# 利用新冠病毒疫情讨论群组传播恶意附件风险提示

安恒应急响应中心

2020 年 1 月

# 1.恶意行为

近日，安恒应急响应中心监测到有恶意攻击者利用社交网络上的新冠病毒疫情讨论群组传播恶意附件的行为，监测发现在 Telegram 上相关“武汉肺炎疫情”、“新型冠状病毒”、“实时疫情真相”、“防范知识”等新冠病毒疫情交流讨论群里有人恶意投放包含这些关键词的文件附件诱骗用户打开从而感染电脑病毒和植入木马程序，建议针对这些可疑附件尽量不要下载和打开，以免遭受恶意病毒和后门植入攻击。

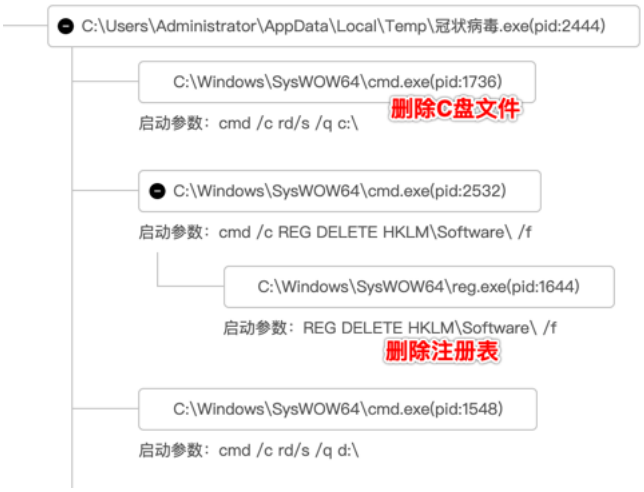
# 2.影响范围

目前发现的样本主要以诱骗用户主动下载运行的可执行文件为主，有明显带.exe 可执行文件后缀的恶意文件（比如：冠状病毒.exe、逃离武汉.exe），也有带.zip 的压缩包诱导用户解压执行（比如：中国新型冠状病毒已经出现 4000 多.zip）。

根据恶意文件格式大类型来看，未来可能会出现文本文件类型（比如 DOC、PDF 等）或脚本类型（JS、VBS 等）的附件，建议提高警惕谨慎点击。

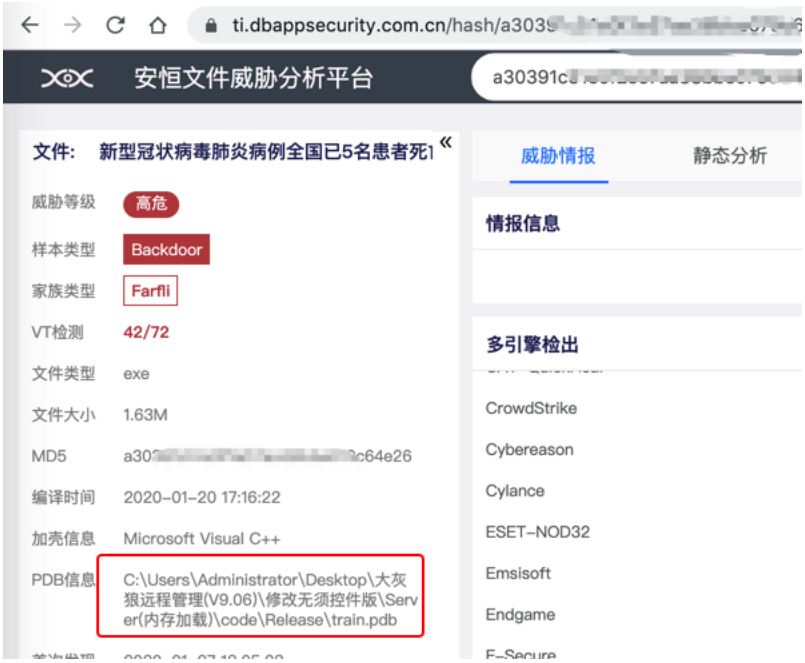
# 3.恶意样本

病毒样本：分析“冠状病毒.exe”样本，该文件是一个 VB 编写的程序，会对系统进行破坏性攻击，通过动态行为图可以发现，删除系统盘、注册表等信息。




后门样本：分析“新型冠状病毒肺炎病例全国已 5 名患者死亡；警惕！！.exe”样

本，发现其 pdb 信息包含“大灰狼远程管理(V9.06)”信息，很明显的该文件是大灰狼远程控制木马：




通过动态分析分析，发现其收集系统信息回连香港 IP：202. XX. XXX. 80 的 5073 端口。

# 4. 防范措施

高危：目前的样本显示带有破坏性（删除系统盘、注册表等）和后门性质（远控木马），建议提高警惕并安装和更新必要的杀毒软件，不要下载或打开文件名中带有：“武汉肺炎疫情”、“新型冠状病毒”等相关名称，但文件扩展名又为*.exe 后缀，或相关名称的 zip、rar 等压缩包中为*.exe 后缀的可执行文件。