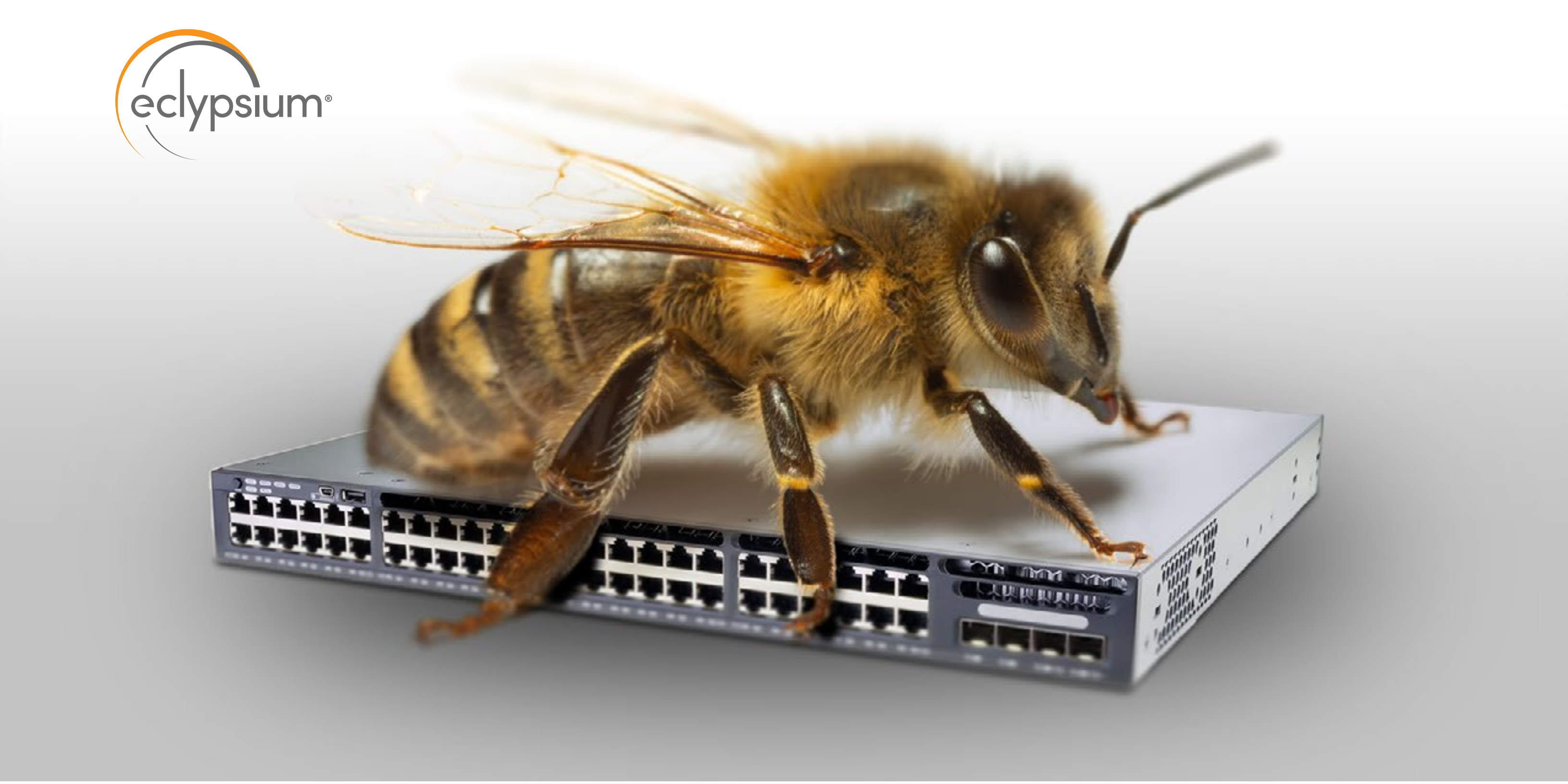


WHEN HONEY BEES BECOME MURDER HORNETS

What do you do when two million cheap and powerful devices become the launchpad for one of the most powerful botnets ever? You stop treating the threat like a newly discovered and unexpected honey bee hive and you start remediating like you've discovered a Murder Hornet nest.

