It Is Time For Some Router Maintenance

A little over a month ago the computer security firm Talos Intelligence revealed the existence of an advanced form of malware which infects routers, the device that everyone uses to connect their home network to the broader internet. They are calling this malware VPNFilter. This malware is quite sophisticated and bears some resemblance to pieces of the malware which was used to crash the Ukrainian electric grid in late 2015. It is believed that VPNFilter is connected to a nation-state or a nation-state affiliated group. Most major brands of routers have known infections:

- Asus
- D-Link
- Huawei
- Linksys
- MikroTik
- Netgear
- TP-Link
- Ubiquiti
- Upvel
- Qnap (NAS devices)
- ZTE

As you can see this list includes just about every popular make of router.

The design of this malware allows it to be dynamically configured by downloading modules as directed by a command and control server. So far some of the modules found allow a man-in-the middle attack to be used to monitor the contents of encrypted traffic, inject code into devices on the target network and even to destroy the device on which it is running. Talos characterizes is as a “workhorse intelligence-collection platform”.

The FBI has taken control of the network resources used to provide the initial instructions to the stage 1 malware, but it is important to reset or reboot your router to ensure that you are not infected by the stage 2 malware. You should also perform some additional maintenance to ensure that your router is a more difficult target in the future.

Remediation

There are several steps involved in securing your router beyond just rebooting it. They are:

- Change administrator (not the WiFi) password
- Turn off remote management, if supported
- Update to the latest firmware

I’m going to provide instructions on how to perform these tasks on a Netgear router, but other popular routers have similar features. If you are planning on doing a factory reset do that before performing any

of the following operations (note that a factory reset requires a button on the back of the router to be depressed using a paperclip).

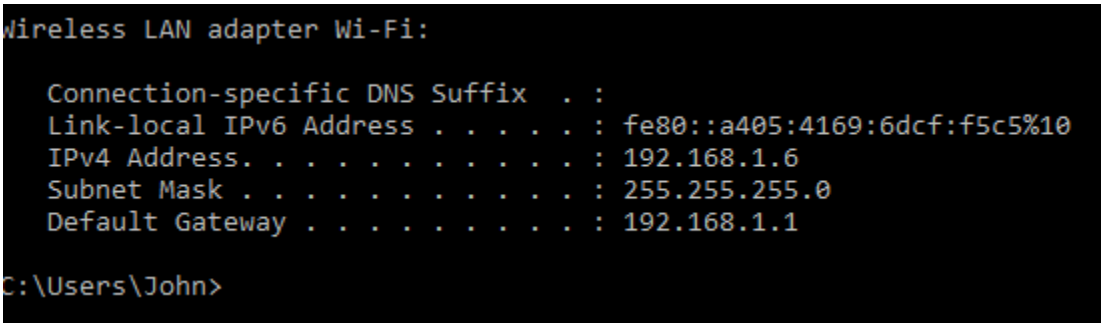
If You Perform a Factory Reset

A factory (paperclip) reset will erase any changes you have made to the router configuration. In particular if you have created any address reservations or changed the DNS server these changes will be lost. It is a good idea to copy your address reservations, if any, down so that you can reenter them once the router has finished its reset process.

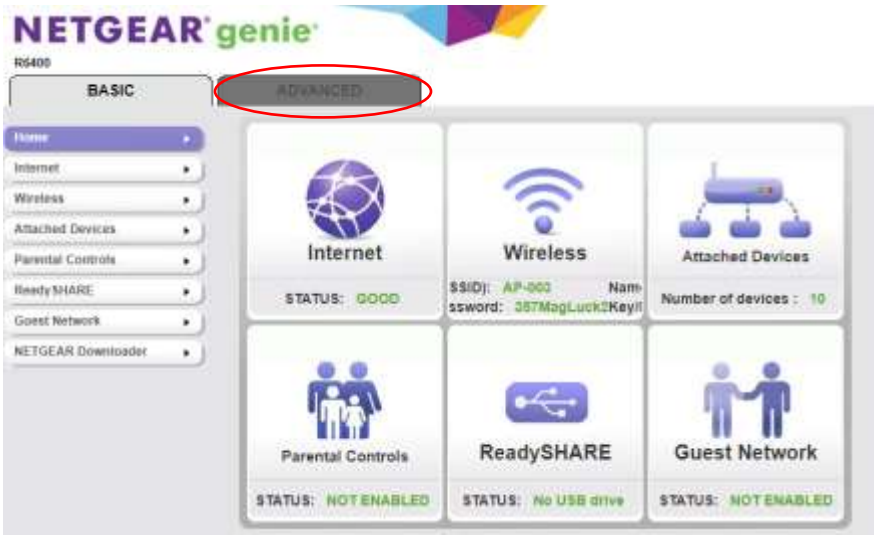
Log In To Your Router

Before you can do anything else, you need to log in to your router's administrative interface. This is reached through your web browser. The first thing you need to do is figure out your router's IP address if you do not know it already. On a PC this is most easily done by opening a command prompt. On Windows 10, you can right click on the Windows icon on the toolbar and select "Command Prompt". On Windows 7 open the start menu, select "Run…" and type "cmd" into the text box.

