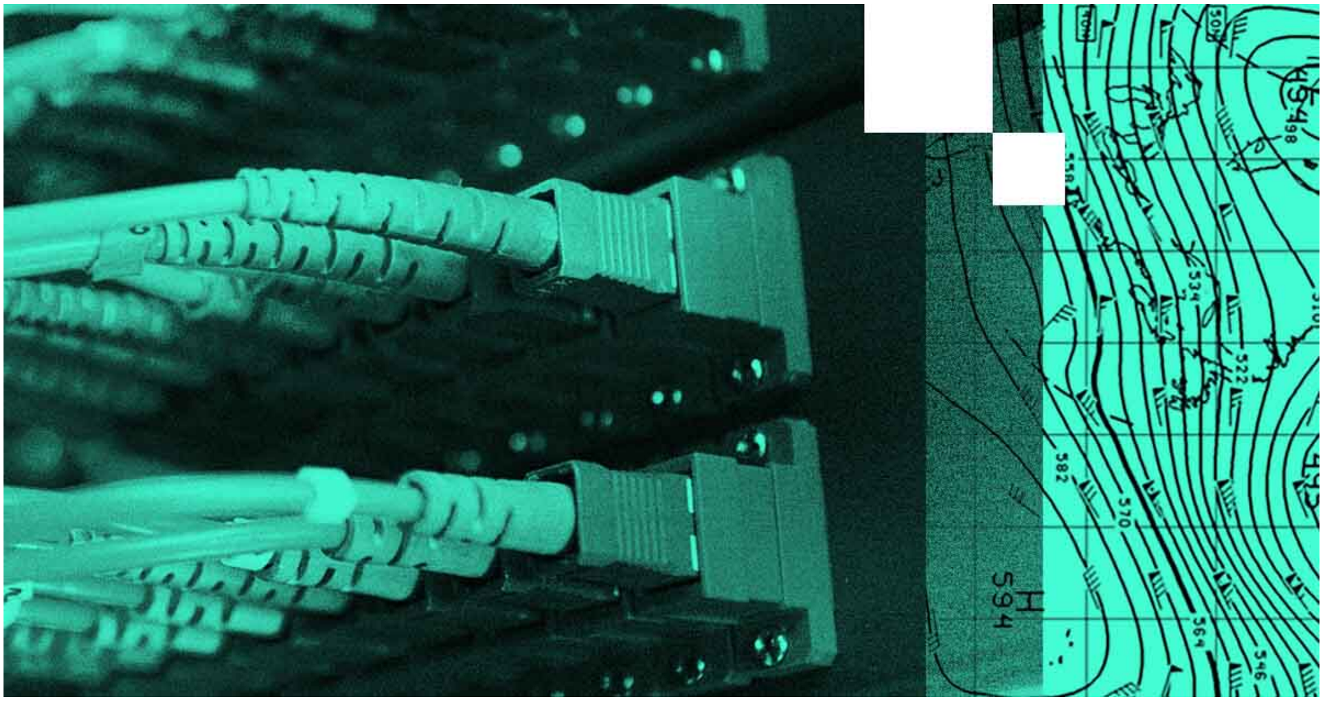
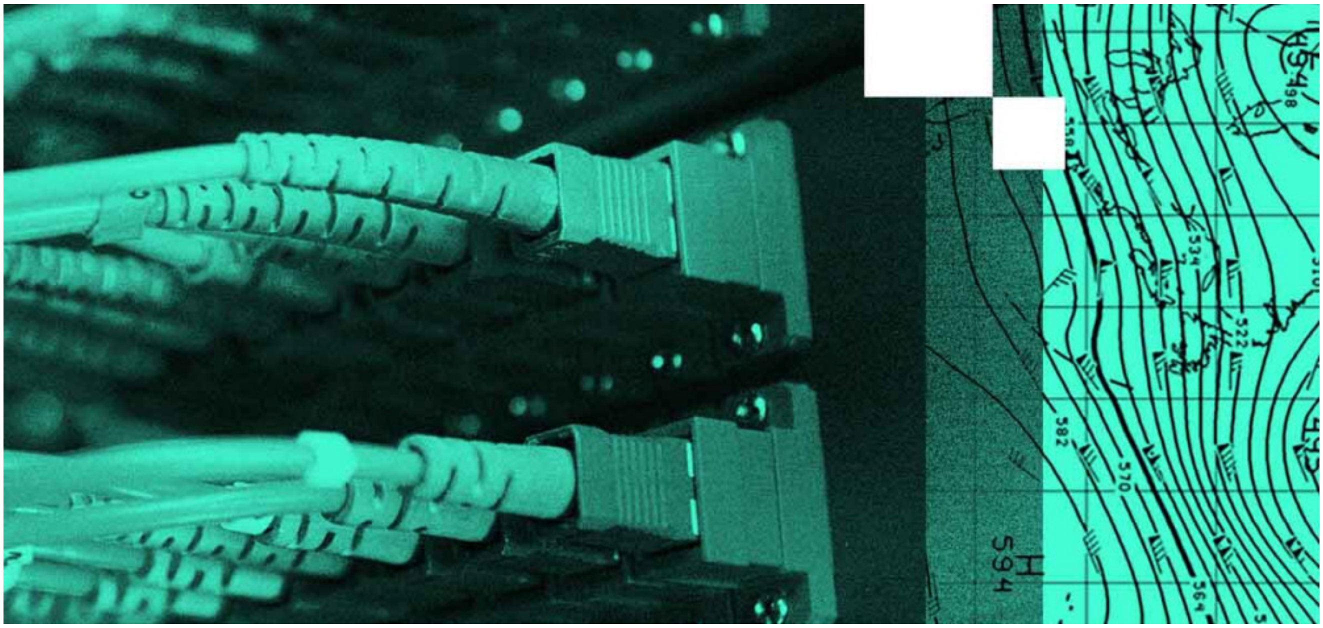
Trickbot Up to Its Old Tricks

