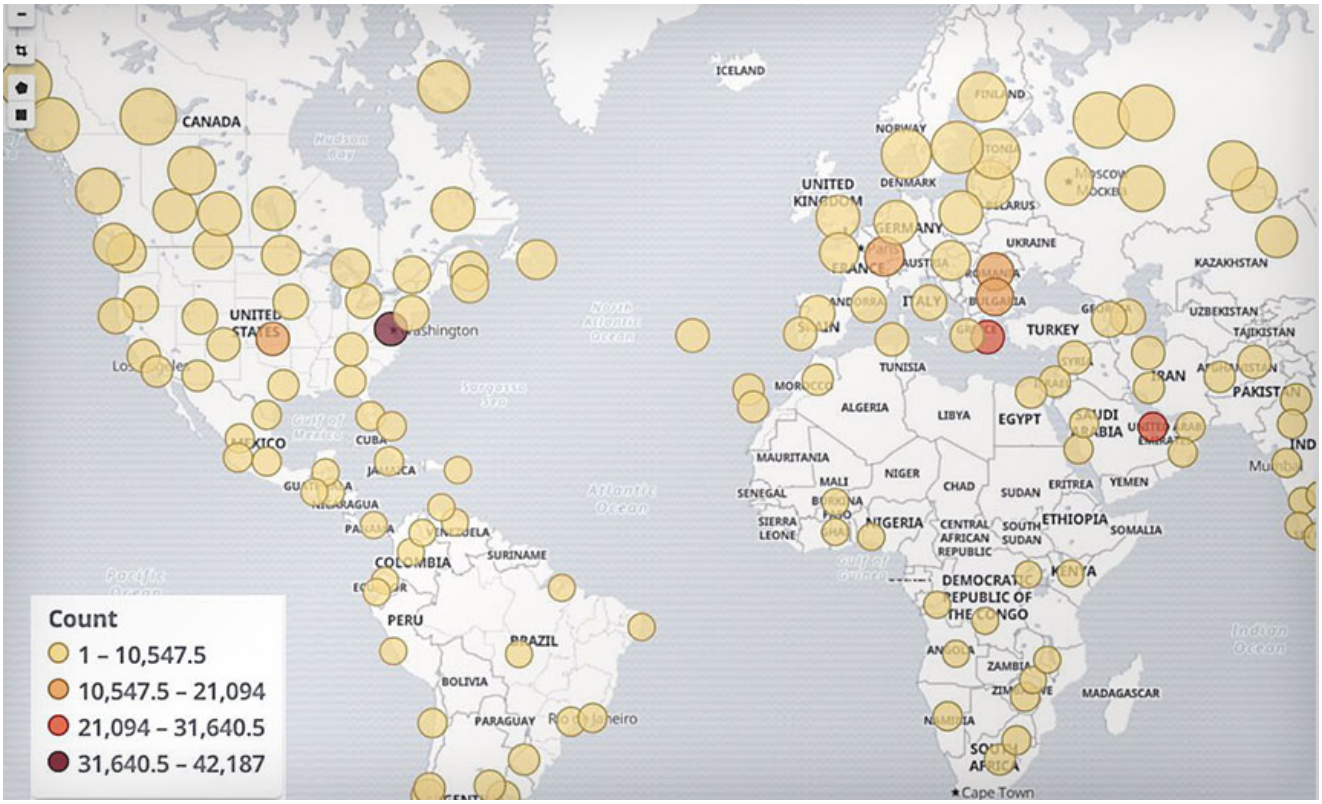
Cybercrime Moves: Conti Ransomware Absorbs TrickBot Malware

bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573

Critical Infrastructure Security , Cybercrime , Cybercrime as-a-service

TrickBot Being Used to Gain Initial Access to Victim's Network, Researchers Say Mathew J. Schwartz (euroinfosec) • February 22, 2022



TrickBot infections detected in the fall of 2020 (Source: AdvIntel)

The group that runs Conti ransomware has a new trick up its sleeve: hiring some of the top staff responsible for having developed the venerable TrickBot malware.

See Also: OnDemand | Understanding Human Behavior: Tackling Retail's ATO & Fraud Prevention Challenge

So reports New York-based threat intelligence firm Advanced Intelligence, aka AdvIntel, which says that Conti first began working with TrickBot a year ago, in an exclusive arrangement giving it initial access to numerous networks.