Once you have a command prompt, type "ipconfig" to display some basic information about your network configuration. You are looking for the section which looks like this:



The address of your router is the address of the Default Gateway, in this case 192.168.1.1. Enter this into the address bar of your browser. You should see a page which looks like this (for a Netgear router):



If you did a factory reset, or you have never logged into your router you can find out what the default username and password are by doing a simple Google search for "<your brand> <your model> default password". For example, I would search for "netgear r6400 default password" and find out that the username is admin and the password is password. Since all the following operations fall under the advanced category, click on the advanced tab circled in the above illustration.

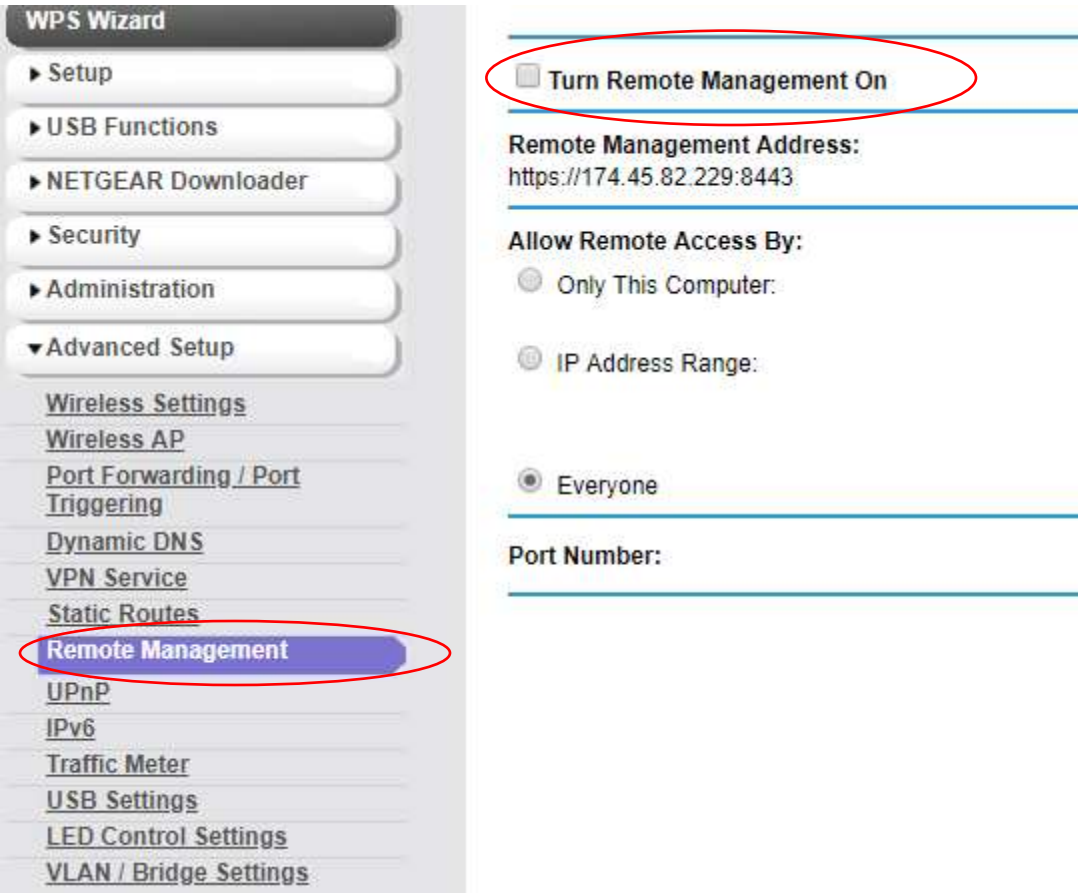
Change Administrative Password

If you have never changed your administrative password, now is a good time to do so. Click on the Administration tab in the sidebar, and then click on "Set Password".

This will take you to a page where you can change your password. Do it, "password" is not a very secure password.

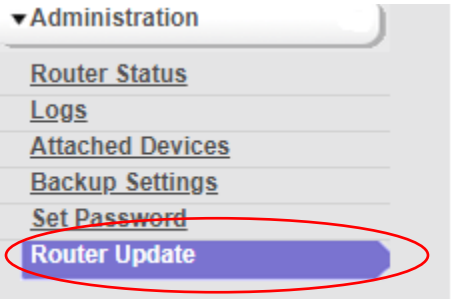
Disable Remote Management

If your router supports remote management, this should be disabled. To do this click on the "Advanced Setup" tab and then click on "Remote Management". Make sure the "Turn Remote Management On" checkbox is *not* checked and then click the green "Apply" button at the top of the page.



Update Your Router Firmware

Strangely enough, most routers do not automatically check for new releases of the firmware. You should make it a habit to log in to your router every few months and check for a new release of the firmware and install it. If you go for a while without seeing an update, it probably means that your router is no longer being supported by the manufacturer and should probably be replaced. On Netgear routers, click on the Administration tab and then click on the "Router Update" item:



Click on the purple "Check" button at the upper right-hand side of the page to check for a new version of the firmware. If a new version is available, you should update to it. This takes several minutes, during which the internet will not be available, so you should check with any other users in your house or office before updating.

The most recent update to Netgear routers now includes a feature to automatically update when a new version of the firmware becomes available. You should enable this feature so that you get security updates as soon as they are available.

Summary

Although the instructions provided in this document describe how to perform the required operations on Netgear routers, most routers have similar interfaces and features. Performing these operations is necessary to ensure that your router remains secure and that no harm can come to your home network. As always keeping your device up-to-date and using secure passwords is important.

If you wish to know all the bloody details of this new form of malware, you can find them here:

https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html