Internet of Vulnerable Things (IoVT): Detecting Vulnerable SOHO Routers

Prabaharan Poornachandran, Sreeram R, Manu R. Krishnan, Soumajit Pal, Prem Sankar A U, Aravind Ashok
Amrita Center for Cyber Security Systems and Networks
Amrita Vishwa Vidyapeetham University
Kollam, India
{praba, sreeramr, manurk, soumajit, premsankar, aravindashok}@am.amrita.edu

Abstract— **There has been a rampant surge in compromise of consumer grade small scale routers in the last couple of years. Attackers are able to manipulate the Domain Name Space (DNS) settings of these devices hence making them capable of initiating different man-in-the-middle attacks. By this study we aim to explore and comprehend the current state of these attacks. Focusing on the Indian Autonomous System Number (ASN) space, we performed scans over 3 months to successfully find vulnerable routers and extracted the DNS information from these vulnerable routers. In this paper we present the methodology followed for scanning, a detailed analysis report of the information we were able to collect and an insight into the current trends in the attack patterns. We conclude by proposing recommendations for mitigating these attacks.**

Keywords—SOHO routers; DNS Changer; Internet of Vulnerable Things; Information Security; Vulnerabilities.

I. Introduction

Internet has evolved from a simple homogeneous research network model in the early days to a vast complex combination of homogeneous and heterogeneous networks. In the current world, it is no more a network of computers alone. Today, mobile phones, smartphones, smart TVs, refrigerators, surveillance cameras etc in a house are forming a small network, smart enough to communicate with the rest in the internet. Cisco [8] estimates that the number of devices that are getting connected to the internet was roughly 5 billion till 2012 and it is expected to grow up to a higher figure of 20 billion by 2020.

In the past few years there has been a tremendous shift and focus in the IoT paradigm. However most of the protocols that are supposed to make IoT possible are still in their infant stage from security point of view. With IoT anything and everything could be connected to the internet. One of the major problems faced by all the IoT devices is that the internet was not designed to connect these devices. Also the protocols still being in their development stage, majority of these devices are vulnerable and susceptible to attacks. There is no single, solid way to say a device connected to the Internet is secure unless we have well defined protocols that dictate the process of secure connection to the internet, which as of today is not available.

In 2012 FBI carried out an extensive operation to bring down multiple malicious DNS servers that were involved in DNS based phishing attacks [15]. The main tool that was used for this attack was a variety of malware that exploited misconfigurations and default settings in both computers and consumer grade home routers. This attack rendered thousands of users vulnerable to other forms of attacks. The mitigation opted by FBI was to take down the malicious DNS servers. Early 2014 saw the first IoT based botnet, the *"Thingbots"* [24], that sent out 7, 50,000 of spam mails from 1,00,000 consumer devices like home routers, connected multimedia devices, televisions and even 1 refrigerator.

The current state of the vulnerable IoT devices leads us to re-term the phrase Internet of Things to Internet of Vulnerable Things (IoVT). In this paper we discuss the security state of the basic internet connection at home. The fundamental question is "Are the devices that provide internet connectivity at home secure?" From phishing to DDoS, we looked into different attacks that were employed to exploit home routers. We scanned the Indian AS networks without disrupting the privacy of its users. Our aim here was to study the depth of the spread of certain common vulnerabilities know to the security community, thus gaining an understanding on the current security state of these devices in our country and identify solutions to mitigate these threats. We were able to find thousands of vulnerable home routers in the Indian AS space, identified different patterns in attacks and serious security concerns in the manner in which these net-works and devices are configured. In this paper, we also discuss in detail the analyses we performed on the vulnerable routers, the security implications of these vulnerabilities and the state of security in the Indian AS space. We also explain our experimental setup and its architecture we used to scan these networks. We also propose suggestions for mitigating these attacks and secure these networks. The key point to be noted is that we neither intruded into the privacy of any user nor performed any attack. This study's sole purpose is to put forward the security limitations currently present in the IoT paradigm.

