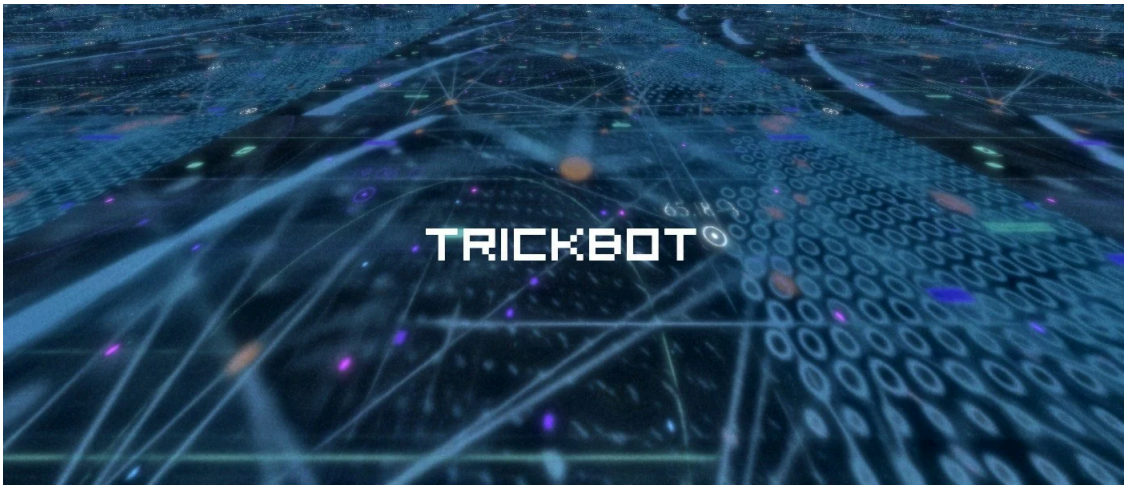
Trickbot updates its VNC module for high-value targets