While some other big-name ransomware operations have disappeared since last summer, Conti lives on. Experts say this seems to be due in part to its TrickBot ties, the operation largely eschewing the use of third-party initial access brokers, and its being run as a tightly

controlled group, including training its own network penetration specialists.

Security experts say Conti-wielding attackers have likely earned profits worth hundreds of millions of dollars. As of December 2021, a Conti ransom demand averaged $657,000, according to ransomware incident response firm Coveware, based on thousands of incidents it investigated.

Conti's single biggest known haul involved a ransom worth about $34 million, AdvIntel says.

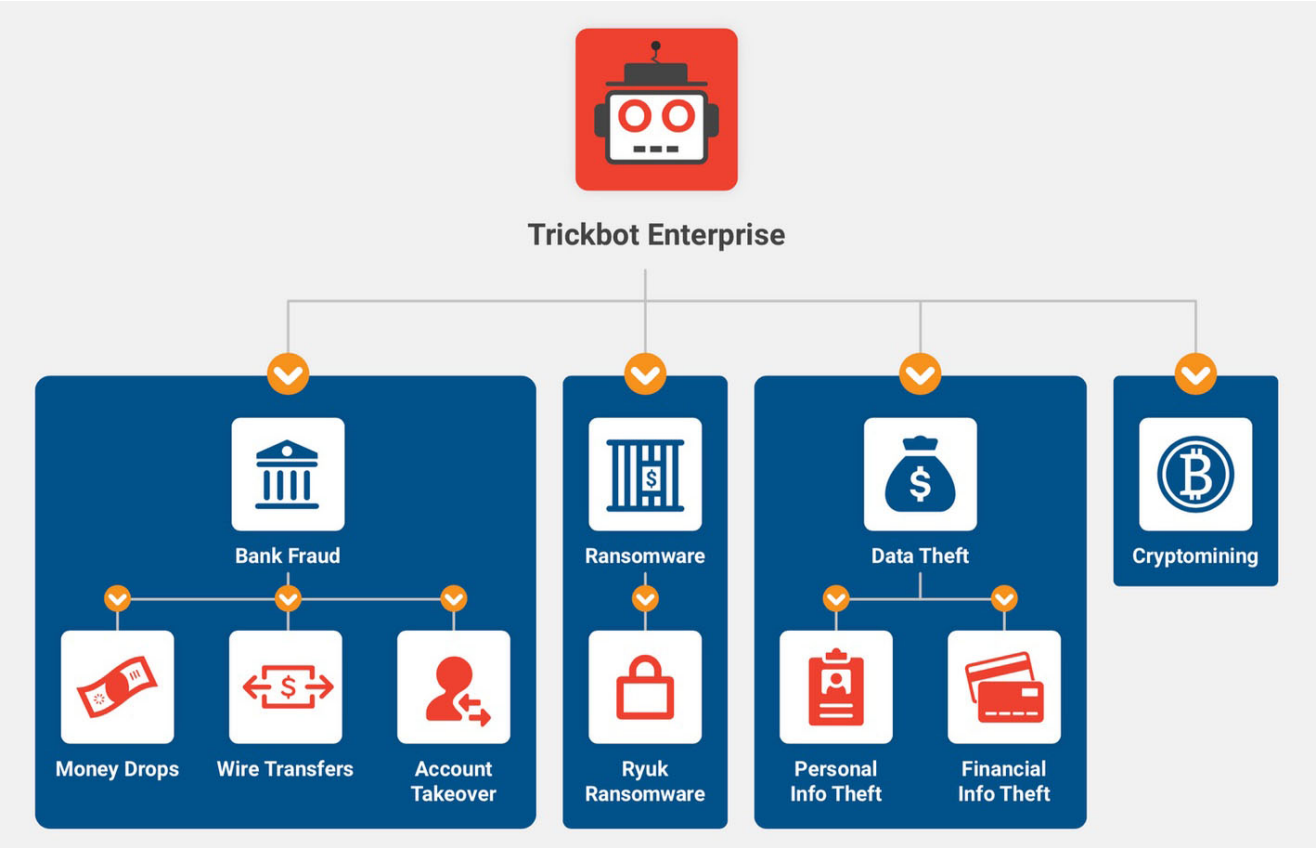
Possible Ryuk Successor - or Splinter

Conti first appeared at the end of 2019. At the time, experts said that it reused code from Ryuk, which debuted around August 2018. In June 2020, Conti attacks began surging, and in July 2020 Ryuk attacks began declining, which some read as a sign that there had been a changing of the guard. Subsequently, however, a new version of Ryuk appeared.

