Hacking the router: characterizing real attacks targeting low cost routers using a honeypot router

Christian Scholten
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
c.p.b.scholten@student.utwente.nl

ABSTRACT

In this paper real hacker attacks against low cost routers will be investigated with the goal to get a better understanding of the intents of hackers and to find ways to improve defense mechanisms for these devices. This will be achieved by characterizing and analyzing real hacker attacks performed against a honeypot router device in a cloud environment. RouterOS from MikroTik will be recreated and run in a cloud environment to capture real hacker attacks. Furthermore, the different types of attacks against low cost routers will be discussed including which of these attacks can be mapped and how these attacks can be mapped.

Keywords

low cost routers, MikroTik, RouterOS, honeypot, security, vulnerabilities, hacker attacks

1. INTRODUCTION

Low cost routers have been a popular infrastructure device in underdevelopment countries, where they are used for expanding internet coverage in remote places. Low cost routers are cheap router devices which can be used as a home router or as a local area router with more advanced routing features such as the Border Gateway Protocol (BGP). These devices have been a popular target hackers with these attacks becoming more and more popular, with lots of regular news coverage of these devices actively being exploited. For example, the FBI discovered that hundreds of thousands of home routers were vulnerable against attacks from Russian hackers [1].

There are many different vendors providing these low cost router devices. Some of the popular vendors include Huawei, TP-Link, NetGear and MikroTik. With over 1.6 million devices publicly visible [2], MikroTik is a popular manufacturer of these low cost routers. In recent years, multiple vulnerabilities for MikroTik routers with a CVSS [3] score of 7 or higher were discovered [4]. These vulnerabilities have been a source for many attacks, one of which included two hundred thousand compromised MikroTik routers being used for mining cryptocurrency [5]. To protect systems and improve the security of the internet, it is important to characterize the attacks to such devices. By doing that, we can understand the intends of the hackers and set proper defenses.

In this paper, attacks on low cost routers will be characterized by using a honeypot router device in a cloud environment to capture real hacker attacks. A honeypot is a computer system intended to mimic targets of cyber attacks. These honeypots can be used to detect attacks or to deflect attacks from a real target [6]. The honeypot for this research will mimic RouterOS from MikroTik. MikroTik RouterOS is an important subject to study, due to the number of vulnerabilities published in recent years and the number of devices in underdevelopment countries. Another reason to choose MikroTik is that MikroTik supports downloading current and previous RouterOS releases as an image to run in a virtual machine or cloud environment. This makes it possible to test with different versions of RouterOS without the need to buy a MikroTik device. To be able to successfully detect hacker attacks against the honeypot, research will be done on the different attacks and how these attacks can be mapped.

2. RELATED WORKS

This section elaborates on related work to this research, after which the impact of this research is discussed.

M. Niemietz and J. Schwenk [7] evaluated routers from ten different manufacturers and shows how all of these are vulnerable for XSS attacks, UI redressing and fingerprinting attacks. The researchers were able to circumvent the security of all of the investigated routers. It discusses how these vulnerabilities can be exploited and provides countermeasures to make home routers more secure.

One of the protocols vulnerable for attacks is the BGP protocol. In the memo of S. Murphy [8] the vulnerabilities in the BGP protocol are analyzed. The memo discusses how the BGP protocol on routers can be used to delete, forge, or reply data with the potential to disrupt network routing.

Honeypots have been a common tool used by researchers to detect hacker attacks and the conference proceeding ”Honeypot router device for router protocols protection [9]” uses a honeypot to capture hacker attacks on routers. The honeypot was used to capture a real RIP attack. The proceeding offers a great insight in how a honeypot router can be created and used to capture real hacker attacks.

A similar conference from 2006 had a proceeding about dynamic honeypots by C. Hecker, K. L. Nance and B. Hay [10]. This proceeding argues for the use of a dynamic honeypot instead of a static or low/high interaction honeypots and explains the ways to set up a dynamic honeypot router with honeyd.

31st Twente Student Conference on IT Jul. 5th, 2019, Enschede, The Netherlands.

While no research has been done on using RouterOS as a honeypot device, some research has been done on monitoring attacks on MikroTik RouterOS. The article "Live Forensics on RouterOS using API Services to Investigate Network Attacks [11]" discusses using live forensics on RouterOS as a technique to capture hacker attacks. The article specifically mentions that only internal attacks were researched and research should be done on using live forensics to discover hacker attacks from external networks. This research was fairly limited and only included a proof of concept attack and did not involve any monitoring and characterization of real hacker attacks.

2.1 Impact

This research adds substantial information to the fields of analyzing attacks on low cost routers. A lot of research is available on the different types of vulnerabilities, with some research available about the subject of honeypots. All in all, very little research is available regarding the characteristics of real hacker attacks. The only research discussing attacks on MikroTik routers [11] only captured a proof of concept attack and only focused on attacks from the internal network. Characterizing the real attacks against routers will provide a better insight in the intents of hackers and can be used to provide new defend mechanisms against attacks on low cost routers.

2.2 Research aims

In this research the following research questions will be answered. The research questions are ordered in such a way that the that all previous questions need to be answered before the next question can be answered.

RQ1 What are the different types of attacks low cost routers are vulnerable to.
RQ2 Which attacks on low cost routers can be mapped and what methodology could be used to map each type of attack?
RQ3 How can attacks on low cost routers be characterized by analyzing real hacker attacks on a honeypot router?

3. METHODOLOGY

In the following section, the proposed method to answer each research questions will be discussed.

3.1 On answering RQ1

To answer **RQ1**, the different types of attacks that can be performed against low cost routers needs to be studied with the likelihood of these attacks happening. This will be done by with a literature review on the vulnerabilities in low cost routers and the different attacks that hackers perform on low cost router devices.

3.2 On answering RQ2

A understanding of which attacks on low cost routers can be mapped and the methodology to map these attacks is necessary to create the honeypot device. When knowing how these attacks can be mapped, choices can be made on which functionalities of the router should be recreated for the honeypot and how the attacks on the honeypot can be monitored. This is necessary to answer **RQ2** and ensure that the honeypot system will be most effective in capturing the attacks and allows for capturing the most important real hacker attacks on the device. To do this, testing will be done on a virtual machine running RouterOS, which will be used for testing purposes to recreate some of the possible attacks. The critical vulnerabilities in RouterOS will be tested with the intent to discover if these vulnerabilities can be exploited in order to gain access to the management interface or a root shell on the router.

3.3 On answering RQ3

To characterize the attacks on low cost routers in **RQ3**, the user interface or command line interface of a low cost router will be recreated and installed on a public IP-address as a honeypot device. The system will be set up to appear exactly as a regular router and will capture all requests and user interactions with the system. To appear as a convincing MikroTik router, it needs to be created such that the device appears convincingly enough as a MikroTik device with a vulnerable RouterOS installation with the same port setup visible on `shodan.io`. A visible Apache server, for example, could be an indicator to hackers that this is not a real routing device and make this research less effective. The captured attacks against the honeypot by real hackers will be analyzed to discover the intent of the hackers. This will be done by gathering statistics about the attacks performed on the honeypot by using the methodologies to map the different types of attacks from **RQ2** and it will involve analyzing the different types of attacks performed on the honeypot to characterize the different types of attacks and to discover the intent of the hackers. A literature review will be done and the statistics from the collected attacks on the honeypot router will be used in order to perform this characterization.

4. PRELIMINARY FINDINGS

In the preliminary research, information was searched for vulnerabilities in MikroTik RouterOS, to get a better understanding of the severity of the vulnerabilities and on how these vulnerabilities can be exploited. More research still needs to be done on the reproducability of these vulnerabilities and how these vulnerabilities can be detected. This is not a full list of vulnerabilities on RouterOS, but it does include some recent vulnerabilities with a high score on the CVSS scale.

4.1 Vulnerabilities in RouterOS

CVE-2018-7445 is a vulnerability with the maximum score of 10 following the CVSSv2 scale. The vulnerability involves a bug in the Server Message Block (SMB) service of RouterOS, which could cause a stack overflow. The overflow happens when before authentication, causing an unauthenticated hacker to be able to execute malicious code. According to Core Security, the exploit takes place in a function parsing NetBIOS names, receiving two stack allocated buffers. These buffers will be copied over to the destination buffer without any size validation on the original buffer. If the original buffers are larger than the destination buffer, a stack overflow will happen. With an appropriate payload, a hacker can use this to execute malicious code or even gain root [12]. The vulnerability has been solved by MikroTik in RouterOS 6.41.3/6.42rc27. A workaround is disabling the SMB functionality on the router [12].

