河南省教育信息安全监测中心

incaseformat 蠕虫病毒

预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2021 年 1 月 14 日

incaseformat 蠕虫病毒预警

事件描述

近期发现一种名为 incaseformat 的蠕虫病毒在国内爆发，该蠕虫病毒主要针对 Windows 系统，执行后会自复制到系统盘 Windows 目录下，并创建注册表自启动，一旦重启主机，使得病毒母体从 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，对系统造成巨大损失。

影响范围

涉及政府、医疗、教育、运营商等多个行业，目前多数感染主机为财务管理相关重要应用系统。

安全建议

一、防御及恢复措施

1、该病毒只有在 Windows 目录下执行时会触发删除文件行为，重启会导致病毒在 Windows 目录下自启动，因此，在未做好安全防护及病毒查杀工作前请勿重启主机。

2、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。

3、尽量关闭不必要的共享，或设置共享目录为只读模式。

4、严格规范 U 盘等移动介质的使用，使用前先进行查杀。

5、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。

二、自查及清除措施

1、检查任务管理器，查看是否有 ttry.exe 进程，如果有，就结束掉进程。

2、文件夹选项勾选显示扩展名，显示隐藏的文件、文件夹或驱动器。

3、查看 C:\Windows 目录下，是否有 tsay.exe 和 ttry.exe，如果有就删除。

4、Win+R 执行 regedit 打开注册表，查看是否有 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\下是否有 msfsa 键的项，如果有就删除。

5、删除各驱动器下的 incaseformat.log。

6、使用各类主流安全产品进行全盘查杀。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052