A Review on DNS Rebinding

Guo Xuanzhen[a], Pan Zhulie, and Shen Yi[b]

National University of Defense Technology, Hefei 230031, China

[a]18707017967@163.com,[b] shenyi@nudt.edu.cn

Keywords: DNS Rebinding, SOP, IoT, defense measurement

Abstract: As an indispensable infrastructure of the Internet, the DNS system carries the task of mapping domain names and IP addresses to each other, and is closely related to various Internet activities. On the other hand, DNS has become an important springboard for malicious attacks and an important tool as a threat to the Internet security. As an attack method using the DNS system, DNS Rebinding appeared as early as the late 1990s. It can use the victim's browser as a springboard to enter the internal network, steal sensitive data, and obtain the control right of devices. With the popularity of IoT devices, DNS Rebinding technology has new uses. This paper studies the development and changes of DNS Rebinding technology in the past 20 years, and has a general grasp of the development trend of DNS Rebinding. It better understands this attack method and puts forward corresponding defense opinions.

1. Introduction

As an important infrastructure of the Internet, the domain name system performs a vital role in connecting various applications and resources on the Internet. It provides key support services for the normal operation of various domain-based Web applications, email, and distributed systems.

At present, the total number of global domain names exceeds 300 million, and the number exceeds 10 million, providing 100 billion query services per day. Therefore, the security of the DNS system is the key to the fluent operation of the Internet. With the increasing commercial value of the Internet, malicious attackers have begun to use DNS systems to carry out malicious network attacks. Some large malicious organizations can even use their special capabilities to conduct attacks, which seriously affects the overall operation of the Internet. In order to improve the security protection ability of the DNS system, a large number of excellent research results have emerged. However, with the continuous development of computer technology, the battle between attack and defense around the DNS system are constantly, and the DNS system will still face many security and technical challenges.

Despite many advances in the detection and handling of cybersecurity threats, the Internet and its users have been the target of a series of attacks based on the DNS ecosystem. DNS attacks can be divided into two types, attacks using DNS systems and attacks against DNS systems. Attacks using the DNS system can be divided into two types, DNS-based attacks and DNS abuse. DNS protocol attack refers to a vulnerability related to DNS implementation that results in DNS mapping information exchanged between the client and server [1]. Man-in-the-middle attacks, DNS spoofing, and DNS Rebinding are known attacks based on the DNS protocol [2]. Attacks against the DNS system are designed to affect the normal function of the DNS system. The purpose is to consume resources, control operational resources, or operate stored information. Denial of service attacks, distributed denial of service attacks, server hijacking and cache poisoning are all typical attacks against DNS systems.

DNS rebinding can be traced back to as early as 1990s, and brought a greater impact. For example, in 1996, Princeton University research team made based DNS java applet of rebinding attack [3]. Stanford University web security research team, in 2007, published a white paper on DNS rebinding attacks. With the increasing popularity of the Internet of Things devices, this slightly old attack

methods gained new life. In the 27th Defecon, researchers demonstrated the use of DNS rebinding technology, the Google home, Roku TV, sony stereo equipment, Sonos Wifi Speakers, radio thermostat and other equipment to attack and capture device control authority [4]. Using DNS rebinding stealing bits credits Ether square in. Things security company Armis Disclosure worldwide nearly 500 million devices under threat of such attacks in [5]. CVE-2018-1002103 has shown the fact that using DNS rebinding to reach remote code execution on Minikube, and realize virtual machine escape effect. 2018, Blizzard gaming platform repair a DNS rebinding vulnerabilities, an attacker could exploit the vulnerability, sending commands to the privileged target by Blizzard Update Agent of JSON-RPC service.

2. Background

2.1 Same Origin Policy

The same-origin policy is a security measurement adopted by the browser. The same-origin policy restricts which network messages one origin can send to another. Scripts from different sources cannot read or write each other's resources without explicit authorization. Only the script from the same source grants permissions to dom, read and write cookies, session, ajax and other operations. A URL is composed of a protocol, a domain name, a port, and a path. If two URLs have the same protocol, domain name, and port, the two URLs are the same. Restrict the source. Do not use the source "document" to read or set certain properties on the current "document". Without being restricted by the same-origin policy, tag loading with the "src" attribute is actually a GET request initiated by the browser. Unlike XMLHTTPRequest, they load resources through the src attribute. But the browser restricts the permissions of JavaScript, making it impossible to read and write the content returned by it.

