Analysis Of Online Underground Market

Mingan Huang
Case Western Reserve University
Cleveland, US
mxh805@case.edu

Yanhan Lin
Case Western Reserve University
Cleveland, US
yxl1954@case.edu

Jiawei Xu
Case Western Reserve University
Cleveland, US
hxx334@case.edu

Jawad Adel A Kheyami
Case Western Reserve University
Cleveland, US
jxk11824@case.edu

ABSTRACT

Nowadays, many underground markets are emerging from the internet. These markets not only provide social contract within users, but also support some criminal activities. So to help the law enforcement communities to devise effective strategies, we need to gain deep insights of the underground markets. In this project, we collect the thread data from hack forums and analysed its representativeness. We first create our own criteria to choose key players, then we make some further analysis on them and add some manual selection to find the key players. Finally we concluded a storyline about the key players' trading network. And based on our insight of underground market, we introduce the countermeasures to our focused crimeware and CaaS.

KEYWORDS

Crimeware, CaaS, botnet, DDOS, Security, Storyline, Underground online market

ACM Reference Format:
Mingan Huang, Yanhan Lin, Jiawei Xu, and Jawad Adel A Kheyami. 2018. Analysis Of Online Underground Market. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

1.1 Background and motivation

In today's world, the use of technology has increased. Several websites offer valuable services for users for free and at the same time they try their best to collect users' information for improving their services. The effects of collecting user information may not be obvious for regular users, while for computer specialists and cyber criminals is very clear. This information could be used for several useful purposes such as, helping users' in making decisions, offering better services, and predicting users' needs. On the other hand, this information could be used for Distributing Denial of Service (DDoS) attacks, steal data, and send spam[4]. These threats could be avoided or limited with performing sufficient exploration of cyber criminal's activities.

Online underground market is a dark market that virtually gather individuals with interests in cyber-crimes[7]. The underground market contains many active users and most of them are considered as safe users, however; there are several users considered as cyber criminals who perform attacks and target others systems[12]. Several recent criminal attacks are made with the help of underground markets and their effects harmed many systems. Crime-as-a-Service (CaaS) is one of the crime models that have been used in underground market to allow underground buyers to perform cyber-crimes[12]. Using crimeware and CaaS cybercriminals have gotten a suitable environment for exchanging information, tools, and services with other criminals.

The increase of cybercrime parallels the development of underground markets, where attacking tools and services become easy to access at low cost or even for free[12]. To allow law enforcement communities to develop defenses aiming to prevent cybercrime, rather than stopping or recovering from; therefore, gaining deep insights into the underground ecosystem became an important. Similarly, the huge support of underground market to cybercriminals increased the need for investigating and analyzing cybercriminals activities to improve information security and data prevention.

In our project we performed deep data analysis to understand crimeware and CaaS that are supported in underground market. HackForums and Nulled are one of the most common underground markets that we have chosen to study in our project. HackForums is a website ranked as the second top hacking website that facilitate cybercrimes for criminals[1]. Nulled is also another common hacking website that describes itself as a hacking community for breaching data and steal information[9]. In our project we have done deep insights analysis for these two underground forums which facilitated gaining good understanding of their impact in cyberspace.

Botnets are a key factor in performing Distriputed-Denial-of-Service (DDoS) attacks for end systems, and in recent years Botnets attacks became one of the most dangerous attacks for cyber network [4]. Botnets have been used to reduce network resources, steal other person data, and harm their systems [4]. In our project we have studied Botnets and DDos attacks in details to analyze online underground market attacks, to distinguish cybercriminals, and to

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

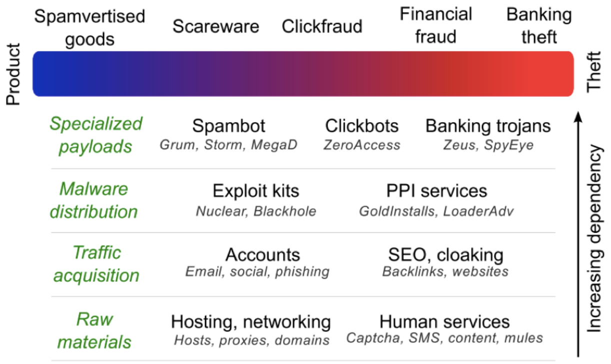


Figure 1: Taxonomy of underground actors

understand their characteristics. Furthermore, to investigate security threats related to Botnet and CaaS crimeware we have chosen in this project to analyze underground market using web scraping and collecting data such as, thread, comment, ID, replies and views from the underground market for our analysis. This study also facilitates understanding attackers' attitudes and behavior to create some useful solutions to lower and limit their crime attacks in the network.

1.2 Related Survey

The 21st century was the actual transformation of viruses spreading from individuals to collaborative organization and businesses. The essential cause of this transformation is the development of underground market that have become accompanying the growth of cybercrimes. Underground market became a fertile environment for gaining profit through exchanging criminal experience. This permits cybercriminals the opportunity to sell and buy crimeware and CaaS [16].

Underground market became very dangerous since it allows users to share illegal services such as cyber attacks, money laundering, and infections. Underground forums work by three actors. Firstly, underground producer who build CaaS and send the data to underground advertiser to distributie it in the underground market. Secondly, underground advertiser who work to publish CaaS information to all users. Thirdly, underground buyer who order crimeware services and pay for it then receive the crimeware [12].

The same article also talks about a taxonomy of underground market[12]. It separates the underground market into several levels, includes Specialized playloads, Malware distribution, Traffic acquisition, and Raw materials. And for each level, the market has corresponding elements to operate the whole crimeware network. For example, in order to distribute malware the market may use exploit kits or PPI service. They also argued about abuse irrespective of profit center for compromised hosts and basic human services, which helps us to get a better understanding of underground markets.

1.3 Research Goals

One of our main goals in the research is gaining a deep understanding of the relationship between underground ecosystems and cybercrimes. Similarly, studying crimware and CaaS that have been supported in underground forums. Furthermore, discussing the common characteristic of cybercriminals and key players in Hack-Forums and Nulled websites. Additionally, in this project we aim to examine Botnets and DDoS attacks involved in the ecosystem to have a better understanding of crimeware and CaaS.

2 DATASET CREATION

2.1 Tools

2.1.1 Web scraper. Web Scraper is a web site data extraction tool on Google Chrome. We could create our own plan (sitemap) how a website should be traversed and what data should be extracted by using this extension. It also has the feature to scrap multiple pages by using a well-designed sitemap, and the scraped data can be exported as CSV.

2.1.2 Rstudio. Rstudio is an open source IDE for R. It includes a console, syntax-highlighting editor that supports direct code execution, as well as tools for plotting, history, debugging and workspace management. It is also an open source software so that you can download any packages online depends on what you want to accomplish. In our project, we used Rstudio to do data annotation, related codes are in our "Source Codes" folder (Word.r and Denotation.r).

2.1.3 tm package in R. The tm package in R provides a text mining framework for R. The main structure for managing documents in tm is an abstract concept called Corpu[5], which represents a collection of text documents. In our project we could generate a new structure of documents by using Corpus so that it is possible for us to annotate our dataset automatically. Once we have corpus we usually want to modify the documents depends on what is our goal. In tm package, all functionalities of modification are related to the concept called "Transformation" [5], which are done by the "tm_map()" function in this package. As for our project, we utilize this function to find the frequencies of all words in comments.

2.1.4 SnowballC package in R. Snowball is an R interface to the C "libstemmer" library that implements Porter's word stemming algorithms. We also used this package in our data annotation.

2.1.5 Microsoft Excel. Excel is a common tool for data science.

2.2 Data Collection

Web Scraper was used to collect data from both hackforum and nulled. The general steps to use Web Scraper to scrape a webpage is as follows:

- Create a new sitemap with a name and the url of this webpage.
- Define different selectors level by level for the information you need.
- Preview the data at each level to make sure you get what you want when you finish the whole structure.
- Scrape the whole webpage.
- Export the data as a csv file.

The webpage was scrapped is the searching result on Hack Forum and Nulled. Each thread on this webpage has required keyword (e.g. Botnet or DDOS) in its title, and number of replies above 30 (defined as a condition in advanced search).

In order to correctly scrap the data we want, it is required to define selectors appropriately. There are many different types of selector on Web Scraper, the types were used in our project includes Text, Link, Element, and Element click. Text selector is for text information on the webpage; Link selector is for url on the webpage; Element selector is for multiple entries with the same type on the website (the crucial part to scrape every thread and comment); Element click is for some special webpage, which requires user to keep clicking "Load more" for more entries.

