Asian Research Consortium

Asian Journal of Research in Social Sciences and Humanities
Vol. 6, No. 10, October 2016, pp. 1859-1867.

ISSN 2249-7315
A Journal Indexed in Indian Citation Index
DOI NUMBER:10.5958/2249-7315.2016.01134.5
Category:Science and Technology

Asian Journal of Research in Social Sciences and Humanities

www.aijsh.com

Spamming Website Detection using Domain Name Server based Passive Probing

V. Rajakumareswaran*; Dr. S. Nithiyanandam**

*Cheran College of Engineering,

Karur, Tamilnadu, India.

**Jay Shriram Group of Institutions,

Tirupur, Tamilnadu, India.

Abstract

Domain Name Server (DNS) is used to maintain the IP address of each domain in the internet. The botnets attacks the DNS to resolve the actual IP address to their own IP address or to position their Command and Control servers to malfunction the website. Detecting these types of attacks using passive monitoring of DNS queries is an efficient technique. In this work, on analysing a number of behaviours of this IP queries we have detected the botnets and their C & C traffic in the DNS. The time based analysis, in bound and out bound analysis and Hash based probing detects the botnet in an efficient way.

1. Introduction

More number of attacks in internet is performed using malicious URLs. The URLs are compromised to do spamming and phishing like attacks. This DNS based attacks are growing day by day. It has become a common channel to facilitate Internet criminal activities such as drive-by-download, spamming and phishing. Many attackers try to use these web sites for spreading malicious programs or stealing identities. Kaspersky Lab [14] reports that browser-based attacks in 2012 increased from 946,393,693 to 1,595,587,670 and 87.36% of these used malicious URLs. The Anti-Phishing Working Group (APWG) [4] also reports that phishing attacks using malicious URLs increased from 93,462 to 123,486 in the second half of 2012. Of the millions of URLs used each day less than 0.01% is malicious and furthermore they are short-lived in order to avoid blacklist blocking. There is an urgent need to develop a mechanism to detect malicious URLs from the high volume, high velocity and high variety data. Many information security companies and

organizations offer malicious URL detection including Google's safe browsing [9] and Trend Micro's web reputation services [16].

Monitoring the DNS to probe the intruder is one of the best methods in IP filtering. Domain Name System (DNS) is a protocol and service widely used on internet. A very basic use of DNS is to map domain names to its IP address. Whenever a user enters a domain name in their web browser, DNS performs a forward lookup to find one or more IP addresses for that domain. This is called as 'A' record. The User's network stack now can send http traffic to the destination IP address. DNS is constantly being enhanced to provide more features. Particularly DNS can be used for pruning out irrelevant and harmful IP address. Monitoring the DNS passively for attack is efficient way of detecting attacker as they will be unaware of what it has been done. So in this work we have developed 5 steps in detected the attackers in DNS queries.

Methodology

The proposed system will gather the complete details of the Domain Name System and will analyse the harmful IP in the list. The basic idea of our methodology includes the following steps.

1. Extracting attributes for Monitoring
2. Time based Feature Detection
3. Find the in degree and out degree of Malicious IP address for most frequently used IP
4. Find the link farm technique
5. Locality sensitive hashing implementation.

1.1 Extracting attributes for Monitoring

The DNS should be monitored for queries to detect the harmful IPs. In this phase all the parameters of IP address are extracted to analyse the attacker. Given an IP address a, we define BGP(a) to be IPs within the BGP prefix of a, and AS(a) as the set of IPs located in the autonomous system in which 'a' resides. In addition, we can create these functions to take as input a group of IPs:

Given IP set $Z = z_1,z_2,...,z_N$, $BGP(Z)=U_{j=1..N}\ BGP(i_j)$; AS(i) is similarly extended. To extract the properties of each domain d we proceed as follows. First, we consider the most current set $Z_c(d)=\{zi\}i=1..m$ of IP addresses to which d points. Then, we can query our DNS repository to retrieve the following information.

2.1.1 IP Probe: It is used to probe all the IP addresses stored in the DNS repository Z_i.

2.1.2 Domain Probe: It is used to probe all the domains mentioned for that IP addresses stored in the repository, D_i.

Let $D = \{d_1, d_2,\ldots d_n\}$ be the set of domains and A(D) is the set of IP Addresses pointed by any domain d.