Table 1 Same Origin Policy

URL 1	URL 2	Same origin
http://a.com/index.html	http://a.com/welcome.html	yes
http://a.com/index.html	https:// a.com/index.html	no
http://a.com/index.html	http://b.com/index.html	no

2.2 Types of DNS Rebinding

DNS Rebinding can be divided into three forms: multiple A Records, time varying DNS, and multi-pin.

The first type is Multiple A records, which means that when the user wants to resolve a domain name through the victim, the authoritative name server will resolve to multiple A records and point to the IP address that he wants to access. The first DNS rebinding implemented in 1996 was to use multiple A records to trick the JVM virtual machine. However, due to changes in the Java security policy, the Java Virtual Machine no longer has this vulnerability. Because java applets can only establish connections with IP addresses within the same origin [6] [7].

The second type is called Time-Varying DNS, and it has the same principle as quick-swap DNS. That is, within a short period of time, there are two different resolution results for the same domain name. This requires that the TTL value set in the domain name resolution packet returned by the DNS server is very short, and the first resolution corresponds to the IP of the attacker's web server, and the second resolution is an intranet IP [8].

The third type is called multi-pin. Browsers use many plugins to render web pages. Many plugins allow socket connections to other resources within the same source. In order to fight against DNS pinning, DNS Rebinding uses various plug-ins to maintain different DNS pin databases. If the pin of one kind of plug-in is mapped to the IP address of the attacker, the other kind of plug-in is mapped to the intranet address [9].

2.3 How DNS Rebinding Works

Although there are many types of attack methods, the core idea of DNS rebinding is always the same, that is, the purpose of bypassing the same-origin policy is achieved through the IP conversion of DNS answer packets.

The specific steps of a DNS rebinding attack are:

① First, the attacker needs to control a domain name attack.com;

② The victim's domain name resolver will continuously send DNS resolution requests for the attacker's domain name. The domain name server controlled by the attacker will return a completely legal DNS response packet (IP = 158.45.1.23), but the time-to-live (TTL) value will be very small;

③ The victim successfully opened the attacker's webpage, and XHR or JS script was embedded in the return message of http, which requires access to a file under the current domain name after a period of time. This operation is happening all the time on the Internet, and it is completely legal.

④ But at this time, the TTL value expires, the DNS cache is cleared, and the attack.com needs to be resolved again. However, this time the DNS return packet is different from the previous one. The IP value is the IP that the attacker wants to access, so that it can be bypassed smoothly. Through the protection of the same-origin policy, the purpose of the attack is achieved.

Fig.1 Launch of DNS Rebinding(1)

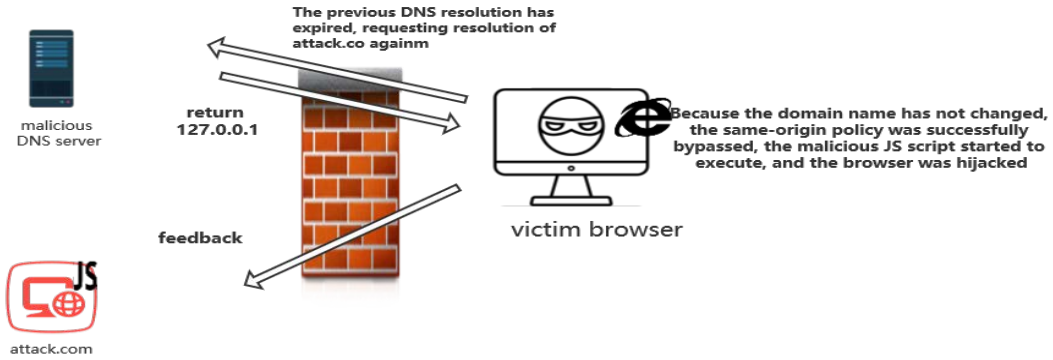

Fig.2 Launch of DNS Rebinding(2)

3. The development of DNS Rebinding

The development of DNS Rebinding can be divided into three phases: starting phase, maturing phase, developing phase.

3.1 Starting Phase

Same Origin Policy was introduced in 1996. Soon after its introduction, the Princeton University's

Secure Internet Programming team first mentioned this attack method in 1996.

This attack method returns two IP addresses to the victim: the IP of the attacker's server, the server that loaded the applet, and another IP that points to the target of the attack. When the attacker can control the order of the values in the DNS response message, the applet may be spoofed and connected to the target system.

With the emerge of JavaScript, Adam Megacz extended the DNS Rebinding attack form to Javascript in 2002 [10]. In total, Megacz showed two attack methods. The first attack method he used domain relaxation technology. The second method is called quick-swap DNS, that is, in a short period of time, the IP resolved by DNS is different.

