed among Enterprise Social Network (ESN)-s [41]. In an enterprise setting, message length increases for managers, while it drops considerably for other employees upon using emails as communication [42]. Such role-based demarcation is also expected in hacker forums among the different strata of members. Thus, we define average message length in terms of average character content for each user. Extant studies have applied such measure to analyze posts from web-forum participants [43] [44]. Therefore we hypothesize the following:
H6. Characters spent per message determine the expertise of the hacker.

H7. Words spent to explain and discuss queries determine the expertise of the hacker.

H8. Special characters used in messages to express emotions determine the expertise of the hacker.

H9. URLs and web-links used in the forum messages determine the expertise of the hacker.

The keywords content of the average hacker message is an important determinant of the expertise of the user. Relevant cyber security keywords can be found in higher number in the messages of an expert. Therefore we hypothesize:
H10. Cyber security keywords used in messages determine the expertise of the hacker.

4.3 Expertise based on Sentiment Features

The sentiment index determines the overall attitude of community members – whether it is positive or negative. It can also combine the opinions that are implicitly expressed in discussions. The theory of selective perception states that human beings take help of their mental map to decide whether to absorb a particular information or to reject it [46]. Members who possess an inherent positive attitude, search for helpful information and intend to provide a similar type of feedback and answers. Those who are skeptical, always look for negatively loaded messages and respond in that tone [50]. Consequently, we expect expert hackers to disseminate knowledge and thus post messages with high sentiment value (either positive or negative).
H11. Positive or negative sentiments from the messages determine the expertise of the hacker.

We employ multinomial logistic regression model for classification into different hacker roles. A multinomial logistic regression model is used when the dependent variable is unordered, categorical, and the independent variables can be continuous or categorical. In future, we intend to extend this model employing ensemble text classification techniques. We observed that maximum entropy classifier works well with our textual data. Further, a maximum entropy classifier is equivalent to a multinomial logistic regression model. We have eight target classes for the dependent variable so that there will be seven variants of Equation (1). Figure 1 shows our proposed research model.

$$\ln\left\langle \frac{P(Y_i = k)}{P(Y_i = 0)} \right\rangle = \beta_0$$
$$+ \beta_1^{(i)}(duration) + \beta_2^{(i)}\ (total\ threads)$$
$$+ \beta_3^{(i)}(total\ \ messages) + \beta_4^{(i)}(replies\ \ per\ thread)$$
$$+ \beta_5^{(i)}(total\ attachments)$$
$$+ \beta_6^{(i)}(characters\ \ used) + \beta_7^{(i)}(words\ used)$$
$$+ \beta_8^{(i)}(special\ symbols) + \beta_9^{(i)}URLs$$
$$+ \beta_{10}^{(i)}(keywords\ similarity)$$
$$+ \beta_{11}^{(i)}(message\ \ sentiment) \quad , i = 1,2,\ldots,7 \qquad (1)$$

