首先确认主机是否被感染

被感染的机器屏幕会显示如下的告知付赎金的界面：

如果主机已被感染：

则将该主机隔离或断网（拔网线）。若客户存在该主机备份，则启动备份恢复程序。

如果主机未被感染：

则存在四种方式进行防护，均可以避免主机被感染。针对未感染主机，方式二是属于彻底根除的手段，但耗时较长；其他方式均属于抑制手段，其中方式一效率最高。
从响应效率和质量上，360 建议首先采用方式一进行抑制，再采用方式二进行

方式一：启用蠕虫快速免疫工具

免疫工具的下载地址：http://dl.b.360.cn/tools/OnionWormImmune.exe
请双击运行OnionWormImmune.exe 工具，并检查任务管理器中的状态。

方式二：针对主机进行补丁升级

请参考紧急处置工具包相关目录并安装MS17-010 补丁，微软已经发布winxp_sp3 至win10、win2003 至win2016 的全系列补丁。

微软官方下载地址：

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-forwannacrypt-attacks/

快速下载地址：

https://yunpan.cn/cXLwmvHrMF3WI 访问密码 614d