一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

Finding Malicious Authoritative DNS Servers

Yin Minn Pa Pa† Daisuke MAKITA† Katsunari YOSHIOKA† and Tsutomu MATSUMOTO†

†Graduate School of Environment and Information Sciences

Yokohama National University

79-7 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 JAPAN

E-mail: †{yinminpapa-xg, makita-daisuke-jk,yoshioka,tsutomu}@ynu.ac.jp

Abstract This study proposes an approach to find authoritative DNS servers that are heavily involved with malicious online activities. For example, in order to construct a fast flux network, attackers need to have full control on authoritative DNS servers so that he or she can abuse on their round robin feature. These DNS servers may have been setup by attackers themselves or they may be legitimate servers compromised and misused by the attackers. Either way, we believe that focusing on such maliciously used authoritative DNS servers can be a new aspect for understanding the underlying malicious online activities. In this study, we consider four features, fraction of blacklisted domains, Server Fail response history, TTL of DNS server's domain, and domain flux size, to evaluate an authoritative DNS server. Using these features, we evaluate 74,830 authoritative DNS servers of domains observed at a cache DNS server. As a result, we determine 31, 15, and 85 servers as malicious, respectively using fraction of blacklisted domains, TTL of DNS server's domain, and domain flux. We confirm that 21% of the detected servers are true positive according to several published security reports exhibiting the possibility of these features as metric to find malicious DNS servers.

Keywords Malicious Authoritative DNS Server

1.Introduction

Domain Name System (DNS) is an important infrastructure of the Internet. In order to use network services like web, file transfer and mail, etc., every host needs to access DNS for resolving domains to IP address of servers providing the services.

In the same way, attackers often utilize DNS for many reasons such as having compromised hosts connect their Command and Control (C&C) servers and finding the target of DoS attack, etc. Moreover, the attackers have enhanced flexibility and robustness of the name resolving services, for instance, by adopting a flux network to avoid blacklisting of their domains and IP addresses. Although such enhancements have been successful and gained the workload of defenders, they require heavier involvements of malicious entities to DNS.

For example, in order to construct a fast flux network, attackers need to have full control on authoritative DNS servers so that he or she can abuse on their round robin feature. These DNS servers may have been setup by attackers themselves or may be legitimate servers compromised and misused by the attackers. Either way, we believe that focusing on such maliciously used authoritative DNS servers can be a new aspect for observing and understanding the underlying malicious online activities.

In this study, we consider four features, fraction of blacklisted domains, Server Fail response history, TTL of DNS server's domain, and domain flux, to evaluate an authoritative DNS server. Using these features, we evaluate 74,830 authoritative DNS servers of domains observed at a cache DNS server. As a result, we determine 31, 15, and 85 servers as malicious, respectively using fraction of blacklisted domains, TTL of DNS server's domain, and domain flux. We confirm that 21% of the detected servers are true positive according to several published security reports exhibiting the possibility of these features as metric to find malicious DNS servers.

There are some related studies by Mcafee in which the analysis on registration of malicious domains on .com TLD zone file is conducted. In contrast with the related works, our contributions are as follow:

- Our study aims at finding malicious DNS servers in general rather than looking for the malicious domains registered in a particular DNS server for a particular zone.
- Previous studies focus on malicious domain registration at the registry level, namely TLD DNS servers. In contrast, our method looks for malicious authoritative DNS servers at the lowest level whose malicious activities may not be noticeable from the registry level.

2. Background

2.1 Fluxing in DNS

Attackers such as bot headers need technologies to resist blacklisting of their domains and IP addresses to keep the channel between their bot agents and C&C infrastructure. For that, fluxing is one of the most suitable technologies. There are two types of fluxing: IP flux and domain flux.

IP flux refers to the constant change of IP addresses related to a particular fully qualified domain name (FQDN). As the changes of IP addresses happen in a short time, IP flux is commonly referred to as "fast-flux". There are two types of fast-flux: single-flux and double-flux [2]. Single flux is an IP flux in which the associating IP address for a particular FQDN changes rapidly. The native DNS's round robin and TTL configuration of A record are abused to realize the single flux. In double flux, not only the IP address of FQDN (A RR) but also IP address of domain DNS server (NS RR) changes rapidly.

Domain flux is the inverse of IP flux. The domain flux can be referred to the constant change of FQDN related to a particular IP address. Native wildcard feature of DNS is abused for realizing domain flux. The list of FQDN may be hard-coded in the bot agents, obtained from remote hosts, or internally generated by Domain Generation Algorithm (DGA) in the bot agents. DGA creates a dynamic list of multiple FQDN. Since the domain names are dynamically generated in volume and typically have a life of only a single day, the rapid turnover makes it very difficult to investigate or block every possible domain name [3].

2.2 Domain Registration

The registrant registers a domain at the registrar, the service provider for domain registration. A registration of a domain name establishes a set of Start of Authority (SOA) records in the DNS servers of the parent domain, indicating the IP address (or domain name) of DNS servers that are authoritative for the domain. This provides merely a reference to find the domain data.

The registration of a domain does not automatically imply the provision of DNS services for the registered domain. Most registrars offer DNS hosting as an optional free service for domains registered through them. A number of sites offer free DNS hosting, either for second level domains registered with registrars that do not offer free DNS service, or as third level domains (selection.somedomain.com). Many third-party DNS hosting services provide Dynamic DNS. [4]

If DNS services are not offered, or the registrant opts out, then it is responsible for procuring or self-hosting DNS services [5].

2.3 Malicious Authoritative DNS Servers

In this study, we consider an authoritative DNS server that is heavily involved in the malicious online activities as a malicious authoritative DNS server. There can be at least four types of malicious authoritative DNS servers:

- The DNS servers setup by the attackers
- The compromised DNS servers with which an attacker has full control
- The DNS servers on server hosting services (e.g. bullet proof hosting services)
- The dynamic DNS services abused by attackers

For fast flux domains, attackers need to have full control in changing RR of an authoritative DNS server so that he or she can abuse on round robin feature of DNS. For this, they need to register NS record for their SLD domain in TLD zone through registrar. An example zone file of a TLD DNS server with malicious domains is shown in figure-1.

```
malicious.tld.      360  IN  NS  ns1.malicious.tld.
malicious.tld.      360  IN  NS  ns2.malicious.tld.
ns1.malicious.tld.  180  IN  A   1.2.3.4.
ns2.malicious.tld.  180  IN  A   5.6.7.8.
```

Figure -1 An Example of TLD Zone with Malicious Domains

After the registration, the attacker has control on "malicious.tld" zone that is stored in his own authoritative DNS servers, namely, 1.2.3.4 and 5.6.7.8. In the single flux, these two NS records will be static. In the double flux, the attackers change these two A records in time by adding a proxy layer to prevent their own DNS server [6] from being spotted.

Another existing technique is the domain flux with DGA generated domains. The attackers implement an algorithm to internally generate domain names of C&C servers for their bot agents to contact. Because the input of the algorithm often includes time information, the output domains can vary over time. For this scenario, the attacker registers a portion of DGA generated domains beforehand. The registration of such DGA domains can be realized with all types of DNS servers described above.

In case of W32.Morto worm [8], it has added another C&C communication vector by supplying remote commands through DNS records. The record type that W32.Morto uses for its communication protocol is the TXT record [8]. In this case, the authoritative DNS server replying TXT records may be attackers own DNS server or compromised one.

All these attacks take advantage of the existing DNS infrastructure. We point out that in order to efficiently realize such attacks as their needs the attackers should have authoritative DNS servers in their control and finding such malicious servers is the objective of this study.

3. Features for detecting Malicious Authoritative DNS servers

In this chapter, we explain four features for detecting malicious authoritative DNS servers.

Feature 1: Fraction of blacklisted domains

In the first feature, the fraction of blacklisted domains for which the evaluated DNS server is authoritative is calculated for its evaluation. The matching can be done with existing blacklists such as EXPOSURE [10], Zeus Tracker [11], and Malware domain list [12] and Spybot domains [13]. However, the coverage of these blacklists is limited and we can miss some malicious DNS servers. In our experiment described in the next chapter, we extend the blacklists by considering all domains sharing the same IP address with a blacklisted domain as black. The simplest way to apply this feature for detecting malicious DNS servers is adopting a threshold. Namely, we can determine that a DNS server is malicious if the fraction of blacklisted domains that the server is authoritative for exceeds the threshold. In the experiment, we set the threshold to 0.9.

Feature 2: Server Fail Response History

The DNS servers of the popular and benign domains are normally very stable. In fact, Server Fail response error is rarely found in our study of authoritative DNS servers hosting popular top 1000 domains of Alexa list. In contrast, in fast flux network, normal malware infected PC can be used as proxy to redirect to actual DNS servers [6]. In such case, the quality of service of DNS server cannot be as high as real DNS servers because the PC may be shut down by its user and server fail errors can be occurred. That is why we focus on the history of DNS Server Fail error response for evaluating DNS servers. At this moment, we have not determined how exactly we are going to use this feature for detecting malicious DNS servers.

Feature 3: TTL of DNS Server's Domain Name

Time to Live (TTL) value of the DNS server's domain is also an important factor of differentiating malicious DNS servers. When a cache (recursive) DNS server queries the authoritative DNS server for a resource record, it will cache that record for the time in seconds specified by the TTL. The A records of malicious DNS server involving in fast flux service network change rapidly. That is why, the TTL for each A resource record is set to very low value such as a few seconds [6]. Again the simplest way to apply this feature for detection of malicious DNS servers is to adopt a threshold. Namely, if a DNS server has a domain name whose TTL value is smaller than the threshold value, we determine that the server is malicious.

Feature 4: Domain Flux

In this feature, we check the existence of domain flux in each of DNS server. For finding domain flux, we count the number of domains sharing the same IP address. If the number exceeds a threshold, then we consider there is a domain flux. In the experiment of the next chapter, we set the threshold as 100.

4. Experiment

The experiment for the evaluation of the four

features is done using real traffic of a cache DNS server. The process of the experiment is shown in figure-2.

In the first step, we extract domains from the DNS reply packets of the analyzed traffic of the cache DNS server. The data used for the evaluation of the proposed method is 65-minute-long DNS traffic captured between a cache DNS server and its clients of approximately 1 to 2 million. There are 3 to 4 million domains resolved in the traffic.

In the second step, we filter out certain domains by three filtering rules. Firstly, domains relating to security software and domains used for DNS blacklist check and the reverse lookup domains are filtered out. Secondly, the domains matching with top 1,000,000 popular domains of Alexa domain list are filtered out. Thirdly, the domains that do not have proper domain format as described in RFC 1035 [9] are dropped.

In the third step, the authoritative DNS servers of each domain are looked for. The resolver program built on Perl Net::DNS::Resolver module is used for this step. In this step, for each of investigated domains, NS, A, SOA RRs are queried programmatically to receive a list of authoritative DNS servers.

In the fourth step, the analysis on the outputs of the third step is conducted. The database of DNS servers and their domains are reconstructed based on the outputs of the third step.

In the fifth step, the four features described in the previous chapter are evaluated.

Feature 1 (Fraction of blacklisted domains)

Firstly, the total of 111,883 known black domains are collected from EXPOSURE [10], Zeus Tracker [11], Malware domain list [12] and Spybot domains observed by our malware sandbox analysis [13]. Then, we extended the blacklist by considering all domains sharing the same IP address as a blacklisted domain as black.

In order to extend the blacklist, A records associated with the domains of each of the DNS servers are queried by the resolver script based on Net:DNS:Resolver. Then, for each DNS server, domains with the same A records are clustered. Each of the clustered groups is matched again with known blacklisted domains. If one domain of the cluster matches with a known black domain, the other domains in each cluster are considered as extended black domains.

Finally, the fraction of black domains is calculated for evaluating each DNS server. In the experiment, we determine that an authoritative DNS server with more than 90% of its observed domains blacklisted is a malicious one although the threshold should be discussed further.

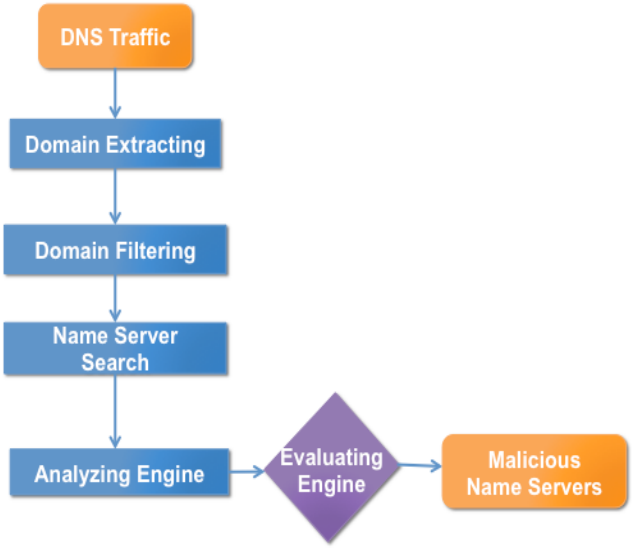

Figure -2 The flow of Experiment

Feature 2 (Server Fail History)

We evaluate each DNS server by checking whether any client has received Server Fail response when querying for an authoritative answer to it.

Feature 3 (TTL of DNS server's domain name)

We evaluate each DNS server by the TTL value of its domain name. The domain name of a DNS server can be obtained by using dig command with trace option. The automated trace route queries to A records of the DNS servers' domain names are investigated in this feature.

Feature 4 (Domain Flux)

The experiment is conducted on 74,830 name servers. The domains for which each of the DNS servers is authoritative are first clustered by their corresponding IP addresses. Then, we extract the clusters with a domain flux using a threshold of flux domains of 100.

5. Results and Discussions

From the cache DNS server traffic described above, approximately 20 to 30 million DNS response packets are extracted. From these response packets, 4 million domains are extracted. In the second step, after

applying three filtering rules to the extracted domains, the remaining domain is 879,297. In the third step, authoritative DNS servers of each of the domains are looked for. As a result of the third step, we found 74,830 authoritative answers for 294,059 domains. Other domains receive errors like NXDomain and ServFail. In the fourth step, the analysis on these DNS servers is conducted. The database for 74,830 DNS servers and their respective domains are constructed in this step.

As the first feature of evaluation engine, DNS servers hosting black domains are investigated. From this analysis, 430 DNS servers, for which at least one of their domain names is blacklisted, are found. Out of 430 DNS servers, 31 DNS servers are found with 90% of their domains blacklisted. The list of these DNS servers and the percentage are shown in the table-1. In addition, out of the 430 DNS servers, 22 are listed on KnujOn [14] as the top 20 spam domain hosting DNS servers.

As the analysis result of the second features, we confirm that 60% of the 31 DNS servers found in the previous analysis have server fail history of at least one time.

As for the third feature in which TTLs are investigated, 40 DNS servers have very low TTL values ranging from zero to 5 minutes. Out of these 40 servers, 15 DNS servers have very low TTL value of zero to 100 seconds. These DNS servers and their TTL values are shown in table-2.

We check on web in order to know whether these 15 DNS servers are concerning with malicious online activities or not. In report for spam domains of KnujOn [15], dns01.gpn.register.com is reported as DNS server serving many spamming domains. In addition, at Malwareurl.com [16] dns01.gpn.register.com to dns05.gpn.register.com are reported as DNS servers hosting 129 malicious domains relating with 8 different types of malware, click fraud and exploits. The analysis result on each of the DNS server's domains name based on the information on web is shown in column 3,4 and 5 of table 2. Finally, 9 out of 15 DNS servers are confirmed as DNS servers relating with malicious online activities.

As for the fourth feature, by analyzing 74,830 DNS servers, we found 85 servers with at least one flux of more than 100 domains. We found a DNS server with as many as 145 fluxes. Out of the 85 servers, 13 are found on web reports as worst name servers of this year hosting spam domains, illicit Pharmacies domains and malware domains. In addition, 22 name servers out of the 85 are hosting at least one known black domain derived in the experiment for the first feature.