CVE-2018-1156 is a vulnerability in the license upgrade system of MikroTik routers, which can be used to trigger a buffer overflow on the router and allow a hacker to remotely execute code. The vulnerability could be exploited by a remotely authenticated user with the following request [13]:

```
GET /ssl_conn.php?usrname=%s&passwd=%s&softid
=%s&level=%d&pay_type=%d&board=%d HTTP/1.0
```

CVE-2018-14847 was originally published as a low priority bug where an attacker could only gain read only access to

Table 1. Research Planning

Week	17	18	19	20	21	22	23	24	25	26	27
Finding related research	▨	▨									
Draft proposal		5/5									
Peer review draft proposal			7/5								
Proposal			12/5								
Researching attacks **RQ1**			▨	▨							
Mapping attacks **RQ2**				▨	▨						
Building honeypot					▨	▨					
Gathering attack data						▨	▨	▨			
Analyzing attacks **RQ3**						▨	▨	▨			
Draft paper							▨	▨	23/6		
Peer review draft paper										25/6	
Draft presentation									▨	▨	5/7
Final paper										30/7	
Presentation											5/7

all files on the router. The bug is a directory traversal error in WinBox, an application from MikroTik to remotely access to router. A researcher from Tenable Research discovered that there was more to this vulnerability than expected. The vulnerability could also be used to write files on the file-system via WinBox or HTTP, without requiring any authentication [14]. This discovery increased the CVSSv2 score from a 5 to the maximum score of 10. Tenable estimates that of the vulnerable devices, 70% will remain vulnerable [14].

CVE-2019-3934 is a similar vulnerability to CVE-2018-14847. This is another directory traversal vulnerability in the WinBox software, which allows the hacker read and write access to all files on the router. The main difference with CVE-2018-14847 is that this vulnerability requires authentication before it can be invoked [15].

5. PLANNED RESULTS

To answer the research questions, the research will deliver the following results:

1. An overview of the different types of attacks low cost routers are vulnerable to.
2. An overview of which of the attacks can be mapped and for each of these attacks a methodology for mapping them.
3. An evaluation of real hacker attacks performed on the honeypot device and a characterization of these attacks to discover the intent of hackers and proper defense mechanisms against attacks on low cost routers.

6. RESEARCH PLANNING

The planning for the research project is summarized in Table 1.

7. REFERENCES

[1] J. Menn and S. N. Lynch, "Fbi warns russians hacked hundreds of thousands of routers." `https://www.reuters.com/article/us-usa-cyber-routers-idUSKCN1IQ2DY`, May 2018. Accessed 29 April 2019.

[2] "Shodan search for 'mikrotik'." `https://www.shodan.io/search?query=mikrotik`. Data retrieved on 1 May 2019.

[3] "Nist - vulnerability metrics - cvss." `https://nvd.nist.gov/vuln-metrics/cvss`. Accessed on 3 May 2019.

[4] "Mikrotik routeros security vulnerabilities." `https://www.cvedetails.com/vulnerability-list/vendor_id-12508/product_id-23641/Mikrotik-Routeros.html`. Accessed on 29 April 2019.

[5] "200k mikrotik routers exploited to serve cryptocurrency miner." `https://www.pcmag.com/news/362889/200k-mikrotik-routers-exploited-to-serve-cryptocurrency-mine`, Aug. 2018. Accessed 29 April 2019.

[6] Norton by Symantec, "What is a honeypot? how it can lure cyberattackers." `https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html`. Accessed on 8 May 2019.

[7] M. Niemietz and J. Schwenk, "Owning your home network: Router security revisited," *arXiv*, June 2015.

[8] S. Murphy, *BGP Security Vulnerabilities Analysis.* The Internet Society, Jan. 2006.

[9] A. Ghourabi, T. Abbes, and A. Bouhoula, "Honeypot router for routing protocols protection," in *2009 Fourth International Conference on Risks and Security of Internet and Systems*, pp. 127–130, Oct. 2009.

[10] C. Hecker, K. L. Nance, and B. Hay, "Dynamic honeypot construction," in *Proceedings of the 10th Colloquium for Information Systems Security Education*, pp. 95–102, June 2006.

[11] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live forensics on routeros using api services to investigate network attacks," *International Journal of Computer Science and Information Security*, vol. 15, pp. 406–41, Feb. 2017.

[12] Core Security, "Mikrotik routeros smb buffer overflow." `https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow`, Mar. 2018. Accessed on 30 April 2019.

[13] Tenable Research, "[r1] mikrotik routeros multiple authenticated vulnerabilities." `https://www.tenable.com/security/research/tra-2018-21`, Aug. 2018. Accessed on 30 April 2019.

[14] Tenable Research, "Mikrotik routeros vulnerabilities: There is more to cve-2018-14847." `https://www.tenable.com/blog/mikrotik-routeros-vulnerabilities-there-s-more-to-`

cve-2018-14847, Oct. 2018. Accessed on 30 April 2019.

[15] Tenable Research, "Mikrotik routeros authenticated directory traversal." https://www.tenable.com/security/research/tra-2019-16, Apr. 2019. Accessed on 30 April 2019.