

The TrickBot Saga's Finale Has Aired: Spinoff is Already in the Works

By Yelisey Boguslavskiy



”

At this point, AdvIntel's adversarial visibility can clearly confirm that TrickBot is still operational, however, the botnet is reaching its limits. According to our sensitive source intelligence, the availability of TrickBot IOCs have made it highly detectable, and Conti is no longer using it.

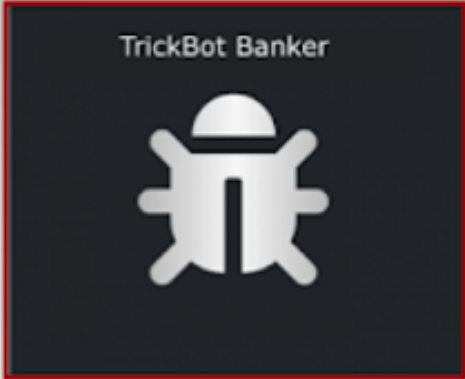


The source of the report intelligence is sensitive TLP: RED internal communications between Conti and TrickBot operators. The report is declassified as TLP: WHITE in the interest of public awareness.

Our investigative intelligence work at AdvIntel is primarily directed at top-tier cybercriminal groups. We perceive cybercrime as a constantly-maturing community from which its most skilled actors merge together to form elite collectives, capable of taking down GDP-size infrastructures and extorting tens of millions of dollars, while the less gifted are left to gossip on darknet forums.

In past years, we've established visibility into even the most advanced cyber gangs and syndicates, but within this selective world, there has been one group that has been especially outstanding—TrickBot.

Targeted Botnet Card



The logo for TrickBot Banker is a white stylized robot icon on a dark background. The robot has a semi-circular head, a vertical body, and four limbs. Above the robot, the text "TrickBot Banker" is written in white.

- **Name:** TrickBot
- **Type:** Credential Stealer, Multi-Purpose Loader-as-a-Service
- **Functionality:** Credential Stealing, Ransomware Loading
- **Distribution:** Phishing emails, Botnets
- **Threat Level:** Very High
- Can Upload **Ryuk/Conti Ransomware**
- **Attribution:** Eastern European Crime Group

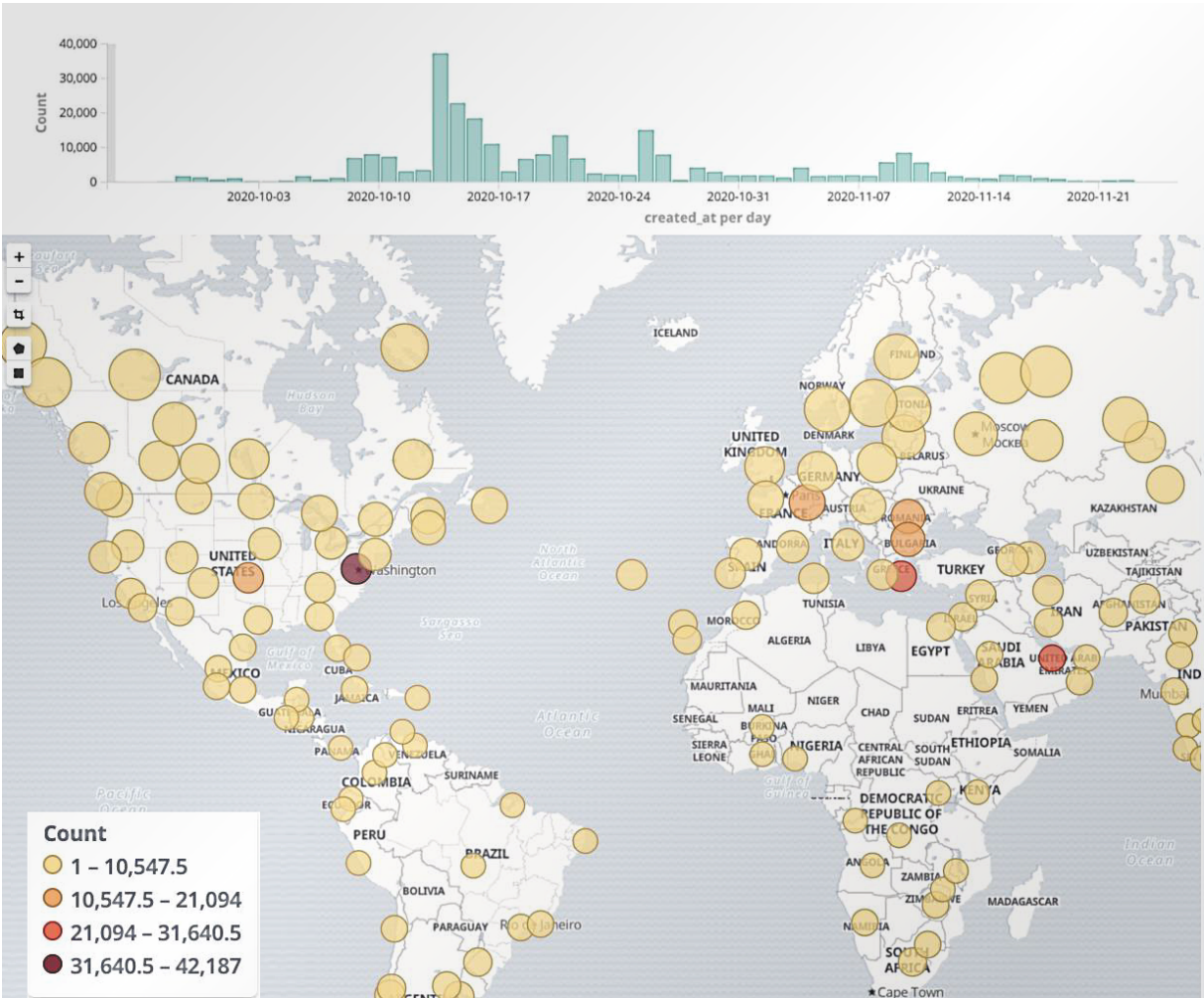
TrickBot, also known as Trojan.Win32.Trickster, TrickLoader, is a prolific banking trojan designed to steal personal and financial data. The trojan was developed based on Dyre (Dyreza) banking malware with an added webinject attack vector.

