Offensive Hacking: Tactical & Strategic - IE6052

MS19814452 – W.T. N. Perera

M.Sc. (Specialized in Cyber Security)

Sri Lanka Institute of Information Technology

Domain Name System Vulnerabilities and Attacks

Abstract

DNS - Domain Name System is a fundamental service in the IP network and Internet concept. DNS directory contains the details of matching domains request by clients worldwide. This review paper focusing on identifying and analyzing the current DNS vulnerabilities that can affect a large impact to the DNS users including large organizations and companies. First and second parts of this paper discuss of main theory behind the DNS and how it works. The third section describes the vulnerabilities exist on current DNS concepts and attacks take places based on it. Forth section discuss about a latest group of vulnerabilities named as NAME: WRECK which disclosed by Forescount partnering with JSOF. New NAME: WRECK vulnerabilities appears in well-known IT Software and IOT firmware devices. These flaws allow for a Denial of Service attack or Remote Code Execution. Finally this paper present the mitigation and preventive actions could be taken.

I. INTRODUCTION

Domain Name System can be compared to the Yellow pages in old days. Simply this means DNS is a directory which contains the details of matching domain names with their IP addresses. In early days' people used to access particular sites using their IP addresses, but when the internet got complicated and more and more devices and people get involved with the internet, remembering each and every IPs for devices became unrealistic. Hence people used the domain name of particular server/device instead of the IP address. Middle server named as Domain Name System resolves the particular name and provide the IP matches with that name.

II. BACKGROUND

DNS considered to be a fundamental and mandatory service in IP network and internet concept. All IP requests initiates with DNS resolution. If in case this service become unavailable most of the applications become unavailable too. Therefore, attackers target to find a flaw in DNS or to bypass the standard function of this protocol. DNS protocol accept by all IT security solutions but with very limited verifications. This made this protocol a better vector to create backdoor of a system.

There are more than one servers used for this purpose with the large growth of the internet. When a device requests a name, it direct to its DNS server and if it does not store in that

server, it will request it from other interconnected DNS server. These querying process for a particular domain can go up to upstream until it leads back to authority name server. These Authoritative name servers are managed by administrators in which admins can add, change or remove server details - name and IP.

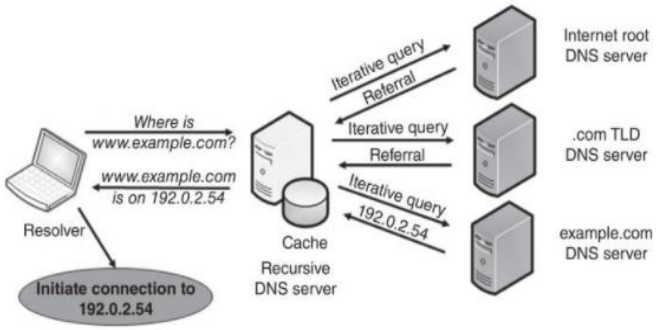

Figure 1: Flow of Basic DNS resolution process

Basically 4 DNS servers involved in loading a web page requested by a host machine. DNS Resolver is the server which receives the query directly from the host via application (web browser). Then this request is being forwarded to Root Server to resolve the request domain name into IP Address. Then the TLD (Top Level Domain Server) name server gets involved. Last part of the requested hostname is being search via the TLD name server. Finally, the Authoritative name server access the specific requested record and returns the IP address to the DNS Resolver server. [1]

III. VULNERABILITIES AND ATTACKS

Attackers have different intentions but all are mainly focused on interrupting businesses, manipulate or corrupt data and steal important and sensitive information which will help them to gain access to a system or to get a ransom payment. Hence attackers look for existing vulnerabilities and develop DNS attacks.

Domain Name System itself has several vulnerabilities which has been used by the attackers during past decades to exploit and abuse the DNS. Generally, all the DNS threats are bound with specific DNS functions including cache, recursive and authoritative.

