TrickBot Gang Likely Shifting Operations to Switch to New Malware

thehackernews.com/2022/02/trickbot-gang-likely-shifting.html

February 24, 2022

TrickBot, the infamous Windows crimeware-as-a-service (CaaS) solution that's used by a variety of threat actors to deliver next-stage payloads like ransomware, appears to be undergoing a transition of sorts, with no new activity recorded since the start of the year.

The lull in the malware campaigns is "partially due to a big shift from Trickbot's operators, including working with the operators of Emotet," researchers from Intel 471 said in a report shared with The Hacker News.

The last set of attacks involving TrickBot were registered on December 28, 2021, even as command-and-control (C2) infrastructure associated with the malware has continued to serve additional plugins and web injects to infected nodes in the botnet.

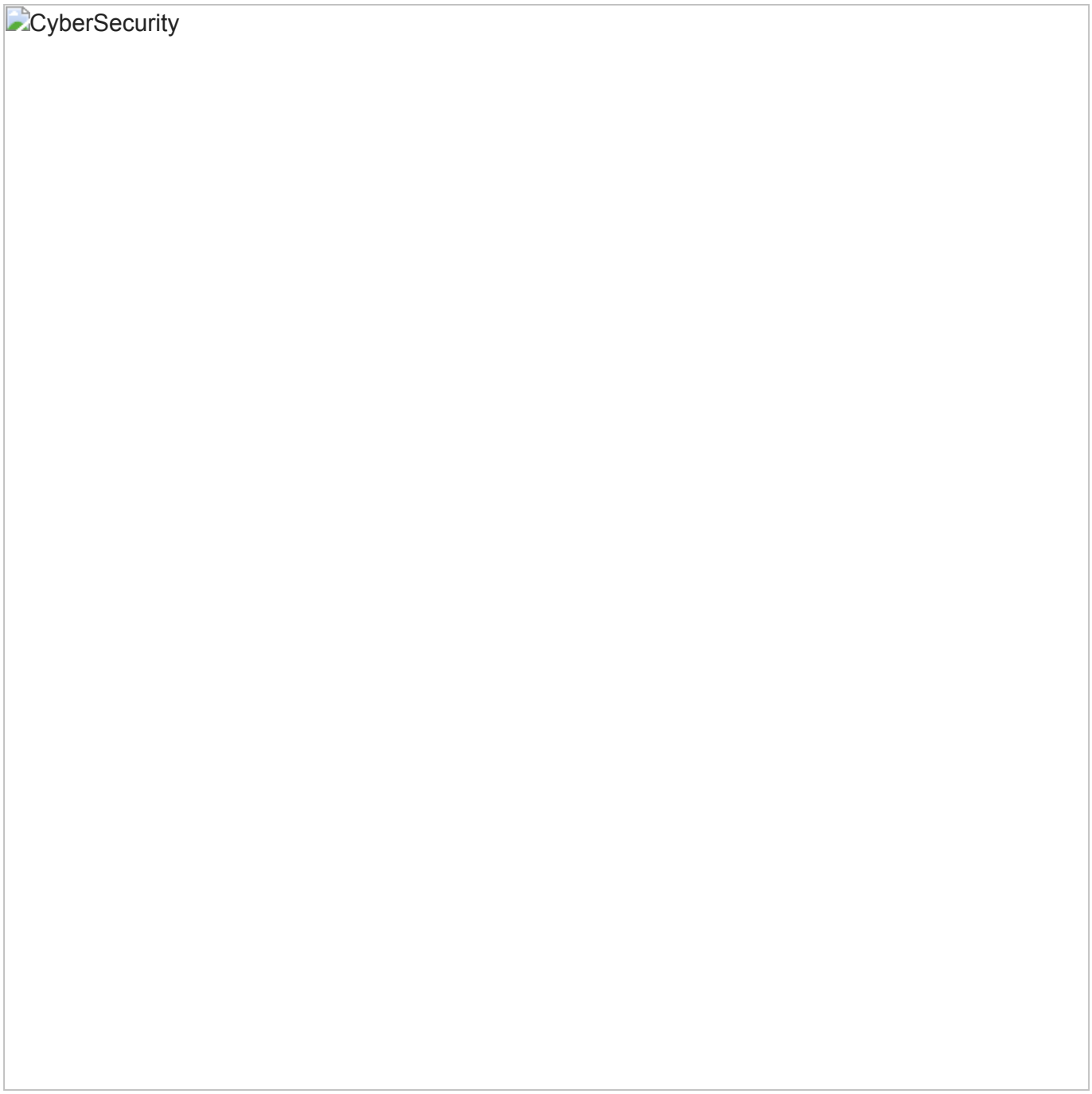
Interestingly, the decrease in the volume of the campaigns has also been accompanied by the TrickBot gang working closely with the operators of Emotet, which witnessed a resurgence late last year after a 10-month-long break following law enforcement efforts to tackle the malware.

The attacks, which were first observed in November 2021, featured an infection sequence that used TrickBot as a conduit to download and execute Emotet binaries, when prior to the takedown, Emotet was often used to drop TrickBot samples.

"It's likely that the TrickBot operators have phased TrickBot malware out of their operations in favor of other platforms, such as Emotet," the researchers said. "TrickBot, after all, is relatively old malware that hasn't been updated in a major way."

Additionally, Intel 471 said it observed instances of TrickBot pushing Qbot installs to the compromised systems shortly after Emotet's return in November 2021, once again raising the possibility of a behind-the-scenes shake-up to migrate to other platforms.

With TrickBot increasingly coming under the lens of law enforcement in 2021, it's perhaps not too surprising that the threat actor behind it is actively attempting to shift tactics and update their defensive measures.



According to a separate report published by Advanced Intelligence (AdvIntel) last week, the Conti ransomware cartel is believed to have acqui-hired several elite developers of TrickBot to retire the malware and switch to upgraded variants such as BazarBackdoor.

"Perhaps a combination of unwanted attention to TrickBot and the availability of newer, improved malware platforms has convinced the operators of TrickBot to abandon it," the researchers noted. "We suspect that the malware control infrastructure (C2) is being maintained because there is still some monetization value in the remaining bots."

SHARE □ □ □ □ □
SHARE □
Malware, Trickbot