Trickbot, a sophisticated trojan that has evolved significantly since its discovery in 2016, has continually expanded its capabilities and, even with disruption efforts and news of its infrastructure going offline, it has managed to remain one of the most persistent threats in recent years. The malware's modular nature has allowed it to be increasingly adaptable to different networks, environments, and devices. In addition, it has grown to include numerous plug-ins, access-as-a-service backdoors for other malware like Ryuk ransomware, and mining capabilities. A significant part of its evolution also includes making its attacks and infrastructure more durable against detection, including continuously improving its persistence capabilities, evading researchers and reverse engineering, and finding new ways to maintain the stability of its command-and-control (C2) framework.

This continuous evolution has seen Trickbot expand its reach from computers to Internet of Things (IoT) devices such as routers, with the malware updating its C2 infrastructure to utilize MikroTik devices and modules. MikroTik routers are widely used around the world across different industries. By using MikroTik routers as proxy servers for its C2 servers and redirecting the traffic through non-standard ports, Trickbot adds another persistence layer that helps malicious IPs evade detection by standard security systems.

The Microsoft Defender for IoT research team has recently discovered the exact method through which MikroTik devices are used in Trickbot's C2 infrastructure. In this blog, we will share our analysis of the said method and provide insights on how attackers gain access to MikroTik devices and use compromised IoT devices in Trickbot attacks.

This analysis has enabled us to develop a forensic tool to identify Trickbot-related compromise and other suspicious indicators on MikroTik devices. We published this tool to help customers ensure these IoT devices are not susceptible to these attacks. We're also sharing recommended steps for detection and remediating compromise if found, as well as general prevention steps to protect against future attacks.