As security firm Emsisoft has said, Conti could be a Ryuk splinter group.

Conti has continued to evolve. In September 2020, the operation launched its own leak site, allowing it to name and shame victims and threaten to leak data via double-extortion tactics.

TrickBot, meanwhile, debuted in late 2016 as a banking Trojan, before undergoing numerous modifications. As with many other prior banking Trojans, TrickBot's developers continued to refine the code and expand its capabilities, transforming it into information-stealing malware sporting modular capabilities. In particular, after infecting a system, TrickBot was designed to serve as a downloader for installing additional modules with specific capabilities. Some of these modules have the ability to steal credentials, as well as web injection capabilities that allow the malware to spoof legitimate online banking and cryptocurrency exchange sites.



TrickBot has been used to support many different types of attacks (Source: AdvIntel)

By 2020, TrickBot was often being used in combination with two other pieces of malware: Emotet and Ryuk ransomware (see: *Emotet, Ryuk, TrickBot: 'Loader-Ransomware-Banker Trifecta'*).

In such attacks, Emotet was often used as a downloader for TrickBot, which then installed tools such as Cobalt Strike penetration testing beacons, which attackers regularly repurpose to use as malware. The goal: to try and obtain Domain Admin credentials to an organization's Active Directory, after which they could steal data and then deploy Ryuk ransomware to encrypt endpoints and hold them to ransom.

Close Ties to TrickBot

Subsequently, Conti-wielding attackers began working with TrickBot, AdvIntel says. For TrickBot-infected endpoints, the malware provides remote access, giving Conti a beachhead from which it could attempt to access other parts of the victim's network, gain administrative control in Active Directory and then deploy ransomware across the organization.

Other security firms have also highlighted apparently close ties between Conti and TrickBot. Last October, threat intelligence firm Mandiant detailed a cybercrime group with the code name FIN12 that it says has used both Conti and Ryuk ransomware and that has an affinity for targeting the healthcare sector.

Whether FIN12 is part of the core group that developed either strain of ransomware or an affiliate isn't clear. "Mandiant has only directly observed FIN12 deploy Conti ransomware in one case," it said. "Based on information from various sources, we have high confidence that the management and development staff of Conti and TrickBot are closely aligned."

In-House Approach

Some ransomware operations, or oftentimes the affiliates of these operations who use the malware to infect targets, will work with initial access brokers. Brokers sell ready access to corporate networks, allowing affiliates and others to spend more time infecting targets, versus having to find targets in the first place.

Through TrickBot, however, Conti didn't need to rely on third parties, either to provide initial access to victim networks or to distribute the malware, AdvIntel says.

"This partnership enables the Conti syndicate to answer the unfulfilled demand for initial accesses on an industrial scale, while competitor groups such as LockBit or Hive will need to rely on individual low-quality access brokers," AdvIntel reported in December 2021 (see: *HHS Warns Health Sector About LockBit 2.0 Threats - Again*).

From a business standpoint, this arrangement turned out to be a wise move.

"Its relationship with TrickBot was one of the primary reasons for the rapid rise of Conti, possibly even for its survival," Yelisey Boguslavskiy, head of research at AdvIntel, says in a recent report. "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."

Whereas ransomware-as-a-service operations typically share a massive amount of profit with affiliates - the independent contractors who infect victims often get 70% or 80% of every ransom paid - Conti instead appears to have focused on training staff and paying relatively low wages, based in part on a leaked, Russian-language training manual. This means greater profits for operators, and apparently also greater stability.

"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," Boguslavskiy reports. "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."

Boguslavskiy's analysis is based in part on internal communications AdvIntel obtained between Conti and TrickBot.

