

TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider


* trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider

The image shows the header of a blog post. On the left, it says 'BLOG POST' in blue. In the top right corner is the TRM logo, which consists of a starburst icon followed by the letters 'TRM'. The main title is 'Connecting Wizard Spider, Conti, and Ryuk' in a large, bold, dark blue font. Below the title is a subtitle: 'TRM blockchain analysis corroborates suspected ties between ransomware groups'. At the bottom left of the header is a blue button with the text 'READ THE POST'. On the right side of the header is a diagram showing a network of nodes connected by lines, with a blue circle highlighting a central cluster of nodes.

Insights

April 6, 2022

TRM Insights > Insights

 TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider

April 6, 2022

Key Findings

An analysis of leaked private messages of Conti group members, open-source reporting, and on-chain investigations of salary-related addresses by TRM investigators indicates ties between two ransomware groups, Conti and Ryuk. Both Conti and Ryuk also appear to be part of the Wizard Spider cybercriminal group, and are responsible for the TrickBot botnet.

- Not only do on-chain investigations indicate funds for salary paid by a Conti core member were derived from a known Ryuk ransomware address, similarities in code and other factors suggest that Conti is a rebranding of the Ryuk ransomware. Such a tactic of rebranding is widely known to be used by ransomware syndicates to cover their tracks as described by [BleepingComputer](#).

- On February 27, 2022, an individual with apparent inside access to Conti's infrastructure leaked nearly 160,000 messages from internal chats and other data shedding light on more than a year of Conti's operations, uncovering the syndicate's ecosystem as well as hundreds of crypto addresses used to extort victims and fund the group's activities. Authentication of leaks as having come from Conti infrastructure was confirmed by the threat intelligence community including [TheRecord](#).
- The leak was sparked by Conti's official statement on February 25, 2022, announcing full support to the Russian State and threatening the world with offensive operations if any Russian infrastructure is attacked as a possible response to Russia's invasion of Ukraine.

Background

Ryuk ransomware, which was active from mid-to-late 2018, was responsible for a high number of ransomware attacks resulting in millions of USD in losses. For several years, the threat intelligence community has suspected that both Ryuk and Conti ransomware were operated by a single group identified as Wizard Spider by [CrowdStrike](#) based on the similarities in code and other factors.

After Ryuk's suspected rebrand to Conti in approximately May of 2020, the ransomware continued becoming even more destructive, eventually merging with the group running the TrickBot botnet at the end of 2021 according to threat intelligence firm [AdvIntel](#). TrickBot initially emerged in 2016 as a banking Trojan designed to steal user credentials and personally identifiable information (PII). The prolific botnet then expanded its capabilities to credential harvesting, crypto mining, and gaining a foothold into the victims' systems to deploy ransomware.

TrickBot and Wizard Spider's Ryuk business relationships first followed a BaaS (Botnet-as-a-Service) model and grew to a partnership after Ryuk's rebranding to Conti. Working with TrickBot, Conti quickly became one of the most profitable and prolific ransomware syndicates. Threat researcher Jack Cable, who runs the crowdsourcing ransomware site [ransomwhe.re](#), estimated Conti as being the most profitable group through mid-2021.