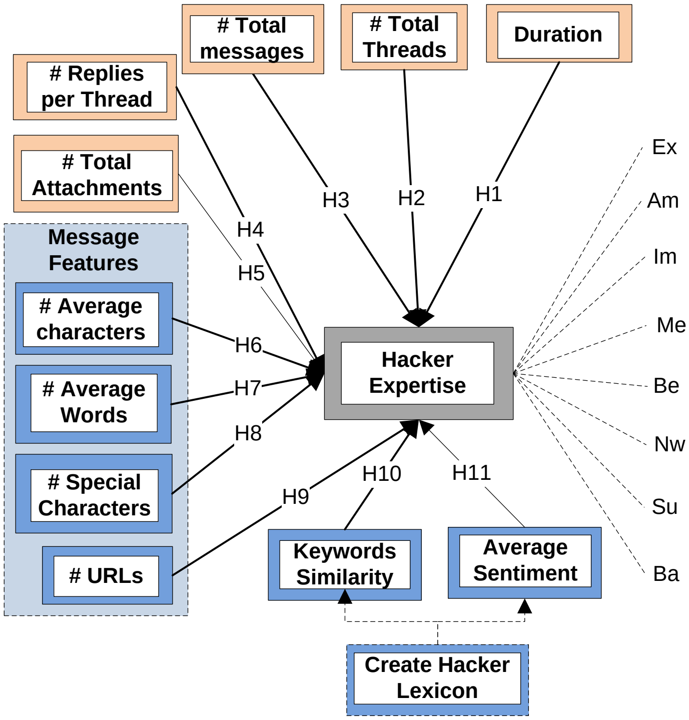

Figure 1. – Proposed Research Model

5. Data Preparation and Methodology

The data was available from the University of Arizona Hacker database collected from hackhound.org [47]. The dataset contains messages posted between October 2012 and September 2015. Forum users assigned reputation scores to each other based on the quality of answers received, posts, code files shared and technical guidance offered. Expertise ranking in the forum was then derived from the reputation score. The original dataset contains 5754 posts with 4236 clean messages posted by 808 unique members. Out of them, we remove 14 user records with junk or blank author names. Next, we look for clean and complete records in the {author-Name, flat-content} tuple. This cleaning technique leads to 700 users and their message posts. We combine messages from each of this user (hacker) and create a text corpus. Following are the aggregations of classes to achieve a cohesive result in the classification: (i) *Intelligence Service* and *Expert*, (ii) *Advanced Member* and *Advanced*, (iii) *Intermediate Member*, (iv) *Member*, (v) *Beginner*, (vi) *Newbie*, (vii) *Suspended*, and finally (viii) *Banned*. We observe that the dataset is imbalanced regarding class distribution. Other CQA services such as TurboTax Live Community (TTLC) and StackOverflow.com also demonstrate such behavior [51]. Super users in TTLC constitute 0.01 percent of overall users [52].

Role (Y)	Count	Percentage
Expert (Ex)	4	0.60%
Advanced Member (Am)	10	1.40%
Intermediate Member (Im)	35	5.00%
Member (Me)	79	11.30%
Beginner (Be)	158	22.60%
Newbie (Nw)	375	53.60%
Suspended (Su)	1	0.10%
Banned (Ba)	38	5.40%
Total	700	100%

Table 1. –Summary of User Roles

5.1 TF-IDF and Overlap Scores

We combine term-frequency (*tf*) and inverse-document-frequency (*idf*) to produce a composite weight for each term in each user corpus. We use the normalized *tf-idf*, which is given as:

$$tf_{i,j}.idf_{i,j} = \left(n_{i,j} \Big/ \sum_k n_{k,j} \right) . \log_2 \left(|D| / |d| t_i \in d \,| \right) \text{where}$$

$tf_{i,j}$ is the number of occurrences of t_i in document d_j normalized by the total count, $idf_{i,j}$ is the inverse ratio of documents with t_i and total documents in the corpus D. We apply the *Overlap Score Measure* [45] as the cumulative sum of *tf-idf* scores over all terms (or features) appearing in the cyber security keyword list, multiplied by the number of times each of the cyber security keywords occurs in *d*, and is given by $Score = \sum_{t \in k} tf_t - idf_{t,d}$.

5.2 Sentiment Analysis

We performed sentiment mining applying the *SentiStrength* software [47]. *SentiStrength* has been previously tested and validated in extant studies [48] [50]. We create our own positive and negative word lists from the generated list of significant cyber keywords and assign weightage to them. We append them to the list of existing keyword files of our

SentiStrength software so that it now picks up the modified lexicon. For example, we assign a score of -3 to *virus*, *malware*, and *crypter*, 3 to *antivirus*, -2 to *anonymous*, *overflow*, *backdoor*, 0 to *login*, and so on. In this way, we build our sentiment dictionary. To calculate the sentiment content in each message, we consider the absolute sentiment (both positive and negative) and combine them as follows.

Total Sentiment = |*Positive Sentiment*| + |*Negative Sentiment*|

6. Results

Based on the range, mean, and standard deviation values of the independent variables used in our model, we take help of log-transformation of some of the variables to adjust for over-dispersion and normality. To analyze hypotheses H_1 through H_{11}, we test the multinomial logistic regression model given by (1). We also find that H_1, H_5, and H_7 are not significant predictors for hacker expertise. Analysis of the results from the multinomial logistic regression (see Table 2) leads to the significant predictors of hacking behavior in dark forums.