2.1.3 Feature Assessment

After extracting the entire IP addresses Z_i and Domain name $D_{i,}$ we need to extract number of details associated to Z_i and $D_{i.}$ The characteristics are

2.1.4 Historical Association vs Geographical Association

Once the list of IP addresses 'Z' are stored after IP probe, the set of other IP address which are historically associated with 'Z' and their geographical locations will be extracted and noted. The historical association is the history

2.1.5 Token Analysis

After we receive the domain list using Domain probe, we will analysis number of property of domains like domain name, number of domains used, number of occurrence of each domain, their bandwidth, their frequency etc., and will be noted.

2.1.6 Black Sheep IP's

So we have got the domains and all their details, IP address and their details after the above analysis. Now using this statistics, we will be analysing the black sheep IP by undergoing the next stages one by one. The black sheep IP can be analysed by listing the IP that have contacted the intruder IP's found in the trained dataset.

2.1.7 Pruning the IP Addresses

Now the repository of both legitimate and unauthorized IP has been categorized. Now it should be pruned out so that no unauthorized IPs escaped the list. Now a score would be maintained for each IP depending on their history.

2.1.8 Features of BGP

By using the BGP features we can detect the country in which the IP address belongs to and the organization that owns it, the number of IP addresses it has, all the prefix of the domain and the time of DNS query made by each IP. This can be analyzed by finding the number of second level and third level domain address of the IP. We can also assess the number of countries that a two sets of prefixes belongs to.

2.1.9 Autonomous System Feature

It has the details of number of autonomous IPs in the given domain. It can be detected by its first level domain, second and third level of domain name in the IP Address of the autonomous system.

2.1.10 IP Entry Feature

It has details like number of unique that are associated with the given IP, the diversity in registration dates over the given IP, the total number of registrars associated with the IP address in the second level and third level domain of the autonomous system.

So by analysing the above features of the IP addresses we can get to know that the professional harmless internet services will have a stable network profile which will have very low network features in it. Whereas malicious networks while considering will change the profile more frequently so that the features will be assigned with higher values. Also the legitimate domain exhibits only a small values in its autonomous system feature as it belongs to only same organization or small number of different organization. On the other hand, the domain with malicious IP could reside in large number of networks. So the AS features will have high values. Also in the context of homogeneity of the registration information, the attacker domains will have higher feature value as they resides in different registrars with different registration dates whereas the legitimate domain will have lower feature values. So by using the above techniques the complete features of all the domains in the DNS will be noted.

2. Time-sensitive Feature Detection

On noting the time of request by all the IP address to the DNS, we can find that the attacker domains will have similar live time span and similar visit pattern. We are extending our research on the basis of this feature. In attacked network some botnet will utilize one or more 2LD and 3LD to we can trace the origin of the botnet. Every domain has their own active time, but they have identical life span. As all bots in one botnet are controlled by the same C&C, create a lot of subdomains for later use. If we cluster these domains into one group and the whole network command response time of interaction is computed in advance, the visit of every bot to all domains have similarity and coherence. As described in Fig.1 we are considering the traffic of all the domains from the previous technique to filter the traffic depends on the time and combine the data of such traffic.

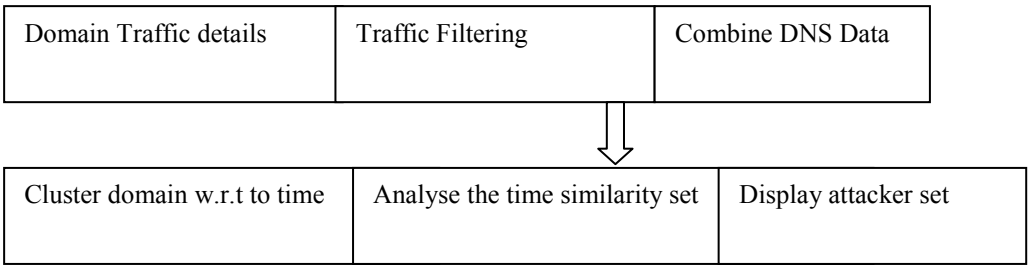


Fig. 1 Time based Traffic Analysis

On making the time based analysis we can detect that few IP's will have uniform time of access of DNS. On viewing this, we can easily determine a certain group of queries will be arriving the DNS in an uniform time sequence. This can be determined as attacker IPs. Here in the fig 2, we can detect with testing for 9 IP queries for 6 ms, that IP1, IP2, IP3, IP7 and IP8 have uniform time of 2ms for DNS query and it can be determined as attack.

