Journal of Convergence for Information Technology
Vol. 9. No. 9, pp. 52-57, 2019

e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.9.052

Attack Evolution of 'DNSpionage' and Countermeasures on Survey

홍성혁
백석대학교 ICT학부 부교수

‘DNS피오나지’ 공격의 진화에 따른 대응방안

Sunghyuck Hong
Associate Professor, Division of ICT, Baekseok University

Abstract DNS stands for 'Domain Name System' and uses IP addresses to identify devices connected to the network on the network. IP is a protocol that registers and manages aliases such as IPs because it is difficult for general users to remember. In recent years, the abuse of such DNS is increasing abroad, and behind the scenes, called 'DNS pionage,' are developing and evolving new rules and malware. DNSpionage attack is abusing DNS system such as Increasing hacking success rate, leading to fake sites, changing or forged data. As a result it is increasing the damage cases. As the global DNS system is expanding to the extent that it is out of control. Therefore, in this research, the countermeasures of DNSpionage attack is proposed to contribute to build a secure and efficient DNS system.

Key Words : DNS, IP address, ATP attack, C2 attack, Sea Turtle, DNS tunneling, HTTP

요 약 DNS는 ‘Domain Name System’의 약자로, 네트워크 상에서 네트워크에 연결된 장지를 구분하기 위해 IP 주소를 사용하는데, IP는 일반 사용자가 쉽게 기억하기가 어려워 IP에 해당하는 별명같은 이름을 등록하여 관리하는 시스템을 말한다. 최근 들어 이러한 DNS를 악용하는 사례가 해외에서 늘고 있으며, ’DNS피오나지’ 라고 불리는 배후세력들이 새로운 룰과 악성코드를 개발하여 진화하고 있으며, 이런 공격은 해킹 성공률을 높이며, 가짜 사이트로 유도를 하는 등 데이터를 변경하거나 위조하고 있어 피해 사례가 증가되고 있는 상황이다. 글로벌 DNS 시스템 등 점점 통제를 할 수 없는 범위로 확대되고 있어, 이를 통제하기 위해 DNS피오나지 공격에 대한 분석과 대응책을 제시하여 안전한 DNS 시스템을 구축을 제안한다.

주제어 : DNS, IP 주소, ATP 공격, C2 공격, Sea Turtle, DNS 터널링, HTTP

1. Introduction

While the use of computers has become popular, it offers the advantage of convenience to users, but on the contrary, various security problems such as hacking are becoming serious. The effectiveness of programs such as vaccines is fairly limited, and the extent of damage that can not be solved by these programs is increasing. In recent years, cyber-hacking and personal information leakage incidents have been continuing due to the introduction of more daring hackers. With the development of various information and communication technologies, information security breach types and attack methods are becoming more and more evolved [1].

The biggest problem now is that the damage is

*This paper was supported by 2019 Baekseok University Fund.

*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)

Received August 1, 2019
Revised September 2, 2019
Accepted September 20, 2019
Published September 28, 2019

growing nationally. The government and private companies are also affected. Recently, 'DNSpionage Ji' is increasingly hacking to increase the success rate, and it seems that countermeasures are needed to control it. The paper organization is that chapter 2 explains definition of DNSpionage. Chapter 3 suggests the countermeasure for DNSpionage. Then, I will finish with the description of 'DNSpionage', the current situation, the countermeasures, and conclusion at the end.

2. DNSpionage

2.1 DNS

DNS stands for 'Domain Name System' and means the unique address of the computer or the Internet, that is, the IP address. It is organized and classified by country, institution, and communication network. That is, they do not all have the same IP address. Typically, the country code for Korea is .kr. In this way, each country is unique by institution.

It is called 'DNSpionage'. Recently, new tools and malicious code have been developed and hacked into new areas.

Fig. 1 is a detailed process of DNS. For example, assuming that an ordinary user is going to enter Naver using a mobile phone or a computer, the Korean mobile communication company will check the IP address the user wants to access. After that, it connects the user's IP address with the neighbor node. To get this result, you need to know the IP address of Naver as well as your IP address [2]. Although the site itself is so famous that it is expected to be easily connected, it is not easy to connect Naver in the other country. So DNS is important and necessary.

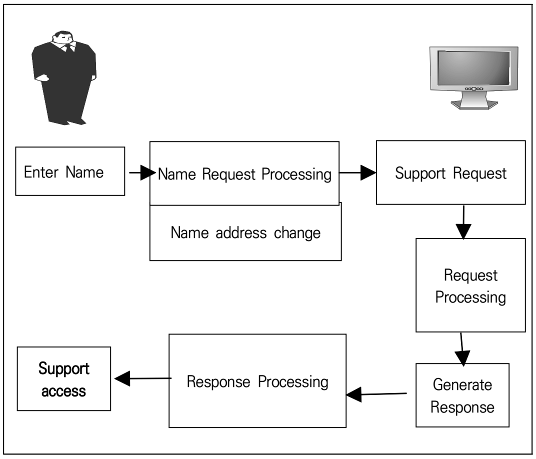

Fig. 1. DNS

2.2 DNSSec

DNSSec stands for DNS Security Extension and is a DNS security extension. DNSSec is intended to secure various levels of server-to-server communication involved in DNS lookups. The attacker makes hijacking by allowing the normal site request to be answered by the malicious site IP address. To solve this problem, each page of the DNS server requests a digital signature. As a result, the attacker can not intercept the request sent by the user in the middle, and can verify the integrity of the request at each step by forming the trust chain. Furthermore, DNSSec verifies the existence of a domain name, and prevents the innocent requestor, that is, the domain name interpretation, from being forwarded to the attacker if not verified [16].

2.3 DNS attack method

There are a few problems that we typically experience when DNS is compromised by outsiders. It is important to realize these problems because we know that we have anomalies and we have to deal with them soon.

In order for these problems to occur, it is important to understand how the attack is compromised. First, the attacker connects the incoming server itself to a location that you specify, allowing it to infiltrate itself. This allows attackers to create attack platforms in a much more efficient manner. Or traffic logs [3], where important information of users is gathered.

The second is to use outgoing email. This is much worse than the first method, because attackers can send infiltrated email to the corporate domain on behalf of the enterprise. It is very difficult for a user to distinguish whether the e-mail that came to him is really from the enterprise or from the attackers who attacked the company and learned the e-mail.

The biggest problem is that, in recent years, attackers are using both of these methods to attack.

2.4 DNS Attack Techniques

The first is a DNS reflection attack. DNS reflection attack is an attack that takes a victim by sending a mass message from the resolver server. When the resolver responds to a large number of transmitted messages, the user receives an enormous amount of unsolicited DNS data and the system becomes paralyzed [4]. The second is DNS cache poisoning. Cache poisoning will attract users to malicious web sites. If you entice a user to a fake site, you can enter your password or cause malicious code to crash.

The third is DNS resource exhaustion. DNS resource exhaustion attacks are attacks that prevent ISP customers from accessing Internet sites. The attacker registers the domain name and uses the victim's server as the authentication server. After generating a large number of requests to the domain, the victim's name server interpretation request is caused to congest and consequently the system is paralyzed [5]. Fig. 2 shows amplification attack.

The last is the DNS amplification attack. The key is to use a DNS server as shown above. This attack method, also called DNS Reflector Attack, is a method using UDP protocol port 53. Since UDP protocol does not require authentication procedure, this method is characterized by packet manipulation [6].

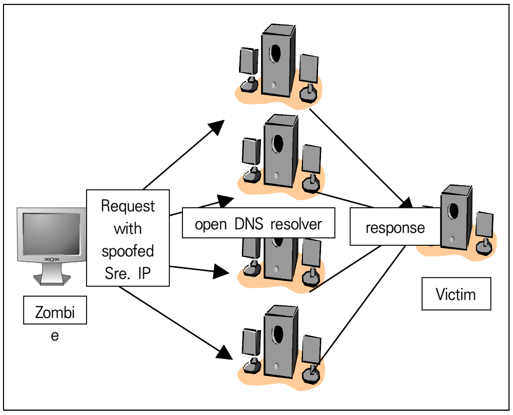

Fig. 2. DNS amplification attack

2.5 DNS attacker type

Although the topic covered in this paper is a hot topic in recent years, there is not much data on it, but I will talk about the new types of attacks that experts are paying attention to. The DNS tunneling attack technique, which is well-known, is a form that DNSpionage has used before it has a new attack form. This is the part that we have been able to solve as the countermeasures we have used so far. Since it was possible to detect or detect, it is noteworthy that the new form of attack is enough to avoid it. These attacks are seen as Iranian hackers to say the experts to date. They are not limited to a single country, but are targeted around the world. Manipulate DNS records, intercept network traffic, and collect it. It is a kind of spy attack.

2.6 DNSpionage

We will discuss DNS in detail, and from now on we will talk about DNSpionage, which refers to the backseat of various attacks such as hacking using DNS. In the meantime, there are many cases of hacking using IP address, and various damages are occurring. Furthermore, these areas are growing intelligently, which is the time when countermeasures are needed right away because they are experiencing national harm. I think this paper is very important to prevent further damage.