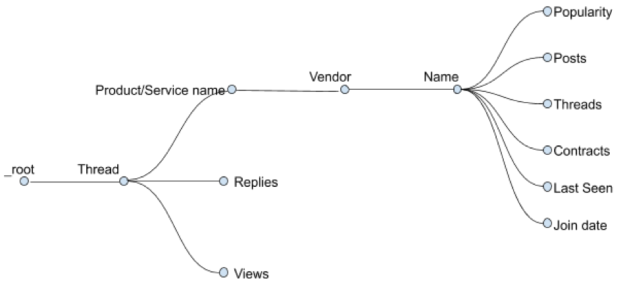


Figure 2: The selector graph for Web Scraper to collect threads data

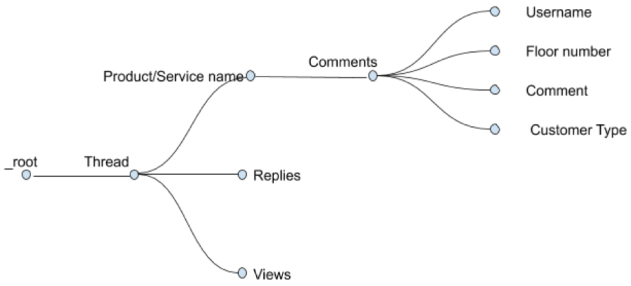


Figure 3: The selector graph for Web Scraper to collect comments data

Figure 2 is the selector graph of our sitemap to collect data of threads, besides the required information (Name, URL, Replies, Views), there are more additional information about the vendor, such as his or her popularity, contracts completed, which will be used for our criteria to pick our key vendors. Figure 3 is the selector graph of our sitemap to collect data of comments, in this figure "Product/Service name" is a Link selector, but for figure 2 "Vendor" is the Link selector. So for each thread, all data in it was collected includes every comment with corresponding username, floor number, customer type (will be used for our criteria to pick key buyer). Then we combined our data for Botnet and DDOS then processed it before the annotation.

Data processing:

- Manually add some required information (e.g. from which market, category of product)
- Sort the data according to the service or product, then sort according to the floor number (comments.xlsx only)
- Assign thread ID for each thread for both threads.xlsx and comments.xlsx
- Manually adjust data, includes removing redundant columns, adding the price, unit, and payment method for threads.xlsx

Challenges:

The challenging part for scraping is that you may get some redundant information, depends on the setup of this webpage; for example, we would like to get the number of popularity for a vendor, but what we have scrapped is "XXXX: number, XXXX". Our solution is to use regular expressions to specify what we want, such as "(?<=:)+̣" means every number after a ":". It is also a challenge to scrape the information of price, unit, and payment method, we tried to use regular expressions to solve this problem as well, but it did not come up with an appropriate result because these information are located on image. Therefore, we have to collect these information manually.

2.3 Data Dnnotation

We used Rstudio to annotate our data because R is a convenient language to deal with data. In order to annotate if the comment is a QA, we simply used R to check if there exists a "?" in the comment, and return 1 if true, 0 otherwise.

The annotation of trade and review are more complicated because there is no standard (a well defined standard such as "?" indicates a question) to define if it is a trade comment or a review for this thread. Our solution is to divide this problem into three steps:

- Using R to show the frequencies for each word in comments.xlsx.
- Choosing a list of words represents trade, a list of words represents positive review, and a list of words represents negative review.
- Using R to annotate each comment; if there exists any word in our "tradelist.csv", it will be annotated 1 for trade; if there exists any word in our "positivelist.csv", it will be annotated 1 for review; if there exists any word in our "negative.csv", it will be annotated -1 for review

One more thing to talk about is the logic to determine if this comment is a positive, negative, or neutral review. First, we annotate every comment as 0 (neutral). Then we check if there exists any word in our "positivelist.csv", and annotate 1 (positive) for a "True" return, otherwise do nothing. At the end, we check if there exists any word in our "negativelist.csv", and annotate -1 (negative) for a "True" return, otherwise do nothing. This logic is based on our assumption that negative reviews have the highest priority, positive reviews have the second highest priority, and neutral reviews have the lowest priority. In other words, our dataset is more negative-focused since a negative word could transform a review from positive to negative.

2.4 Data Set

This section includes some basic information about our dataset. Notice that these two tables only describe the information we collected from Hack forum, the data we collected from nulled were only used to analyze the distribution of comments because it only has a few threads that satisfied our requirements.

Table I shows that we have 171 threads in total, and 165 unique

Table 1: Dataset for threads

total entries	unique vendor	thread per vendor
171	165	1.04
replies per thread	views per thread	price per thread
115	5396	45

Table 2: dataset for comments

total entries	unique username	comment per user	Q&A per user
11739	3705	3.17	1.56
trade per user	positive review per user	negative review per user	
1.56	1.49	0.13	

vendors among these threads. Other information includes the average threads per vendor is 1.04, the average replies per thread is 115.56, the average views per thread 5420.91, and the average price per thread is 45.
Since we used advanced search (threads has more than 30 replies) on Hack forum before scraping the web page, thus all these threads are considered popular on Hack forum. The average price of these products is . . .

Table II shows that we have 11739 comments in total, and 3705 unique user among them. Other information includes the average comments per user is 3.17, the average Q&A comments per user is 1.56, the average trade comments per user is 1.56, the average positive reviews per user is 1.49, and the average negative reviews per user is 0.13. This table gives us some brief ideas about users. 3.17 comments per user means that either a user posts multiple comments on one thread or a user posts comments on different threads, and if it is the second case, these users could be our possible key buyers. 1.56 Q&A comment and 1.56 trade comment per user do not mean too much since the threads we collected are all located in premium markets (a section on Hack forum), users in this section tend to ask for products and buy products. 1.49 positive reviews per user and 0.13 negative reviews per user indicates that these products are reliable since users tend to post positive comments much more than negative comments.

3 ANALYSIS

3.1 Distribution Of Comments

After we got the data from web scraping, we made some analysis on our comments data. We first sorted the comments data by user name, then we made the pivot table of this column to count the number of each user's comments, and with the new data, we made the distribution graphs of different users and the number of their comments for the underground markets we studied. We also considered the influence of the thread's poster's own comments, we made the fan diagram of user and vendor's total comments number. As we can see from the Fig3.1.1, the vendor's own replies account for nearly 30 percent of the total comments, so it needs to be eliminated when showing distribution. Then we marked out those comments that have the same user names with the vendors and removed them, finally we got the data consisted of only users and made new distribution graphs with it.

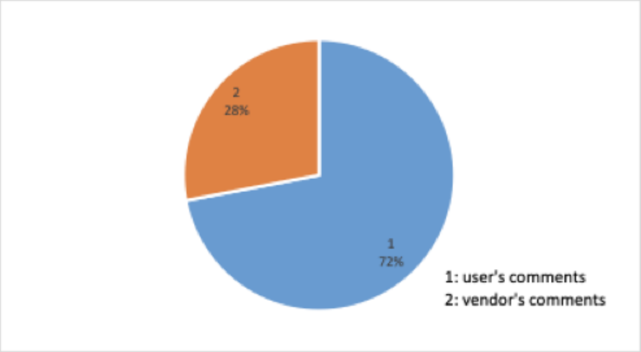


Figure 4: Ratio of user's and vendor's comments number from hack forum

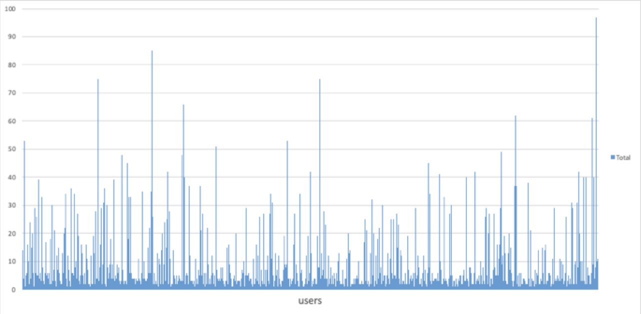


Figure 5: Distribution of user's comments from hack forum

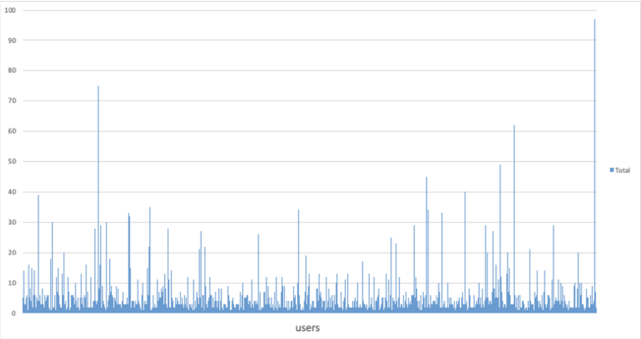


Figure 6: Distribution of user's comments from hack forum(vendor removed)

We also made distribution graphs of the data form nulled, but the available data is pretty small, so we won't choose it for later key player study. Through the figure 6 we can see that these large amounts of comments are posted by many different users, rather than just a few same users. So we make sure that our data has representativeness for later analysis. We can also see that there are many names that have high comments number removed in the second distribution graph Figure 6, which means basically vendors