AdvIntel's TrickBot card, from 2020

TrickBot: Origins

AdvIntel has been closely following TrickBot since it was primarily a banking trojan designed to steal personal financial data. By 2019, it had evolved into the most prolific tool of information theft.

TrickBot relies on a *modular* system. This means that its separate modules can be utilized for different purposes, making it especially flexible malware. For instance, [in July 2020](#), TrickBot test piloted a mysterious module known as *grabber.dll* linked to the arrest of [Vladimir Dunaev](#), identified by AdvIntel earlier. The module version was meant for browser theft and affected *Google Chrome, Internet Explorer, Mozilla Firefox, and Microsoft Edge* as well as *browser cookies*.

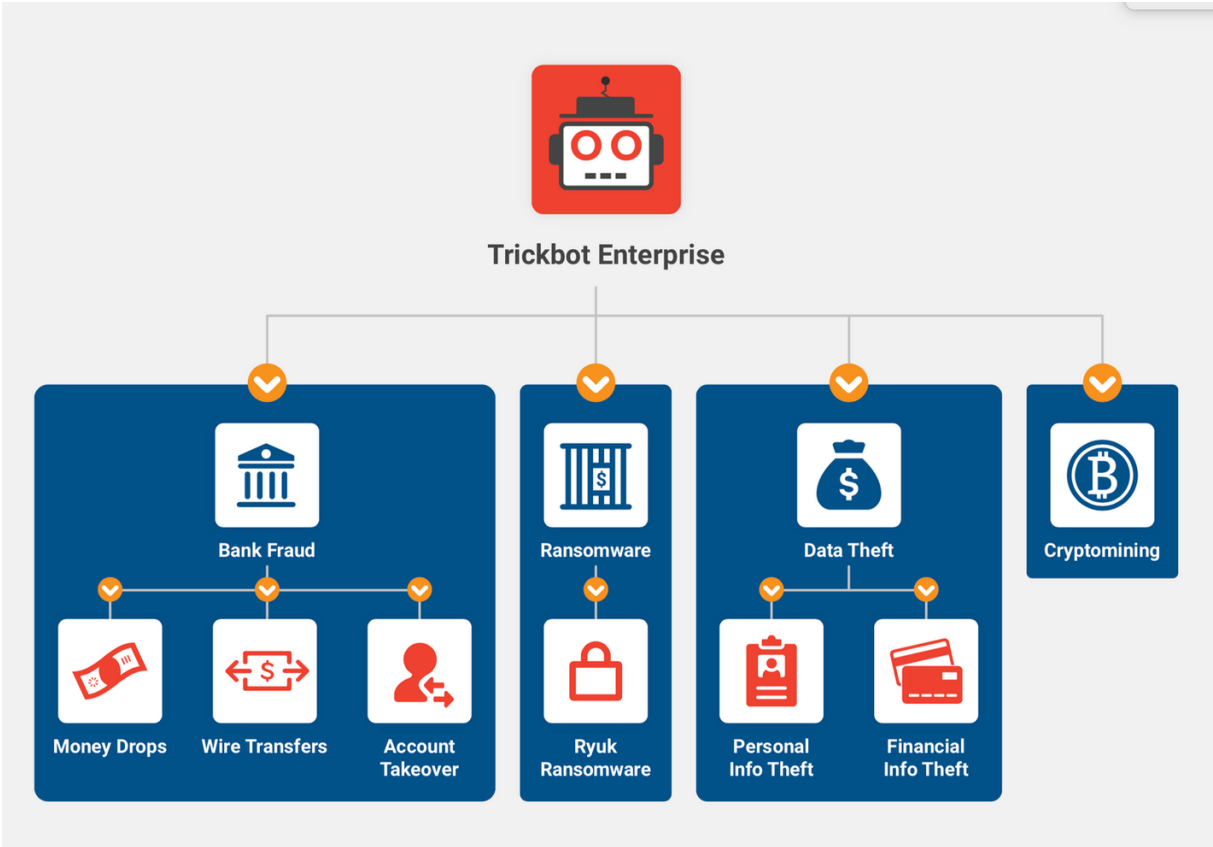


A sample for AdvIntel TrickBot monitoring - Fall 2020

The Future of Cybercrime

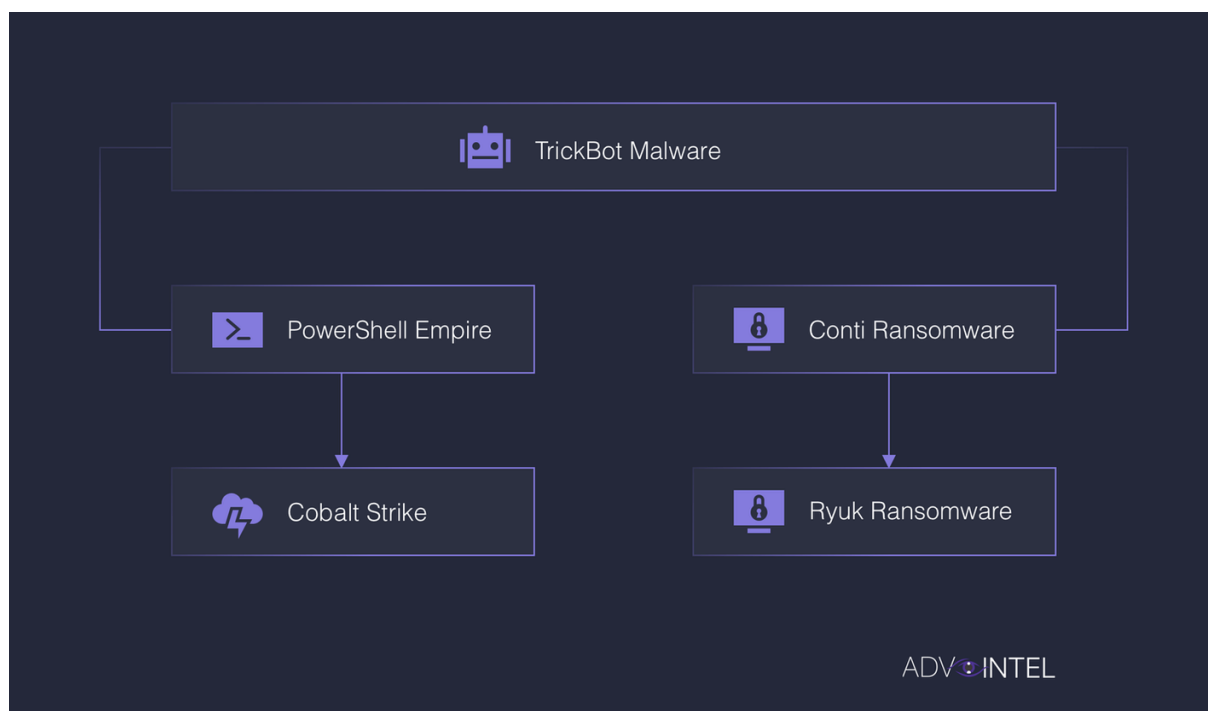
In October 2021, TrickBot even developed a function designed to inspect the [UEFI/BIOS firmware](#) of its targets, in order to survive any system re-imagining efforts during the recovery phase of a *Ryuk (Conti)* ransomware event, further allowing adversaries to semi-permanently brick an affected device. The installation framework

