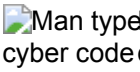
You have absolutely, positively been hacked. FBI warns Russians hacked hundreds of thousands of routers

Reuters **By Joseph Menn and Sarah N. Lynch**

Reuters



FILE PHOTO: A keyboard is displayed in front of the cyber code displayed on this illustration picture taken on March 1, 2017. REUTERS/Kacper Pempel/Illustration

More

By Joseph Menn and Sarah N. Lynch

(Reuters) - The FBI warned on Friday that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic.

The U.S. law enforcement agency urged the owners of many brands of routers to turn them off and on again and download updates from the manufacturer to protect themselves.

The warning followed a court order Wednesday that allowed the FBI to seize a website that the hackers planned to use to give instructions to the routers. Though that cut off malicious communications, it still left the routers infected, and Friday's warning was aimed at cleaning up those machines.

Infections were detected in more than 50 countries, though the primary target for further actions was probably Ukraine, the site of

many recent infections and a longtime cyberwarfare battleground.

In obtaining the court order, the Justice Department said the hackers involved were in a group called Sofacy that answered to the Russian government.

Sofacy, also known as APT28 and Fancy Bear, has been blamed for many of the most dramatic Russian hacks, including that of the Democratic National Committee during the 2016 U.S. presidential campaign.

Earlier, Cisco Systems Inc said the hacking campaign targeted devices from Belkin International's Linksys, MikroTik, Netgear Inc, TP-Link and QNAP.

An FBI official told Reuters that the kinds of devices known to be affected by the hack were purchased by users at electronic stores or online.

However, the FBI was not ruling out the possibility that routers provided to customers by internet service companies could also be affected, the official added.

Cisco shared the technical details of its investigation with the U.S. and Ukrainian governments. Western experts say Russia has conducted a series of attacks against companies in Ukraine for more than a year amid armed hostilities between the two countries, causing hundreds of millions of dollars in damages and at least one electricity blackout.

The Kremlin on Thursday denied the Ukrainian government's accusation that Russia was planning a cyber attack on Ukrainian

state bodies and private companies ahead of the Champions League soccer final in Kiev on Saturday.

"The size and scope of the infrastructure by VPNFilter malware is significant," the FBI said, adding that it is capable of rendering peoples' routers "inoperable."

It said the malware is hard to detect, due to encryption and other tactics.

The FBI urged people to reboot their devices to temporarily disrupt the malware and help identify infected devices.

People should also consider disabling remote-management settings, changing passwords and upgrading to the latest firmware.

(Reporting by Sarah N. Lynch in Washington and Joseph Menn in San Francisco; Editing by David Gregorio)