Table -1 DNS Servers with high % of black domains

Name Server's domain	Known Black	Existing Domain	Extended Black	% of black
ns1.pulsarserve.net	1	2	2	100
ns1.salenames.ru	1	14	14	100
ns2.ndoverdrive.com	2	17	17	100
ns2.pulsarserve.net	1	2	2	100
ns2.salenames.ru	1	14	14	100
ns37.coopertino.org	1	2	2	100
ns38.coopertino.org	1	2	2	100
ns5.no.cg.shawcable.net	1	3	3	100
ns6.so.cg.shawcable.net	1	3	3	100
sk.s2.ns1.ns92.kolmic.com	1	466	466	100
sk.s2.ns2.ns92.kolmic.com	1	466	466	100
ns1.namebrightdns.com	2	391	384	98.2097187
ns2.namebrightdns.com	2	391	384	98.2097187
ns1.dsredirection.com	44	1520	1485	97.6973684
ns3.domainingdepot.com	1	43	42	97.6744186
ns4.domainingdepot.com	1	43	42	97.6744186
ns2.dsredirection.com	44	1520	1481	97.4342105
ns.counter.co.kr	1	31	30	96.7741935
ns.induce.com	1	31	30	96.7741935
sell.internettraffic.com	32	1239	1197	96.6101695
buy.internettraffic.com	32	1239	1198	96.6908797
ns1.csof.net	7	23	22	95.6521739
ns2.csof.net	7	23	22	95.6521739
ns1.wordpress.com	49	570	541	94.9122807
ns1.parkingcrew.net	3	208	197	94.7115385
ns2.parkingcrew.net	3	208	197	94.7115385
ns2.bodis.com	10	414	389	93.9613527
ns1.bodis.com	9	413	388	93.9467312
ns1.dnslink.com	2	260	242	93.0769231
ns2.dnslink.com	2	260	242	93.0769231
ns2.wordpress.com	49	570	520	91.2280702

Table-2 DNS Servers involving in Fast Flux

No	Domain Name of DNS Server	TTL in Sec	Report on Web	Malicious Domain in Report	Detail
1	dns01.gpn.register.com.	60	Malwareurl.com/KnujOn	129/many	Malware
2	dns02.gpn.register.com.	60	Malwareurl.com	129/many	Exploits
3	dns03.gpn.register.com.	60	Malwareurl.com	129/many	Click fraud
4	dns04.gpn.register.com.	60	Malwareurl.com	129/many	Spam
5	dns05.gpn.register.com.	60	Malwareurl.com	129/many	
6	dns082.d.register.com.	60	No Report		
7	dns1.wavenet.com.ar.	0	No Report		
8	dns151.a.register.com.	60	Malwareurl.com	1	Malware
9	dns159.c.register.com.	60	Malwareurl.com	1	Malware
10	dns164.b.register.com.	60	No Report		
11	ns.induce.com.	60	No Report		
12	ns1.h69.hvosting.ua.	60	No Report		
13	ns1.hidc.co.kr.	100	Malwareurl.com	10	Malware
14	ns2.h69.hvosting.ua.	60	No Report		
15	ns2.hidc.co.kr.	100	Malwareurl.com	10	Malware

6. Related Works

There are some related studies by McAfee in which the analysis on name registration of malicious domains on .com TLD zone file is conducted.

Yuanchen He from Mcafee [17] tried to detect malicious domain registration in .com TLD DNs server. The insight in this study is that legitimate domains consist of English words or look like meaningful English while many malicious domain names are randomly generated and do not include meaningful words. The study shows that it is possible to transform this intuitive observation into statistically informative features using second order Markov models. Four transition matrices are built from

known legitimate domain names, known malicious domain names, English words in a dictionary, and based on a uniform distribution. The probabilities from these Markov models, as well as other features extracted from DNS data such as the total number of DNS servers that ever hosted a domain, the number of DNS servers that hosted this domain but not host it anymore, the average, maximum, and minimum string lengths of DNS servers hosting it, and so on are used to build a Random Forest classifier.

