Conti vs. Monti: A Reinvention or Just a Simple Rebranding?

intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding

It's a familiar sounding story. A young organization with a hot software product and skyrocketing revenues, employee hiring fairs, lucrative salaries, bonuses and team recognition programs. But this story is not about a vibrant tech company in Silicon Valley or Austin; rather it is a real story of a criminal organization that manages and supports the insidious Conti ransomware.

Conti is advanced ransomware that first emerged in early 2020. It uses a bespoke encryption routine to identify and encrypt files quickly and efficiently, making it especially dangerous. The Conti gang uses a "double-extortion" technique, which encrypts victims' data and demands payment. They also take copies of the victims' data, permitting them to expose or sell the data if the victim refuses to pay.

The operators behind the malware are a high-profile ransomware group responsible for multiple high-impact attacks. They are otherwise known as Wizard Spider and may be part of the wider Trickbot cybercrime syndicate. Reportedly, they are based in Russia and support the Russian government's agenda, including the war in Ukraine. The malware is distributed under a Ransomware as a Service (RaaS) model. The Conti gang distributes access to its malware to "affiliates" in exchange for a share of collected ransom payments. This aspect allows them to scale operations. Some reports cite the Conti gang operates as a modern start-up with salaries, bonuses and employee recognition awards.

In just a few years, the Conti ransomware has caused damage and disruption globally. Conti has targeted hospitals, governments, financial institutions and enterprises including Snapon, Shutterfly, the Irish healthcare system and several agencies of the Costa Rican government. The FBI describes the Conti ransomware as “the costliest strain of ransomware ever documented.” It estimates more than 1,000 victims have suffered Conti-associated attacks and total victim payouts exceed USD $150 million as of early 2022.

The end of Conti

As with any organization, disgruntled employees sometimes turn against their employers. In March 2022, a Ukrainian researcher working for the Conti gang went rogue. Thought to be unhappy with the Conti gang’s Russian government affiliation and its support for the war in Ukraine, the researcher leaked 393 files containing over 60,000 internal messages from the Conti gang's private chat server. The leaked information has been dubbed the Conti Leaks and includes other sensitive data about the gang's operations, tools, and costs.

Since then, infosec researchers everywhere have been sifting through this massive data treasure trove. The internal breach has proved tremendously costly for the Conti gang, leaving them terribly exposed.

To add to their pain, in May 2022 the Rewards for Justice group within the US State Department announced new bounties of up to USD $10 million for anyone who provides useful information about individual members of Conti. Specifically, the agency wants to know about five specific gang members: actors using the handles Professor, Reshaev, Tramp, Dandis, and Target.

On May 19, 2022, the admin panel of the Conti ransomware gang's official website shut down. Shortly thereafter, in the wake of the Conti Leaks and (perhaps) the Rewards for Justice announcement, the gang shut down its attack infrastructure.

Out with the old…the emergence of Monti

In recent months, Conti’s activities have quieted. Some researchers have suggested that Conti’s diminished actions result from a rebranding exercise like many ransomware strains have done before, with a number of Conti gang members likely involved. Other reports indicate that other RaaS operations have employed ex-Conti operators including Karakurt and BlackByte.

Though there is no iron-clad evidence of Conti rebranding as Monti, Conti source was leaked publicly in March 2022. Consequently, it is possible that anybody could use the publicly available source code to create their own ransomware based on Conti. This could be the case with Monti from our analysis of the disassembled code. Monti's entry point is very

similar to Conti's, as seen below. As such, Monti could be a rebrand of Conti or simply a new ransomware variant that has been developed using the leaked source code mentioned above.

Whether this is Conti being rebranded as Monti, in a bid to mock the former strain, or it is just another new ransomware variant on the block, it is likely we will continue to see this new variant impact businesses globally. Nevertheless, using publicly available binaries to create a new ransomware or relaunch an old one will hopefully give defenders an edge when dealing with Monti as it evolves.