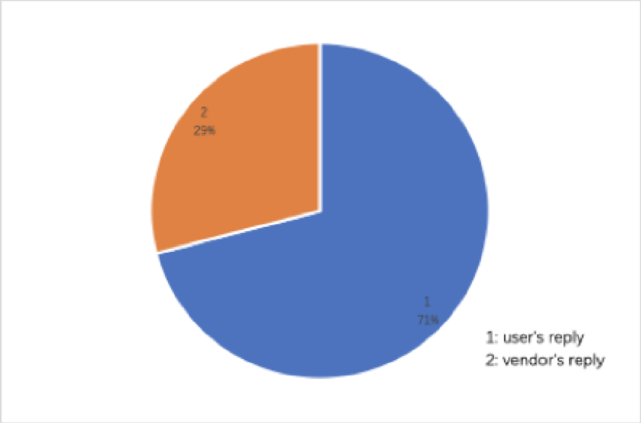


Figure 7: Ratio of user’s and vendor’s comments number from nulled

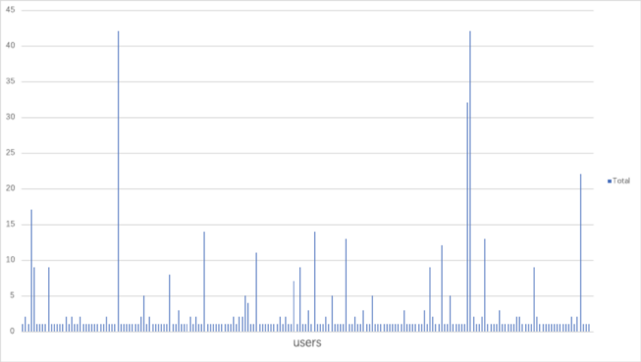


Figure 8: Distribution of user’s comments from nulled

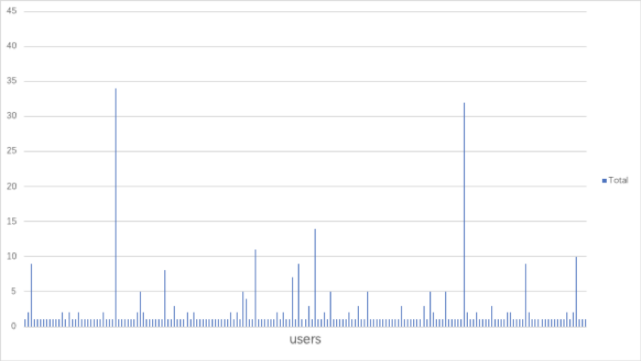


Figure 9: Distribution of user’s comments from nulled(vendor removed)

post more comments than users. And those remaining high comments number names also give us some insights, as they may be our potential key players.

3.2 Criteria To Pick Key Players

To gain deep insights into the underground market, we need to analyze the key players’ activities. Based on our previous data, we set the criteria to pick a key player. From the users’ profile that already scraped, we chose 5 parameters for the formula of key player score, they are popularity, post number, thread number, completed contracts number and user active time. For each parameter, we considered its impact on user’s activities, and appointed different factor K in the formula.

According to the available data, we made different criteria formulas for vendors and buyers.

Key vender formula:

$$S = M * \frac{K_1 * popularity + K_2 * posts + K_3 * threads + K_4 * contracts}{activetime}$$

For vendors we added another parameter M, which is a multiplier based on the frequency of selected products or services. Since the uses’ profile we collected is about the entire underground market, but our project focus is only botnet and DDoS. So even if some vendors’ participation in the whole underground market is low, they may still have high participation in our focused fields. By adding this parameter M, the score of vendors that provide both botnet and DDoS will increase relatively. For the value of factor K, we chose the completed contracts number to be the most important parameter, as it reflects the trades that actually happened. And we chose the popularity parameter to be the second important parameter, as high popularity means more likely to be advertised to potential buyers in the underground markets. And for the thread number and post number, some of the data is very large that will significantly influence the score, but we think post threads and comments may not directly lead to key activities in underground markets, so we applied them a relatively small factor. To make it more fair between vendors who have different active time in underground market , we summed all these parts together and divided it by each vendor’s active time.

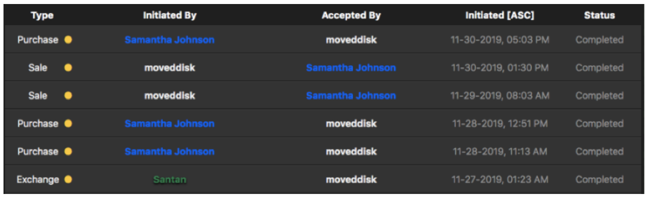
Key buyer formula:

$$S = \frac{K_1 * popularity + K_2 * posts + K_3 * threads + K_4 * contracts}{activetime}$$

Then for buyers, we noticed that there is an information in the profile about whether this user is a contracted customer. Key buyers should have multiple times of trade, so we chose to select our key buyers from these contracted buyers. And we also traced the trade history of some top key vendors, try to figure out whether some of his closest buyers are also key buyers.

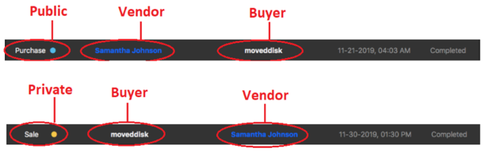
3.3 Transaction Records

The transaction record is one of the most important evidence among the online underground markets, it provided a lot of information about the activities in this market, which is our primary source to generate a storyline. Figure 10 shows the transaction record of user “moveddisk”; the type shows if this transaction is a purchase, sale, or exchange; the initiator shows who initiates this transaction and the acceptor shows who accepts this transaction; transaction time and status are also included in a transaction record. The challenge to analyze the transaction records is that a type “Purchase” does not mean the user (who holds these records) is a buyer, and a type “Sale” does not mean this user is a vendor. Figure 26 shows a solution for this problem, it indicates that if the type is “Purchase”, the initiator is a vendor, and the acceptor is a buyer; while if the type is “Sale”,



Type	Initiated By	Accepted By	Initiated [ASC]	Status
Purchase ●	Samantha Johnson	moveddisk	11-30-2019, 05:03 PM	Completed
Sale ●	moveddisk	Samantha Johnson	11-30-2019, 01:30 PM	Completed
Sale ●	moveddisk	Samantha Johnson	11-29-2019, 08:03 AM	Completed
Purchase ●	Samantha Johnson	moveddisk	11-28-2019, 12:51 PM	Completed
Purchase ●	Samantha Johnson	moveddisk	11-28-2019, 11:13 AM	Completed
Exchange ●	Santan	moveddisk	11-27-2019, 01:23 AM	Completed

Figure 10: An example of transaction records



Purchase ●	Samantha Johnson	moveddisk	11-21-2019, 04:03 AM	Completed
Sale ●	moveddisk	Samantha Johnson	11-30-2019, 01:30 PM	Completed

Figure 11: Result of transaction analysis

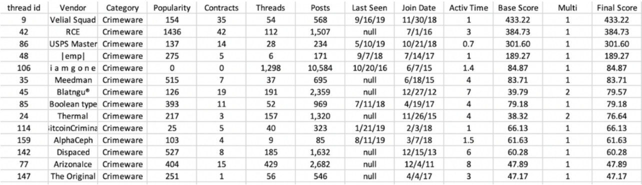
the initiator is a buyer and the acceptor is a vendor. The color next to "Type" indicates if this transaction is public or private.

3.4 Key Players

A rank of vendor for Botnet is generated based on our criteria (as figure 12), the final score is the product of base score times the multiplier (mentioned in 3.2). We did not choose the vendor with the highest score, which is "Velial Squad", as our key vendor for Botnet because this vendor closed his account on Hack Forum recently. The vendor with the second highest score may also be a good choice, which is "RCE", however this user has a huge social network and he has too much contracts to analyze. In order to have a complete storyline for a key player, we selected the vendor "Meedman", who ranked in 6th place, has the second highest popularity but reasonable number of contracts.

