

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)

> Security (<https://www.bleepingcomputer.com/news/security/>)

> Conti ransomware gang takes over TrickBot malware operation

# Conti ransomware gang takes over TrickBot malware operation

By

February 18, 2022

10:11 AM

0

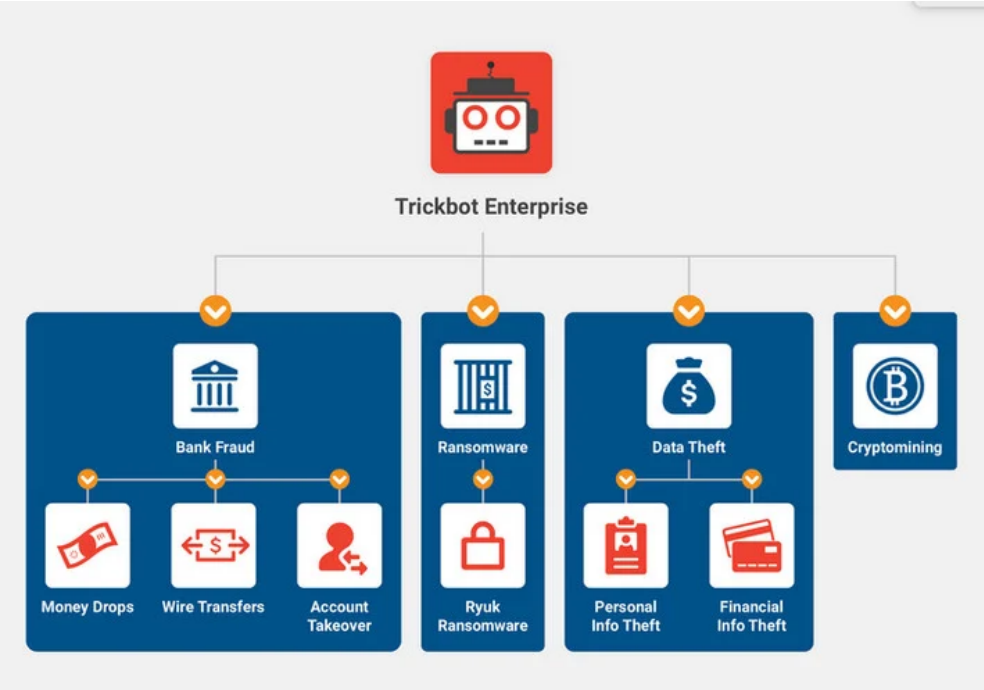
**Ionut Ilascu**  
(<https://www.bleepingcomputer.com/author/ionut-ilascu/>)



After four years of activity and numerous takedown attempts, the death knell of TrickBot has sounded as its top members move under new management, the Conti ransomware syndicate, who plan to replace it with the stealthier BazarBackdoor malware.



TrickBot is a Windows malware platform that uses multiple modules for various malicious activities, including information stealing, password stealing, infiltrating Windows domains, initial access to networks, and malware delivery.



Top Articles



([https://www.bleepingcomputer.com/news/security/cisa-warns-of-hybrid-operations-threat-to-us-critical-infrastructure/?traffic\\_source=Connatix](https://www.bleepingcomputer.com/news/security/cisa-warns-of-hybrid-operations-threat-to-us-critical-infrastructure/?traffic_source=Connatix))

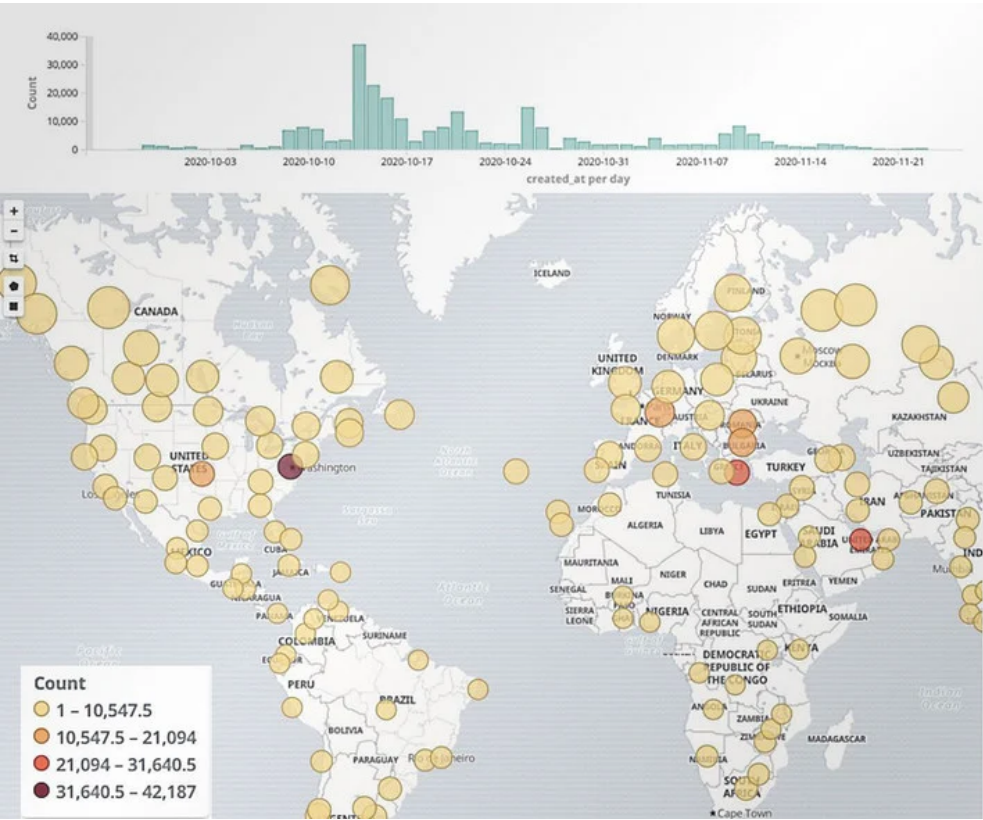
CISA warns of hybrid operations threat to US critical infrastructure

