ERT Threat Alert
The Mikrotik RouterOS-Based Botnet
March 27, 2018

Abstract

A newly discovered botnet targets TCP port 8291 and vulnerable Mikrotik RouterOS-based devices. MikroTik, a Latvian hardware manufacturer, products are used around the world and are now a target of a new propagating botnet exploiting vulnerabilities in their RouterOS operating system, allowing attackers to remotely execute code on the device. Such devices have been making unaccounted outbound winbox connections.[1] Radware's Emergency Response Team (ERT) has spotted an increase in malicious activity following Kaspersky's publication about the Slingshot APT malware that infected Mikrotik routers.[2] It is believed this botnet is part of the Hajime botnet.[3] Radware is witnessing the spreading mechanism going beyond port 8291 into others and rapidly infecting other devices other than MikroTik (such as AirOS/Ubiquiti). The concern is that this new botnet will be leveraged to launch DDoS attacks. This is another event demonstrating the struggle for control between various bot-herders.

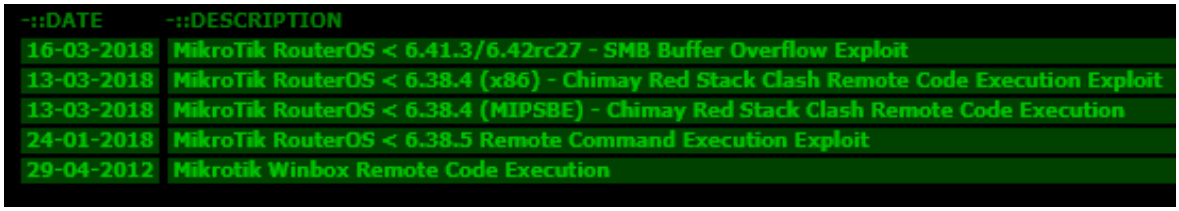

Figure 1: Multiple MikroTik exploits are available on GitHub and other sites

RouterOS Vulnerability

RouterOS is an operating system based on the Linux kernel, which implements functionalities normally used by ISPs, such as BGP, IPv6, OSPF or MPLS. RouterOS supported by MikroTik and its user community, providing a wide variety of configuration examples. RouterOS is embedded in MikroTik's RouterBOARD product line, focused on small- and medium-sized Internet access providers that typically provide broadband access in remote areas.

Preliminary analysis suggests that the botnet is exploiting known Mikrotik vulnerabilities (HTTP, SMB) as well as password brute-forcing. The worm has a highly efficient propagation mechanism by aggressively scanning for port 8291 in order to identify publicly available Mikrotik devices and using the password cracking capabilities to infect neighbor devices.

Mikrotik RouterOS SMB Buffer-OverflowVulnerability

A buffer overflow state occurs in MikroTik's RouterOS SMB service when processing NetBIOS session request messages. Remote attackers exploiting this vulnerability can execute code on the system. As the overflow occurs before authentication takes place, an unauthenticated remote attacker can easily exploit it.[4]

ChimayRed HTTP Exploit

The MikroTik RouterOS software running on the remote host is affected by a flaw in its HTTP web server process due to improper validation of user-supplied input. An unauthenticated, remote attacker craft a POST request to write data to an arbitrary location within the web server process, resulting in a denial-of-service condition or the execution of arbitrary code.[5]

---

[1] https://forum.mikrotik.com/viewtopic.php?f=2&t=132368

[2] https://www.bleepingcomputer.com/news/security/cyber-espionage-group-infects-victims-through-microtik-routers/

[3] https://forum.mikrotik.com/viewtopic.php?f=2&t=132368#p650340

[4] https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow

[5] https://www.tenable.com/plugins/nessus/99763

Infection Method

On 2018-03-24, 15:00 UTC time, Radware ERT research team has detected a huge spike on activity for TCP port 8291 in its global honeypot network.

