NGTIM

A Deep Dive into DNS Spoofing and Security Measures

KUKUTLA TEJONATH REDDY,
International Center for AI and Cyber Security Research and Innovations (CCRI), Asia University, Taiwan, tejonath45@gmail.com

ABSTRACT

In this article, we will look into the details of DNS Spoofing. DNS spoofing is a dangerous cyberspace attack that undermines the trustworthiness of the DNS. The article gives a clear definition of the operations involved in DNS spoofing including the probable effects and the challenges in real life as exemplified by issues such as Kaminsky attack and Sea Turtle campaign. The attacks that are used by the attackers such as are DNS cache poisoning and Man-in-the-Middle attacks are discussed in detail. In particular, the article casts light on the dim areas of DNS Spoofing and provides countermeasures and best practices like DNS Sec deployment and network partitioning to make defense against these malignant hacks powerful. Being very useful as it engages, informs, and provides technical information that allows readers of different caliber of understanding to grasp, fight, and block such danger as DNS Spoofing in modern communication networks.

KEYWORDS: DNS Spoofing, Cybersecurity, Domain Name System, DNS Cache Poisoning, Man-in-the-Middle Attacks

I. INTRODUCTION

The domain name system otherwise referred to as DNS operates in an environment that does not take pauses. This article seeks to demystify DNS Spoofing, a common cyber threat that undermines the integrity of the DNS architecture. Due to this, it is easy to see why people who intend to conduct malicious activities target the DNS as a gateway which converts human readable domain names into machine readable IP addresses. This article is a walk through into understanding the essence of DNS spoofing from its meaning, working procedure, real world effects and array of attacks. In addition, equipped with knowledge about effective responses strategies and appropriate measures as well as readers would be in position to safeguard their online realms from impending DNS Spoofing. Unraveling the complex world of cyber dangers with focus on DSN spoofing [1].

II. What is DNS Spoofing?

The DNS Spoofing/Domain Name System Spoofing is a type of an attack directed towards the Domain Name System (DNS), in order to convince its users and divert their traffic [1]. The

backbone of the internet's structure is its Domain Name System (DNS), which converts user readable domains like www.example.com, into numerical IP addresses that computers understand. A malicious actor takes advantage of vulnerabilities in the process of resolving DNS queries – that's what happens in the case of a DNS spoofing attack.: It should trick computers into mapping a properly registered domain name with wrong IP addresses. Manipulation can direct users to undesired or even perilous sites [2].

For example, think that you need to go to some secure site like a bank's online portal. An example is a DNS Spoofing attack in which an online requester would be directed to a fake website instead of the real one. In such a case, an attacker could try and steal your passwords or any confidential data.

The technique for the DNS spoofing is often referred to as the "cache poisoning". This involves inserting bogus DNS records into the cache of a DNS resolver machine in this technique. This results into a scenario whereby, once a user inquiry about a certain domain, the attacker's infected DNS resolves it and direct the user to an illegal or harmful web destination. This type of cyber-attack is very alarming because it allows for Phishing attacks; spreads malware and engages in other wrongdoings. To guard against DNS spoofing, it is imperative to have strong security features like those found in DNS SEC and close surveillance of DNS traffic for oddities [3].

III. RELATED WORKS

DNS Security Extensions (DNSSEC):

Several studies have investigated the ability of DNS Securities Extension (DNSSEC) to improve DNS security against DNS spoofing. Technical aspects of DNSSEC implementation have been investigated in research carried out by Eastlake and Panitz with reference to DNS vulnerability mitigation problems [1].

Man-in-the-Middle Attacks and Network Security:

In the wider field of Man-in-the-Middle attacks that comprises DNS spoofing, scholars like Ferguson and Schneier have undertaken broad studies. The research conducted brings in a clearer picture of how attackers carry out their interception or falsification exercises on communication and explains why strong network security measures are required.

Real-world DNS Spoofing Incidents:

Studies on actual DNS Spoofing incidents like the Kaminsky Attack would give significant information about how attackers work as well as the effects of successful DNS Spoofing. Examining such occurrences helps clarify ever-changing nature of threat environment.

DNS Traffic Analysis and Anomaly Detection:

An investigation of techniques for identifying unnatural patterns observed in DNS queries/responses was performed by Antonakakis et al. This research supports measures that can be used in

advance to detect and stop DNS Spoofing attacks [3].

DNS-based Threat Intelligence:

DNS based threat intelligence (for example, Antonakakis & Perdisci) examines on using DNS data for the advance warning of attacks. By doing this, it becomes easier to foresee and forestall possible DNS spoofing situations that may arise.

Impact of DNS Spoofing on Cybersecurity Landscape:

Allodi and Massacci extend research on impact of DNS spoofing towards cyber security scenario. Investigating the Cascades of Successful DNS Spoofing Attacks for Individuals, Organizations, and Trust in Online Communications.

IV. How DNS Spoofing Works:

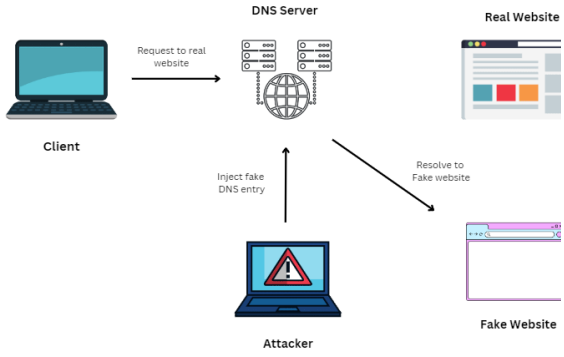

Figure 1: Working of DNS Spoofing

It is a type of attack which capitalizes on a weakness in DNS – an essential technology whose function is to convert readable domain names to machine-readable Internet Protocol (IP) addresses [4]. The attack involves the hijacking of a domain name system (DNS) such that users are inadvertently connected with fake or hostile servers. There are two primary methods through which DNS Spoofing is executed: including cache poisoning and MITM attacks [5].

Cache Poisoning:
The latter method is known as the cache poisoning technique that targets the DNS resolver's cache. Resolvers are used to reduce time in queries as they stored domain name and its matched IP address. This will lead the attacker to inject false DNS information into this cache that will cause the resolver to respond to legitimate domain name queries with malicious IP addresses. Afterwards, unsuspecting people are taken to phony sites with similar traits like popular ones; they may be caught by phishers or hackers.

Man-in-the-Middle Attacks:
These attacks are, in particular, Man-in-the-middle attacks used for DNS spoofing. In this case, the attacker lies in between the user and the DNS server such that it can read all the messages sent back and forth. In this type of attacks, the attacker misleads the target by making them respond to DNS query with incorrect information in order to provide a legit connection but lead to malicious location. Such attacks enable the malefactor to intercept personal messages and data that a user could send to a particular serviceman creating an opportunity for some illegal actions.

The main aim in case of both cache poisoning and man-in-the-middle attacks is to mislead the DNS resolution process into believing that malicious IP should be trusted rather than a genuine one. However, DNS spoofing success has varying results that may include phishing and malware distribution as well as other

advanced threats that could cause serious harm to people or businesses.

V. Consequences and Risks

Phishing Attacks:

Phishing commonly used as preceded DNS spoofing. Attackers lure users to fake sites which seem like real ones so that they can obtain confidential data including login credentials and bank account numbers.

Malware Distribution:

Attackers also use spoof spoofed DNS responses to direct victims to servers of their malware programs. Downloaded materials can contain malicious software, leading to breach of system integrity and data loss.

Denial of Service (DoS)

Attackers may conduct a similar process by flooding a DNS server using false requests. This way, the server is overloaded and its normal DNS resolution services are denied to genuine users, thus achieving a denial-of-service attack on genuine customers.

Real-world Scenarios

Kaminsky Attack (2008)

Dan Kaminsky discovered a significant flaw on DNS Protocol in 2008 that resulted into an attempt to update all the DNSs globally. Vulnerability enabled attackers to easily pollute DNS cache and route the users towards harmful websites.

Sea Turtle Campaign (2019)

The Sea Turtles campaign employed phishing and malware by infecting DNS registrars and tampering with DNS records aimed at organizations. A complex intrusion for reconnaissance purposes illustrating actual ramifications for DNS spoofing.

The tools and methods used in DNS spoofing.

DNS Cache Poisoning Tools

Common tools used in DNS cache poisoning include “Dnsmasq” and “Inception”. They leverage DNS-cache poisoning, which involves inserting malicious DNS records in vulnerable DNS resolver caches.

Man-in-the-Middle Tools

These include “Ettercap” and “Wireshark”, which help in DNS spoofing via the changing of already sent DNS requests.

VI. Countermeasures and Best Practices

It is therefore necessary to establish reliable countermeasures and best practices to shield against the deceitful danger of DNS Spoofing. The following strategies are effective in fortifying the Domain Name System (DNS) infrastructure and mitigating the risks associated with DNS Spoofing:

DNS Security Extensions (DNSSEC):

A basic solution that can be adopted to improve the integrity of the DNS is to implement DNS Security Extensions (DNSSEC). Cryptographic signatures are added to DNS data through the use of DNSSEC. Through this, DNS resolvers can validate these signatures and ensure that they are not from attackers looking to manipulate DNS records for their own benefits.

