http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (8): 1048-1055, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.1048.1055

Fast-Flux Botnet Detection Based on Weighted SVM

Xiangzhan Yu, Bo Zhang, Le Kang and Juan Chen
School of Computer Science and Technology,
Harbin Institute of Technology, Harbin, 150001, China

Abstract: Botnet is one of the most active threats on the Internet today. Fast-flux technique is a popular way employed by botnet to evade detection. In this paper, we used data mining techniques to detect the fast-flux botnets. By analyzing the patterns of the Domain Name System (DNS) queries from the fast-flux botnets, we extract six features for constructing the weighted Support Vector Machine (SVM) in order to distinguish the normal network domain access from the fast-flux botnet domain access. The evaluation suggested that the approach is effective in detecting the fast-flux botnets.

Key words: Botnet, support vector machine, Fast-flux, Domain name system

INTRODUCTION

Botnet is one of the key threats to the current Internet. It provides a platform which facilitates many types of Internet attacks, such as spam, distributed denial-of-service (DDoS), identity theft and phishing (Arce and Levy, 2003; Sandeep and Andreas, 2007). Therefore, it sparks the interest of a research community recently. Broadly, two approaches on the botnet detection have been proposed: (1) static probes and (2) dynamic analysis of DNS migration. The effectiveness of the static probes in detecting botnet in wide-area network is limited by its deployment scale. The flexible, dynamic and distributed structure of botnets also makes it difficult for static probes to detect the variety of botnets which may exhibit different dynamic behaviors (Zhuge *et al*., 2008). The approach of detecting the botnet of analyzing the DNS migration recently becomes a hot research topic.

As network security problems have been serious increasingly, many researchers focus on the identification of traffic anomaly, trying to look for the characteristics which can give a clue to detect malicious nodes or behaviors (Zhen *et al*., 2008; Yan and Zheng, 2009; Al-Momani *et al*., 2011). Some researchers also observe that the DNS query traffic can be used for the anomaly detection of the Internet (Takemori *et al*., 2009; Romana *et al*., 2008). By observing the portions of queries associated with a specific IP or domain name in the DNS query traffic, the violent changes of the Internet access pattern can be detected. Studies (Choi *et al*., 2007, 2009) suggest that the DNS traffic of a botnet usually exhibits the following characteristics: the hosts of a botnet usually query a specific domain name with similar behavior. Based on this, they forward a mechanism to detect the botnets by monitoring the group activities in the DNS traffic. However, this approach ignores the fact that many networking applications, such as the Instant Messaging (IM) software, the P2P clients, have similar Internet access patterns (Wang *et al*., 2010). Leveraging this observation in botnet detection would lead to a huge number of false positives.

Now-a-days, more complex and intelligent techniques, such as the fast-flux, are adopted by the botnets to enhance the robustness and survival rate. The fast-flux technique establishes a one-to-many mapping from the DNS record to the IP addresses. The mapping changes in a relatively fast speed so that the DNS query returns a dynamically changing IP address each time. The botnet controller, who has the full control of the bots (this was defined in the introduction), assigns a number of computationally strong bots with static IP addresses as flux-agents. Instead of directly communicating with the C and C servers, the bots communicate with these agents to redirect to the C and C servers. In this way, the many-bots-to-one-server access pattern of a botnet is broken. Meanwhile, the frequently changed agent IP addresses make the botnet harder to be detected with traditional approaches.

Several recent studies address the detection of botnets with fast-flux technique. Similar with P2P traffic identification (Modarresi *et al*., 2008; Chen *et al*., 2011), fast-flux botnet is mainly detected by analyzing the characteristics (Nazario and Holz, 2008). Holz *et al*. (2008) used linear classification to distinguish the fast-flux

Corresponding Author: Bo Zhang, School of Computer Science and Technology, Harbin Institute of Technology, Harbin, 150001, China Tel: +86 13836109416

botnet from the RRDNS and CDN networks through several known characteristics of the botnet. Meanwhile, Passerini *et al*. (2008) used the Naïve Bayes to detect the Fast-flux Service Network (FFSN) with nine features. However, in real network, it is quite difficult to determine the prior probability and the threshold Bayes algorithm needs and training a Bayes classifier requires huge amount of samples. IP addresses and Autonomous Systems (AS) are used to detect the FFSN with SVM (Wang, 2009) and the evaluation shows that this approach is accurate and low false positive rate. However, their evaluation is based on a rather small dataset which only includes 90 normal domains and 39 fast-flux domains. This dataset can hardly represent the real world situation. Meanwhile, the experiments suggest that the two features chosen are not sufficient for classification.