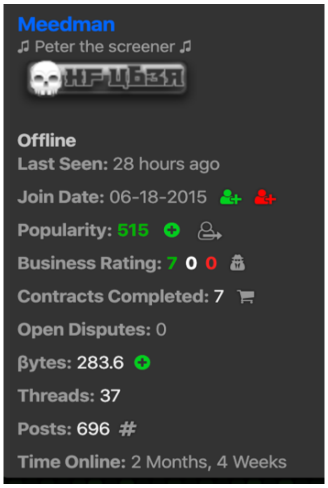
- Botnet vendor: Meedman
- Individual or organization: Organization
- Products selling: Botnet, Web Scanner, Virtual Crypt
- Influence in the market: provide multiple services, provide help, vouch for other sellers
- Activity in another market: None

According to Figure 14, "Meedman" has a reply said that "we just finish a market campaign with . . . ", which indicates that he belongs to an organization. There are also other replies from him show that he is appreciated for some customers who bought their product. Then we found some other products "Meedman" is selling according to his profile page, such as Web Scanner and Virtual Crypt. Afterwards, we analyzed his bio box for all recent threads and posts on Hack Forum. Several evidence were found (Figure 15 and Figure 16) to illustrate his influence in the market, includes providing compensable service, being a middleman between vendor and buyer, and recommending other sellers. We tried to find if "Meedman" is also active in another market, but there is no result showing the same username on other markets.



thread id	Vendor	Category	Popularity	Contracts	Threads	Posts	Last Seen	Join Date	Activ Time	Base Score	Multi	Final Score
9	Velial Squad	Crimeware	154	35	54	568	9/16/19	11/30/18	1	433.22	1	433.22
42	RCE	Crimeware	1436	42	112	1,507	null	7/1/16	3	384.73	1	384.73
86	USPS Master	Crimeware	137	14	28	234	5/10/19	10/21/18	0.7	301.60	1	301.60
48	|emp|	Crimeware	275	5	6	171	9/7/18	7/14/17	1	189.27	1	189.27
106	i a m g o n e	Crimeware	0	0	1,298	10,584	10/20/16	6/7/15	1.4	84.87	1	84.87
35	Meedman	Crimeware	515	7	37	695	null	6/18/15	4	83.71	1	83.71
45	Blatngu®	Crimeware	126	19	191	2,359	null	12/27/12	7	39.79	2	79.57
85	Boolean type	Crimeware	393	11	52	969	7/11/18	4/19/17	4	79.18	1	79.18
24	Thermal	Crimeware	217	3	157	1,320	null	11/26/15	4	38.32	2	76.64
114	꞉itcoinCrimina	Crimeware	25	5	40	323	1/21/19	2/3/18	1	66.13	1	66.13
159	AlphaCeph	Crimeware	103	4	9	85	8/11/19	3/7/18	1.5	61.63	1	61.63
142	Dispaced	Crimeware	527	8	185	1,632	null	12/15/13	6	60.28	1	60.28
77	ArizonaIce	Crimeware	404	15	429	2,682	null	12/4/11	8	47.89	1	47.89
147	The Original	Crimeware	251	1	56	546	null	4/4/17	3	47.17	1	47.17

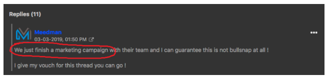
Figure 12: Rank of vendor for Botnet



Meedman
♫ Peter the screener ♫

Offline
Last Seen: 28 hours ago
Join Date: 06-18-2015
Popularity: 515
Business Rating: 7 0 0
Contracts Completed: 7
Open Disputes: 0
βytes: 283.6
Threads: 37
Posts: 696 #
Time Online: 2 Months, 4 Weeks

Figure 13: Meedman's information



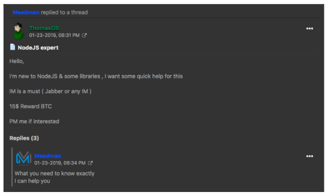
Replies (11)

Meedman
03-03-2019, 01:50 PM

We just finish a marketing campaign with their team and I can guarantee this is not bullsnap at all !

I give my vouch for this thread you can go !

Figure 14: Meedman's reply to a thread



Meedman replied to a thread

ThomasGB
01-23-2019, 08:31 PM

NodeJS expert

Hello,

I'm new to NodeJS & some libraries , I want some quick help for this

IM is a must (Jabber or any IM)

15$ Reward BTC

PM me if interested

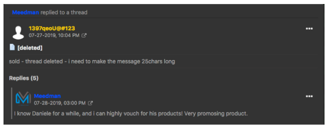
Replies (3)

Meedman
01-23-2019, 08:34 PM
What you need to know exactly
I can help you

Figure 15: Meedman's reply to a thread to provide help

Another rank of contracted buyer for Botnet is generated based on our criteria. Different from the vendor, the rank is not the only basis of choosing an active buyer. We tried to find is there any relationship between the key vendor we chose and the buyer in this list. According to the transaction of "Meedman", we found that a "moveddisk" is a buyer of "Meedman" and another active vendor in our list called "Blatngu", the details will be discussed in our storyline.

- Botnet buyer: moveddisk
- Individual or organization: Individual
- Individual or organization: Botnet, Amazon gift cards



Meedman replied to a thread

1397qeoU@#123
07-27-2019, 10:04 PM

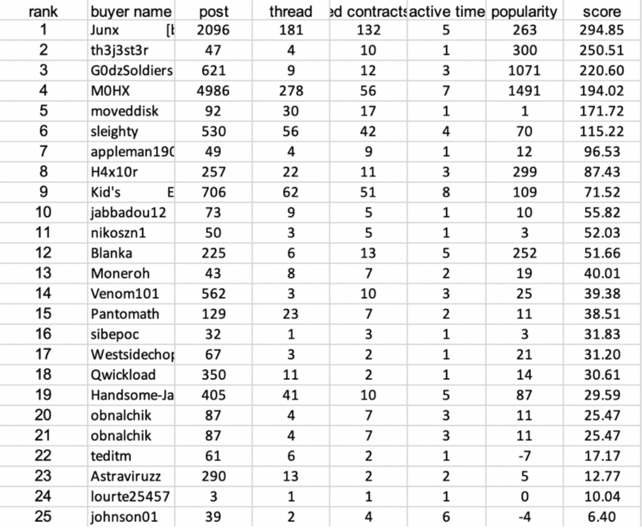
[deleted]

sold - thread deleted - i need to make the message 25chars long

Replies (5)

Meedman
07-28-2019, 03:00 PM
I know Daniele for a while, and i can highly vouch for his products! Very promosing product.

Figure 16: Meedman's reply to a thread to vouch for another seller



rank	buyer name	post	thread	ed contracts	active time	popularity	score
1	Junx [t	2096	181	132	5	263	294.85
2	th3j3st3r	47	4	10	1	300	250.51
3	G0dzSoldiers	621	9	12	3	1071	220.60
4	M0HX	4986	278	56	7	1491	194.02
5	moveddisk	92	30	17	1	1	171.72
6	sleighty	530	56	42	4	70	115.22
7	appleman19(	49	4	9	1	12	96.53
8	H4x10r	257	22	11	3	299	87.43
9	Kid's E	706	62	51	8	109	71.52
10	jabbadou12	73	9	5	1	10	55.82
11	nikoszn1	50	3	5	1	3	52.03
12	Blanka	225	6	13	5	252	51.66
13	Moneroh	43	8	7	2	19	40.01
14	Venom101	562	3	10	3	25	39.38
15	Pantomath	129	23	7	2	11	38.51
16	sibepoc	32	1	3	1	3	31.83
17	Westsidechop	67	3	2	1	21	31.20
18	Qwickload	350	11	2	1	14	30.61
19	Handsome-Ja	405	41	10	5	87	29.59
20	obnalchik	87	4	7	3	11	25.47
21	obnalchik	87	4	7	3	11	25.47
22	teditm	61	6	2	1	-7	17.17
23	Astraviruzz	290	13	2	2	5	12.77
24	lourte25457	3	1	1	1	0	10.04
25	johnson01	39	2	4	6	-4	6.40

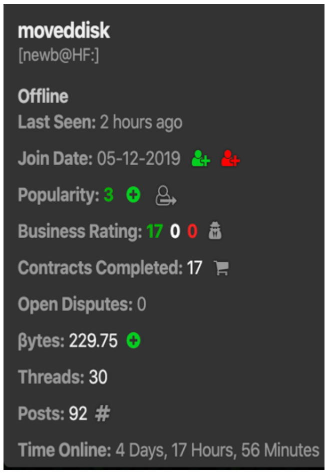
Figure 17: Rank of buyer for Botnet

- Influence in the market: vouch for other sellers, try to re-sell botnet to others
- Activity in another market: None

There is no evidence shows that "moveddisk" belongs to an organization. According to his transaction records (Figure 19), we found some other products he bought from Hack Forum, most of them are Amazon gift cards. He vouches for some sellers on Hack Forum just like most buyers, and we also found that he tried to re-sell Botnet, which he bought from "Meedman" and "Blatngu", the details will be discussed in our storyline. Moreover, there is no evidence shows that he has activity in another market.

For key vendors of DDoS, we also applied the formula to the comments data and got a ranked list of high score vendors (Figure 20). We eliminated those vendors whose contracts number is too low or whose accounts already closed. We also traced the buyers of these vendors, the popularity of vendors' buyer are quite different, we chose the Blatngu as our key vendor for DDoS, as many of his buyers are very active in underground markets.

