奇安信
新一代网络安全领军者

incaseformat 病毒事件

安全风险通告

奇安信 CERT

2021 年 01 月 13 日

目录

第1章 安全通告

尊敬的客户：

奇安信 CERT 监测到格格病毒（incaseformat）会在今日发作，表现为电脑中招后，除系统 C 盘以外其他文件全部被删除。奇安信 CERT 研判，该病毒为多年前的老病毒，不具网络传播性，奇安信天擎可支持该病毒查杀和预防，已安装天擎用户不受任何影响，请客户不必恐慌。

奇安信 CERT 将持续关注该事件进展，并第一时间为您更新该事件信息。

第2章 文档信息

文档名称	incaseformat 病毒事件安全风险通告
关键字	incaseformat、格格病毒
发布日期	2021 年 01 月 13 日
分析团队	奇安信 CERT

第3章 事件信息

3.1 事件描述

格格病毒（incaseformat）今日发作，电脑中招后，除系统 C 盘以外其他文件全部被删除。奇安信 CERT 研判，该病毒为多年前的老病毒，不具网络传播性，奇安信天擎可支持该病毒查杀和预防，已安装天擎用户不受任何影响，不必恐慌。

奇安信安全团队发现，格格病毒通过 U 盘等移动存储介质传播，具备定时删除文件的能力，会在特定时间定时发作，删除电脑中除 C 盘之外的其他盘符中的所有文件，并在磁盘根目录创建“incaseformat.txt”文本文档。

奇安信安全专家表示，关于此次格格病毒发作事件，有以下四个需要注意的事实：

1、今天是一个“病毒发作事件”，不是“病毒传播事件”。这个病毒类似“定时炸弹”，如果在机器中潜伏，今天会发作。

2、病毒没有网络传播性，不必恐慌。它是通过 U 盘和文件共享传播的老病毒，最早出现在几年前，一般没有安装杀毒软件的电脑才会中招。

3、因为该病毒定时发作，如果今天未开电脑，建议明日再开机杀毒。

4、对于已经中招的电脑，把专杀放在 U 盘上启动，待杀毒完成后，可请专业公司恢复数据。

病毒相关信息如下：

【恶意程序家族】：incaseformat

【关键字】：#incaseformat.txt　　#tsay.exe　　#ttry.exe

【家族详情】：

病毒类型：蠕虫

传播方式：

1. U 盘隐藏正常文件夹，并替换为同名样本母体

行为特征：

1. 运行后拷贝副本至 C:\windows\tsay.exe、C:\windows\ttry.exe
2. 创建注册表启动项：

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\msfsa　C:\windows\tsay.exe
3. 重启后启动项中的母体文件运行，并删除系统盘以外盘符所有文件，然后释放大小为 0kb 的文件 incaseformat.txt。

3.2 风险等级

奇安信 CERT 风险评级为：高危

风险等级：蓝色（一般事件）

第4章 处置建议

1. 提高员工安全意识，使用 U 盘前用杀毒软件进行病毒扫描后再使用；也可以通过管控功能禁止不明移动存储设备进入内网。

2. 提升内网杀毒软件覆盖率，确保主要终端和服务器均安装有杀毒软件，并定期更新病毒库到最新。

3. 对于不慎感染的终端，使用奇安信天擎进行全盘查杀。查杀前确认信任区是否不明文件，清理信任区之后再进行全盘扫描。

尚未安装的奇安信天擎的用户，可以使用奇安信“格格病毒”（incaseformat）专杀工具，对系统进行全盘扫描，并清除病毒。清理完病毒之后尝试使用专业数据恢复工具或寻找第三方数据恢复公司进行数据恢复。

专杀工具下载地址：http://dl.qianxin.com/skylar6/FocusTool.latest.zip

第5章 产品解决方案

5.1 奇安信天擎终端安全管理系统解决方案

使用奇安信天擎进行全盘查杀。查杀前确认信任区是否不明文件，清理信任区之后再进行全盘扫描。

第6章 参考资料

https://mp.weixin.qq.com/s/k_Uhuvd8kumo5MSlj-HFkA

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT