日常感防护建议、感染后处置建议

一、日常防护建议

1、做好主机日常安全防护。安装必要的防病毒软件和安全防护软件，及时升级操作系统补丁，我校已为教职员工学生准备了正版windows10操作系统（URL：ms.hfut.edu.cn），更新至最新补丁的计算机在自带的defender保护下可以预防该病毒。

2、养成良好的U盘和网络下载习惯。严格规范U盘等移动介质使用，在使用移动介质前要先进行病毒木马查杀，尤其是U盘根目录下隐藏的autorun.inf，关闭计算机的自动播放功能（详见后文）；不要随意下载安装未知软件，尽量在官方网站进行下载安装；不随意打开或运行未知来源的电子邮件附件，避免恶意邮件攻击。

3、注意重要数据的离线备份。规范重要数据存储，定期做好重要数据备份并离线保存，供磁盘损坏或被恶意删除后能够及时恢复和保全。

二、关闭自动播放功能

以windows10为例：组合键“win”+“R”，在弹出的运行窗口中输入“gpedit.msc”，找到下图1中的“windows组件”的“自动播放策略”，按照图2设置。



图1 windows组件



图2自动播放策略设置

三、感染Incaseformat蠕虫病毒的判定

根据公开信息，感染该病毒的计算机会弹出印尼语图片，感染的蠕虫文件名为tsay.exe，运行后复制自身到Windows系统目录下并创建相应的自启动的注册表值：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\msfsa

Value: String: C:\windows\tsay.exe

如果系统重新启动，会创建并执行文件：c:\WINDOWS\ttry.exe

删除非系统磁盘的文件，并创建文件大小为0K，文件名为incaseformat.log的文件；同时复制病毒自身到D盘，并将病毒文件名命令为删除的文件夹名。

四、感染后处置建议

根据公开信息，该病毒只有启动操作系统执行Windows目录下相应命令时才会触发删除文件行为，因此在发现感染该病毒后请在进行病毒查杀和数据备份前不要重启计算机。

感染病毒后如没有重启：

1、断开主机网络，使用干净（如新格式化的）U盘从其他主机下载主流防病毒和安全防护软件（如360、腾讯、天融信、瑞星等厂商产品）的最新版本（含病毒木马特征库），安装和进行全盘病毒查杀。

2、备份主机重要数据至移动存储介质并离线保存后，再尝试重新启动计算机来验证病毒查杀情况。

感染病毒后已重启：

1、清除病毒。

在任务管理器中结束进程ttry.exe和图标为文件夹的进程；

删除病毒文件：c:\WINDOWS\ttry.exe c:\WINDOWS\tsay.exe

删除非系统盘根目录中的incaseformat.log文件。

2、使用R-Studio等数据恢复软件进行文件恢复。