That was quick: Trickbot is back after disruption attempts

intel471.com/blog/trickbot-online-emotet-microsoft-cyber-command-disruption-attempts

The Trickbot botnet looks to be working once again, despite separate efforts in the past few weeks aimed at disrupting its operation.

On October 14, 2020, the Emotet spam botnet — which is often the precursor to TrickBot being loaded onto a system — began receiving spam templates intended for mass distribution. These spam templates contained a Microsoft Word document attachment with malicious macros that fetch and load a copy of Emotet onto the victim machine. The Emotet bots reached out to their controllers and received commands to download and execute Trickbot on victim machines.

The Trickbot group tag that Intel 471 identified is tied to a typical infection campaign that information security researchers have been observing for the past 6 months or more.

Additionally Intel 471 researchers saw an update to the Trickbot plugin server configuration file. Fifteen server addresses were added, and two old servers were retained in the configuration, along with the server's .onion address. This was likely done as a fix that would help operators maintain that their infrastructure remains operational.

The fix is another round in the back-and-forth between Trickbot's operators and the separate parties that have attempted to disrupt the botnet's actions. On Oct. 10, 2020, the Washington Post reported that "four U.S. officials" claimed U.S. Cyber Command was conducting an operation to disrupt Trickbot. This action, first reported by Brian Krebs on Oct. 2, 2020, was identified by Intel 471's Malware Intelligence systems on Sept. 22, 2020.

Additionally, Microsoft issued a public statement on Oct. 12, 2020 that it had taken legal action to "combat ransomware ahead of U.S. elections." The legal action involved Microsoft attempting to disrupt a number of Trickbot command and control server IP addresses that are in the United States.

The fact that Trickbot has resumed normal operations despite the best efforts of U.S. Cyber Command and Microsoft shows how resilient of an operation Trickbot is and how much more effort is needed to fully take the botnet offline for good. The botnet's operators have all the IT support of legitimate enterprises — continuity planning, backups, automated deployment, and a dedicated workforce — that allow them to quickly react to disruptive measures.

"About 10 years ago it was much easier to completely take over or significantly disrupt a botnet, but cybercriminals are students of takedowns and have learned to make their operations more resilient to takedown efforts," said Intel 471 COO Jason Passwaters. "That's why every takedown attempt has some potential of giving ground to the adversary. You're teaching them where the weaknesses in their armor are and they have a team of developers ready to act on that information. So unless you strike a killing blow, you're not going to impact them long term.”

While the actions taken this past week let Trickbot’s operators know they are not operating free of consequence, an multi-pronged effort needs to be made if the botnet is to be fully knocked offline:

- Law enforcement efforts should be multinational and focus on arresting the core operators of the botnet.
- Any further efforts to disrupt infrastructure should focus on the main infrastructure, not just that of countries where a court order is needed.
- Governments and companies should work together on mass “de-infection” campaigns, similar to those used to eliminate the Bredolab botnet in 2010 and Retadup botnet in 2019.

Whether this is a realistic endeavor in today’s world is another question altogether.