duo.com/decipher/trickbot-up-to-its-old-tricks



SEARCH



Oct 16, 2020 By Dennis Fisher

Just a few days after Microsoft and a coalition of security firms took action against the infrastructure used by the Trickbot malware operators, taking control of command-and-control servers and locking down the malicious content on them, the botnet has bounced back and is humming right along with new C2 servers in several European and South American countries.

On Monday, Microsoft announced a coordinated takedown operation aimed at disrupting the Trickbot botnet, a global malware distribution and operation network that has been operating since at least 2016. The takedown involved Microsoft obtaining court orders to seize control of some Trickbot C2 servers based in the United States and also filing a copyright infringement claim against the operators for misusing Microsoft's software. The operation follows a familiar road map that security companies and law enforcement agencies have used to target botnets for more than a decade, targeting the C2 infrastructure to cut off communications between infected machines and the Trickbot operators.

This method has worked well in some cases, but cybercrime groups have paid attention and taken steps to ensure that their infrastructure is resilient and can survive a takedown attempt. In the case of Trickbot, the operators have already set up a new fleet of C2 servers outside the U.S., many of them in Germany, and others in the Netherlands, Colombia, Russia, and Indonesia. These are the first layer of command servers that infected machines reach out to, with other layers of control behind them. Unlike other botnets that use virtual private servers on bulletproof hosting services for C2, the current crop of Trickbot control servers are housed on compromised MikroTik consumer routers.

"It was a very well set up network and geographically distributed to make it hard to take down. Microsoft's action only affected the servers in the U.S., and it didn't surprise me at all to see new control servers pop up this quickly," said Mark Arena, CEO of Intel 471, a security firm that tracks Trickbot activity closely.

"They've learned from previous takedowns because Microsoft and others have used these tactics before."

The Trickbot malware is often associated with the Emotet loader and recently, the Ryuk ransomware. The operators of Trickbot sell access to infected machines to other cybercrime groups, especially high-level groups that have established reputations in the cybercrime underground. Those sales are not just limited to underground groups, however. This past summer, Intel 471 published research demonstrating a link between Trickbot and an attack group known as Lazarus that is tied to the North Korean government. In the linked operations, it appears that the Trickbot group sold access to compromised machines and networks to DPRK actors, who then used that access for their own purposes.

"TrickBot certainly appears to be a source of compromised accesses that DPRK threat actors can leverage. The operators or users of TrickBot seem to be well-versed in identifying interesting organizations they've compromised for follow-up intrusion activity, be it through Anchor or common intrusion tools (Metasploit, Cobalt Strike, BloodHound, Empire, etc.), or to pass off or sell to other threat actors, i.e., DPRK threat actors," the research report says.

Within a few days of the Microsoft takedown operation this week, researchers observed the Emotet botnet, which sends malicious spam, delivering new spam templates to infected machines. Those templates included malicious documents that eventually loaded the Emotet trojan, which then contacted a C2 server to download and run Trickbot. Business as usual. But that doesn't mean the actions by Microsoft and the U.S. Cyber Command, which reportedly has been running its own effort to disrupt Trickbot, were futile.

“From a company perspective, it's hard for this to be effective unless you're willing to go on the offensive like Cyber Command,” Arena said. “But it's good for the U.S. to be seen as a hard target for these groups.”

Botnet Malware