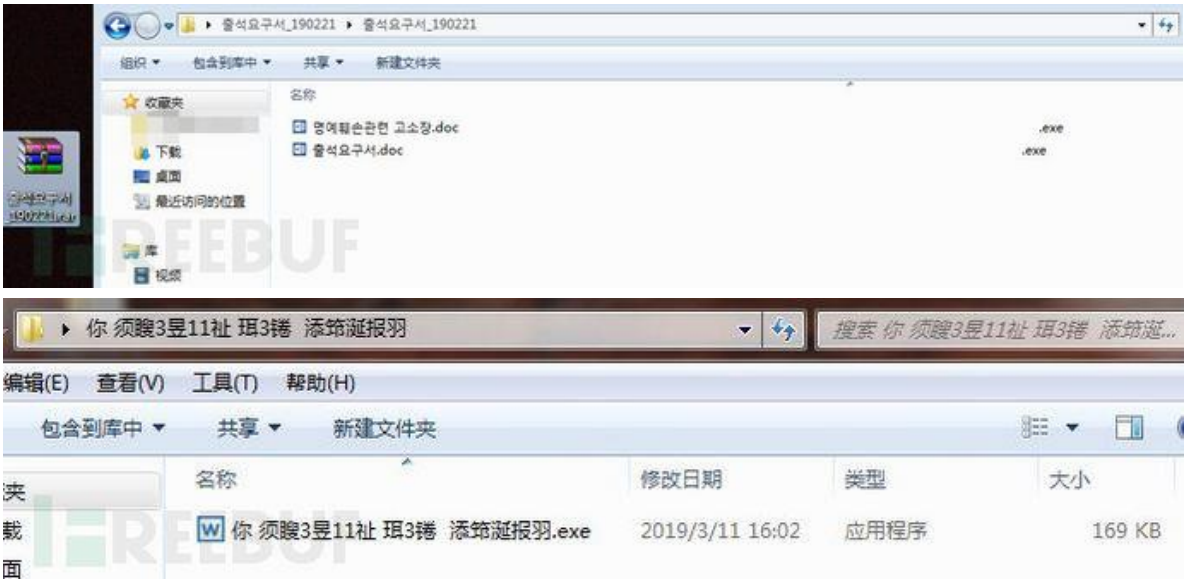
附件 1. 防范 GANDCRAB 勒索病毒安全防护措施

根据多个安全组织反馈,GANDCRAB 勒索病毒通过 Windows 远程桌面暴力破解、VNC 暴力破解、恶意邮件(包括定向钓鱼邮件)、网页挂马、操作系统漏洞利用、U 盘移动介质等途径传播，感染后受害者主机中的文件将被加密，且一般无法解密，须缴纳高额赎金后才可能找回原有文件。

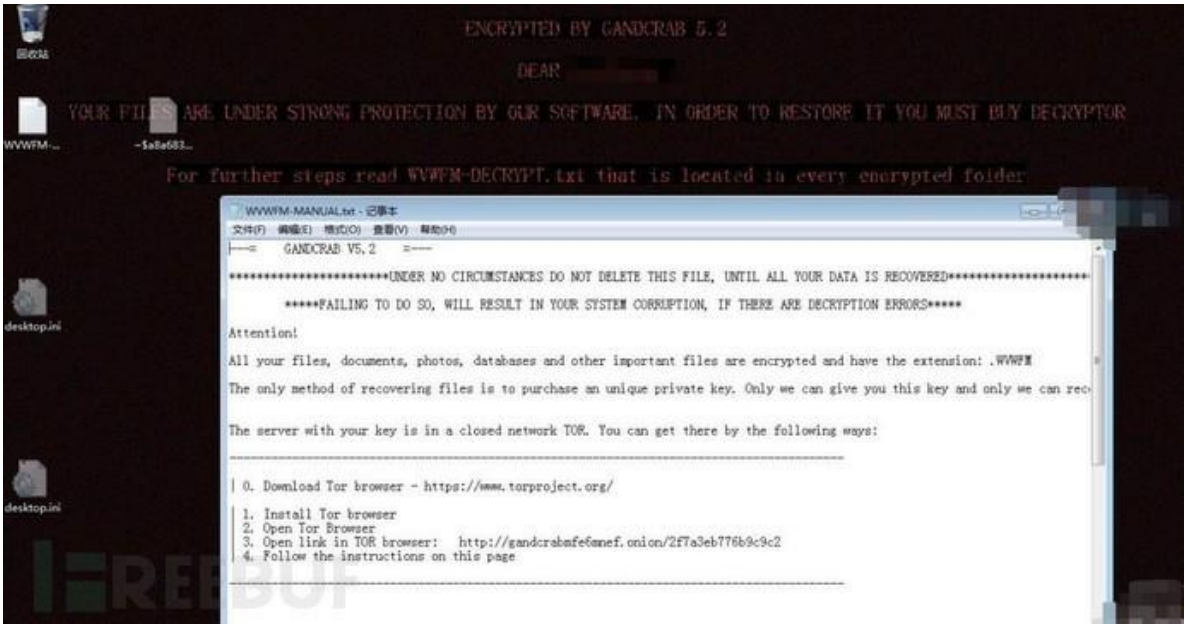
GANDCRAB 勒索病毒是 2018 年勒索病毒家族中最活跃的家族，多次出现版本更新，持续增加攻击方式，危害性极大。以下是来源于互联网信息的某类 GANDCRAB 勒索病毒攻击过程：

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。



4）攻击者要求受害者下载 Tor 浏览器，通过浏览器打开特定的页面，例如下图所展示的暗网地址是：http://gandcrabmfe6mnef.onion/2f7a3eb776b9c9c2。

5）该地址打开之后，要求用户查找并上传 -DECRYPT.txt 或 -MANUAL.txt 文件，才能进行下一步支付赎金操作。而使用 Tor 浏览器和进行支付后无法保证攻击者提供解密手段，受害者电脑内文件丢失的风险极大。

Windows 个人主机和服务器的防护措施建议（Windowes 系统具体操作参见《附件 3.GANDCRAB 勒索病毒防范指南》）如下：

1）启用并打开“Windows 防火墙”，进入“高级设置”在入站规则里禁用“文件和打印机共享”相关规则；尽量关闭 445、135、137、138、139、3389、5900 等不用的端口；关闭网络文件共享和远程桌面连接服务。

2）通过 Windows 系统补丁自动升级、主要安全厂商安全客户端等，将 Windows 主机系统更新升级到最新状态。

3）通过 Windows 系统组策略或主要安全厂商安全客户端，禁用 U 盘、光驱自动运行功能。

4）安装主流杀毒软件，将软件病毒库升级至最新。

5）清理 Windows 系统内无关账号，管理员账户避免使用弱口令，复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种以上字符类型组合以上）。

6）保持良好的网络使用习惯：

- 不随意打开不明来源的 Office 文档、可执行文件（特别是电子邮件附件文档）；
- 使用 Chrome、Firefox、360 安全等安全防护功能较好的浏览器；
- 不打开来源不明的网络链接；
- 不下载、不安装来源不明的主机应用和移动应用。

特别的，建议对于有大量重要文档信息的个人主机和服务器，经常性进行**重要文件备份**，并将备份介质**离线保存**（也就是将备份的硬盘断开与主机的 USB 连接后存放）；停止使用 Windows XP、Windows 2003 等微软公司已不再提供安全更新的操作系统，及时升级操作系统补丁到最新。