By Ionut Ilascu

Published: 2021-07-14 · Archived: 2026-04-05 23:45:13 UTC

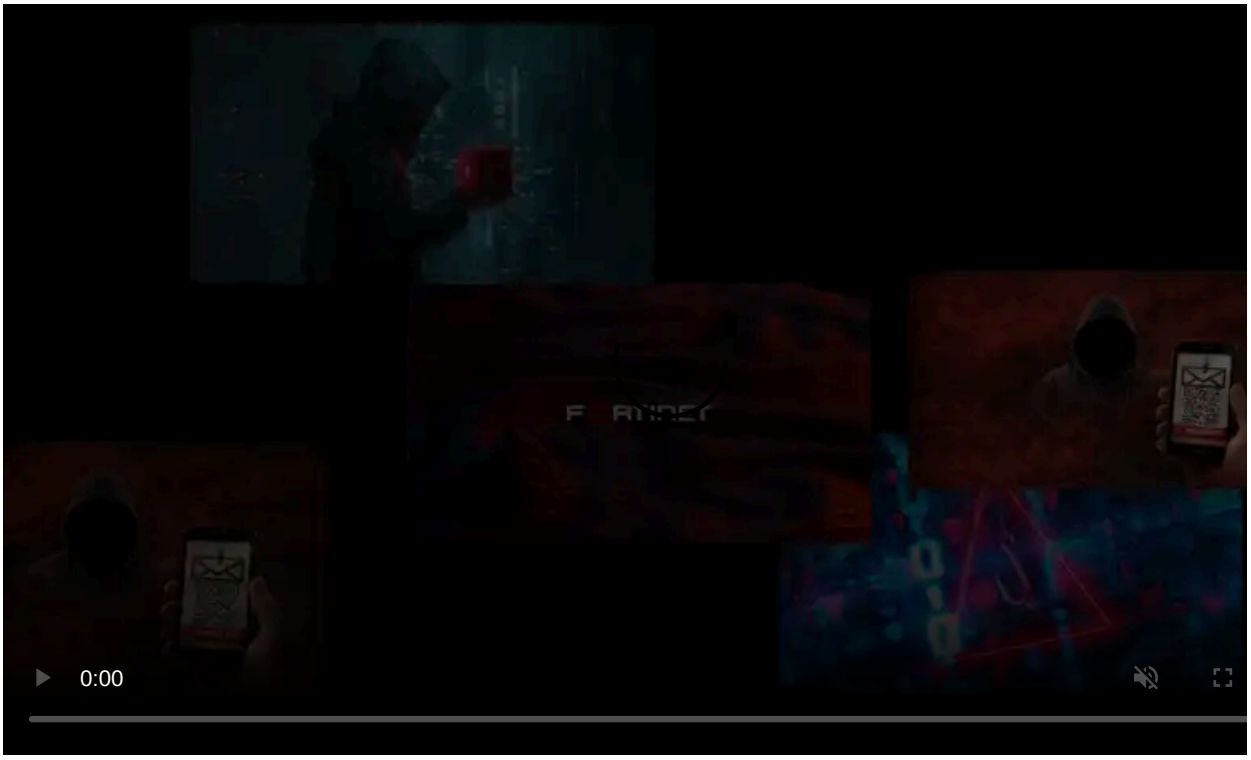


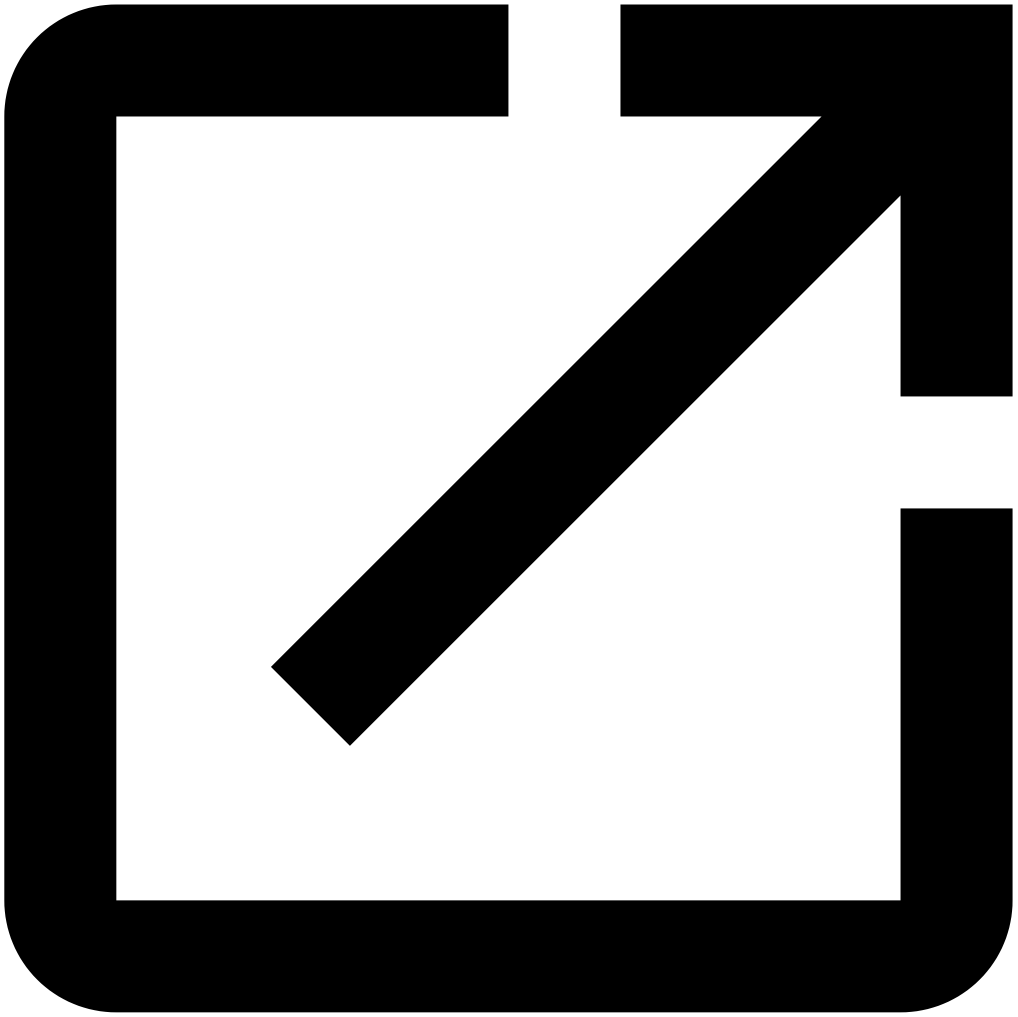
The Trickbot botnet malware that often distributes various ransomware strains, continues to be the most prevalent threat as its developers update the VNC module used for remote control over infected systems.

