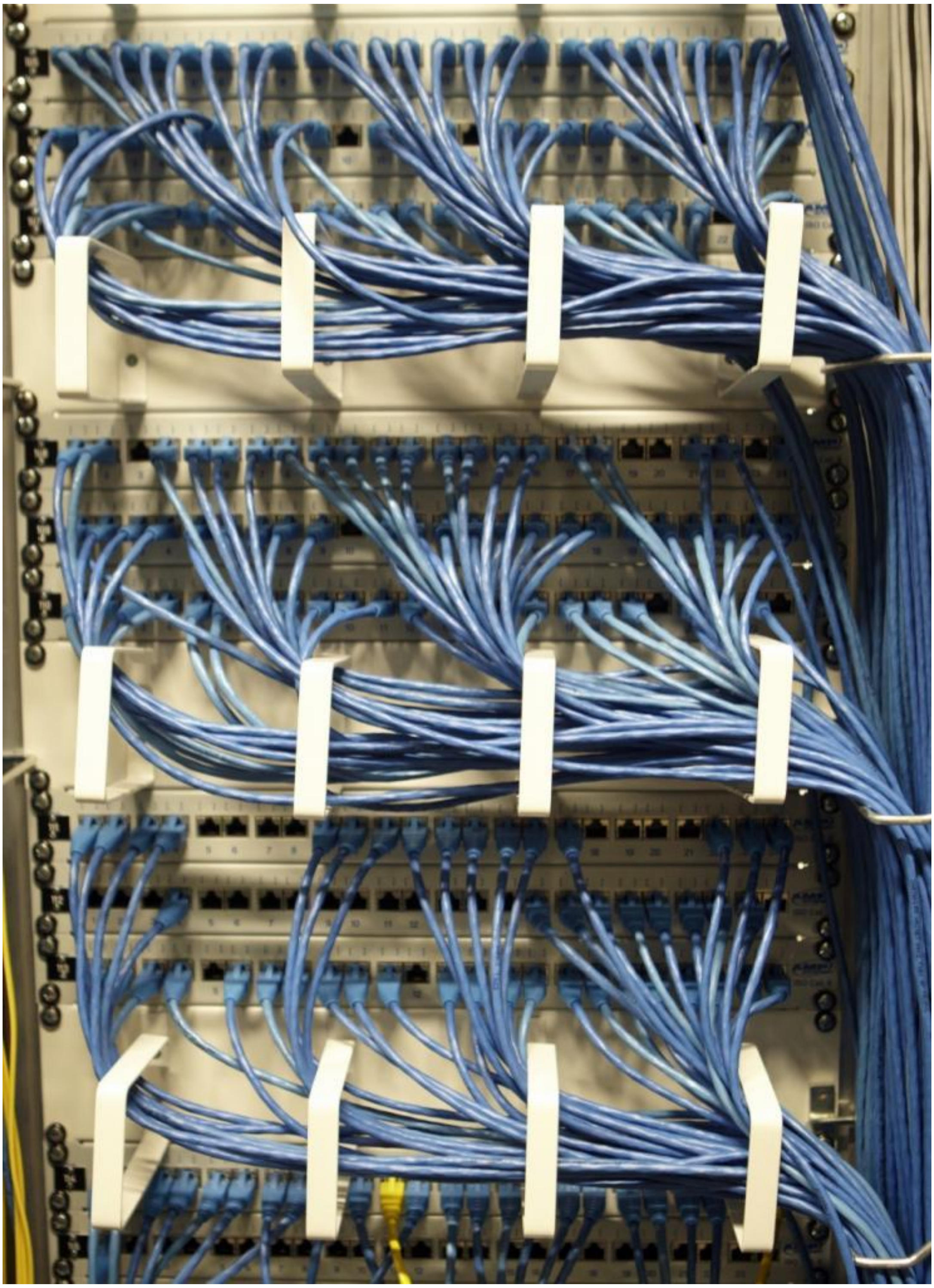
Router Hack Creates 'Ultimate Listening Device' To Monitor a Country's Entire Internet Traffic

By David Gilbert @daithaigilbert d.gilbert@ibtimes.com on September 15 2015 12:59 PM EDT



A flaw in router security and the architecture of the Internet allows attacks to monitor, reroute and copy the Internet traffic of an entire country - Reuters

LONDON - Malicious software that can infect the hardware that comprises much of the core architecture of the Internet has allowed hackers to create what has been dubbed the "ultimate listening device."

