Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme

S. M. Zia Ur Rashid*, MD. Imtiaz Kamrul†, Asraful Islam‡
*‡*Department of Electrical and Electronic Engineering*
†*Department of Electronic and Telecommunication Engineering*
International Islamic University Chittagong
Chattogram, Bangladesh
Email: *smziaurrashid@gmail.com, †imtiazshuvo10@gmail.com, ‡asrafulalam.iiuc@gmail.com

***Abstract*—With the impetuous improvement of cyber intelligence and networking technology, cybersecurity becomes an important area of research. Domain name system (DNS) has been an essential aspect of cyber security and a crucial part of internet services. The nameservers are responsible for the functionality and safety of their corresponding domain names. But due to the laggings of proper security and DNS misconfiguration, there is a chance to takeover subdomain from the assigned external services e.g., cloud platform, e-commerce or content delivery service, which can lead to several high severity risks. Due to trackless and easier exploitation effort, subdomain hijacking has become an alluring attack vector among the hackers, which raise serious concern on cyber security. This paper focuses on comprehensive analysis on subdomain takeover and figures out the security vulnerability reason and attack scenarios. Element for subdomain enumeration, subdomain takeover process and finally, a proposed inclusive prevention model of subdomain takeover have been discussed throughout the paper.**

***Keywords*—subdomain takeover, domain hijacking, dns security, cybersecurity**

I. Introduction

DOMAIN name system (DNS) represents IP addresses in the form of human-recognizable domains, which is a crucial part of internet services. In today's world, most of the persons or companies are using a domain or website for their portfolio, service, business purpose and many more. Also in that time subdomain is one of the most essential things for a website. Basically, a subdomain is used for the mobile or web-based site, email, blog, different niche or e-commerce site & increasing SEO (search engine optimization) performances. Under a domain, the owner can create unlimited subdomain by knowing his needs. Yet, DNS has been an attractive target to hackers for domain or subdomain hijacking [1]. DNS cache-poisoning, DNS application attack etc. [2]–[4] has been commonly used to attack on DNS, [RFC1034, RFC1035]. Recently, a new attack vector, subdomain hijacking has appeared which remain masked over a long period of time and left no trace for forensic analysis [5]. This vulnerability type appears when organizations assign its domain or subdomain DNS entries i.e., A record or CNAME (canonical name) record to a third-party service, but forget to claim ownership of the subdomain or to remove DNS configuration while switching different services. In this case, an attacker could easily claim and takeover that subdomain by registering an account on the same external service, thus poses a severe threat to cybersecurity. A yearly statistics of publicly disclosed subdomain takeover data collected from HackerOne bug bounty platform is illustrated in Figure 1 to exhibit the emerging risk on subdomain hijacking. In recent years, several researches conducted on domain hijacking. For example, A domain hijacking detection and forensic analysis model is designed by A. Borgwart and S. Boukoros group [6]. C. Lu and T.R. Valladares proposed a chaos-based security method to fight against DNS hijacking [7], D. Liu and S. Hao shed light on a potential threat in DNS posed by dangling DNS records [8]. A brief analysis of DNS vulnerabilities, advanced attacks and protection have been carried out by A. Ali, E. Ali [9]. Peter Thomassen, J. Benninger and M. Margraf investigated subdomain hijacking via subzone registration [10].

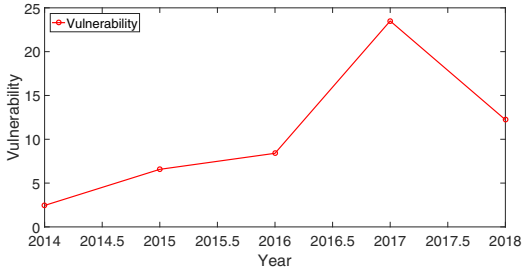

Fig. 1. Yearly statistics of publicly disclosed subdomain takeover report

This paper intends to provide an in-depth analysis of subdomain takeover vulnerability and proposed an inclusive subdomain hijacking prevention model. The leftover of this paper is formed as follows. Section II discussed about subdomain gathering techniques in brief. In section III, the steps for subdomain vulnerability detection and takeover process are explained and in section IV, we have outlined the potential risk and impact of subdomain hijacking. In section V, a prevention process is described and finally, we conclude the paper in section VI.