#	**Hypothesized Relationship**	χ^2	**Support**
	Intercept	19.231***	---
H_1	Duration → Ex	9.113	N
H_2	Threads → Ex	32.173***	Y
H_3	Messages → Ex	95.771***	Y
H_4	Thread Replies → Ex	16.493**	Y
H_5	Attachments → Ex	3.052	N
H_6	Characters → Ex	15.399**	Y
H_7	Words → Ex	4.097	N
H_8	Special Chars. → Ex	14.245**	Y
H_9	URLs → Ex	12.825**	Y
H_{10}	Keywords → Ex	29.640***	Y
H_{11}	Sentiment → Ex	10.201***	Y

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$; Ex = Expertise

Table 2. – Likelihood Ratio Tests

Table 4 reports the comparison results of the execution of various classification algorithms with our forum data. Regular CART based decision tree and k-nearest neighbor algorithm perform poorly at around 65% overall accuracy. Boosted tree algorithm performs closest to our multinomial logistic model.

Algorithm Employed	**Overall Accuracy**
CART	65.91%
Boosted Tree	77.72%
SVM	72.90%
k-NN	65.43%
Multinomial Logit	80.57%

Table 3. – Comparison of Algorithms

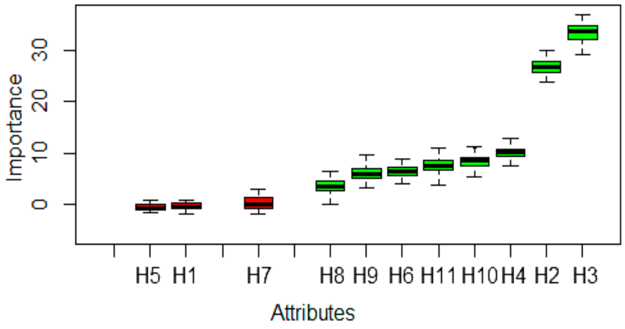

Figure 2. – Feature Ranking for the classification task.

Table 3 reports the significant predictors of hacking behavior in dark forums. Figure 2 shows the top features – *messages, threads, thread replies, keywords*, and *sentiment of messages*. The dataset is imbalanced for each class as in Table 1. So relying simply on classification accuracy makes our analysis incomplete. To overcome this problem, we consider alterative measures of effectiveness. We compute the precision, recall, and F1 scores for each class in our multi-class problem as shown in Table 4.

	Precision	**Recall**	**F1-Score**
Ex	0.80	1.00	0.44
Am	0.88	0.80	0.42
Im	0.65	0.80	0.36
Me	0.81	0.73	0.38
Be	0.68	0.79	0.37
Nw	0.87	0.88	0.44
Su	1.00	1.00	1.00
Ba	1.00	0.21	0.17

Table 4. – Summary of User Roles

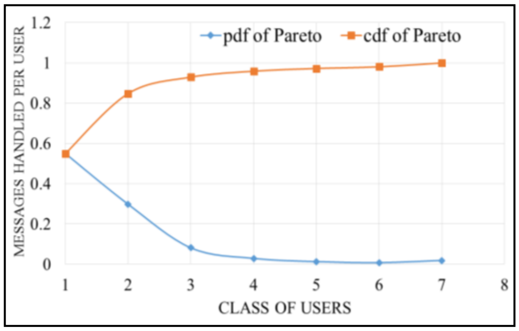

Figure 3. – Message Replies in Threads

		Predicted									
		Ex	Am	Im	Me	Be	Nw	Su	Ba	Total	% Correct
Actual	Ex	4	0	0	0	0	0	0	0	4	100.00
	Am	1	8	1	0	0	0	0	0	10	80.00
	Im	0	0	28	4	2	1	0	0	35	80.00
	Me	0	0	8	58	4	9	0	0	79	73.42
	Be	0	0	2	6	125	25	0	0	158	79.11
	Nw	0	1	1	4	37	332	0	0	375	88.53
	Su	0	0	0	0	0	0	1	0	1	100.00
	Ba	0	0	3	0	15	12	0	8	38	39.47
	Total	5	9	43	72	183	379	1	8	700	**80.57**

