Biotech research firm Miltenyi Biotec hit by ransomware, data leaked

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

Sergiu Gatlan

By <u>Sergiu Gatlan</u>

- November 13, 2020
- 05:45 PM
- 0



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.

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 <u>here</u>.

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.

<u>Mount Locker ransomware</u> 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.

The second secon))
← → C ① File C/Se@ac@@Desktop/RecoveryManual.html	☆ €	•
Your ClientId:		
g I Marken In With & Stateman California State State State States S		
/!\ YOUR COMPANY' NETWORK HAS BEEN HACKED /!\ All your important files have been encrypted and copied to our private servers!		
ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT. DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES. But keep calm! There is a solution for your problem! For some money reward we can decrypt all your encrypted files. Also we will delete all your private data from our servers. To prove that we are able to decrypt your files we give you the ability to decrypt 2-3 files for free. So what is you next step ? Contact Us! Contact us for price and get decryption software. http://fmlzahkc7vejytppbghqjou4jpffgs3gizof2x4zklblliayhsqb3wad.onion/cage6_25y26	Open Albert	
Follow the instructions to install/run Tor Browser: 1. Go to Tor Project using your default browser. 2. Click "Download Tor Browser", choose version depends on you operation system, usually it is Windows. Download and install it 3. After installation you will see new folder on your desktop: "Tor Browser". Open this folder and run "Start Tor Browser" link. 4. Using Tor Browser go to http://fomlzahkc7vejytppbqhqjou4jpftes3gizof2x4zklblliayhsqb3wad.onion/? cide_f12_30_4192457_dos_fa_01_422150_444_450_50_50_441_50_50_50_44_50_50_50_50_50_50_50_50_50_50_50_50_50_	e is Money! Co	ontac

Mount Locker ransom note

The gang <u>launched</u> 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.

Related Articles:

BlackCat/ALPHV ransomware asks \$5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Mount Locker
- <u>Ransomware</u>
- <u>Research</u>

<u>Sergiu Gatlan</u>

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
- <u>Next Article</u>

Post a Comment <u>Community Rules</u> You need to login in order to post a comment Not a member yet? <u>Register Now</u>

You may also like: