A Look Over on The Usages of Relatively Rare Types of DNS Resource Records

Hikaru ICHISE[†a)], **Yong JIN**[††b)], **Satoru SUNAHARA**[†††c)], **Takao KONDO**[††††d)], ***Members***, ***and*** **Katsuyoshi IIDA**[††††e)], ***Senior Member***

1. Introduction

Domain Name System (DNS) contains many types of resource records each of which has been standardized for the specific purpose in the Internet services. In addition, recently some new types of DNS resource records also have been added or under the review process. For example, the HTTPS resource record is one of the new types of DNS resource records which is designed for the usage of accessing Web sites [1]. Another example is the ALIAS resource record which provides Amazon Route 53 services to the Internet users [2]. On the other hand, there are also some obsoleted resource record types such as MD (Mail Destination) and MF (Mail Forwarder) resource records, which had been replaced by MX (Mail Exchange) resource record [3]. It is more likely that some own-developed type and obsoleted resource records are used for malicious communication causing various attacks as unknown resource records.

Based on this observation, we aim to analyze and investigate the usage of relatively new types of DNS resource records using DNS traffic. In this paper, we describe the analysis methodology of DNS traffic for the relatively new types of resource records.

2. Analysis and Investigation methodology

Figure 1 illustrates the architecture to obtain DNS traffic for the analysis. We intend to obtain all DNS traffic between internal computers and DNS full-service resolver (1. Internal DNS traffic) and between DNS full-service resolver and the Internet (2. External DNS traffic) by port mirroring. Moreover, the DNS query and response pairs (DNS traffic) are stored in DNS traffic server for the further analysis. Note that the IP address of the internal computer is anonymized for protecting the user privacy before the analysis. After that, we analyze and investigate the obtained DNS traffic based on the following procedures.

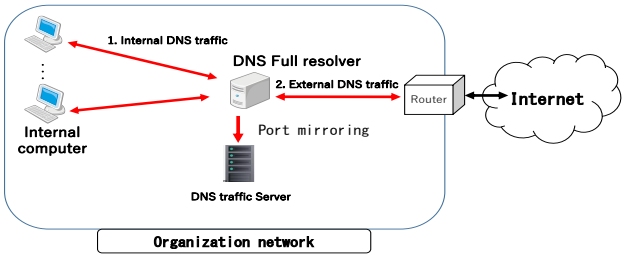

Fig. 1 Architecture to obtain DNS traffic

(1) Statistically analyze the obtained DNS resource record types such as A, MX, HTTPS, and ALIAS, etc.
(2) Statistically analyze the Time To Live (TTL) value of each resource record.
(3) Investigate the usages of each resource record.
(4) Check the destination IP addresses of the DNS query packets for unknown resource record type on the third-party Web site like Virustotal.com.
(5) Check the destination IP addresses of the DNS query packets for obsoleted resource record type on the third-party Web site like Virustotal.com.

Based on the above analysis, our objective is to check the usage of new types of DNS resource records. In addition, we will consider the detection system for addressing the unknown DNS traffic through the analysis.

3. Conclusion

We explained the analytical methodology of DNS traffic captured from the DNS full-service resolvers setup in an organization network. Our main objective is to check the usage of relatively new types of DNS resource records from the obtained DNS traffic. In future work, we plan to present the analysis results and also consider the detection system of malicious usages of DNS resource records.

References

[1] B. M. Schwartz, M. Bishop , E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)," *IETF Internet-Draft*, May. 2023.
[2] Amazon Ins, "Alias records," `https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html`, Accessed on June. 26, 2023.
[3] P. Mockapetris, "Domain System Changes and Observations," *IETF RFC973*, Jan. 1986.

[†]Open Facility Center, Tokyo Institute of Technology, Japan.
[††]Global Scientific Information and Computing Center, Tokyo Institute of Technology, Japan.
[†††]Faculty of Science and Engineering, Chitose Institute of Science and Technology, Japan.
[††††]Information Initiative Center, Hokkaido University, Japan.
a) E-mail: hichise@nap.gsic.titech.ac.jp
b) E-mail: yongj@gsic.titech.ac.jp
c) E-mail: s-sunaha@photon.chitose.ac.jp
d) E-mail: latte@iic.hokudai.ac.jp
e) E-mail: iida@iic.hokudai.ac.jp