Towards classification of DNS erroneous queries

Yuta Kazato
Waseda University, Japan
kazato@fuji.waseda.jp

Kensuke Fukuda
NII, Japan
kensuke@nii.ac.jp

Toshiharu Sugawara
Waseda University, Japan
sugawara@waseda.jp

ABSTRACT

We analyze domain name system (DNS) errors (i.e., ServFail, Refused and NX Domain errors) in DNS traffic captured at an external connection link of an academic network in Japan and attempt to understand the causes of such errors. Because DNS errors that are responses to erroneous queries have a large impact on DNS traffic, we should reduce as many of them as possible. First, we show that ServFail and Refused errors are generated by queries from a small number of local resolvers and authoritative nameservers that do not relate to ordinary users. Second, we demonstrate that NX Domain errors have several query patterns due to mostly anti-virus/anti-spam systems as well as meaningless queries (i.e., mis-configuration). By analyzing erroneous queries leading to NX Domain errors with the proposed heuristic rules to identify the main causes of such errors, we successfully classify them into nine groups that cover approximately 90% of NX Domain errors with a low false positive rate. Furthermore, we find malicious domain names similar to Japanese SNS sites from the results. We discuss the main causes of these DNS errors and how to reduce them from the results of our analysis.

Categories and Subject Descriptors

C.2.0 [**Computer Communication Networks**]: General

General Terms

Measurement, Management, Security

Keywords

DNS, Classification, DNS error, Mis-configuration

AINTEC'13, November 13–15, 2013, Chiang Mai, Thailand.

1. INTRODUCTION

The domain name system (DNS) is one of the most important functionalities in the Internet. It provides translation service between domain names and IP addresses. However, it is reported that the DNS has also been abused for non-legitimate purposes such as spam and distributed denial of service (DDoS) attacks. Therefore, it is necessary to understand abnormal and unnatural DNS behaviors for preventing queries from malicious systems for Internet security purposes.

To date, many studies have been devoted to DNS measurement and analysis [1–11, 13, 14, 16]. DNS errors are caused by un-resolvable DNS queries from local resolvers. We still have less enough knowledge about the causes of the DNS errors for reducing them. In addition, a huge number of DNS errors unnecessarily consume network resources as well as those of DNS servers.

Thus, we analyze the DNS traffic using passive DNS measurement at an external connection link of an academic backbone network in Japan. In particular, we focus on DNS errors, such as ServFail, Refused, and NX Domain, sent from authoritative nameservers in external networks to local resolvers in the academic network. We report on a number of abnormal phenomena likely caused by malicious and abnormal systems. First, we find that most of ServFail and Refused errors are replies to queries from a small number of resolvers. We also discuss a number of problematic authoritative nameservers that always send back these errors. Second, we classify NX Domain errors with the proposed heuristic classification rules that identify the main causes of such errors from the features of observed domain names. We show that they fall into nine groups covering with 88.7% of observed unique domain names. As a result, we confirm that NX Domain errors are mostly caused by specific anti-virus client software and anti-spam systems that generate many queries for checking if domains are registered on a black-list for legitimate purposes, as well as mis-configurations of servers and end-user machines that query wrong domain names. We also find a set of malicious domains for spam by applying one of the classification rules to legitimate answer domains. Finally,

we discuss possible improvement approaches to reduce such DNS errors from the results of our analysis.

2. RELATED WORK

DNS measurement studies are classified into two types: analysis of traffic from the perspective of authoritative nameservers [1, 4, 7, 10, 11, 14] and from the perspective of local resolvers [2, 3, 5, 6, 8, 9, 13, 16]. Refs. [14] and [4] analyzed DNS queries to root DNS servers. They found that the number of queries per local resolver was highly biased, and 98% of the queries to the root servers were worthless or redundant queries. The AS112 project [11] also accommodated PTR queries for RFC 1918 private addresses that were sent up to the root server, caused errors. Refs. [5, 8, 13] collected their traffic data from campus networks. In contrast, we captured more large-scale traffic data at an external connection link of an academic network and observed DNS traffic from/to local resolvers of universities and institutes in Japan.

Characterizing DNS errors is an important field in DNS research [6, 9, 12]. Ref. [6] analyzed negative answers, which are queries that do not return "NOERROR", from DNS traffic data. Ref. [9] also characterized DNS query failures by analyzing DNS failure graphs to identify suspicious and malicious activities. Ref. [12] revealed specific types of mis-configurations in the DNS. In this paper, we focused on analyzing these erroneous queries in deeper levels of DNS errors.