Based in Latvia, MikroTik may not be a household name, but it has been a popular supplier of routers and wireless ISP devices since 1996 with more than 2,000,000 devices deployed worldwide. These devices are both powerful, and as our research shows, often highly vulnerable. For the money, there is hardly a more powerful device a consumer can get their hands on.

This has made MikroTik devices a favorite among threat actors who have commandeered the devices for everything from DDoS attacks, command-and-control (aka "C2"), traffic tunneling, and more. The ability to proxy and manipulate traffic should be of particular interest to enterprise security teams. With the increase in users working from home, attackers now have a wealth of easily discoverable, vulnerable devices that can provide attackers with easy access to both the employee's home devices, as well as devices and resources of the enterprise. In effect, the perimeter has as many holes as a bee's nest has hexagons.

And while threat actors have the tools to find vulnerable MikroTik devices, many enterprises do not. Even the default Shodan searches for MikroTik leave entire swaths of these devices undiscovered. Part of our research aim is to shine a light on this problem by mapping the MikroTik attack surface and providing researchers and security teams with tools that they can use to find both vulnerable and *already-compromised* MikroTik devices.

Given such a vast percentage of these devices have been in a vulnerable state for many years on end, it is simply not enough to find 'old' (vulnerable) devices. Instead, we need to leverage the very same tactics, techniques, and procedures (TTPs) the attackers use. We need to discover whether a given device might already be compromised and determine whether it is patched or not. Even non-vulnerable device firmware versions can still be readily configured for malicious purposes.

WHY IS MIKROTIK BEING TARGETED?

MikroTik devices present an enticing set of traits from the perspective of an attacker. First of all, they are plentiful with more than 2,000,000 devices deployed worldwide, and also particularly powerful and feature-rich devices. In addition to serving SOHO environments, MikroTik routers and wireless systems are regularly used by local ISPs. The same horsepower that can make MikroTik enticing to an ISP, can also be enticing to an attacker.

MikroTik devices are also prone to vulnerabilities. Like many SOHO and IoT devices, they often come with default credentials of admin/empty password, and even devices that are intended for corporate environments come without default settings for the WAN port. Additionally, MikroTik's auto-upgrade feature is rarely turned on, meaning that many devices are simply never updated. They also have an incredibly complex configuration interface, making it easy for users to make risky mistakes. All of this leads to a situation where there are thousands of vulnerable and EOL devices easily discoverable on the Internet, some of them over a decade old.

Lastly, MikroTik devices contain serious, remotely exploitable vulnerabilities. There are three CVEs from the past 3 years that can lead to remote code execution and a complete takeover of a device. Given the challenges of updating MikroTik, there are large numbers of devices with these 2018 and 2019 vulnerabilities. Collectively, this gives attackers many opportunities to gain full control over very powerful devices, positioning them to be able to target devices both behind the LAN port as well as target other devices on the Internet.

KNOWN THREATS AND CAPABILITIES

The Eclypsium Research Team began looking into MikroTik routers in early September of 2021. Based on our previous research into TrickBot and its firmware-targeting module TrickBoot we were particularly interested in how threat actors such as TrickBot used compromised routers as C2 infrastructure. Around this time last year, TrickBot was able to fall back on MikroTik infrastructure (and other SOHO devices) after US Cyber Command successfully disrupted their main infrastructure. This made us want to better understand the MikroTik attack surface and how attackers might use them once compromised.

No sooner had we begun our research, when news broke of a new record-breaking DDoS attack, with initial reports pointing to the Meris botnet. The Meris botnet, as you may have guessed, runs on MikroTik routers. Meris was able to use the SOCKS4 proxy of the MikroTik router and tunnel attack traffic to their targets. In previous research, Troy Hunt had observed infected MikroTik routers injecting cryptojacking scripts as the devices were routing web traffic.

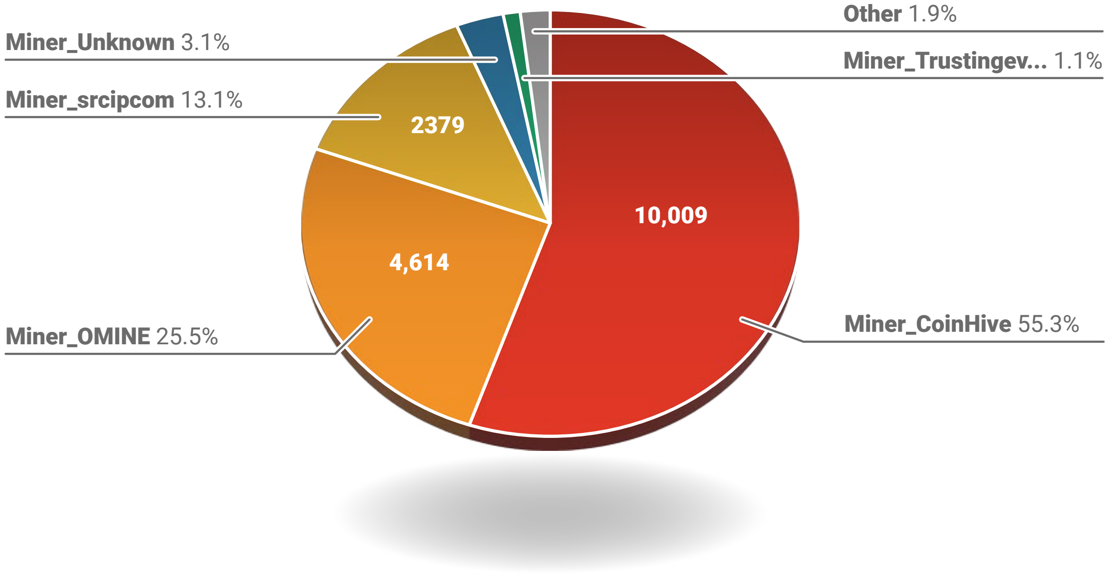
The capabilities demonstrated in these attacks should be a red flag for enterprise security teams. The ability for compromised routers to inject malicious content, tunnel, copy, or reroute traffic can be used in a variety of highly damaging ways. DNS poisoning could redirect a remote worker's connection to a malicious website or introduce a machine-the-middle. The router could scan the internal network behind the router. An attacker could use well-known techniques and tools to potentially capture sensitive information such as stealing MFA credentials from a remote user using SMS over WiFi. As with previous attacks, enterprise traffic could be tunneled to another location or malicious content injected into valid traffic. These types of attacks are not remotely far-fetched given that sophisticated threats such as TrickBot are already known to be using MikroTik devices.

PLOTTING THE MIKROTIK ATTACK SURFACE IN THE WILD

Based on the significance of these devices, we wanted to map out the exposure in the real world. We started by collecting basic information such as the device version, configuration, and other traits. During this process, we managed to find around 20,000 devices with proxy open and injecting mining scripts into web pages that the user visited. We have collected them into a dataset.

Top Crypto-Mining Scripts Observed on Exposed MikroTik Devices

(# of Occurences)



This is similar to the results found in previous research by Troy Hunt, after he was able to take over coinhive.com. At the time, they presumed MikroTiks are involved as well, but only about a half of the devices we found are directly attempting to connect to now-offline coinhive. Some of these devices still connect to active mining services.

We next followed with other security researchers to see if there were any ongoing campaigns related to MikroTiks. We found out that Meris malware was continuing to infect MikroTik devices en-masse, which correlated to our previous information.

Hunting the Botnet

The next step would be to find which exact hosts are already infected or potentially can be infected. However, direct testing would involve trying to log in to actual routers, which would require approval from the device owners. As a result, we first wanted only to use Shodan to map out the attack surface of vulnerable devices.

After reviewing a list of potential CVEs, we picked 4 that were the most impactful (pre-authentication, leading to full device takeover):

<= 6.45.6 - CVE-2019-3977, CVE-2019-3978 (winbox-based)

<= 6.42 - CVE-2018-14847 (winbox-based)

(recently added to CISA's KNOWN EXPLOITED VULNERABILITIES CATALOG)

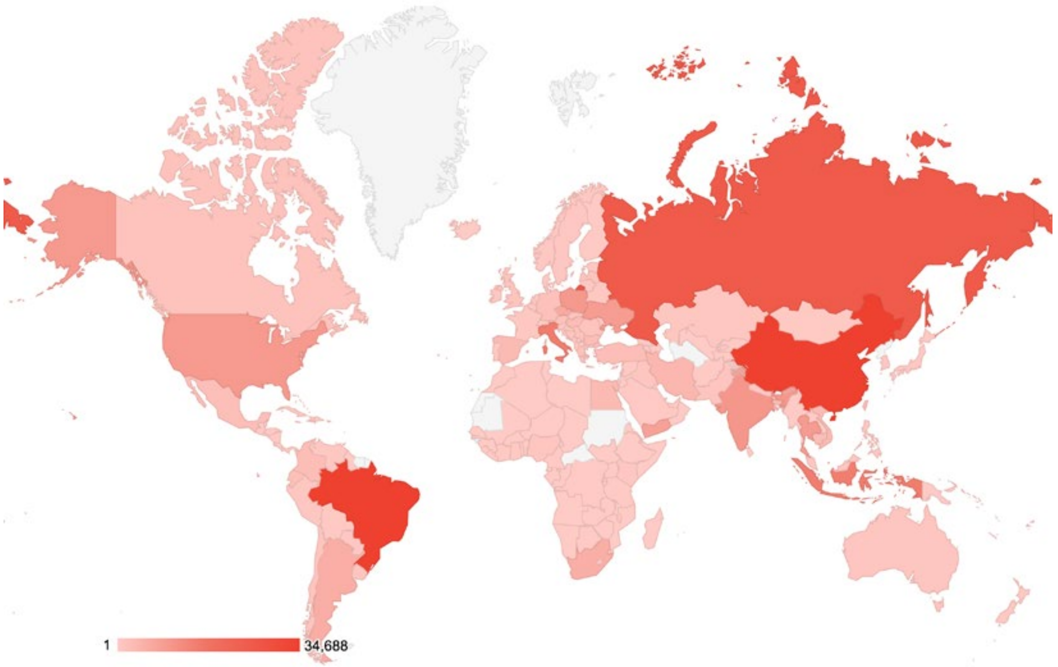
<= 6.41.3 - CVE-2018-7445 (smb-based)

As we can see, we are looking for:

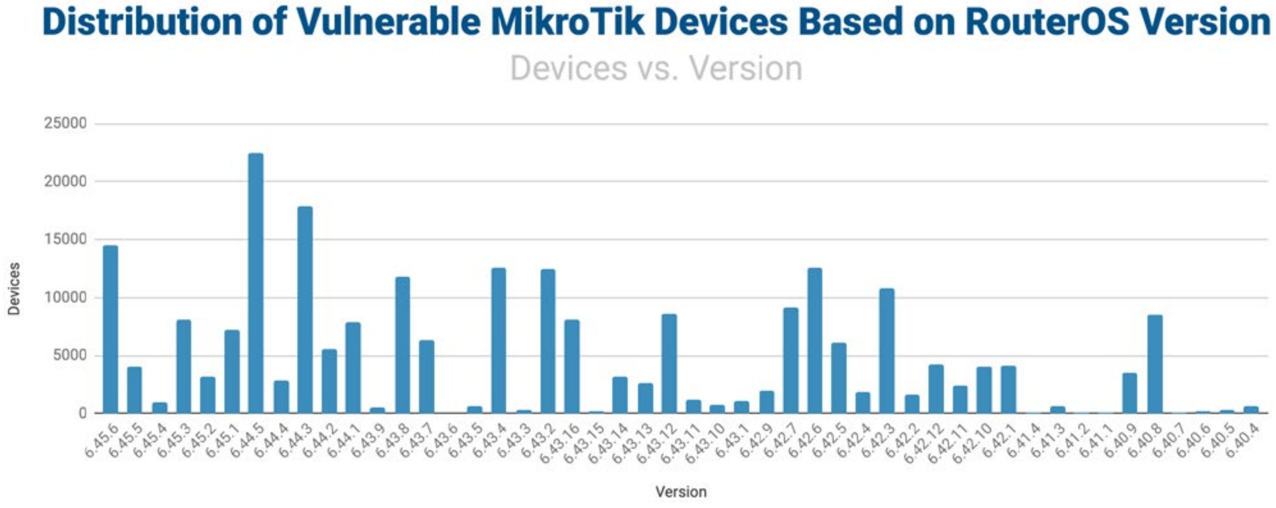
1. Devices with WinBox protocol exposed
2. Devices with RouterOS version <= 6.45.6