of TrickBot's notorious *AchorDNS* malware has also been used by some of the most notorious (specifically Russian and North Korean) threat actors to target healthcare, finance, telecoms, education, and critical infrastructure.



By 2019, TrickBot possessed a highly developed organizational network, with operations in all avenues of cybercrime.

However, the most salient and worrisome prediction for TrickBot was its role as the most dangerous tool in ransomware's future arsenal. The group's elite division, called *Overdose*, managed the TrickBot campaigns that resulted in the creation of Conti and Ryuk ransomware. 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).



Typical TrickBot-Ransomware Kill Chain. (Source: AdvIntel)

AdvIntel has been tracking this specialization of TrickBot since its early stages, remaining vigilant in monitoring its relationship with Ryuk (now Conti) which became one of the most damaging cybercrime alliances in recent history. After Ryuk’s rebrand and subsequent attempt to take down TrickBot in October, we have observed that this partnership in crime began to change.

Notably, [Alla Witte](#), a Latvian national, even was hired specifically under the alias “max” to develop another ransomware called internally “Enigma”, or “Diavol” for TrickBot backcompatilability to be extradited and arrested by the Department of Justice.

An Offer TrickBot Couldn’t Refuse

In 2022, Conti has expanded to the point that they now fit the definition of a crime **syndicate**, hitting many key hallmarks such as *A) the unification of many highly skilled and proficient members of the same craft with little autonomy (in contrast to other RaaS groups)* and *B) the organization’s clear end-goal to monopolize the market*. Currently, only **EvilCorp** has earned this title in the ransomware community.

Its relationship with TrickBot was one of the primary reasons for the rapid rise of Conti, possibly even for its survival. The *Emotet-TrickBot-Ryuk* supply chain was extremely resilient. And with a stable and high-quality supply of accesses coming from a single organized source, Conti was able to maintain its image without any major structural changes. When the rest of the ransomware gangs were massively hiring random affiliates and delegating them to breach corporate networks, Conti was working in a

trust-based, team-based manner. And when said *random* affiliates began to *randomly* hack Western infrastructure and *randomly* blackmail Western leaders, calling the wrath of the Russian security apparatus on their heads, Conti merely kept a clear code of conduct and continued operations as normal.

As its competitors began going down one-by-one, either hit by the sudden crackdown of Russia's government or simply incapable of breaching enough networks to survive, Conti prospered. Suddenly TrickBot, formally Conti's partner and equal, was turning into its subsidiary. 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*.

BazarBackdoor's Kiss of Death

At this point, AdvIntel's adversarial visibility can clearly confirm that TrickBot is still operational, however, the botnet is reaching its limits. According to our sensitive source intelligence, the availability of TrickBot IOCs has made it highly detectable, and Conti is no longer using it.

Conti has already hired TrickBot's top members, and can now invest in newer and better products. Take [BazarBackdoor](#) - TrickBot group's newer, stealthier replacement malware that is now being leveraged at high-value targets. BazarBackdoor was formerly a part of Trickbot's toolkit arsenal but has now become its own fully autonomous tool.

Moreover, the Conti syndicate is powerful enough to have even [summoned Emotet from the dead](#), not to mention *QBot* and *IcedID*, with more sophisticated email campaigns dropping *Cobalt Strike*.

Leaving the "Backdoor" Open for a Sequel

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.

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.

In addition to monitoring TrickBot, AdvIntel provides early warning services for all its alternatives used by the top-ransomware groups, including Emotet, QBot, IcedID, Log4shell CVE adversarial datasets, and others.

To learn more on how to efficiently defend yourself from these precursors, please reach out to us.