978-1-5386-9111-3/19/$31.00

II. Subdomain Gathering

A. Manual Gathering

Subdomain enumeration is an important part of reconnaissance for black box penetration testing as well as for security research. To conduct manual subdomain enumeration, we discussed below some advanced techniques.

1) Finding Subdomain from Search Engines: It is easy to gather subdomain of a specific domain from various search engines like Google, Bing etc. by using advanced search operator (dork). For example, we can find subdomains for ieee.org in Google search using "site" operator as follows: site:*.ieee.org

2) Collect Sub-domains from Certificate Transparency: Certificate Transparency is basically a collection of all certificates that have been issued. The simplest way to look up certificates for a domain is to use search engines that store the CT logs. Some such search engines are mentioned below:

- https://crt.sh/
- https://censys.io/
- https://google.com/transparencyreport/https/ct/
- https://developers.facebook.com/tools/ct/

3) Brute Force: Dictionary-based enumeration is another technique to find sub-domains with generic names. Making a list of common subdomains, we can detect available subdomains by running a dictionary brute force method.

4) HTML Source Code: Extracting HTML source code of web pages & from directory detection, we can discover subdomain.

5) Permutation Scanning: It is another interesting technique to identify sub-domains. Using this technique, we can identify new sub-domains using permutations, alterations and mutations of already known domains or sub-domains.

6) DNS Lookup: DNS lookup is another process to find subdomain. dnsdumpster.com provides free web-based DNS recon to find subdomains. It also checks wildcard zone transfer to gather subdomains.

7) Zone Transfer: Zone transfer contains a copy of full or part of its zone file to another DNS server. If zone transfers are not configured securely, anyone can get a get a copy of the zone file from the nameserver. In general, zone file contains a lot of information about the zone and the hosts that reside in the zone.

B. Automated Enumeration using OSINT

There are some open source intelligence tools (OSINTs) available on GitHub which will help us to make the process easier and automated. Among them Aquatone, Sublist3r, Knockpy, Amass, Sub-finder, Massdns etc. are mentionable. To demonstrate the sub-domain gathering process, we used microsft.com domain which is under the scope of their responsible disclosure program and allows security researchers to conduct penetration testing.

1) Aquatone: Aquatone is a ruby based open source tool designed to perform reconnaissance on a target domain. It can discover and gather subdomains on a given domain by utilizing various open sources & services like Shodan, Google Transparency Report, DNSDB, ThreatCrowd, Way Back Machine, Riddler, Netcraft, HackerTarget, Virustotal, Passivetotal, PTRArchive and dictionary brute force. After discovering a bunch of subdomains, it can then perform hosts scan for detecting common web ports and gather HTTP response headers, HTML bodies and screenshots can be collected and consolidated into an excellent report for easy analysis of the attack surface.

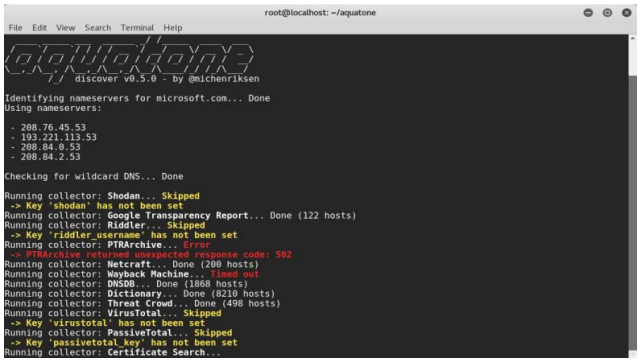

Fig. 2. Subdomain enumeration using Aquatone tool

2) Sublist3r: Sublist3r is an open source python based tool designed to enumerate and gather subdomains of a given website using brute force techniques and data from publicly available sources. It enumerates subdomains from a wide range of popular search engines such as Google, Bing, Yahoo, Ask, Baidu and also discovers subdomains using ReverseDNS, Virustotal, Netcraft, DNSdumpster and ThreatCrowd. Additionally, a DNS-query spider tool named Subbrute was integrated with it to gather more subdomains using brute force with an extensive word list.

