

Taiwanese Apple and Tesla contractor hit by Conti ransomware

bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/

Sergiu Gatlan

By

[Sergiu Gatlan](#)

- January 27, 2022
- 02:28 PM
- [0](#)



Delta Electronics, a Taiwanese electronics company and a provider for Apple, Tesla, HP, and Dell, disclosed that it was the victim of a cyberattack discovered on Friday morning.

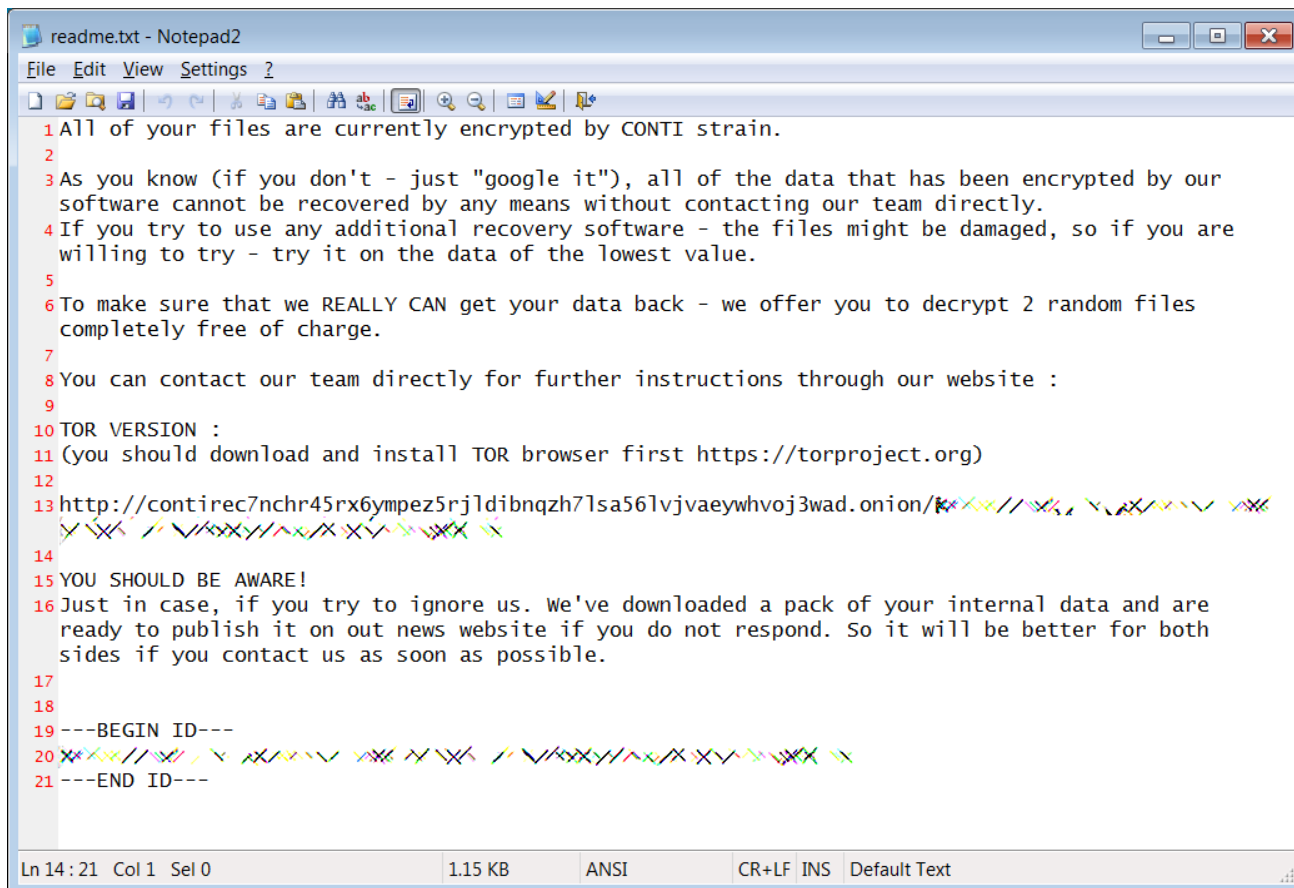
Delta claims to be the world's largest provider of switching power supplies and reported sales of over \$9 billion last year.