Its activity has been increasing constantly since the complete disruption of the Emotet botnet in January, which acted as a distributor for both Trickbot and other high-profile threat actors.

Most prevalent threat

Trickbot has been around for almost half a decade and transitioned from a banking trojan to one of the largest botnets today that sells access to various threat actors.


0:00



Some of the ransomware operations using this botnet for network access include the infamous Ryuk, Conti, REvil, as well as a new one called Diavol, the Romanian for Devil.

Since Emotet's takedown by law enforcement, Trickbot activity started to increase to such levels that in May it was the most prevalent malware on Check Point's radar.

The malware maintained its position this month, too, the cybersecurity company notes in a report today, adding that Trickbot's maintainers are constantly working to improve it.

According to Check Point's telemetry, Trickbot impacted 7% of organizations across the world, followed by the XMRig cryptocurrency miner the Formbook info stealer, which affected 3% of the organizations that Check Point monitors worldwide.

New VNC module in the works

In another report, Romanian cybersecurity company Bitdefender says that its systems caught a new version of Trickbot's VNC module (vncDLL), used after compromising high-profile targets.

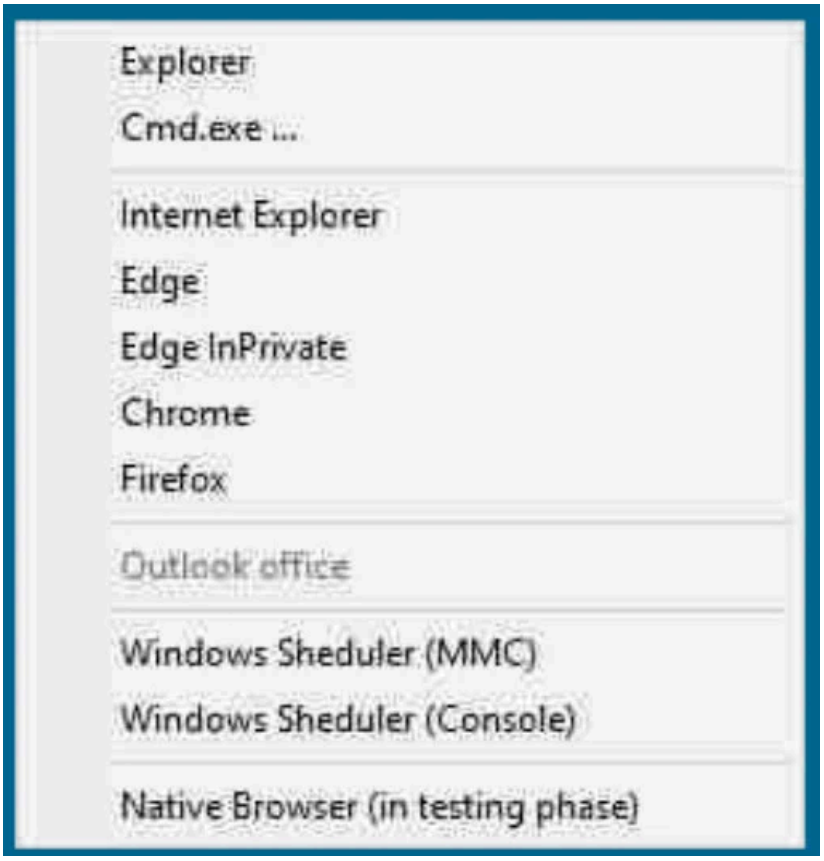
The updated module is called tvncDLL and allows the threat actor to monitor the victim and collect information that would enable pivoting to valuable systems on the network.

Although tvncDLL was discovered on May 12, the Romanian researchers say that it is still under development, "since the group has a frequent update schedule, regularly adding new functionalities and bug fixes."

Bitdefender's analysis of the module points out that it uses a custom communication protocol and reaches the command and control (C2) server through one of nine proxy IP addresses that enable access to victims behind firewalls.