In this paper, the compromised hosts in botnets are called bots. The botmaster-the human operator who established the botnet-sets up a number of Command and Control servers (C and C server). The bots obtain commands from the C and C servers periodically. When bots communicate with the C and C servers, some patterns emerge from the network access. From the DNS perspective, the patterns are reflected by regular domain name queries. It enables us to detect the botnets by analyzing the DNS records and queries.

In this paper, we decide to use the weighted SVM technology in the fast-flux botnet detection. From a long term study on the logs of the two heavily used DNS servers, we extract six features as the input to the SVM classifier. The evaluation shows that this approach is both efficient and accurate.

FAST-FLUX BOTNET DETECTION

The emerging fast-flux botnets change the flux-agents frequently for robustness. They frequently change the mapping from a domain name to the IP addresses to notify the bots. From a long term study, we observe that some features, such as the TTL (Time to Live) of DNS records and the geographical distribution of IP addresses for a domain name, can be used to identify the botnets.

Feature selection: The feature selection plays an important role in detecting botnets. We extract six features for detecting the botnets. These features are classified into three categories: the domain property, the network property and the IP distribution of the flux-agents. The features are summarized in Table 1.

Table 1: Features selected

Category	Label	Description
Domain property	F1	Domain age
Network property	F2	Number of IP addresses of a distinct DNS A record
	F3	TTL
IP distribution of the flux-agents	F4	National distribution
	F5	Autonomous system distribution
	F6	Organizational distribution

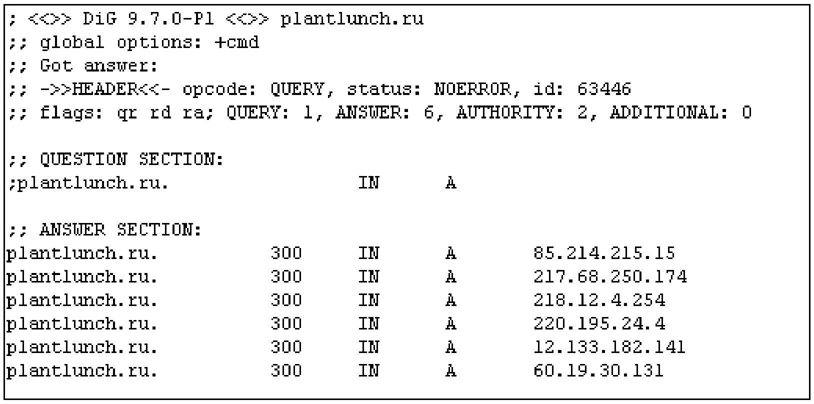
TTL features: In order to enhance the robustness, the fast-flux botnet changes their flux-agents frequently and notifies the bots by setting up the DNS record. The botmaster always sets the TTL of the DNS record small in order to make sure that the bots can contact the server and the flux-agents when the botmaster changes the record.

Figure 1 shows the authorized answer of fast-flux botnet plantlunch.ru (Abuse.ch, 2012). Form the Fig. 1, we can find that the TTL of the record is 300 sec, different with those normal ones whose TTL are typically 86400 seconds. For the CDNs or other sites with RRDNS techniques, the TTL of the records can also be pretty small. In this situation, the remaining five features are used for classification.

To analyze the domain queries with small TTL in the overall queries, we checked 375,885 authorized answers from our DNS servers. From the results, shown in Fig. 2, we find that 23.98% domain names have a TTL less than 600s and 9.63% domain names have a TTL less than 300s. One of the key features of the fast-flux techniques is the frequent change of the domain-name-to-IP-address mapping, so the TTL is typically under 600s. Therefore, we can focus on the queries with TTL under 600s to filter the dataset.

Number of IP addresses associated with a distinct DNS record: Since the bots are physically uncontrollable by the attacker, it is common that some flux-agents may be offline. Additionally, the flux-agent keeps migrating in order to evade detection. When the botnet is active, the number of IP addresses used by fast-flux botnet will continue to increase within a certain period of time and the cumulative number of IP addresses will be very large. For a normal domain, the service machine can not be changed frequently. Therefore, during the same period of time, the IP addresses retrieved by DNS queries will be stable.

