



# 500,000 home and small-office routers hacked — and could be used to attack others

It has infected half-a million routers in homes and businesses around the world, and that malware is vicious enough to destroy the devices with a single command.

Following an announcement from Cisco on Wednesday, the malware can intercept communications and launch attacks on others.

The details of the attack are concerning, Cisco said. It is not known how many in the U.S. have been attacked. The announcement says the Ukraine is among the hardest hit regions so far.

Working with our partners, we estimate the number of infected devices to be around 500,000 in at least 54 countries. The known devices affected by the malware are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well as QNAP network-attached storage (NAS) devices. No other vendors, including Cisco, have been observed as infected by VPNFilter, but our research continues."

The malware can steal website credentials and perform destructive cyber attacks, the announcement states.

The malware can also be leveraged to collect data that flows through the network. "This could be for straightforward data-collection purposes, or to exploit the potential value of the network that the device serves," the announcement says. "If the network was deemed as having information of interest to the threat actor, they may choose to continue collecting that passes through the device or to propagate into the connected devices for data collection."