大家好，今天小编来为大家解答比特币勒索病毒t这个问题，比特币勒索病毒贴吧很多人还不知道，现在让我们一起来看看吧！

本文目录

万一自己电脑中了勒索比特币的病毒怎么办？第一时间应采取什么措施？

1、不要给钱。即使交了之后未必能恢复数据。

2、迅速多次备份数据。已中毒的，重装系统前把硬盘低格

3、安装反勒索防护工具，不要访问可以网站、不打开可疑邮件和文件

4、关闭电脑包括TCP和UDP协议135和445端口

5、win7系统格外注意，不要使用校园网落，cmcc也不行

6、还不懂的，把网掐了。

比特币勒索病毒爆发进入高峰期，作为普通的笔记本电脑用户该如何防范它的入侵？

最简单的，升级到最新版本的win10就行了！或者下载一个最新版本的360！老周家的软件早就有解决办法了！

其实没必要担心了，这款病毒是通过445端口入侵的，微软早就把个人系统的445端口给关闭掉了！要不然怎么可能中毒的大多是学校的系统呢！

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。

比特币勒索病毒，不感染win10。只感染win7,这是为什么呢？

445端口在普通用户是关闭的，电信运营商早已过滤，但是高校、政府、某些公司具有特殊性，没有关闭这个端口，所以这次中招的很多都在这类。win10早已更新漏洞，此次win7很多都是没有更新修复漏洞或者没有安装安全软件

好了，文章到此结束，希望可以帮助到大家。