Related news

cyberscoop.com/trickbot-shutdown-conti-emotet/

February 25, 2022

threats

TrickBot malware suddenly got quiet, researchers say, but it's hardly the end for its operators

(Getty Images)
Written by Joe Warminsky
Feb 25, 2022 | CYBERSCOOP
The operators of TrickBot have essentially shut down the notorious malware, multiple reports say, but evidence suggests the gang has begun using other platforms or folded operations into another cybercrime group altogether.

Researchers at Intel471 and AdvIntel noted a sharp dip in recent TrickBot activity in separate reports Thursday, even though the command-and-control infrastructure for the malware remains operational.

Intel471 said “it’s likely that the Trickbot operators have phased Trickbot malware out of their operations in favor of other platforms,” probably Emotet — a development researchers have been tracking for months.

AdvIntel’s Yelisey Boguslavskiy, meanwhile, said in his report that TrickBot’s operators had been subsumed into Conti, a Russia-linked cybercrime group known for offering “ransomware as a service” packages to its affiliates. Researchers previously had noted TrickBot connections with Conti.

“In name, at least, this means that TrickBot’s four-year saga is now coming to a close — the liaison that has defined the cybercrime domain for years has been reborn into a newer, possibly even deadlier form,” Boguslavskiy wrote. “However, the people who have led TrickBot throughout its long run will not simply disappear. 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.”

The Conti group, meanwhile, put its support behind Russia on Friday, saying it would use its full capabilities to strike back at any entity that threatens Russian critical infrastructure.

“See you soon … or not” AdvIntel CEO Vitali Kremez tweeted at Trickbot Thursday.

Busy, but in other ways

TrickBot first drew attention as trojan malware aimed at the banking industry, but it soon developed into a broader framework of tools for gaining access to sensitive networks in general. Separate takedowns led by U.S. Cyber Command and Microsoft in late 2020, as well as prosecutions of TickBot leaders by U.S. law enforcement in 2021, put a significant dent in the gang’s operations.

The skills of TrickBot’s core group remain sharp, researchers say. A report earlier this month from Check Point Research noted recent upgrades to some Trickbot modules. The BazarBackdoor tool, for example, has become a brand unto itself for cybercriminals who want access to high-value targets, according to Intel471 and AdvIntel.

Alexander Chailytko, Check Point’s cybersecurity research and innovation manager, told CyberScoop that there were some signs of successful requests of TrickBot command-and-control servers as recently as this week. Old infrastructure for the malware appeared to be “still maintained and operational” into 2022, Chailytko said, but has not been nearly as busy over the past two months.