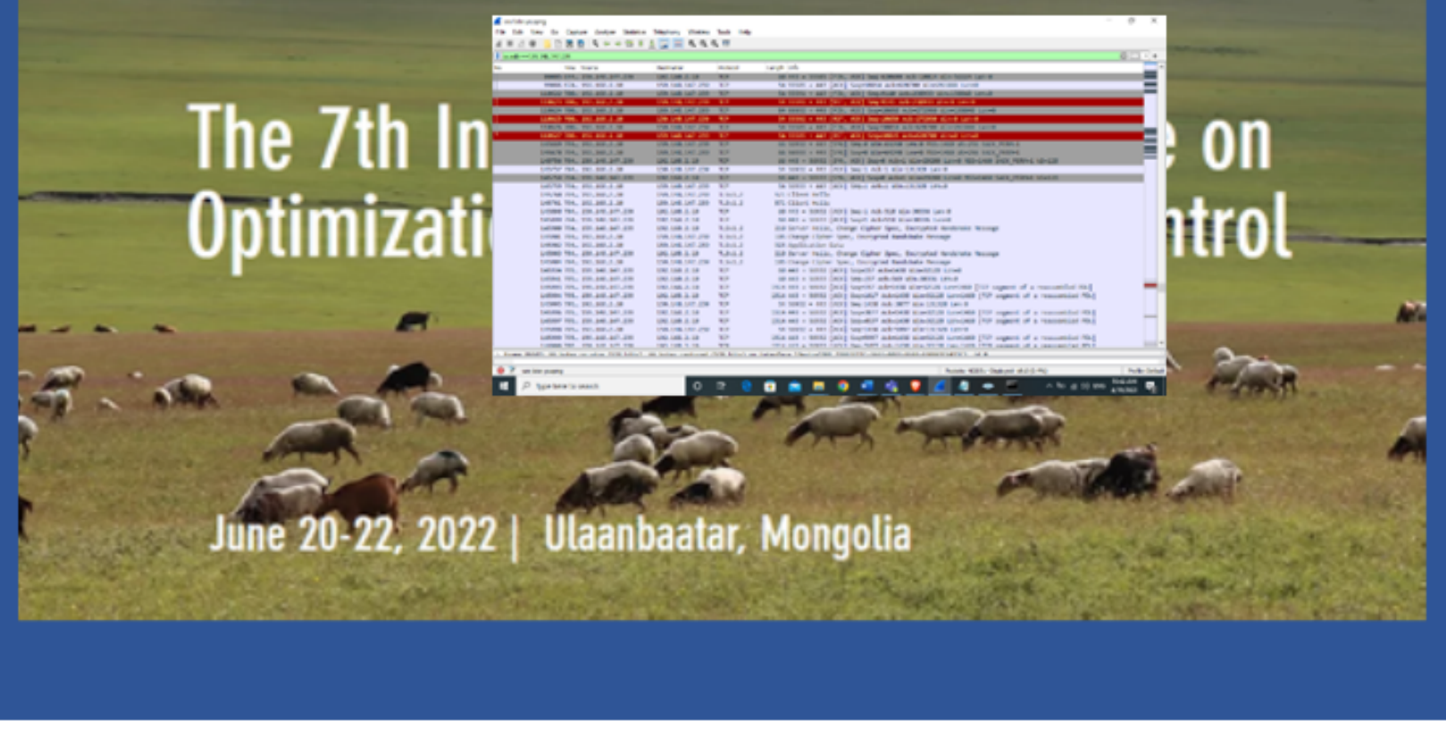
2. Surveillance
3. Obtain access rights
5. Perform the analysis on the basic configuration of WAF.
4. Maintain access
In this study router vulnerability research Wireshark [3] , By analysis using the Zen map [4-7] tool attack and FIG how chorus cause harm that is will be defined.



