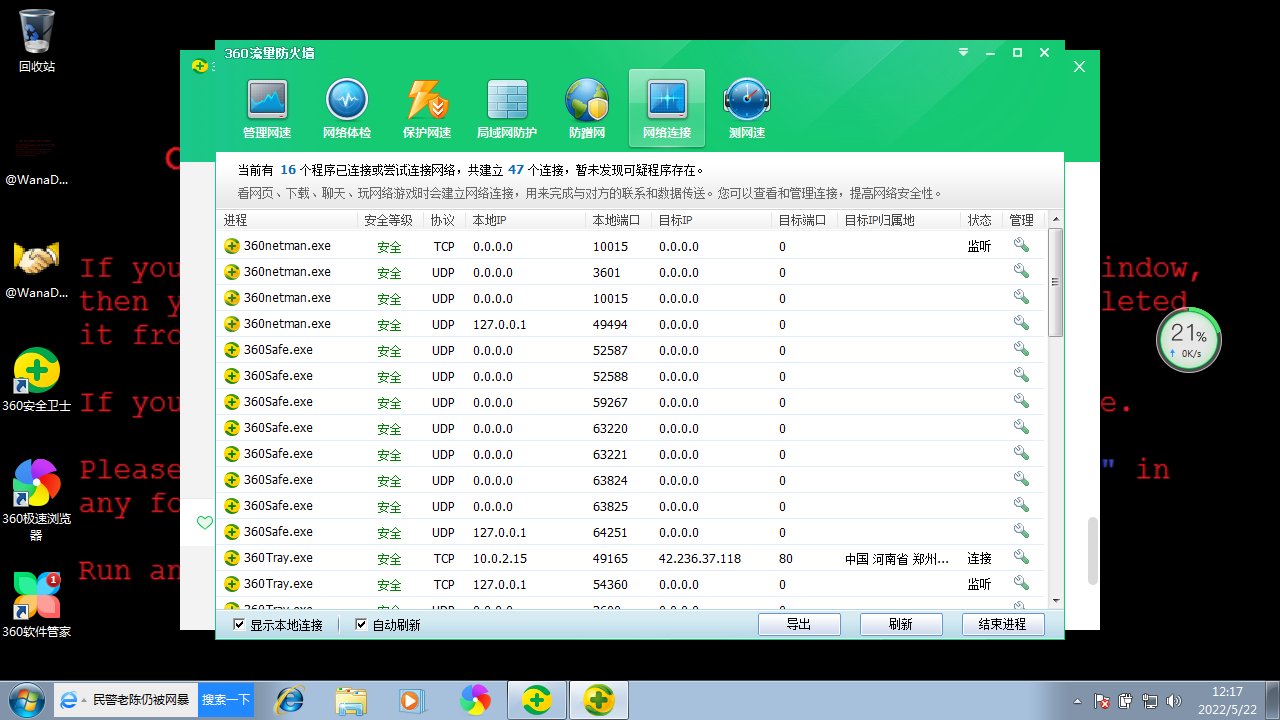
Win系统与桌面安全实践

任务一：安装虚拟机



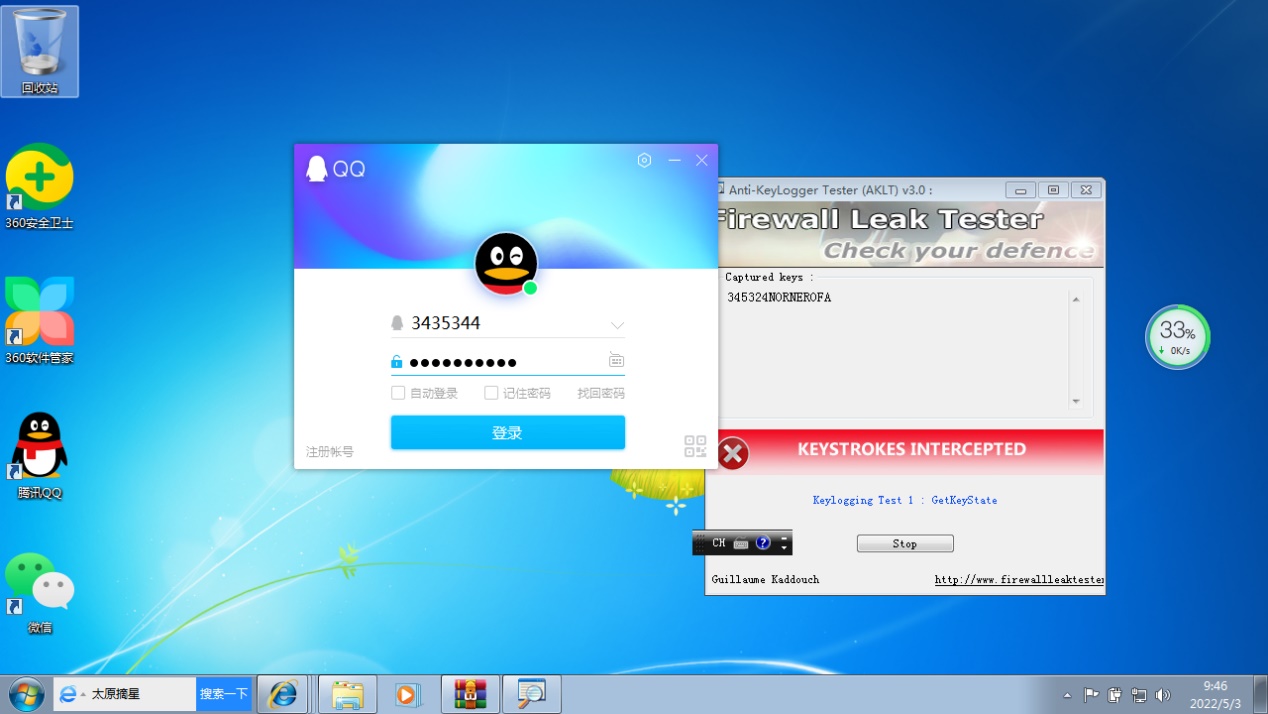
