Computer hardware giant GIGABYTE hit by RansomEXX ransomware

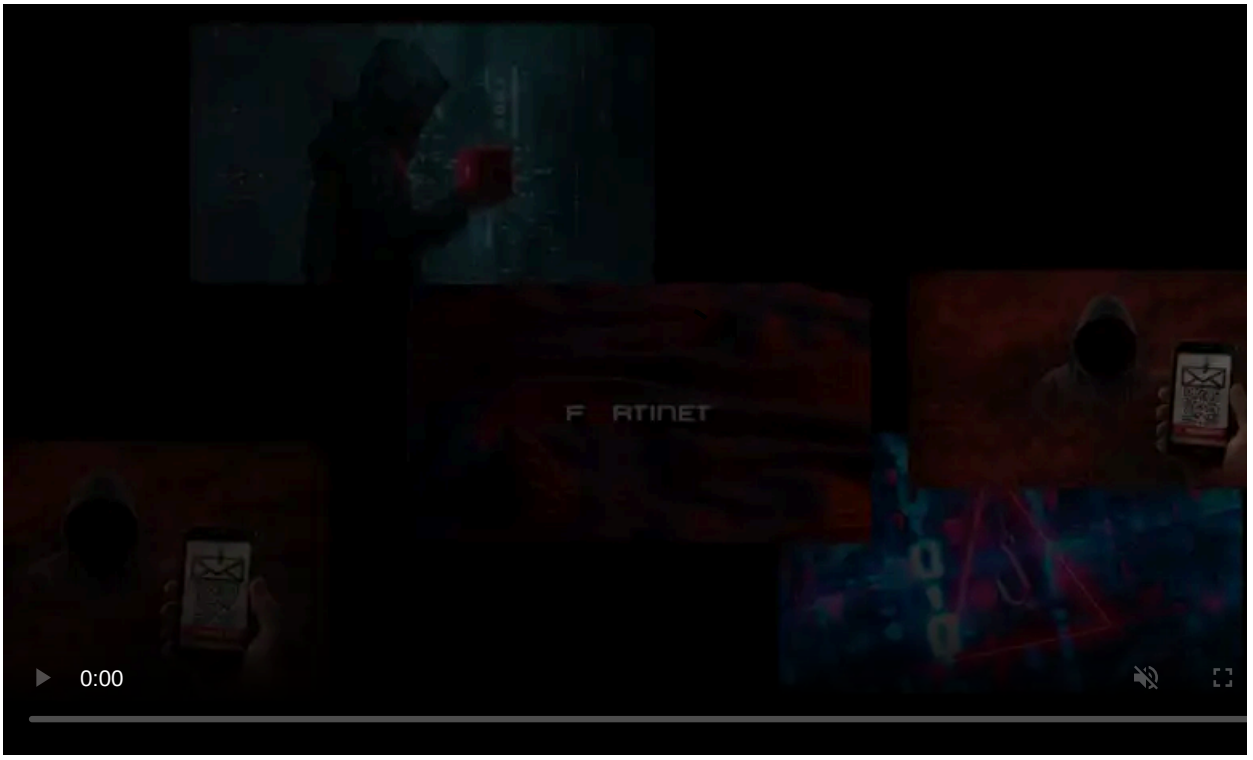
By Lawrence Abrams

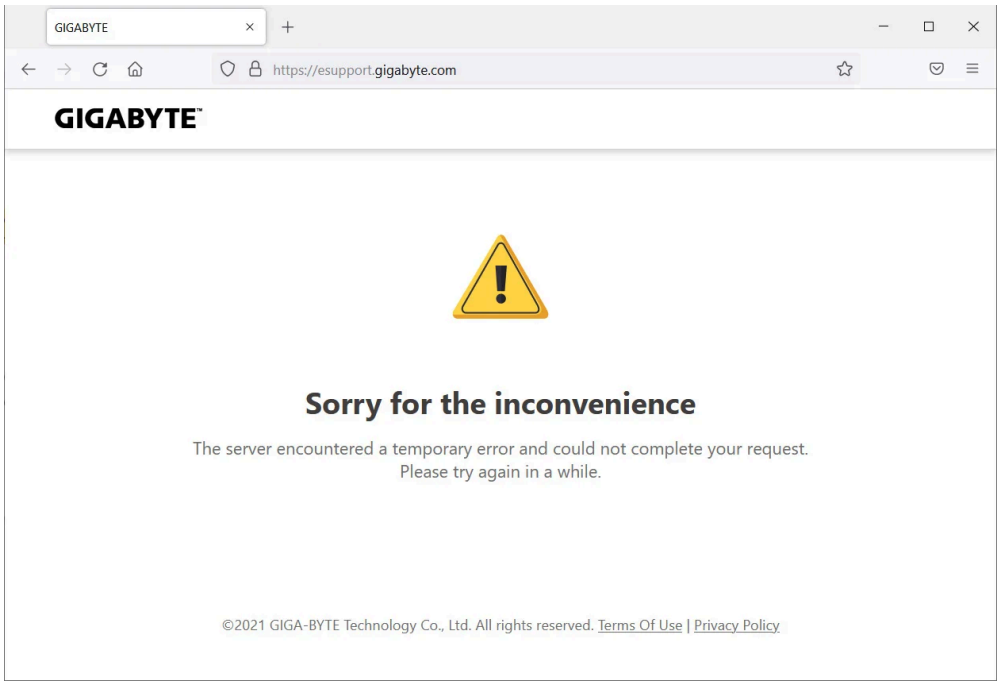
Published: 2021-08-06 · Archived: 2026-04-05 22:45:45 UTC

Taiwanese motherboard maker Gigabyte has been hit by the RansomEXX ransomware gang, who threaten to publish 112GB of stolen data unless a ransom is paid.

