

Cybercrime loves company: Conti cooperated with other ransomware gangs

 intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

Software developers often depend on the collective knowledge of the industry to build their products. Whether it's through reverse engineering, poaching talent, or straight up cloning things, developers often lean on this collective knowledge to build operating systems, social media services, messaging applications or many other kinds of software.

Ransomware gangs are apparently no different. Thanks to the Conti Leaks, Intel 471 researchers found evidence that the Conti ransomware group kept a close eye on other ransomware groups and borrowed some of their techniques and best practices for its own operations. Additionally, Intel 471 also observed the Conti group's affiliates and managers cooperating with other gangs, which included the LockBit, Maze and Ryuk teams.

From reworking encryption algorithms, to copying sections of ransom notes, to using developers that worked on several different kinds of ransomware, Intel 471 found that Conti's operations were powered by information gleaned from competitors.

Ryuk

The Conti and Ryuk ransomware strains have widely been attributed to the same group, with Ryuk likely serving as a predecessor to Conti.

The metamorphosis of this strain has been debated for some time. Some research hypothesizes that Ryuk ransomware operators initially joined the Conti team as its own division in order to use TrickBot to distribute Ryuk, while others believe Conti was just a rework of Ryuk.

However the metamorphosis occurred, it's clear from the Conti Leaks chats that top-level Conti operatives had direct access to actors who were behind Ryuk. Intel 471 researchers found conversations tied to one of Conti's senior managers that contained multiple references to the group behind Ryuk.

For example, on June 23, 2020, the senior manager discussed a Bleeping Computer article where researchers pointed at the Ryuk ransomware gang's slowdown in operations. The manager told another top associate that the Ryuk gang's operations would soon return to normal (**Ed. Note:** *Handles have been changed to mask true identities*):

[bluejay]: "Kremez told us that Ryuk infections have slowed down lately, as the threat actor is likely in a vacation kind of state."
[bluejay]: =)
<...>
[puffin]: Ryuk should get back from holidays soon
[puffin]: he'll take all the bots that will be available
[puffin]: it's he who needs 5k companies

On July 16, 2020, the two actors revealed their plans to use money earned from Ryuk ransomware campaigns to cover rent and other expenses (translated from Russian):

[bluejay]: July and August 26 + a new office for the autumn, this means spending more than a couple of thousands
[bluejay]: in any case, it will be necessary to make this money back
[bluejay]: and, as far as I understand, this will be done via Ryuk
[puffin]: yes, among other things

On Aug. 26, 2020, the two actors discussed compensation and recruitment issues pertaining to the Ryuk team (translated from Russian):

[puffin]: Re Ryuk. Just give him five people. I can also allocate some budget
[bluejay]: Re Ryuk: we'll start next week, then my people from the office will establish cooperation with his people within 1-2 weeks, like this: they get the objects > Ryuk's people immediately start working on them > if something goes wrong or Cobalt Strike doesn't load: they solve the issue or infect some other entry points, maybe. We'll start working gradually in this way, and by the end of the month, we'll step back from these processes with Ryuk: let his people and mine work with each other directly
[bluejay]: in October, if everything goes according to Wood Duck's plan, we provide targets for Ryuk and we provide targets for our hackers (the office)...Wood Duck will bring in someone else important from the main team plus office employees (there will be 30-40 people in total in three offices) who will receive salaries + bonuses.

These chats, among others, show that high-level Conti managers were knowledgeable about Ryuk ransomware operations and most likely had direct access to the threat actors using it.

Maze

Intel 471 researchers found chats that revealed Conti's alleged coder claimed to have copied features from Maze ransomware while developing Conti.

On July 17, 2020, the head developer had a conversation with the senior manager, claiming to have changed the Conti's cryptographic algorithm from the AES-256 block cipher to the ChaCha20 stream cipher, which increased encryption speed:

<...>
[sparrow]: Hi, regarding the ransomware, I changed the algorithm to chacha20, it's several times faster than AES. I also introduced pattern encryption, which increased the encryption rate... So, the encryption rate is now almost three times higher after the algorithm change.
[puffin]: what algorithm do Maze and Ryuk use?
[sparrow]: Maze uses chacha20, Ryuk uses AES 256.
<...>

On July 8, 2020, another top developer communicated with the senior manager, claiming that a Maze ransomware developer provided access to the group's administrative panel.