安装完成。

任务二：360安全卫士分析系统虚拟状态

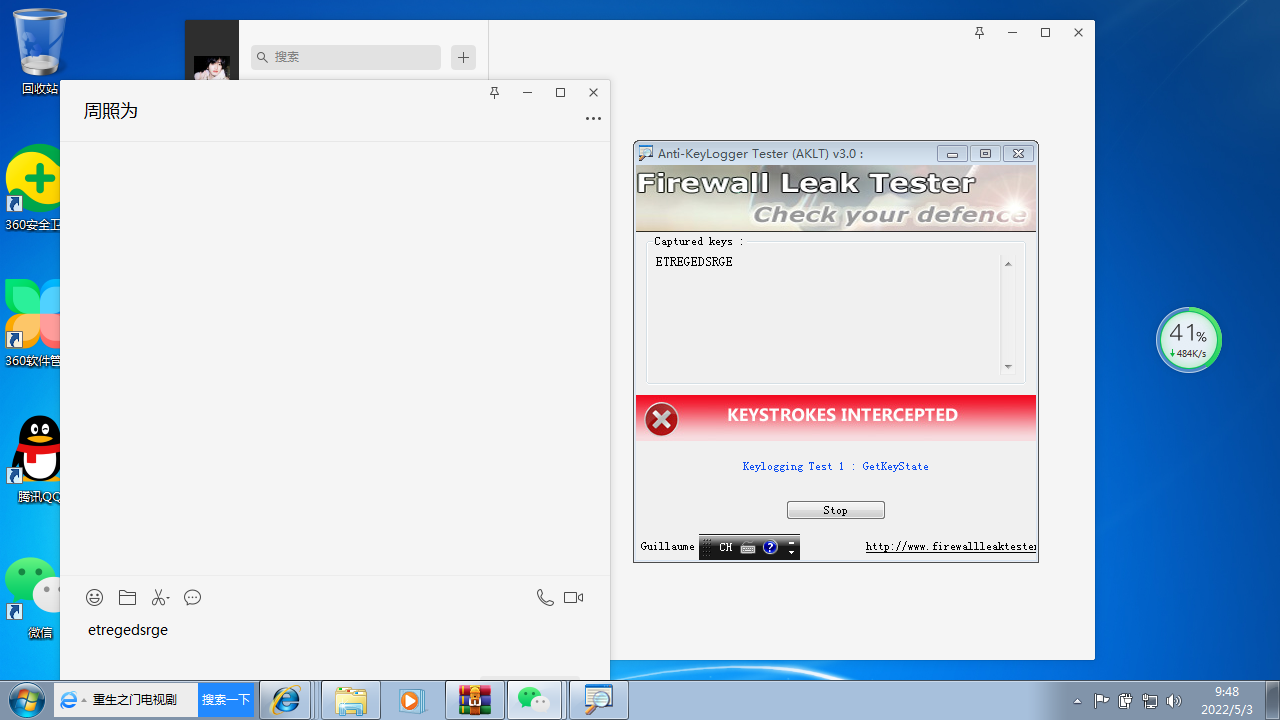


任务三：Windows钩子测试