II. Related Work

Internet Wide Scanning: Lot of research has been done where Internet wide-scan is used as to collect data. Work done in [1],[2],[3],[18],[19],[20] gives an insight into Internet wide device identification mechanisms and the different scenarios

978-1-5090-0487-4/15 $31.00 © 2015 IEEE
DOI 10.1109/ICIT.2015.49

involved. The present day Internet is not just a network of computer, routers and servers, but a jungle of all kind of devices. Even at a national level the networks of connected devices are measured in millions and trying to identify a device without knowing the IP address is like finding a needle in a haystack. Scanning IP addresses and identifying open and responsive ports are easy; the difficulty is in identifying the device sitting behind the IP address sending out the responses. Tools like Nmap [15] fingerprints the TCP stack of the software giving out these responses and tries to identify the devices based of the fingerprints. Though Nmap has an exhaustive list of fingerprints of common IT devices, they do not have the fingerprints of these "least important" community home routers. Now the only way left is to track the banners given out by services like HTTP, FTP, TELNET, etc. to identify the devices.

A couple of years back, the vastness of internet used to provide its own security by obscurity. With the advent of internet wide scanning tools like Zmap [1] and Masscan [11], it is not any more the same case. Still this only helps us to identify the open ports. Last couple of years has seen lot of studies happening in device detection [9]. The capability to detect devices in the internet lets us identify the different security issues with the current system. The ability to identifying vulnerabilities in these networks will help us reduce the risk of attacks.

Internet Wide Device Detection for Security Research: In 2014 Tiilikainen et al. [9] scanned the internet for identifying Industrial Control Systems that are directly connected to the internet. Though the scanning was limited to networks in Finland, they were able to identify automation devices ranging from thousands of Building Management Systems to Industrial Actuators and SCADA based systems. They also identified vulnerable services being run by these systems that can lead to remote access, information leakage and several other attacks.

DNS Changer Malware: In 2007, DNSChanger malware [14] first surfaced in the internet, affecting home routers and computers, redirecting their DNS request to multiple malicious DNS server. In 2012 a working group including FBI and several White Hat Security Groups was formed to curb this attack. They [6] identified the malicious servers, and shut them down and also provided tools for users to detect remove these malwares. An update report by Team Cymru [7] suggests the presence of new malicious DNS servers in the Internet and India has the second largest number of devices redirecting DNS traffic to these servers. Team Cymru tracks traffic to these servers to identify the affected devices. In this study, we attempt to identify vulnerable devices in the Indian networks by scanning the Indian AS network space and come out with proposals to secure these devices.

III. Methodology

To identify vulnerable home routers and to extract information from the routers, we came up with a scanner that is fast and efficient. The scanner is modularized and split into two phases. *Fig. 1* shows the architecture of the scanner.

A. Scan Phase

The scan phase deals with device identification and Internet wide scanning capabilities of the scanner. This phase has three modules working in sequence to identify home routers.

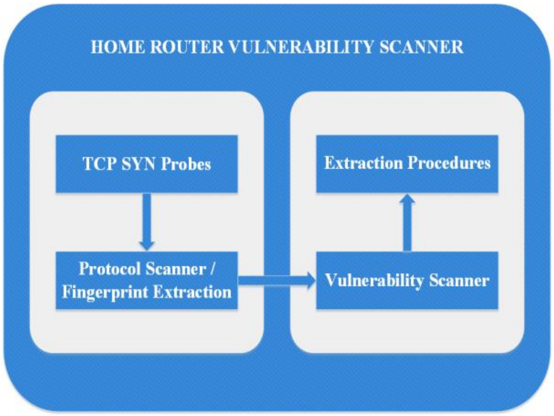
HOME ROUTER VULNERABILITY SCANNER
TCP SYN Probes
Protocol Scanner / Fingerprint Extraction
Extraction Procedures
Vulnerability Scanner

Fig 1. Modularized architecture of Vulnerability Scanner

The input to the scanner is the IPv4 subnets allotted to each network in India. The TCP SYN Probe module sends out TCP SYN requests to all IP addresses in the networks in the input file and listens to the incoming traffic to identify the response. All the requests are send out with a specific sequence number to help us track the responses. This module keeps track of all the IP address that responds to the SYN request and sends out RST to close the connection.

