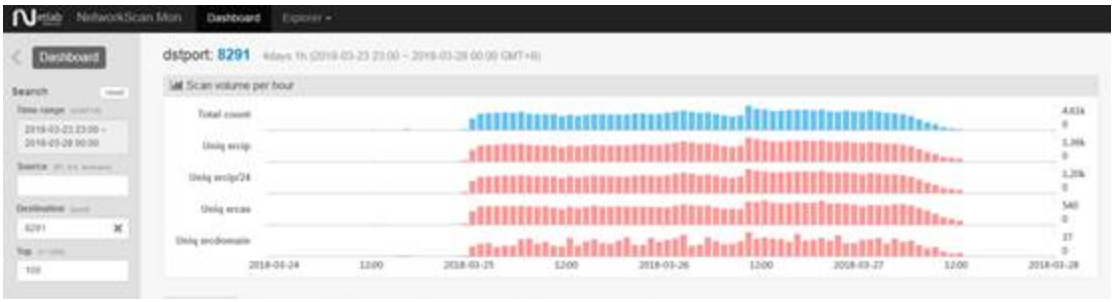
Quick summary about the Port 8291 scan

blog.netlab.360.com/quick-summary-port-8291-scan-en/

RootKiter March 28, 2018

28 March 2018 / Hajime



Summary

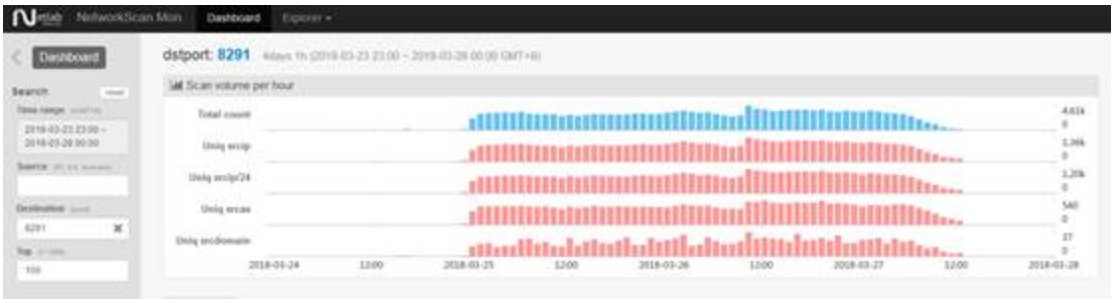
This 8291 scan event is caused by a Hajime botnet variant. Compared to the old Hajime, this one adds two new features:

1. Check port 8291 to determine if the target is a MikroTik device
2. Use 'Chimay Red' Stack Clash Remote Code Execution Loophole vulnerabilities to infect and spread.

For more details about the Hajime, please check our previous blog here

The sharp scan increase

At around 0:00 on March 25, Beijing time, our Scanmon system suggested a large number of scan activity is happening on port 8291 on a global scale.



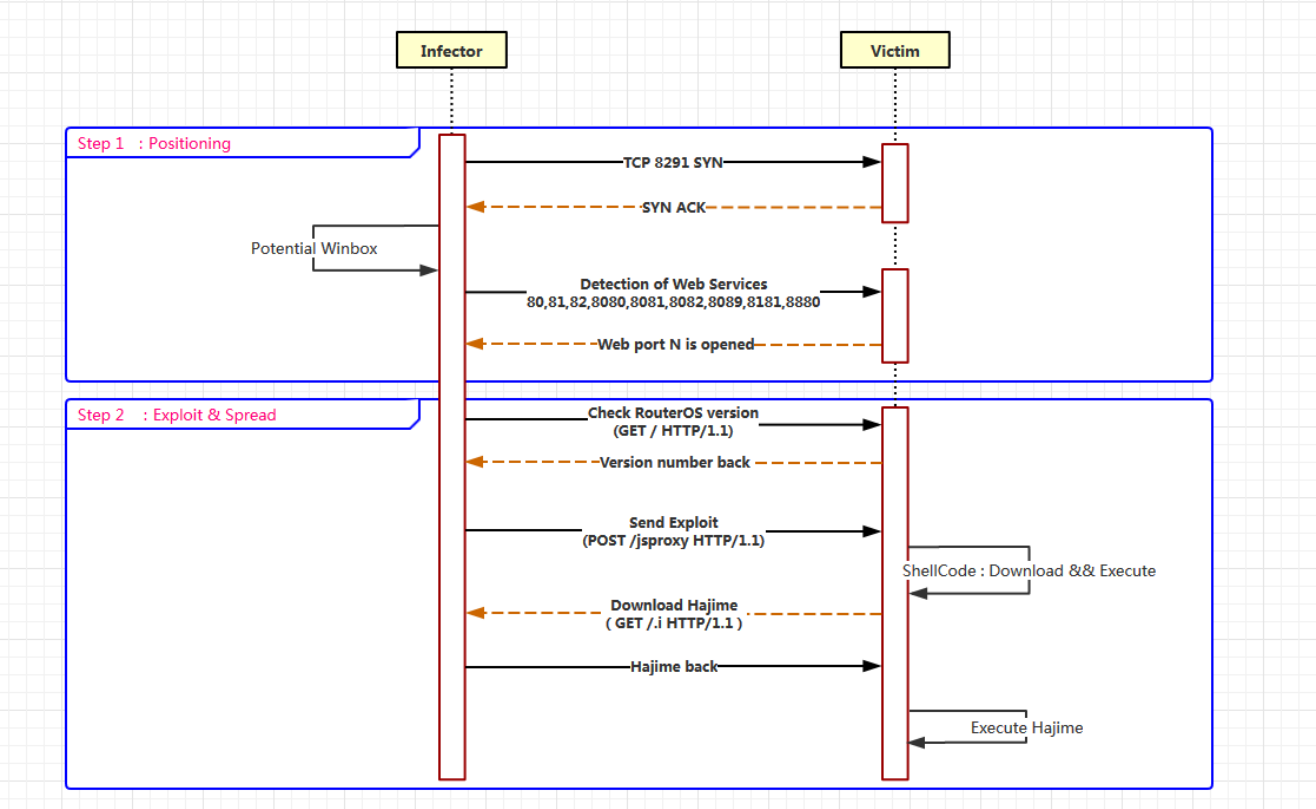
Around 2 pm, our honeypot data indicated this sudden spike was related to Hajime. Our preliminary conclusion based on its UPX_MAGIC_LE32 and some sample features confirmed that the sample is Hajime based. And we found the 'Chimay Red' Stack Clash Remote Code Execution" vulnerability related attack code in their atk module.

