CORPORATE

ABOUT CORPORATE

A Gurgaon based textile company

GOALS

To recover files from malware (Onion) affected hard drive

APPROACH

The client approached Stellar Data Recovery Service Center - Gurugram to recover the Microsoft Access Files

RESULTS

Stellar Data Recovery successfully recovered files from the virus infected hard drive.

STELLAR HAS SUCCESSFULLY RECOVERED DATA FROM ONION MALWARE AFFECTED HARD DRIVE - CASE ID: G29615

The company has made a tremendous growth in the Textile Products Sector, and as of today, it is the major player in the Indian Industrial Setup.

Over the course of years, the company has created a trusted name in the Indian Textile Sector.

THE CLIENT WAS THE VICTIM OF ONION MALWARE

As the comapny is a global Manufacturer, Exporter, and Supplier of Textile Yarn and Fabrics. They used 12TB Western **external hard drive** (3.5 inches in size and the model no. is WD20PURX-64P6ZY0) to store critical details such as transaction history, customer data, spreadsheets, Microsoft Access Files, demographic related-reports, etc.

Regrettably, the hard disk was infected by Onion malware which encrypted the data stored on it. Upon encryption, all the files and folders turned inaccessible until a ransom was paid to decrypt the same.
Each time the client tried to open the files, they showed an error and there was a change in the name of the file format. For example, the actual file name was: xyz.mdb which changed to xyz.mdb.jhgb1232121@.onion.
The potentially destructive virus obstructed the client's day-to-day business routine. Therefore, it became imperative to remove the Onion virus to resume the business.

THE CLIENT'S RIGHT COURSE OF ACTION

The client visited Stellar Data Recovery Service Centre – Gurugram with the affected hard drive and enquired about the data recovery services. Moreover, he presented his side of the story to the executive and requested for the quotation. The client specified that his concern was to get the access of Microsoft Access files, and that too, on an immediate basis. After getting through the client's difficult situation, the executive requested him to submit the hard drive and assured him of complete data recovery without compromising on the privacy and integrity of the data.

STELLAR’S ANSWER TO THE VIRUS

The data recovery professional examined the hard drive and found out that the media had some logical problems. On analysing the encrypted files, the team observed that the “Onion” virus has led to the renaming of the files.
The data recovery team followed the below-stated procedure to recover the files:

- The team cloned the client’s HDD to prevent further damage to the original one
- Then the team analysed the internal structure of each file and made internal changes to counter the Onion’s algorithm. For this, the team used various in-house developed software
- After putting in lots of efforts, the team recovered the required Microsoft Access files of data size 44.3GB.

THE CLIENT GOT HIS MICROSOFT ACCESS FILES WITHOUT PAYING THE RANSOM

The executive informed the client about the successful completion of the data recovery process and requested him to come to the center and collect his files. After going through each file, the client assented to the recovery and was pleased with the results. He breathed a sigh of relief and thanked the team for recovering his Microsoft Access files from the affected HDD.