The IP that responds to the SYN request with a successful acknowledgement is then forwarded to the Protocol Scanner/Fingerprint Extraction module which sends out HTTP HEAD request to each IP address and tracks the response. The operation is multithreaded to improve the efficiency of the scan. We look for devices running RomPager HTTP server. The responses are sent to the parser which parses the HEAD section of the HTTP responses to identify the routers.

B. Extraction Phase

In the extraction phase we look into the known vulnerabilities in the device. We look into two common vulnerabilities, default configuration vulnerability and the ROM-0 vulnerability. This module checks whether a given IP address has the above mentioned vulnerabilities and if either of the two vulnerabilities are found, the required data from the router is extracted.

ROM-0 Vulnerability: This module checks whether the IP address is susceptible to ROM-0 vulnerability and if yes, it extracts the router configuration. This vulnerability allows us to download the backup configuration file of the router without any authentication. We identified that the compression used in the ROM-0 file is LZS. After following an automated decompressing technique, we found the file holds the admin password of the router.

It should be noted that we opt for exploiting the ROM-0 vulnerability rather that brute forcing the default configuration. Only in cases where ROM-0 vulnerability is not present, we proceed to check for the default configurations.

***Default Configurations Vulnerability*:** We collected an exhaustive list of default passwords of commodity home routers, especially those with running RomPager HTTP server, from different online sources. By simple brute forcing techniques -access to the router can be gained.

IV. Experiment results

As we are well aware of the privacy implications, we have taken special care while probing these devices. No user information is stored what so ever.

We performed a number of experiments to study the security state of these devices in India. We concentrated on three basic questions:

- How secure these devices are?
- Types of attacks employed by the attackers?
- Security Implications of the attacks?

A. Security state of consumer grade devices

In order to determine the current security state of SOHO routers in the Indian networks, we chose two common vulnerabilities found in low end consumer grade devices, and used them to extract DNS settings information. We identified that majority of these devices are vulnerable to attacks on default configurations. Another common attack, with a bit of sophistication was on the ROM-0 vulnerability. We scanned the Indian AS space for devices with any of these vulnerabilities.

We ran multiple scans over a period of 3 months with each scan spanning over a period of 4 days, scanning at an average of 100,000 IP in the Indian space running HTTP services. We identified 14,209 routers running RomPager HTTP server of which 4,514 are vulnerable to ROM-0 vulnerability and 2,403 routers have default configurations. Both vulnerabilities would grant an attacker administrative access to the routers.

A great deal of information could be extracted from the routers right from PPPoE credentials to WAN configurations. On detailed analysis, we identified lapses on the side of the ISPs in providing basic security measures to secure these networks.

B. Types of Attack Employed by Attackers

Studying the data gave us a deep insight into the types of attacks happening in Indian networks. Majority of the attacks are DNS based phishing attacks. Out of the 4,515 routers we found are vulnerable to attack, we identified 556 routers that redirect traffic to known malicious servers outside India. 3,312 routers redirect DNS requests to unknown servers outside India (not to known public DNS servers). Team Cymru's [6],[7] report identifies 9 malicious servers and we found 419 routers redirecting DNS traffic to these malicious server. Only 783 routers could be considered safe. This proves the wide spread attacks taking place in these networks and users or ISPs are not even aware of this. *Fig. 2* reflects the above mentioned statistics in a graphical format.