The VNC component can stop Trickbot and unload it from memory. When an operator initiates communication, the module creates a virtual desktop with a custom interface.

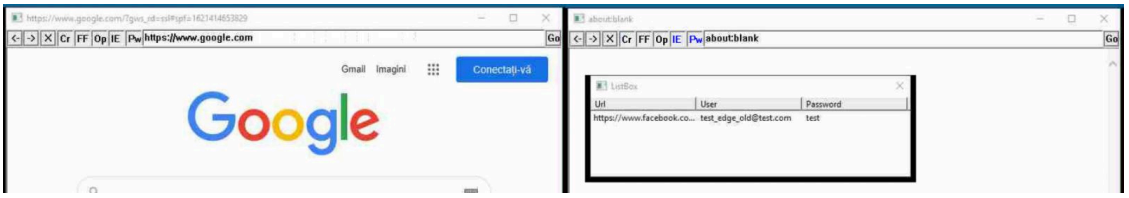
"During normal operation, the alternate desktop is created and fully controlled by the module, copying the icons from the desktop, creating a custom taskbar for managing its processes and creating a custom right-click menu, containing custom functionality," Bitdefender researchers write in their report.



Using the command prompt, the threat actor can download fresh payloads from the C2 server, open documents and the email inbox, steal data from the compromised system.

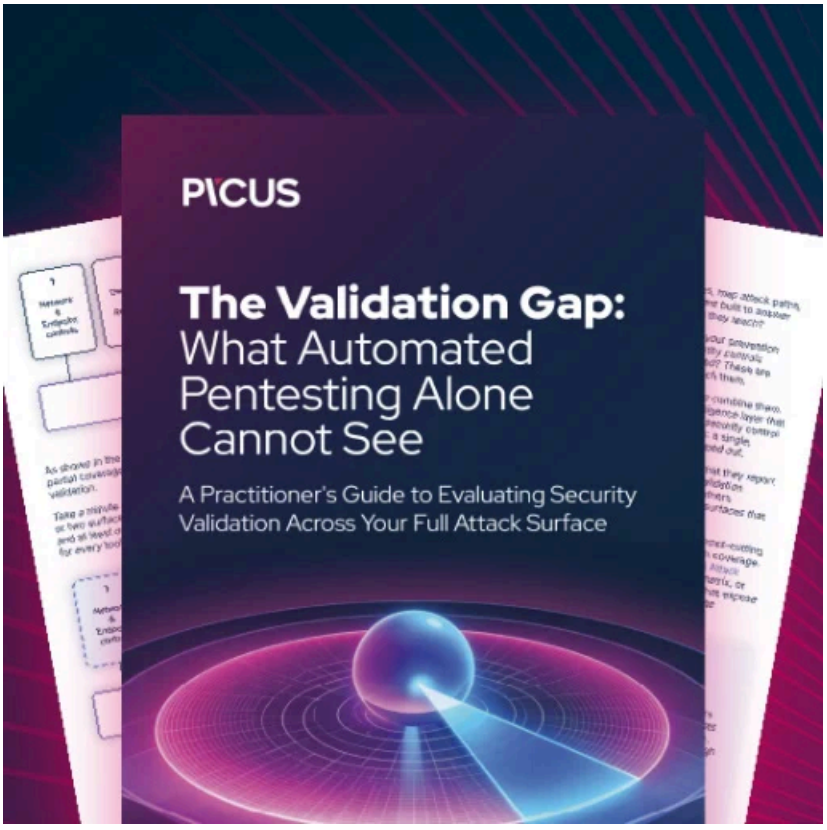
Another option called Native Browser fires up a web browser by taking advantage of the OLE automation feature in Internet Explorer.

The function is under development and its purpose is to steal passwords from Google Chrome, Mozilla Firefox, Opera, and Internet Explorer.



The researchers say that while the old vncDLL module has been in use since at least 2018, its successor became active in the wild on May 11, 2021, according to evidence revealed during their investigation.

Telemetry data from Bitdefender data shows Trickbot's C2 servers spread on almost all continents, with the largest number (54) located in North America. According to the company, the number of C2 servers has increased significantly this year, jumping from around 40 in January to more than 140 in June.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/trickbot-updates-its-vnc-module-for-high-value-targets/