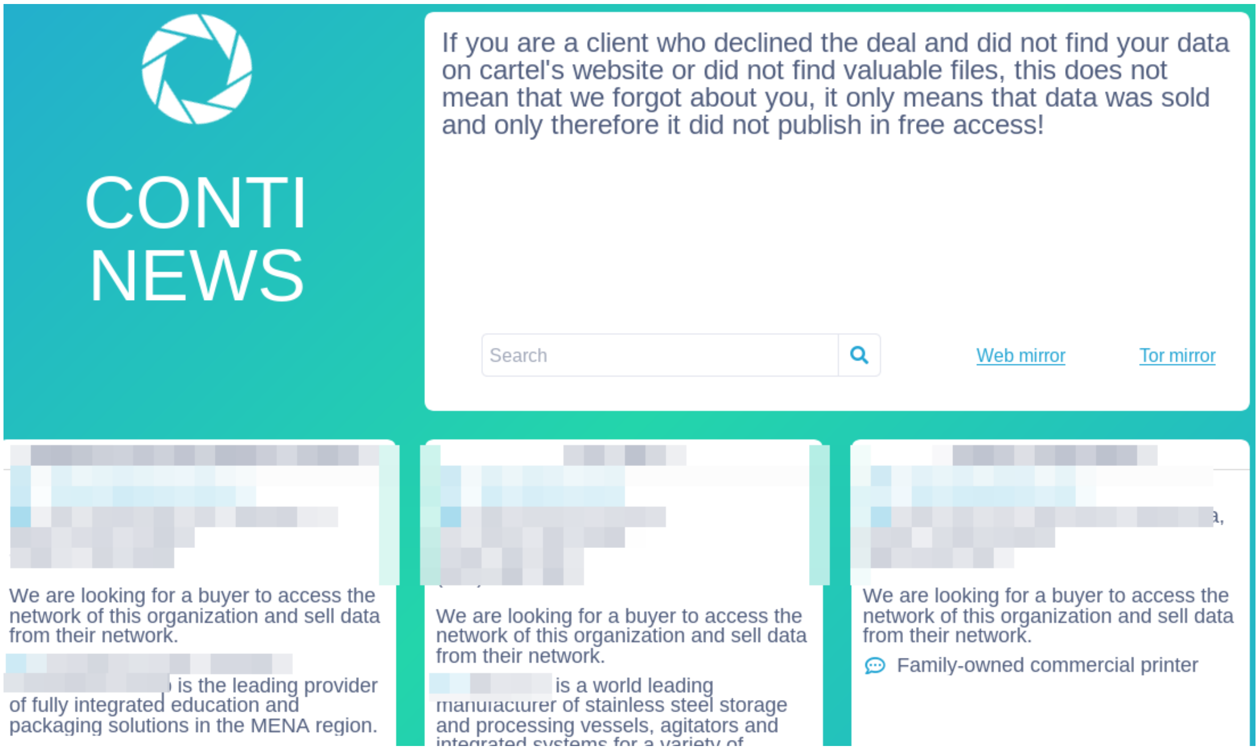
Conti Ransom Gang Starts Selling Access to Victims

krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/

The **Conti** ransomware affiliate program appears to have altered its business plan recently. Organizations infected with Conti's malware who refuse to negotiate a ransom payment are added to Conti's victim shaming blog, where confidential files stolen from victims may be published or sold. But sometime over the past 48 hours, the cybercriminal syndicate updated its victim shaming blog to indicate that it is now selling access to many of the organizations it has hacked.



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

[redacted]

We are looking for a buyer to access the network of this organization and sell data from their network.

[redacted] is the leading provider of fully integrated education and packaging solutions in the MENA region.

[redacted]

We are looking for a buyer to access the network of this organization and sell data from their network.

[redacted] is a world leading manufacturer of stainless steel storage and processing vessels, agitators and integrated systems for a variety of

[redacted]

We are looking for a buyer to access the network of this organization and sell data from their network.

Family-owned commercial printer

A redacted screenshot of the Conti News victim shaming blog.