Internal Domain Name System server stores almost all the domain names of other servers and their IP addresses. These record shared with any party who request for particular details. This simple means that these are rich resources for anyone who seeks that for legitimate or illegal purposes. Attackers use the information collected from these DNS servers specially in the reconnaissance phase. [1] Another vulnerability in the DNS servers are that their caches are not authoritative. Hence they can be manipulating so easily. Which simply means attackers can poison the

record with bad data and who ever requesting for that poisoned records can be fooled in to accessing attacker command and control servers. Also attackers make use of covert channels to exhilarate information from these server because of its behavior.

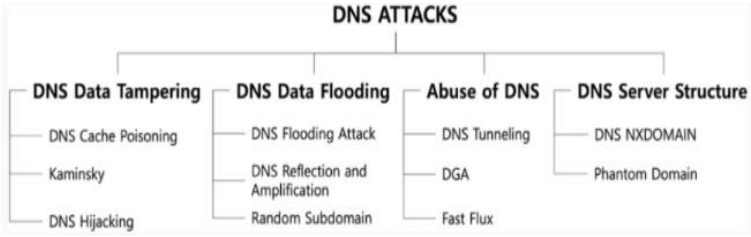

Figure 2: DNS attack categories

a) DNS Data Tampering

Data Tampering simply means that an attacker intercepts the unencrypted traffic between the client and the DNS server and changes the data into false or bad information. This can be done in various ways based on the flaws in insecure DNS data. These attacks can be done by cache poisoning or hijacking.

DNS Cache poisoning is a DNS protocol abusing attack. Attacker insert false data in to DNS resolver cache memory in way that DNS name server send incorrect/invalid IP for future client requests as well. [1] Hence all the DNS traffic is diverting to the attacker's server.

Hijacking of DNS is done in various ways including Phishing, Farming or Subdomain hijacking. Hijacking technique involves with modifying the settings of the DNS records so that it points to a malicious DNS server of an attacker. Attacker then get access the bogus DNS server and change the IP Address which mapping with the domain address. Modified DNS records can redirect the client into phishing website.

b) DNS Data Flooding

DNS flooding also known as volumetric Dos attacks for DNS server is conducted by overwhelming the DNS server. Same as the normal DoS attack method, attacker use one or more sources to send large number of requests to the DNS server and flood it with the requests so that service crashes and become unavailable to the legitimate users. [1]

DNS reflection and amplified DoS attacks differs from the general flooding attacks since it attempts to flood the network by high bandwidth network traffic by making use of flaws of third party resolvers available in the network. Attacker send small amount of request to more open source recursive Domain Name System Servers including a spoofed IP. Those requests leads to large amount of response packets.

c) **Abuse DNS attacks**

Most of the resent cyber attackers use the concept of Command and Control - C&C when conducting an attack. There are thousands of malicious machines which is also known as bots interconnected into a C&C server. This malicious network knows as botnet and attacker make use of these botnets to exploit servers due to the reason that the inability of finding the attackers machine. Attacker send malicious queries from inside network to outside C&C server bypassing the internal firewall. In a scenario like that, attacker can hide the C&C server information by using the DNS records. [1]

Attackers use various techniques including DNS tunneling, DGA Algorithms and Fast flux for the purpose of bypassing an internal defense system such as firewall. Domain Generation Algorithm - DGA use for random creation of domain names in large amount for a one IP address. Attacker initially try to conduct an attack by sending bad queries to bots in a C&C botnet. Some malware uses various names generated by the algorithm to change the name of the C&C server continuously. Although most of the time defense systems identify and block the C&C server by the IP address, they failed to identify the continuous changing domain names. Hence locating and blocking of the C&C server have become impractical task with this DGA technique.