The software, the origin of which is not publicly known, targets routers, which control the flow of traffic on the Internet. The hack, which replaces the routers' native operating system, lets attackers silently monitor, reroute and copy all online communications passing through that device.

Dubbed Synful Knock by the researchers at Mandiant, who revealed the situation Tuesday**,** it has so far been shown to be exploited in the wild only on Cisco Systems Inc. routers in four countries -- Mexico, Ukraine, Phillipines, and India.

"We have only been able to prove its existence in the wild for actual attacks on Cisco routers, but we actually believe that Huawei routers or Juniper routers have the same vulnerabilities and ultimately can be exploited in a similar way. The mass of the router architecture of the world is at risk," Dave DeWalt, the CEO of security company FireEye Inc. which owns Mandiant, told International Business Times.

The vulnerability relates to a router implant, which DeWalt describes as "a rewrite of an operating system for a router" and is one which was until now only known to exist as a theoretical flaw, and has never before been seen in the wild. This new attack vector is so hard to identify that it allows hackers to remain undetected on networks. It's believed the hackers accessed the routers through stolen passwords or credentials. Cisco in August alerted customers to the problem.

While most exploits typically attack the core systems of a network -- meaning they have breached a firewall, PC or mobile device -- by attacking routers those groups exploiting this vulnerability are attacking the edge of the network. "There is no amount of security spending in the world that could have found this or could have resolved this. All the security products and capabilities are focused inside the perimeter of an organization," DeWalt said.

The Ultimate Listening Device

While most people will be aware of routers as the devices which sit in the corner of their living rooms and connect them to the Internet, on a much larger scale they are used as the backbone for online communications around the world -- and this is why Synful Knock is so powerful:

"The vulnerability is the gateway to entire countries' infrastructure. The targets could be just about any company, any entity in that infrastructure. It is the ultimate listening device," DeWalt said.

Neither Mandiant or DeWalt would speculate on the specific identity of the attackers, but due to the hugely sophisticated nature of the attacks DeWalt believes that only nation states with deep resources and technical knowledge are capable of carrying them out. DeWalt added that multiple countries are actively using this exploit to spy on other nations and that this could exist in a lot more locations and a lot more countries.

Mr. David G. Dewalt | FindTheCompany

Playing With The Brain Of The Internet

In order to exploit this security flaw, the attackers would need to implant a new operating system without taking the router offline, which is a highly difficult task.

You are playing with the brain of the internet, and if you make a mistake you could bring down the internet infrastructure of the world," DeWalt said.

We Need To ReBoot the Internet

Because the issue is partly down to the way the Internet is built, fixing the problem is going to be all but impossible, according to FireEye's CEO:

"We need an Internet reboot. We need to re-image the operating systems of the routers in the world. We have to reset the encryption capabilities on the routers. And we have to reset the passcodes and authentication of all the routers -- and of course doing that is a pretty mammoth task."

In February, Kaspersky Lab published research into one of the most sophisticated cyber-espionage groups in the world, known as the Equation Group and linked to the U.S. government, revealing the use of a malicious implant which rewrote the firmware of a computer's hard drive in order to avoid detection and, like Synful Knock, persists on the infected device.

DeWalt said that these examples show that the "implants into core components of technology we take for granted -- things like disc drives or routers -- is emblematic of the cyber arms race we are seeing in the world today among nation states, all trying to gain an advantage on one another."

U.S. President Barack Obama and Chinese President Xi Jinping shake hands after their joint news conference in Beijing in November 2014. Cyberwarfare claims are an increasing problem between the two countries. Reuters/Kevin Lamarque

As the cyber-arms race accelerates, tools like Synful Knock will become increasingly powerful as countries look to gain an advantage over each other, and while some of the shock of learning about the capabilities of these tools has been muted since Edward Snowden's revelations, the fact that multiple nations are using this exploit to spy on other countries will be hugely worrying for all governments and citizens.

Next week U.S. President Barack Obama will meet Chinese President Xi Jinping and the White House has said it will raise concerns about the increase in Chinese hacking of U.S. government networks and those of U.S. industries.

Visit the ASP Website: http://www.advancedsecurityprotection.com/services/technical-surveillance-countermeasures-tscm-debugging