3.2 Maturing Phase

In 2006, Martin Johns discovered a technology that can effectively make Firefox and IE browsers abandon the mapping of IP and domain names, making it possible for DNS rebinding attacks using JS scripts [11]. In the following months, several new DNS rebinding methods have been disclosed. Konatoka showed in an article called anti-DNS pinning + socket to implement this attack through Flash Applet. Konatoka and Johns use the conversion of Live-Connect JS code to Java code, and use Java to achieve the purpose in the process of DNS rebinding [6].

In 2007, Jackson and others discovered a large number of previously undiscovered DNS rebinding attacks [12]. These attacks make use of the interaction between the browser and the plug-in. The Java LiveConnection is established through various plug-ins to achieve deceptive effects and bypass DNS pinning. Their research proves that DNS rebinding can penetrate devices that cannot be reached by other means, and can even hijack the victim's IP address, thereby expanding the attack surface.

3.3 Developing Phase

Yunxing Dai et al. Proposed an attack method called Firedrill in 2013 [13], which integrates DNS rebinding attacks and DNS flooding attacks. By using the browser's DNS cache table and combining existing DNS rebinding attack technologies, Effective bypass for DNS pinning. And Dai et al. Compared Firedrill with other DNS rebinding methods (multiple A, multi-pin, time-varying), and summarized the dynamics and effectiveness of the method. Although there are many types of attack methods, the core idea of DNS rebinding is always the same, that is, the purpose of bypassing the same-origin policy is achieved through the IP conversion of DNS answer packets. Dai et al. Set up a malicious DNS server and set up a malicious JavaScript proxy on the victim's host. It maintains a websocket connection to the attacker's webserver and receives proxy commands in JSON format. The existence of JavaScript proxy is helpful to maintain the integrity of the data. HTML files, binary files and images can be transmitted. At the same time, firedrill provides an attacker interface to facilitate the attacker to grasp the real-time attack situation. At the same time, Dai uses time-to-launch and impact-of-the-attack as indicators to evaluate the effectiveness of Firedrill's attacks.

In 2018, DNS rebinding, an ancient attack method with a history of more than two decades, has recently become the focus of attention again. According to a report by network security company Armis, IOT devices allowed in many large enterprise environments have been affected. Threat of DNS rebinding attacks. Around 496 million devices have been affected worldwide [5].

Table 2 IoT Devices threatened by DNS Rebinding

the type of vulnerable devices	vendors	Number of vulberable devices
87% of switch and router	Aruba,Cisco,Dell,Netgear	14 million
78% of streaming media player	Apple,Google,Roku,	5.1 milllion
77% of IP phones	Avaya,Cisco,Nec,Polycom	124 million
66% of printers	Epson,Konica,Lexmark	15 million
57% of smart telephones	Samsung,Vizio	28.1 million

It can be seen that the most threatened are IP phones and printing equipment, and the equipment used for network connection is also threatened accordingly. Because firewalls generally focus only on in-band links and not on out-of-band links. Through DNS rebinding, the browser sends control

commands directly to relevant IOT devices in the intranet.

Gunes Ascar et al from Princeton University studied the control technology of local IoT devices based on web attacks [14]. This is said to be the first study to apply DNS rebinding attacks to the control of IOT devices. This article describes two attack methods, namely network topology mapping and device discovery attacks, and DNS rebinding attacks. Attack one is used to obtain intranet information, and attack two (namely, DNS rebinding) is used to obtain device permissions. In 2006, Lam et al. Scanned local devices by spreading worms through web pages. Unlike previous research, attacks can work on web pages based on the HTTPS protocol and can be performed in parallel. It bypasses the same-origin policy through HTML5 MediaError interface error messages to realize the detection of the internal network, but cannot control the internal network devices. Attack 2 bypasses the same-origin policy through DNS rebinding attacks to control the device. Experiments have shown that it can affect D-link wifi camera, Samsung SmartCam HD pro and other devices. But this attack method has large false positive rate and failure rate.

In 2018, Alexandre Kaskasoli proposed using the browser's Headless feature to implement DNS rebinding attacks [15]. Take Chrome as an example. Headless Chrome browser is a browser without an interface. Headless browsers can still execute JS code, and the default page timeout is 240 seconds. The author proposes a DNS rebinding automation attack framework dref, which uses this framework to send a constructed spoofed http message to a list of URLs, and records the return time, User-agent based on the message returned by the website. Whether it can execute JS code. After screening, we found that Chrome headless browser meets the requirements. Using the dref framework to successfully implement a DNS rebinding attack, malicious JS scripts can be executed in the browser's internal network to achieve the purpose of bypassing the same-origin policy, entering the internal network, and stealing sensitive information.