2.7 Attack of DNSpionage

If you look closely at the attack type, you will see the word DNS hijacking. This is a major attack on DNSpionage. It is a technique that manipulates the DNS records and bypasses the user, that is, when the victim enters a particular website address, to an irrelevant and strange place that is completely irrelevant [8,17].

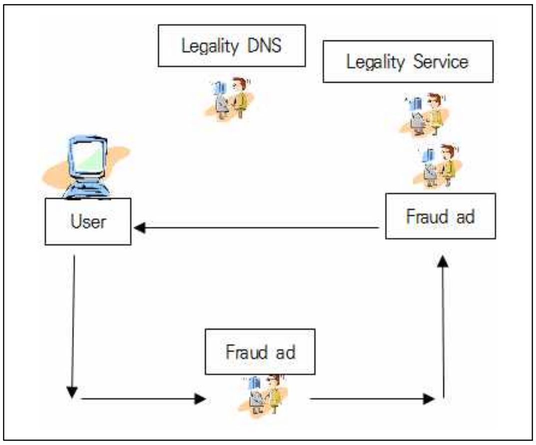

Fig. 3. DNS Hijacking

Fig. 3 shows DNS hacking. However, there are many ways to deal with this attack technique, and it is becoming more and more effective. It is analyzed that it intends to increase the efficiency of attack.

The new technique they are introducing is Karkoff. We also changed the usual phishing document to "Excel" to distribute to increase its efficiency and success rate. Although all the documents were converted to Excel, the malicious macros contained in them are the same. In other words, they have changed the surrounding things [9].

Karkoff supports the DNS communication function and HTTP, and is connected to the C & C server. However, it is not necessarily installed just after the initial penetration. After the additional reconnaissance phase, Karkoff is planted in the organizations that are judged to be infectious, ie effective organizations.

Then, when the carcass is planted, information about the computer and the user's name, local environment, and domain name is collected. Avira and Avast confirm the presence of vaccine products and, if either of them is found, will trigger a specific flag. At the same time, some options in the configuration file are changed [10].

3. How to deal with 'DNSpionage' attacks

The biggest problem is that you can no longer block DNSpionage's attacks by individual or company. The problem is that even the country has no solution as much as it has to solve. However, in such a case, we must personally respond. It may sound boring, but I must prevent it. It is impossible to say that the method itself is precise and 100% solved by prevention. It is possible to access the harmful site without knowing it, and information of the user may be leaked. It is important to keep your information as small as possible, and at the national level, it is important to minimize the extent of the system and minimize the range of hackers' penetration. However, more importantly, it is important to conduct periodic security checks as much as possible. Since it is too late to lose, it is necessary to prevent it beforehand. It is recommended to limit access to overseas sites as much as possible and to be active only in limited places. You should also avoid illegal downloads or downloads to the wrong path. Furthermore, in the worst case, blocking the physical port is one way [11]. However, since this method itself uses the Internet, it is recommended to use it only in the worst case because there is a great inconvenience such as external connection. If you see signs, you should move important data to a safe place. Because of the high risk of Ransomware, it is necessary to have a habit of storing important data in advance like USB in the first place. They are becoming more and more dense and approaching us at a faster pace in an increasingly powerful way. In order to prevent this, we should not only depend on national protection but also it can protect individually. To prevent DNSpionage attack, In a separate DNSpionage campaign, the attackers used the same IP address to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated to encrypt certificates for the redirected domains. These certificates provide X.509 certificates for Transport Layer Security (TLS) free of charge to the user.

4. Conclusion

DNS is an abbreviation of Domain Name System. It is a unique IP address of each page when we connect to any page. It is an address that is not the same in each country and company. From the past, DNS attacks have been repeated. Hackers have used DNS addresses to attack, and IP addresses are an important part of the attack, so if they are compromised, they will do great damage. One of the primary safeguards before DNS is attacked is DNSSec. This is a method of signing each server with a digital signature, which attaches importance to security in accessing each server. This prevents the user's information from flowing to the wrong place, that is, the attacker.

Basically, the attacking method of attacking DNS has a method of creating the attack platform by introducing the server itself into the wrong place. Or the e-mail of the recipient is used to infiltrate the user with confusion. DNS attack methods include reflection attacks through mass messages, cache addiction attacks through malicious websites, and finally amplification attacks using protocols.

The latest attacker type using the core DNS is called 'DNSpionage'. Previously, if you used tunneling techniques, you are using new techniques that have evolved in recent years and have no obvious solution. The most talked about technique is DNS Hijacking. This is a clever technique to manipulate DNS records in the first place. As a result, the user can enter the originally connected IP address, and the information is leaked [12-15].

