附件 1:

GANDCRAB 勒索病毒攻击过程

GANDCRAB 勒索病毒是勒索病毒家族中最活跃的家族，多次出现版本更新，持续增加攻击方式，危害性极大。以下是来源于互联网信息的某类 GANDCRAB 勒索病毒攻击过程:

1.受害者邮箱收到一封邮件，标题为“你必须在 3 月 11 日下午 3 点向警察局报到!”邮件内容则是一个以日期命名的 rar 格式压缩包。

2.压缩包中的病毒伪装文件多样，有的是乱码的 exe 可执行文件，也有用“XXX.doc.exe”这种包含多个空格，以此来伪装成 word 文件的,也有直接伪装成 PDF 文件的。

3.只要受害者警惕性低的情况下打开病毒文件，电脑就很可能被感染，电脑中文件被加密，并随即添加文件后缀，并被告知如何支付赎金。