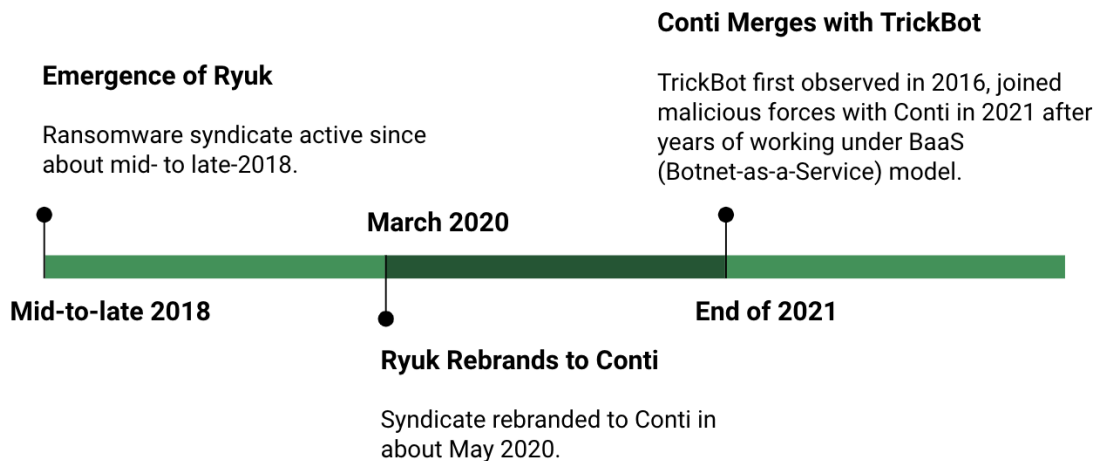


Image Source: TRM Labs

Conti Supports Russia, Issues Threats

According to the chatter observed on top-tier dark-web forums, the Russian invasion of Ukraine and the ongoing military conflict have split the Russian-speaking cybercriminal community. In dark web chatter, many cybercriminals, including ransomware threat actors, voiced support for a particular side, while others, like LockBit2.0, tried to maintain a level of neutrality. On February 25, 2022, Conti openly voiced its support for the Russian State and posted a threat to the “Western world” on its official extortion site, stating it would strike back with offensive operations if any of the Russian infrastructures is attacked.

“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

Source: Conti’s Extortion Site

Shortly after Conti’s official statement, on February 27, 2022, an individual with apparent inside access to Conti’s infrastructure leaked purported internal chat logs consisting of nearly 160,000 messages via Twitter, shedding light on more than a year of Conti’s operations. The individual who leaked the chats claimed in online tweets to be doing so in retaliation for Conti’s support of the Russian invasion of Ukraine. The leak also included hundreds of

crypto addresses, which appear to have been used in the group's illicit activity to extort victims and pay for services such as the salaries of the group's members. Authentication of leaks as having come from Conti infrastructure was confirmed by the threat intelligence community including [TheRecord](#).

Connecting Wizard Spider, Conti, and Ryuk

An analysis of the Conti leaks, specifically information within the leaked messages related to salary payments, as well as the on-chain flow of funds revealed unique insights into the operation of Wizard Spider. TRM analysts found that, unlike most ransomware syndicates, Conti implements a model of wage-based employees in addition to the percentage-based affiliate model used by traditional RaaS (Ransomware-as-a-Service) groups.

TRM on-chain analysis corroborated payments discussed on July 14, 2020; the chats show actors "Salamandra", the threat actor in charge of Conti's HR, and "Stern", a senior Wizard Spider team member, discussing a potential candidate for hire, called "bonen". bonen, a coder with 20 years of experience was hired with a salary of 150,000 Rubles per month (approximately \$2,112 USD at the time). In addition, bonen was paid 15,000 Rubles (approximately \$207 USD) for completing a test assignment. This transaction was also confirmed by TRM on-chain analysis.

The on-chain investigation also confirmed a transfer of \$85,000 USD from Stern to a team lead on one of the Conti teams operating under the alias "Mango." The transfer was made to pay for the salary of Mango's team. Mango requested the transfer from Stern on July 19, 2021, according to the leaks, so that the funds could then be split across the team of nearly 100 people consisting of pentesters, coders, OSINT investigators, and reverse engineers. Some of the funds were also set aside for payments for servers and test assignments for new hires according to the chats between Stern and Mango.

“We want to create our own cryptosystem such as etherium, polkadot, and binance smart chain,” Stern said to their team members on June 28, 2021. “We need to study the principles, code, and other things to be able to build on. And then, we will be able to integrate NFT, DEFI, DEX, and all the existing and upcoming trends,” they added.

“Do we think that any of us are gurus of Blockchain and trends? Anyone has any idea the direction we can take to develop it?”, Stern continued on July 8, 2021. Stern’s crypto aspirations were met with less enthusiasm from other threat actors such as Mango: “This is a great idea, but very complicated at the same time. Let’s be realistic, we can’t handle it on our own with so little experience and resources.”

Despite the fact that the Blockchain project still has not been developed, the threat actors’ interest in expanding into the cryptocurrency and the Defi space does raise significant concern. Based on the chats, the overall goal for Wizard Spider is to create a threat actor-friendly blockchain product. TRM assesses with a high level of confidence that would provide an additional stream of revenue as well as an internally controlled payment environment for the cybercrime underground.

Wizard Spider Likely to Remain a Threat

TRM assesses that Wizard Spider will continue to be a significant threat despite recent setbacks, notably the phasing out of their long used TrickBot tool at the beginning of February due to its high detection followed by the leak of internal Conti’s information. Wizard Spider quickly resumed their operations, posting its first victim on March 2, 2022, on their extortion site. As of March 23, 2022, the syndicate published 41 victims in total with 22 of them being US entities. These victims are likely to have been breached by Wizard Spider before the leak and it is unclear if the syndicate was able to obtain access to any new victims since then.