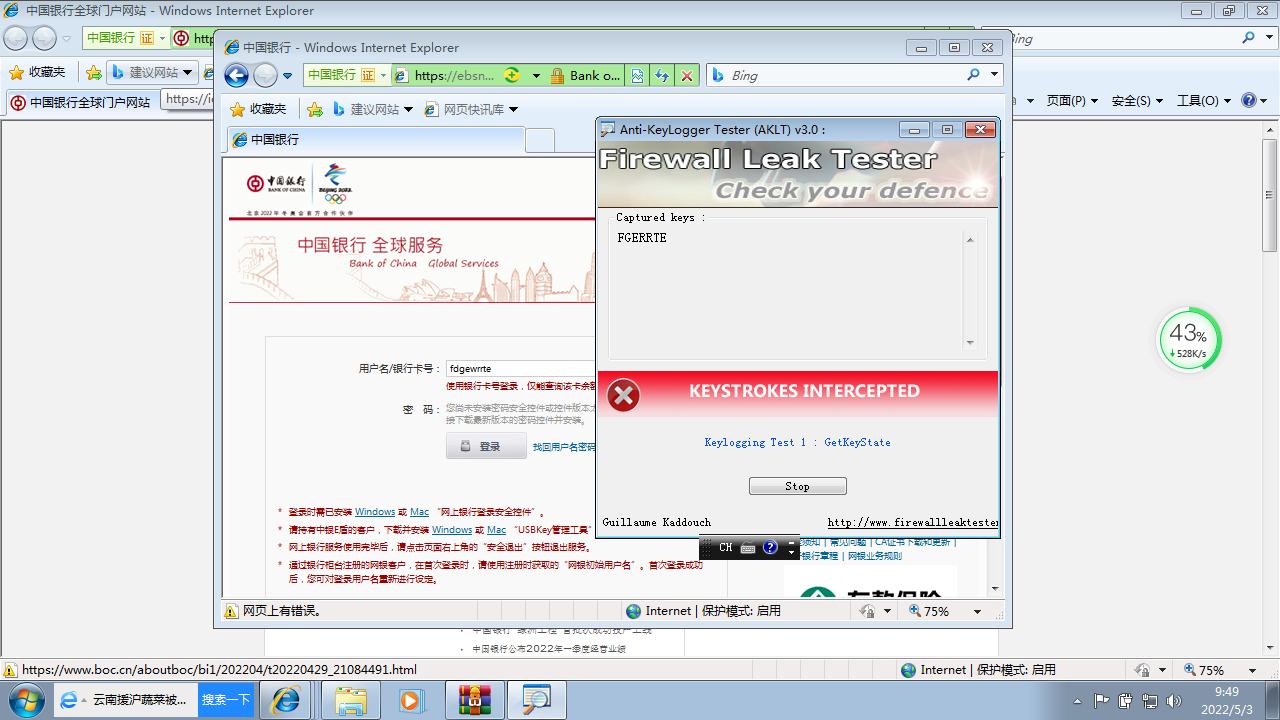
1）QQ



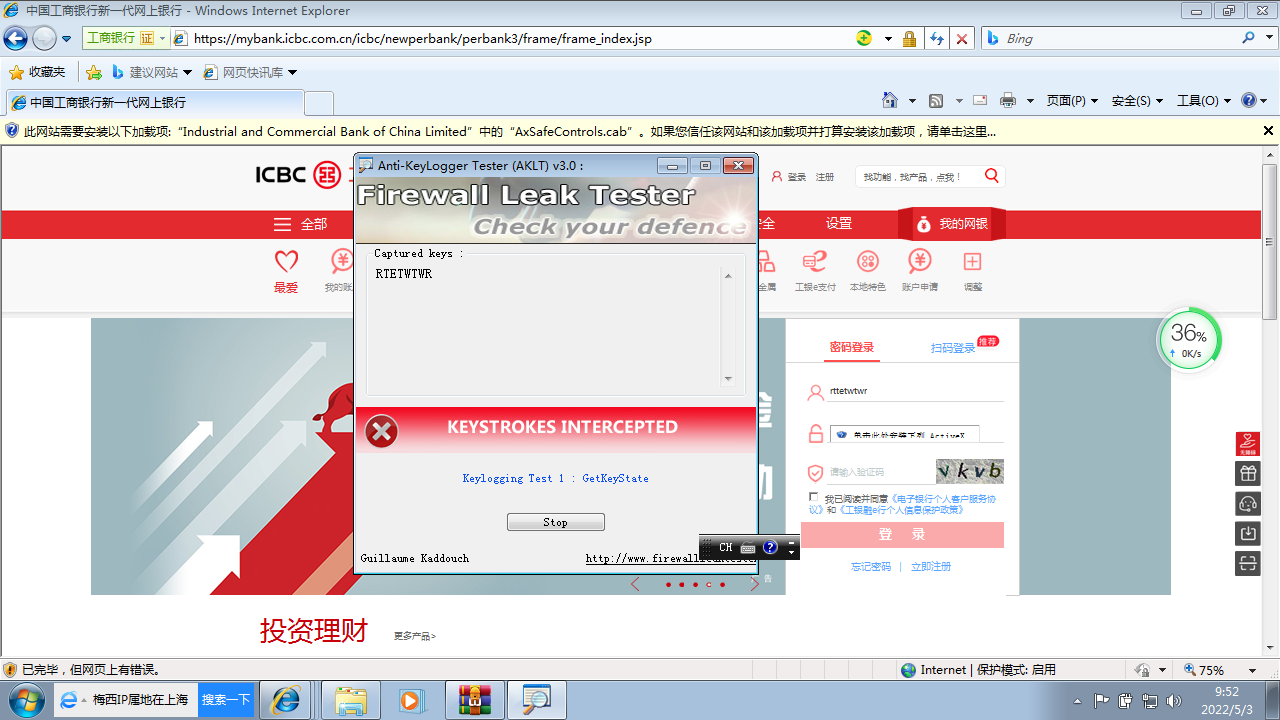
2）微信聊天框



3）中国银行



4）工商银行