Table 5. – Classification and Overall Accuracy

In Figure 3, we show that the *average replies to messages in threads* by each hacker follows a Pareto distribution. We plot the *rate of replied messages per class of user* with the *respective class* so that: "1" denotes *Expert*, "2" denotes *Advanced*, "3" denotes *Intermediate*, "4" denotes *Member*, "5" denotes *Beginner*, "6" denotes *Newbie*, "7" denotes *Banned* and *Suspended*. The *CDF* (cumulative distribution function) shows that top hackers and experts contribute to more than 90 percent of the replies. This finding confirms our theoretical assumption of *leadership in the community of practice* to enable maximum knowledge sharing and managing technical discussions. Such phenomenon is also observed in CQA forums such as StackOverflow [51] [52] where super users have delivered over 78 percent of expert answers during discussions.

In Table 5, the overall classification accuracy is 80.57 %. Only 39% of *Banned* members are correctly identified. Whereas, the classification of *Experts* and *Advanced Members* are highly accurate at 100 and 80 percent respectively.

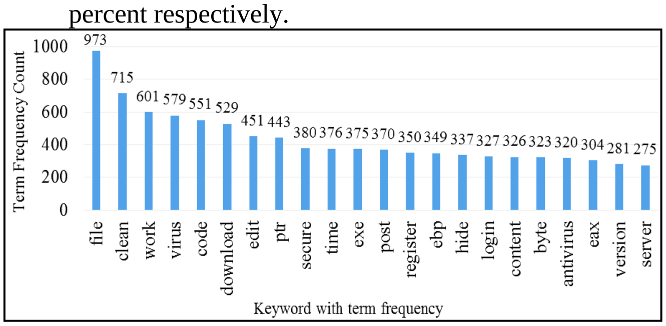

Figure 4. – Top cyber security keywords used in Hackhound forum (term frequency).

The list in Figure 4 is based on the *tf* measure. The importance of each term cannot be singlehandedly based on term frequency as analyzed in [10][15][16]. So, we combine *tf* and *idf* score for each keyword terms in the corpus of each user. The list in Figue 5 is based on the *tf-idf* measure. Comparison of Figure 4 and Figure 5 shows us that *file* is the most discussed word. The top 6 keywords have four in common – *file*, *virus*, *download*, and *code*.

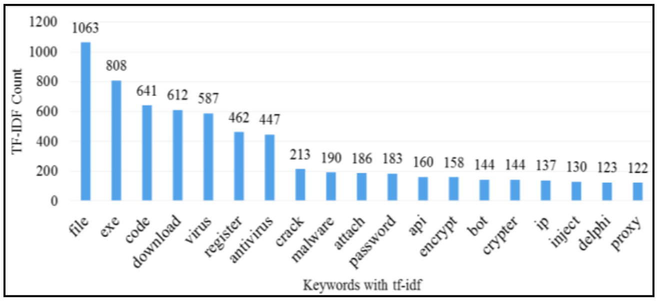

Figure 5. – Top cyber security keywords used in Hackhound forum (tf-df).

We observe that the cluster of top keywords have a much higher value than the next cluster of keywords , as seen from the sudden drop in Figure 5. It signifies that the keywords with lower count are now reduced in count-value by using *tf-idf* instead of only *tf*. Figures 6, 7, and 8 show the top 20 unigrams, bigrams, and trigrams from Hackhound text corpus.