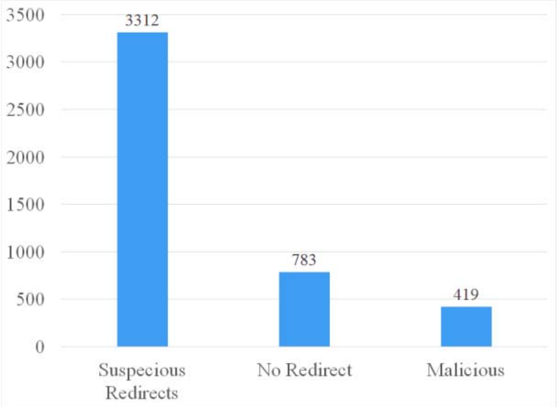

Fig 2. Type of DNS redirects by vulnerable home routers

The above results are limited to the number of routers we tested using two well-known vulnerabilities. There are lots of other vulnerabilities in the wide internet that attackers employ to gain unauthorized access to these devices. The alarming fact is that the home users in the India are under constant attacks by the adversaries and majority of these attacks goes undetected. The amount of defence mechanisms employed is almost nil leaving these networks susceptible to attacks.

C. Security Implications

After analysing the depth of attacks taking place, we looked into the security mechanisms put up by ISPs to prevent these attacks. These devices are configured by ISPs before the users actually use them. ISPs tend to provide weak authentication credentials that can be easily guessed. Another fact that came into our notice was that the ISPs do not follow any standards during the initial configuration process of the devices. Simple mechanisms like forwarding incoming requests to a non-existent private IP to prevent remote access could also be implemented.

We looked into the DNS redirection on a country basis as shown in Fig.3. By default, all routers should be redirecting their DNS requests to DNS servers provided by the respective ISPs. We discovered that only 17% of the routers forward their DNS traffic to the legitimate DNS server. It is alarming that majority of the vulnerable routers are redirecting traffic to unknown server in a wide range of countries as shown in *Fig 4.*

We also analyzed the security standards employed by the vendors of these devices. Strict security standards for firmware updates and security patches are not followed by the low end vendors in India.

Running multiple scans over a period of 3 months gave us the ability identify new malicious DNS server being employed by attackers. Team Cymru [7] reports that there is large scale SOHO router farming happening across the Internet and Indian networks are popular targets. Cymru reports that more than 9000 devices redirect their DNS traffic to servers in Russia.

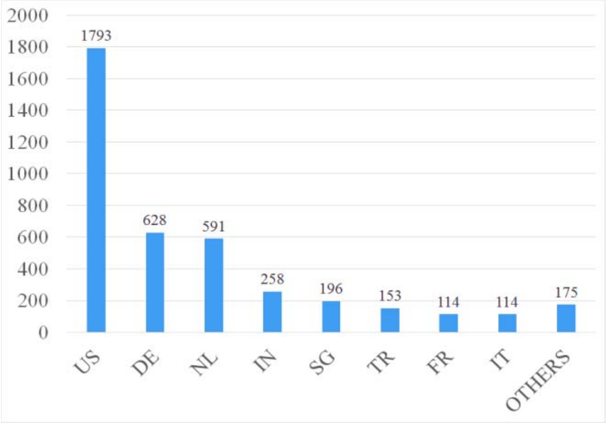

Fig 3. Country-wise classification of DNS traffic

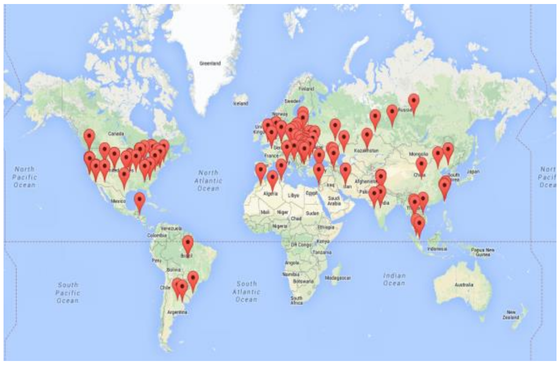

Fig 4. Country-wise distribution of DNS Servers

V. Threat Identification

The next logical step was to identify the source of these vulnerabilities so that we can come up with mechanisms to mitigate them. Fig. 5 shows a typical home routers' lifecycle. We have identified the vulnerabilities that are associated with each phase which helped us in identifying vulnerabilities in each stage and come up with mitigation solutions.