5）建设银行



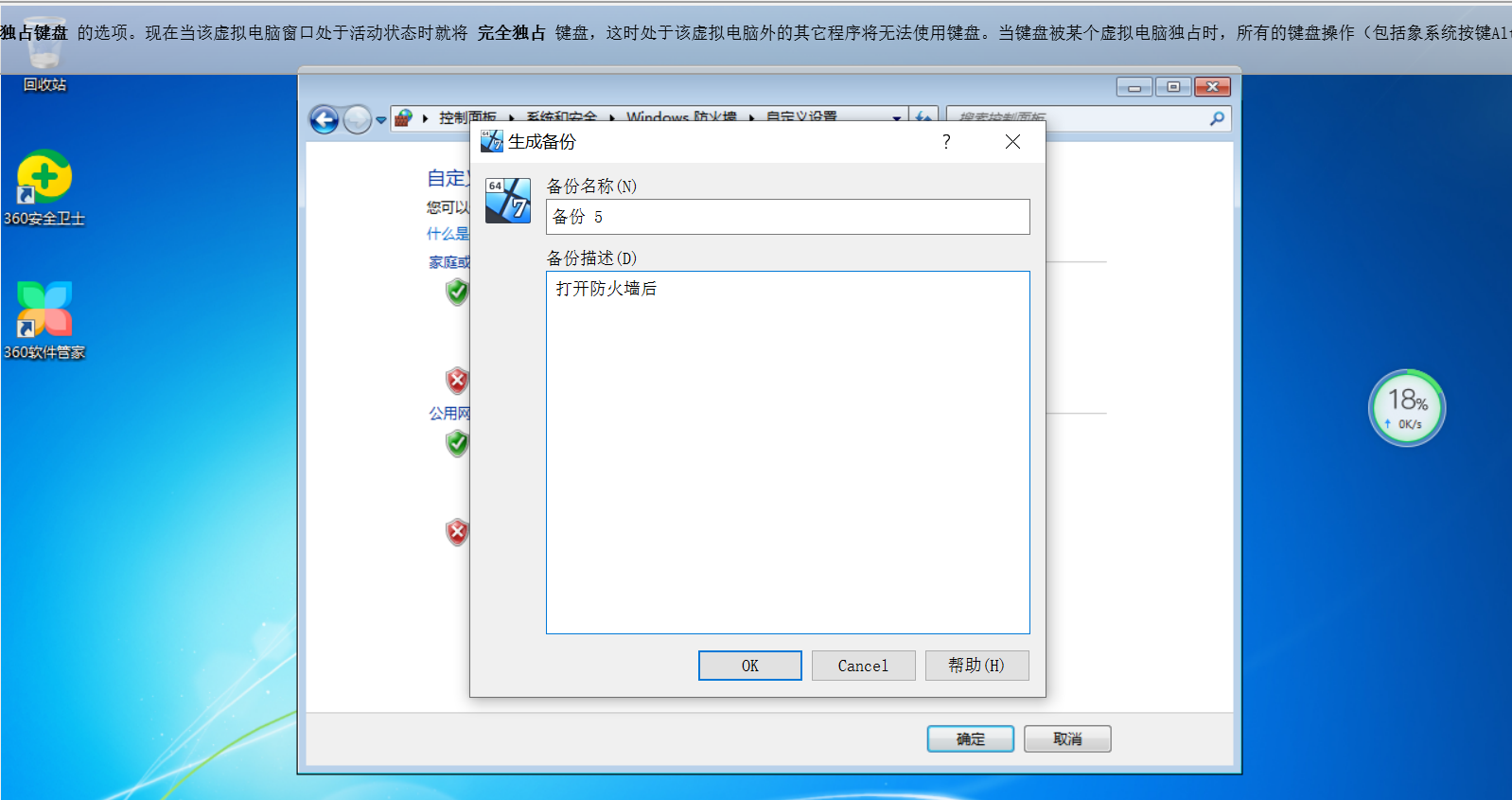
以上五个平台均已成功，但测试表明中国农业银行登陆系统无法使用钩子工具入侵。

任务四：wannacry病毒测试