In 2018, Brannon Dorsey demonstrated that through DNS rebinding, UPnP protocol and http protocol, it successfully bypassed the protection of firewall and browser same-source policies, and gained control of a large number of smart devices in home WiFi environments. And Dorsey open sourced the DNS rebinding attack framework used-DNS rebinding toolkit. Through this attack framework, remote attackers can bypass the network firewall and use the victim's browser as a springboard to communicate directly with internal network devices. DNS rebinding toolkit is a front-end Javascript-based DNS rebinding utilization framework [16].

In 2019, Dennis Tatang et al. used DNS Rebinding to test the security of several IoT devices[17]. The team proved that Top 100 websites in Alexa Top list were not associated with DNS Rebinding.

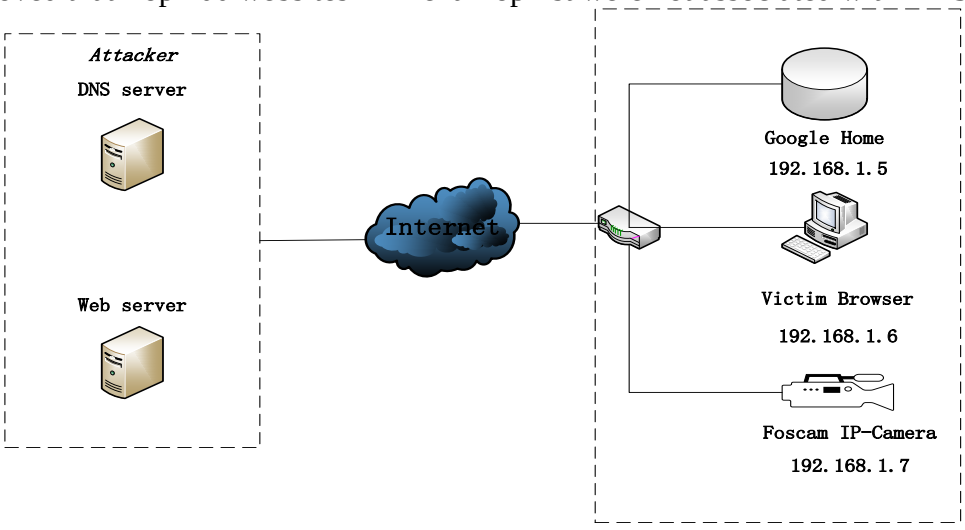

Fig. 3 Test Experiment

4. DNS rebinding defense technology

The main response of most browsers and plug-in vendors to DNS rebinding is the introduction of

DNS pinning. Ignoring the TTL value, only the unique IP (the IP that first parsed the feedback) was used for the same URL [18]. When DNS pinning is used, the IP-to-DNS mapping of Web resources will be maintained for a long time, and ideally will exceed the lifetime of the resource. Although DNS pinning can provide the necessary protection, DNS pinning also has several functional flaws. DNS pinning is inherently incompatible with all DNS response technology measures that rely on dynamic and potential changes, such as load balancing, disaster recovery, or CND networks. At the same time, when the web proxy is part of the communication path with the server, it cannot provide effective protection.

Restrict intranet IP: Due to the special nature of DNS rebinding, the internal server is the main target of the attack. Therefore, several techniques are proposed to protect internal network resources from external script attacks. Generally, these methods primarily protect resources that reside on private network blocks in the IPv4 space, as defined by RFC 1918. First, this protection can be implemented at the DNS level: DNSWall is a daemon that is designed to work with existing recursive DNS resolvers. It filters out private addresses in DNS responses. In addition, the Open DNS service provides a similar option. In addition, similar protection can be implemented in the browser: Opera refuses to access scripting code obtained from external sources to access the internal RFC 1918 IP range.

HTTP headers and fingerprint of the origin must be checked. Every origin of requests must be authorized and has its unique fingerprint. For those Http requests from hostnames in blacklist, the browser must turn to reject these requests.

Strengthen the defence of plug-ins. Flash player, SWF and java-applet can easily be used by DNS Rebinding as a loophole into the internal network. Refuse any socket connection to unknown or vicious sources. Stopping and blocking any connection to internal private IPs.

5. DNS rebinding detection technology

In 2013, Siva Brahmasani proposed a secondary detection method for DNS rebinding attacks[19]. For the generation of DNS rebinding attacks, either multiple DNS requests or multiple IP addresses are used to have multiple A records in the DNS response packet, using fast -flux frequently changes the IP address. However, the current defensive measures against DNS rebinding are either client-based or server-based. A defensive measure that takes into account both the client and the server is needed. Therefore, Brshmasani proposed a secondary DNS rebinding detection method. Check whether the DNS traffic is valid by querying the reverse query message.