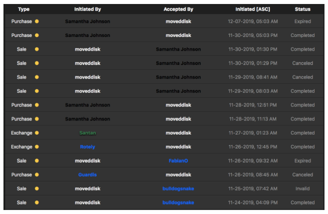
- DDOS vendor:Blatgn
- Individual or organization: individual
- Products selling:bot shop setup, automation
- Influence in the market: vouch for other sellers, reselling others' products
- Activity in another market:none



moveddisk
[newb@HF:]

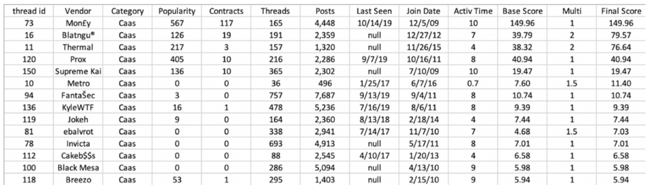
Offline
Last Seen: 2 hours ago
Join Date: 05-12-2019
Popularity: 3
Business Rating: 17 0 0
Contracts Completed: 17
Open Disputes: 0
βytes: 229.75
Threads: 30
Posts: 92
Time Online: 4 Days, 17 Hours, 56 Minutes

Figure 18: Moveddisk's information



Type	Initiated By	Accepted By	Initiated [ASC]	Status
Purchase ●	Samantha Johnson	moveddisk	12-07-2019, 05:03 AM	Expired
Purchase ●	Samantha Johnson	moveddisk	11-30-2019, 05:03 PM	Completed
Sale ●	moveddisk	Samantha Johnson	11-30-2019, 01:30 PM	Completed
Sale ●	moveddisk	Samantha Johnson	11-30-2019, 01:29 PM	Canceled
Sale ●	moveddisk	Samantha Johnson	11-29-2019, 08:41 AM	Canceled
Sale ●	moveddisk	Samantha Johnson	11-29-2019, 08:03 AM	Completed
Purchase ●	Samantha Johnson	moveddisk	11-28-2019, 12:51 PM	Completed
Purchase ●	Samantha Johnson	moveddisk	11-28-2019, 11:13 AM	Completed
Exchange ●	Santan	moveddisk	11-27-2019, 01:23 AM	Completed
Exchange ●	Rotely	moveddisk	11-26-2019, 12:45 PM	Completed
Sale ●	moveddisk	FabianO	11-26-2019, 09:32 AM	Expired
Purchase ●	Guardis	moveddisk	11-26-2019, 08:45 AM	Canceled
Sale ●	moveddisk	bulldogsnake	11-25-2019, 07:42 AM	Invalid
Sale ●	moveddisk	bulldogsnake	11-24-2019, 04:09 PM	Completed

Figure 19: Moveddisk's information



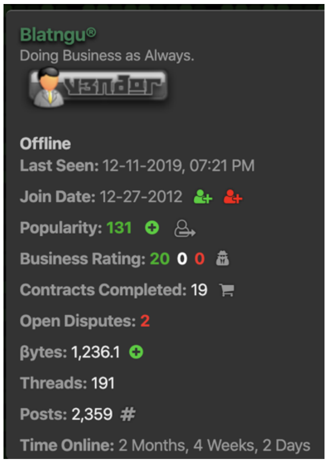
thread id	Vendor	Category	Popularity	Contracts	Threads	Posts	Last Seen	Join Date	Activ Time	Base Score	Multi	Final Score
73	Mon£y	Caas	567	117	165	4,448	10/14/19	12/5/09	10	149.96	1	149.96
16	Blatngu®	Caas	126	19	191	2,359	null	12/27/12	7	39.79	2	79.57
11	Thermal	Caas	217	3	157	1,320	null	11/26/15	4	38.32	2	76.64
120	Prox	Caas	405	10	216	2,286	9/7/19	10/16/11	8	40.94	1	40.94
150	Supreme Kai	Caas	136	10	365	2,302	null	7/10/09	10	19.47	1	19.47
10	Metro	Caas	0	0	36	496	1/25/17	6/7/16	0.7	7.60	1.5	11.40
94	FantaŠec	Caas	3	0	757	7,687	9/13/19	9/4/11	8	10.74	1	10.74
136	KyleWTF	Caas	16	1	478	5,236	7/16/19	8/6/11	8	9.39	1	9.39
119	Jokeh	Caas	9	0	164	2,360	8/13/18	2/18/14	4	7.44	1	7.44
81	ebalvrot	Caas	0	0	338	2,941	7/14/17	11/7/10	7	4.68	1.5	7.03
78	Invicta	Caas	0	0	693	4,913	null	5/17/11	8	7.01	1	7.01
112	Cakeb$$s	Caas	0	0	88	2,545	4/10/17	1/20/13	4	6.58	1	6.58
100	Black Mesa	Caas	0	0	286	5,094	null	4/13/10	9	5.98	1	5.98
118	Breezo	Caas	53	1	295	1,403	null	2/15/10	9	5.94	1	5.94

Figure 20: Rank of vendor for DDOS

As for whether Blatngu is an individual or an organization, we traced all of Blatngu's posts. According to Figure 23, we found that he replied to a group recruit as an individual, so he is an individual. And he is very active in the underground markets, besides ddos service, he also provides lots of other services, such as bot shop setup and automation, web developing. We also found Blatngu vouched for many other sellers, including another top score vendor Mon£y(Figure 24), and he posted lots of threads for reselling products he bought from other sellers.

As for the selection of key buyer of DDoS, because all of this kind of buyers haven't contracted vendors before, so we just traced the trade history of several top high scores vendors, and collected the buyer profile of these venders. Then we applied our formula to get the buyer's rank. Although some buyers have very high contracts number, we found their contracts are mainly about currency exchange rather DDoS and we did not choose this kind of buyers.

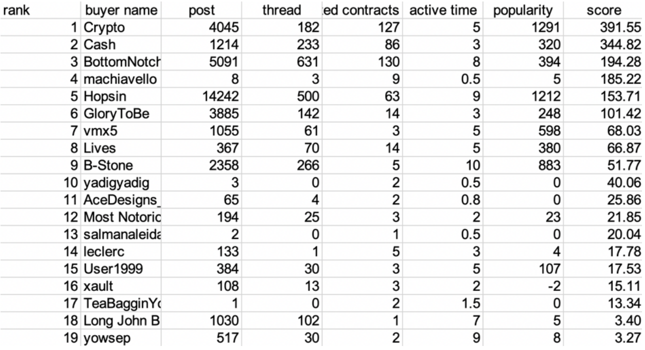
- DDOS buyer:BottomNotch
- Individual or organization:individual
- Products buying: DDoS, amazon gift cards



Blatngu®
Doing Business as Always.

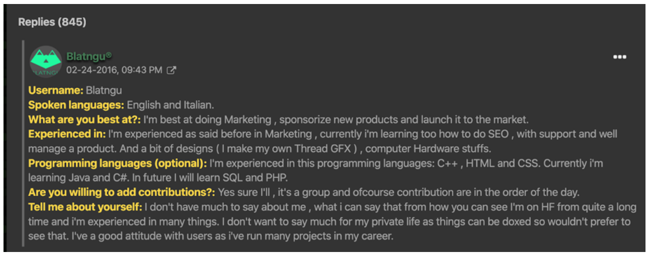
Offline
Last Seen: 12-11-2019, 07:21 PM
Join Date: 12-27-2012
Popularity: 131
Business Rating: 20 0 0
Contracts Completed: 19
Open Disputes: 2
βytes: 1,236.1
Threads: 191
Posts: 2,359 #
Time Online: 2 Months, 4 Weeks, 2 Days

Figure 21: key vendor for DDOS



rank	buyer name	post	thread	ed contracts	active time	popularity	score
1	Crypto	4045	182	127	5	1291	391.55
2	Cash	1214	233	86	3	320	344.82
3	BottomNotch	5091	631	130	8	394	194.28
4	machiavello	8	3	9	0.5	5	185.22
5	Hopsin	14242	500	63	9	1212	153.71
6	GloryToBe	3885	142	14	3	248	101.42
7	vmx5	1055	61	3	5	598	68.03
8	Lives	367	70	14	5	380	66.87
9	B-Stone	2358	266	5	10	883	51.77
10	yadigyadig	3	0	2	0.5	0	40.06
11	AceDesigns_	65	4	2	0.8	0	25.86
12	Most Notoric	194	25	3	2	23	21.85
13	salmanaleida	2	0	1	0.5	0	20.04
14	leclerc	133	1	5	3	4	17.78
15	User1999	384	30	3	5	107	17.53
16	xault	108	13	3	2	-2	15.11
17	TeaBagginYc	1	0	2	1.5	0	13.34
18	Long John B	1030	102	1	7	5	3.40
19	yowsep	517	30	2	9	8	3.27

Figure 22: Rank of buyer for DDoS

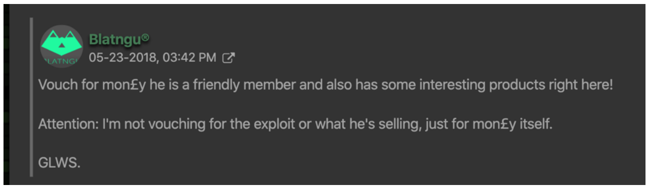


Replies (845)

Blatngu®
02-24-2016, 09:43 PM

Username: Blatngu
Spoken languages: English and Italian.
What are you best at?: I'm best at doing Marketing , sponsorize new products and launch it to the market.
Experienced in: I'm experienced as said before in Marketing , currently i'm learning too how to do SEO , with support and well manage a product. And a bit of designs (I make my own Thread GFX) , computer Hardware stuffs.
Programming languages (optional): I'm experienced in this programming languages: C++ , HTML and CSS. Currently i'm learning Java and C#. In future I will learn SQL and PHP.
Are you willing to add contributions?: Yes sure I'll , it's a group and ofcourse contribution are in the order of the day.
Tell me about yourself: I don't have much to say about me , what i can say that from how you can see I'm on HF from quite a long time and i'm experienced in many things. I don't want to say much for my private life as things can be doxed so wouldn't prefer to see that. I've a good attitude with users as i've run many projects in my career.

