大家好，比特币病毒上海相信很多的网友都不是很明白，包括比特币病毒事件也是一样，不过没有关系，接下来就来为大家分享关于比特币病毒上海和比特币病毒事件的一些知识点，大家可以关注收藏，免得下次来找不到哦，下面我们开始吧！

本文目录

比特币网络病毒是怎么传播的？

比特币敲诈病毒是最早在2015年初传入中国的，是国外病毒最泛滥的家族之一。随后出现爆发式传播。该病毒通过远程加密用户电脑文件，从而向用户勒索赎金，用户只能在支付赎金后才能打开文件。其最新变种的敲诈金额为3个比特币，约合人民币6000余元。该病毒通过伪装成邮件附件，一旦受害者点击运行，就会弹出类似“订单详情”的英文文档。这时病毒已经在系统后台悄悄运行，并将在10分钟后开始发。但由于此病毒使用匿名网络和比特币匿名交易获取赎金，难以追踪和定位病毒的始作俑者，目前病毒元凶仍逍遥法外。

病毒侵入到大学生的电脑，关系到毕业论文等学术文件与个人信息。曾有学校贴出通知，建议师生防范病毒，有学校贴出通知，细数特币敲诈病毒的危害并提供了应对方法。

为防止毕业论文等重要文件被恶意攻击，腾讯电脑管家第一时间推出“勒索病毒免疫工具”，广大用户可通过官网下载运行，防御勒索病毒攻击。五月份的勒索病毒爆发，腾讯电脑管家就起到了很大的作用。近期推出的“文档守护者2.0”，基于管家的安全防御体系，通过对系统引导，边界防御，本地防御，执行保护，改写保护，备份等多个环节的保护构建完整的防御方案，保护用户的文档不被加密勒索。除支持已知430多种勒索病毒的免疫之外，还能提供对未知的勒索病毒的拦截和备份能力，进一步保证文档安全。

为有个良好的上网环境还是应该下载腾讯电脑管家等杀毒软件。

我就想知道让各大高校瘫痪的比特币病毒到底是什么鬼？

这个病毒叫做“WanaCrypt0r2.0”（WanaCry直译过来，应该叫“想哭”），主

要针对微软的Windows操作系统。

如果你不小心通过点开可疑邮件、未经扫描的附件等方式中招，那么等待你的将是：电脑所有文件会被加密锁定，制作病毒的黑客还会通过修改桌面壁纸和弹窗的方式，温馨提示被感染的机主（病毒提示内容甚至可因地区不同，而翻译成当地不同语言）。需要在指定时间内，支付价值300美元的比特币才能纾困，超时翻倍，拒绝的话，电脑中的文件可能会被彻底清空。

WannaCry病毒攻击的漏洞，是通过微软的Windows操作系统中的网络端口（如445、135、137、138、139端口等）以及网络共享等途径实现感染和攻击。这也解释了为什么中国成为此次病毒攻击的主要受害地区——在中国，教育网因为没有关闭445端口而成为感染重灾区。

对普通用户来说，如果你及时升级，事情没有那么可怕，升级地址：

https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

根据提示升级操作系统补丁就行了。

该病毒与美国国家安全局的黑客工具有关，或者最起码本次袭击借鉴了被泄露的NSA（美国国家安全局，好莱坞大片里经常见到）工具。去年起，一个自称为影子黑客（ShadowBrokers）的组织在网上公布了NSA针对Windows文件与打印机共享系统漏洞的黑客编程代码，但NSA从没有正面承认过。

比特币病毒来了怎么办

1.重装系统，但受感染的文件不能恢复。

2.预防文件丢失与病毒入侵：

(1)数据备份和恢复措施是发生被勒索事件挽回损失的重要工作，因此一定要及时对重要文件数据进行异地备份，防止感染病毒造成损失。

(2)确保所使用的电脑防火墙处于打开状态。

(3)不要轻易打开不明邮件或链接。

如果把比特币病毒和熊猫烧香、冲击波、红色代码之类的老病毒放一起会怎么样？

这次勒索病毒其实不能算是一个真正意义上的病毒，更像是个小孩子搞的“恶作剧”，因为它本身并不破坏电脑系统，只是将某些文件，主要是一些文档，照片和视频等进行加密，而且还留有解密恢复正常的途径，就好像小孩子为了零花钱把你的重要的东西给藏起来了，然后你给钱他就还给你。但传统意义上的病毒则主要以破坏为目的，其过程是不可逆的，所以后果更严重！

好了，文章到此结束，希望可以帮助到大家。