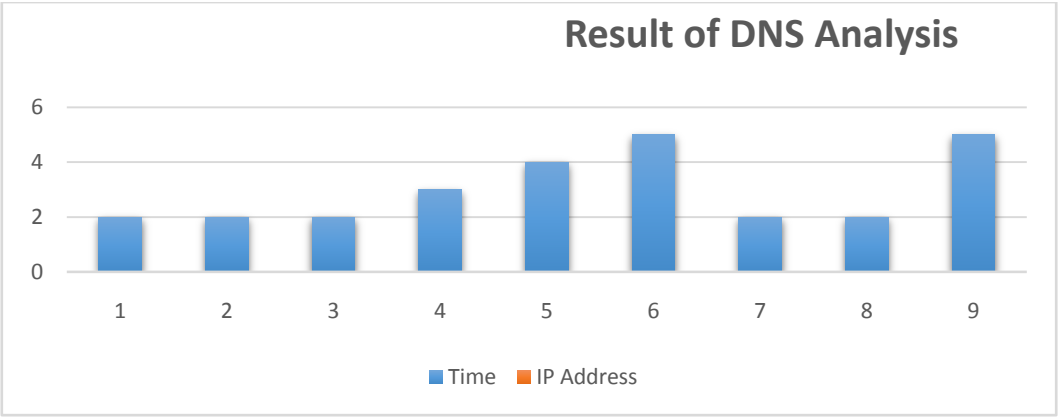


Fig 2: Time based Analysis of Attacker and Legitimate IPs

For a given time period T, on dividing all domain names belong to a particular period into groups according to same second-level, third-level and parsed IP, we can get domain sets. The domain set is expressed as D = $\{s_1, s_2 \ldots s_n\}$. If domain s_1 is queried at a time T_1 for the first time, and get the last query at T2, then this domain's active life is between T_1 and T_2. We are expressing this domain's life span as S, and uses count() to represents the attacker's domain number which belong to one domain set. So for a domain set D, the domain's active situation can be expressed as:

$\{count(DT_1)count(DT_2)..count(DT_n)\}$

When the value of count() increases rapidly for the huge proportion then the domain can be reported as an attacker. Using Distribution(D) we can represent the domain set active time distribution as,

$Distribution(D) = \max(count(\Delta T_i)) / \sum_{i=1}^{n} count(\Delta T_i)$

The greater value of Distribute (D), the active time length distribution of domain set will be high. Using this feature we can filter out suspected attacker domains.

3. Find the In-degree and Out-degree of Malicious IP Address for most Frequently used IP

After performing the time based analysis the suspicious attacker domain could be detected. Next we need to analyse the in-degree and out-degree of the flow of query of each node to the DNS. The out-degree of the node is defined as a number of data flow passes from the node through the DNS and the in-degree of the node can be defined as the number of data flow enters into the node. The in and out degree of the botnets will be different than the legitimate IP address. We have seen earlier that the characteristics of the botnets and the request flow will vary from time to time and the amount of request will also vary accordingly. That means the flow of packet from one IP address to another over time will differ for both malign and benign IP's. According to a statistics[5] there are two characteristics of data flow of an attacker IP. The inbound and outbound of attacker IP over a particular time will be lesser and the quantity of data transferred will also be less due to the fact that

botnet maintains the privacy by reducing its communication. So in order to transfer more control and packet signal from one IP to another it makes frequent motion with less density of data.

Through this mean we can detect that a botnet had attacked the DNS. So we need to consider a few parameters over a time. On time 't1', when a nodes have out-degrees as zero i.e. node with out-degree $N_{out} = 0$ or when a nodes with in-degree $N_{in} = 0$ then it can be suspected as botnet. Also if there is a maximum number of in-degree i.e $N_{in} > t$ or out-degree $N_{out}>t$ where 't' is the threshold then it can be suspected as botnet. This maximum flow occurs in botnet in order to communicate with the C & C server more frequently. By making the time based analysis and in and out-degree based analysis, we can determine almost all of the malign IP Addresses. Next we need to analysis is there any domains attacked by the C&C server.

4. Find the Link Farm to Detect the C&C Server

Command and Control server contains server and other infrastructure used to maintain malwares using botnets to attack the IP addresses in the network. The Command and Control server is the server that controls all the spam links from different IP Address. Sometimes Botnet uses DNS as a communication channel for C&C traffic. We can trace this using our link farm technique. In this technique the statistics received from the previous analysis can be taken into account to detect C&C attack. On observing the behaviour of the DNS query flow we can find two features to trace the C&C traffic.