Based on tracking the continued level of activity and messages posted by Wizard Spider, TRM analysts assess that the group is likely to fully restore their operational capacity in the near future and will continue to run their operations under the same name and not rebrand. Unlike several other major ransomware operations, which have stated publicly and on the dark web that they do not target critical infrastructure, Conti/Ryuk has continued to target the healthcare system even during the COVID-19 pandemic as noted in the Health & Human Services report “Conti Ransomware and the Health Sector.”

Proprietary source reporting has indicated that several other ransomware groups have struggled to keep up with all of the entities they have gained access to or to develop an effective pipeline of accesses, due to a lack of employees such as programmers, negotiators, and others. Conti’s focus on hiring can be seen as evidence of Conti’s efforts to be able to run their operation on an industrial scale, bringing things like gaining access and distribution of the malware in house, allowing them to net hundreds of millions in victim payments over the years, based on TRM analysis.

Conti's hiring process consists of the interview and test assignment to measure the candidate's skills level. In order to attract new employees "Salamandra", the threat actor in charge of the group's HR, utilizes many available resources, from dark web forums to the Russian commercial job posting site hh[.]ru.

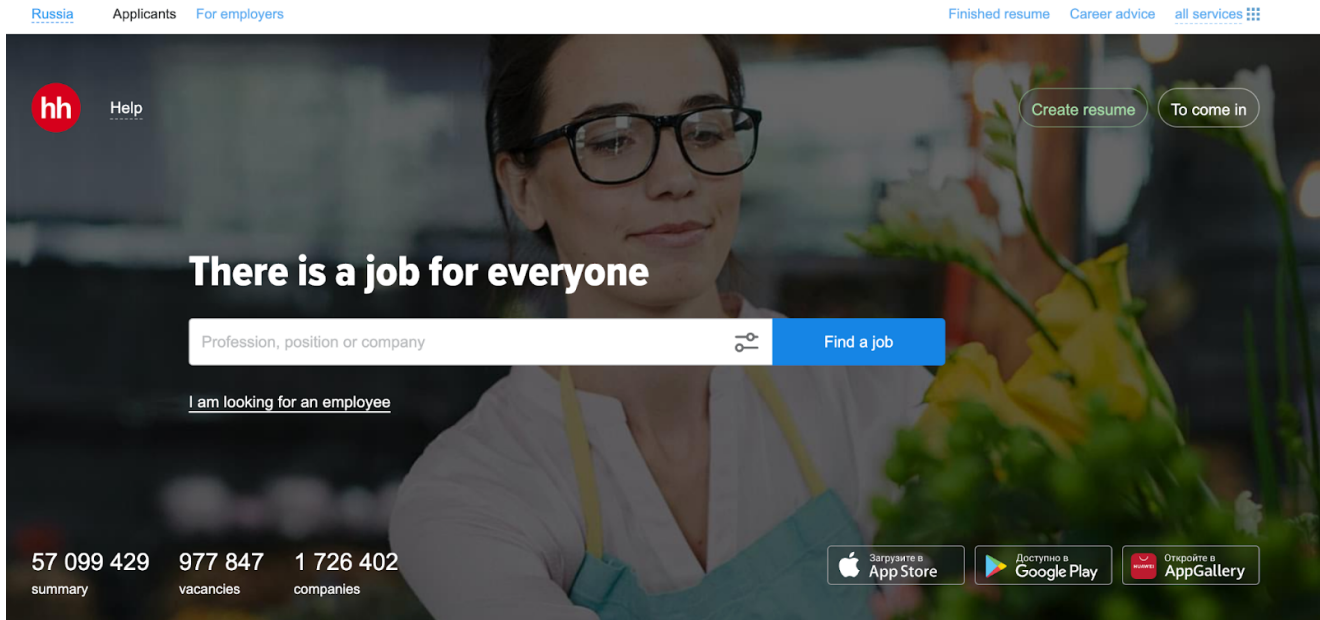


Image: Russian commercial job posting site hh[.]ru

Based on the chats, the average salary for threat actors is nearly \$2,000 USD a month. While that salary is nearly two times higher than the average salary in the IT industry in Russia according to salaryexplorer[.]com, the compensation can seem low when compared to the millions of dollars in payments that Wizard Spider received from its victims. The ability to spend a relatively small percentage of their income on salaries may be one of the reasons the core members of Wizard Spider preferred to work with full-time employees as opposed to the profit-sharing ransomware-as-a-service that most other ransomware groups currently prefer.