Using customized shodan queries, we managed to build a dataset of ~ 300 000 IP addresses vulnerable to at least one of these exploits. Analyzing the data we can see that vulnerable MikroTik devices are particularly widespread. China, Brazil, Russia, Italy, and Indonesia had the most total vulnerable devices with the United States having the 8th most.

Geographic Distribution Of Vulnerable Mikrotik Devices



Next, we looked at the distribution of devices based on the specific vulnerable version of RouterOS. The data was very irregular in terms of distribution, with some of the older versions accounting for large numbers of vulnerable devices. This highlights the large number of MikroTik devices that are simply never being updated.



BUILDING THE TOOL

Next, we wanted to arm administrators with a tool that could let them answer the following simple questions:

1. “Am I vulnerable?”
2. “Am I infected?”

However, automating such a test can be tricky as many devices only expose a proprietary WinBox protocol or a web UI based on this protocol. Additionally, the Meris malware only performs subtle configuration changes to the device, which makes it troublesome for admins to patch out. As a result, we wanted to code a new tool that would provide administrators with the ability to:

1. Identify MikroTik devices with CVEs that would allow the device to be taken over.
2. Attempt to log in with a given list of credentials (plus those found from the CVEs).
3. Check for IoCs of Meris on the device to infer compromise

Note, users of the tool should only attempt to login to devices that they own, and will take liability for their actions. Given that the Meris infector malware uses SSH, WinBox, and HTTP API, we wanted to integrate with all 3 protocols.

WinBox

Tenable had previously performed extensive research into RouterOS, and WinBox. https://github.com/tenable/routeros. In particular, their “By the Way” PoC (CVE-2018-14847, https://github.com/tenable/routeros/tree/master/poc/bytheway) and WinBox protocol implementation were particularly useful. We decided to use this implementation for WinBox integration, although it only supports older MikroTik versions. We cleaned up the PoC to not enable the devel user (which would be a backdoor), but only expose admin credentials. We also implemented a binary that, using provided credentials for the device, will dump the scheduler scripts from the device using the WinBox protocol.

HTTP API

The HTTP API is well-documented and has open-source modules: https://github.com/socialwifi/RouterOS-api.

SSH

For SSH, a simple command (/system scheduler export) can be used to list all the scheduler scripts.

Using this, we implemented the tool (link to the tool) that will attempt to:

- Exploit the list of IP addresses using the CVE-2018-14847
- Attempt to login using the exposed credentials (or using provided credentials)
- Check the listing of scheduler scripts for scripts with known-bad domains, or URLs that look similar to Meris C&C URLs.

In short, it will attempt to imitate the botnet, minus the infection part, and instead, detect the presence of the infection.

WHAT ENTERPRISE SECURITY TEAMS CAN DO ABOUT IT

Enterprise security teams should take steps to identify any vulnerable or compromised MikroTik devices in their environment and take appropriate action to mitigate their risk. Eclypsium customers can use the platform to automatically identify MikroTik devices and check them for vulnerabilities or threats. However, we are also providing access to a free tool (LINK) that anyone can use to check devices for the presence of a scheduler or CVE-2018-14847.