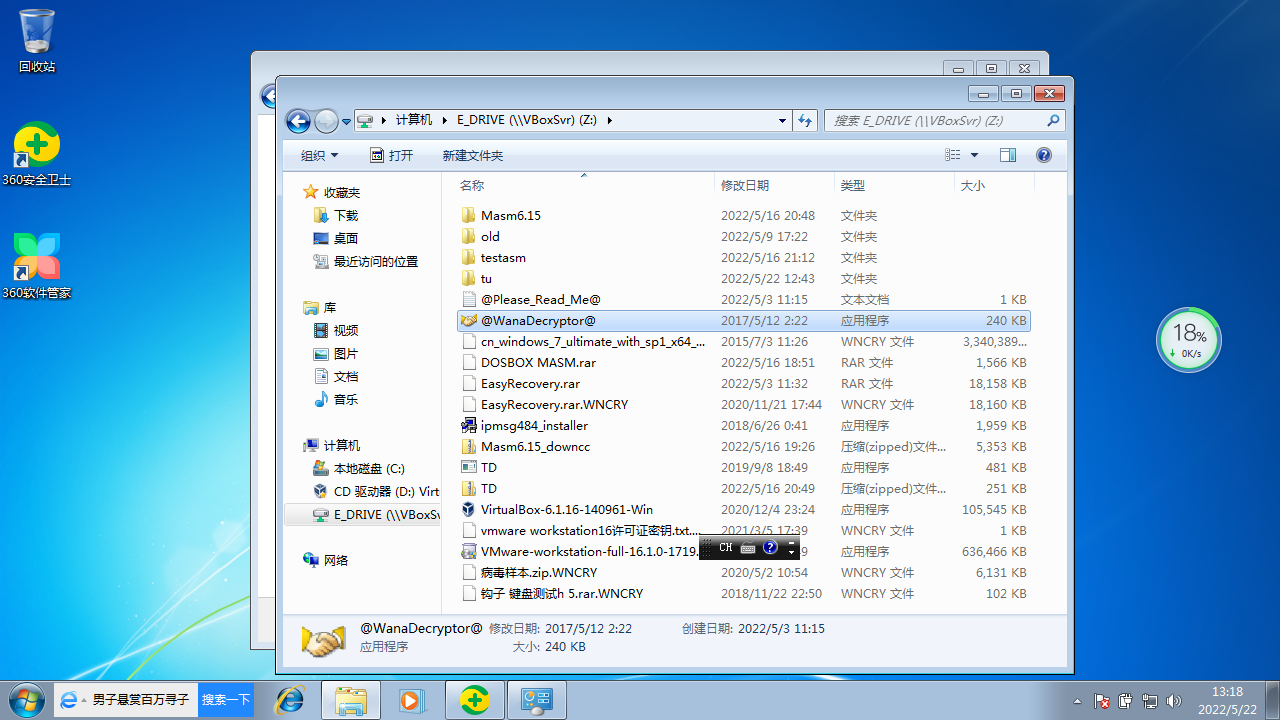
1. 防火墙已打开



1. 虚拟机做镜像备份



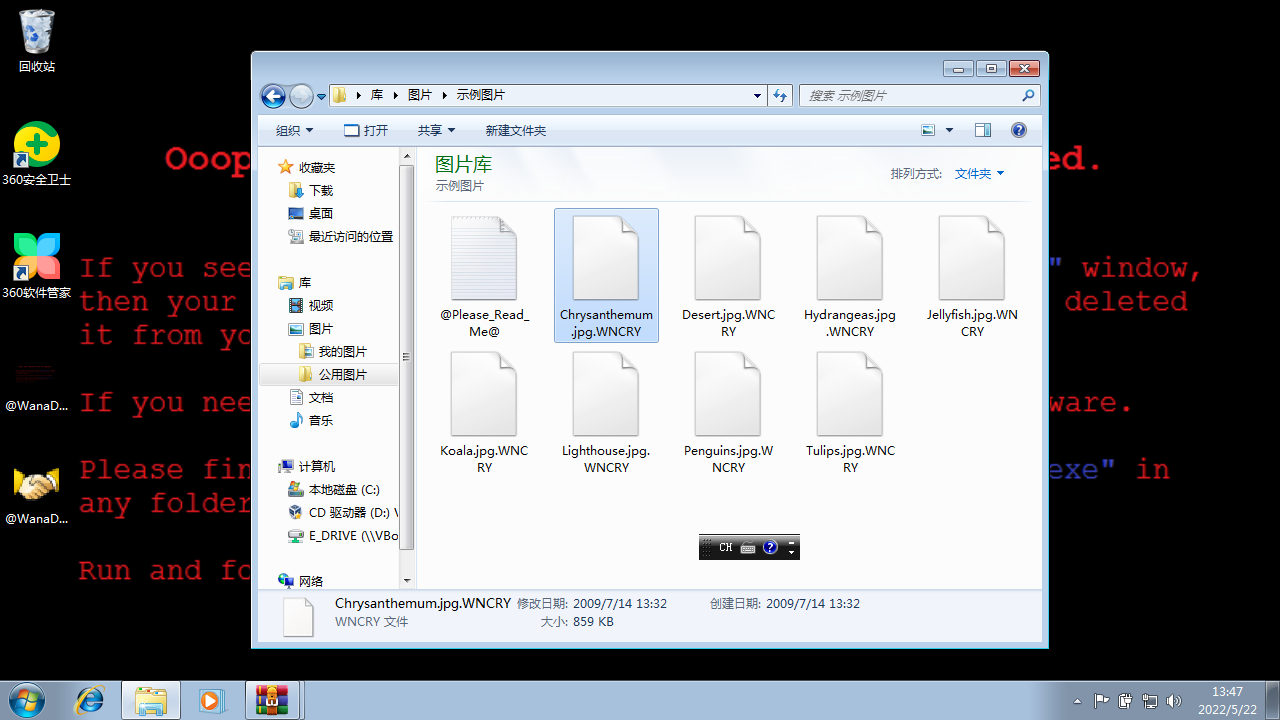