Figure 23: Blatngu's reply to a group recruit



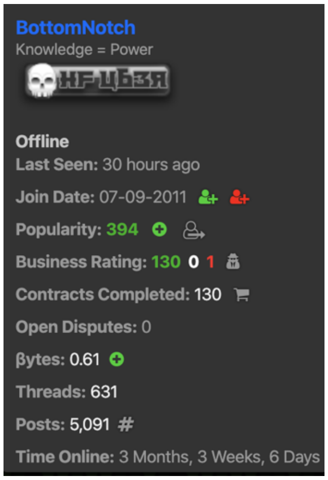
Blatngu®
05-23-2018, 03:42 PM

Vouch for mon£y he is a friendly member and also has some interesting products right here!

Attention: I'm not vouching for the exploit or what he's selling, just for mon£y itself.

GLWS.

Figure 24: Blatngu vouched for another top vendor



BottomNotch
Knowledge = Power

Offline
Last Seen: 30 hours ago
Join Date: 07-09-2011
Popularity: 394
Business Rating: 130 0 1
Contracts Completed: 130
Open Disputes: 0
βytes: 0.61
Threads: 631
Posts: 5,091 #
Time Online: 3 Months, 3 Weeks, 6 Days

Figure 25: key buyer for DDOS

- Influence in the market: vouch for sellers, currency exchange
- Activity in another market: none

3.5 Storyline

We concluded a storyline for the key player "Meedman" based on transaction records, user's bio box, posts and replies. I will further explain each connection in detail and the evidence related to it. Figure 27 shows the transaction between "Meedman" and a user called "Secret Agent", this record shows that "Meedman" has bought rep, which is popularity, from "Secret Agent" on June 12th 2018. This record only indicates "Meedman" has purchased popularity from "Secret Agent" once, but we do not know if there exist any more private transaction between them. It is reasonable to have this doubt because the transaction record of "Secret Agent" Figure 28 shows that he sold popularity to many vendors in this market, what is the point for these vendors to buy only 3 popularity? Because of the trade of popularity on Hack Forum, we decided to lower the K value for popularity in our criteria (mentioned in 3.2). Since the profit of this trade is pretty low, we have an arrow to show the low profit flow from "Meedman" to "Secret Agent". Next it is the flow from a vendor "Frenchy" to our key player "Meedman", which is inferred by 29. This screenshot shows "Meedman" replied to "Frenchy's" thread of C++ crypting service. Moreover, this product allows the crime to have the ability to bypass anti-malware software, which is significant for Botnet. From the reply of "Meedman", he said that he knows "Frenchy" for five years, but there is no information to indicate that they belong to the same organization. This crypting service is sold for $80 BTC, which is lower than the price of "Meedman's" Botnet ($200)". Thus, we have an arrow to show the medium profit flow from "Meedman" to "Frenchy". Then it is our main target Botnet, there is a flow from "Meedman" to "moveddisk", recall that "moveddisk" is our key buyer for Botnet (3.3). The price is $200 BTC according to Figure 30. Furthermore, there is another vendor "Blatngu" (who has a high rank in both Botnet and DDOS list) selling Botnet to "moveddisk" based on 31. We assigned another two arrows to show the high profit flow from "moveddisk" to these two vendors. One interesting part I mentioned in key players

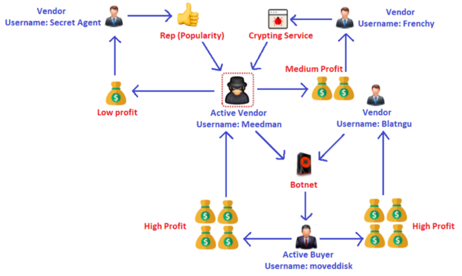
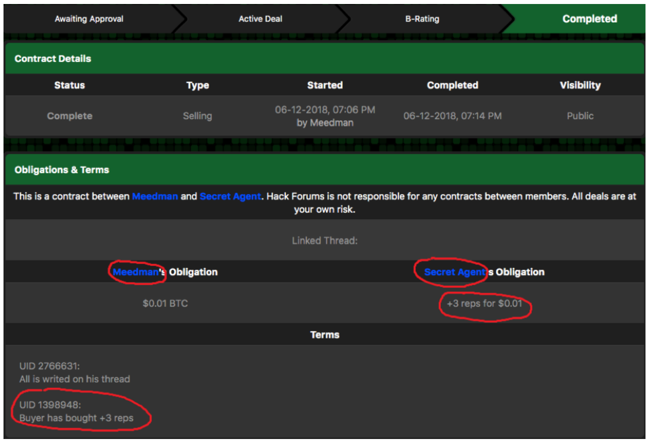


Figure 26: The Storyline of our key player



Awaiting Approval	Active Deal	B-Rating	Completed

Contract Details

Status	Type	Started	Completed	Visibility
Complete	Selling	06-12-2018, 07:06 PM by Meedman	06-12-2018, 07:14 PM	Public

Obligations & Terms

This is a contract between Meedman and Secret Agent. Hack Forums is not responsible for any contracts between members. All deals are at your own risk.

Linked Thread:

Meedman's Obligation	Secret Agent's Obligation
$0.01 BTC	+3 reps for $0.01

Terms

UID 2766631:
All is writed on his thread

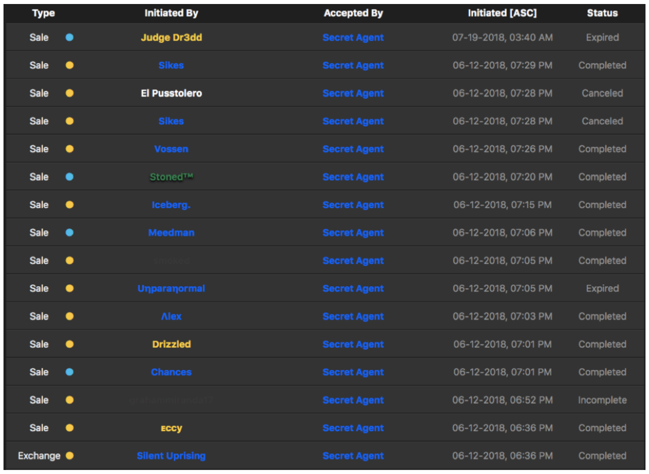
UID 1398948:
Buyer has bought +3 reps

Figure 27: Transaction record between Meedman and Secret Agent. Meedman is the buyer and Secret Agent is the vendor

(3.4) is that “moveddisk” tried to re-sell the Botnet he bought from these two vendors. Unfortunately, he deleted this thread and we were not able to find any transaction record about it; but some new information about this may appear in the future, which means that we could further develop our storyline about these key players.

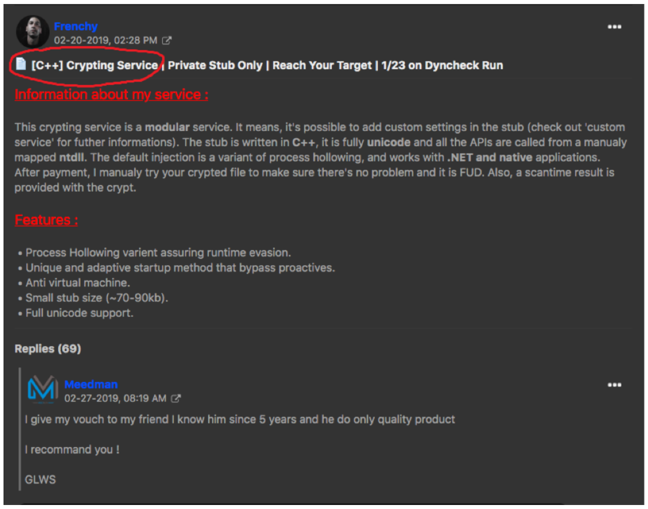
3.6 Limitations

The most significant limitations in our analysis of online underground market relate to some legal aspects. In other words, our methods are constrained by the conflict between the right to privacy and the right to information. In order to further analyze our key players, we need to check their profile, traverse their history of social activities, and navigate each transaction record from them. All this information can be considered as their private information on Hack Forum. In addition, we may need information about their bank account to analyze the cash flow and trade process. This information is definitely private either in real life or on the internet. There is another concern in our Key players part (3.4) that we were not able to find the same username on different markets. It does not mean that these key players are only active on Hack Forum because they may use a different username on another market. In order to find out the relationship between two different usernames, one robust way is to check the IP addresses. But the IP