Figure 3 and 4 show the increase of IP address number of a fast-flux botnet domain in comparison with a normal domain. In Fig. 3, the number of the IP addresses retrieved from DNS queries for a large site



```
; <<>> DiG 9.7.0-P1 <<>> plantlunch.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63446
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;plantlunch.ru.                 IN      A

;; ANSWER SECTION:
plantlunch.ru.          300     IN      A       85.214.215.15
plantlunch.ru.          300     IN      A       217.68.250.174
plantlunch.ru.          300     IN      A       218.12.4.254
plantlunch.ru.          300     IN      A       220.195.24.4
plantlunch.ru.          300     IN      A       12.133.182.141
plantlunch.ru.          300     IN      A       60.19.30.131
```

Fig. 1: The authorized answer of fast-flux botnet plantlunch.ru

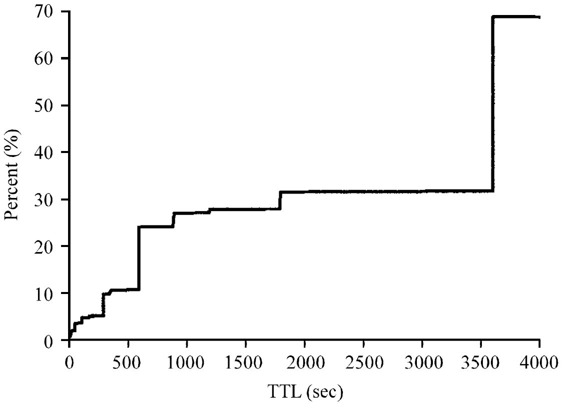


Fig. 2: TTL distribution of authority response during 3 days

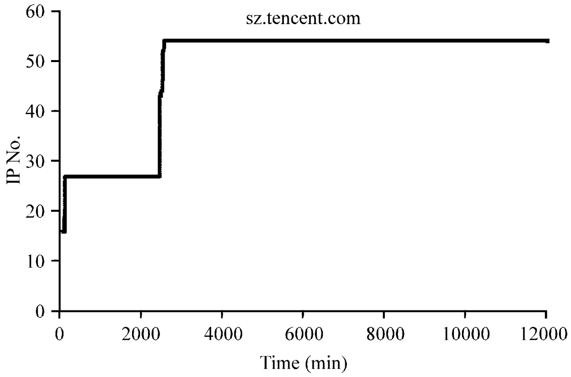


Fig. 3: The increase of IP address number of a normal domain

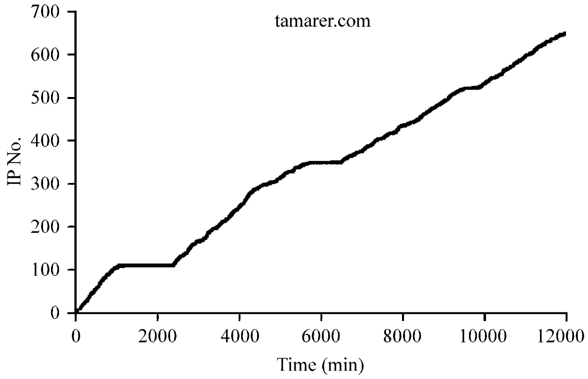


Fig. 4: The increase of IP address number of a fast-flux botnet domain

(sz.tencent.com) with CDN services is 16 initially. There is a leap from 16 to 27 and the number of IP addresses received from the DNS queries remains stable during a quite long time period. Then, there is another leap from 27-54 and remains stable at 54. The leaps may be caused by the increment of servers by the company. During the following 5 days, the number of IP addresses keeps unchanged. In contrast, the number of IP addresses for a botnet domain keeps increasing during our observation period, as shown in Fig. 4. It is nearly impossible that a well-behaved domain will grow at such a pace.

