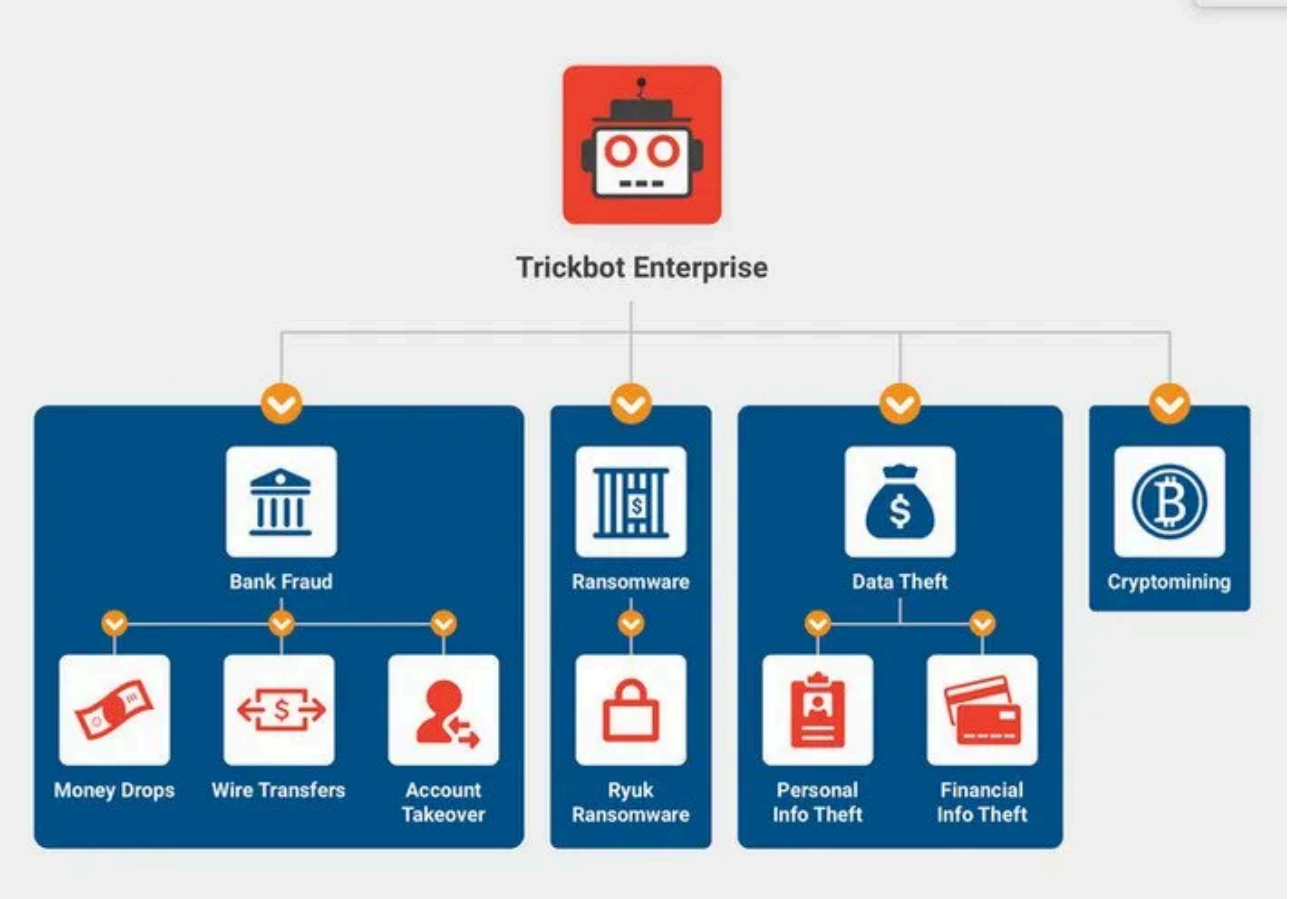
Trickbot operation is now controlled by Conti ransomware