"We are looking for a buyer to access the network of this organization and sell data from their network," reads the confusingly worded message inserted into multiple recent victim listings on Conti's shaming blog.

It's unclear what prompted the changes, or what Conti hopes to gain from the move. It's also not obvious why they would advertise having hacked into companies if they plan on selling that access to extract sensitive data going forward. Conti did not respond to requests for comment.

"I wonder if they are about to close down their operation and want to sell data or access from an in-progress breach before they do," said **Fabian Wosar**, chief technology officer at computer security firm **Emsisoft**. "But it's somewhat stupid to do it that way as you will alert the companies that they have a breach going on."

The unexplained shift comes as policymakers in the United States and Europe are moving forward on efforts to disrupt some of the top ransomware gangs. *Reuters* recently reported that the U.S. government was behind an ongoing hacking operation that penetrated the computer systems of REvil, a ransomware affiliate group that experts say is about as aggressive and ruthless as Conti in dealing with victims. What's more, REvil was among the first ransomware groups to start selling its victims' data.

REvil's darknet victim shaming site remains offline. In response, a representative for the Conti gang posted a long screed on Oct. 22 to a Russian language hacking forum denouncing the attack on REvil as the "unilateral, extraterritorial, and bandit-mugging behavior of the United States in world affairs."

"Is there a law, even an American one, even a local one in any county of any of the 50 states, that legitimize such indiscriminate offensive action?" reads the Conti diatribe. "Is server hacking suddenly legal in the United States or in any of the US jurisdictions? Suppose there is such an outrageous law that allows you to hack servers in a foreign country. How legal is this from the point of view of the country whose servers were attacked? Infrastructure is not flying there in space or floating in neutral waters. It is a part of someone's sovereignty."

Conti's apparent new direction may be little more than another ploy to bring victim companies to the negotiating table, as in "pay up or someone will pay for your data or long-term misery if you don't."

Or maybe something just got lost in the translation from Russian (Conti's blog is published in English). But by shifting from the deployment of ransomware malware toward the sale of stolen data and network access, Conti could be aligning its operations with many competing ransomware affiliate programs that have recently focused on extorting companies in exchange for a promise not to publish or sell stolen data.

However, as **Digital Shadows** points out in a recent ransomware roundup, many ransomware groups are finding it difficult to manage data-leak sites, or hosting stolen data on the dark web for download.

After all, when it takes weeks to download one victim's data via Tor — if indeed the download succeeds at all — the threat of leaking sensitive data as a negotiation tactic loses some of its menace. It's also a crappy user experience. This has resulted in some ransomware groups exposing data using public file-sharing websites, which are faster and more reliable but can be taken down through legal means quite quickly.

Data leak sites also can offer investigators a potential way to infiltrate ransomware gangs, as evidenced by the recent reported compromise of the REvil gang by U.S. authorities.

"On 17 Oct 2021, a representative of the REvil ransomware gang took it to a Russian-speaking criminal forum to reveal that their data-leak sites had been 'hijacked'," Digital Shadows' **Ivan Righi** wrote. "The REvil member explained that an unknown individual accessed the hidden services of REvil's website's landing page and blog using the same key owned by the developers. The user believed that the ransomware gang's servers had been compromised and the individual responsible for the compromise was 'looking for' him."

A recent report by Mandiant revealed that **FIN12** — the group believed to be responsible for both Conti and the **Ryuk ransomware operation** — has managed to conduct ransomware attacks in less than 3 days, compared to more than 12 days for attacks involving data exfiltration.

Seen through those figures, perhaps Conti is merely seeking to outsource more of the data exfiltration side of the business (for a fee, of course) so that it can focus on the less time-intensive but equally profitable racket of deploying ransomware.

"As Q4 comes near, it will be interesting to see if issues relating to managing data leak sites will discourage new ransomware groups [from pursuing] the path of data-leak sites, or what creative solutions they will create to work around these issues," Righi concluded. "The Ryuk ransomware group has proven itself to remain effective and a top player in the ransomware threat landscape without the need for a data-leak site. In fact, Ryuk has thrived by not needing a data leak site and data exfiltration."