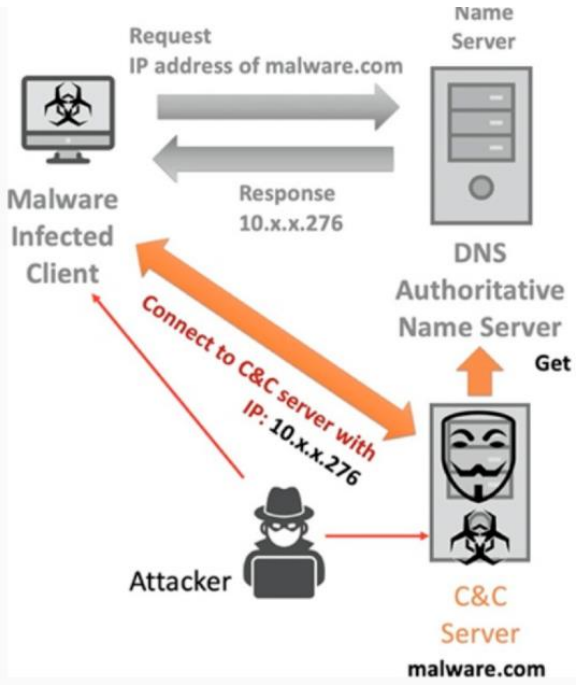

Figure 3: DNS attack using abuse of DNS

On the other hand, Fast flux is a technique uses the concept of DGA in a vise versa manner. Meaning that it can allocate multiple IPs to single domain name. This is done by changing the settings of the DNS response.

IV. LATEST DNS VULNERABILITY - NAME: WRECK

Forescount Cyber security researches partnering with JSOF Israeli Boutique Cyber Security Consultancy group has disclosed and published a security report on nine

Domain Name System vulnerabilities on 13th April 2021.

They named it as NAME: WRECK which have the ability to DoS attack or RCE - Remote Code Execution attack. This allows attackers not only to control the device but also to take down the system.

NAME: WRECK affects DNS implementations by affecting least 4 famous TCP/IP stacks -FreeBSD, IPNEt, NetX and Nucleus NET.

FreeBSD act as the basis for computers, printers and other commercial networking devices. This is generally being used for High performance servers. NetX run by ThreadX RTOS included in medication devices, printers, consumer electronics, smart clocks and industrial controlling systems. Nucleus NET is a real time OS used in millions of ultrasound machines, VoIP, storage systems and other critical systems. [2]

Attacker gain access to the network by compromising a device which issues a DNS query to the internet. For the initial access, attacker exploit Remote Code Execution vulnerability in the Nucleus NET. [2] [3] Attacker then can other compromised entry points to get access to DHCP server. Furthermore, can do a lateral movement by executing the bogus piece of code on the vulnerable FreeBSD servers. Finally, attacker is able to make use of the internally compromised servers to persist the network as per their target. Other vise make use of the

CVE	Stack	Affected Feature	Potential Impact	CVSSv3
CVE-2016-20009	IPNet	Message compression	Remote Code Execution	9.8
CVE-2020-15795	Nucleus NET	Domain name label parsing	Remote Code Execution	8.1
CVE-2020-27009	Nucleus NET	Message compression	Remote Code Execution	8.1
CVE-2020-7461	FreeBSD	Message Compression	Remote Code Execution	7.7
CVE-2020-27736	Nucleus NET	Domain name label parsing	Denial of Service	6.5
CVE-2020-27737	Nucleus NET	Domain name label parsing	Denial of Service	6.5
CVE-2020-27738	Nucleus NET	Message Compression	Denial of Service	6.5
Not Assigned	NetX	Message Compression	Denial of Service	6.5
CVE-2021-25677	Nucleus NET	Transaction ID	DNS Cache Poisoning	5.3

Figure 4: New nine vulnerabilities in NAME:WRECK

vulnerable IOT device to exhilarate data. (Figure 5)

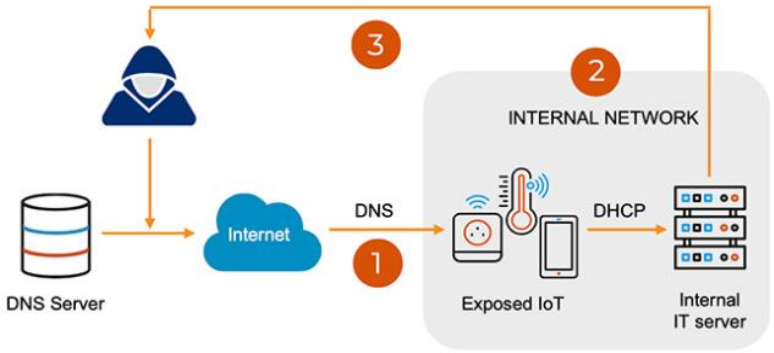

Figure 5: Attack scenario of NAME:WRECK vulnerabilities on internal & external targets

V. MITIGATION

Using a separate and isolated internal DNS server environment can reduce most of the DNS web application attacks. Maintaining such environment helps to close all unwanted ports, stop unwanted services of OS, traffic filter based on the firewall.

