BLEEPINGCOMPUTER

Ransomware gang threatens to wipe decryption key if negotiator hired

The Grief ransomware gang is threatening to delete victim's decryption keys if they hire a negotiation firm, making it impossible to recover encrypted files.

Last week, BleepingComputer first reported that the Ragnar Locker ransomware gang threatened to automatically publish a victim's stolen data if they contacted law enforcement or negotiation firms.

Ransomware gangs do not like professional negotiators to be involved in attacks, as it can lead to lowered profits and the stalling of time while a victim performs an incident response.

Ragnar Locker argues that ransomware negotiation firms are only there to make money and are not in the victim's best interest.

"The recovery company will charge you, maybe even help you return the piece of data if our operation was not perfect, they will try to bring down the price, and as a result, the data of their clients will simply be in the public domain, because we will publish it," Ragnar Locker posted on their data leak site.

Since they made this warning, Ragnar Locker has already claimed to publish a victim's entire stolen data after they hired a ransomware negotiator.

Grief gang takes it a step further.

On Monday, the Grief gang (aka 'Pay or Grief') took these threats one step further by saying they will delete a victim's decryption key if they hire a ransomware negotiator.

"We wanna play a game. If we see professional negotiator from Recovery Company™ - we will just destroy the data.

Recovery Company™ as we mentioned above will get paid either way. The strategy of Recovery Company™ is not to pay requested amount or to solve the case but to stall. So we have nothing to loose in this case. Just the time economy for all parties involved.

*What will this **Recovery Companies™** earn when no ransom amount is set and data simply destroyed with zero chance of recovery? We think - millions of dollars. Clients will bring money for nothing. As usual." - Grief ransomware gang.*

They are saying that if a Grief victim hires a negotiator, the ransomware gang will delete the victim's decryption key, making it impossible to recover files.

Worse than we are_

URL

https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police/

Details

Few days ago one group posted interesting thoughts about the situation here.
We'd like to make some comments and maybe extend some thoughts from our point of view.

Police, FBI and **Recovery Company™**. Who cares about the data in a ransom case?
But answer is too simple to be truth: 2 sides are interested.
One side is company affected. Second side is ransom operator. Nobody else.

Also interesting is common reaction in media: The question is – when your company gets hit by Ragnar Locker, are you going to let them determine the rules or not?
Ofcourse much better way is to pay **Recovery Company™** upfront.
And now they determine the rules. But in this rules there is no place for data safety.
It's just a business model where **Recovery Company™** earns it's money just because it exists.
They must be significant specialist in recovery. But no, unable to recover most of data without proper backups.
They must be perfect negotiaitors. But no once again. They just use variations of same script.
Do they interested in solution? And you know the answer: **NO**. They will get paid either way.
It's also looks like that some of those companies are affilates of some groups with huge number of targets.
Conveyor for a percentage.

Don't pay ransom. Pay that "good guys". But what for? Would they recover data? Nope. Would they prevent the release of sensitive data? No. And what do they do? They are "good".

We wanna play a game. If we see professional negotiator from **Recovery Company™** - we will just destroy the data.
Recovery Company™ as we mentioned above will get paid either way. The strategy of **Recovery Company™** is not to pay requested amount or to solve the case but to stall. So we have nothing to loose in this case. Just the time economy for all parties involved.

What will this **Recovery Companies™** earn when no ransom amount is set and data simply destroyed with zero chance of recovery? We think - millions of dollars. Clients will bring money for nothing. As usual.

Full post by Grief ransomware gang

While Grief is making this threat to put further pressure on victims, it is likely also made for another reason, to evade US sanctions.

Grief ransomware is believed to be tied to a Russian hacking group known as Evil Corp, which the US government has sanctioned.

By banning ransomware negotiation firms, they hope that the victims will not be alerted of sanctions risks and thus not pay.

Evading US sanctions

Evil Corp is a cybercrime group best known for creating and distributing the Dridex banking Trojan and various ransomware families.

When the group first started, it used the Dridex trojan to steal online banking credentials and transfer funds to bank accounts under their control.

In 2017, the gang started using the BitPaymer ransomware in attacks against the enterprise.

In 2019, a new ransomware operation emerged called DoppelPaymer, which shares much of the same code as BitPaymer. However, it is not clear if DoppelPaymer is operated by Evil Corp (aka INDRIK SPIDER) or another group.

"Both BitPaymer and DoppelPaymer continue to be operated in parallel and new victims of both ransomware families have been identified in June and July 2019. The parallel operations, coupled with the significant code overlap between BitPaymer and DoppelPaymer, indicate not only a fork of the BitPaymer code base, but an entirely separate operation," CrowdStrike explained in a report at the time.

"This may suggest that the threat actor who is operating DoppelPaymer has splintered from INDRIK SPIDER and is now using the forked code to run their own Big Game Hunting ransomware operations."

After the US charged members of the Evil Corp for stealing over $100 million, it also added the cybercrime gang to the Office of Foreign Assets Control (OFAC) sanction list.

The US Treasury later warned that ransomware negotiators may face civil penalties for facilitating ransomware payments to ransomware gangs on the sanction list.

Evil Corp began deploying new ransomware variants under different names to evade US sanctions, such as WastedLocker, Hades, Phoenix CryptoLocker, and PayLoadBin.

While Evil Corp used these different variants, the DoppelPaymer operation concurrently ran until May 2021, when they stopped listing new victims on their data leak site.

One month later, the new Grief ransomware gang emerged, which is believed to be a rebrand of DoppelPaymer as it uses much of the same code.

As organizations believe there is a strong enough nexus between DoppelPaymer/Grief and Evil Corp, they likely rebranded to avoid US sanctions.