International Conference on Optimization, Simulation and Control
Detects an organization's network router being vulnerable to attack

Munkhjargal.B , Ms[1]; Byambadorj. D, PhD[1]; Densmaa B, PhD, *Associate professor*[1]
[1]Ulaanbaatar State University

Abstract

As part of our research, we conducted an analysis on Forum.mikrotik.com. A closer look at the site reveals that it contains malware and that the Micro-Tik router, which is commonly used in Mongolia, threatens to disrupt the network by eavesdropping on basic user information by putting corporate networks at risk. Therefore, most of the attacks on our country are directed at gateway routers. In the future, this study needs to be compared in more detail with DDoS-type attacks.

Introduction

With the rapid development of the information technology sector, ensuring information security has become a priority. Therefore, it is necessary to protect and control the computer network that transmits the information, and there are ways to protect it with security software such as antivirus and firewall, but it is not possible to fully protect it. Output routers pose a significant risk to an organization's information security operations. A study of router vulnerabilities provided a comparative assessment of static and dynamic analysis of risk assessments by vulnerabilities and threats to the organization's network [2]. There are five basic steps to doing this research.

1. Planning and survey
2. Surveillance
3. Obtain access rights
4. Maintain access
5. Perform the analysis on the basic configuration of WAF.

In this study router vulnerability research Wireshark [3], By analysis using the Zen map [4-7] tool attack and FIG how chorus cause harm that is will be defined.

RESEARCH METHODOLOGY

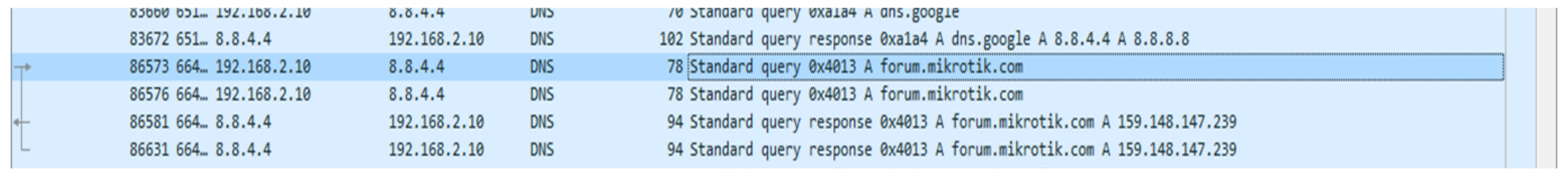
In order to check for common errors in the Micro-Tik router commonly used in Mongolia, a specially controlled and protected environment was created on a specially designed computer. Once a controlled isolation environment has been established, the initial state of the operating system is collected and analyzed for network traffic using the following programs.

EXPERIMENTS AND RESULTS

This work analyzes the normal and intrusive packets of the intranet. The test was performed on a computer with a 4 gigabyte frame with an I7 processor and WMware installed and created Windows 7 operating system in a virtual environment using the program. Regshot operating system registry information in a virtual environment After the application collects the information of the port information of the LAN devices, the computer registers connected to the network Zen map defined by the program. Analyzed packets over the network using Wireshark 2.0.1. Intranet router detects an attack from a network data stream with Wireshark or IP 159.148.147.239 was identified as a result of analysis of data transmission and received protocols of suspicious packets based on host-level packet information . The IP 159.148.147.239 address www.virustotal.com The following results were obtained by uploading to the site . F orum.mikrotik.com The site identified the following malware loading. These include:

- ➢AutoViewer.exe
- ➢Router Scan 2.60 Beta Portable by Stas'M.7z
- ➢Simple Traffic Bot.exe

Above malware Forum.mikrotik.com According to www.virustotal.com, malware can attack HYPERLINK "http://www.virustotal.com" a victim's computer by downloading it from the site.