Although this method can detect attacks on SOHO routers. However, the design of the detection system is flawed, because it involves unnecessary repeated detection, so when detecting DNS rebinding, there are problems of low efficiency and low accuracy. At the same time, in the face of the recent implementation of DNS rebinding, the system cannot identify it well. And the detection system needs to be integrated into the browser. No more filtering is performed on the intercepted message, and it is directly transferred to the decision algorithm. In addition, the TTL value of the domain name corresponding to the CDN network is also small, which is likely to cause misjudgment.

In 2014, Hongming Xin of the National University of Defense Technology developed Router Protector to resist DNS rebinding attacks on routers [20]. Because the use of DNS Rebinding to invade routers has strong concealment and harmfulness. Router Protector can automatically obtain the router's IP address and provide timely attack warning and effective security protection for the router, which has a strong practical significance. However, it still faces the problems of poor detection performance, unsatisfactory detection rate and false alarm rate, and slow detection speed.

6. Conclusion

In this paper, we have studied the developing trend of DNS Rebinding attacks in recent years, and concluded that due to the growing popularity of the Internet of Things, the scope of DNS Rebinding's influence has become wider. And summarize the defense measures of DNS Rebinding.

References

[1] Zhen RongFeng, Peng Hua et al. esearch on DNS hidden channel detection method based on requested domain name [J]. Information Network Security.2015

[2] Li Dong etal. Fast-Flux botnet detection method based on SVM [J]. Intelligent computer and application.2011

[3] Princeton University. DNS Attack Scenario. [online], http://www.cs.princeton.edu/sip/news/dnsscenario.html.

[4] Brannon Dorsey. Attacking Private Networks from the Internet with DNS Rebinding.2018. DEFCON 27

[5] Armis.DNS Rebinding Exposes Half a Billion Devices in the Enterprise[R].2017

[6] D. Byrne. Anti-DNS Pinning and Java Applets. Posting to the Bugtraq mailing list[C]. July 2007.

[7] D. Dean, E. Felten, and D. Wallach. Java Security: From Hot-Java to Netscape and Beyond[C]. IEEE Symposium on Security and Privacy, SP ’ 96, pages 190 – , Washington, DC, USA, 1996. IEEE Computer Society.

[8] He Xu. Impact of DNS rebinding on web browsers [J].Computer Engineering.2010

[9] C. Karlof, U. Shankar, J. Tygar, and D.Wagner. Dynamic pharming attacks and the locked same-origin policies for web browsers[C]. The 14th ACM Conference on Computer and Communication Security (CCS ’07), October 2007.

[10] D. Atkins and R. Austein, “Threat Analysis of the Domain Name System (DNS)[C]. Network Working Group, Request for Comments: 3833, August 2004.

[11] S. Alrwais, K. Yuan, E. Alowaisheq, Z. Li, and X.Wang, Understanding the Dark Side of Domain Parking[C] 23rd USENIX Security Symposium (USENIX Security 14), pp. 207 – 222, 2014.

[12] Jackson.et al.Protecting Browsers from DNS Rebinding Attacks [J]. ACM Transactions on the Web. Volume 3 Issue 1, January 2009

[13] Yunxing Dai and Ryan Resig. FireDrill: Interactive DNS Rebinding[C]. In USENIX Workshop on Offensive Technologies (WOOT), 2013.

[14] Gunes Acar.et al. Web-based Attacks to Discover and Control Local IoT Devices[C].IoT S&P.2017

[15] Alexandre Kaskasoli.et al. DNS Rebinding Headless Browsers[C].Blackhat.2018

[16] Brannon Dorsey. Attacking Private Networks from the Internet with DNS Rebinding[C].2018. DEFCON 27

[17] Dennis Tatang.et.al. Study of DNS Rebinding Attacks on Smart Home Devices[C]. International Workshop on Attacks and Defenses for Internet-of-Things.2019

[18] Martin Johns.et al. Eradicating DNS Rebinding with the Extended Same-Origin Policy[C]. USENIX Security Symposium. 2013

[19] Siva Brahmasani.et al. Two Level Verification for Detection of DNS rebinding attacks. [J]. International Journal of System Assurance Engineering and Management .2013

[20] Xin Hongmin. Research on the Impact of DNS Rebinding on Router and Its Protection Strategy [J]. Journal of Chengdu University of Information Technology.Vol.29 No.6.2014