Furthermore, we use the technique called 'kikov'. Excel is a key element in this technique, and Excel is not just about damaging individual users, it is also attacking companies and other countries.

As such, hacking cases that exploit DNS have become increasingly smart. The problem is that the country is looking away from its own domain. However, there is currently no clear solution to stop it at the national level. However, it is necessary to make efforts to protect individual information personally. Often the hacking, security checks and relevant information should be avoided not just the right to personal saving and force access to harmful sites. For a nation is to avoid the need quick responses, possible damage to the country from Iran, foreign about it, it is necessary to ensure that the path setting. It is important to check for frequent contact with the outside, with restrictions on the route.

If we use the Internet, DNS is an inseparable part. You need to keep this important part in order to use healthy and safe internet. This does not mean that the nation will protect it in a one-dimensional way, but it has to protect its own PC.

REFERENCES

[1] A. Liska & G. Stowe. (2016). DNS network security. *DNS Security,* 93-119.
DOI : 10.1016/b978-0-12-803306-7.00006-1

[2] A. P. Siahaan. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *Int. J. Sci. Res. Sci. Technol, 3(6),* 470-473.
DOI : 10.31227/osf.io/g6emr

[3] A. Liska & G. Stowe. (2016). Anycast and other DNS protocols. *DNS Security,* 193-206.
DOI : 10.1016/b978-0-12-803306-7.00011-5

[4] C. Sun, B. Liu & L. Shi. (2008). Efficient and Low-Cost Hardware Defense Against DNS Amplification Attacks. *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference.* (pp. 1-5).

DOI : 10.1109/glocom.2008.ecp.397

[5] E. Al-Shaer. (2014). Modeling and Verification of Firewall and IPSec Policies Using Binary Decision Diagrams. *Automated Firewall Analytics,* 25-48.
DOI : 10.1007/978-3-319-10371-6_2

[6] B. Wang, H. Chen & B. Zhang. (2013). Design and implementation of UDP-based terminal adaptive protocol. *Journal of Computer Applications, 33(4),* 943-946.
DOI : 10.3724/sp.j.1087.2013.00943

[7] DNS and IPv6. (2005). *Pro DNS and BIND,* 77-92.
DOI : 10.1007/978-1-4302-0050-5_5

[8] T. Kim & H. Ju. (2011). Effective DNS server fingerprinting method. 2011 13th Asia-Pacific Network Operations and Management Symposium. (pp. 1-4). IEEE.
DOI : 10.1109/apnoms.2011.6076955

[9] Document management. Change management for successful electronic document management system (EDMS) implementation. (2011).
DOI : 10.3403/30181562

[10] A. M. Lopes, J. P. Andrade & J. T. Machado. (2016). Multidimensional scaling analysis of virus diseases. *Computer Methods and Programs in Biomedicine, 131,* 97-110.
DOI : 10.1016/j.cmpb.2016.03.029

[11] M. Chen, Y. Liu, Z. Li, J. Xiao & J. Chen. (2016). A low jitter supply regulated charge pump PLL with self-calibration. *Journal of Semiconductors, 37(1),* 015006.
DOI : 10.1088/1674-4926/37/1/015006

[12] S. Hong. (2013). Countermeasure for Anti-financial hacking. *Journal of Convergence for Information Technology, 3(1),* 43-48.

[13] S. Hong & S. Y. Jeong. (2018). The Analysis of CCTV Hacking and Security Countermeasure Technologies : Survey. *Journal of Convergence for Information Technology, 8(6),* 129-134.
DOI : 10.22156/CS4SMB.2018.8.6.129

[14] P. S. Shin & J. M. Kim. (2014). Security and Hacking on Wireless Networking for Small and Medium Business : Survey. *Journal of Convergence for Information Technology, 4(3),* 15-20.

[15] J. K. Cho. (2019). Study on Improvement of Vulnerability Diagnosis Items for PC Security Enhancement. *Journal of Convergence for Information Technology, 9(3),* 1-7.
DOI : 10.22156/CS4SMB.2019.9.3.001

[16] M. Andrews & S. Weiler. (2006). *The DNSSEC Lookaside Validation (DLV) DNS Resource Record.*
DOI : 10.17487/rfc4431

[17] A. Liska & G. Stowe. (2016). Windows DNS security. *DNS Security,* 139-158.
DOI : 10.1016/b978-0-12-803306-7.00008-5

홍 성 혁 (Sunghyuck Hong) [종신회원]

· 2007년 8월 : Texas Tech University, Computer Science (공학박사)
· 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
· 관심분야 : 블록체인, 사물인터넷 보안, 경량보안프로토콜
· E-Mail : sunghyuck.hong@gmail.com