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 re-work 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):

Conti Dialog image1

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):

Conti Dialog image2

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

Conti Dialog image3

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:

Conti Dialog image4

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.

Conti Dialog image5

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):

Conti Dialog image6

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:

Conti Dialog image7

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.

Conti Dialog image8

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

Screen Shot 2022 04 27 at 2 29 26 PM

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.