The TrickBot and MikroTik Connection – A Story of Investment and Collaboration

By Wicus Ross

Published: 2018-12-12 · Archived: 2026-04-05 15:25:34 UTC

In my professional capacity I perform several tasks. One involves tracking and collecting indicators of compromise (IoC) used to identify malware campaigns. Another involves tracking incidents reported in mainstream media, establishing trends, and distilling the information into actionable items for clients and colleagues. The fun part of my job involves writing tools or playing with those authored by others.

This is a story where all these aspects neatly intersect. It's also a story which highlights the need for security companies to invest in their staff, and to encourage creativity to build a safer online environment for businesses and consumers.

Tracking TrickBot

Security companies across the globe track malware campaigns, including one named TrickBot. TrickBot monitors the web surfing activity of its victim, and activate when certain websites, such as internet banking, are accessed. It then attempts to capture account details of its victim when he or she browses to a login URL that is being monitored.

If we look at industry trends, this one is definitely a contender on the top ten offender list. Among the others are those which target unsecured IoT devices, subverting them into what is called a botnet – the likes of Mirai, Satori, VPNFilter, and Slingshot. The latter two have been linked to APT or nation state actors, Mirai and VPNFilter have been associated with distributed denial of service attacks, while Slingshot was reportedly used to pivot into internal networks. So, a pretty bad bunch!

We've noticed, in our own tracking of botnets, the increasing involvement of MikroTik devices, and also noted vulnerable MikroTik routers, through publicly disclosed vulnerabilities that were attributed to others. This, coupled with poor vulnerability management, has meant an increase in the number of compromised MikroTik hosts.

Where internal investment plays its part

On to the fun part. Our team takes a creative approach to cybersecurity and they're constantly expanding their capabilities, building tools not only because they have to, but out of curiosity.

Enter my esteemed colleague, Willem. A few weeks ago, Willem saw that Pastebin was running a lifetime Pro subscription promotion. Willem signed up, and a couple of hours later had created Pastebot, a Pastebin scraper that hooked into cloud-based collaboration platform, Slack. It was not long before Pastebot started spamming our SD Labs' Slack workspace with all kinds of nasties found on Pastebin.

Fast forward to one Monday morning just before lunch. I received a Slack message from Willem with a link to a Pastebin post that hosted XML config for a TrickBot campaign. This was picked up by Pastebot because Willem was looking for Pastebin posts that contain names of certain well-established financial institutions. This returned a TrickBot XML file containing 38 IP addresses and port pairs across the world.

Next, a quick spot check using Shodan, which provided us with a sense of what we were dealing with: several were associated with MikroTik routers. We verified this and the result was surprising. Of the 38 IPs, Shodan returned info on 37 hosts, 19 of which were identified as MikroTik routers. This suggests that either the routers or the hosts behind them had been compromised – or both.

One of the MikroTik routers reported the latest version of firmware which had been fully patched against known exploits. All the 19 MikroTik routers had their bandwidth test services exposed to the internet, and 18 had default SSH ports exposed to the internet.

Tools and tactics

We passed MikroTik router IPs through IOCParlor (a tool created by our team that helps automate IOC collection and verification) to get a sense of how naughty these hosts really are. IOCParlor queried VirusTotal and returned a list of 14 IPs flagged as malicious.

To verify the results, we picked one IP and manually reviewed it using the VirusTotal web client, which produced an MS Word document.

Of the 61 malware engines that scanned the document, 35 reported it as malicious. Several of the malware engines classified the document as a trojan downloader, meaning that when Word opens the file it will download malware.

The community tab associated with the VirusTotal report had several comments, including one from by dvk01 of My Online Security, a phishing and malware campaign reporting site that the SD Labs team regularly uses. dvk01 labelled the malware as TrickBot and links to an article that describes how the same contagion was used for a malicious Bank of America email.

In September 2018, there were reports in the industry that highlighted the increasing number of MikroTik routers that are ensnared in malicious activity. What was interesting was that TrickBot is using C2 hosts that have MikroTik routers involved.

Had the SD Labs not been tinkering with cybersecurity tools, this discovery may not have been made. Leveraging seemingly unrelated events and tying them together with other analysis demonstrates the need to not only examine obscure incidents across the industry, but also the kind of tactics needed to protect organizations against threats that could never have been imagined.

Continued investment in research and tooling is needed across industry, coupled with a creative approach and some outside-the-box thinking.
