Like the Energizer Bunny, Trickbot Goes On and On

By Jai Vijayan

Published: 2020-11-12 · Archived: 2026-04-05 17:22:27 UTC

Operators of the Trickbot botnet that has infected more than 1 million systems worldwide with ransomware and other malware are providing a textbook example of just how difficult it can be to truly take out international cybercrime operations.

Weeks after US Cyber Command, Microsoft, and several others took coordinated action to extensively disrupt Trickbot activity, there are signs the botnet operators have still not fully given up yet.

Threat intelligence firm Intel 471 this week reported it had observed signs that a new version of Trickbot is being distributed via spam even as the operators of the malware have begun using a different tool known as BazarLoader to distribute Ryuk ransomware.

According to Intel 471, BazarLoader appears to have been developed by the same group behind Trickbot, sharing some of the same code and infrastructure as the latter. It's presently unclear whether Trickbot operators have switched completely to BazarLoader or if they would return to using the Trickbot botnet at a later date, the threat intelligence firm said in a report this week.

The Ryuk ransomware version that's being distributed in growing numbers has also been associated with Trickbot, Intel 471 said. Together, the data indicates that the group behind Trickbot is still successfully launching targeted ransomware attacks, though their original infrastructure appears to have been all but wiped out, Intel 471 said.

Kacey Clark, threat researcher at Digital Shadows, says Ryuk and Conti ransomware delivery has increased in recent weeks, as has threat groups who are purchasing access to Trickbot-infected machines to leverage in their own attacks.

"Throughout the takedown efforts carried out by security practitioners, Trickbot operators have continuously attempted to spin up new [command-and-control] instances," Clark says. "[As a result], Trickbot operators still maintain access to non-US-based infrastructure, allowing them to continue their attacks."

Trickbot and the group behind it have presented a persistent problem for defenders for several years. The malware first surfaced in 2016 as a banking Trojan and over the years has morphed into a sophisticated tool for delivering ransomware, cryptominers, and other banking Trojans. The operators of the malware itself have established what is believed to be a lucrative crimeware-as-a-service operation that, among other things, sells access to thousands of networks they have previously breached.

The group has been associated with a particularly sophisticated malware toolset called Anchor, which is designed for use against high-value targets. Last year, Trickbot operators are believed to have provided North Korea's Lazarus Group with access to Anchor in a first-of-its-kind collaboration between a cybercrime group and an

advanced persistent threat actor. Earlier this year there were concerns about the group potentially targeting election infrastructure as well.

Coordinated Takedown Attempts

Between September and early November, US Cyber Command, Microsoft, and several others including the Financial Services Information Sharing and Analysis Committee (FS-ISAC) took a series of steps to disrupt and break Trickbot activities. The efforts included disrupting the group's back-end servers and seizing numerous IP addresses associated with Trickbot command-and-control (C2) servers.

Mark Arena, CEO of Intel 471, says US Cyber Command, among other actions, likely breached the back end of Trickbot's infrastructure and used that to modify the configuration files that were sent to Trickbot infected systems.

"The tactics used by US Cyber Command appeared to be orientated toward cutting off the actors behind Trickbot from the systems they had infected," Arena says. It's likely that the action caused Trickbot operators to lose access to a "decent amount" of infected systems, he says.

Microsoft's focus, meanwhile, was on taking down Trickbot's control servers by contacting the respective hosting companies and ISPs using court orders.

The actions have considerably disrupted Trickbot operations but have not erased them completely. With each infrastructure hit, the group has kept devising ways to regain control of it. For instance, when Cyber Command initially succeeded in poisoning Trickbot configuration files, the group was able to restore working files on their C2 servers in 24 hours Intel 471 said. Similarly, when Microsoft began its takedown operations, Trickbot kept setting up new infrastructure in response.

For the moment, the substantial efforts to squelch Trickbot activity appear to have largely worked. At the very least, the actions have forced the threat actors to spend time devising new ways to respond.

"It's expected that they will invest greater efforts in redundancy, including globally distributed command-and-control servers and backup command-and-control methods that are resistant to takedowns," Arena says. "The only real long-term blow that we expect to be effective at halting Trickbot permanently would be arrests of the criminals behind Trickbot."

Clark says the continued Trickbot activity shows how resilient and quick on their feet malware operators can be when pressured.

"As the takedown efforts forced a significant amount of Trickbot infrastructure offline, operators identified new C2 servers and leveraged out-of-band infrastructure to continue their campaign," she says. "Unfortunately, operations of this caliber are resilient and complex, making it very challenging to rid the malware from existence entirely."

About the Author

Contributing Writer

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year career at Computerworld, Jai also covered a variety of other technology topics, including big data, Hadoop, Internet of Things, e-voting, and data analytics. Prior to Computerworld, Jai covered technology issues for The Economic Times in Bangalore, India. Jai has a Master's degree in Statistics and lives in Naperville, Ill.
