KrollOntrack™
By KrolLDiscovery

Data Recovery **UK**

Case Study

Important hospital databases rescued after ransomware attack.

Data recovery of: Dell™ EqualLogic PS6500ES

Ransomware attack makes critical Oracle databases in LUN virtualised storage arrays disappear in a large German hospital.

The situation

A ransomware attack with the 'Locky' virus had severe effects for a large German hospital.

Not only were many servers paralysed by the virus limiting hospital operations, but also allegedly uninfected servers were affected as during the panic these were separated while the power supply was still operating. The problem, especially in highly complex virtualised storage systems, is that there may be unexpected issues resulting from a power shutdown. This was the case of a Dell EqualLogic PS6500ES storage array with a total of 148 professional 100-gigabyte hard drives. After the hospital's IT staff and Dell's technical support were unable to solve the problem, the specialists of Kroll Ontrack were called in to help. All disks were delivered to the data recovery laboratory in Germany where they were assessed.

The Dell EqualLogic PS6500ES system contained multiple hard disks, which typically consist of 16 or 48 HDD shelves, which are connected together to form RAID 5 or RAID 50 systems (sub-arrays). These sub-arrays in turn are connected to 'members', with one or more members belong to a logical unit (a group). There the LUNs are created and stored, fragmented and distributed over all members and sub-arrays. They are 'tracked' by a map, which in turn distributes itself to the members or to the various sub-arrays when it gets proportionally large.

In this case our specialists found out that from those 7 shelves with 148 hard disks, 3 shelves with 80 hard disks contained the LUN with the Oracle databases needed. However, many of the links (mappings) of the data fragments (which were distributed over all hard disks) were either corrupted or no longer available, so assigning the fragments proved to be a very difficult task. The mapping of an EqualLogic PS system is also encoded in a specific logic, so the links here aren't easy to find either.

The solution

To map the links specialist engineers from other Kroll Ontrack offices were involved and new software tools had to be developed especially to solve the logic and the corruption problems regarding both the RAID and the LUN addressing.

With the help of the new tools, the experts were able to recreate the RAID 5 and RAID 50 systems as well as display the LUN. Within this LUN a virtual HDD (a VMDK file) was located, in which an NTFS file system with two Oracle databases were hidden. Two file layers had to be identified and recovered within the LUN before these databases could be finally exported.

The resolution

The data recovery engineers from several Kroll Ontrack offices were finally able to successfully extract and recover the required databases and send the data by courier to the client.

The hospital was very pleased with the mediation support from Dell to Kroll Ontrack and the fact that they finally had all their important data available again. In addition, the tools developed for this project can be used again in upcoming data recovery cases of Dell EqualLogic PS Array systems and therefore significantly reduce future data recovery times.