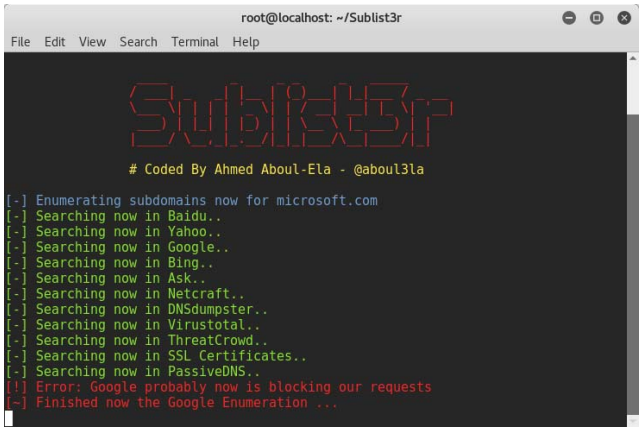

Fig. 3. Subdomain gathering using Sublist3r tool

III. Subdomain Takeover Process

A. Detection of Subdomain Takeover Vulnerability

Making a final list of the available or valid domains and subdomains, we have to find out whether there DNS records are assigned to external services or not. For this we have to check their assigned specific A record or CNAME record by DNS lookup & HTTP response/status code as follows:

1) Checking DNS Record: We can check DNS record of a subdomain by using Linux command dig or DNS lookup i.e. dig subdomain.ieee.org and also from free tools available in online like viewdns.info or dnsrecord.io. If the subdomain appears to assign to an external service, then we'll move forward to check its HTTP response.

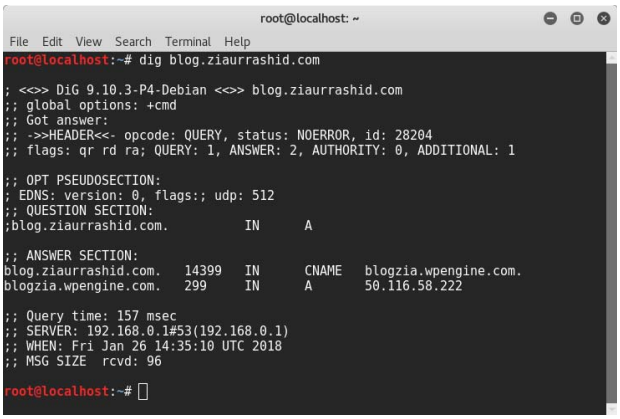

Fig. 4. Checking DNS Record using dig command

2) Checking HTTP Response: Either by visiting the subdomain we can see the HTTP response or using Linux command curl we can also detect HTTP response. If we get 404 responses and see a default 404 error page of the external service as shown fingerprint in Table I, we can initially assume the subdomain as vulnerable and move forward to takeover process.

TABLE I
Some Vulnerable Services

Services	Fingerprint (404 Page Response)
S3 Bucket	The specified bucket does not exist
Bitbucket	Repository not found
Cargo Collective	404 Not Found
Feedpress	The feed has not been found.
Ghost	The thing you were looking for is no longer here
Github	There isn't a Github Pages site here.
Help Juice	We could not find what you're looking for.
Help Scout	No settings were found for this company:
JetBrains	is not a registered InCloud YouTrack
Azure Web App	404 Web Site not found
Readme.io	Project doesnt exist... yet!
Surge.sh	project not found
Tumblr	doesn't currently exist at this address
UserVoice	This UserVoice subdomain is currently available!
Wordpress	Do you want to register *.wordpress.com?

B. Subdomain Claiming

After gathering the unused DNS entries for the particular subdomain for external services anyone can easily claim that subdomain by creating an account on that same external service whereas the subdomains are pointed. For example, subdomain (e.g. demo.domain.com) uses a CNAME record pointed to an external service domain (e.g. service.cloud.com). But the external service domain (service.cloud.com) is not claimed or the service is expired which is available to anyone for registration. Since CNAME record from subdomain (demo.domain.com) is not removed, anyone can take full control over the subdomain by registering external service domain (servuce.cloud.com) until the CNAME entry is present from subdomain (demo.domain.com).

