大家好，如果您还对比特币
勒索不太了解，没有关系，今天就由本站为大家分享比特币 勒索的知识，包括比特币勒索的问题都会给大家分析到，还望可以解决大家的问题，下面我们就开始吧！

本文目录

勒索病毒全球泛滥，用比特币支付赎金，是巧合还是变相炒作？

比特币的特殊性有两点：第一，它是全球性的，没有哪个国家能限制它。第二，它的交易是查不到个人的，所以你支付比特币给罪犯，罪犯是相当安全的。它现在涨到一万多一个很正常，因为它就是一个最好的洗钱工具。

在本次比特币勒索病毒风波中有一个反复出现的445端口，是个什么样的存在？

谢邀:445端口和139端口一起是IPC$入侵的主要通道。445它让我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了445，黑客们才有了可乘之机，他们能通过该端口偷偷共享你的硬盘，甚至会在悄无声息中将你的硬盘格式化掉，我们所能做的就是想办法不让黑客有机可乘，就要封堵住445端口漏洞。

比特币勒索病毒有人中了吗？毕业论文加密了怎么办？

如果你提前备份了或者发给过导师或其他人，，，还好说。如果没有，先试试360近期发布的病毒文件解锁补丁，据说可以解锁部分文件。如果还不行，就重新抓紧赶一份吧，网上的一些恢复视频我看了一些，靠谱的不多

比特币勒索邮件怎么处理？

比特币勒索邮件是指邮箱里收到一封电子邮件，邮件的内容一般含有：电脑上的恶意软件已经通过网络摄像头捕获到了收件人的不雅照片、知道收件人的真实密码等，让收件人产生恐惧，并要求以“比特币”的形式支付封口费。

这种比特币勒索邮件的内容往往是以英文或者日文的形式出现，如下图：

英文版

日文版

这种勒索邮件并不可信

这种手法其实是特别拙劣，你的电脑也没有所谓的恶意软件和木马。真正的恶意软件勒索长这样：

并且电脑内的文件都会被加密。对于黑客而言，他通过木马获得密码，也会直接使用病毒勒索，而不是使用门槛最低的邮件。

那勒索邮件内的密码，是从哪里获得的呢？

密码可能并不是从我们本地的电脑泄露的，而是由一些网站或平台因为各种原因，泄露了用户的账户名或明文密码。

一些黑客就将他们打包成“数据包”，在暗网上公开出售。而这些账户，大多为邮箱名，所以只能通过邮件进行敲诈勒索。

举个例子：

2011年CSDN曾曝出遭遇密码泄露事件，600万用户信息被泄露。随后，密码泄露事件波及天涯论坛等网站，4000万账户密码陆续遭泄露。这些密码，全部都是以明文的形式泄露，成为了敲诈勒索的渠道。

这种勒索邮件只是最普通的勒索方式，可怕的是针对特定对象的定制勒索。比如勒索邮件中附带的一张PS的“不雅照片”，这种PS痕迹是比较严重的，只有头像是自己的，照片中的身份和背景并不是自己的。

为什么勒索比特币？

与比特币相关的勒索案件屡见不鲜，花样百出，就是比特币匿名、难以追踪，一串私钥就对应一笔“钱”，正好符合勒索人的需求。

与常见的货币不同，比特币不依靠特定的货币机构发行，它只是依据特定的算法通过大量的计算产生，所以它可以绕开银行系统，并且可以轻易的跨国交易。比特币

使用这个P2P网络中众多节点构成的分布式数据库来确认、记录交易行为，并使用密码学设计来确保各个环节的安全性。这些都让比特币具有了不易溯源，不会暴露身份，而且可以快速广泛流通。

在很多人眼中，“自带光环”的比特币成为了争取货币自由、实现资产增值、发展致富技术的有声力量，但它还有着另一幅面孔：犯罪分子的帮凶。

中国互联网金融协会发布《关于防范比特币等所谓“虚拟货币”风险的提示》，称比特币等所谓“虚拟货币”缺乏明确的价值基础，比特币等所谓“虚拟货币”日益成为洗钱、贩毒、走私、非法集资等违法犯罪活动的工具，投资者应保持警惕，发现违法犯罪活动线索应立即报案。

收到比特币勒索邮件该怎么办？

一般情况下是可以忽略这种邮件，因为这种邮件都是大规模群发的，虚晃到一个是一个。如果涉及到真实的账户和密码，可以分析一下是通过什么渠道泄露出去的，并且马上更改一些重要的密码。

如果勒索人通过邮件还会有下一步的行动，并且确实掌握了很多重要的资料。那么无论如何都不要给勒索人转比特币，这绝对是一个无底洞，保留好所有的证据，报警是好的选择。

以上个人浅见，欢迎批评指正。

认同我的看法，请点个赞再走，感谢！

喜欢我的，请关注我，再次感谢！

好了，文章到此结束，希望可以帮助到大家。