Autonomous system distribution: Due to the restriction on the hosts when the controller of the fast-flux chooses flux-agents, the distribution of the flux-agents depends on the distribution of the bots. The distinct normal domain name server using CDN or RRDNS technology may have many IP addresses and these IP addresses may also belong to different autonomous systems. For a single DNS server, most users' autonomous system is the same with the DNS server's. Then IP addresses of this autonomous system are returned when these users

Table 2: The IP diverse of botnet

Category	Domain	Number of IP addresses	National distribution	Autonomous system distribution
Fast-flux domain	envoyee.com	246	35	111
	rrx-online.com.	825	40	138
	findnewfriendsonline.com	844	39	138
	stg.odnoklassniki.ru	20	2	3
	mynaughtysite.net	833	39	136
	collagegangbang.net	836	40	139
	leolati.com	237	31	109
Normal domain	image.mop.com	10	1	1
	xiamen.gw.com.cn	10	1	1
	61.dc.ftn.qq.com	10	1	1
	sz9.tencent.com	25	1	1
	talkx.l.google.com	25	1	1
	41.dc.ftn.qq.com	28	1	1
	lashou.com	28	2	1
	dl-web.dropbox.com	181	1	1
	pingfore.imqq.com	21	1	2

request the domain name servers with CDN or RRDNS technology. In a word, CDN or RRDNS technology is used in load balance and provide a better service for users. However, for a large botnet, the distribution of its IP addresses will be broadly distributed. The IP addresses corresponding to a domain name are dynamic under the fast-flux technology. When a user queries a domain name server in a short period, he may get different IP addresses. These IP addresses may also belong to different autonomous systems.

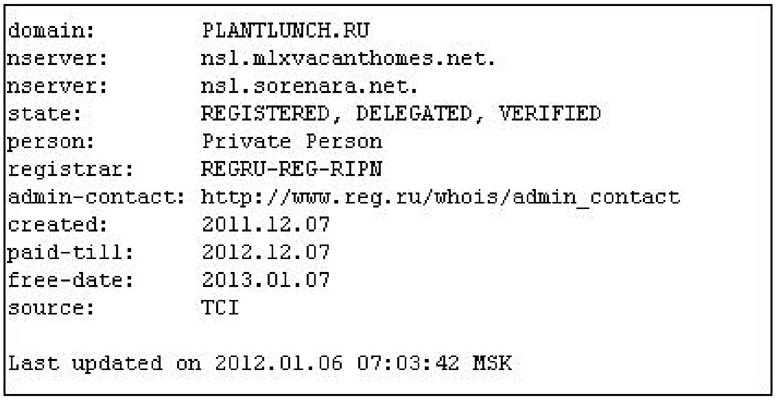
Table 2 shows the tracking result of some typical fast-flux botnets in comparison with normal DNS domain names during 10 days. The table indicates that the IP addresses got from fast-flux botnet belong to dozens or even hundreds of different autonomous systems. On the other side, the IP addresses corresponding to a normal domain name are generally in one autonomous system. For instance, 246 IP addresses of envoyee.com, a fast-flux botnet, are distributed over 111 autonomous domains, but all of the 10 IP addresses of image.mop.com, a normal domain, belong to the same autonomous domains. However, there are some exceptions. For example, 20 IP addresses of stg.odnoklassniki.ru, a fast-flux botnet, belong to 3 different autonomous systems which is similar to many normal domains. This phenomenon is mainly caused by the demise of this botnet when a lot of flux-agents have been removed.

National distribution: Similar to the autonomous system distribution of a domain name, the national distribution can also be used for identifying the domain names for botnets. For a large botnet, its corresponding flux-agent's IP addresses are generally distributed across different countries. This feature is very important to distinguish fast-flux botnets from normal fast-flux services. For a normal domain, its IP addresses may be distributed across different autonomous domains, but they all belong to the same country because of country restrictions. However, for a fast-flux botnet, its flux-agent can be distributed over many countries.

Table 2 shows the national distribution and autonomous system distribution of some known fast-flux botnets. The agents' hosts are distributed in many different countries because the hosts controlled by the botnets are widely distributed. In contrast, the IP addresses of the typical FFSN services are generally distributed in a small number of countries. Table 2 shows that among the seven fast-flux botnets, only the IP addresses of the stg.odnklassniiki.ru are distributed less than 30 countries. For the normal domain names, their IP addresses are mostly distributed in one to two countries when tracing for one probing point. Therefore, the IP addresses' national distribution can be used to identify the fast-flux botnets.