Type	Initiated By	Accepted By	Initiated [ASC]	Status
Sale ●	Judge Dr3dd	Secret Agent	07-19-2018, 03:40 AM	Expired
Sale ●	Sikes	Secret Agent	06-12-2018, 07:29 PM	Completed
Sale ●	El Pusstolero	Secret Agent	06-12-2018, 07:28 PM	Canceled
Sale ●	Sikes	Secret Agent	06-12-2018, 07:28 PM	Canceled
Sale ●	Vossen	Secret Agent	06-12-2018, 07:26 PM	Completed
Sale ●	Stoned™	Secret Agent	06-12-2018, 07:20 PM	Completed
Sale ●	Iceberg.	Secret Agent	06-12-2018, 07:15 PM	Completed
Sale ●	Meedman	Secret Agent	06-12-2018, 07:06 PM	Completed
Sale ●	smoked	Secret Agent	06-12-2018, 07:05 PM	Completed
Sale ●	Uηparaηormal	Secret Agent	06-12-2018, 07:05 PM	Expired
Sale ●	Λlex	Secret Agent	06-12-2018, 07:03 PM	Completed
Sale ●	Drizzled	Secret Agent	06-12-2018, 07:01 PM	Completed
Sale ●	Chances	Secret Agent	06-12-2018, 07:01 PM	Completed
Sale ●	grahammiranda17	Secret Agent	06-12-2018, 06:52 PM	Incomplete
Sale ●	ᴇccy	Secret Agent	06-12-2018, 06:36 PM	Completed
Exchange ●	Silent Uprising	Secret Agent	06-12-2018, 06:36 PM	Completed

Figure 28: Transaction record of Secret Agent



Frenchy
02-20-2019, 02:28 PM

[C++] Crypting Service | Private Stub Only | Reach Your Target | 1/23 on Dyncheck Run

Information about my service :

This crypting service is a **modular** service. It means, it's possible to add custom settings in the stub (check out 'custom service' for futher informations). The stub is written in **C++**, it is fully **unicode** and all the APIs are called from a manualy mapped **ntdll**. The default injection is a variant of process hollowing, and works with **.NET and native** applications. After payment, I manualy try your crypted file to make sure there's no problem and it is FUD. Also, a scantime result is provided with the crypt.

Features :

- Process Hollowing varient assuring runtime evasion.
- Unique and adaptive startup method that bypass proactives.
- Anti virtual machine.
- Small stub size (~70-90kb).
- Full unicode support.

Replies (69)

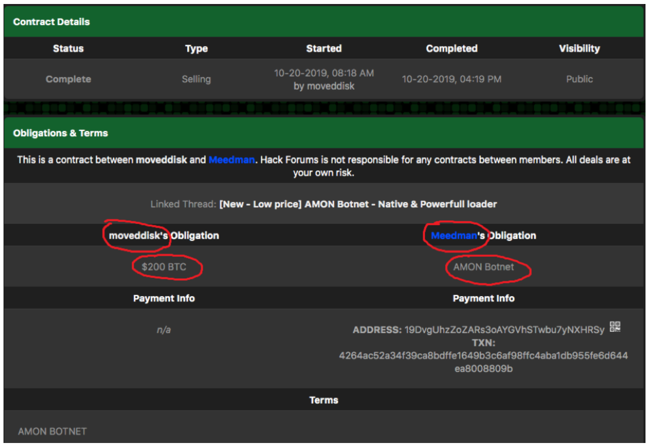
Meedman
02-27-2019, 08:19 AM

I give my vouch to my friend I know him since 5 years and he do only quality product

I recommand you !

GLWS

Figure 29: Transaction record of Secret Agent



Contract Details

Status	Type	Started	Completed	Visibility
Complete	Selling	10-20-2019, 08:18 AM by moveddisk	10-20-2019, 04:19 PM	Public

Obligations & Terms

This is a contract between moveddisk and Meedman. Hack Forums is not responsible for any contracts between members. All deals are at your own risk.

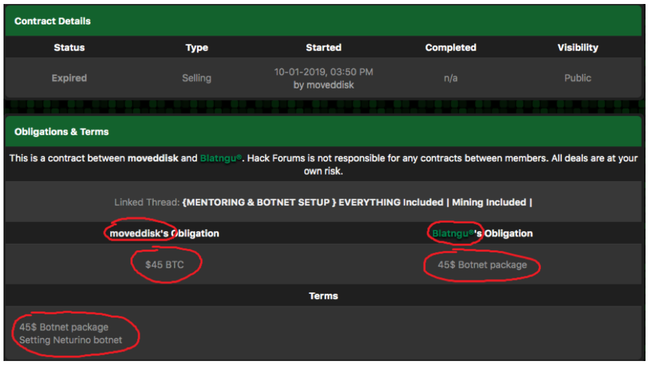
Linked Thread: **[New - Low price] AMON Botnet - Native & Powerfull loader**

moveddisk's Obligation	Meedman's Obligation
$200 BTC	AMON Botnet
Payment Info	**Payment Info**
n/a	ADDRESS: 19DvgUhzZoZARs3oAYGVhSTwbu7yNXHRSy TXN: 4264ac52a34f39ca8bdffe1649b3c6af98ffc4aba1db955fe6d644ea8008809b

Terms

AMON BOTNET

Figure 30: Transaction record between moveddisk and Meedman. Meedman is the vendor and moveddisk is the buyer



Contract Details

Status	Type	Started	Completed	Visibility
Expired	Selling	10-01-2019, 03:50 PM by moveddisk	n/a	Public

Obligations & Terms

This is a contract between **moveddisk** and Blatngu®. Hack Forums is not responsible for any contracts between members. All deals are at your own risk.

Linked Thread: **{MENTORING & BOTNET SETUP } EVERYTHING Included | Mining Included |**

moveddisk's Obligation	Blatngu®'s Obligation
$45 BTC	45$ Botnet package

Terms

45$ Botnet package
Setting Neturino botnet

Figure 31: Transaction record between moveddisk and Blatngu. Blatngu is the vendor and moveddisk is the buyer

addresses are personal data supported by laws in some countries, such as Switzerland[2] and Sweden[3]. Their main focus is that each user in these areas are not allowed to be identified through the combination of a timestamp and an IP address.

4 COUNTERMEASURES

Various countermeasures to the botnet and DDOS threat have been founded and applied. They are approximately divided into two parts: technical approaches and social and regulatory approaches.

4.1 Technical Approaches To Botnet

The approaches to the botnet presented in this section apply at technical level. Command-and-control infrastructure of botnet is point of these approaches. For instance, filtering botnet-related traffic, sinkholing domains with the assistance of DNS registrars or obtaining the shutdown of malicious servers in data centers. One of considerations is that taking down of the command-and-control infrastructure do infect the complicated machines in the botnet, which means the infections that remain can cause severe security issues[8]. Moreover, one possibility exists in there is that this activity may continue until other measures are taken to interrupt if bots have received commands that require others to stop their actions [8].

4.1.1 Blacklisting. blacklisting as a supporting process instead of a direct countermeasure against botnet which provides input for further technical means of resistance[8]. A blacklist contains multifaceted and various parties from different sectors. It can be used to provide single IP addresses of malicious hosts or whole subnets containing suspicious activities. On the other hand, it also can be applied to block all traffic from included addresses. Furthermore, a collection of URLs in blacklist can be used by search engines, or a browser is to filter or mark websites with suspicious contents[8]. Some systems or tools are developed to improve blacklisting technology like SpamTracker, which uses behavioral blacklisting to classify email senders by their detailed behavior[10].

4.1.2 DNS-based countermeasures. DNS based countermeasures is other approach we are going to describe in this section. Many malwares samples use fixed domain names as identifiers for their underlying C&C infrastructure due to the type of botnet, which is included by compromised hosts[8]. Actually, a domain should be shut down by the responsible register if its name can be found to be related to malware, and it has been established for malicious purpose only. However, the act of shutting down a domain still exists various dependencies[8]. Therefore, this approach cannot be applied if a botnet uses a legitimate domain or service to perform its communication.