A. Manufacture Phase

This is the first phase in the life cycle of a consumer grade router, when it comes out of the manufacturer. We looked for vulnerabilities that are initiated at this phase.

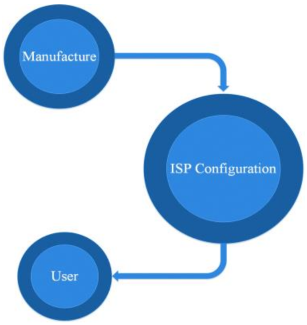

Fig 5. Life-cycle of Home Routers

Firmware Vulnerabilities: These vulnerabilities are generally caused as a result of design flaws or bad coding techniques where the developers tend to miss out on some possible vulnerable scenarios. Most of the time these vulnerabilities surface only after mass production and only if there is a prompt patching protocol in place, these devices can be patched. We found some of the cheaper models do not even have a patching mechanism in place nor do they publish firmware updates.

Default Configurations: Most of the home router manufactures provide restore to factory setting option used to reset the router credential to a default value. These devices are generally used by novice users who being unaware of the security implications do not change the password.

B. ISP Configurations Phase

All home routers are reconfigured by ISPs to work with their network. Vulnerabilities are induced to these devices at this stage too.

Common Passwords: The main configurations done at ISP level are to configure the PPPoE credentials and reset the WPA credentials (in case of wireless routers). The problem is that ISPs sometime tend use common password when configuring these devices. We found that even PPPoE credentials setup by the ISP tend to be the same in many cases, as we detected routers in the same IP subnet having the same password which is alarming from a security point of view.

***Lack of Security Protocols*:** We found that ISPs doesn't follow security standards and protocols to safeguard the home routers. Most of the routers have remote access privileges becoming and entry point for attackers. The best possible way to secure these devices is to prevent remote access.

C. End Users' Phase

Here we mention the vulnerabilities induced due to end user's lack of security knowledge.

Misconfigurations: User misconfigurations can render these devices vulnerable to attack. The best example will be leaving your wireless connection open.

Default Configuration Reuse: Users tend to continue using the credentials given to them by ISPs. We found that 70% of the passwords to be generally easily guessable or predictable based on the work by Malone et.al [26] [25].

VI. Suggestions

Based on the threats we identified we suggest various methods that could be incorporated at ISP level, the manufacturer level and the users to curb the vulnerabilities. Manufacturers should have proper standards in place to manage firmware updates and security patches on a regular basis. We understand it is not always possible to come up a complete solution, but should always be ready to take action when situation demands. Manufacturers could mandate periodical password change policies or change default settings policy on first use.

Even if the router models have known vulnerabilities, ISPs can play a major role in securing these devices. Setting up basic protocols to be followed when con-figuring these devices can be a game changer. We suggest ISP follow the following steps during initial configuration of the device into their network.

- Have proper ACL for remote access.
- Update router firmware and install all latest security patches available.
- Use random password generators for setting wireless passwords as well as PPPoE credentials.
- Make the user aware of the security risks involved and give out basic configuration guidelines.

VII. Conclusion

There is wide spread attacks happening all round the Internet and majority are believed to go undetected. By this study, we are making an attempt to unravel the security state our basic Internet connection.

We experimentally scanned the entire Indian ASN space and detected vulnerable home routers which are the basic interface to Internet for the common man. It was alarming that only 17% of the routers we identified could be considered safe for now. We explored the security protocols in place at both manufacture level as well as ISP level and found gaping holes in the system that simply renders this low end consumer grade devices vulnerable to attacks. We also came up with recommendations for both manufacturers as well as ISP to secure these devices.

