# Related news

cyberscoop.com/ransomware-gang-conti-bounced-back/

March 7, 2022

financial

## Ransomware gang Conti has already bounced back from damage caused by chat leaks, experts say

(Getty Images)
Written by Suzanne Smalley
Mar 7, 2022 | CYBERSCOOP
A Twitter account known as ContiLeaks debuted to much fanfare in late February, with people around the globe watching as tens of thousands of leaked chats between members of the Russia-based ransomware gang Conti hit the web.

In the days after the leaks, many celebrated what they thought would be a devastating blow to Conti, which a Ukrainian security researcher had apparently punished by leaking the internal chats because the gang threatened to “strike back” at any entities that organized “any war activities against Russia.”

But ten days after the leaks began, Conti appears to be thriving.

Experts say the notorious ransomware gang has pivoted all too easily, replacing much of the infrastructure that was exposed in the leaks while moving quickly to hit new targets with ransom demands. According to Vitali Kremez, CEO of the cybersecurity firm AdvIntel, by Monday morning Conti had successfully completed two new data breaches at U.S.-based companies.

“Conti is back and still operational and will pursue more targets,” Kremez said. “They’re safe and sound.”

Kremez and other experts said that in the days after the chats first leaked on Feb. 27, Conti may have been back on its heels, but it was never fully disabled. The gang’s leadership made a significant effort in the early days following the leaks to transition its infrastructure that was exposed in the hacks to new systems, which slowed down ransomware activity initially, experts said. That interregnum has come to an end.

Allan Liska, a threat analyst at Recorded Future, said that because so many victims do not disclose ransomware attacks it is hard to know if Conti was totally inactive in the first few days after the leaks, but he said his firm had “definitely noticed a slowdown” in activity from Conti.

Liska said nothing was posted to Conti’s extortion sites — where the gang publicizes data belonging to users who don’t pay ransoms — for a few days after the leaks began. However, Liska said Conti doesn’t post daily to the site even in normal circumstances so it is hard to know for sure if the two events are linked.

The threat analysis community has been buzzing about Conti’s increasing network activity in the past few days, Liska said. While Liska was unaware of the new data breaches disclosed by Kremez, he said he has heard about a recent increase in “attempted breaches or phishing emails being sent, things like that, that are indicative that they’re [Conti] still trying to gain access.”

“The botnet and the command and control activity is starting to tick back up,” Liska said.

Much of Conti’s infrastructure was down in the initial days after the chats leaked — at least 25 different servers were exposed in the leaks, according to Liska, and those remain down. But Liska said Conti’s “command and control” server is very large and not all of it has fallen.

Liska said he estimates that Conti has between 50 and 100 servers running at any time, making the 25 or so that have been taken down a survivable injury. In recent days, Liska said, Conti has used the same software that powered the old infrastructure and simply moved everything to new Internet Protocol addresses.

## A history of resilience

Many experts said they are unsurprised by Conti's staying power. As a collective whose members are highly skilled and anonymous even to each other, nothing short of a law enforcement takedown will truly put them out of business, experts said.

John Shier, a senior security adviser at the hardware and software security firm Sophos, said that other ransomware collectives have bounced back from seemingly devastating blows.

"Whenever one of these groups gets gets disrupted, the temptation is to celebrate a little bit, but there's always going to be that okay, well, what's next?" Shier said. "Where are they going to pop up next, under what kind of new model potentially are they going to pop up? Because these groups can be fairly resilient."

Shier said Conti's bitcoin wallet reportedly had about $2 billion in it, a figure he called "staggering." It's also a figure that compels groups like Conti to rise from the dead. Emsisoft threat analyst Brett Callow put it bluntly: Ransomware, he said, is "so massively profitable it isn't going to go away quickly or easily."

Liska and Shier agreed on one thing that will likely change as a result of the leaks: Cybercriminals may be more careful about taking on as many affiliates as they have in the past to counter security risks. In the affiliate ransomware model, gangs loan their malware to other hackers in exchange for a share of profits.

The Conti chat leaker is known to be a Ukrainian security researcher and not an affiliate, according to Kremez. But seeing the ease with which the Conti chats were leaked, as well as the damage they caused, will doubtlessly cause more gangs to think twice about sharing sensitive information with far-flung affiliates whom they don't know as well as core gang members, Shier and Liska predicted.

Shier said he was struck by the fact that nearly 70 people participated in one of the Conti chats.

"That's a lot of people and not all of them were likely to be Russian citizens living in Russia," Shier said. "If the people who are the principles behind Conti believe in their geopolitical agenda of supporting Russia, and they want to prevent others who don't share that view within their group from causing harm to the group, I can only see them severing ties with them. They can still be successful without affiliates — they just won't make as much money."

Even if Conti sheds affiliates and scales down in response to the leaks, the gang won't be put out of business until the Russian government pursues criminal charges or allows the U.S. government to do so, experts said.

"The core members that are in Russia, are going to be insulated from any kind of prosecution or anything that comes from outside of Russia," Shier said. "Nothing will be the end of them until the Russian government allows them to be investigated and prosecuted."

Shier said it is possible Conti will rebrand under another name, but the group will live another day with the same leadership it has now.

“I don’t see there being any kind of incentive for the Russian government to do anything with them right now,” Shier said.

Just Monday, Shier said, Conti posted four new data dumps for entities which didn’t pay ransoms on their extortion site. There were other data dumps posted on Saturday and Sunday, he said.

Kremez said Conti may lose some members, but they will revamp and come back stronger because they “learn from mistakes.”

Kremez said that in some ways the leaked chats will hurt the effort to snuff out Conti. He said he expects gang members will change aliases so they will be more difficult to track. The gang will update its infrastructure. It will cut affiliates who are deemed too risky.

“They will reemerge more powerful and better than ever and more bulletproof,” Kremez said. “They will adapt, they will improve, some members will relocate. But they [Conti] will definitely not be pushed out of the market.”