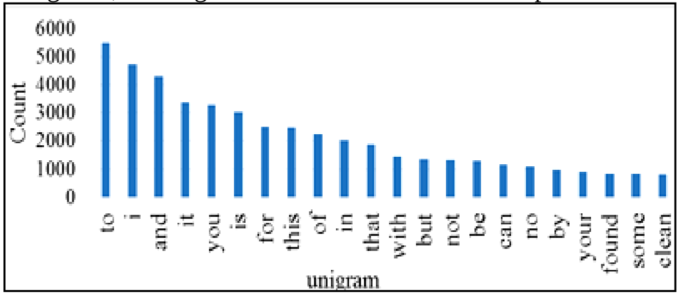

Figure 6. – Top 20 most frequent unigrams

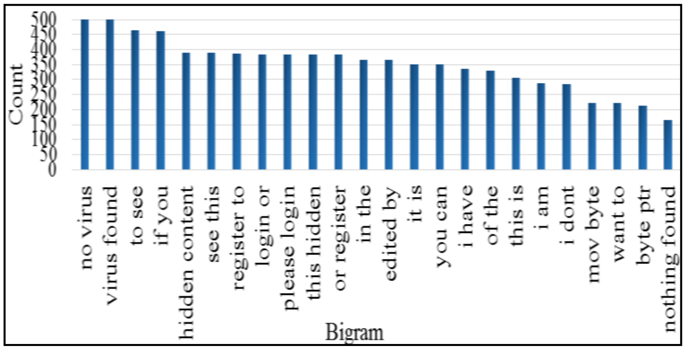

Figure 7. – Top 20 most frequent bigrams

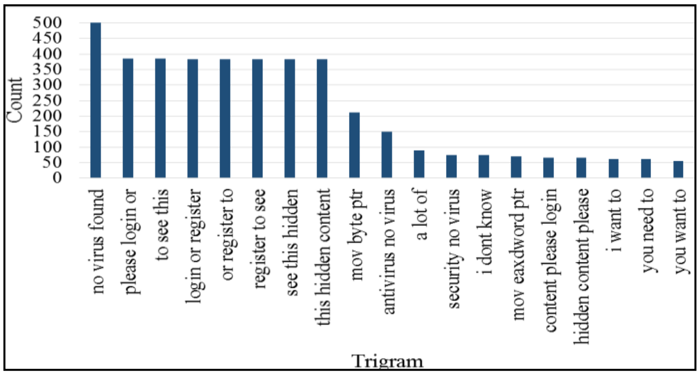

Figure 8. – Top 20 most frequent trigrams

7. Discussion of results

We observe that H_1, H_5, and H_7 are not significant for the analysis. Table 3 reports the significant predictors of hacking behavior in dark forums.

We find that the effect of *duration is insignificant to determine hacker expertise*. Our finding is matched with the results reported for both Hackhound and Unpack datasets [17].

We also find that the effect of *discussion threads is highly significant* to determine *hacker expertise*. We infer that an expert hacker significantly submits messages and posts in different types of threads. This is in line with [17]. What matters more that the absolute number of messages per thread is the total number of unique threads an advanced hacker is associated with [33].

We note that the effect of the *number of messages posted by each hacker is highly significant* to classify hackers based on their meritocracy. Our results match partly with that of [17], who considered total messages, while we worked with total messages per user. *Number of answers* also emerges as a significant predictor in CQA forums such as StackOverflow and TTLC [51] [52] [53].

We find that the effect of the *number of responses in each thread posted by a hacker is highly significant to classify hackers*. Our results do not match with [17]. However we establish this as an important determinant of the classification based on expertise. Such phenomenon is also observed in CQA forums such as StackOverflow where frequency of contribution emerges as a significant predictor [51] [52]. Further, we identify that the *average number of replies per thread* follows a Pareto distribution.

In this study, we show that the effect of the *number of attachments shared in each message posted by a hacker is not a significant predictor of hacker role classification.* Our results do not match with [17], who have earlier shown that it helps to identify an expert hacker. It may be possible that the behavior of sharing attachments by hackers have changed over the years. [17] reported the results from an older dataset, and our testbed [47] contains messages from 2012 to 2015.

We find that the effect of the *average message size posted by a hacker is a highly significant predictor of hacker role classification.* In our study, the message size is determined by the number of characters used in the messages, contrary to a study by Benjamin and Chen [17], who did not find substantial evidence.

Our study finds that the effect of the *total words used in each post by a hacker fails to significantly predict* the hacker role classification. In our study, we separately use *average words used in each post* as well as *special characters*. This means that in such online communities, the language of communication might not follow English Grammar.

