It’s hard to keep a big botnet down: TrickBot sputters back toward full health

By Tim Starks

Published: 2020-11-30 · Archived: 2026-04-05 20:04:21 UTC

Mounting evidence suggests that TrickBot, the vast botnet that both U.S. Cyber Command and a Microsoft-led coalition sought to disable around the 2020 elections, is on the mend and evolving.

The separate campaigns featured Microsoft going to court to disable IP addresses associated with TrickBot command and control servers, as Cyber Command’s operation also targeted command and control servers.

Hints of its rebound began in late October, shortly after signs of success in the bids to dismantle the TrickBot network of zombie computers. While Cyber Command and Microsoft always billed their assaults as a disruption rather than a full takedown, the TrickBot comeback is proof that it’s difficult to kill a botnet outright.

Botnets are dangerous because they can be used to conduct a range of harmful activities, like distributed denial of service attacks that overwhelm a site with traffic or ransomware attacks, the latter of which were a major issue of concern for U.S. national security officials going into Election Day.

Several security researchers saw a new version of the TrickBot malware, its 100th, appear shortly after the election — for which Cyber Command and Microsoft feared TrickBot could cause trouble. The latest iteration came with new ways to hide its activity, among other features.

“We believe that this shows a determination on the part of the actors behind Trickbot to defy the disruption activity against their operation,” Mark Arena, CEO of Intel 471, said via email.

Huntress Labs published an analysis of the new obfuscation scheme last week. It’s simple, but clever, said John Hammond, senior security researcher.

“It’s using and taking advantage of the Microsoft Windows command prompt and the scripting language that that inherently uses,” Hammond said. “That is native and built into Windows, so just about every work station computer, and it doesn’t need any external compiler or some other sort of code or language to build that and be able to execute that on the system. It does that automatically.”

Many organizations saw TrickBot begin to again gain momentum not long after Microsoft published its first update on a disruption campaign. That campaign initially drew skeptical responses, but later won over some converts.

SentinelOne’s vice president of research, Brian Hussey, said he asked his team to look at TrickBot activity over the past year.

"The findings were pretty interesting, in that we've seen a continual and steady usage for the last year. No real spikes, but a slight dip in late October that lasted around a week," Hussey said. "November has not shown a major spike as they worked to come back online, rather just a continual level that we've seen for the entire year. From our telemetry it appears to be business as usual."

ESET, which was involved in the Microsoft disruption, said last week that TrickBot remained "weakened" by the effort in a chart that tracked number of detections. Yet also last week, the Any.Run malware analysis service portrayed TrickBot as "coming back on track."

It might be the case, then, that it's too early to conclusively assess how TrickBot is faring, even if the evidence points toward a rebound of some kind. "I'm sure, as more time goes by we'll get a better look at 'post-takedown activity and better view of any impact," Hussey said via email.

It is possible to fully destroy a botnet, as the case of 3ve shows. 3ve began operation in 2013, and ended in 2018 when a joint operation between government agencies and technology companies including Google brought it down. But in the case of TrickBot, as Bitdefender put it, "the endeavor proved to be more like a 'kneecapping' operation rather than cutting the hydra's heads."

Corrected, *11/30/20: Corrected for misnaming of John Hammond.*