Creation time of domain name: The fast-flux technique has only been applied to the botnets recently. Thus, the creation time of such domain names are generally new. At present, a number of domain names are generated by a particular algorithm when botnets start the attack. Attackers register these domain names in the domain name service provider before building a botnet; then the bots query the corresponding IP addresses according to the algorithm, thereby connecting the control server. The algorithm may generate dozens or even hundreds of domain names in one day, controlling servers of botnet to transit from some domain names to the new ones.

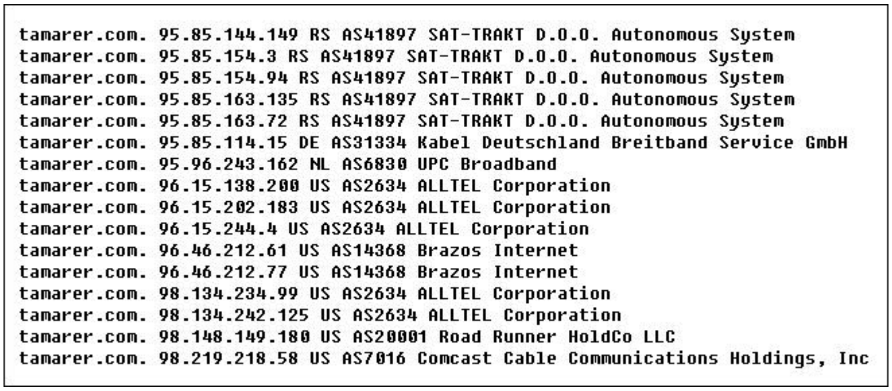
Figure 5 shows the WHOIS information of plantlunch.ru. This fast-flux botnet was active in December 2011. From Fig. 5, we can find that the creation time of this domain is 2011-12-07. Additionally, the authorized servers of this domain belong to different service providers and are created by the same person. For normal web sites, the names servers are generally from the same service provider. Meanwhile, a normal person typically does not need as many domain name records as



```
domain:         PLANTLUNCH.RU
nserver:        ns1.mlxvacanthomes.net.
nserver:        ns1.sorenara.net.
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      REGRU-REG-RIPN
admin-contact:  http://www.reg.ru/whois/admin_contact
created:        2011.12.07
paid-till:      2012.12.07
free-date:      2013.01.07
source:         TCI

Last updated on 2012.01.06 07:03:42 MSK
```

Fig. 5: The WHOIS information of plantlunch.ru



```
tamarer.com. 95.85.144.149 RS AS41897 SAT-TRAKT D.O.O. Autonomous System
tamarer.com. 95.85.154.3 RS AS41897 SAT-TRAKT D.O.O. Autonomous System
tamarer.com. 95.85.154.94 RS AS41897 SAT-TRAKT D.O.O. Autonomous System
tamarer.com. 95.85.163.135 RS AS41897 SAT-TRAKT D.O.O. Autonomous System
tamarer.com. 95.85.163.72 RS AS41897 SAT-TRAKT D.O.O. Autonomous System
tamarer.com. 95.85.114.15 DE AS31334 Kabel Deutschland Breitband Service GmbH
tamarer.com. 95.96.243.162 NL AS6830 UPC Broadband
tamarer.com. 96.15.138.200 US AS2634 ALLTEL Corporation
tamarer.com. 96.15.202.183 US AS2634 ALLTEL Corporation
tamarer.com. 96.15.244.4 US AS2634 ALLTEL Corporation
tamarer.com. 96.46.212.61 US AS14368 Brazos Internet
tamarer.com. 96.46.212.77 US AS14368 Brazos Internet
tamarer.com. 98.134.234.99 US AS2634 ALLTEL Corporation
tamarer.com. 98.134.242.125 US AS2634 ALLTEL Corporation
tamarer.com. 98.148.149.180 US AS20001 Road Runner HoldCo LLC
tamarer.com. 98.219.218.58 US AS7016 Comcast Cable Communications Holdings, Inc
```

Fig. 6: The ownership of tamarer.com

large companies or organizations. These personal domain names with large number of records are suspicious.

Organizational distribution: The IP addresses are globally assigned to many organizations. We can analyze the organizational distribution of the IP addresses of a domain name. However, as an exception, some large international companies, such as Google, have the IP addresses assigned to multiple organizations because of their commercial cooperation with other organizations. Since, there are only a few cases, we can manually filter them with white lists. For fast-flux botnet, the flux-agents are distributed around the world and their corresponding IP addresses may belong to different organizations.