1. 解压病毒压缩包



1. 运行病毒

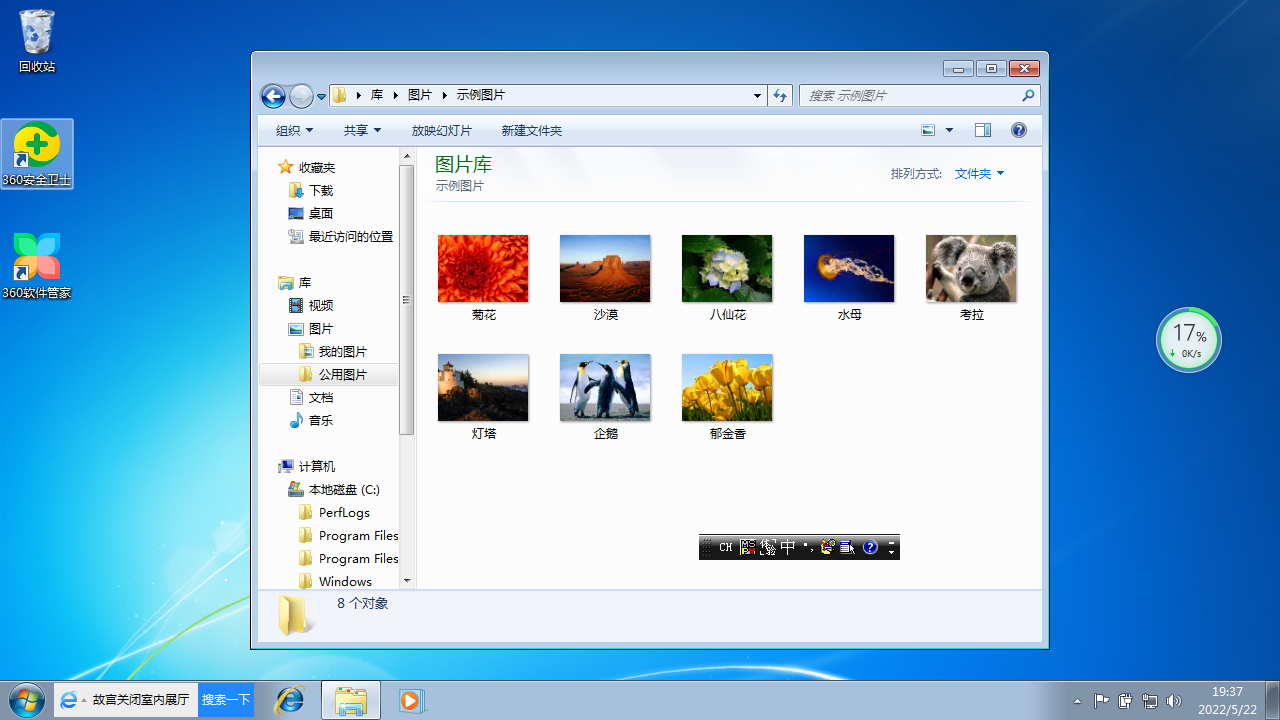


1. 系统变化（以系统自带图片为例）

