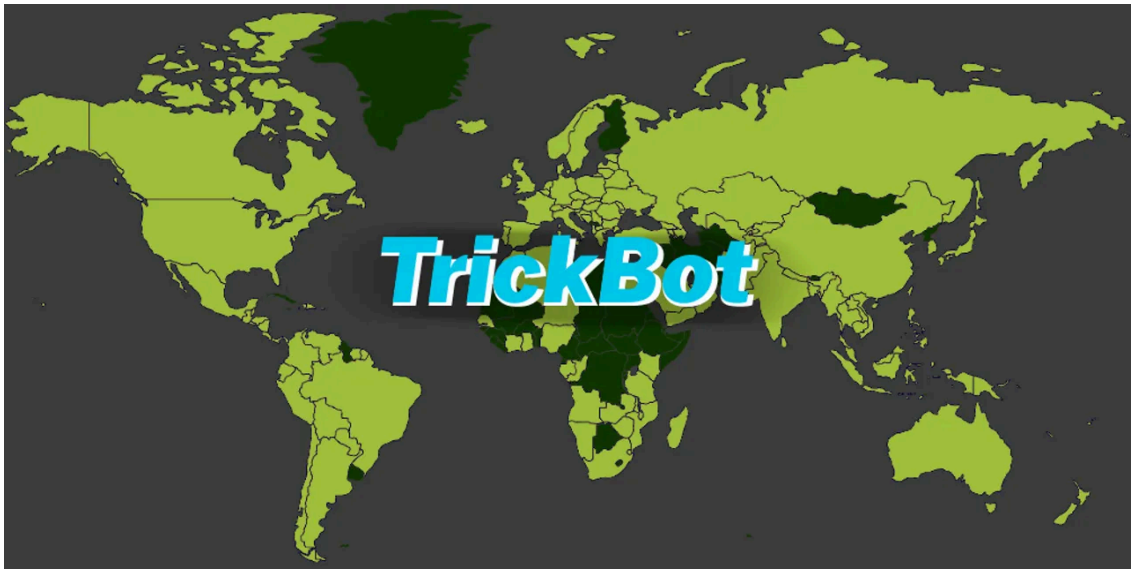
TrickBot botnet survives takedown attempt, but Microsoft sets new legal precedent

By Catalin Cimpanu

Published: 2020-10-13 · Archived: 2026-04-05 23:48:36 UTC



The TrickBot botnet has survived a takedown attempt orchestrated by a coalition of tech companies on Monday.

TrickBot command and control (C&C) servers and domains seized yesterday have been replaced with new infrastructure earlier today, multiple sources in the infosec community have told ZDNet.

Sources from companies monitoring TrickBot activity described the takedown's effects as "temporal" and "limited," but praised Microsoft and its partners for the effort, regardless of its current results.

"Our estimate right now is what the takedown did was to give current victims a breather," a security researcher said.

While some companies agreed to go on the record, ZDNet decided to refrain from using any of our interviewed source's names to avoid indirectly criticizing the entities involved in the takedown (Microsoft's Defender team, FS-ISAC, ESET, Lumen's Black Lotus Labs, NTT, and Broadcom's cyber-security division Symantec).

But in private interviews, even security researchers at ESET, Microsoft, and Symantec told ZDNet that they never expected to take down TrickBot for good in one quick hit.

One source described Monday's action as "kneecapping" the botnet rather than "cutting its head. ZDNet was told that even from the early planning phases, the involved parties expected TrickBot to make a comeback, and planned ahead for follow-up actions.

"As we've seen with prior [takedown] operations, the results of a global disruption involving multiple partners shows up in stages," Tom Burt, CVP of Customer Security and Trust at Microsoft, told ZDNet in an email on Monday.

"We anticipate Trickbot's operators will attempt to revive their operations, and we will take additional legal and technical steps to stop them if necessary," Burt added.

This multi-phased approach to disrupting TrickBot is a direct result of the botnet's complex infrastructure, much of which runs on bulletproof hosting systems, which are unresponsive or slow to react to takedown attempts.

In a threat intelligence bulletin with restricted distribution shared with ZDNet on Monday night, security firm Intel471 noted that TrickBot began moving C&C servers to the EmerDNS decentralized domain name system as a way to counter the ongoing takedown attempt. By Tuesday morning, the botnet's infrastructure had recovered, although it wasn't as active as in previous days.

Even a failed takedown attempt has its effects

But speaking to ZDNet, sources said the disruption efforts weren't only focused on taking down TrickBot servers, which they knew would be temporary and would have no long-standing effects.

Other goals were also discussed and taken into consideration. This included incurring adding additional costs to TrickBot authors and delaying current malware operations, such as ransomware attacks that are usually delivered using TrickBot as a conduit.

Furthermore, security researchers also sought to damage TrickBot's reputation in cybercrime circles.

TrickBot is one of today's Top 3 most successful Malware-as-a-Service (MaaS) operations on the cybercrime underworld. The botnet uses email spam campaigns to infect computers, downloads its malware, and then steals data from infected hosts that it later resells for profit. But the botnet also rents access to infected computers to other criminal groups, which also accounts for a significant portion of its profits. These "customers" include operators of infostealer trojans, BEC fraud groups, ransomware gangs, and even nation-state hacking groups.

Microsoft and its partners wanted to damage this reputation among other cybercrime gangs and send a message that TrickBot isn't as untouchable as its "customers" might think.

A botnet that can be disrupted risks exposing and compromising the operations of "customers," some of which may not want to be exposed to law enforcement tracking. A botnet that can be disrupted isn't reliable businesswise, especially for TrickBot's regular customers who are paying considerable fees to have access to infected systems at precise times.

Researchers hope the slap TrickBot received this week reverberates across its business.

A new legal precedent

But the TrickBot takedown also played another role, one that was invisible to most observers. The court case that preceded the takedown also helped Microsoft set a new legal precedent.

In court, the OS maker argued that the TrickBot malware abused Windows code for malicious purposes, against the terms of service of the standard Windows software development kit (SDK), on which all Windows apps are used.

Microsoft successfully argued that TrickBot was infringing on Microsoft's copyright of its own code by copying and using its SDKs for malicious purposes.

Some might call this approach to taking down a botnet as petty or pedantic, but it's also a genius legal move.

In previous cases, Microsoft or law enforcement usually had to present evidence and be ready to prove that the malware was incurring financial damages to victims in a certain jurisdiction, steps that usually meant identifying and contacting victims.

The new approach focused on the misuse of its Windows SDK code is both easier to prove and argue, but it can also be used in any jurisdiction, providing Microsoft's legal team with a more agile approach to going after malware gangs — which is why Microsoft is likely to reuse it for faster crackdown in the future.