Recently, several studies have attempted to identify domains used for malicious activities (i.e., Botnet, Spambot, and DDoS) from passive DNS analysis [1,2,6,7,15]. Kopis [1] and Exposure [2] are malicious domain detection systems using the DNS features of legitimate and malicious domains. Ref. [15] detected algorithmically generated domain names and found several groups such as a Botnet group, trojan group, and group sharing of a single IP address. We provide another approach that uses the DNS features of observed domains and the heuristic classification of malicious domains.

3. DATASET

We collected UDP port 53 packets passing through a transit link in a Japanese academic backbone network by using the tcpdump command for 1 month in Feb. 2013. The total number of captured packets were approximately 15.8 billion packets (size: 175.1 GB). The UDP packets contained DNS queries from local DNS resolvers in the academic network to authoritative nameservers in external networks (35.7%), DNS replies from authoritative nameservers in external networks (27.6%), DNS queries from DNS resolvers in external networks (12.4%), DNS replies from authoritative nameservers in the academic networks (16.6%), and other packets that are not related to the DNS (7.8%). Due to the asymmetric nature of routing, inbound and outbound traffic volumes are synchronized but are not the same. We mainly analyzed DNS replies from authoritative nameservers in external networks to local resolvers in an academic network. The total number of unique cache resolver's IPs in the academic network and authoritative nameserver's IPs in external networks were 21,537 and 62,827, respectively. The local resolvers in the academic network were located mainly at universities (approximately 90%).

4. ANALYSIS

4.1 Temporal behavior of DNS error

We first categorized DNS replies from authoritative nameservers in external networks into four types: (1) correct answer reply, (2) DNS delegation reply, (3) DNS error reply that authoritative nameservers could not answer, and (4) reply from OpenDNS resolvers and Google public DNS resolvers in external networks, not authoritative servers. We investigated (1) and (3) because these replies show the final answers to the request from local resolvers. Then, we classified errors in the datasets into the following three types: (a) NX Domain errors, (b) ServFail errors, and (c) Refused errors (see also Table 1). In addition, the number of replies from OpenDNS and Google public DNS was a total of 1,184 packets, however, we excluded these replies in the following analysis due to negligible contribution.

Table 1: Type of DNS error

Error type	Explanation
NX Domain	Domain name referenced in the query does not exist.
ServFail	authoritative nameserver could not process due to a problem with authoritative nameserver.
Refused	authoritative nameserver refuses to perform the operation for policy reasons.

We focused on the following time series (bin = 1 hour) constructed from the original DNS reply packets:

- the number of the DNS correct answer replies and DNS errors
- the number of the unique local resolvers and authoritative nameservers
- the percentage of queried resource record types (QTYPEs) that reply DNS errors
- the maximum number of queries per local resolver and per authoritative nameserver
- the entropies of the number of queries per local resolver and per authoritative nameserver

Figure 1 shows the daily variation in DNS reply packets that sent from authoritative nameservers in external networks to local resolvers in the academic network for

one month period. 19% of the replies were DNS errors. The number of correct answer replies increased in the daytime and decreased at night, correlating to activities at Japanese universities. In contrast, the number of DNS errors did not vary substantially compared to that of correct answer. Moreover, at label A (3-5pm, 23rd Feb) in Fig. 1, there was an abnormal event in which 1,255 authoritative nameservers sent 73,168,465 replies to one local resolver in the academic network. These replies show the A record answers of root DNS servers and the same QTYPE, ANY. The figure also confirms periodic spikes at 4-5am.

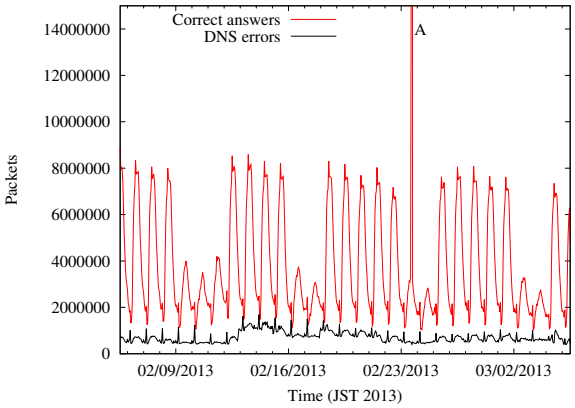

Figure 1: Daily variation in DNS replies from authoritative nameservers to local resolvers

Figure 2 shows the number of the three DNS errors. The temporal traffic pattern was different among the types of DNS errors. The fluctuations in the replies of ServFail errors were not characterized by a diurnal pattern because they varied sharply regardless of human activity. The fluctuations in the replies of Refused errors also exhibited periodic huge spikes at a certain time (4-5am). Thus, these characteristic phenomena in the two types of errors were not human oriented and were mainly caused by external reasons. The fluctuations in the replies of NX Domain errors, however, showed the following two important points: (1) they are synchronized to the total DNS traffic, as shown in Fig. 1, meaning that the cause of this error is likely due to ordinary users. (2) At 4-5am, they exhibited periodic spikes that were not human oriented. In addition, we found that the number of replies of ServFail errors greatly decreased at 10-12am on 4th Mar. Table 2 lists the percentage of the QTYPE of the DNS errors. We confirm that the main causes of the errors were A and PTR record queries. Furthermore, the QTYPE of ServFail and Refused errors represent for higher percentages of PTR record than that of NX Domain errors.