TrickBot has dominated the malware threat landscape since 2016, partnering with ransomware gangs and causing havoc on millions of devices worldwide.



### Cyber Range Training Platform

Train virtual and in-house SOC teams in a hyper realistic platform anytime, anywhere



The Ryuk ransomware gang initially partnered with TrickBot for initial access to works, but were replaced Conti Ransomware gang who has been using the malware for the past year to gain access to corporate networks.

It is estimated that the group handling TrickBot campaigns - an elite division known by the name Overdose, has made at least \$200 million from its operations,

## Conti takes over TrickBot operation

Researchers at cybercrime and adversarial disruption company Advanced Intelligence (AdvIntel (<https://www.advintel.io/>)) noticed that in 2021 Conti had become the only beneficiary of TrickBot's supply of high-quality network accesses.

By this time, TrickBot's core team of developers had already created a stealthier piece of malware, BazarBackdoor (<https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/>), used primarily for remote access into valuable corporate networks where ransomware could be deployed.

As the TrickBot trojan had become easily detectable by antivirus vendors, the threat actors began switching to BazarBackdoor for initial access to networks as it was developed specifically to stealthily compromise high-value targets (<https://www.bleepingcomputer.com/news/security/bazarloader-used-to-deploy-ryuk-ransomware-on-high-value-targets/>).

However, by the end of 2021, Conti managed to attract "multiple elite developers and managers" of the TrickBot botnet, turning the operation into its subsidiary rather than a partner, AdvIntel notes in a report shared with BleepingComputer.

Based on internal Conti conversations that the researchers had access to and shared with BleepingComputer, AdvIntel says that BazarBackdoor moved from being part of TrickBot's toolkit to a standalone tool whose development is controlled by the Conti ransomware syndicate.

The main admin for the Conti group said that they took over TrickBot. However, as the "bot is dead" they are moving Conti from TrickBot to BazarBackdoor as the primary way of gaining initial access.

"After being "acquired" by Conti, [TrickBot leaders] are now rich in prospects with secure ground beneath them, and Conti will always find a way to make use of the available talent" - AdvIntel

(<https://www.advintel.io/post/the-trickbot-saga-s-finale-has-ai-red-but-a-spinoff-is-already-in-the-works>)

Ever since its launch, the Conti operation maintained a code of conduct that allowed it to rise as one of the most resilient and lucrative ransomware groups, unfazed by law enforcement crackdowns on its competitors (<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-29th-2021-making-arrests/>).

AdvIntel says that the group was able to run their normal cybercriminal business by adopting a “trust-based, team-based” model instead of working with random affiliates that would cause action from law enforcement due to the organizations they hit.

While TrickBot malware detections will become less common, AdvIntel's recent findings show that the operation is not finished and it just moved to a new control group that takes it to the next level with malware better suited for high-value targets.

## Related Articles:

The Week in Ransomware - February 18th 2022 - Mergers & Acquisitions (<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-18th-2022-mergers-and-acquisitions/>)

The Week in Ransomware - February 4th 2022 - Critical Infrastructure (<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-4th-2022-critical-infrastructure/>)

HHS: Conti ransomware encrypted 80% of Ireland's HSE IT systems (<https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/>)

KP Snacks giant hit by Conti ransomware, deliveries disrupted (<https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliveries-disrupted/>)

The Week in Ransomware - January 28th 2022 - Get NAS devices off the Internet (<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-28th-2022-get-nas-devices-off-the-internet/>)

