Conti gang threatens to dump victim data if ransom negotiations leak to reporters

By Catalin Cimpanu

Published: 2022-12-16 · Archived: 2026-04-05 13:45:57 UTC

The Conti ransomware gang has published a rare public statement today threatening hacked companies that they will leak their stolen files if details or screenshots of the ransom negotiations process are leaked to journalists.

These ransom negotiations usually take place after Conti (or any other ransomware gang) breaches a company and encrypts their files. A ransom note is left on affected desktops, with instructions on how the victim could contact the attackers.

Typically, ransomware gangs prefer leaving an email address where the victim can reach out, but more often than not, they provide a unique URL to a so-called "*payment site*" where victims are asked to log in and talk to the attackers via a web-based chat feature.

If an employee of the attacked company uploads a copy of the ransom note or the ransomware binary on malware-scanning portals like VirusTotal, the details included in these ransom notes, including links to the web-based chat feature, can also be discovered by security researchers, who often access these negotiations pages and sometimes share them on social media.

Over the past few years, news outlets specialized in cybersecurity coverage have often worked with security researchers to find links to these secret chats in files uploaded on VirusTotal.

Reporters then used the screenshots to reveal details about ransomware incidents — especially when the hacked organization wasn't upcoming with such information in the first place.

Most of these screenshots typically show a banal negotiations process between the ransomware gangs and the victim, with the two working to agree on a final ransom fee, and then the ransomware gang sharing Bitcoin addresses where they ask for the payment.

However, other screenshots have also shown information about the attack itself, how the victim was breached, what kind of data the attackers stole from the victim's network, threats against a victim and its employees, or how companies were trying to disguise payments to groups sanctioned by the US Treasury.

Today, many ransomware gangs like to delude themselves that they are running a "professional backup & recovery" or "penetration testing" fantasy business. These leaked screenshots show the true nature of their actions, all being nothing more than a good old extortion scheme.

Conti angered of recent JVCKenwood negotiations leak

Across the years, screenshots from almost all ransomware gangs' negotiations have leaked on social media or have been shared with reporters.

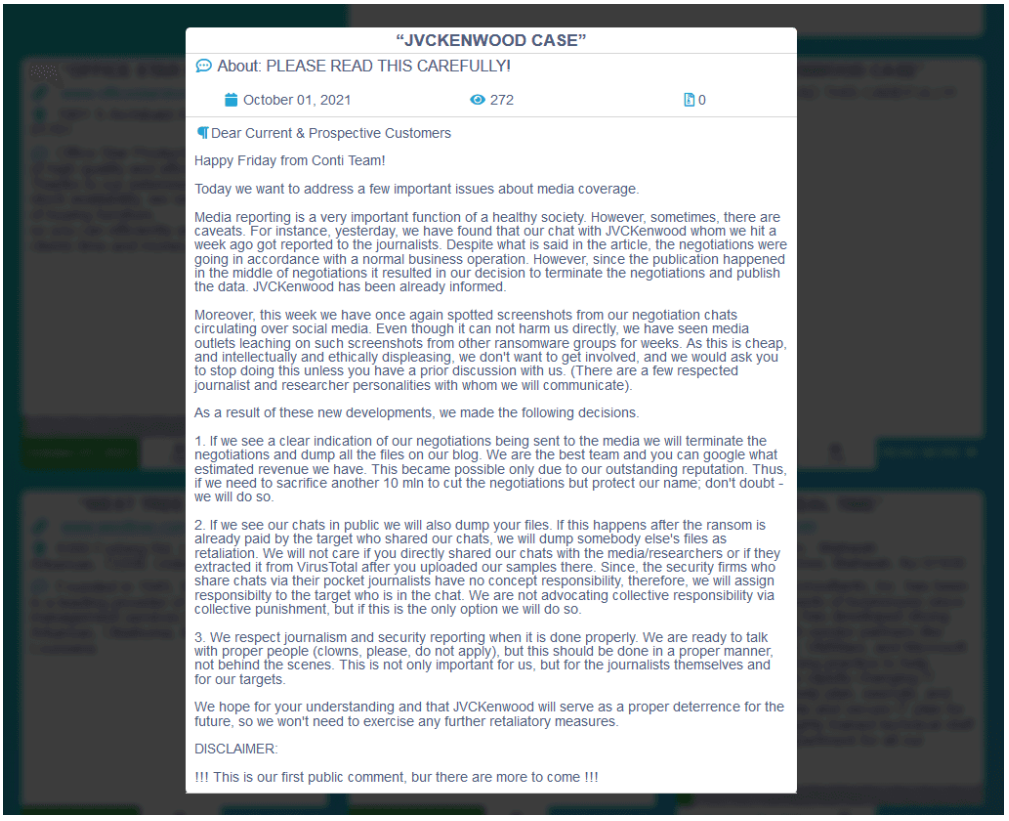
But in a message posted on its blog today, the Conti gang said that it would not tolerate incidents where screenshots of its negotiations process are leaked online anymore.

