Microsoft releases open-source tool for securing MikroTik routers

April 18, 2022 | Theodoros Karasavvas

This blog was written by an independent guest blogger.

In mid-March, Microsoft released a free, open-source tool that can be used to secure MikroTik routers. The tool, RouterOS Scanner, has its source code available on GitHub. It is designed to analyze routers for Indicators of Compromise (IoCs) associated with Trickbot. This article will introduce some background on the MikroTik vulnerability, the Trickbot malware, and some ways you can protect yourself.

Trickbot emerges from the darknet

Trickbot was first discovered in 2016 and, despite efforts by Microsoft to stamp it out, has continued to remain a threat online. One of the main reasons for Trickbot's persistence is that it has continued to change and evolve over the years. As a result, Trickbot has proven to be an adaptable, sophisticated trojan of modular nature, molding itself for different networks, environments, and devices.

As Trickbot has evolved, it began to reach Internet of Things (IoT) devices like routers. Since Trickbot continuously improves its persistence capabilities by dodging researchers and their reverse engineering attempts, it has been able to maintain the stability of its command-and-control (C2) framework.

Why is the MikroTik security flaw important?

Malware is particularly dangerous because it can be ransomware, a special type of malware that takes control over your computer or devices. Trickbot, as it has grown and evolved, now includes a plug-in for backdoor access for Ryuk, a piece of ransomware with crypto-mining capabilities.

Once it had expanded its reach to networking devices, Trickbot began infecting MikroTik routers and modules and using them as proxy servers for its C2 servers and redirecting router traffic through alternative non-standard ports.

What makes the infection of MikroTik routers so significant is that they are used by millions of homes and organizations worldwide. The broad distribution of MikroTik routers gave Trickbot extensive infrastructure. Security flaws, like the MikroTik one, can be particularly important for web design because coders that work on the back end have to ensure that web pages are secure.

How does Trickbot work?

Researchers at Microsoft on the Microsoft Defender for IoT team discovered the exact mechanism that Trickbot's C2 system used to exploit MikroTik devices. Hopefully, by discovering its inner workings, Trickbot will be stamped out for good.

The reason hackers use Trickbot is that it allows compromised IoT devices to communicate between the C2 server and other compromised devices. Hackers then breach target routers, typically using a combination of brute force and exploits.

One of the key ways brute force techniques are used by malware to infect MikroTik devices is by utilizing default MikroTik passwords. They also exploit brute force attacks that utilize passwords harvested from other MikroTik devices. Finally, they exploit the CVE-2018-14847 vulnerability utilizing RouterOS versions older than 6.42. This exploit allows hackers to read files from the device like user.dat, which often contains passwords.

Once they've gotten access, they start issuing commands that redirect traffic between two ports on the router. Redirecting traffic creates the communication line between impacted devices and the C2.

In the end, catching on to how Trickbot worked involved sniffing out commands that were specific to the unique operating system, RouterOS and RouterBOARD, used by MikroTik IoT devices.

All IoT devices are vulnerable

The important takeaway for professionals and end-users is that all IoT devices are vulnerable. In fact, many journalists have recently brought attention to the dangers of networked security cameras in your home.

A professionally-installed ADT security system was exploited by a technician who used his access to watch people's deeply personal private lives. All of these cameras were IoT devices.

Although your smart fridge probably isn't spying on you, it's important to remember that the security landscape continues to expand as more and more devices become connected to the Internet. Devices that perform limited functionality, like routers and cameras, can often become prime targets for hackers because they are not regularly updated like smartphones and computers.

How do you protect yourself?

Utilizing special software tools can be a great way to protect yourself from cybersecurity threats. Microsoft's RouterOS Scanner is the go-to way to resolve the MikroTik router vulnerability. As you can see, exploiting one MikroTik device opens up the possibility for exploiting many more.

Microsoft did the tech community a huge favor by giving away their security tool for free, but this may not be the end for Trickbot. Unfortunately, as long as MikroTik devices continue to operate without having their firmware updated and their devices monitored, Trickbot will probably stay around.

Starting a cybersecurity audit can be a good way to find other ways your company might be at risk. Understanding your digital security needs is the first step in securing your network and enterprise. AT&T offers several enterprise-level cybersecurity network solutions that are worth examining.

Another thing all Internet users should do is change their default passwords to more secure unique passwords. Much of the damage done by Trickbot and the MikroTik exploits was because of default passwords shipped with the devices. Changing your default passwords will ensure that brute-forcing your network will be much harder.

Generating hard-to-guess unique passwords is actually the number one cybersecurity tip. Whether you're starting a blog for your small business or running a large company with hundreds of staff, creating a strong password is the best way to decrease your vulnerability to cyberattacks and loss of data privacy and security.

Staying educated is another way to ensure you stay on top of cyber security threats. Many large organizations offer training to employees to help them understand the terminology surrounding IT. It's important to continue to educate yourself, too, as threats can change, vulnerabilities can be patched, and new technologies can make how we approach security shift overnight.

Finally, enable multi-factor authentication or MFA whenever it's available. MFA can help cut down on unauthorized device access by requiring you to authenticate your identity every time you try to log on. MFA is a critical component of building a zero-trust cybersecurity model, which is the preferred way of securing your business today.

Conclusion

From Russia hacking Ukrainian government websites to the Okta hack that demonstrated even digital security firms are vulnerable to hackers, hacks and exploits have been all over the news lately. The release of Microsoft's MikroTik router tool marks a turn in digital security and demonstrates that companies and teams are working hard to ensure that digital security can be maintained.