We find that the effect of *special characters used in each post by a hacker is significantly linked* to predicting the hacker class. Often the hacker might use emoticons, smileys, punctuation marks, and all sorts of non-alphanumeric patterns and characters in their message. Our study provides a pioneering approach using text-mining analysis to identify the importance of such message-coding.

We find that the effect of *website links and URLs used in each post by a hacker is significantly linked* to hacker class prediction. Apart from using all sorts of non-alphanumeric characters, the expert hacker also shares relevant URLs in their message. In an attempt to encourage knowledge sharing initiative and problem-solving in the dark community, expert hackers have shared URLs in their messages.

Now, if we look back and compare the results of H_7, H_8, and H_9 combined with H_6, it is evident why H_7 did not appear significant in our study. A message may contain many different items(s) other than just words – URLs, special characters, ASCII, numbers and finally English language words. Due to the novel text-mining technique applied in this study, we were able to segregate this behavior of expert hackers evident while analyzing messages. We believe these factors are unique to hacker forums and were not reported earlier in analysis of CQA forums such as StackOverflow and TurboTax [51] [52] [53].

We also find that the *effect of hacker keywords used in the message post is significantly linked to hacker expertise.* An otherwise easy and straightforward solution would be only to classify using the term document matrix (tdm) or document-term matrix (dtm) features as the input predictors for classification.

We observe that the *effect of the total opinion within the message post is significantly linked to hacker expertise.* As a novel finding, we add our own list of significant cyber keywords generated from H_{10} and assign relative weightage to them before calculating the sentiment scores. Experts (Ex) and advanced members (Am) show much higher sentiment values in their messages and discussions. Intermediate members (Im) and members (Me) are medium in opinion content. Newbies (Nw) are the lowest in sentiment value of their forum messages.

8. Conclusion

Apart from a few distinct features, it is not possible for an outsider to find out the actual rule-base followed in hacker forums to pinpoint a user as an expert, advanced user or a beginner.

- Analyze top hacker forums, and carry out a precognitive CTI exercise.
- In such online forums of community learning, proper language of communication might not be followed by grammar rulebook.
- We also contribute by designing a robust keyword lexicon for similarity check.
- The word list is split into positive and negative opinions for further application in sentiment analysis.

We use text mining and sentiment analysis of hacker messages, to provide a pioneering approach to determining hacker forum participation. Also, we derive significant predictors of leadership patterns in dark forums. Firms need to contemplate upon those factors which we examined in our study. We identify hacker forums and dark OSNs as “communities of practice” where top hackers exhibit leadership roles. Based on their role-specific behavioral traits, we can identify significant predictors which will act as proactive CTI mechanisms to prevent cyber-attacks for businesses.

9. References

[1] World Economic Forum: Global Risks Report 2017, Available: https://www.weforum.org/reports/the-global-risks-report-2017.

[2] Graham, L. Cybercrime costs the global economy $450 billion: CEO. (2017). Available: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

[3] Mahmood, A.M.; Siponen, M.; Straub, D.; Rao, H.R.; and Raghu, T.S. Moving toward black hat research in information systems security: An editorial introduction to the special issue. MIS Quarterly, 34(3), 2-22. (2010).

[4] National Science and Technology Council. Federal Cybersecurity Research and Development Strategic Plan. (2016).Available: https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

[5] Greenwald, G. NBC News: Snowden Docs Show UK Spies Attacked Anonymous, Hackers, (2014). Available: https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361/.

[6] Farnham, G. Tools, and Standards for Cyber Threat Intelligence Projects, Available:https://www.sans.org/readingroom/whitepapers/warfare/tools-standards-cyber-threat-intelligenceprojects-34375.

[7] Shackleford, D. Who’s Using Cyber threat Intelligence and How? Available:https://www.sans.org/readingroom/whitepapers/analyst/cyberthreat-intelligence-how-35767.