Gigabyte is best known for its motherboards, but also manufactures other computer components and hardware, such as graphics cards, data center servers, laptops, and monitors.

The attack occurred late Tuesday night into Wednesday and forced the company to shut down systems in Taiwan. The incident also affected multiple websites of the company, including its support site and portions of the Taiwanese website


F RTINET
0:00



Gigabyte support down due to ransomware attack

Customers have also reported issues accessing support documents or receiving updated information about RMAs, which is likely due to the ransomware attack.

According to the Chinese news site United Daily News, Gigabyte confirmed they suffered a cyberattack that affected a small number of servers.

After detecting the abnormal activity on their network, they had shut down their IT systems and notified law enforcement.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Gigabyte suffers RansomEXX ransomware attack

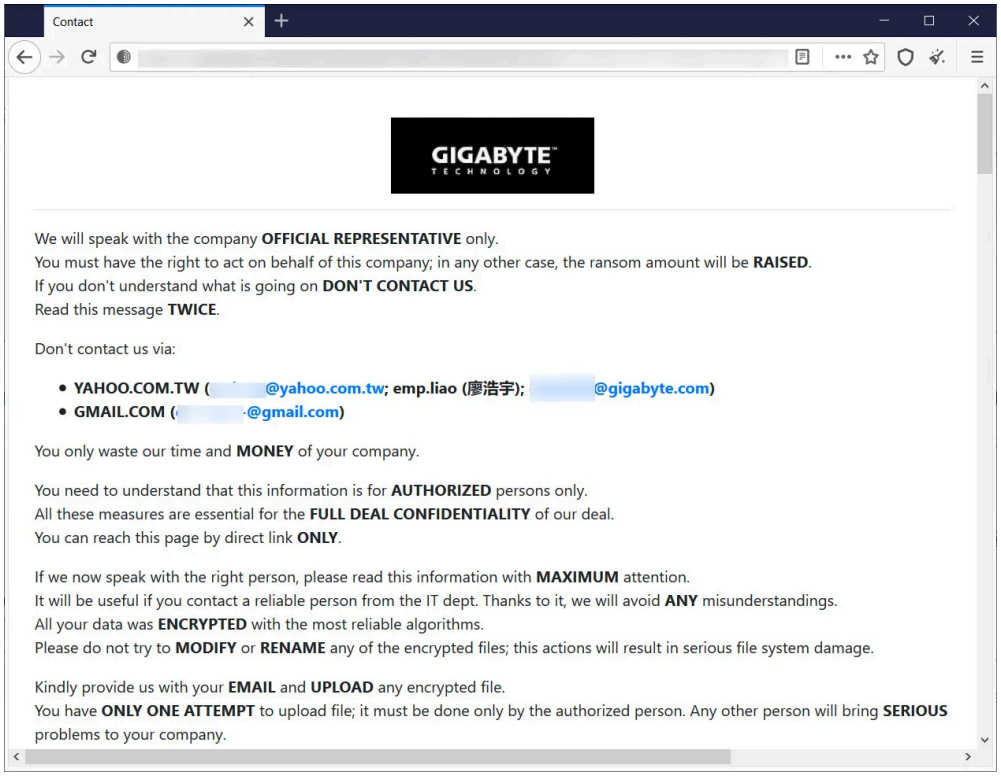
While Gigabyte has not officially stated what ransomware operation performed the attack, BleepingComputer has learned it was conducted by the RansomEXX gang.

When the RansomEXX operators encrypt a network, they will create ransom notes on each encrypted device.

These ransom notes contain a link to a non-public page meant to only be accessible to the victim **to test the decryption** of one file and to leave an email address to begin ransom negotiations.

Today, a source sent BleepingComputer a link to a non-public RansomEXX leak page for Gigabytes Technologies, where the threat actors claim to have stolen 112GB of data during the attack.

In a ransom note also seen by BleepingComputer, the threat actors state "Hello, Gigabyte (gigabyte.com)!" and include the same link to the private leak page shared with us by our source.



Non-public Gigabyte data leak page

On this private leak page, the threat actors claim to have stolen 112 GB of data from an internal Gigabyte network, as well as the American Megatrends Git Repository,

> We have downloaded 112 GB (120,971,743,713 bytes) of your files and we are ready to PUBLISH it.
> Many of them are under NDA (Intel, AMD, American Megatrends).
> Leak sources: newautobom.gigabyte.intra, git.ami.com.tw and some others.

The threat actors also shared screenshots of four documents under NDA stolen during the attack.

While we will not be posting the leaked images, the confidential documents include an American Megatrends debug document, an Intel "Potential Issues" document, an "Ice Lake D SKU stack update schedule," and an AMD revision guide.

BleepingComputer has attempted to contact Gigabyte about the attack but has not heard back at this time.

What you need to know about RansomEXX

The RansomEXX ransomware operation originally started under the name Defray in 2018 but rebranded as RansomEXX in June 2020 when they became more active.

Like other ransomware operations, RansomEXX will breach a network through Remote Desktop Protocol, exploits, or stolen credentials.

Once they gain access to the network, they will harvest more credentials as they slowly gain control of the Windows domain controller. During this lateral spread through the network, the ransomware gang will steal data from unencrypted devices used as leverage in ransom extortion.

RansomEXX does not only target Windows devices but has also created a Linux encryptor to encrypt virtual machines running VMware ESXi servers.

Over the past month, the RansomEXX gang has become more active as they have recently attacked Italy's Lazio region and Ecuador's state-run Corporación Nacional de Telecomunicación (CNT).

Other high-profile attacks by the ransomware gang include Brazil's government networks, the Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies.

Source: https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/