

【单位名称】 中工投建设有限公司

【介质描述】 U8SOFT 财务服务器被黑客攻击

【数据恢复故障描述】 登陆U8报错服务器所有文件文件后缀为makkonahi,服务器被黑客攻击（勒索病毒）

【数据恢复故障分析】

我公司数据恢复中心工程师对SQL物理库文件底层分析后，文件头尾2M左右数据体被加密

用户有4月前未被加密的BAK文件

【数据恢复过程】

1:使用SQL工具对加密的库获取数据表结构，还原BAK文件后对表结构比对无丢失损坏

2:交替使用truncate table delete from
清空好库数据表，使用SQL工具解析加密库后

导入清空数据的好库

3:导入成功后 DBCC CHECKDB 查询无错误，在用户U8环境里面测试无报错