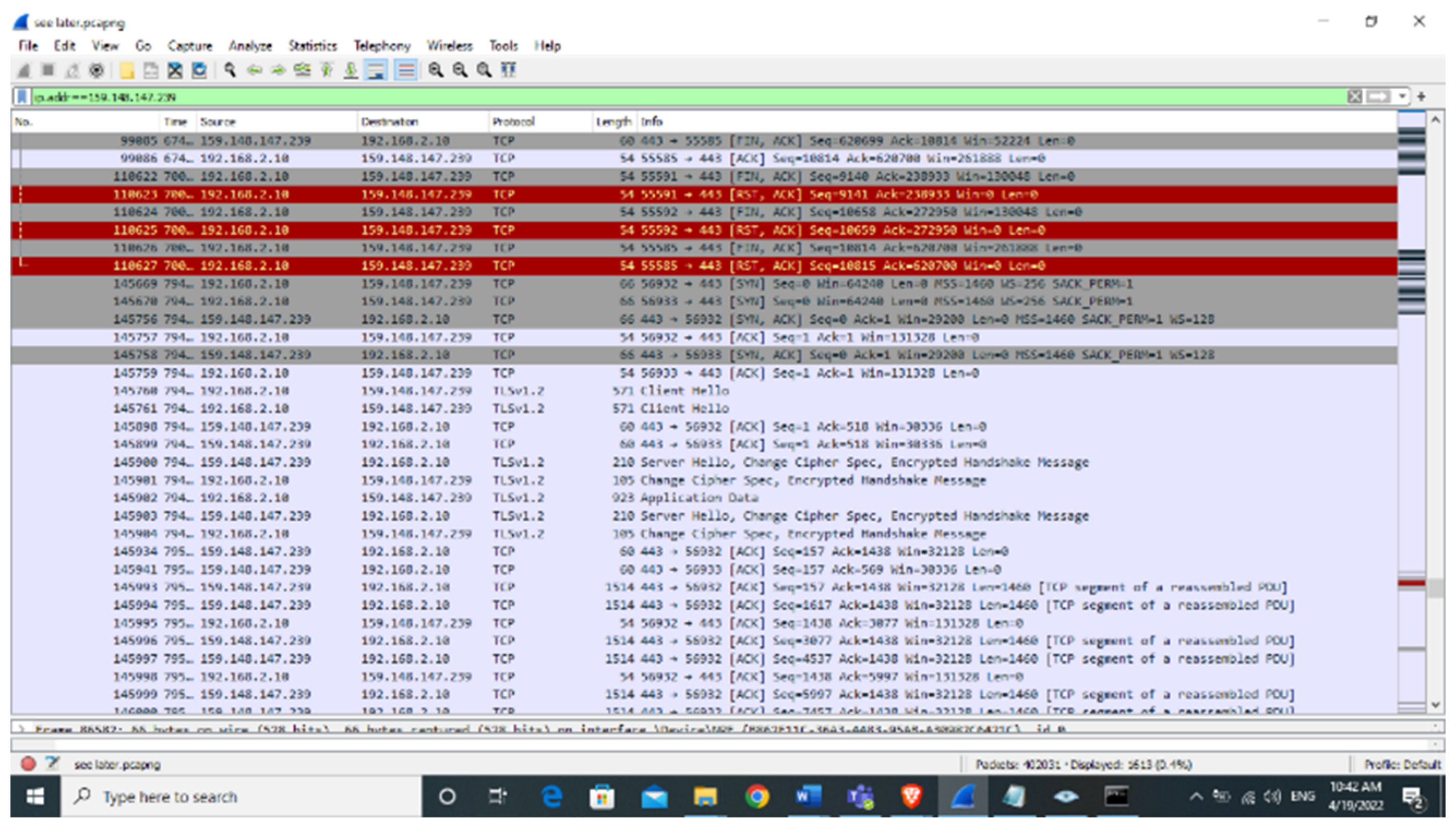


```
83660 651… 192.168.2.10   8.8.4.4        DNS    70 Standard query 0xa1a4 A dns.google
83672 651… 8.8.4.4        192.168.2.10   DNS   102 Standard query response 0xa1a4 A dns.google A 8.8.4.4 A 8.8.8.8
86573 664… 192.168.2.10   8.8.4.4        DNS    78 Standard query 0x4013 A forum.mikrotik.com
86576 664… 192.168.2.10   8.8.4.4        DNS    78 Standard query 0x4013 A forum.mikrotik.com
86581 664… 8.8.4.4        192.168.2.10   DNS    94 Standard query response 0x4013 A forum.mikrotik.com A 159.148.147.239
86631 664… 8.8.4.4        192.168.2.10   DNS    94 Standard query response 0x4013 A forum.mikrotik.com A 159.148.147.239
```

Figure 1. Loading Forum.mikrotik.com.