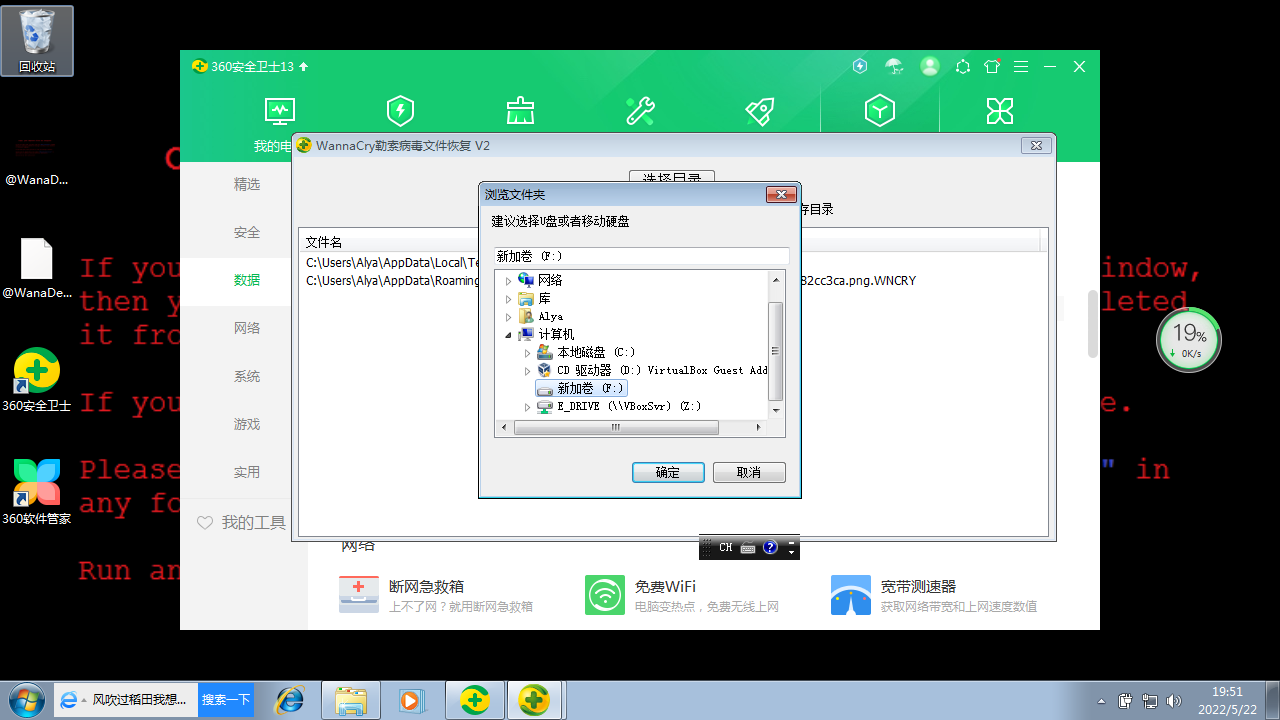


后缀变为WNCRY

1. 恢复系统



1. 再次运行并尝试使用360恢复



恢复到一个新的磁盘上



恢复成功！

小结：

本次实验之初出现了一些意外，例如无法将虚拟机和本机共享磁盘，运行病毒前没有备份等等，造成了很多效率的降低。但是也相应的对虚拟机更加了解，对钩子和wannacry病毒有具体认识。希望未来的使用上可以有所突破。