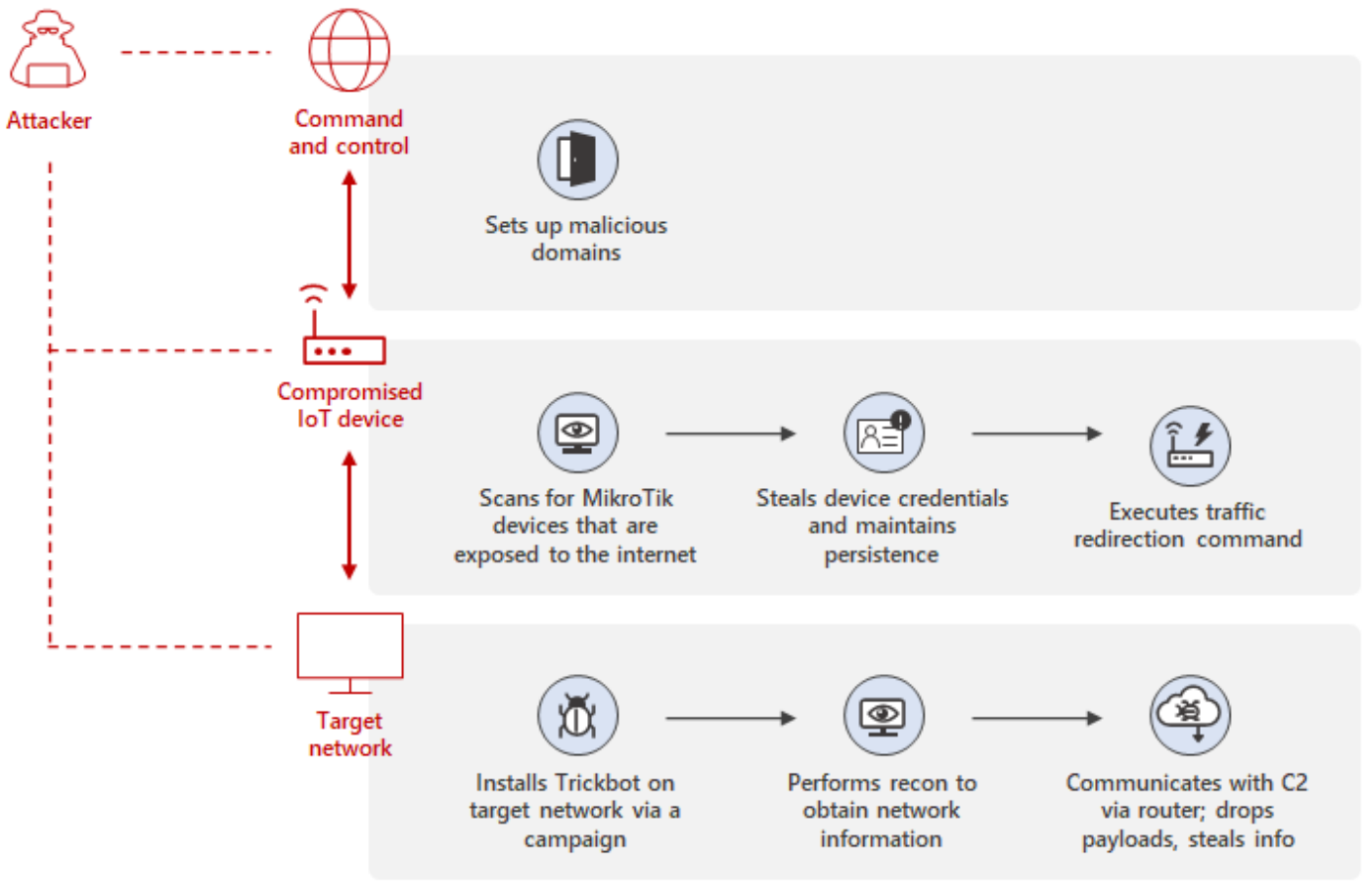

Figure 1. Trickbot attack diagram

How attackers compromise MikroTik devices for Trickbot C2

The purpose of Trickbot for using MikroTik devices is to create a line of communication between the Trickbot-affected device and the C2 server that standard defense systems in the network are not able to detect. The attackers begin by hacking into a MikroTik router. They do this by acquiring credentials using several methods, which we will discuss in detail in the following section.

The attackers then issue a unique command that redirects traffic between two ports in the router, establishing the line of communication between Trickbot-affected devices and the C2. MikroTik devices have unique hardware and software, RouterBOARD and RouterOS. This means that to run such a command, the attackers need expertise in RouterOS SSH shell commands. We uncovered this attacker method by tracking traffic containing these SSH shell commands.

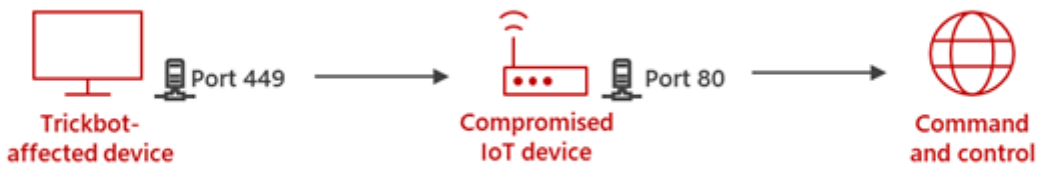

Figure 2. Direct line of communication between the Trickbot infected device and the Trickbot C2

Accessing the MikroTik device and maintaining access

Attackers first need to access the MikroTik shell to run the routing commands. To do so, they need to acquire credentials. As mentioned earlier, based on our analysis, there are several methods that attackers use to access a target router:

- Using default MikroTik passwords.
- Launching brute force attacks. We have seen attackers use some unique passwords that probably were harvested from other MikroTik devices.
- Exploiting CVE-2018-14847 on devices with RouterOS versions older than 6.42. This vulnerability gives the attacker the ability to read arbitrary files like user.dat, which contains passwords.

To maintain access, the attackers then change the affected router's password.

Redirecting traffic

MikroTik devices have a unique Linux-based OS called RouterOS with a unique SSH shell that can be accessed through SSH protocol using a restricted set of commands. These commands can be easily identified by the prefix "/". For example:

/ip /system /tool

These commands usually won't have any meaning on regular Linux-based shells and are solely intended for MikroTik devices. We observed through Microsoft threat data the use of these types of commands. Understanding that these are MikroTik-specific commands, we were able to track their source and intent. For example, we observed attackers issuing the following commands:

/ip firewall nat add chain=dstnat proto=tcp dst-port=449 to-port=80 action=dst-nat to-addresses=<infected device> dst-address=<real C2 address>

From the command, we can understand the following:

- A new rule, similar to iptables, is created
- The rule redirects traffic from the device to a server
- The redirected traffic is received from port 449 and redirected to port 80

The said command is a legitimate network address translation (NAT) command that allows the NAT router to perform IP address rewriting. In this case, it is being used for malicious activity. Trickbot is known for using ports 443 and 449, and we were able to verify that some target servers were identified as TrickBot C2 servers in the past.