IP 159.148.147.239 to study the address in detail. F orum.mikrotik.com Regshot how the site is loading on a virtual machine and how it affects the host and the internal network and Wireshark , as shown in Figure 1-2.

Figures 1 and 2 describe the Denial of Service type ACK flooding attack and the Middle attack type attack. The attack revealed that sending a large number of ASCs and knocking down the TCP protocol slowed down the host's ability to eavesdrop on basic user information and passwords, causing system corruption and disrupting the Internet connection



```
ip.addr==159.148.147.239

No.    Time  Source           Destination      Protocol Length Info
 99885 674… 159.148.147.239  192.168.2.10     TCP        60 443 → 55585 [FIN, ACK] Seq=620699 Ack=10814 Win=52224 Len=0
 99886 674… 192.168.2.10     159.148.147.239  TCP        54 55585 → 443 [ACK] Seq=10814 Ack=620700 Win=261888 Len=0
110622 700… 192.168.2.10     159.148.147.239  TCP        54 55591 → 443 [FIN, ACK] Seq=9140 Ack=238933 Win=130048 Len=0
110623 700… 192.168.2.10     159.148.147.239  TCP        54 55591 → 443 [RST, ACK] Seq=9141 Ack=238933 Win=0 Len=0
110624 700… 192.168.2.10     159.148.147.239  TCP        54 55592 → 443 [FIN, ACK] Seq=10658 Ack=272950 Win=130048 Len=0
110625 700… 192.168.2.10     159.148.147.239  TCP        54 55592 → 443 [RST, ACK] Seq=10659 Ack=272950 Win=0 Len=0
110626 700… 192.168.2.10     159.148.147.239  TCP        54 55585 → 443 [FIN, ACK] Seq=10814 Ack=620700 Win=261888 Len=0
110627 700… 192.168.2.10     159.148.147.239  TCP        54 55585 → 443 [RST, ACK] Seq=10815 Ack=620700 Win=0 Len=0
145669 794… 192.168.2.10     159.148.147.239  TCP        66 56932 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
145670 794… 192.168.2.10     159.148.147.239  TCP        66 56933 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
145756 794… 159.148.147.239  192.168.2.10     TCP        66 443 → 56932 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
145757 794… 192.168.2.10     159.148.147.239  TCP        54 56932 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
145758 794… 159.148.147.239  192.168.2.10     TCP        66 443 → 56933 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
145759 794… 192.168.2.10     159.148.147.239  TCP        54 56933 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
145760 794… 192.168.2.10     159.148.147.239  TLSv1.2   571 Client Hello
145761 794… 192.168.2.10     159.148.147.239  TLSv1.2   571 Client Hello
145898 794… 159.148.147.239  192.168.2.10     TCP        60 443 → 56932 [ACK] Seq=1 Ack=518 Win=30336 Len=0
145899 794… 159.148.147.239  192.168.2.10     TCP        60 443 → 56933 [ACK] Seq=1 Ack=518 Win=30336 Len=0
145900 794… 159.148.147.239  192.168.2.10     TLSv1.2   210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
145901 794… 192.168.2.10     159.148.147.239  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
145902 794… 192.168.2.10     159.148.147.239  TLSv1.2   923 Application Data
145903 794… 159.148.147.239  192.168.2.10     TLSv1.2   210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
145904 794… 192.168.2.10     159.148.147.239  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
145934 795… 159.148.147.239  192.168.2.10     TCP        60 443 → 56932 [ACK] Seq=157 Ack=1438 Win=32128 Len=0
145941 795… 159.148.147.239  192.168.2.10     TCP        60 443 → 56933 [ACK] Seq=157 Ack=569 Win=30336 Len=0
145993 795… 159.148.147.239  192.168.2.10     TCP      1514 443 → 56932 [ACK] Seq=157 Ack=1438 Win=32128 Len=1460 [TCP segment of a reassembled PDU]
145994 795… 159.148.147.239  192.168.2.10     TCP      1514 443 → 56932 [ACK] Seq=1617 Ack=1438 Win=32128 Len=1460 [TCP segment of a reassembled PDU]
145995 795… 192.168.2.10     159.148.147.239  TCP        54 56932 → 443 [ACK] Seq=1438 Ack=3077 Win=131328 Len=0
145996 795… 159.148.147.239  192.168.2.10     TCP      1514 443 → 56932 [ACK] Seq=3077 Ack=1438 Win=32128 Len=1460 [TCP segment of a reassembled PDU]
145997 795… 159.148.147.239  192.168.2.10     TCP      1514 443 → 56932 [ACK] Seq=4537 Ack=1438 Win=32128 Len=1460 [TCP segment of a reassembled PDU]
145998 795… 192.168.2.10     159.148.147.239  TCP        54 56932 → 443 [ACK] Seq=1438 Ack=5997 Win=131328 Len=0
145999 795… 159.148.147.239  192.168.2.10     TCP      1514 443 → 56932 [ACK] Seq=5997 Ack=1438 Win=32128 Len=1460 [TCP segment of a reassembled PDU]

Packets: 402031 · Displayed: 1613 (0.4%)        Profile: Default
```