Figures 3 and 4 represent the number of local resolvers and that of authoritative nameservers per correct answers (OK) and type of errors, respectively. One local resolver (or authoritative nameserver) can be counted multiple times and appear in multiple time series. The fluctuations in the number of local resolvers clearly represent the diurnal traffic pattern. Additionally, the fluctuations in the number of local resolvers involved with Refused and ServFail errors represents the spiky behavior at 4-5am with the diurnal pattern consistent with the previous figure. The fluctuations in the number of authoritative nameservers that answer NX Domain errors also showed the spiky behavior at 4-5am. We confirm that these spikes are significant in abnormal and unnatural behaviors of local resolvers and authoritative nameservers. We found that the number of authoritative nameservers that answer the replies of NX domain errors and the correct answers increased at midnight (0-5am). This large number of queries were sent by one local resolver in the academic network.

We further investigated the details of local resolvers and authoritative nameservers that are related to receiving or sending a large number of DNS query packets. We found that 98% of ServFail errors were replies to queries sent from three local resolvers inside one organization in the academic network. Moreover, all of the replies were sent from one authoritative nameserver in external networks. Then, at 10-12am on 4th Mar, these replies greatly decreased because three local resolvers stop sending the queries. Similarly, over 20,000 packets of Refused errors per hour were replies to queries sent from two local resolvers inside one organization in the academic network from one authoritative nameserver in

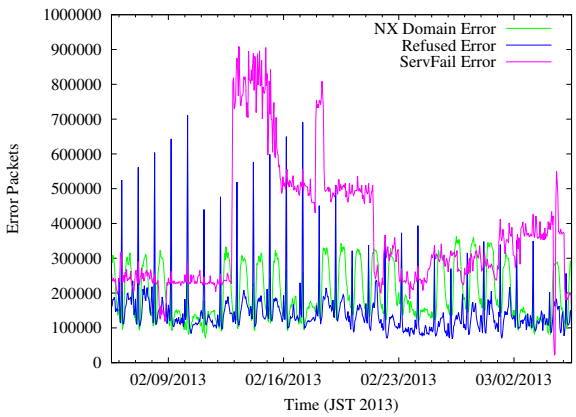

Figure 2: Number of DNS errors

Table 2: QTYPE of erroneous queries

QTYPE	NX (%)	ServFail (%)	Refused (%)
A	56.4	58.1	47.6
PTR	23.9	36.1	37.6
AAAA	5.8	2.8	6.0
MX	0.6	2.9	2.5
Others	13.3	0.1	6.3

the external networks. At 4-5am, over 170,000 replies of Refused errors was sent to 1,275 local resolvers from two authoritative nameservers. These two authoritative nameservers located inside one organization and periodically sent a large number of replies (4-5am), then all of these (queried) QTYPEs were PTR records that requested IP addresses assigned to this organization. Moreover, the maximum number of NX Domain errors were the replies sent from the root DNS servers. The spikes at 4-5am were due to some local resolvers requested PTR record queries, different from those of Refused Errors.

