Trickbot Activity Increases; new VNC Module On the Radar

By Radu TUDORICA

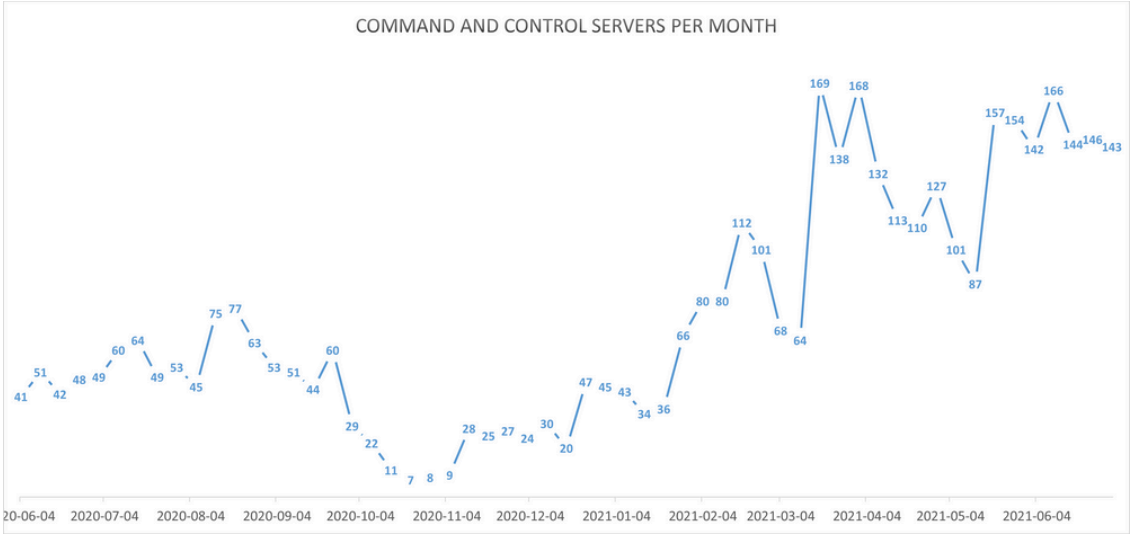
Archived: 2026-04-05 19:59:58 UTC

Trickbot has been around since late 2016, when it appeared in the form of a banker and credential-stealing application. Drawing inspiration from Dyre (or Dyreza), Trickbot consists of an ecosystem of plugin modules and helper components. The Trickbot group, which has infected millions of computers worldwide, has recently played an active role in disseminating ransomware.

We have been reporting on notable developments in Trickbot's lifecycle, with highlights including the analysis in 2020 of one of its modules used to bruteforce RDP connections and an analysis of its new C2 infrastructure in the wake of the massive crackdown in October 2020.

Despite the takedown attempt, Trickbot is more active than ever. In May 2021, our systems started to pick up an updated version of the **vncDll** module that Trickbot uses against select high-profile targets. This module, known as **tvncDll,** is used for monitoring and intelligence gathering**.** It seems to be still under development, since the group has a frequent update schedule, regularly adding new functionalities and bug fixes.

In addition to upgraded modules, Bitdefender has noted a significant increase in command-and-control centers deployed around the world.



This new research focuses on an updated VNC module, which includes new functionalities for monitoring and intelligence gathering.

Additionally, Bitdefender researchers have identified the software application that the attackers use to interact with the victims through the C2 servers. This tool is described in a dedicated chapter.

A complete analysis of the new component can be found in the researcher paper available below. An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users.

Download the whitepaper