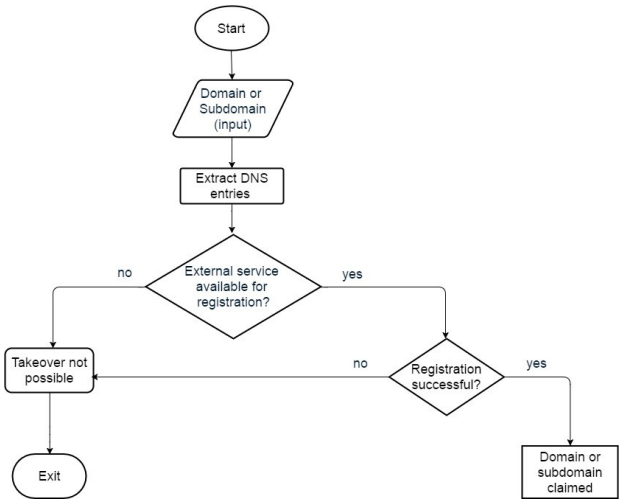

Fig. 5. Simplified detection and takeover process

IV. Risk Analysis of Subdomain Takeover

Typically, most of the organizations don't check or audit their website DNS record on a regular basis. Most of the cases, the organizations do not have a standardized process for surveillance DNS configuration and logging changes. Consequences of a subdomain hijacking as we introduce in this paper can lead to very high severity risks as mentioned below.

1) Phishing and Malware Attack: Doppelganger domains or Typosquatting are often used by the attackers to mimic the reputable website or domain for phishing purpose [11]. An attacker can utilize a hijacked legitimate domain or subdomain to launch mass spare phishing campaign to collect victims personal information including credit card and can trick victims in order to distribute malware which can be enhanced by issuing a valid SSL certificate from Let's Encrypt Authority.

2) Cross-site Scripting and Account Takeover: Adversaries can misuse the hijacked domain or subdomain to steal users sensitive cookies over HTTP request and can takeover users account capturing the session from Single Sign-On (SSO) wildcard session cookies [12]. Moreover, it is also possible

to execute malicious code on another domain that allows executing JavaScript code from the hijacked domain or subdomain using content security policy.

V. Mitigation

To mitigate the attack for the affected domain or subdomain, the user should promptly remove the abandoned DNS entries or claim the service on the external service whether the domain or subdomain was pointed. As this vulnerability can be considered as high severity, to prevent this attack pattern we proposed an ownership verification model for third-party services that is illustrated in Figure 6. The proposed model is divided into two sections as follows:

1) Availability Checking: In this stage, user inputted domain or subdomain will be cross-checked with database to check the availability. The process will move to the next step when the domain or subdomain is available to register otherwise the process will be terminated.

2) Verification: This stage contains three verification types such as DNS record (A, CNAME, TXT etc.) verification, given file upload verification and administrative webmail verification. User may choose any of these verification options to register domain or subdomain. For DNS record verification, a randomly generated A, CNAME or TXT record and a HTML file will be provided to user for DNS record and file upload verification process respectively. If user can able to configure the given records or file for his domain or subdomain then the ownership will be verified. For webmail verification process, a verification link will be sent to domain administrative webmail i.e., admin@domain.com or webmaster@domain.com to verify the ownership.