In a statement shared on January 22, 2022, the company said the incident impacted only non-critical systems, which had no significant impact on its operations. AdvIntel "Andariel" platform detected the attack on January 18.

Delta is now working on restoring systems taken down during the attack and says it hired the services of third-party security experts to help with the investigation and recovery process.

The electronics provider also said it notified government law enforcement agencies to assist with the follow-up investigation.

While Delta's statement did not say who was behind the attack, an undisclosed information security company found a Conti ransomware sample deployed on the company's network, as CTWANT first reported.



```
1 All of your files are currently encrypted by CONTI strain.
2
3 As you know (if you don't - just "google it"), all of the data that has been encrypted by our
  software cannot be recovered by any means without contacting our team directly.
4 If you try to use any additional recovery software - the files might be damaged, so if you are
  willing to try - try it on the data of the lowest value.
5
6 To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files
  completely free of charge.
7
8 You can contact our team directly for further instructions through our website :
9
10 TOR VERSION :
11 (you should download and install TOR browser first https://torproject.org)
12
13 http://contirec7nchr45rx6ympez5rjldibnqzh7lsa56lvjvaeywhvoj3wad.onion/XXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
14
15 YOU SHOULD BE AWARE!
16 Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are
  ready to publish it on our news website if you do not respond. So it will be better for both
  sides if you contact us as soon as possible.
17
18
19 ---BEGIN ID---
20 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
21 ---END ID---
```

Delta Electronics Conti ransom note (BleepingComputer)

\$15 million ransom for decrypting thousands of devices

According to negotiations between Conti and Delta (also seen by BleepingComputer), the Conti operators claim to have encrypted 1,500 servers and 12,000 computers out of roughly 65,000 devices on Delta's network.

The Conti ransomware gang asked Delta to pay a \$15 million ransom for a decryptor and stop leaking files stolen from its network. Also promised a discount if the company would pay quickly.

While Delta is still reportedly working with Trend and Microsoft's security teams to investigate the incident and claims that its production has not been affected, its website is still down one week after the attack.

Delta's customers can use [this alternate domain](#) while the company brings back online its [main website](#), still down following the ransomware attack, as [The Record](#) found.

"The Conti ransomware group revealed a specific pattern part of the Delta attack leveraging Cobalt Strike with Atera for persistence as revealed by our platform adversarial visibility. Certainly, this attack is reminiscent of the REvil Quanta one affecting one of the Apple suppliers," Vitali Kremez, CEO of AdvIntel, told BleepingComputer.

[Conti](#) is a Ransomware-as-a-Service (RaaS) operation linked to the Russian-speaking [Wizard Spider](#) cybercrime group.

The ransomware gang's operators have breached other high-profile orgs in the past, including Ireland's [Department of Health \(DoH\)](#) and [Health Service Executive \(HSE\)](#), and the [RR Donnelly \(RRD\)](#) marketing giant.

A Delta Electronics spokesperson was not available for comment when contacted by BleepingComputer earlier today.

Related Articles:

[The Week in Ransomware - May 20th 2022 - Another one bites the dust](#)

[Conti ransomware shuts down operation, rebrands into smaller units](#)

[The Week in Ransomware - May 13th 2022 - A National Emergency](#)

[Costa Rica declares national emergency after Conti ransomware attacks](#)

[US offers \\$15 million reward for info on Conti ransomware gang](#)

- [Conti](#)
- [Delta Electronics](#)
- [Ransomware](#)
- [Taiwan](#)

[Sergiu Gatlan](#)

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:

