Kroll Ontrack

CASE STUDY

Kroll Ontrack is assisted by NetApp's technology to solve a ransomware infection.

The Situation

A single user's laptop at a large pharmaceutical company was infected with CryptoLocker Ransomware. This malware encrypts the user's files and withholds the encryption key until you pay the ransom amount. The laptop was connected to the corporate network which allowed the malware to infect a CIFS volume which was set up as a file share on a NetApp FAS. The malware was able to infiltrate the file share and encrypt the majority of the files. The IT team was not notified of the infection until after the backup retention period had expired, meaning that the backup contained only encrypted data.

The total impact resulted in:

- 46 drives
- 1 aggregate
- 1 volume infected on a RAID DP

To perform the recovery, the aggregate needed to be taken offline which affected 17 volumes in total.

The Solution:

The customer brought their 46 drives, RAID DP into our New Jersey lab for evaluation and Kroll Ontrack engineers got to work on a solution. The engineering team from Kroll Ontrack:

- Virtually rebuilt the RAID groups which were strewn across 10 different shelves
- Virtually rebuilt the aggregate
- Virtually rebuilt the critical volume

An additional challenge on this recovery was that the aggregate was in use for two weeks after the incident occurred which resulted in some data being overwritten.

The Resolution OR Conclusion:

Kroll Ontrack was able to virtually rebuild the volume containing the CIFS share and encrypted data. Leveraging NetApp's proprietary OS (OnTap) and file system (WAFL), Kroll engineers used multiple consistency points to "walk back" in time to find and merge unencrypted copies of the critical data to return to the customer. This type of recovery is only possible on storage like NetApp's FAS because of the way the data is stored on the volume.

CONTACT

For more information, call or visit us online:
800.645.3649 in the U.S. and Canada
+1.952.937.5161
www.krollontrack.com

Kroll Ontrack