

Asteelflash electronics maker hit by REvil ransomware attack

By Lawrence Abrams

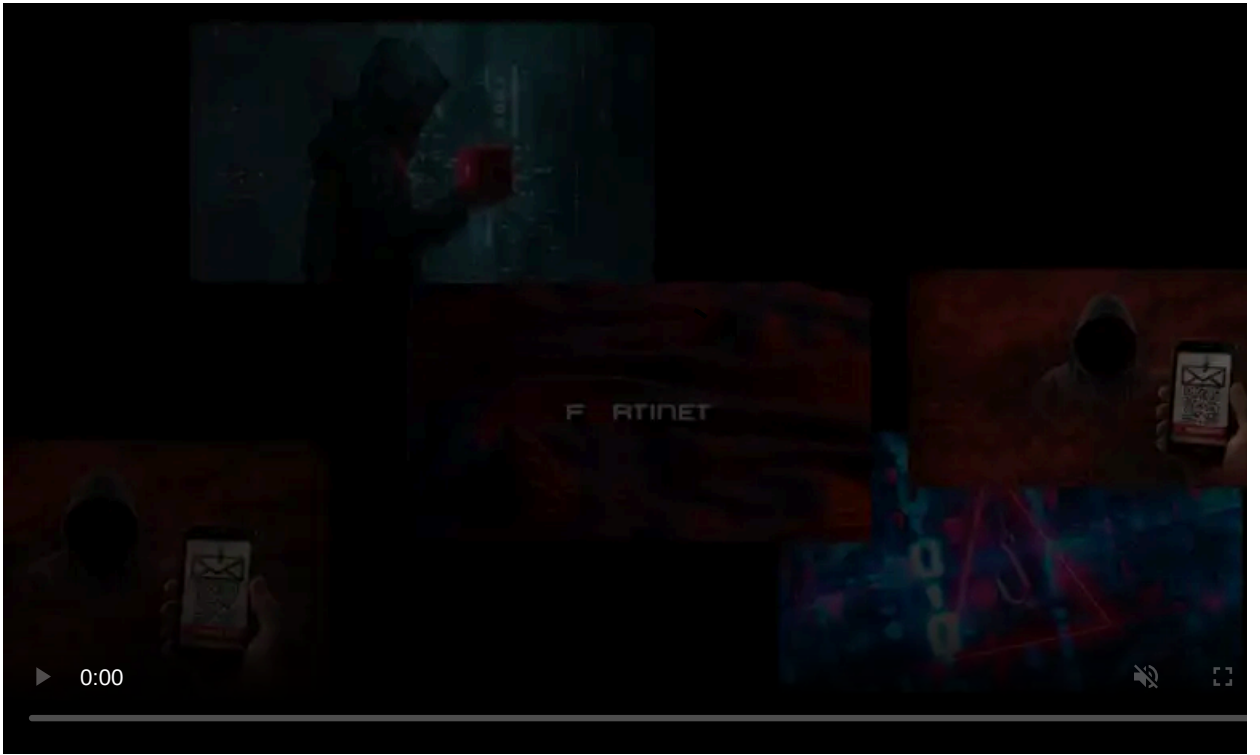
Published: 2021-04-02 · Archived: 2026-04-06 00:06:57 UTC



Asteelflash, a leading French electronics manufacturing services company, has suffered a cyberattack by the REvil ransomware gang who is demanding a \$24 million ransom.

Asteelflash is a world-leading French electronics manufacturing services (EMS) company that specializes in the design, engineering, and printing of printed circuit boards.


While Astelflash has not publicly disclosed an attack, BleepingComputer found this week a sample of the REvil ransomware that allowed access to the Tor negotiation page for their cyberattack.




Visit Advertiser website [GO TO PAGE](#)

This page shows that the REvil ransomware group, also known as Sodin and Sodinokibi, was initially demanding a \$12 million ransom, but as the time limit expired, the ransom doubled to \$24 million.


Your network has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - General-Decryptor



Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

Time is over
* You didn't pay on time, the price was doubled

Current price

94084.32 XMR
≈ 24,000,000 USD

REvil ransom demand for Asteelflash cyberattack

Source: BleepingComputer

The Tor payment site showed a brief conversation between the REvil threat actors and Asteelflash. As part of this conversation, the threat actors shared a file named 'asteelflash_data_part1.7z' that was shared to prove that files were stolen during the attack. Metadata of some of the shared files show that Asteelflash employees authored them.

At this point, the conversation between the two parties has stalled and there are no details about the company's intentions regarding the ransom.

BleepingComputer has contacted Asteelflash multiple times but has not received a response to our inquiries. LeMagIT had more success, an Asteelflash representative [stating](#) for them that the "the incident is being evaluated."

Neither BleepingComputer nor LeMagIT could confirm whether the attack was successful in encrypting files on affected systems.

For more than a year, ransomware gangs started to steal data from their victims before locking the computers. This allows them to extort victims by promising not to publish or sell the information.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/asteflash-electronics-maker-hit-by-revil-ransomware-attack/>