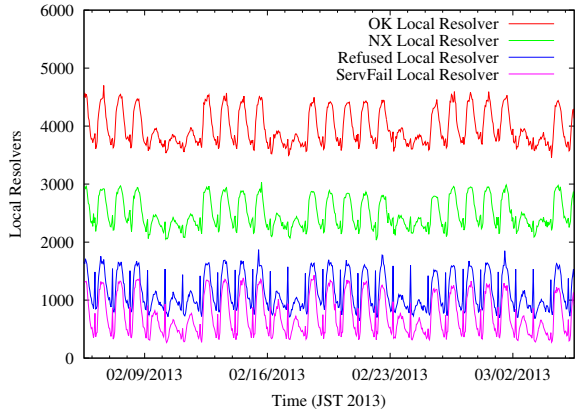

Figure 3: Number of local resolvers

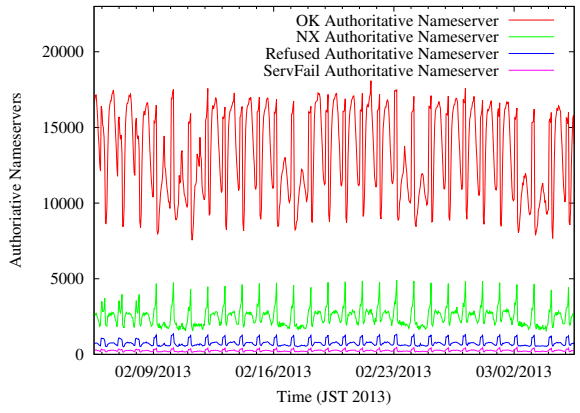

Figure 4: Number of authoritative nameservers

We also calculated the entropies of the number of queries per local resolver and authoritative nameserver. Entropy is a metric to indicate the diversity of a dataset; in our context, a small entropy corresponds to the situation in which a small number of resolvers receive (or nameservers send) most replies to queries, and a large entropy means that each resolver receives (or nameserver sends) replies to queries equally. Figures 5 and 6 show the entropies of the local resolvers and those of the authoritative nameservers, respectively. The entropy of replies and that of NX Domain errors in local resolvers indicate diurnal patterns; however, the entropies of Refused and ServFail errors do not. We also found periodic spikes in Refused errors in both figures at 4-5am. We observed that a large number of replies of Refused error are sent to 1,275 local resolvers from two authoritative nameservers at 4-5am. Therefore, fluctuations in the entropies of the authoritative nameservers in Refused errors decreased and those of increased due to the skew of sending queries from two authoritative nameservers to many local resolvers in the academic network.

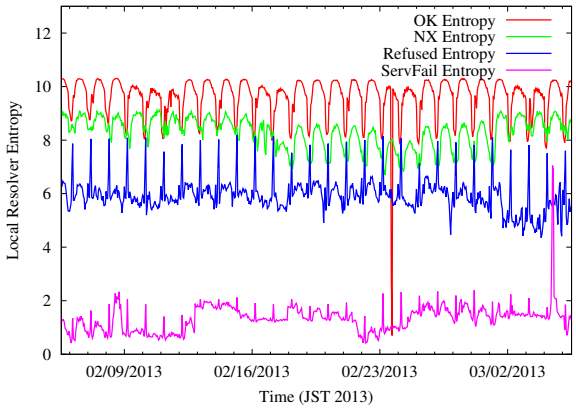

Figure 5: Entropy of local resolver

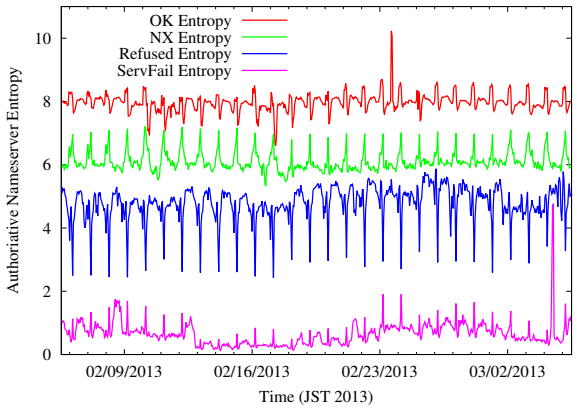

Figure 6: Entropy of authoritative nameserver

Figure 7 shows a scatter plot of the entropy of local resolvers and authoritative nameservers. The plots are roughly characterized by a linear relationship. However, we also visually confirm multiple clusters in the same group. In Refused errors, a cluster labeled B corresponds to the time period we observed spiky behavior. Another cluster C represents the behavior of correct replies at midnight. These results show that the specific local resolvers or authoritative nameservers re-

peated the same behaviors each day.

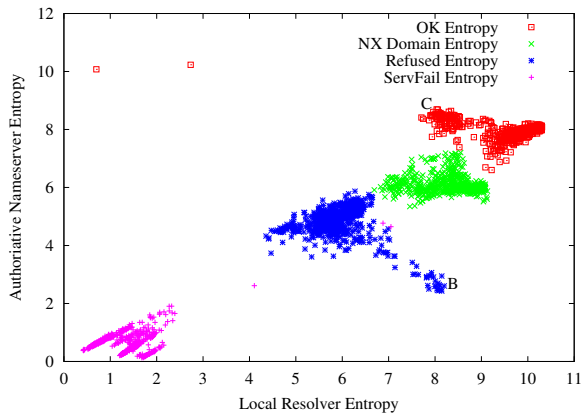

Figure 7: Scatter plot of correlation between entropy of local resolvers and authoritative nameservers

4.2 Outliers in DNS error

Let us turn to the characteristics of query content. The DNS reply from authoritative nameserver contains QNAME filed in its question section. Thus, question section has a QNAME field that includes the domain name requested the local resolver. In this work, we refer to a domain name in QNAME as a "query name".