As the botnet needs to communicate few information to C&C like spam templates, email addresses or fraud URLs it needs extra flow of queries between them and so the C&C channel maintains an extra level of persistence as discussed in previous techniques. Here we have defined some behavioural features of botnet over C&C traffic. Initially we measure the size of all response messages and assess the corresponding bandwidth over the time't'. We can understand that the volume of data transmitted between the DNS C&C server and the botnets will be remarkably larger than the regular DNS usage, as DNS is naturally not used for data transmission. So it will produce either larger messages or increased bandwidth consumption between the bots and the C&C server.

Secondly, the information flow between bot instance and the C&C server will be more persistent as discussed earlier. We measure this time of persistence by measuring the maximum time consumed between two DNS query responses and the communication time between the initial and the final message exchanged with a C&C server. To be simple, these two behavioural communications can be said to be effective enough in order to confirm the C&C traffic over the DNS. To classify the DNS attack by C&C, we compute the mean cluster centroids of the two clusters derived in time based detection. The feature vector is scaled by using the normalization technique from our training phase. Finally, we calculate the Euclidean Distance between classifier to detect the most nearest cluster to the determined feature vector.

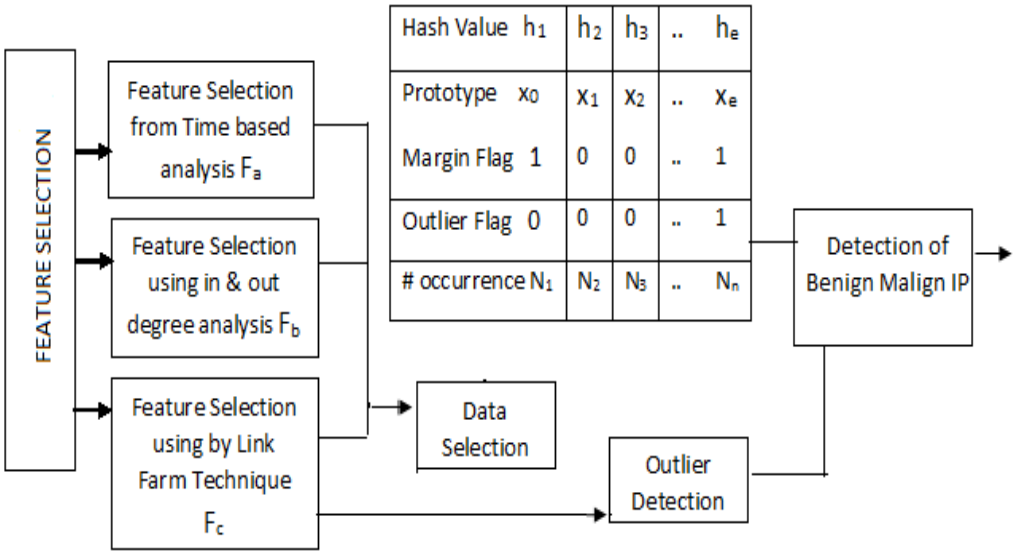
5. Locality Sensitive Hashing Implementation to Contrast Malicious IP with Benign IP

After performing all the above testing, we can implement the LSH technique to group the malign IP's and benign IP's into separate buckets. Learning the characteristics of large number of IP

addresses in a dynamic environments like our application is difficult. In order to handle this task to differentiate the attacker from benign IP we are implementing this Locality Sensitive Hashing (LSH) technique. After we learn the characteristics of attacking IP address we analyse the IP which is located close to our above stated characteristics are assigned as 1 in hash table which will be defined as malign IP and the rest of the IP Address which are outlier to the stated characteristics will be classified as benign IP and can be assigned 0.

In this work our hash table is composed of five items: hash value he, prototype x_e, margin flag F_eM, outliers flag F_b and numbers of occurrence N_e. The index or a hash value is used as a key to find a matching entry e. The second item corresponds to a prototype xe (i.e., representative data of a sub-region) which is calculated as a mean vector of training data in each subregion. A prototype is used to verify whether the bucket of a training data (query) lies in either 'well-learned' region or not, which is represented by the third item FeM called margin flag. If FeM = 1, it represents that a training data is located within a well-learned region. Then, such a training data is not necessary to be trained. Whereas, the data with FeM = 0 should be selected as a training data. The fourth and fifth items F_0 and Ne are used in the outlier detection. Here, initially we will be define the values that need to be stored in the Hash table and the other outlier IP addresses that needs to be filtered. Then by finding the mean vector of the list of attacker IP's we detect the similar characteristic IPs and the flag will be set to denote that that IP has been detected as attacker. On continuing this process for the entire set we can detect and store only the attacker in the hash table.