In Fig. 6, the ownership of IP addresses of tamarer.com is shown. From this figure, we can see that 16 IP addresses belong to 6 different organizations. Thus, the organizational distribution of IP addresses can be used to distinguish the normal domain name from the fast-flux botnet domain name.

Feature acquisition

IP ownership: Many existing IP databases provide the IP information look-up service, including the national information, the autonomous domain information and the owner organization. We use the free version of GeoIP database for this study (GeoIP, 2011). It claims that the accuracy of IP information in this database is 99.8%.

Through the C-language interface provided by GeoIP library, we have identified all IP information about ownership of nation, autonomous domains, organizations etc.

TTL of domain name: In the DNS cache, according to RFC1035, the TTL of each domain should be decreased by one every second. Once the TTL of the A record reaches

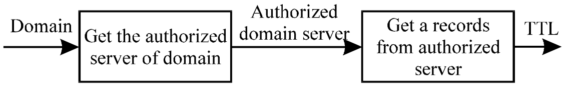

Domain
Get the authorized server of domain
Authorized domain server
Get a records from authorized server
TTL

Fig. 7: The flow chart of deriving TTL

0, it will be evicted from the DNS cache. Therefore, the TTL is the maximum time lag so that the DNS service can tolerate the inconsistency between the authorized name server and the cached server. It is necessary to query the authorized server if the maximum survival time is desired. The process of obtaining TTL is shown in Fig. 7. First, NS records of a domain name are queried to get the authorized server by using DIG tool. Second, A records are retrieved from authoritative server in order to obtain the domain names' TTL.

Creation time of domain name: Generally, the creation time of domain name is obtained by querying the WHOIS database. The information stored in WHOIS database is referred to in the second level domain. Therefore, we need to obtain the second level domain for the domain names. We use a script and a WHOIS tool in Linux to obtain this information.

SVM algorithm and experiment: The goal of SVM is to construct an objective function to separate two types of model possibly according to structural risk minimization principle (Nello and John, 2004; Liejun *et al*., 2008; Yao *et al*., 2012; Shahrabi *et al*., 2009). Generally, it is divided into two categories for discussion: linear separable and linear inseparable. For the six features selected in this paper, it is a linear separable problem of the division of the fast-flux botnet domain name and normal domain name.

It is a challenge to train a SVM filter to identify the fast-flux botnets. We choose the linear kernel function for SVM algorithm because the problem itself is a linearly separable problem.

We dump the DNS queries on two testing DNS servers for two weeks and we also trace the IP changes of the fast-flux botnets with the DIG tool.

We process the data and obtain 49,698 domain queries manually. After the data pre-processing step, the remaining 29945 domains are marked manually. Together with 32 active fast-flux botnet domains out of 55 fast-flux domains traced by DIG, we take these data as the training set. For the test data set, it contains 19,753 domain names after date pre-processing and 8 fast-flux domains. We compare our algorithm with Thorsten Holz's linear classification algorithm (Holz *et al*., 2008). As it's shown in Table 3, Thorsten Holz's linear classification algorithm leads to 233 false positives, but no false negative. Our method has only 2 false positive but 2 false negative as well.

Table 3: The comparison of two algorithms

Linear classification		SVM	
False positive	False negative	False positive	False negative
1.18%(233/19761)	0%	0.01%(2/19761)	0.01%(2/19761)

The false positive domains are shown in Table 4 and 5. We can see that for some normal domains, the number of corresponding IP addresses is very large and these IP addresses are distributed over widely spread autonomous systems or different countries. Such as europe.pool.ntp.org, it is distributed in 25 countries and 11 autonomous systems. In this case, we have to consider the domain's creation time. Generally, fast-flux botnets domains are newly created, but there are exceptions, such as send-safe.com in Table 4. Table 4 shows the 2 false negative cases using the SVM algorithm. We can not detect send-safe.com because it's not active any more, so the features obtained are the same as normal domains. The main reason for sdlls.ru being omitted is the model over-fitting. The number of fast-flux domains in the training data is pretty small and the unbalanced data and high detection accuracy in the training data causes model over-fitting.

