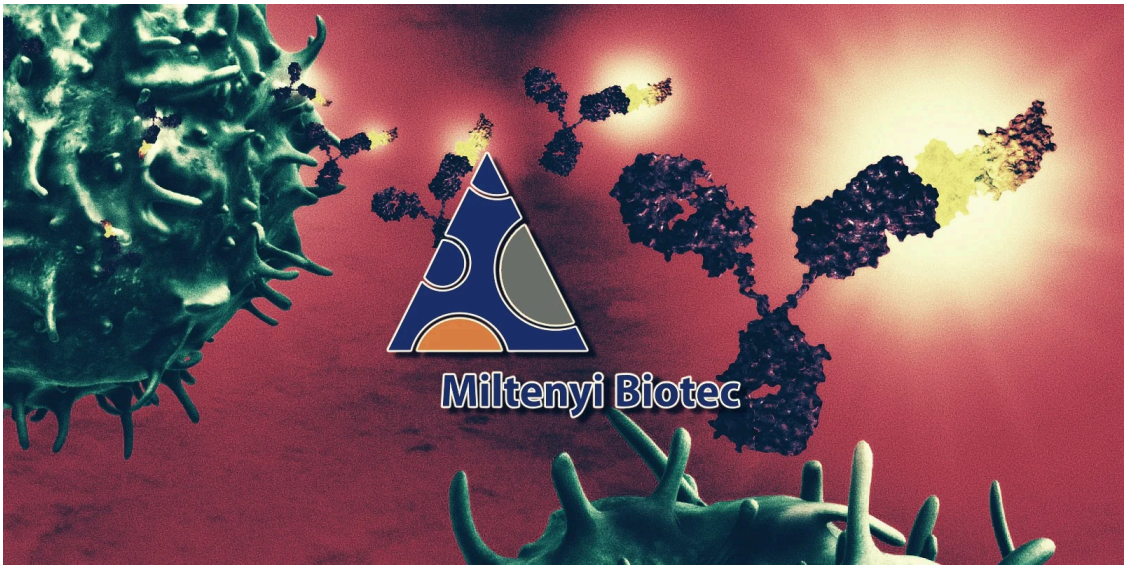
Biotech research firm Miltenyi Biotec hit by ransomware, data leaked

By Sergiu Gatlan

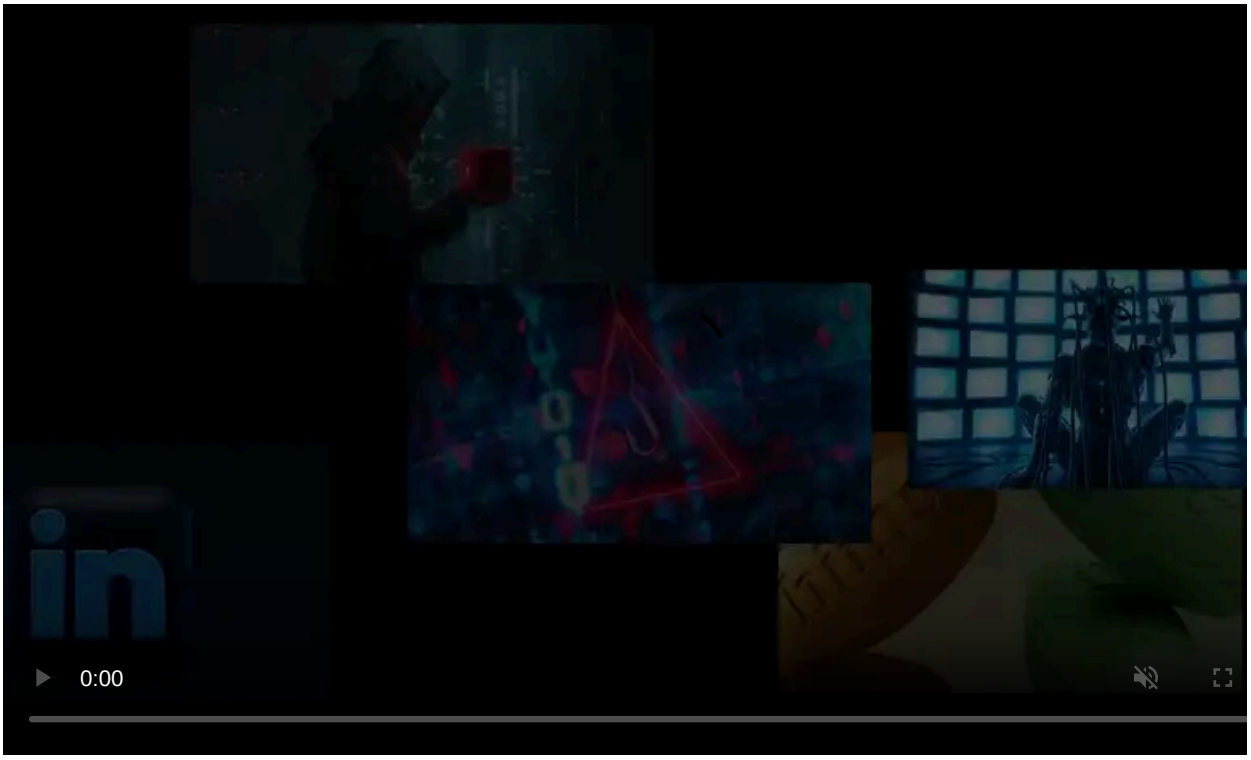
Published: 2020-11-13 · Archived: 2026-04-05 17:35:00 UTC

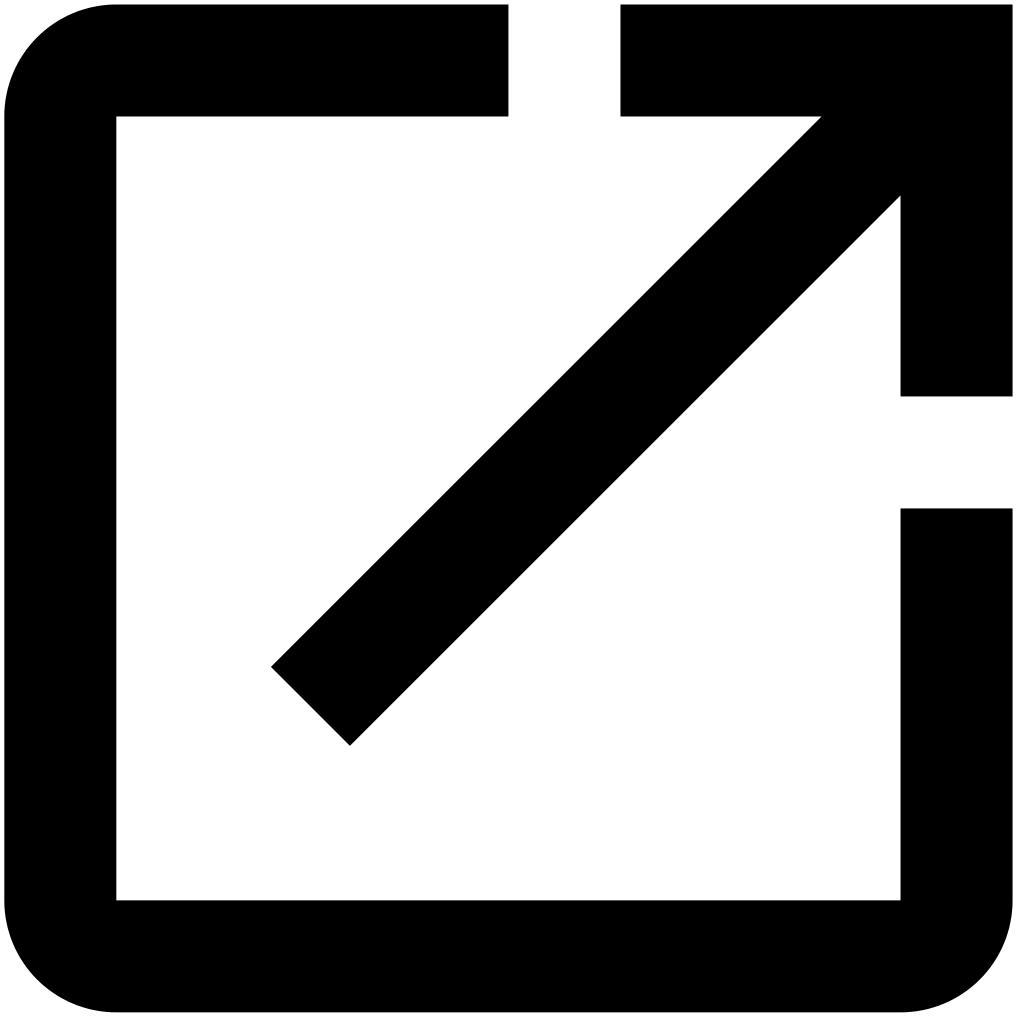


Biomedical and clinical research company Miltenyi Biotec says that it has fully restored systems after a malware attack that took place last month and affected the firm's global IT infrastructure.

Miltenyi Biotec's 2,500 employees from 28 countries are developing cell research and therapy products for clinicians and researchers who are working on covid-19 vaccines and treatments.