DNS servers should be up to dated which means latest patches should be applied in timely manner. Best security practice is to hide the Bind version of the DNS. Other step is to restrict the DNS zone transfer to specific IP Addresses. Furthermore, using two factor authentication and DDoS mitigation provider also most of the previously elaborated attacks can be mitigated.

Recommendations to mitigate the NAME: WRECK vulnerabilities highlights of limiting the network exposure of these vulnerable devices through the network segmentation. Also they suggest to rely on the internal DNS server. Furthermore, apply the necessary patches for these critical vulnerable devices once the vendor release advisories

VI. CONCLUSION

This review paper is focused on DNS vulnerabilities and possible attacks. Although DNS is a fundamental protocol for the operation of internet, it has several critical loopholes that can subjected to various attacks. Domain Name System itself has several vulnerabilities which has been used by the attackers during past decades to exploit and abuse the DNS. Generally, all the DNS threats are bound with specific DNS functions including cache, recursive and authoritative. This review paper provides novel analysis of DNS functions, how it works in term of cyber security. Also on later parts it discusses in details of the existing vulnerabilities generally in DNS and the attacks that could occur due to the flaws. Mitigation actions and systems should be implemented so that most of the DNS related vulnerabilities could be avoided.

References

[1] T. Kim and D. Reeves, "A survey of domain name system vulnerabilities and attacks", *Journal of Surveillance, Security and Safety*, 2020. Available: 10.20517/jsss.2020.14 [Accessed 7 May 2021].

[2] "NAME: WRECK: Nine DNS Vulnerabilities Found in Four Open Source TCP/IP Stacks", *Tenable®*, 2021. [Online]. Available: https://www.tenable.com/blog/namewreck-nine-dns-vulnerabilities-found-in-four-open-source-tcpip-stacks. [Accessed: 11- May- 2021].

[3] "New DNS vulnerabilities have the potential to impact millions of devices - Help Net Security", *Help Net Security*, 2021. [Online]. Available: https://www.helpnetsecurity.com/2021/04/13/dns-vulnerabilities/. [Accessed: 14- May- 2021].

[4] *Forescout.com*, 2021. [Online]. Available: https://www.forescout.com/company/resources/namewreck-faq/. [Accessed: 12- May- 2021].

[5]"Vulnerabilities in TCP/IP stack may affect millions of devices, warn researchers | IT World Canada News", *IT World Canada - Information Technology news on products, services and issues for CIOs, IT managers and network admins*, 2021. [Online]. Available: https://www.itworldcanada.com/article/vulnerabilities-in-tcp-ip-stack-may-affect-millions-of-devices-warn-researchers/446081. [Accessed: 14- May- 2021].

[6] "SecurityTrails | 8 tips to prevent DNS attacks", *Securitytrails.com*, 2021. [Online]. Available: https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks#:~:text=Close%20all%20unneeded%20server%20ports,chances%20of%20a%20DNS%20attack. [Accessed: 09- May- 2021].

[7] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC", 2007. [Accessed 15 May 2021].

[8]"DNS Attacks List", *EfficientIP*, 2021. [Online]. Available: https://www.efficientip.com/dns-attacks-list/. [Accessed: 12- May- 2021].

[9]"Zero Day Initiative — The March 2021 Security Update Review", *Zero Day Initiative*, 2021. [Online]. Available: https://www.zerodayinitiative.com/blog/2021/3/9/the-march-2021-security-update-review. [Accessed: 14- May- 2021].

[10]"Vulnerabilities in Microsoft DNS Server", *Security Advisory 2021-014*, 2021. [Accessed 15 May 2021].

[11]"What is DNS, How it Works + Vulnerabilities | Varonis", *Inside Out Security*, 2021. [Online]. Available: https://www.varonis.com/blog/what-is-dns/. [Accessed: 12- May- 2021].