步骤1：找准中毒原因，修复薄弱环节，避免二次中毒。

我强烈建议企业找专业的安全团队进行溯源分析。如果不想花费这个费用并且你自己具备钻研精神，那就从以下几个思路入手。

1.从各类网络设备的日志中查找异常（防火墙日志）；

2.从服务器操作系统安全日志查找异常；（windows安全日志，下图中日志被黑客清空了）

3.从客户端操作系统查找异常；（客户端异常登录日志）

4.利用网络上免费的病毒溯源工具查找异常。

步骤2：格式化中毒的服务器并重装系统。强烈建议不要用GHOST版本系统安装。

GHOST版本系统有非常多的系统漏洞和预装软件的后门。如果企业单位批量电脑，建议自己动手做一个干净的母盘进行安装。个人电脑也建议用纯净版一步步安装。

注意！！！！！！！！ 注意！！！！！！！注意！！！！！！！！！

安全防护绝对不是买一套防火墙或者装几套杀毒软件就能解决问题的。

任意一个新的勒索病毒的变种就可以躲开几乎所有的杀毒软件和防火墙。这也是为

什么各大厂商的杀毒软件和防火墙都在持续不断的更新自己的病毒库的原因，因为只有安全人员捕获了病毒特征才有机会识别并杀掉病毒。这意味着肯定得有一部分人要先中毒牺牲掉自己，才能引起各大杀软和防火墙公司的注意。

1.2 数据重要但不紧急（这里的不紧急是指可以等上1-3年）

步骤1. 通过PE模式或者安全模式进入服务器，把重要的数据备份一遍（最好是全盘备份至一个空的移动硬盘）

1.3 数据重要且紧急

步骤1：先断网而不是先关机。 我们从大量勒索病毒案例中分析得出，勒索病毒的黑客攻击的时间集中在晚上或者非工作日。因为晚上和非工作日不容易被发现，有充足的时间进行加密。当发现ERP服务器中毒或者金蝶用友财务服务器中勒索病毒之后，应该把中毒服务器的网线断开，如果是虚拟机可以把网卡禁用，防止横向扩展传播。

不要着急关机的原因有两个

原因1：中毒服务器不关机，就有可能从内存DUMP中找到加密的私钥（我们成功用此方法找到过过密钥）这种方法找到私钥的可能性不大，但至少是一种可能。

原因2：如果服务器的数据量非常大，黑客加密程序正在加密过程中突然断电，那么会导致这个文件加密不完整，彻底损坏掉。即使黑客也无法解密此类文件。这个道理很容易理解，就好比你正在编辑一个EXCEL，如果没有保存直接断电，很可能这个EXCEL再打开就会乱码。财务工作人员应该都遇到过这个问题。因为我修复过很多这种原因损坏的EXCEL。