Figure 2. Attack on IP 159.148.147.239

Table №1 shows how the registry changes in the host operating system were compared with the non-infected registry information and the infected registry information after the physical machine-based virtual operating system registry information was pre-collected by Regshot.

TABLE 1 . THE REGISTER WAS CHANGED SECTIONS

Windows registry	DoS attack
HKLM \ Software \ Microsoft	
HKLM\System\ControlSet001\Control\	
HKLM\Hardware\	
HKLM\System\CurrentControlset\Services\	
HKLM\Software\Microsoft\Cryptography\	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	
HKU\S-1-5-21-602162358-492894223-299502267-500\Software\Microsoft\Windows\CurrentVersion\Run	X
HKLM\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication	

Conclusions

As part of our research, we analyzed F orum.mikrotik.com. A closer look at the site reveals that it contains malware, and that the micro-Tik router commonly used in Mongolia threatens to disrupt the network by eavesdropping on basic user information by putting corporate networks at risk. Therefore, most of the attacks on our country are directed at the gateway routers. In the future, this study needs to be compared with DDoS -type attacks.

Contact

Munkhjargal.B , Ms[1]; Byambadorj. D, PhD[1]; Densmaa B, PhD, *Associate professor*[1]
Mongolia, Ulaanbaatar
densmaa@usu.edu.mn
97689090981

References

1. Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection techniques for cyber-physical systems, April 2014, ACM Computing Surveys Volume 46 Issue 4
2. "About," Wireshark. [Online]. Available: http://www.wireshark.org/about.html. [Accessed: 18-Apr-2014]The History and Future of Nmap. Nmap.org. Retrieved on 2013-02-01.
3. The History and Future of Nmap. nmap.org. Retrieved 2008-05-14.
4. "Matrix mixes life and hacking". BBC News. 2003-05-19. Retrieved 2009-01-14.
5. Nmap Scripting Engine. Nmap.org. Retrieved on 2013-02-01
6. Tanenbaum, Andrew S. (2003-03-17). Computer Networks (Fourth ed.). Prentice Hall.ISBN 0-13-066102-3.
7. http://en.wikipedia.org/wiki/Windows_Registry
8. http://kb.chemtable.com/ru/windows-registry-main-keys.htm#hkcu
9. https://en.wikipedia.org/wiki/Man-in-the-middle_attac