Exagrid pays $2.6m to Conti ransomware attackers

By Valéry Rieß-Marchive

Published: 2021-06-01 · Archived: 2026-04-05 15:26:54 UTC

jamdesign - stock.adobe.com

jamdesign - stock.adobe.com

Backup appliance specialist hit by Conti ransomware in May with cyber criminals downloading employee and customer data, confidential contracts and source code

-
-

By

- Valéry Rieß-Marchive,
- Antony Adshead, Computer Weekly

Published: 01 Jun 2021 13:00

Backup appliance supplier ExaGrid has paid a $2.6m ransom to cyber criminals that targeted the company with Conti ransomware.

The ransom was paid in the form of 50.75 bitcoins on 13 May, according to information gained by ComputerWeekly.com's French sister publication LeMagIT.

Accession to the ransomware attacker's demands was made more embarrassing when the backup appliance supplier – which makes a big play of its strengths against ransomware – accidentally deleted the decryption tool and had to ask for it again.

Submission to the ransomware attack came in the same month as US pipeline operator Colonial Pipeline paid $4.5m after being hit by Darkside ransomware and the Irish health service was targeted, also by Conti ransomware.

The negotiations, to which LeMagIT had access, began on 4 May with a person with the title “IT lead technician with ExaGrid Systems”.

The cyber criminals got straight to the point, and said: “As you already know, we infiltrated your network and stayed in it for more than a month (enough to study all of your documentation), encrypted your file servers, SQL servers, downloaded all important information with a total weight of more than 800GB.”

They went on to describe how they had got hold of the personal data of clients and employees, commercial contracts, NDA forms, financial data, tax returns and source code. The initial ransom demanded was $7,480,000.

ExaGrid wanted to test the decryption on a sample, and a photo of the front of an ExaGridEX63000E NAS box was provided. Negotiations continued and lasted until 13 May. All through this period, the attackers shared files with ExaGrid via Sendspace to show what they had been able to access. Some archives shared in this way had not been deleted for some time after negotiations finished and could still be downloaded.

The cyber criminal’s negotiator seemed more experienced than others. After an initial offer from ExaGrid of more than $1m, she responded: “Thank you for your efforts. This is a fair and reasonable initial offer. We now have the opportunity to negotiate. We are prepared to offer you a discount of $1m. Your fee will now be $6,480,000.”

In contrast to the heavy-handed approach of other cyber criminals, the negotiator added: “We understand that your work here is not easy and requires some effort to convince the members of your board. But, we are still far from agreement.”

A week later, the ExaGrid negotiator raised their offer to $2.2m. The cyber criminals then reduced their demand to $3m. At that point, the exchanges intensified as the two parties sought to quickly reach an accord. That came soon with an agreement at $2.6m, and the bitcoin address indicated that the negotiated amount was paid. The decryption tool was provided via an account at Mega.nz, where the stolen data was stored. The data and the accounts were immediately deleted.

But then, two days later, the ExaGrid negotiator asked for the decryption tool to be sent again because “we deleted it by accident”. The cyber criminals made it available for download the next day.

The attack is particularly embarrassing for Exagrid, which last December announced it had won seven industry awards, as well as the launch of a new solution for restores following ransomware attacks.

On its website, on the subject of ransomware, ExaGrid says: “ExaGridoffers a unique approach to ensure that attackers cannot compromise the backup data, allowing organisations to be confident that they can restore the affected primary storage and avoid paying ugly ransoms.”

ExaGrid has been asked for comment, but was not available at time of publishing.

Next Steps

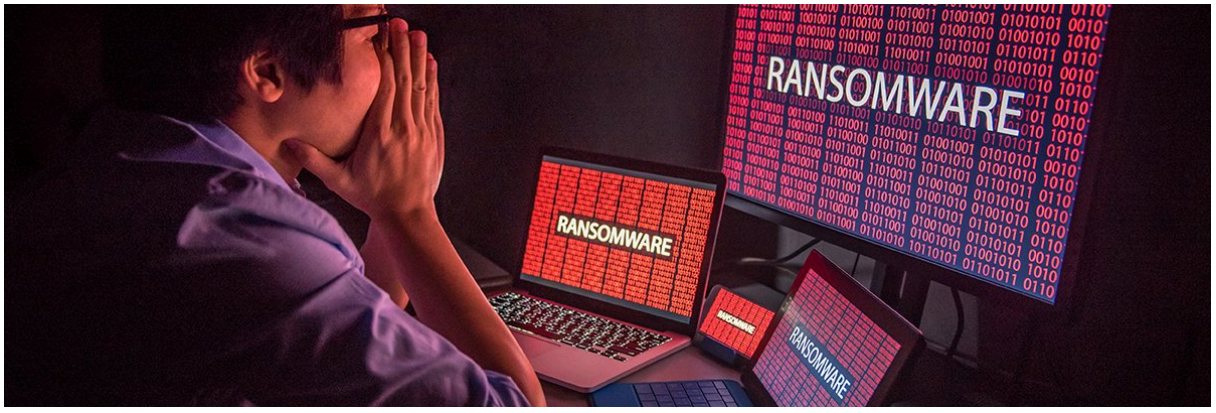
ExaGrid revealed as latest Conti ransomware casualty

Read more on Data centre hardware

- 

Broken decryptor leaves Sicarii ransomware victims adrift

By: Alex Scroxton

- 

Streisand effect: Businesses that pay ransomware gangs are more likely to hit the headlines

By: Bill Goodwin

- 

Ransomware negotiation: Does it work, and should you try it?

By: Mary Pratt

- 

GuidePoint talks ransomware negotiations, payment bans

By: Arielle Waldman