Use of DNS Firewalls:

DNS firewalls are like barriers blocking harmful DNS activities. The firewalls analyze DNS requests and responses comparing them with the threat intelligence database. A malicious request can be blocked by the firewall if it detects that the communication message is harmful and thus prohibiting users from visiting unlawful web pages.

Regular Software Updates:
It is important to update DNS software and systems in order to address existing vulnerabilities. Such enhancements on DNS software may not be complete without regular updates and patches which are provided as a part of updates made on DNS software by their vendors. Applying these updates immediately preserves the strength of DNS infrastructure despite developing cyber-attacks.

Network Segmentation:
Network segmentation as a preventive step used to reduce the damages brought about by DNS attack. Organizations should disconnect important network elements to hinder the spread of attackers to vulnerable systems where confidential information is held. This containment approach bars sideways runners after a probable succeed in DNS Spoofing attack and limits possible results.

VII. Conclusion

DNS Spoofing emerges as one formidable threat to the stability and security of the Domain Name System. This cyber-attack method exploits vulnerabilities right into the very fabric of online communication and trust that users place on DNS with such extreme risks as mentioned above. Nevertheless, with a grasp of how it operates as well as reliable countermeasures such as DNSSEC or security firewalls and vigilant surveillance in place, people and organizations will be well placed to resist this attack. In the fast-changing cyber environment, there is need for a proactive and collaborative strategy to ensure the integrity of the Internet system and a sustainable defense approach towards emerging menaces.

VIII. References

[1] Houser, R., Hao, S., Li, Z., Liu, D., Cotton, C., & Wang, H. (2021, September). A comprehensive measurement-based investigation of DNS hijacking. In *2021 40th International Symposium on Reliable Distributed Systems (SRDS)* (pp. 210-221). IEEE.

[2] Yang, D., Li, Z., Jiang, H., Tyson, G., Li, H., Xie, G., & Zeng, Y. (2022). A deep dive into DNS behavior and query failures. *Computer Networks*, *214*, 109131.

[3] Saidi, S. J., Matic, S., Gasser, O., Smaragdakis, G., & Feldmann, A. (2022, October). Deep dive into the IoT backend ecosystem. In *Proceedings of the 22nd ACM internet measurement conference* (pp. 488-503).

[4] Wei, L., & Heidemann, J. (2020). Whac-A-Mole: Six Years of DNS Spoofing. *arXiv preprint arXiv:2011.12978*.

[5] Volini, A. G. (2020). A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues. *J. Intell. Prop. L.*, *28*, 291.

[6] Moura, G. C., Davids, M., Schutijser, C., Hesselman, C., Heidemann, J., & SMARAGDAKIS, G. (2023). Deep Dive into NTP Pool Popularity and Mapping.

[7] Steinhoff, U., Wiesmaier, A., & Araújo, R. (2006, June). The state of the art in DNS

spoofing. In *Proc. 4th Intl. Conf. Applied Cryptography and Network Security (ACNS)*.

[8] Deccio, C., Hilton, A., Briggs, M., Avery, T., & Richardson, R. (2020, October). Behind closed doors: a network tale of spoofing, intrusion, and false DNS security. In *Proceedings of the ACM Internet Measurement Conference* (pp. 65-77).

[9] van Rijswijk-Deij, R. M. (2017). *Improving DNS security: a measurement-based approach*. University of Twente.

[10]Zhang, J., Wang, Z., Wang, D., Zhang, X., Gupta, B. B., Liu, X., & Ma, J. (2021). A secure decentralized spatial crowdsourcing scheme for 6G-enabled network in box. *IEEE Transactions on Industrial Informatics*, *18*(9), 6160-6170.

[11]Shankar, K., Perumal, E., Elhoseny, M., Taher, F., Gupta, B. B., & El-Latif, A. A. A. (2021). Synergic deep learning for smart health diagnosis of COVID-19 for connected living and smart cities. *ACM Transactions on Internet Technology (TOIT)*, *22*(3), 1-14.

[15]Prathiba, S. B., Raja, G., Bashir, A. K., AlZubi, A. A., & Gupta, B. (2021). SDN-assisted safety message dissemination framework for vehicular critical energy infrastructure. *IEEE Transactions on Industrial Informatics*, *18*(5), 3510-3518.

[16]Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, 1-25.

[17]Almomani, A., Alauthman, M., Shatnawi, M. T., Alweshah, M., Alrosan, A., Alomoush, W., & Gupta, B. B. (2022). Phishing Website Detection With Semantic Features Based on Machine Learning Classifiers: A Comparative Study. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-24.