[8] Hackett R. Facebook Awards Server-crushing Hacker with Its Biggest Ever Bounty, (2017). Available: http://fortune.com/2017/01/19/facebook-hacker-bug-bounty/. [Accessed: 28-Apr-2017].

[9] Odabas, M. Toward an Economic Sociology of Online Hacker Communities. In Proceedings of 27th SASE Annual Meeting. (2015).

[10] Benjamin, V., Zhang, B., Nunamaker, J. F., and Chen, H. Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities, Journal of Management Information Systems, 33(2), 482–510. (2016).

[11] Benjamin, V., & Chen, H. Developing understanding of hacker language through the use of lexical semantics. In Proceedings of the International Conference on Intelligence and Security Informatics (ISI), 79-84. (2015).

[12] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. An Analysis of underground forums, In Proceedings of ACM SIGCOMM Conference on Internet Measures, 71, (2011).

[13] Holt, T. J. & Kilger, M. Know Your Enemy: The Social Dynamics of Hacking, Honeynet Project, 1–17. (2012).

[14] Yip, M., Shadbolt, N. & Webber, C. Why Forums? An Empirical Analysis of the Facilitating Factors of Carding Forums, ACM Web Science, (2013).

[15] Samtani, S., Chinn, R., & Chen, H. Exploring hacker assets in underground forums. In Proceedings of the International Conference on Intelligence and Security Informatics (ISI), 31-36, (2015).

[16] Samtani, S., Chinn, K., Larson, C., & Chen, H. AZSecure Hacker Assets Portal: Cyber threat intelligence and malware analysis. In Proceedings of the International Conference on Intelligence and Security Informatics (ISI), 19-24. (2016).

[17] Benjamin, V., & Chen, H. Securing cyberspace: Identifying key actors in hacker communities. Proceedings of the International Conference on Intelligence and Security Informatics (ISI), 24-29, IEEE. (2012).

[18] Lu, Y., Luo, X., Polgar, M., & Cao, Y. Social network analysis of a criminal hacker community. Journal of Computer Information Systems, 51(2), 31-41. (2010).

[19] Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. Examining the social networks of malware writers and hackers. International Journal of Cyber Criminology, 6(1), 891. (2012).

[20] Samtani, S., & Chen, H. Using social network analysis to identify key hackers for keylogging tools in hacker forums. In Proceedings of the International Conference on Intelligence & Security Informatics (ISI), 319-321. (2016).

[21] Benjamin, V., Chung, W., Abbasi, A., Chuang, J., Larson, C. A., & Chen, H. Evaluating text visualization for authorship analysis. Security Informatics, 3(1), 10. (2014).

[22] Benjamin, V., Samtani, S., & Chen, H. Conducting 4 large-scale analyses of underground hacker communities. Cybercrime through an Interdisciplinary Lens, 26, (2016).

[23] Wenger, E. Communities of practice: Learning as a social system. Systems thinker, 9(5), 2-3. (1998).

[24] Wenger, E. C., & Snyder, W. M. Communities of practice: The Organizational Frontier. Harvard Business Review, 78(1), 139-146. (2000).

[25] Dupouët, O.: Le rôle des interactions entre structures formelles et informelles dans la firme. Une analyse en termes de communautés. Unpublished PhD dissertation. University Louis Pasteur – Strasbourg I. (2003)

[26] Cohen, W. M., & Levinthal, D. A. Absorptive capacity: A new perspective on learning and innovation. Administrative Science Quarterly, 35, 128–152. (1990).

[27] Muller, P. Reputation, trust and the dynamics of leadership in communities of practice. Journal of Management and Governance, 10(4), 381-400. (2006).

[28] Liu, Y.Y., Slotine, J.J. & Barabási, A.L. Controllability of complex networks, Nature, 473, (2011).

[29] Aggarwal, C. C. An introduction to social network data analytics. Social network data analytics, 1-15. (2011).

[30] Xu, J. & Chen, H. Criminal network analysis and visualization: a data mining perspective, in Communications of the ACM, 48(6), (2005).

[31] Wasko, M. M., & Faraj, S. Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. MIS Quarterly, 35-57. (2005).