> https://www.exploit-db.com/exploits/44283/

Infection process

This Hajime variant adds a support of using "'Chimay Red' Stack Clash Remote Code "Execution" to perform worm-like spreading, and its propagation process is roughly divided into two steps:

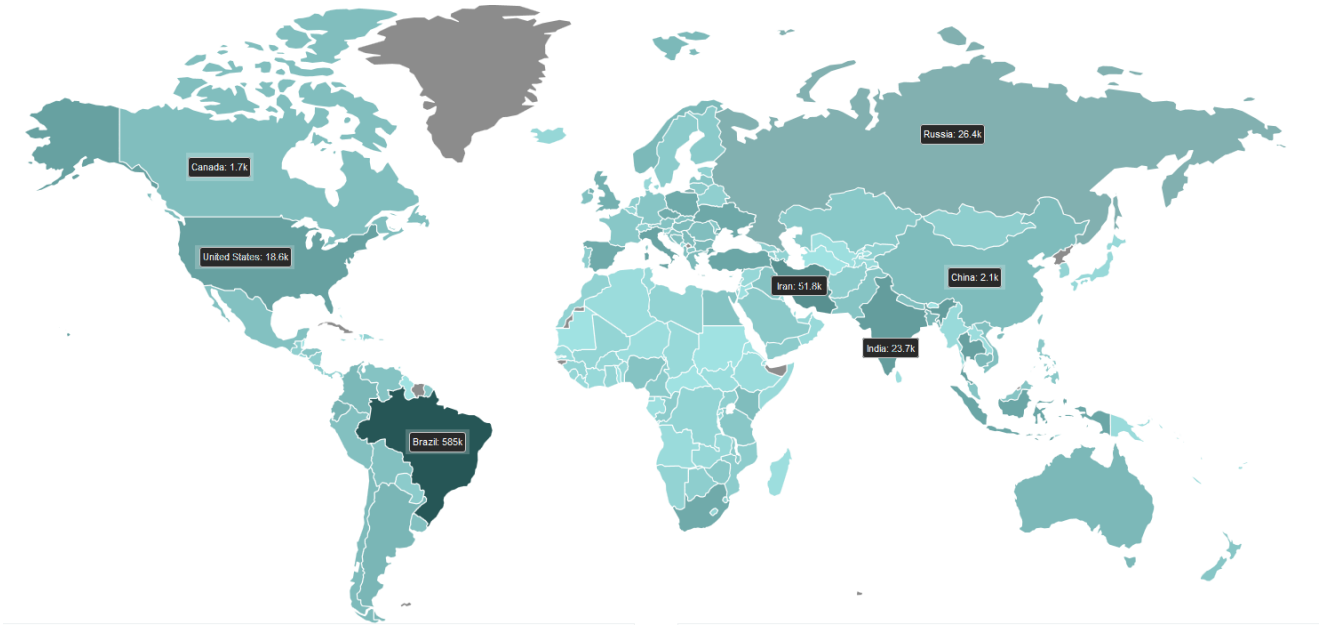
1. Find a MikroTik device by checking if the target port is open on port 8291, if this port is open,the other common web ports (80,81,82,8080,8081,8082,8089,8181,8880) will be probed next.
2. Check the version number of the device and send the Exploit which carried the Shellcode. Once the vulnerability is successfully exploited, Hajime will be downloaded and executed.



Number of unique ips

From 2018-03-25 00:00 to 2018-03-27 12:36(GMT+8), We logged a total of 861,131 unique scan source IPs (72 Hours).(Please bear in mind that device may change ip due to device reboot etc and it does not necessary mean all these devices are MikroTik devices as all the Hajime bots will perform this task as long as they have the most recent version of Hajime code running. Also naturally there will be some noises such as researcher ips in it)

Scan Source Distribution



From the above figure, it is not difficult to find the top three sources of the scan source are: Brazil (585k), Iran (51.8k), Russia (26.4k).

Mitigation

1. block unnecessary 8291 port request
2. Update to the latest version from MikroTik.

We will continue to monitor this activity, if readers have new discoveries, feel free to contact us on our twitter.

IOC

06B4D50254C6C112437A3ED893EF40B4 .i.mipseb
93A1A080FCDE07E512E7485C92861B69 atk.mipseb
fc834c015b357c687477cb9116531de7 atk.mipseb.upx.unpack

Refer