It also provides SARS-CoV-2 antigens to researchers involved in SARS-CoV-2 vaccine development.


0:00



Back up after restoring systems in roughly two weeks

"During the last two weeks, there have been isolated cases where order processing was impaired by malware in parts of our global IT infrastructure," Miltenyi Biotec said in an official statement.

"Rest assured, all necessary measures have now been taken to contain the issue and recover all affected systems. Based on our current knowledge, we have no indication that the malware has been inadvertently distributed to customers or partners."

At the moment, the company said that it has successfully restored all operational processes impacted in last month's malware attack. However, the company is still facing issues in some countries with their email and telephone systems.

Miltenyi Biotec added that customers should expect order delays caused by the temporary operational issues affecting systems during the last two weeks.

Clients are also advised to reach out whenever they have to deal with any urgent cases that required immediate assistance.

"Please accept our apologies for any inconvenience this may have caused you," Miltenyi Biotec added.

Customers experiencing difficulties can reach out using a list of alternative contact numbers available here.

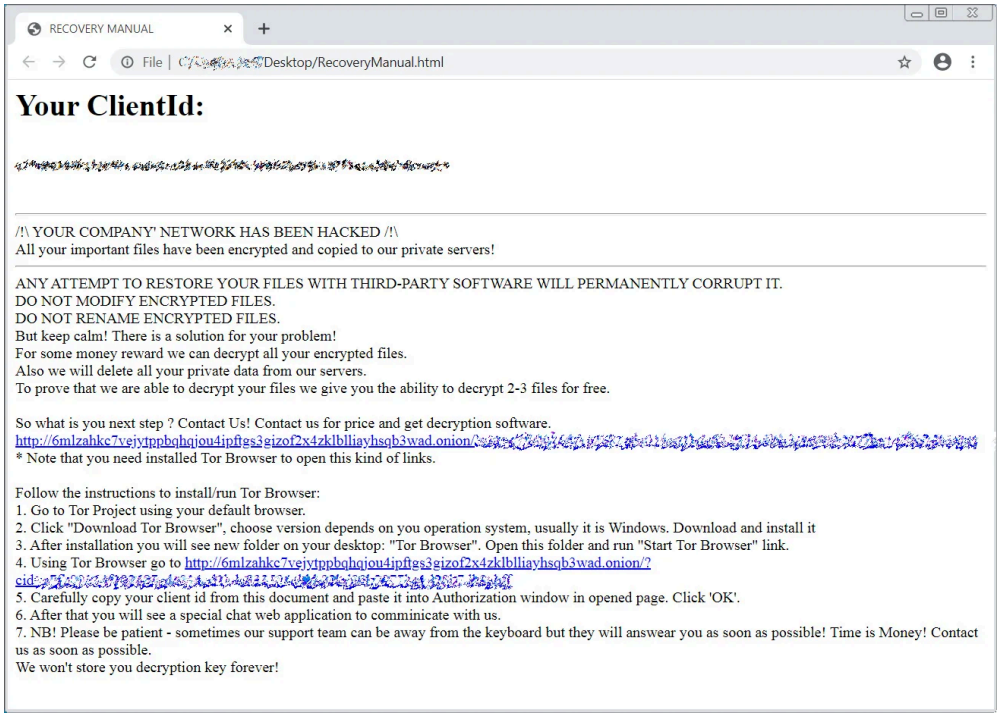
Mount Locker ransomware attack

Even though Miltenyi Biotec has not disclosed the nature of the malware that caused the operational downtime during the last two weeks, the Mount Locker ransomware gang has claimed the attack earlier this month.

The ransomware actors have leaked 5% out of the 150 GB of data they claim to have stolen from the company's network on their data leak site on November 4, 2020, in the form of a ZIP archive containing just over 1 GB of Miltenyi Biotec documents.

Mount Locker ransomware became operational in July 2020 after they started to breach corporate networks, stealing sensitive data and deploying payloads to encrypt systems on the victims' network.

Mount Locker ransom notes seen by BleepingComputer show that, in some cases, the Mount Locker ransomware gang is demanding multi-million dollar ransoms.



Mount Locker ransom note

The gang launched a 'Mount Locker News & Leaks' site used to publish the stolen files of victims who refuse to pay the ransom.

Mount Locker is also known for threatening victims to contact the media, TV channels, and newspapers if the ransom is not paid.

Unfortunately, Mount Locker ransomware uses ChaCha20 + RSA-2048 and, at the moment, there is no way to recover encrypted files for free.

BleepingComputer reached out to a Miltenyi Biotec spokesperson for additional details but did not hear back at the time of publication.

Source: https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/