[32] Wasko, M. M., Teigland, R., & Faraj, S. The provision of online public goods: Examining social structure in an electronic network of practice. Decision Support Systems, 47(3), 254-265. (2009).

[33] Zhang, J., Ackerman, M. S., & Adamic, L. Expertise networks in online communities: structure and algorithms. In Proceedings of the 16th International Conference on World Wide Web, 221-230. ACM. (2007).

[34] Bogenrieder, I., & Nooteboom, B. Learning groups: What types are there? A theoretical analysis and an empirical study in a consultancy firm. Organization studies, 25(2), 287-313. (2004).

[35] McPherson, M., Smith-Lovin, L., & Cook, J. M. Birds of a feather: Homophily in social networks. Annual review of sociology, 27(1), 415-444. (2001).

[36] Ansari, A., Koenigsberg, O., & Stahl, F. Modeling multiple relationships in social networks. Journal of Marketing Research, 48(4), 713-728. (2011).

[37] Braun, M., & Bonfrer, A. Scalable inference of customer similarities from interactions data using Dirichlet processes. Marketing Science, 30(3), 513-531. (2011).

[38] Bazarova, N. N., & Choi, Y. H. Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. Journal of Communication, 64(4), 635-657. (2014).

[39] Chávez, J., Montaño, R., & Barrera, R. Structure and content of messages in an online environment: An approach from participation. Computers in Human Behavior, 54, 560-568. (2016).

[40] Xu, J., Fedorowicz, J., & Williams, C. B. It's what you write and how you write about it: the Policing Facebook Experience. (2016).

[41] Hacker, J., Bernsmann, R., & Riemer, K. Dimensions of User Behavior in Enterprise Social Networks. Social Knowledge Management in Action, 125-146. Springer, (2017).

[42] Brotheridge, C. M., Neufeld, D. J., & Dyck, B. Communicating virtually in a global organization. Journal of Managerial Psychology, 30(8), 909-924. (2015).

[43] Siering, M., Koch, J. A., & Deokar, A. V. Detecting Fraudulent Behavior on Crowdfunding Platforms: The Role of Linguistic and Content-Based Cues in Static and Dynamic Contexts. Journal of Management Information Systems, 33(2), 421-455. (2016).

[44] Jiang, S., Chen, H., Nunamaker, J. F., & Zimbra, D. Analyzing firm-specific social media and market: A stakeholder-based event analysis framework. Decision Support Systems, 67, 30-39. (2014).

[45] Manning, C. D., Raghavan, P., & Schütze, H. Introduction to Information Retrieval, 1(1), 496, Cambridge University Press. Cambridge (2008).

[46] Walsh, J.P. Selectivity and selective perception: an investigation of managers' belief structures and information processing, Academy of Management Journal 31 (4), 873–896. (1988).

[47] Samtani. S. Hacker Web Forum Collection: Hackhound Forum Dataset. University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen. Available http://www.azsecure-data.org/ (2016)

[48] M. Thelwall, K. Buckley, G. Paltoglou, D. Cai, & A. Kappas, Sentiment strength detection in short informal text, Journal of the American Society for Information Science and Technology 61 (12), 2544–2558. (2010)

[49] D. Garcia, & F. Schweitzer, Emotions in product reviews — empirics and models, In Proceedings of IEEE International Conference on Privacy, Security, Risk, and Trust, pp. 483–488. (2011).

[50] Salehan, M., & Kim, D. J. Predicting the performance of online consumer reviews: A sentiment mining approach to big data analytics. Decision Support Systems, 81, 30-40. (2016).

[51] Pal, A., Farzan, R., Konstan, J., & Kraut, R. Early detection of potential experts in question answering communities. User Modeling, Adaption and Personalization, 231-242. (2011).

[52] Pal, A., Harper, F. M., & Konstan, J. A. Exploring question selection bias to identify experts and potential experts in community question answering. ACM Transactions on Information Systems (TOIS), 30(2), 10-20. (2012).

[53] Bouguessa, M., & Romdhane, L. B. Identifying authorities in online communities. ACM Transactions on Intelligent Systems and Technology (TIST), 6(3), 30-52. (2015).