今日，深信服安全团队收到多起 incaseformat 蠕虫事件反馈，已有多个用户感染一种名为 incaseformat（文件名可能为 ttry.exe 或 tsay.exe）的蠕虫病毒，病毒在 windows 目录下运行时会删除 C 盘目录外的所有文件，当前已影响多个区域和行业用户，并具有爆发趋势。

一、 影响行业

多行业，截至目前深信服应急响应中心已发现多个地区多个行业用户在同一天爆发。

二、 相关 IOC

IOC	IOC 类型	目的
4B982FE1558576B420589FAA9D55E81A	MD5	恶意删除文件

三、 检测与防御

1、务必对所有设备安装杀毒软件；如果有使用 edr，请检查 edr 加固策略（主要检查实时监控是否有开启），如果没有安装杀毒软件，可以先部署测试 edr。

2、及时对重要数据进行及时备份。

3、使用 U 盘等外设前，使用安全软件关闭自动播放功能，且对外接设备进行扫描后再继续使用。

4、如果已经中毒，电脑一定不要重启，请联系信息化中心人员协助处理。

☆☆☆重要提示：中招的一定不要重启！一定不要重启！一定不要重启！重启后 数据会丢失。☆☆☆