By Pierluigi Paganini

Published: 2022-02-20 · Archived: 2026-04-02 11:32:54 UTC

Pierluigi Paganini February 20, 2022



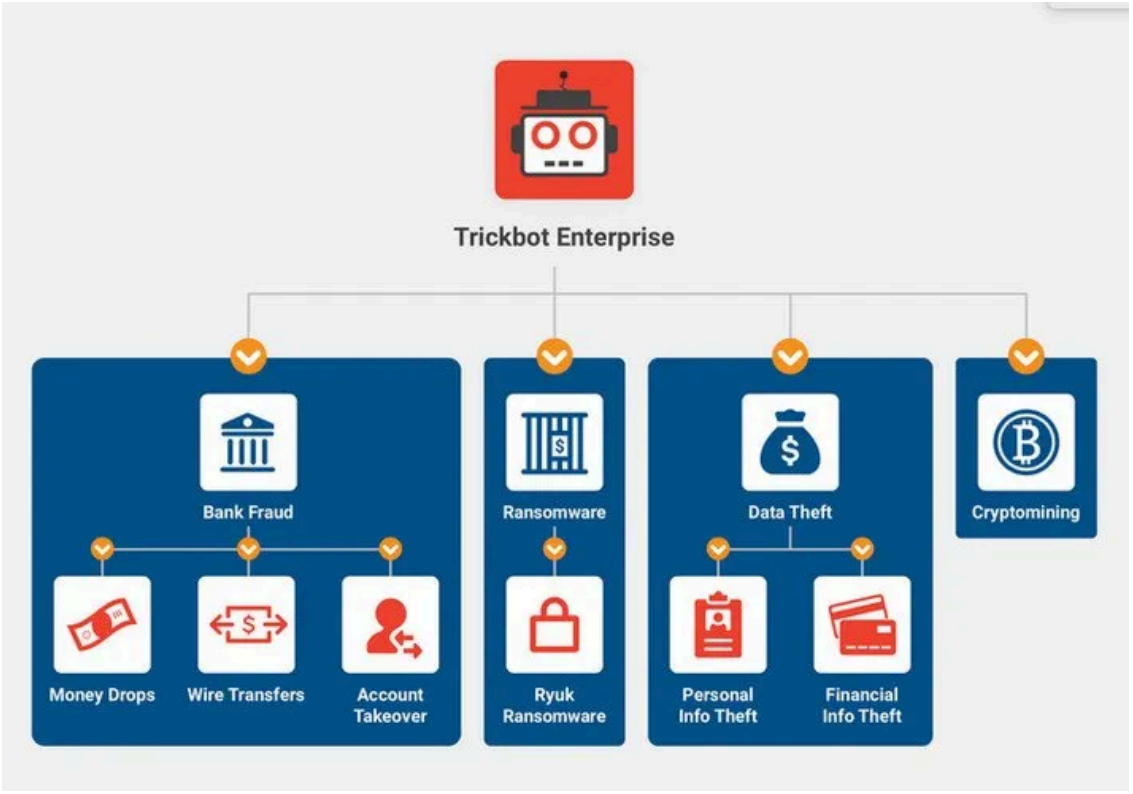
The Conti ransomware group takes over TrickBot malware operation and plans to replace it with BazarBackdoor malware.

TrickBot operation has arrived at the end of the journey, according to AdvIntel some of its top members move under the Conti ransomware gang, which is planning to replace the popular banking Trojan with the stealthier BazarBackdoor.

TrickBot is a popular Windows banking Trojan that has been around since October 2016, its authors have continuously upgraded it by implementing new features, including powerful password-stealing capabilities.

TrickBot initially partnered with Ryuk ransomware that used it for initial access in the network compromised by the botnet. Then Ryuk was replaced by Conti Ransomware gang who has been using Trickbot for the same purpose.

"The group's elite division, called Overdose, managed the TrickBot campaigns that resulted in the creation of Conti and Ryuk ransomware." states the analysis published by AdvInt. "The group has made at least $200 million USD with one extreme case extorting ~$34 million USD from a single victim and has perpetrated a spate of attacks on numerous healthcare organizations, including Universal Health Services (UHS) via BazarBackdoor to Ryuk ransomware (the attack was estimated for an account for $67 Million USD in damages)."



In 2021, the Conti gang used in exclusive the TrickBot to achieve initial accesses in the network of organizations worldwide.

The goal of the Conti gang is to aggregate highly skilled members of the ransomware ecosystem in a structure, which gives them a little autonomy, to monopolize the market.

The TrickBot's core team of developers had already created a stealthier piece of malware dubbed BazarBackdoor, used to achieve remote access into corporate networks and use it to deploy the ransomware.

With the increasing popularity of TrickBot it became easy to detect it with antimalware solutions, for this reason the gang began employing the BazarBackdoor for initial access to networks.

By the end of 2021, Conti gang employed core developers and managers of the TrickBot botnet.

"At the same time, Conti turned into the sole end-user of TrickBot's botnet product. By the end of 2021, Conti had essentially acquired TrickBot, with multiple elite developers and managers joining the ransomware cosa nostra." concludes the post.

"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.”

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(SecurityAffairs – hacking, Conti ransomware)

[adrotate banner=”5″]

[adrotate banner=”13″]

Source: https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html