Attack on Ireland's Health Service

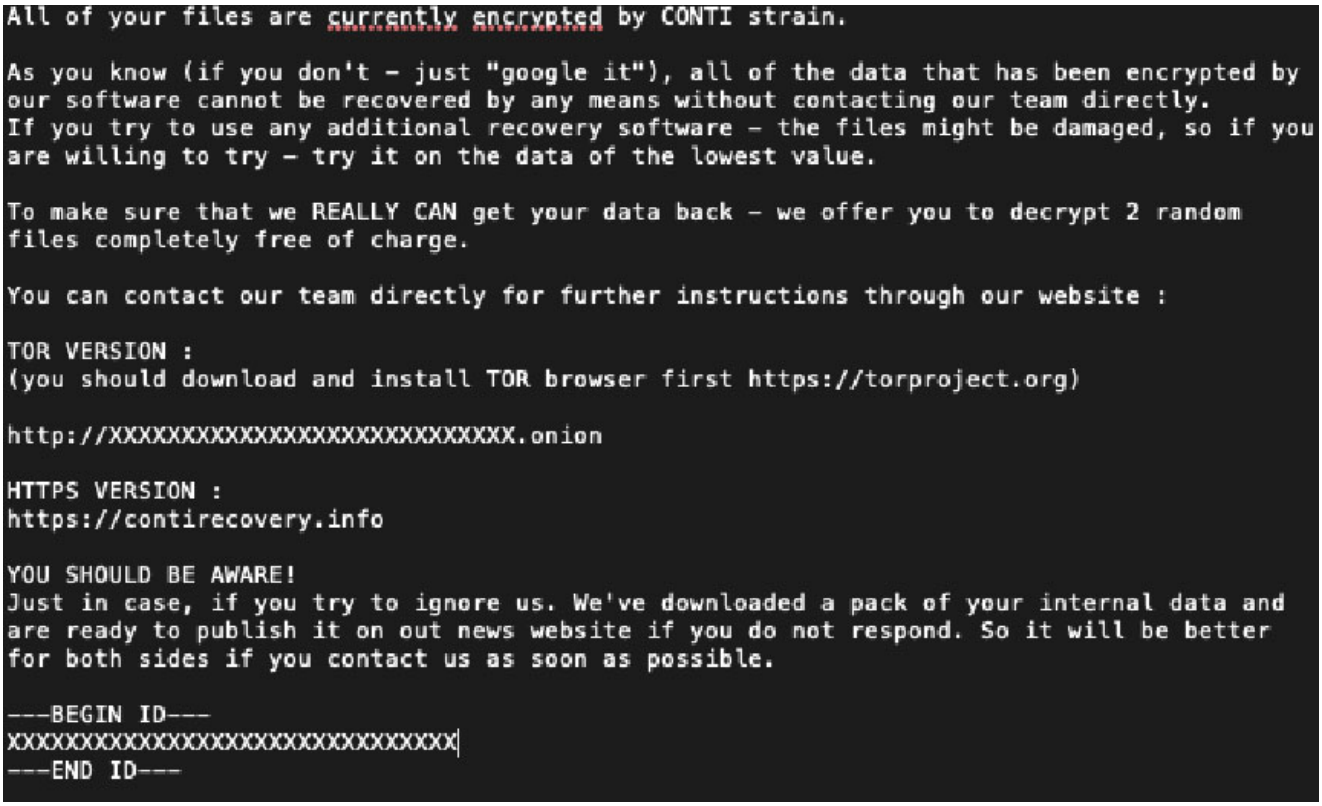
Conti, however, has not been immune to missteps. In May 2021, Conti ransomware infected systems at Ireland's Health Services Executive. While the group gave a decryptor to the Irish government without charge, the damage was already done, and patient care in the country was disrupted for months. Subsequently, the Irish government, backed by Interpol, began targeting Conti's infrastructure for disruption.

Boguslavskiy says that in the aftermath of the HSE attack, Conti reorganized. "Conti split into several semi-autonomous groups," he tells Information Security Media Group. "They do ally with each other and support each other but have the different infrastructure, especially everything which is related to communication. This way they attempt to ensure that if some components of their infrastructure are compromised, the entire organization is not affected. Additionally, after this attack, Conti became more focused on internal security audits and they are changing their servers once every several months."

Using Affiliates Carries Risks

Compared to Conti, many other ransomware operations have fared less well. After an affiliate of DarkSide hit Colonial Pipeline last May, causing Americans to panic-buy fuel, pressure on the group led to it retiring the DarkSide name, to later reboot as BlackMatter and then BlackCat, aka Alphv. REvil, aka Sodinokibi, likewise went dark after hitting big targets and then itself becoming the target of a Western law enforcement crackdown, backed by U.S. Cyber Command.

Conti, however, seems to have continued operating without interruption, despite the HSE hit. "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," Boguslavskiy reports. "And when said *random* affiliates began to *randomly* hack Western infrastructure and *randomly* blackmail Western leaders, calling down the wrath of the Russian security apparatus on their heads, Conti merely kept a clear code of conduct and continued operations as normal."



