**Incaseformat蠕虫病毒安全公告**

近期，蠕虫病毒incaseformat大范围爆发，病毒感染电脑后会通过U盘自我复制感染到其他电脑，导致电脑中磁盘文件被删除，给用户造成极大损失。

该蠕虫正常情况下表现为文件夹蠕虫，执行后会自复制到系统盘Windows目录下，并创建注册表自启动，一旦用户重启主机，病毒在Windows目录执行，病毒进程将会遍历除系统盘外的所有磁盘文件进行删除，对用户造成不可挽回的损失。

该病毒于1月13日集中爆发，下次爆发的时间约为**2021年1月23日**和**2月4日**。

　　该蠕虫病毒在非Windows目录下执行时，会将自身复制到系统盘的Windows目录下，创建RunOnce注册表值设置开机自启，且具有伪装正常文件夹行为：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\msfsa，数值: C:\windows\tsay.exe



　　当蠕虫病毒在Windows目录下执行时，会再次在同目录下自复制，并修改如下注册表项调整隐藏文件：

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt -> 0x1

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\checkedvalue -> 0x0

最终遍历删除系统盘外的所有文件，在根目录留下名为incaseformat.log的空文件。



由于文件夹蠕虫感染后没有给主机带来明显的损失，大多数用户都会疏于防范，且文件蠕虫主要通过文件共享和移动设备传播，一旦感染后容易快速蔓延内网。

预防措施：

**1、**重要数据做好备份；

2、安装正规杀毒软件，并将软件和病毒库升级到最新版；

3**、**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；

4**、**尽量关闭不必要的共享，或设置共享目录为只读模式；

**5、** 严格规范U盘等移动介质的使用，使用前先进行查杀；

**6、** 如发现已感染主机，先断开网络，使用安全产品进行全盘扫描查杀再尝试使用数据恢复类软件。