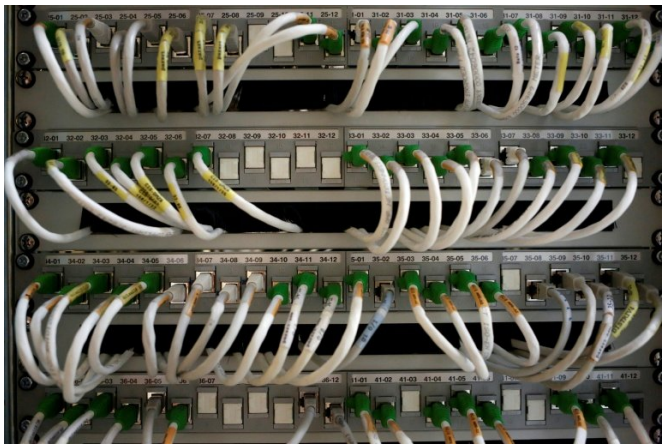
US disrupts Russian botnet of 500,000 hacked routers

24 May 2018, by Paul Handley



US Justice Department seizes "VPNFilter" botnet set up by a hacking group variously called APT28, Pawn Storm, Sandworm, Fancy Bear and the Sofacy Group

The US Justice Department said Wednesday that it had seized an internet domain that directed a dangerous botnet of a half-million infected home and office network routers, controlled by hackers believed tied to Russian intelligence.

The move was aimed at breaking up an operation deeply embedded in small and medium-sized computer networks that could allow the hackers to take control of computers as well as easily steal data.

The Justice Department said the "VPNFilter" botnet was set up by a hacking group variously called APT28, Pawn Storm, Sandworm, Fancy Bear and the Sofacy Group.

The group is blamed for cyber attacks on numerous governments, key infrastructure industries like power grids, the Organization for Security and Co-operation in Europe, the World Anti-Doping Agency, and other bodies.

US intelligence agencies also say it was involved in the operation to hack and release damaging information on the Democratic Party during the 2016 US presidential election, and has engineered a number of computer network disruptions in Ukraine.

"According to cybersecurity researchers, the Sofacy Group is a cyber-espionage group believed to have originated from Russia," the Department of Justice said in a court filing.

"Likely operating since 2007, the group is known to typically target government, military, security organizations, and other targets of intelligence value, through a variety of means," it said.

The Justice filing did not say who was behind Sofacy Group, but US intelligence has in the past linked it to Russia's GRU military intelligence agency, and numerous private computer security groups have made the same connection.

In Wednesday's action, the Justice Department said it had obtained a warrant authorizing the FBI to seize a computer domain that is part of the command and control system of the VPNFilter botnet.

The botnet targets home and office routers, through which it can relay orders from the botnet's controllers and intercept and reroute traffic back to them, virtually undetected by the users of a network.

In a report released in parallel to the Justice announcement, network equipment giant Cisco said VPNFilter had infected at least 500,000 devices in at least 54 countries.

It has targeted popular router brands like Linksys, MikroTik, NETGEAR and TP-Link.

"The behavior of this malware on networking

equipment is particularly concerning, as components of the VPNFilter malware allows for theft of website credentials," Cisco said.

It also has "a destructive capacity that can render an infected device unusable, which can be triggered on individual victim machines or en masse."

Both Justice and Cisco said they were releasing details of the problem before having found a strong, permanent fix. Justice said that by seizing control of one of the domains involved in running VNPFilter, it will give owners of infected routers a chance to reboot them, forcing them to begin communicating with the now-neutralized command domain.

The vulnerability will remain, Justice said, but the move will allow them more time to identify and intervene in other parts of the network.