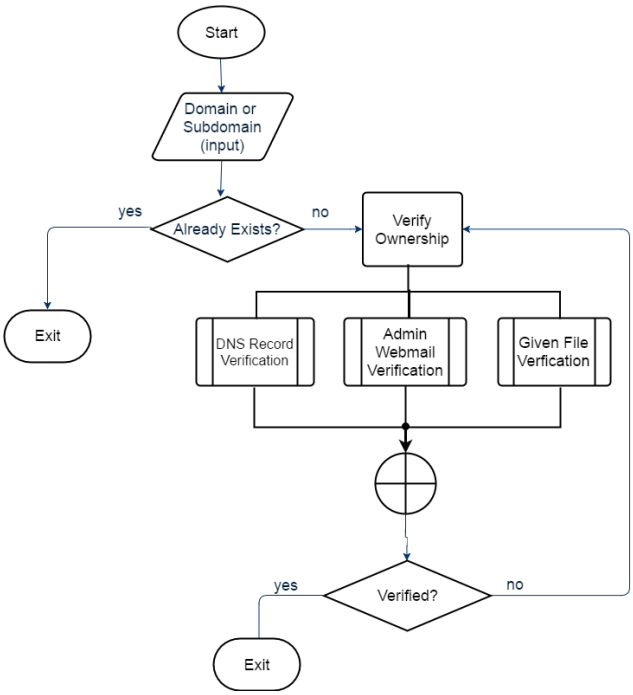

Fig. 6. Flowchart of Proposed Domain Ownership Verification Process

VI. Conclusion

The cyber world is changing day by day. Hackers are always digging for new ways to break down the security and try to get access to various company's internal information, users email, personal information, application or web server for their own purpose. In most of the cases, hacking attempts are automated while fishing for known vulnerabilities such as publicly disclosed 0day, outdated WordPress or Joomla plugins, old application codes etc. On the other hand, sophisticated attacks are more one on one laser targeted to companies with large customer base such as brands. Getting hacked any company's website can result in severe downtimes, private data breach and in some cases domain name hijacking. Subdomain hijacking is a simple, non-traceable and an emerging threat that affects lots of high-rank websites without thier owner's consent. In this paper, we tried to describe the attack scenario and how preventable such hacks could have been since it's mostly due to human negligence. Preventing subdomain takeover starts with proper surveillance and analysis of the DNS records. This paper helps the future researchers to find out the comprehensive scenario for cloud DNS security and automate the monitoring process more smoothly and promptly.

References

[1] T. Vissers, T. Barron, T. Van Goethem, W. Joosen, and N. Nikiforakis, "The wolf of name street: Hijacking domains through their nameservers," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: ACM, 2017, pp. 957–970.

[2] A. Herzberg and H. Shulman, "Fragmentation considered poisonous, or: One-domain-to-rule-them-all.org," in *2013 IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 224–232.

[3] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007, pp. 335–342.

[4] G. D. S. Team, "CVE-2017-14389: Application subdomain takeover," 2017. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-14389

[5] F. Rosen, "DNS hijacking using cloud providers – No verification needed," in *OWASP APPSec Conference Europe 2017*, 2017.

[6] A. Borgwart, S. Boukoros, H. Shulman, C. v. Rooyen, and M. Waidner, "Detection and forensics of domains hijacking," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.

[7] L. Chengsui, T. R. Valladares, and Z. Gang, "Chaos-based secure scheme against dns hijacking in the ip multimedia subsystem," in *International Conference on Cyberspace Technology (CCT 2013)*, 2013, pp. 150–153.

[8] S. H. Daiping Liu and H. Wang, "All your dns records point to us: Understanding the security threats of dangling dns records," in *2016 ACM SIGSAC Conference on Computer and Communications Security*. 2978387: ACM, 2016, pp. 1414–1425.

[9] E. A. Z. H. Adam Ali.Zare Hudaib, "DNS advanced attacks and analysis," *International Journal of Computer Science and Security (IJCSS)*, vol. 8, no. 2, p. 63, 2014.

[10] P. Thomassen, J. Benninger, and M. Margraf, "Hijacking dns subdomains via subzone registration: A case for signed zones," *Open Journal of Web Technologies (OJWT)*, vol. 5, no. 1, pp. 6–13, 2018.

[11] S. Sivakorn, I. Polakis, and A. D. Keromytis, "The cracked cookie jar: Http cookie hijacking and the exposure of private information," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 724–742.

[12] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, "An authentication flaw in browser-based single sign-on protocols: Impact and remediations," *Computers and Security*, vol. 33, pp. 41–58, 2013.