Although no particularly "damaging" screenshot leak occurred, the Conti group cited its recent attack against Japanese electronics maker JVCKenwood as the reason it has taken this step. In Conti's own words, below:

> For instance, yesterday, we have found that our chat with JVCKenwood whom we hit a week ago got reported to the journalists. Despite what is said in the article, the negotiations were going in accordance with a normal business operation. However, since the publication happened in the middle of negotiations it resulted in our decision to terminate the negotiations and publish the data. JVCKenwood has been already informed. Moreover, this week we have once again spotted screenshots from our negotiation chats circulating over social media.

As a result, the Conti gang said it is introducing new rules meant to penalize victims or security researchers who leak screenshots of its ransom negotiations chats to reporters:

1. If we see a clear indication of our negotiations being sent to the media we will terminate the negotiations and dump all the files on our blog. We are the best team and you can google what estimated revenue we have. This became possible only due to our outstanding reputation. Thus, if we need to sacrifice another 10 mln to cut the negotiations but protect our name; don't doubt - we will do so.
2. If we see our chats in public we will also dump your files. If this happens after the ransom is already paid by the target who shared our chats, we will dump somebody else's files as retaliation. We will not care if you directly shared our chats with the media/researchers or if they extracted it from VirusTotal after you uploaded our samples there. Since, the security firms who share chats via their pocket journalists have no concept responsibility, therefore, we will assign responsibilty to the target who is in the chat. We are not advocating collective responsibility via collective punishment, but if this is the only option we will do so.



But the reality of these new rules is that the Conti gang is trying to control the media coverage around its attacks.

The group is effectively trying to put the blame for failed negotiations and the subsequent data leaks on security researchers and journalists — the only two categories of people who can find these chats in the first place — instead of the actual attackers.

With the Biden administration having turned its attention on ransomware attacks, the Conti gang is desperately trying to keep its name out of media coverage.

It's a clever use of whataboutism and intimidation from last month's second most prolific ransomware gang.

Ransomware gangs try to control narrative through press releases

Furthermore, the Conti announcement is just the latest in a long series of press releases that ransomware gangs have begun publishing on their blogs (leak sites) and underground forums this year.

Through simple two-sentence statements or long-winded announcements, various ransomware groups have announced new rules for their "operations."

Groups like LockBit, Darkside, or BlackMatter have pledged not to attack critical infrastructure in an attempt to lift US political pressure against their operations but often broke their own rules for the sake of a big score.

The Ragnar_Locker gang also threatened victims to dump their data if they called law enforcement agencies, in another brazen example of a gang trying to intimidate victims.

In addition, the Grief and DoppelPaymer gangs also threatened to wipe victims' servers if they used professional ransomware negotiators, knowing that negotiators would warn the victim against paying the ransom because the two ransomware operations are effectively sanctioned by the US (via their associations with the Evil Corp cybercrime gang).

All of these are examples of how ransomware gangs try to intimidate victims and control their public image around their attacks. But the reality is that these rules mean nothing for the ransomware gangs, which have no qualms in breaking them for the sake of a big payment.

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