Generally, it is better to have higher false positives rather than false negatives in the network security detection system. In these experiments, it's intolerable that there are two false negatives in SVM, although the SVM algorithm performs significantly better than the Thorsten Holz linear classification algorithm in terms of the false positive rate. To this end, we need to improve the SVM algorithm.

Analysis shows that the main reason that the SVM algorithm generates false negatives is the imbalance in the training set. There is much fewer data for the fast-flux botnets than the normal data. We also assigned the same penalty factor for the normal data and the fast-flux data. It is obvious that the false negatives can be reduced by assigning proper penalty factors. Therefore, we decide to use the weighted SVM in the fast-flux botnet detection. Past experience shows that the weighted SVM could reduce the false negative rate and get a better result than the ordinary SVM in the detection of network security anomalous events.

Table 4: False positive of Thorsten Holz's linear classification and SVM and false negative of SVM

Domain	No. of IP addresses	National distribution	Autonomous system distribution	TTL	Organizational distribution	Creation time
10.courier-push-apple.com.akadns.net.	311	1	1	300	1	1999-05-12
2.debian.pool.ntp.org.	39	3	31	390	31	1997-01-18
91dl.gslb.cloudex.net	55	1	5	120	5	2008-08-06
http.12.11.10.nyucd.net	141	30	85	30	106	2003-09-04
europe.pool.ntp.org	248	25	11	390	102	1997-01-18
Send-safe.com	16	4	7	300	13	2001-11-14
Sdlls.ru	73	12	28	300	23	2010-05-11

Table 5: The comparison of linear classification and weighted SVM

Detection method	False positive rate	False negative rate
Thorsten Holz linear classification	1.18% (233/19761)	0% (0/19761)
Weighted SVM	0.22% (44/19761)	0% (0/19761)

Table 6: The false positives in weighted SVM

Domain	Number of IP addresses	National distribution	Autonomous system distribution	TTL	Organizational distribution	Creation time
smtpx.wanhai.com	19	13	14	30	14	1996-3-28
spf.pearson.com	35	6	18	86400	18	1996-11-25
pool.ntp.org	227	3	121	390	31	1997-01-18
facebook.com	12	6	7	300	7	1997-03-29
img135.imageshack.us	8	6	8	500	6	2003-11-12

We train the weighted SVM with the same training set. In order to increase accuracy, we assign a large penalty factor to the misclassified set of samples. We perform the experiment again using the weighted SVM. In the experiment, the number of fast-flux botnet DNS data penalty factor is 29 times of the normal penalty factor. Table 5 shows the comparison of our weighted SVM and the Thorsten Holz linear classifier.

In Table 5, it is obvious that both weighted SVM and Thorsten Holz linear classification do not issue false negatives. Thorsten Holz linear classification generates 233 false positives. The weighted SVM triggers only 44 false positives which is much lower than the Thorsten Holz linear classification.

The domains which trigger the false positive in the weighted SVM are shown in Table 6. The creation time of these domain names are relatively early and most of the TTLs are relatively large (more than 300 generally). We can make use of the domain name creation time to distinguish them in the next step.

From the experiments, we observe that the weighted SVM, with the six features as inputs, can efficiently identify the fast-flux botnets from the DNS traffic. Its accuracy on the botnet detection is satisfactory.

CONCLUSION

In this study, we use six features extracted from the fast-flux botnets to train a weighted SVM in botnet detection. After experiment, the result of the comparison with the Thorsten Holz linear classification shows that our approach is both accurate and efficient.

ACKNOWLEDGMENT

This study is partially supported by the National High Technology Research and Development Program of China (863 Program) under Grant No. 2010AA012504; the National Natural Science Foundation of China under Grant No. 61173144 and No. 2012BAH37B01.

REFERENCES

Abuse.ch, 2012. ZeuS tracker monitor. The Swiss Security Blog, https://zeustracker. abuse.ch/monitor. php?filter=level5

Al-Momani, A.A.D., T.C. Wan, K. Al-Saedi and A. Altaher, 2011. An online model on evolving phishing e-mail detection and classification method. J. Applied Sci., 11: 3301-3307.

Arce, I. and E. Levy, 2003. An analysis of the slapper worm. IEEE Secur. Privacy, 1: 82-87.