Shuang Hao [18] studied on the malicious domain registration of .com and .net domains. They explore the behavioral properties of these domains from DNS infrastructure associated with the domain and DNS lookup patterns from networks that are looking up the domains initially.

7. Conclusion and Future Works

This study proposes four features for finding malicious authoritative DNS servers. We evaluate the four features using real traffic of cache DNS servers. Our future works include a proposal of comprehensive detection method using the proposed features as well as deriving proper parameters for each feature.

8.Acknowledgement

A part of this study has been supported by PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) project by the Ministry of Internal Affairs and Communications, Japan.

9. Reference

[1] "McAfee—Antivirus, Encryption, Firewall, Email Security, Web Security, Risk & Compliance." [Online]. Available: http://www.mcafee.com/us/.[Accessed: 29-Jan-2013].

[2] "HOW FAST-FLUX SERVICE NETWORKS WORK | The Honeynet Project." [Online]. Available: http://www.honeynet.org/node/132. [Accessed: 21-Jan-2013].

[3] G Ollmann, "Understanding the intricacies of botnet command-and-control" . [Online]. Available: https://www.damballa.com/downloads/r_pubs/WP%20Botnet%20Communications%20Primer%20(2009-06-04).pdf [Accessed: 21-Jan-2013].

[4] "DNS hosting service - Wikipedia, the free encyclopedia." [Online]. Available: http://en.wikipedia.org/wiki/DNS_hosting. [Accessed: 26-Jan-2013].

[5] "Domain name registrar - Wikipedia, the free encyclopedia." [Online]. Available:http://en.wikipedia.org/wiki/Domain_name_registrar. [Accessed: 26-Jan-2013].

[6] "SSAC Advisory on Fast Flux Hosting and DNS",[Online]. Available: www.icann.org/en/groups/ssac/documents/sac-025-en.pdf [Accessed: 27-Jan-2013].

[7] "How Criminals Defend Their Rogue Networks | abuse.ch." [Online]. Available: http://www.abuse.ch/?p=3387. [Accessed: 27-Jan-2013].

[8] "Morto worm sets a (DNS) record | Symantec Connect Community." [Online]. Available: http://www.symantec.com/connect/blogs/morto-worm-sets-dns-record. [Accessed: 19-Dec-2012].

[9] "RFC 1035" [Online]. Available: http://www.ietf.org/rfc/rfc1035.txt. [Accessed: 29-Jan-2013].

[10] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, "Exposure: Finding malicious domains using passive dns analysis," in *Proceedings of NDSS*, 2011.

[11] "ZeuS Tracker :: Monitor." [Online]. Available: https://zeustracker.abuse.ch/monitor.php. [Accessed: 01-Mar-2013].

[12] "Malware Domain List." [Online]. Available: http://www.malwaredomainlist.com/. [Accessed: 01-Mar-2013].

[13] R. Tanabe, Y.Tie, M.Mito,M.Daisuke,M.Kamizono Y.Hoshizawa,K.Yoshioka,T.Matsumoto,"Extracting Signatures from Malware DNS Traffic by Long-Term Sandbox Analysis", in . CSS2012, 712-719, 2012

[14] "By Nameserver Statistics." [Online]. Available: http://knujon.com/nameservers/index.html. [Accessed: 03-Mar-2013].

[15] "Spam domains served from DNS01.GPN.REGISTER.COM - Updated: 2/26/2013." [Online]. Available: http://knujon.com/nameservers/DNS01.GPN.REGISTER.COM.html. [Accessed: 03-Mar-2013].

[16] "MalwareURL." [Online]. Available: http://www.malwareurl.com/ns_listing.php?ns=dns02.gpn.register.com. [Accessed: 03-Mar-2013].

[17] Y. He, Z. Zhong, S. Krasser, and Y. Tang, "Mining DNS for Malicious Domain Registrations," in *Collaborative Computing: Networking, Applications and Worksharing 2010 6th International Conference on*, 2010, pp. 1–6.

[18] S. Hao, N. Feamster, and R. Pandrangi, "Monitoring the initial DNS behavior of malicious domains", in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011, pp. 269–278