<...>
[Wood Duck]: I chatted with the Maze owner and developer... Well, I'll tell you more when you arrive
[Wood Duck]: just in case, Maze's admin panel, a new build: [REDACTED].onion
<...>

Also in early July 2020, Conti group members revealed they used Maze ransomware as a temporary stopgap while Conti was in development. (translated from Russian):

<...>
[oriole]: Hi, man. As far as I understood, Wood Duck took another ransomware. Looks like it's Maze. He says he's been testing it overnight.
<...>

A few weeks later, Conti was in steady use, becoming one of the most active ransomware strains in the latter half of the year.

LockBit 2.0

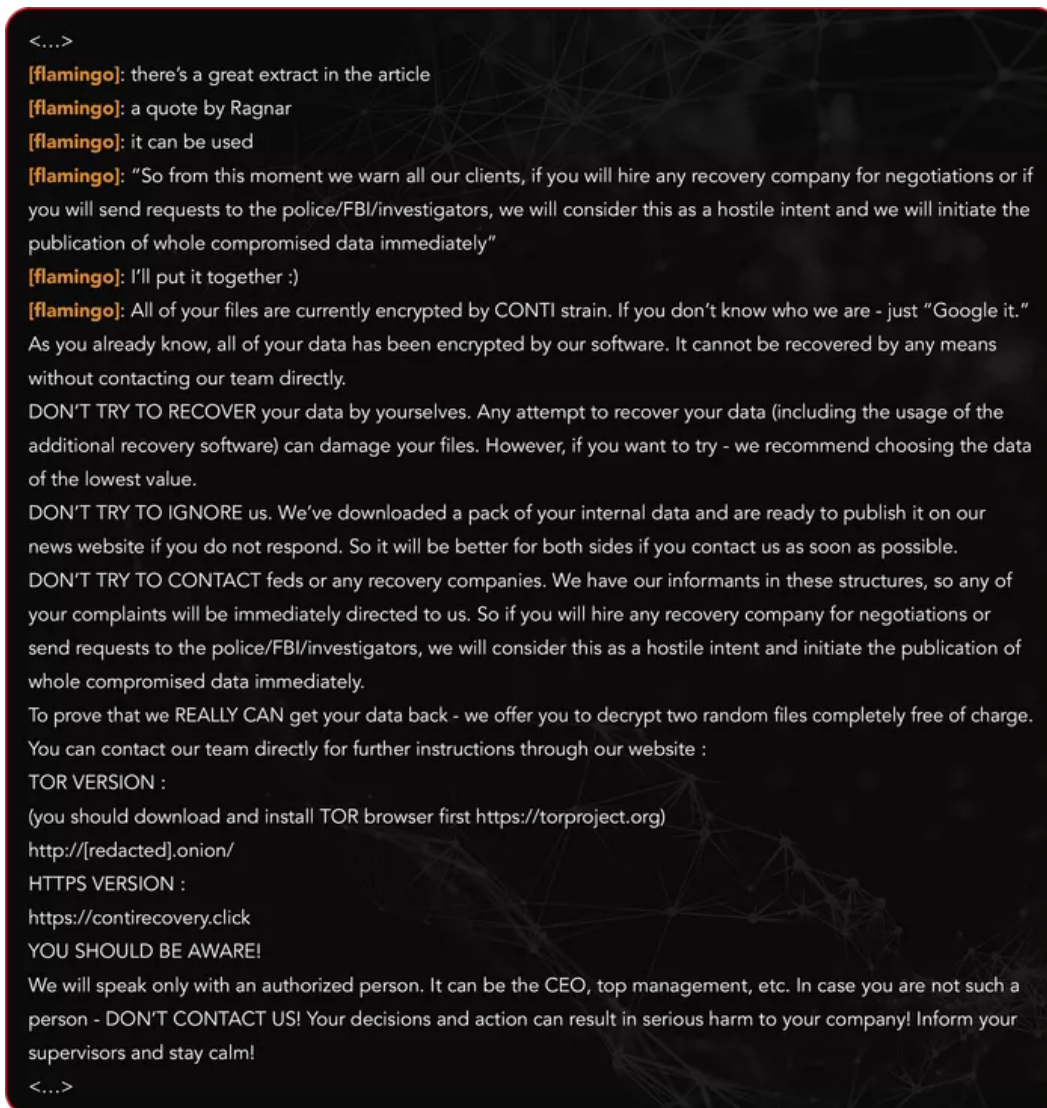
Our researchers found that in November 2021, two high-level Conti managers discussed a partnership with LockBit 2.0. The two managers apparently initially disagreed on the partnership's details, later clarifying it in a leaked conversation:

[macaw]: Looks like we didn't really understand each other regarding LockBit. You said they need networks to work with, but he's saying he actually needs a trojan. :) I didn't get what terms and conditions he's talking about. I gave him your contact details here, he said he'll contact you himself
[macaw]: on what terms should I give him the trojan if I do?
[macaw]: I told him that we usually take a share of the bots with networks, but I don't know which share exactly :
[puffin]: tell him 20 percent. Let's try it like this
[macaw]: we take 20% of the bots with networks, okay

This conversation lines up with what a LockBit 2.0 representative shared on an underground forum in April 2022, where they admitted that they had been in contact with Conti representatives primarily due to interest in using TrickBot.

Ragnar Locker

On Sept. 27, 2021, Conti's open source intelligence (OSINT) team leader had a conversation that revealed he updated the group's ransom note by copying a portion of the text from the Ragnar Locker ransom note.



<...>

[flamingo]: there's a great extract in the article

[flamingo]: a quote by Ragnar

[flamingo]: it can be used

[flamingo]: "So from this moment we warn all our clients, if you will hire any recovery company for negotiations or if you will send requests to the police/FBI/investigators, we will consider this as a hostile intent and we will initiate the publication of whole compromised data immediately"

[flamingo]: I'll put it together :)

[flamingo]: All of your files are currently encrypted by CONTI strain. If you don't know who we are - just "Google it." As you already know, all of your data has been encrypted by our software. It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. However, if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies. We have our informants in these structures, so any of your complaints will be immediately directed to us. So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge. You can contact our team directly for further instructions through our website :

TOR VERSION :

(you should download and install TOR browser first <https://torproject.org>)

[http://\[redacted\].onion/](http://[redacted].onion/)

HTTPS VERSION :

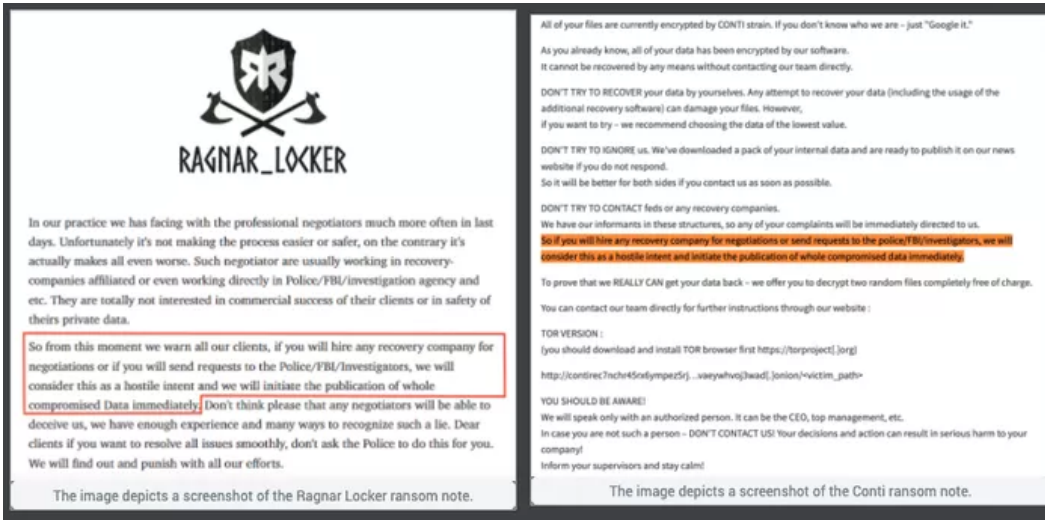
<https://contirecovery.click>

YOU SHOULD BE AWARE!

We will speak only with an authorized person. It can be the CEO, top management, etc. In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company! Inform your supervisors and stay calm!

<...>

Here is the comparison of what victims would get from each ransom note.



Ransomware gangs do not operate in a vacuum. While each gang wants to make as much money as possible, there is a level of cooperation and partnership that each gang uses to ultimately boost their ill-gotten gains. While legitimate companies are also profit-driven, they will often create partnerships or collaborate with each other as a way to be successful. Given all of the other ways ransomware gangs have followed a legitimate business model, it should not be surprising that they would strike accords or lean on each other in order to make as much money as possible.