Notorious TrickBot Malware Gang Shuts Down its Botnet Infrastructure

thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

February 24, 2022

The modular Windows crimeware platform known as TrickBot formally shuttered its infrastructure on Thursday after reports emerged of its imminent retirement amid a lull in its activity for almost two months, marking an end to one of the most persistent malware campaigns in recent years.

"TrickBot is gone... It is official now as of Thursday, February 24, 2022. See you soon... or not," AdvIntel's CEO Vitali Kremez tweeted. "TrickBot is gone as it has become inefficient for targeted intrusions."

Attributed to a Russia-based criminal enterprise called Wizard Spider, TrickBot started out as a financial trojan in late 2016 and is a derivative of another banking malware called Dyre that was dismantled in November 2015. Over the years, it morphed into a veritable Swiss Army knife of malicious capabilities, enabling threat actors to steal information via web injects and drop additional payloads.

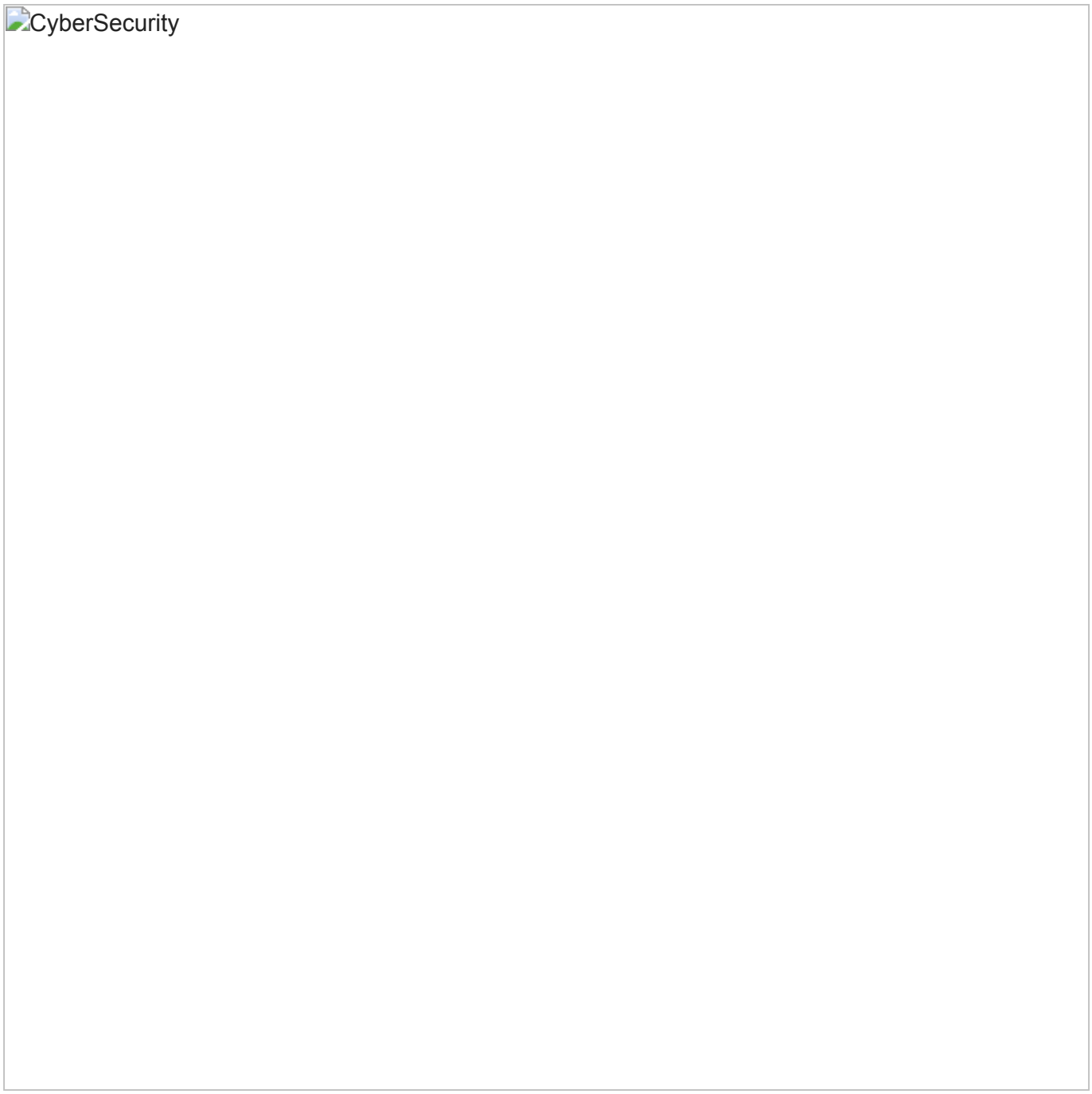
TrickBot's activities took a noticeable hit in October 2020 when the U.S. Cyber Command and a consortium of private security companies led by Microsoft attempted to disrupt most of its infrastructure, forcing the malware's authors to scale up and evolve its tactics.

The criminal entity is said to have invested more than $20 million into its infrastructure and growth, security firm Hold Security was quoted as saying in a WIRED report earlier this month, calling out TrickBot's "businesslike structure" to run its day-to-day operations and "hire" new engineers into the group.

The development comes as twin reports from cybersecurity firms AdvIntel and Intel 471 hinted at the possibility that TrickBot's five-year-saga may be coming to an end in the wake of increased visibility into their malware operations, prompting the operators to shift to newer, improved malware such as BazarBackdoor (aka BazarLoader).

"TrickBot, after all, is relatively old malware that hasn't been updated in a major way," Intel 471 researchers said. "Detection rates are high and the network traffic from bot communication is easily recognized."

Indeed, malware tracking research project Abuse.ch's Feodo Tracker shows that while no new command-and-control (C2) servers have been set up for TrickBot attacks since December 16, 2021, BazarLoader and Emotet are in full swing, with new C2 servers registered as recently as February 19 and 24, respectively.



BazarBackdoor, which first appeared in 2021, originated as a part of TrickBot's modular toolkit arsenal but has since evolved into a fully autonomous malware mainly used by the Conti (previously Ryuk) cybercrime gang to deploy ransomware on enterprise networks.

TrickBot's demise has also come as the operators of Conti ransomware recruited top talent from the former to focus on stealthier replacement malware like BazarBackdoor. "TrickBot has been linked with Conti for a while, so further synergy there is highly possible," Intel 471 told The Hacker News.

Conti has also been credited with resurrecting and integrating the Emotet botnet into its multi-pronged attack framework starting November 2021, with TrickBot, ironically, utilized as a delivery vehicle to distribute the malware after a gap of 10 months.

"However, the people who have led TrickBot throughout its long run will not simply disappear," AdvIntel noted last week. "After being 'acquired' by Conti, they are now rich in prospects with the secure ground beneath them, and Conti will always find a way to make use of the available talent."

SHARE □ □ □ □ □
SHARE □