Outlook

TRM is monitoring the discussion of the leaked chats on the dark web to get a sense of the opinions of other threat actors about the arrangement. In the past, programmers on the dark web have leaked the source code for malware in retaliation when they felt that they had not been paid a sufficient percentage of the profit it generated, as happened in the case of the Buhtrap leak according to proprietary sources.

The research done by TRM analysts demonstrates how critical tracking the flow of funds can be in understanding the operation of cybercriminal organizations. Although cryptocurrency has made it possible for ransomware to run successful operations for years and provides a high level of return on investment for threat actors' efforts, TRM blockchain analytical tool

allows investigations to follow the flow of funds and uncover valuable intelligence that helps to connect the dots. TRM continues to monitor Wizard Spider's activity both on and off-chain to help mitigate the risk posed by Conti ransomware.

Considering Wizard Spider's statement on supporting the Russian State and sharing its political agenda, and their past willingness to target critical infrastructure, the syndicate might also pose a risk to national security due to its level of sophistication.

About TRM Labs

TRM provides blockchain intelligence to help financial institutions, cryptocurrency businesses, and public agencies detect, investigate, and manage crypto-related fraud and financial crime. TRM's risk management platform includes solutions for transaction monitoring and wallet screening, entity risk scoring - including VASP due diligence - and source and destination of funds tracing. These tools enable a rapidly growing cohort of organizations around the world to safely embrace cryptocurrency-related transactions, products, and partnerships.

TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science. To learn more, visit www.trmlabs.com.

To report a lead to Global Investigations, email us at investigations@trmlabs.com.

Sources:

- [https://www.\[.\]zdnet\[.\]com/article/conti-ryuk-joins-the-ranks-of-ransomware-gangs-operating-data-leak-sites/](https://www.[.]zdnet[.]com/article/conti-ryuk-joins-the-ranks-of-ransomware-gangs-operating-data-leak-sites/)
- [https://www.\[.\]bleepingcomputer\[.\]com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/](https://www.[.]bleepingcomputer[.]com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/)
- [https://therecord\[.\]media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/](https://therecord[.]media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/)
- [https://www.\[.\]techrepublic\[.\]com/article/top-5-ransomware-operators-by-income/](https://www.[.]techrepublic[.]com/article/top-5-ransomware-operators-by-income/)
- [https://www.\[.\]bleepingcomputer\[.\]com/news/security/us-targets-darkside-ransomware-and-its-rebrands-with-10-million-reward/](https://www.[.]bleepingcomputer[.]com/news/security/us-targets-darkside-ransomware-and-its-rebrands-with-10-million-reward/)
- [https://www.\[.\]hhs\[.\]gov/sites/default/files/conti-ransomware-health-sector.pdf](https://www.[.]hhs[.]gov/sites/default/files/conti-ransomware-health-sector.pdf)

TRM Labs, Inc.

Privacy Preference Center

When you visit websites, they may store or retrieve data in your browser. This storage is often necessary for the basic functionality of the website. The storage may be used for marketing, analytics, and personalization of the site, such as storing your preferences.

Privacy is important to us, so you have the option of disabling certain types of storage that may not be necessary for the basic functioning of the website. Blocking categories may impact your experience on the website.

Manage Consent Preferences by Category

Essential

Always Active

These items are required to enable basic website functionality.

Marketing

These items are used to deliver advertising that is more relevant to you and your interests. They may also be used to limit the number of times you see an advertisement and measure the effectiveness of advertising campaigns. Advertising networks usually place them with the website operator's permission.

Personalization

These items allow the website to remember choices you make (such as your user name, language, or the region you are in) and provide enhanced, more personal features. For example, a website may provide you with local weather reports or traffic news by storing data about your current location.

Analytics

These items help the website operator understand how its website performs, how visitors interact with the site, and whether there may be technical issues. This storage type usually doesn't collect information that identifies a visitor.

[Confirm my preferences and close](#)

Access our coverage of TRON, Solana and 23 other blockchains

Fill out the form to speak with our team about investigative professional services.

Services of interest

By clicking the button below, you agree to the [TRM Labs Privacy Policy](#).

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.

Subscribe to our latest insights

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.

You can unsubscribe at any time. Read our [Privacy Policy](#).