We characterized the query names of each error and that of each correct answer (OK) reply. The top five most frequent query names of ServFail errors accounted for 93.7% of all these queries. Combined with the previous results, we conclude that most queries causing ServFail errors from the local resolvers inside one organization have the same query names. The most frequent query name of Refused errors also accounted for 27.6% of all these queries, and the reverse lookup query names of the IP addresses assigned to one organization were 15.6% of all these queries. The top seven frequent query names of NX Domain errors are listed in Table 3. These query names include incorrect names such as "local", "-", local IP address, and the domains of the web proxy auto discovery protocol (WPAD). We also confirm that the most frequent query names of replies include the answers of the root DNS servers, "isc.org," and Akamai CDN servers. The results of correct answer replies yield two implications. First, CDNs (like Akamai) control the direction of their traffic frequently and efficiently in the DNS. Second, most queries "isc.org" use ANY QTYPE record. The replies of ANY record contain all information about root DNS servers (at label A in Fig. 1) or "isc.org"; thus, they cause huge traffic volume and consumption of resources. These ANY record queries are known to be used by a DNS amplification attack, which is a popular DDoS attack. Finally, Table 4 lists the number of unique query names in DNS errors. The query names of NX Domain errors include a wide variety of domain names requested by end-users.

Table 3: Top most frequent query names of NX Domain errors

Query name	Percentage (%)
local	7.09
0.0.0.0	0.49
192.168.100.1	0.47
wpad.iptvf.jp	0.37
wpad.flets-east.jp	0.32
-	0.31
wpad.flets-west.jp	0.30

Table 4: Number of unique query names in DNS errors

Error type	Unique query name
NX Domain error	16,269,762
Refused error	305,436
ServFail error	94,825

4.3 Classification of NX Domain error query names

Next, we classified query names of NX Domain errors with our heuristic rules to identify the main causes of such errors. The purpose of this classification is to estimate plausible root causes of NX Domain errors from features of observed query names. We evaluated the following two datasets for the classification. First, we analyzed the error patterns from the dataset that contains query names of NX Domain errors in non-PTR replies (i.e., A, AAAA, and MX QTYPEs) per day and that of replies per day. Second, we analyzed the unique query names appeared in the above datasets.

Our heuristic classification rules are extensions of Ref. [14] and we added new pattern rules from the observed query name features, as shown in Table 5. We finally applied nine rules; Patterns 1 and 2 are rules for domains of anti-virus and anti-spam systems, and Pattern 3 is a rule for non-registered top level domains (TLDs). Patterns 4-9 are rules for unwanted domains in the DNS. We constructed each classification pattern using combinations of regular expressions. Specifically, Pattern 4 estimates the randomness score in query name from the bigram of the correct domain names.

Table 6 lists the classification results of NX Domain errors for query names (i.e., true-positive) and those of replies (i.e., false-positive). Each row represents the number of query names hit by a single rule, and the final results were obtained by all these rules. We classified 73.1% of all the query names of NX Domain error with a low percentage of false positives (0.15%).

Table 7 lists the classification results of NX Domain errors for unique query names and those of correct answer replies. Again, we classified 88.7% unique query

Table 5: Classification rules

No	Rule	Example
1	Used by anti-virus software	waseda.jp.uri.jp1.sophosxl.com
2	Used by anti-spam RBL	1.0.0.0.zen.spamhaus.org
3	Unknown TLD	example.TEst
4	Random words	qebwprbpyy.ac.jp
5	Add "dlv.isc.org"	example.com.dlv.isc.org
6	Configuration words	local, wpad
7	Local name	YUTA-PC
8	(IP Address)+(TLD) or repetition of TLD	192.168.0.11.ac.jp www.waseda.jp.ac.jp
9	RFC 1034 violation	(10.3.1.3).go.jp, ***.com

names of NX Domain errors and a low false-positives rate (1.45%). We also found specific domains, including a string of domain names of social networking services (SNSs) (e.g., mixi, gree, and mbga) in Japan, in the false-positive results of Pattern 4. These query names whose QTYPE is A, NS, and MX point to two IP addresses: 4,179 domains to one IP address and 709 domains to the other IP address. We also confirm 2,134 query names of these special SNS-like domain names in the results of Pattern 4 of NX Domain errors. Table 8 lists examples of SNS-like domain names.

Table 6: Classification results of all query names

Pattern rules	NX Domain datasets		Correct answer datasets	
	true-positive	(%)	false-positive	(%)
Total number	2,957,367		81,407,171	
Pattern 1	578,280	19.6	43,147	0.05
Pattern 2	474,694	16.1	43,704	0.05
Pattern 3	455,968	15.4	168	<0.01
Pattern 4	334,786	11.3	33,124	0.04
Pattern 5	180,967	6.1	262	<0.01
Pattern 6	129,448	4.4	524	<0.01
Pattern 7	138,033	4.7	352	<0.01
Pattern 8	71,769	2.4	3	<0.01
Pattern 9	40,444	1.4	405	<0.01
Final result	2,160,768	73.1	122,385	0.15

Table 7: Classification results of unique query names

Pattern rules	NX Domain datasets		Correct answer datasets	
	true-positive	(%)	false-positive	(%)
Total number	951,126		2,155,635	
Pattern 1	271,260	28.5	13,351	0.62
Pattern 2	188,716	19.8	13,837	0.64
Pattern 3	219,633	23.1	7	<0.01
Pattern 4	164,263	17.3	3,483	0.16
Pattern 5	48,379	5.1	40	<0.01
Pattern 6	28,730	3.0	45	<0.01
Pattern 7	27,238	2.9	33	<0.01
Pattern 8	21,339	2.2	3	<0.01
Pattern 9	21,295	2.2	185	0.01
Final result	843,601	88.7	31,181	1.45

We now investigate the SNS-like domains in detail. First, by manually checking the IP addresses pointing the SNS-like domains by Google searches, we find that those IP addresses were reported as hosts sending spam. Similarly, one of the addresses is listed in the Spamhaus blacklist. Thus, the SNS-like domains are likely used for sending spam. We confirm that these SNS-like domains were mostly requested by only one local resolver in a university during the measurement period. We examined the frequency of these queries per day and the life time from the first to last queries that appeared in the dataset. Figure 8 shows the number of new SNS-like domains appearing in the DNS traffic. Most domains appeared on the first day and the number of domains decreased exponentially over time. We also found that

Table 8: Examples of SNS-like domain names

Domain names	
www.akivcsgree.jp	www.yrjtohjmbga.jp
mail.gtasomgree.jp	www.bsyhdjaskwheatmixi.jp
yrtwetwamixi.jp	www.lkjaysaddlebrowngree.jp
mayonnaisembga.jp	ns1.djbngree.jp

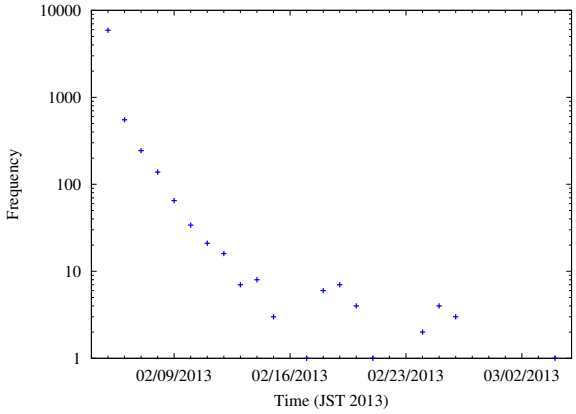

Figure 8: Newly appeared SNS-like domains

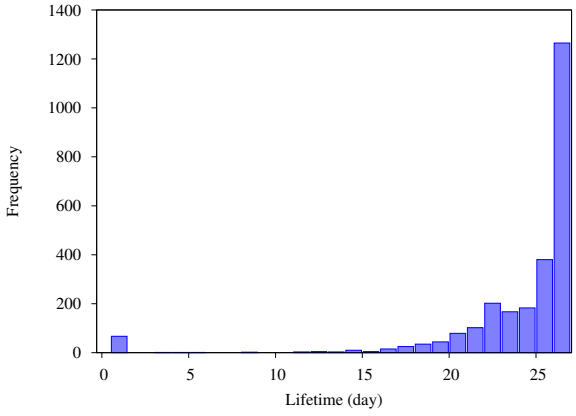

Figure 9: Lifetime of SNS-like domains

the appearance of these domains was stable over time for one month. Figure 9 shows the lifetime of SNS-like domains in the dataset. Most domains remained for one month; however, some disappeared in only one day or in

about twenty days. In summary, the SNS-like domains were stable during our measurement.

5. DISCUSSION

5.1 Types of DNS errors

5.1.1 ServFail error

Most ServFail errors were replies to queries sent from three local resolvers inside one organization in the academic network, and all these replies were sent from one authoritative nameserver in external networks. These abnormal queries caused 98% of observed ServFail errors. Additionally, the top frequent query names were mostly similar. As shown in Fig. 2, the fluctuations in ServFail errors replies did not correlate with the diurnal pattern. Also, the entropies of ServFail errors (Figs. 5, 6 and 7) were smaller than other entropies due to the bias queries of local resolvers and authoritative nameservers. In summary, the DNS queries causing ServFail errors are related to a small number of local resolvers and authoritative nameservers and have a large impact on DNS traffic. We expect that the number of ServFail errors will greatly decrease if we stop specific resolvers, similar to 10-12am on 4th Mar.

5.1.2 Refused error

In Refused errors, we found two notable results; over 20,000 packets of Refused errors were replies to queries sent from two local resolvers inside one organization in the academic network from one authoritative nameserver in the external networks. At 4-5am, over 170,000 replies of Refused error were sent to 1,275 local resolvers from two authoritative nameservers located inside one organization, then all these QTYPEs were PTR records that request IP addresses assigned to this organization. This periodic increase in Refused errors is shown in Fig. 2 and the entropies are shown in Figs. 5, 6 and 7. Also, the number of local resolvers (Fig. 3) resulted in a periodic increase in local resolvers generating Refused errors at 4-5am. These periodic spikes of Refused errors were due to the requests of reverse lookup IP addresses assigned to one organization in external networks in China from many local resolvers in the academic network. These phenomena are most likely caused by infected end-users or applications. Therefore, by blocking these periodic abnormal behaviors, we expect to reduce DNS error traffic.

5.1.3 NX Domain error

The variation in the replies of NX Domain errors was synchronized to the total DNS traffic, as shown in Figs. 1 and 2. The periodic spikes of NX Domain Errors at 4-5am were caused by the PTR record queries from some local resolvers, different from those of Refused errors. It should be noticed that the top frequently used types of query names causing NX Domain errors were incorrect due to mis-configurations (Tab. 3) and many unique query names causing NX Domain errors were requested by local resolvers and different from other errors (Tab. 4). Thus, NX Domain errors are characterized by query patterns of incorrect user inquiries, misconfigurations, and software bugs, which largely differ from the other errors.

5.2 Query names causing NX Domain errors

5.2.1 Main cause of NX Domain error query names

We applied our heuristic classification rules to queries causing NX domain errors. In Section 4.2, we classified 73.1% of all query names of NX Domain errors and 88.7% of unique query names of such errors. The results suggest that Patterns 1, 2, 3, and 4 are significant rules for characterizing NX domain errors. Thus, we conclude that the main causes of NX Domain errors are specific anti-virus client software and anti-spam systems (Patterns 1 and 2), using wrong domains (Patterns 3, 4, 8, and 9), and mis-configuration of servers and end-user machines(Patterns 5, 6, and 7).

5.2.2 False-positives in classification

We could classify most query names of NX Domain errors with our heuristic rules; however, we mis-classified the query names of correct answer replies as false-positive. Table 7 shows higher mis-classification ratios by anti-virus software (Pattern 1) and anti-spam systems (Pattern 2). These queries are in fact legitimate and used effectively for anti-virus software and anti-spam systems, although they generate a huge number of replies of NX Domain errors because anti-spam systems check whether queried domains are on a black-list and generate many A record queries. Additionally, the classification results for NX Domain error query names and for correct reply query names (Table 6) suggest the number of true-positives of Patterns 1 and 2 are approximately 13 times higher than the number of false-positives. Therefore, many replies of NX Domain errors generated by these systems are legitimate.

The false-positive of Pattern 3 (non-registered TLDs) shows 7 query names, but, it should be zero because of no answer to these unknown TLDs in DNS. Our manual inspection clarified that one authoritative nameserver wrongly answers to the query of "local domain.".

5.2.3 Malicious domains

We conducted a randomness test of query names using the bigram list in Pattern 4. As shown in the classification results of unique query names (Table 7), the percentage of false-positives in Pattern 4 (0.16%) was higher than other results. We found the SNS-like do-

main names composed of random strings and SNS domains in Japan (i.e mixi, gree, mbga) in the results of Pattern 4 for correct answer replies. In fact, the A record answers of these domains pointed to two IP addresses. We also found 2,134 query names of these SNS-like domain names in the results of Pattern 4 for NX Domain errors. We confirm that these IP addresses were reported by Google search as hosts sending spam and one of the two IP addresses is listed in the Spamhaus IP blacklists. We again examined the DNS lookup answers of 4,888 SNS-like domain names that point to two IP addresses in July 2013. As a result, 27.8% of these SNS-like domain names answers caused NX Domain errors. We suspect that these SNS-like domain names groups are used for malicious activities, more specifically sending spam, and are throw away domains to avoid blacklisting and de-registering.

5.3 Further improvements

We analyzed DNS errors to understand the causes of such errors, and provided plausible roots of NX domain errors. We now discuss further improvements in reducing DNS errors. First, most ServFail and Refused errors are generated by a small number of local resolvers and authoritative nameservers. For example, 98% of replies of ServFail errors are redundant and generate the abnormal behaviors. Therefore, it is necessary to inform the network administrators of such behaviors and ask them to improve the causes of these behaviors.

Second, there are three main causes of NX Domain errors: specific anti-virus software and anti-spam systems for legitimate purpose, using wrong domains, and mis-configurations. It is also necessary to mitigate the mis-configurations or system bugs that generate these queries. Additionally, server (network) administrators should prevent abnormal queries from their networks. Further traffic growth and deployment of anti-spam software or anti-virus systems using the DNS may hide malicious activities in a large number of NX Domain errors. Thus, the intelligent monitors will be more important in the future. Such monitors located at local resolvers must sense the queries generating errors with high probability. These monitors are expected to reduce the authoritative nameservers load.

6. CONCLUSION

To investigate the main causes of DNS errors, we analyzed DNS queries measured at an external connection link of an academic backbone network in Japan. We found that ServFail and Refused errors are caused by a small number of local resolvers and authoritative nameservers that do not relate to ordinary users. Additionally, we classified NX Domain errors with the proposed heuristic rules. These rules cover with approximately 90% of the unique domain names of NX Domain errors and provide three plausible main causes. We also found malicious domain names, which include SNS-like strings, by conducting a random test to correct answer replies. Finally, we discussed further improvements concerning DNS errors.

Our future work will be microscopic analysis of DNS traffic behaviors including IPv6, evaluation of our classification rules in other datasets, and further investigation on finding malicious activities.

7. ACKNOWLEDGMENTS

This research has been supported by JSPS KAKENHI Grant Number 23680005, and by the Strategic International Collaborative R&D Promotion Program of the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533 (NECOMA).

8. REFERENCES

[1] M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou II, and D. Dagon. Detecting Malware Domains at the Upper DNS Hierarchy. In *USENIX Security Symposium*, page 16, 2011.
[2] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In *NDSS*, page 17, 2011.
[3] N. Brownlee, K. Claffy, and E. Nemeth. DNS Root/gTLD performance measurements. *USENIX LISA*, pages 241–256, 2001.
[4] S. Castro, D. Wessels, M. Fomenkov, and K. Claffy. A Day at the Root of the Internet. *ACM SIGCOMM Computer Communication Review*, 38(5):41–46, 2008.
[5] K. Fujiwara, A. Sato, and K. Yoshida. DNS Traffic Analysis: Issues of IPv6 and CDN. In *SAINT 2012*, pages 129–137, 2012.
[6] H. Gao, V. Yegneswaran, Y. Chen, P. Porras, S. Ghosh, J. Jiang, and H. Duan. An empirical reexamination of global DNS behavior. In *SIGCOMM'13*, pages 267–278, 2013.
[7] S. Hao, N. Feamster, and R. Pandrangi. Monitoring the initial DNS behavior of malicious domains. In *IMC'11*, pages 269–278, 2011.
[8] K. Ishibashi and K. Sato. Classifying DNS heavy user traffic by using hierarchical aggregate entropy. In *WTC 2012*, pages 1–6, 2012.
[9] N. Jiang, J. Cao, Y. Jin, L. E. Li, and Z.-L. Zhang. Identifying suspicious activities through DNS failure graph analysis. In *ICNP 2010*, pages 144–153, 2010.
[10] A. Kalafut, M. Gupta, C. Cole, L. Chen, and N. Myers. An empirical study of orphan DNS servers in the internet. In *IMC'10*, pages 308–314, 2010.
[11] P. Vixie. AS112 project. http://www.as112.net/.
[12] V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, and L. Zhang. Impact of configuration errors on DNS robustness. In *SIGCOMM'04*, pages 319–330, 2004.
[13] D. Plonka and P. Barford. Context-aware clustering of DNS query traffic. In *IMC'08*, pages 217–230, 2008.
[14] D. Wessels and M. Fomenkov. Wow, that's a lot of packets. In *PAM'03*, page 9, 2003.
[15] S. Yadav, A. Reddy, A. Reddy, and S. Ranjan. Detecting algorithmically generated malicious domain names. In *IMC'10*, pages 48–61, 2010.
[16] B. Zdrnja, N. Brownlee, and D. Wessels. Passive Monitoring of DNS Anomalies. In *DIMVA'07*, pages 129–139, 2007.