Mēris botnet

blog.mikrotik.com/security/meris-botnet.html

15th Sep, 2021 | Security

In early September 2021 QRATOR labs published an article about a new wave of DDoS attacks, which are originating from a botnet involving MikroTik devices.

As far as we have seen, these attacks use the same routers that were compromised in 2018, when MikroTik RouterOS had a vulnerability, that was quickly patched.

There is no new vulnerability in RouterOS and there is no malware hiding inside the RouterOS filesystem even on the affected devices. The attacker is reconfiguring RouterOS devices for remote access, using commands and features of RouterOS itself.

Unfortunately, closing the old vulnerability does not immediately protect these routers. If somebody got your password in 2018, just an upgrade will not help. You must also change password, re-check your firewall if it does not allow remote access to unknown parties, and look for scripts that you did not create.

We have tried to reach all users of RouterOS about this, but many of them have never been in contact with MikroTik and are not actively monitoring their devices. We are working on other solutions too.

There are no new vulnerabilities in these devices. RouterOS has been recently independently audited by several third parties.

Best course of action:

- 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 (see below).

In collaboration with independent security researchers, we have found that there exists malware that attempts to reconfigure your MikroTik device from a Windows computer inside your network. This is why it's important to set a better password now (to avoid passwordless login or a dictionary attack by this malware) and to keep your MikroTik router upgraded (since this malware also attempts to exploit the mentioned CVE-2018-14847 vulnerabiliity which has long been fixed).

Configuration to look out for and remove:

- 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.

You can also work with your ISPs to **block** the following addresses, which these malicious scripts are connecting to:

Block these tunnel endpoint domains:

> *.eeongous.com
> *.leappoach.info
> *.mythtime.xyz

Block these script download domains:

- 1abcnews.xyz
- 1awesome.net
- 7standby.com
- audiomain.website
- bestony.club
- ciskotik.com
- cloudsond.me
- dartspeak.xyz
- fanmusic.xyz
- gamedate.xyz
- globalmoby.xyz
- hitsmoby.com
- massgames.space
- mobstore.xyz
- motinkon.com
- my1story.xyz
- myfrance.xyz
- phonemus.net
- portgame.website
- senourth.com
- sitestory.xyz
- spacewb.tech
- specialword.xyz
- spgames.site
- strtbiz.site
- takebad1.com
- tryphptoday.com
- wchampmuse.pw
- weirdgames.info
- widechanges.best
- zancetom.com

As reported by others on the internet, these domains are also used by the botnet:

- bestmade.xyz
- gamesone.xyz
- mobigifs.xyz
- myphotos.xyz
- onlinegt.xyz
- picsgifs.xyz

To blog