Chen, H., H. Xu, C. Wang and K. Zhou, 2011. Incentive mechanism for P2P networks based on Markov chain. Inform. Technol. J., 10: 2242-2251.

Choi, H., H. Lee, H. Lee and H. Kim, 2007. Botnet detection by monitoring group activities in DNS traffic. Proceedings of the 7th IEEE International Conference on Computer and Information Technology, October 16-19, 2007, Aizu-Wakamatsu, Fukushima, pp: 715-720.

Choi, H., H. Lee and H. Kim, 2009. BotGAD: Detecting botnets by capturing group activities in network traffic. Proceedings of the 4th International Conference on Communication System Software and Middleware, June 15-19, 2009, Trinity College Dublin, Ireland, pp: 1-8.

GeoIP, 2011. GeoIP technology. MaxMind, Inc., Massachusetts USA., http://www. maxmind. com/app/ip-location

Holz, T., C. Gorecki, K. Rieck and F. Freiling, 2008. Measuring and detecting Fast-Flux service networks. Proceedings of 15th Network and Distributed System Security Conference (NDSS 2008), February 10-13, 2008, USA, pp: 1-12.

Liejun, W., L. Huicheng and Z. Taiyi, 2008. An improved algorithm on least squares support vector machines. Inform. Technol. J., 7: 370-373.

Modarresi, A., A. Mamat, H. Ibrahim and N. Mustapha, 2008. Measuring the performance of peer-to-peer systems with social networks characteristics. J. Applied Sci., 8: 3895-3902.

Nazario, J. and T. Holz, 2008. As the net churns: Fast-Flux botnet observations. Proceedings of the 3rd International Malicious and Unwanted Software, October 7-8, 2008, Fairfax, United States, pp: 24-31.

Nello, C. and S.T. John, 2004. An Introduction to Support Vector Machines and other Kernel-Based Learning Methods. Publishing House of Electronics Industry, Beijing, China, pp: 47-68.

Passerini, E., R. Paleari, L. Martignoni and D. Bruschi, 2008. FluXOR: Detecting and monitoring fast-flux service networks. Proceedings of the 5th Conference on Detection of Intrusions and Malware and Vulnerability Assessment, July 2008, France, pp: 186-206.

Romana, D.A.L., S. Kubota, K. Sugitani and Y. Musashi, 2008. DNS based spam bots detection in a university. Proceedings of the 1st International Conference on Intelligent Networks and Intelligent Systems, November 1-3, 2008, Wuhan, China, pp:205-208.

Sandeep, S. and T. Andreas, 2007. Measuring the storm worm network. Technical Report 01-10-2007, HiNRG Johns Hopkins University, http://www. cs. jhu. edu/~sarat/storm.pdf

Shahrabi, J., S.S. Mousavi and M. Heydar, 2009. Supply chain demand forecasting: A comparison of machine learning techniques and traditional methods. J. Applied Sci., 9: 521-527.

Takemori, K., D. Romaa, S. Kubota, K. Sugitani and Y. Musashi, 2009. Detection of NS resource record based DNS query request packet traffic and SSH dictionary attack activity. Proceedings of the 2nd International Conference on Intelligent Networks and Intelligent Systems, November 1-3, 2009, Tianjian, China, pp: 246-249.

Wang, X., L. Yang, X. Sun, J. Han, W. Liang and L. Huang, 2010. Survey of anonymity and authentication in P2P networks. Inform. Technol. J., 9: 1165-1171.

Wang, Y., 2009. Fast-flux service network detection method. M. Engineering Thesis, Huazhong University of Science and Technology.

Yan, R. and Q. Zheng, 2009. Using Renyi cross entropy to analyze traffic matrix and detect DDoS attacks. Inform. Technol. J., 8: 1180-1188.

Yao, Y., L. Feng, B. Jin and F. Chen, 2012. An incremental learning approach with support vector machine for network data stream classification problem. Inform. Technol. J., 11: 200-208.

Zhen, L., T. Liang and Z. Ming-Tian, 2008. Research on spam classifier based on features of spammer's behaviours. Inform. Technol. J., 7: 165-169.

Zhuge J.W., X.H. Han, Y.L. Zhou, Z.Y. Ye and W. Zou, 2008. Research and development of botnets. J. Software, 3: 702-715.