4.1.3 Port Blocking. Port blocking is a preventive approach that can be applied by ISPs to reducing the amount of spam mails traversing their network. A network processor has various processing elements supporting multiple simultaneous program threads with access to shared resources[17]. It means that the port or connection on user's computer through which outgoing email must pass. More than 87% of all emails are spam[8]. One destination of method is to mitigate this threat. Port blocking is based on the assumption that use of unauthenticated service via port 25[8]. In many cases, blocking port 25 at ISP level has been recommended and applied as best practice by the Messaging Anti-Abuse Working Group(MAAWG) since 2005[8]. Additionally, any email submission service should be offered via port 587 and use authentication. Port 25 is still a recommendation to be a great practice with a high-impact factor by Global IT Association for Telecommunication (ETIS). ETIS shows that the spam outputs of Turk Telecom and Telecom Italia were successfully mitigated by the introduction of port 25 blocking[8]. port blocking also can be implemented in IPv6 and IPv4[11]. Hence, blocking port 25 at ISP level is also used as best practice.

4.1.4 packet filtering. The packet filtering can be applied at a host, network and ISP level[15]. Desktop firewall as a critical component is performed at host level. The use of it is to monitor the network activities of all active processes. Thus, a large amount of traffic at host is manageable and packet inspection is applicable.

4.2 Social And Regulatory Approaches To Botnet

For the social and regulatory approaches, raising user awareness is a solution to reduce botnet focused on their root causes, namely infected end-users'computers on company networks, which means the occurrence of infections is often the result of computer usage driven by ignorance of potential infection sources and a lack of caution[8]. It is reasonable to improve end-users'technical knowledge and the sense of social responsibility. In detail, there are four topics focused on the improvement. Education in malware-spreading mechanisms, emphasizing the importance of keep system up to date, study the information about the interpretation of potential symptoms of infection and guidance and well considered password management[8].

4.3 Technical Approaches To DDOS

The countermeasures of preventing DDOS attacks at technical level are currently partial solutions at best. As we know, many attacks involving DDOS are being developed by attackers to bypass each new countermeasure employed. Three categories can be applied to solve DDOS attack[13]. Firstly, preventing the setup of the DDOS attack network including preventing secondary victim. Then dealing with a DDOS attack in progress, which includes detecting or preventing mitigating or other stops. Thirdly, there is the post-attack category including network forensics. In detail, preventing secondary victims is one of the best methods in preventing DDOS attacks. It requires a heightened awareness of security issues from users. One mention is that users should check system to make sure no agent programs have been installed on their systems or no agent traffic into the network. Neutralizing handler is also an important approach to stop DDOS attack. study involved communication protocols and traffic patterns between handlers and clients in order to identify network nodes that might be infected. This results that fewer DDOS handler deployed than agents. Egress filtering and Management Information Base(MIB) statistics are commonly applied to prevent or detect potential DDOS. The point of egress filtering is that scanning IP packet headers without a network and checking if they meet criteria. If pass the criteria, they are routed outside of sub-network. If not, the packet will not send[13].

5 CONCLUSION

As we mentioned before, advantage of information communication brings the improvement of quality of our daily life and technology development. However, there are certain considerations that the progress of information technology has negative impact on society. The increasingly amount of threat against information security has becoming a critical problem[15]. Many sophisticated underground markets developed that have emerged in cybercriminals exchange information with criminals and sale illicit tools and service. The rules of these underground markets are that support criminal activities by contacting with buyers. For example, buying or selling crimeware such as CaaS to obtain profit. To further understand what it is and how it produces, we designed our project.

To sum up, our project has been successfully finished and obtained great results. We selected underground markets as our target to explore information about security focused on one crimeware named botnet and one kind of CaaS traded in underground market. We collected data including thread, comment, ID, replies and views by Web Scraper. R studio is analyzing tool to annotate our data and get further information from the ecosystem. After the detailed analysis and set criteria, key players have been found. To do further analysis, we set 5 parameters for the key player score. A storyline also has been constructed with information we collected and analyzed, such as popularity, active time, posts, threads and contracts. According to these evidence, we have better understanding to the ecosystem involved crimeware and CaaS in our case study. In the process of finishing our project, we learnt how to use tools to scrape data and analyze data. In general, our project has achieved all requirements and goals. There are still some limitations in our project, such as information in this market are not all public, which means some results are conjecture based on indirect information. In the future, we could collect more data from other underground market, refine and accurate our criteria and do more analysis of our key players.

6 DISCUSSION

The criteria we developed in part 3.2 may require some evaluation since all the weights of each parameter are defined based on our own tests. And the active time is not accurate because it depends on how long a user has been joined this market, maybe it will be better to develop another criteria based on the time online. However, a common problem to use either our criteria or the criteria depends on time online is that some user has a private setting on their profile. Seems like we need to create a larger dataset in the future if we want to remove these private users and develop a more accurate criteria.

As for our storyline, we could do further research on each actor and expand our network to discover more actors in this crimeware network. Actually, a better way to do it is to develop a mechanism that could automatically detects if there is any relationship between two users. Afterwards, we could possibly design a model to create an advanced model or using a well-defined model such as HIN[14]. It is a methodology that could represent a network based on big data, the data can be extracted features from users on a market[18]. In recent years, the usage of smartphones has increased dramatically (especially college and university students due to the wide range of applications on the app store. The increasing rate for smartphones is 24.8% to 27.8% among students and the rate will keep increasing in the future[6]. Crimeware can be a new trend for our study because of the following reasons:

- Mobile devices are lack of malware detection and defense mechanisms
- The development of updates and patches on smartphones is not as fast as computers. And users have intention to refuse updating the system of their phones.
- Smartphones usually have multiple network interfaces, such as WiFi or Bluetooth, which could make them easy to get infected by malware
- Users have a higher level of trust in messages or links that originate from people they know in real life. And sometimes they may not notice that if the sender is already being infected by malware.
- Users have a higher level of trust in application because there is no large scale malware attacks happen yet.

REFERENCES

[1] [n.d.]. Alexa - Top Sites by Category: Top/Computers/Hacking". https://www.alexa.com/topsites/category/Top/Computers/Hacking. Retrieved 5 August 2019.

[2] [n.d.]. Federal Supreme Court decision regarding Logistep AG. http://www.edoeb.admin.ch/aktuell/01688/index.html?lang=en/. Accessed 2010.

[3] [n.d.]. Swedish court: IP addresses are personal data. European Digital Rights (EDRI). http://www.edri.org/edri-gram/number7.13/sweden-ip-addresses-personal-data. 2009.

[4] Esraa Alomari, Selvakumar Manickam, BB Gupta, Shankar Karuppayah, and Rafeef Alfaris. 2012. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. *arXiv preprint arXiv:1208.0403* (2012).

[5] Ingo Feinerer. 2018. Introduction to the tm Package Text Mining in R. (2018).

[6] Subramani Parasuraman, Aaseer Thamby Sam, Stephanie Wong Kah Yee, Bobby Lau Chik Chuon, and Lee Yu Ren. 2017. Smartphone usage and increased risk of mobile phone addiction: A concurrent study. *International journal of pharmaceutical investigation* 7, 3 (2017), 125.

[7] Sergio Pastrana, Alice Hutchings, Andrew Caines, and Paula Buttery. 2018. Characterizing eve: Analysing cybercrime actors in a large underground forum. In *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 207–227.

[8] Daniel Plohmann, Elmar Gerhards-Padilla, and Felix Leder. 2011. Botnets: Detection, measurement, disinfection & defence. *European Network and Information Security Agency (ENISA)* 1, 1 (2011), 1–153.

[9] 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*. International World Wide Web Conferences Steering Committee, 657–666.

[10] Anirudh Ramachandran, Nick Feamster, and Santosh Vempala. 2007. Filtering spam with behavioral blacklisting. In *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 342–351.

[11] Kaleb August Sieh and Dale N Hatfield. 2012. The Broadband Internet Technical Advisory Group (BITAG) and Its Role in Internet Governance. (2012).

[12] Aditya Sood and R.J. Enbody. 2013. Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6 (03 2013), 28–38. https://doi.org/10.1016/j.ijcip.2013.01.002

[13] Stephen M Specht and Ruby B Lee. 2004. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures.. In *ISCA PDCS*. 543–550.

[14] Yizhou Sun and Jiawei Han. 2012. Mining heterogeneous information networks: principles and methodologies. *Synthesis Lectures on Data Mining and Knowledge Discovery* 3, 2 (2012), 1–159.

[15] Abebe Tesfahun and D Lalitha Bhaskari. 2013. Botnet detection and countermeasures-a survey. *International Journal of Emerging Trends & Technology in Computer Science* 2, 4 (2013).

[16] Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. Framing dependencies introduced by underground commoditization. (2015).

[17] Gilbert Wolrich, Debra Bernstein, and Matthew J Adiletta. 2005. Port blocking technique for maintaining receive packet ordering for a multiple ethernet port switch. US Patent 6,976,095.

[18] Yiming Zhang, Yujie Fan, Yanfang Ye, Liang Zhao, Jiabin Wang, Qi Xiong, and Fudong Shao. 2018. KADetector: Automatic Identification of Key Actors in Online Hack Forums Based on Structured Heterogeneous Information Network. In *2018 IEEE International Conference on Big Knowledge (ICBK)*. IEEE, 154–161.