Fig. 3 Implementation of LSH



Algorithm DNS Hash Update

Input: IP Feature $F = \{(ip_i, f_i)\}_{i=1}^{n}$ and hash table H_t.
Output: H_t// detecting attacker IP and harmless IP
Calculate the hash values $h(ip_i)$ for all ip_i belongs to F.
Find $v = \{1, \ldots, V\}$ unique hash values from $h(ip_i)$.
for all hash values h_v do
Find all ip_i with $h(ip_i) = h_v$ and calculate the mean vector ip_e.
if $h(ip_i)$ found in H & $F_u = 1$ then
    Set $O_c = O_c + c$ where c is the cardinality of similar data ip_i in h_v.
else
    Evaluate the output limit for ip_i and assign the familiarity flag F_u^f.
Set $O_c = c$.
Store $\{h_v, ip_i, F_u, O_c, F_u^f\}$ in H_t.
end if
end for

By implementing the above technique we can detect the complete list of attacker IP addresses to be stored in the Hash Table whereas the harmless IP address will be stored separately.

6. Conclusion

In this work we analysed the significant behaviours of attacker IP in DNS. We apply various techniques to detect the harmful IP and all the C&C attack at different levels of network traffic. Finally we made a hash table based approach which can eliminating the duplicates, detect the outlier data and to list the malign IP's in the DNS.

7. Result and Discussion

We have implemented our methodology in about 1,95,000 DNS resolutions using number of online dataset like WEBSPAM-UK2007 and domains from Tire-1 ISP in India. On making these experiments, we assessed that 20% of the malicious IP address are detected in time based detection and next 25% of the malicious IP's are attracted in in-degree and out-degree analysis and the C&C attacker detection techniques works at the rate of 80% accuracy. We made it more accurate by implementing the hash based technique of detection which makes above 80% of traffic detection. We can make this technique more accurate by scrutinizing the DNS traffic of more dataset by creating more training data sets.

Reference

Arshad S, Abbaspour M, Kharrazi M, et al, An anomaly-based botnet detection approach for identify stealthy botnets, IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE), IEEE, (2011).

Bojan Zdrnja, Nevil Brownlee, and Duane Wessels, University of Auckland, New Zealand, Passive Monitoring of DNS Anomalies, The Measurement Factory, Inc.,

CHEN Chiamei, OU Yahui, TSAI Yuchou, Web Botnet Detection Based on Flow Information, International Computer Symposium (ICS), IEEE, (2010).

Christian J. Dietrich Herbert Bos yz, Christian Rossow, Maarten van Steen Computer Systems Group, On Botnets that use DNS for Command and Control, (2009).

Emmanouil K. Antonakakis, School of Computer Science, Georgia Institute of Technology, Improving Internet Security Via Large-Scale Passive And Active DNS Monitoring, 2012.

LIAO Wenhwa, CHANG Chiaching, Peer to Peer Botnet Detection Using Data Mining Scheme, International Conference on Internet Technology and Applications, IEEE, (2010).

Luca Deri, Simone Mainardi y and Enrico Gregori, Maurizio Martinelli. Institute of Informatics and Telematics (IIT), Italian National Research Council (CNR), Pisa, Italy Department of Information Engineering (IET), Exploiting DNS Traffic to Rank Internet Domains.

Paritosh Pantola, Anju Bala and Prashant Singh Ra, Computer Science and Engineering Department, Thapar University, Patiala, Punjab, India. Consensus based Ensemble model for Spam detection, IEEE, 2015.

Roberto Perdisci, Igino Corona, and Giorgio Giacinto, Senior Member, Early Detection of Malicious Flux Networks via Large-Scale Passive DNS Traffic Analysis, IEEE, 2012.

Wanli Ma, Dat Tran, and Dharmendra Sharma, Faculty of Information Sciences and Engineering University of Canberra, Canberra, Australia, A Novel Spam Email Detection System Based on Negative Selection, IEEE, 2009.

Zeidanloo H R, Bt Manaf A, Vahdani P, et al, Botnet detection based on traffic monitoring, International Conference on Networking and information Technology (ICNIT), IEEE, (2010).

http://www.darkreading.com/analytics/threat-intelligence/5-ways-to-monitor-dns-traffic-for-security-threats/a/d-id/1315868.

http://www.behindthefirewalls.com/2014/01/extracting-files-from-network-traffic-pcap.html.