THE glitch guys

From time to time we will have a section here called the ***"Glitch Corner"*** to help our customers with various topics geared around computers.

This month's topic is Russian Router Hack

You will notice that a lot of my articles are about routers. This is because they are the first line of defense to your home or business network. These little boxes often times with little rabbit ear antennas keep out the bad guys, most of the time.

Though most of the brands out there are reasonably equal in quality and performance I find that the Netgear models give the features most often required by users that don't want to be bothered by this device. First since they were victims of massive hacks a few years ago because they used password as the login password. (Note: this login password is not the same as your wireless password, it is to program the device)

1. Current models force you to change this when you are setting up the new devices.

2. Once you are on the internet the wireless section comes pre-secured with a network name usually NetgearXX (2 numbers just in case you have close neighbors with the same brand) and a wireless password / WPA2 key that consists of two unrelated words like happyriverXXX (folloed by 3 numbers). This comes on a removable stick on the face of the product as well as one on the back. This is extremely helpful in case your *computer genius* decides to "paper clip" or reset and erase all of your settings, it will at least go back to the defaults when you purchased it.

3. Once logged in the unit looks for the latest firmware to make sure your router has the most updated security features. Unfortunately this is often overlooked and never looked at again during the life of the router. The updates are somewhat ambiguous because they can't tell the bad guys all of the fixes, because there are many more out there that are not getting patched.

I have been saying this issue has been around for more than 10 years and the ZDNET article below confirms this. Doing the 3 steps outlined above will give you as much trouble free use of the product for years to come. While I am on the subject of "years", if your router is older than 5 years old, it would be time to get a new one. So much has changed with streaming video, gaming, IoT and others that an older router was not made to handle. You don't have to spend a fortune, a Netgear AC-1200 sells at Walmart for under $60 and Netgear AC-1750 around $100. These are both fine consumer level routers. Spending more does not make the WiFi distance go any further. Running a wire to your devices or placing the router in the center of your usage area is the best idea. If that is not possible there are devices called network extenders, repeaters, and even mesh networks that use a multiple antenna approach to blanket your home with WiFi signal.

Below is the article from ZDNET May 26, 2018:

US JUSTICE DEPARTMENT ANNOUNCES ACTION

The United States Justice Department shortly after announced seizing a domain used in the botnet campaign.

Attributing VPNFilter to Sofacy Group, also known as apt28, sandworm, x-agent, pawn storm, fancy bear, and sednit, DoJ said the group has been operating since at least 2007, targeting government, military, security organisations, and other targets of perceived intelligence value.

"The Department of Justice is committed to disrupting, not just watching, national security cyber threats using every tool at our disposal, and today's effort is another example of our commitment to do that," said Assistant Attorney General Demers.

"This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities."

DEFENDING AGAINST VPNFILTER

Due to the nature of the affected devices, with the majority connected directly to the internet with no security devices or services in place, compounded by the fact that most of the affected devices already have publicly known vulnerabilities not patched by the average user with no built-in anti-malware capabilities, Talos said defending against VPNFilter is extremely difficult.

"The destructive capability particularly concerns us. This shows that the actor is willing to burn users' devices to cover up their tracks, going much further than simply removing traces of the malware," the researchers wrote.

"If it suited their goals, this command could be executed on a broad scale, potentially rendering hundreds of thousands of devices unusable, disabling internet access for hundreds of thousands of victims worldwide or in a focused region where it suited the actor's purposes."

Talos has also developed and deployed more than 100 Snort signatures for the publicly known vulnerabilities for the potentially affected devices.

The researchers recommend users of small and home office-grade routers and NAS devices reset them to factory defaults and reboot them in order to remove the stage 2 and stage 3 malware, and reach out to device manufacturers to ensure up-to-date patching.

End of article

If all this seems too much to bother with, we offer professional setup of your new computer and data transfer and copying to that new unit as well as the above mentioned steps, at very reasonable pricing.

G^2