This analysis highlights the importance of keeping IoT devices secure in today's ever evolving threat environment. Using Microsoft threat data, Microsoft's IoT and operational technology (OT) security experts established the exact methods that attackers use to leverage compromised IoT devices and gained knowledge that can help us better protect customers from threats.

Defending IoT devices against Trickbot attacks

As security solutions for conventional computing devices continue to evolve and improve, attackers will explore alternative ways to compromise target networks. Attack attempts against routers and other IoT devices are not new, and being unmanaged, they can easily be the weakest links in the network. Therefore, organizations should also consider these devices when implementing security policies and best practices.

An open-source tool for MikroTik forensics

While investigating MikroTik and attacks in the wild, we observed several methods of attacking these devices in addition to the method we described in this blog. We aggregated our knowledge of these methods and known CVEs into an open-source tool that can extract the forensic artifacts related to these attacks.

Some of this tool's functionalities include the following:

- Get the version of the device and map it to CVEs
- Check for scheduled tasks
- Look for traffic redirection rules (NAT and other rules)
- Look for DNS cache poisoning

- Look for default ports change
- Look for non-default users

We have published the tool in GitHub and are sharing this tool with the broader community to encourage better intelligence-sharing in the field of IoT security and to help build better protections against threat actors abusing IoT devices.

How to detect, remediate, and prevent infections

Organizations with potentially at-risk MikroTik devices can perform the following detection and remediation steps:

- Run the following command to detect if the NAT rule was applied to the device (completed by the tool as well):

/ip firewall nat print

If the following data exists, it might indicate infection:

chain=dstnat action=dst-nat to-addresses=<public IP address> to-ports=80 protocol=tcp dst-address=<your MikroTik IP> dst-port=449 chain=srcnat action=masquerade src-address=<your MikroTik IP>

- Run the following command to remove the potentially malicious NAT rule:

/ip firewall nat remove numbers=<rule number to remove>

To prevent future infections, perform the following steps:

- Change the default password to a strong one
- Block port 8291 from external access
- Change SSH port to something other than default (22)
- Make sure routers are up to date with the latest firmware and patches
- Use a secure virtual private network (VPN) service for remote access and restrict remote access to the router

Protect IoT devices and IT networks with Microsoft Defender

To harden IoT devices and IT networks against threats like Trickbot, organizations must implement solutions that detect malicious attempts to access devices and raises alerts on anomalous network behavior. Microsoft Defender for IoT provides agentless, network-layer security that lets organizations deploy continuous asset discovery, vulnerability management, and threat detection for IoT, OT devices, and Industrial Control Systems (ICS) on-premises or in Azure-connected environments. It is updated regularly with indicators of compromise (IoCs) from threat research like the one described on this blog, and rules to detect malicious activity.

Meanwhile, Microsoft 365 Defender protects against attacks related to highly modular, multi-stage malware like Trickbot by coordinating threat data across identities, endpoints, cloud apps, email, and documents. Such cross-domain visibility allows Microsoft 365 Defender to comprehensively detect and remediate Trickbot's end-to-end attack chain——from malicious attachments and links it sends via emails to its follow-on activities in endpoints. Its rich set of tools like advanced hunting also lets defenders surface threats and gain insights for hardening networks from compromise.

In addition, working with the Microsoft Defender for IoT Research Team, RiskIQ identified compromised MikroTik routers acting as communication channels for Trickbot C2 and created detection logic to flag devices under threat actor control. See RiskIQ's article.

To learn more about securing your IoT and OT devices, explore Microsoft Defender for IoT.

David Atch, Section 52 at Microsoft Defender for IoT Noa Frumovich, Section 52 at Microsoft Defender for IoT Ross Bevington, Microsoft Threat Intelligence Center (MSTIC)