We hope that there will be similar studies in future concentrating on different devices in the Internet. We believe continued research will help Internet developers come up with protocols and standards to secure the Internet of Things.

References

[1]. Durumeric, Zakir, Eric Wustrow, and J. Alex Halderman. "ZMap: Fast Internet-wide Scanning and Its Security Applications." *USENIX Security*. 2013.

[2]. Leonard, Derek, and Dmitri Loguinov. "Demystifying service discovery: implementing an internet-wide scanner." *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM, 2010.

[3]. Durumeric, Zakir, et al. "Analysis of the HTTPS certificate ecosystem."*Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013.

[4]. Heffner, Craig, and Derek Yap. "Security Vulnerabilities in SOHO Routers."*Retrieved September* (2009).

[5]. Heffner, Craig. "Remote attacks against SOHO routers." (2010).

[6]. Team Cymru,Growig Exploitation of Small Office Routers Creating Serious Risks,"https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/TeamCymruSOHOPharming.pdf"

[7]. Team Cymru, SOHO Farming Update, Online. Available at < https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/TeamCymruSOHOPharmingUpdate.pdf >

[8]. Dave Evans "The Internet of Things How the Next Evolution of Internet is Changing Everything" Cisco White Paper

[9]. Tiilikainen, Seppo. "Improving the National Cyber-security by Finding Vulnerable Industrial Control Systems from the Internet." (2014).

[10]. R. Shirey, "RFC 2828: Internet Security Glossary," May 2000. Status: Informational.

[11]. R. Graham, "Masscan: Mass IP port scanner." Online: https://github:com/

[12]. robertdavidgraham/masscan. Retrieved Sep 19, 2013.

[13]. Schmidt, Andreas. "Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security." *Cyberspace and International Relations*. Springer Berlin Heidelberg, 2014. 181-202.

[14]. Raiu, Costin. "Cyber-threat evolution: the past year." *Computer Fraud & Security* 2012.3 (2012): 5-8.

[15]. DNSChanger Malware [Online], Available: "http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf"

[16]. Lyon, Gordon Fyodor. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure, 2009.

[17]. Wolfgang, Mark. "Host Discovery with nmap." *Exploring nmap's default behavior*1 (2002): 16.

[18]. Berrueta, David Barroso. "A practical approach for defeating Nmap OS− Fingerprinting." *Retrieved March* 12 (2003): 2009.

[19]. M. Allman, W. M. Eddy, and S. Ostermann, "Estimating loss rates with TCP," ACM Performance Evaluation Review, vol. 31, pp. 12–24, 2003.

[20]. M. Allman, V. Paxson, and J. Terrell, "A Brief History of Scanning," in Proc. ACM IMC, Oct. 2007, pp. 77–82.

[21]. G. Bartlett, J. Heidemann, and C. Papadopoulos, "Understanding Passive and Active Service Discovery," in Proc. ACM IMC, Oct. 2007, pp. 57–70

[22]. J. Bethencourt, J. Franklin, and M. Vernon, "Mapping Internet Sensors with Probe Response Attacks," in Proc. USENIX Security, Jul. 2005, pp. 193–20

[23]. K. S. Keith Stouffer, Joe Falco, "Recommended practise: Improving industrial control systems cybersecurity with defense-in-depth strategies," Department of Homeland Security, Control systems security program, national cyber security division, 2009

[24]. Proofpoint Uncovers Internet of Things (IoT) Cyberattack, [Online], Available,< http://www.proofpoint.com/about-us/press-releases/01162014>

[25]. Vance, Ashlee. "If your password is 123456, just make it hackme" The New York Times 20 (2010).

[26]. Malone, David, and Kevin Maher "Investigating the distribution of password choices." Proceeding of the 21st international conference on World Wide Web. ACM, 2012