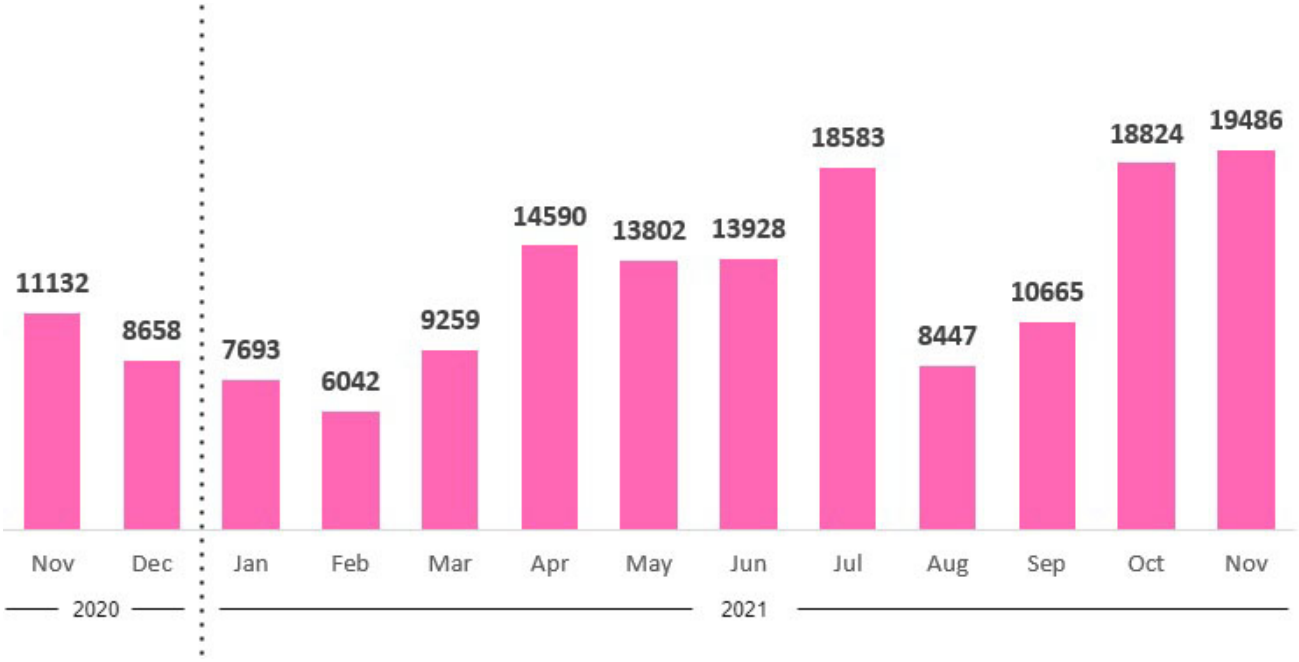
Conti ransom note (Source: Coveware)

TrickBot isn't the only third-party tool up Conti's sleeve. AdvIntel says the gang has continued to use the Bazar backdoor, aka BazarBackdoor, to gain access to targets, and to run spam email campaigns that distributed Cobalt Strike beacons to gain remote access to systems.

TrickBot: Tough to Disrupt

TrickBot has persisted despite multiple arrests and a large-scale attempt to disrupt it.

A U.S. federal indictment unsealed in June 2021 against Latvian national Alla Witte accused her of helping to design TrickBot "to capture online banking login credentials and harvest other personal information, including credit card numbers, emails, passwords, dates of birth, Social Security numbers and addresses," as well as to capture "login credentials and other stolen personal information to gain access to online bank accounts, execute unauthorized electronic funds transfers and launder the money through U.S. and foreign beneficiary accounts," and also to develop ransomware. Witte was arrested in Miami in February 2021 (see: *US Prosecutors Charge Latvian Woman in Trickbot Gang Case*).



Systems infected with Trickbot after its disruption in October 2020 (Source: Check Point Software)

TrickBot's infrastructure was disrupted in October 2020 but later returned.

If there's one piece of good news with the essential acquisition of TrickBot by Conti, it's that nothing lasts forever. AdvIntel reports that because TrickBot's indicators of compromise have become easy to detect, "Conti is no longer using it."

Instead, the group has been investing in the development of other tools. That includes making improvements to the Bazar backdoor, which was formerly part of TrickBot but is now stand-alone, AdvIntel says. Bazar appears now to be used solely to hit more high-value targets, it says.

+++

Update - Feb. 23: Added additional comments from AdvIntel's Yelisey Boguslavskiy.