How to Identify Vulnerable Devices

For Eclypsium Customers - Eclypsium’s Network Devices Scanner is able to fingerprint MikroTik devices based on their HTTP and UPnP responses down to the specific version. The Eclypsium platform also provides automated analysis of MikroTik devices to identify vulnerabilities and threats. Customers should upgrade to version 2.8 or later in order to scan their MikroTik devices. Staff can then easily find MikroTik devices by searching ‘MikroTik’ on the Devices page of the Eclypsium Console or selecting MikroTik from the ‘Manufacturers’ dropdown list. The platform will automatically identify any vulnerabilities or threats present.

For MikroTik Customers without Eclypsium - Any MikroTik user can download our free MikroTik assessment tool here. This tool will check MikroTik devices to see if a scheduler script exists or if the device contains the critical vulnerability CVE-2018-14847.

How to Harden MikroTik Devices

MikroTik has previously published information on their blog in response to the Meris Botnet. This includes instructions on how to secure MikroTik devices and how to identify and resolve any compromises.

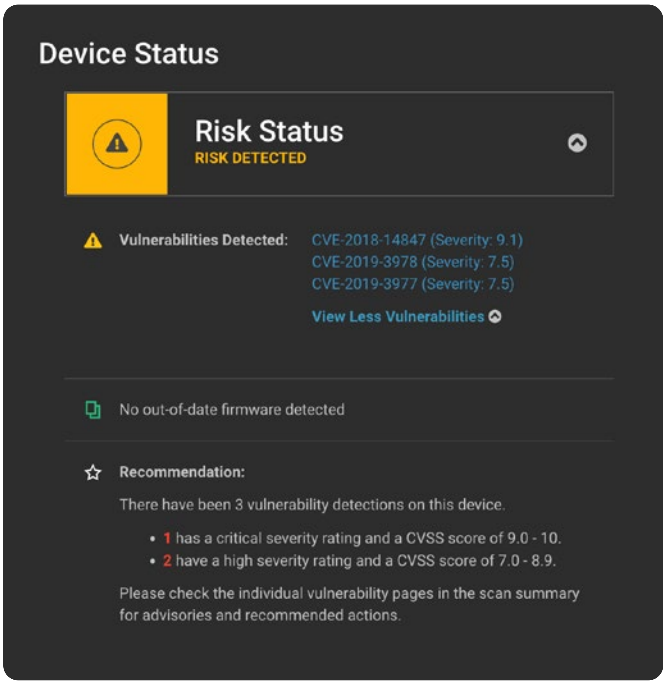
Instructions from MikroTik include:

- Keep your MikroTik device up to date with regular upgrades.
- Do not open access to your device from the internet side to everyone, if you need remote access, only open a secure VPN service, like IPsec.
- Use a strong password and even if you do, change it now!
- Don't assume your local network can be trusted. Malware can attempt to connect to your router if you have a weak password or no password.
- Inspect your RouterOS configuration for unknown settings including:

  System -> Scheduler rules that execute a Fetch script. Remove these.

  IP -> Socks proxy. If you don't use this feature or don't know what it does, it must be disabled.

  L2TP client named "lvpn" or any L2TP client that you don't recognize.
- Input firewall rule that allows access for port 5678.
- Block domains and tunnel endpoints associated with the Meris botnet.



Device Status

Risk Status
RISK DETECTED

⚠ Vulnerabilities Detected: CVE-2018-14847 (Severity: 9.1)
CVE-2019-3978 (Severity: 7.5)
CVE-2019-3977 (Severity: 7.5)

View Less Vulnerabilities

No out-of-date firmware detected

☆ Recommendation:

There have been 3 vulnerability detections on this device.

- 1 has a critical severity rating and a CVSS score of 9.0 - 10.
- 2 have a high severity rating and a CVSS score of 7.0 - 8.9.

Please check the individual vulnerability pages in the scan summary for advisories and recommended actions.

Vulnerabilities in network devices expose users and enterprises to a wide variety of risks. Highly capable devices such as MikroTik routers provide a particularly powerful asset for attackers. However, these devices routinely fly under the radar and are rarely updated or properly managed. Organizations need the ability to identify and assess this important attack surface both in the enterprise as well as their employee's remote work environments.

To learn more about this research, please contact the Eclypsium team at info@eclypsium.com.