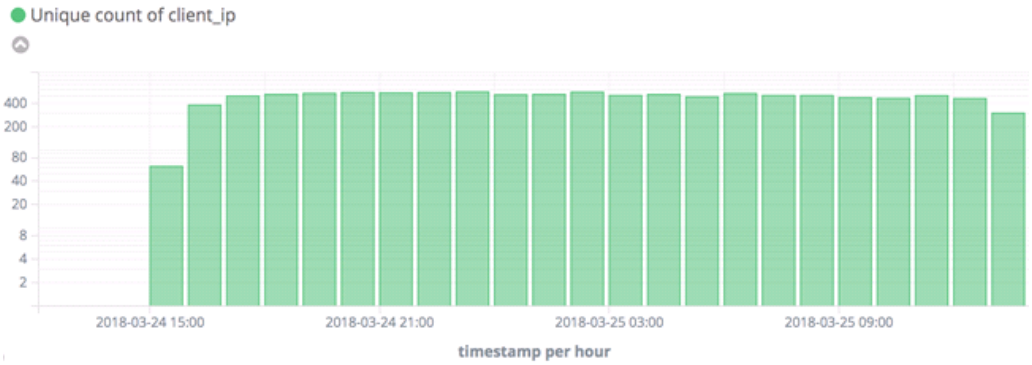

Figure 2: Unique IPs per hour, targeting TCP port 8291. Logarithmic scale

After near-zero activity for months, Radware witnessed over 10,000 unique IPs hitting port 8291 in a single day.

Country	# IPs
Brazil	7067
United States	1403
Iran	1114
Russia	876
India	712
Indonesia	706
Italy	656
Czechia	636
Poland	579

Figure 3: Distribution of unique IPs scanning for the vulnerability

The worm aggressively scans the Internet with SYN packets to port 8291, but it never actually establishes a 3-way handshake on that port, e.g. no payload is sent to the point.

```
1   0.000000 1[redacted].86.156 ?            TCP 54 45883 ? 8291 [SYN] Seq=2714532149 Win=14600 Len=0
2   0.000020          ? 1[redacted].86.156 TCP 58 8291 ? 45883 [SYN, ACK] Seq=4102402235 Ack=2714532150 Win=26883 Len=0 MSS=8961
3   0.394474 1[redacted].86.156 ?            TCP 54 45883 ? 8291 [RST] Seq=2714532150 Win=0 Len=0
```

It appears the worm utilizes this stealth-SYN scan method to quickly identify vulnerable Mikrotik devices, as this port is used almost exclusively by the Mikrotik RouterOS platform. In addition to scanning port 8291, the worm targets the following ports: 80, 81, 82, 8080, 8081, 8082, 8089, 8181, 8880.

Exploits

The worm uses the ChimayRed[6] exploit targeting vulnerable web servers on Mikrotik devices.
The worm will try to send the malicious payload to port 80 as well as other ports described earlier (80 81 82 8080 8081 8082 8089 8181 8880).

The worm has a very high success rate of exploiting and spreading, as mentioned in MikroTik's own post, "Our network had a major attack today as well. It seems like they opened some devices via the http port (quite an old firmware) and they tried to spread or access by brute forcing mikrotik neighbors."[7]

[6] https://github.com/BigNerd95/Chimay-Red/blob/master/POCs/StackClashMIPS_6384.py

[7] https://forum.mikrotik.com/viewtopic.php?f=2&t=132368#p650223

This means that the worm utilizes exploits as well as password brute-forcing attempts to nearby neighbors, speeding up the infection rate.

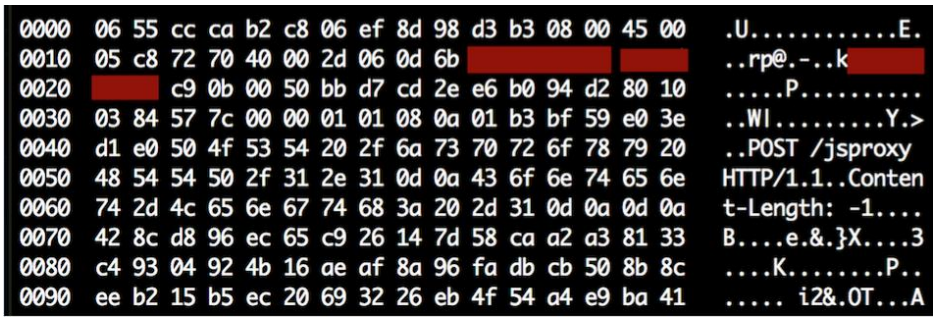

Figure 5: The exploit payload that Radware caught in its honeypot network

Hashes / IOCs

- /flash/bin/.telnetd
- /flash/bin/fifo
- /flash/bin/.p
- /flash/etc/rc.d/run.d/S99telnetd
- POST /jsproxy HTTP/1.1\r\nContent-Length:

Recommendations

Mikrotik recommends to block port 80/8291 (Web/Winbox) with a web application firewall and upgrade RouterOS devices to v6.41.3 (or at least, above v6.38.4). Follow MikroTik's thread on Twitter

Effective DDoS Protection Essentials against IoT botnets

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.