很多朋友对于比特币内网安全吗和比特币网站安全吗不太懂，今天就由小编来为大家分享，希望可以帮助到大家，下面一起来看看吧！

本文目录

比特彗星是干什么的

BitComet(比特彗星)是一个完全免费的BitTorrent下载管理软件，也称BT下载客户端，同时也是一个集BT/HTTP/FTP为一体的下载管理器。

BitComet拥有多项领先的BT下载技术，有边下载边播放的独有技术，也有方便自然的使用界面。

最新版又将BT技术应用到了普通的HTTP/FTP下载，可以通过BT技术加速您的普通下载。

假如回到比特币刚刚发行的时候，有人劝你，买十块钱儿的你愿意吗？

我怀疑我曾经穿越过！我清楚地记得，在2010年前后，我曾经看过一部描写比特币的小说，里面就讲到了比特币，从一文不值到后来可以值几万美元一枚。看了小说以后，我也很心动。我就上淘宝搜了一下，但是没有比特币的交易商家。然后我在百度上搜了以后，下载了比特币的挖矿程序和钱包。但遗憾的是，因为我是中专生，英语不行，当时程序是全英文操作的，我实在是搞不懂，就没有能开始挖矿（补充一点，当时我们单位有个小的局域网，有二十多台电脑连着外网，要是我搞懂了怎么挖矿的话，这些都是我的机器，而且在当时的情况下，根本不用考虑电费什么的）。后来到2014、2015年前后，比特币开始小火的时候，我折回头去找那本小说，却再也找不到了。到目前为止都再也没有看到过那本小说，而且我问了很多喜欢看网络小说的网友，都说没有看过这本小说。我怀疑我是在平行空间里面看过或者是穿越的时候看过的，不然无法解释我记忆里的这个问题。所以说这辈子最遗憾的就是上学时没有学好英语，错失了一个发财的机会，抱憾终身！[快哭了][快哭了][快哭了]

全球爆发大规模勒索病毒，网络安全概念股都高开了，现在买进还来得

及吗？

回答这个问题前需要先讲下什么是“勒索病毒”

这款勒索病毒是利用微软的几个月前的一个漏洞“永恒之蓝”进行攻击的。病毒发作表现为用户的文件被大量锁死，需要支付赎金才能解密。

其实只要用户按时下载补丁，进行更新升级是不会发生感染的。在今年的3月份微软公司已经发布补丁，可以对漏洞进行修补。只是很多用户没有及时下载补丁的习惯，特别是一些公司和机关的内网。

所以此次的“勒索病毒”只是局部的，没有及时安装补丁的一部分电脑。自从病毒爆发以来，世界上众多网络安全公司已经采取安全防范措施，没有中毒的用户只要下载安全补丁即可，中毒的用户只要断网查杀后就能控制住病毒。但是已被锁死的文件暂时无法解密，需要有关网络安全公司慢慢研究解密对策。

所以这次的“勒索病毒”已得到有效的控制，而且也无需什么新的高新技术解决。既然形势没有那么严峻，那么相关网络公司在业绩上就不会获得实质上的高额收益帮助。

在我国A股市场上像蓝盾股份这样的做网络安全的公司并不多，很多涨停的网络安全概念股并不是做网络安全的。像拓尔思与数字认证这样的公司并不是做网络安全的，也被封于涨停板。

可见这就是种概念炒作。

对待概念炒作，在投资中要做到快进快出。要在市场没有搞清其真相时，利空或利好有多大时，在消息朦胧时买入，在利好实施或真相大白前迅速卖出。很显然现在已经到了接近真相大白的时侯了。

现在买入就好比盛宴快结束时，有人冲进了进去。等待他的十有八九是没吃几口就被迫买单。

紧急求助！如何预防比特币病毒？

以支付比特币换取解密为特征的计算机病毒来势汹汹，世界多国计算机均已中毒，其中英国和中国尤为严重。昨天今天被该病毒的消息涮屏了，该病毒危害性不少，特别是面临毕业季，很多学生的论文存在丢失的巨大风险。

首先说如何预防，我的建议是，作为个人计算机用户，首先要关闭445端口，下载微软补丁完成修复，推荐下载360提供的NSA武器库免疫工具，完成该病毒的防护，下载地址连接http://dl.360safe.com/nsa/nsatool.exe

此次病毒于5月12日晚在我国校园网开始蔓延。据360分析分析，该病毒是由NSA泄漏的“永恒之蓝”黑客武器传播的。“永恒之蓝”可远程攻击Windows的445端口，该端口方便用户在局域网中轻松访问各种共享文件夹或共享打印机。

用户计算机如果之前安装的2017年3月的微软补丁，则不会中招。之前由于国内曾多次出现利用445端口传播的蠕虫病毒，中国电信等运营商对个人用户封掉了445端口，但教育网并无此限制，存在大量暴露着445端口的机器，因此成为不法分子使用NSA黑客武器攻击的重灾区。

根据360公司周鸿祎的说法，目前“永恒之蓝”传播的勒索病毒以ONION和WNCRY两个家族为主，受害机器的磁盘文件会被篡改为相应的后缀，图片、文档、视频、压缩包等各类资料都无法正常打开，只有支付赎金才能解密恢复。这两类勒索病毒，勒索金额分别是5个比特币和300美元，折合人民币分别为5万多元和2000多元。

根据360针对校园网勒索病毒事件的监测数据显示，国内首先出现的是ONION病毒，平均每小时攻击约200次，夜间高峰期达到每小时1000多次；WNCRY勒索病毒则是5月12日下午新出现的全球性攻击，并在中国的校园网迅速扩散，夜间高峰期每小时攻击约4000次。

其实，针对NSA黑客武器利用的Windows系统漏洞，微软早在2017年3月已发布补丁修复。360公司也已推出NSA武器库免疫工具，能够一键检测修复NSA黑客武器攻击的漏洞，对WindowsXP、2003等已经停止更新的系统，免疫工具可以关闭漏洞利用的端口，防止电脑被NSA黑客武器植入勒索病毒等恶意程序。

如果你还想了解更多这方面的信息，记得收藏关注本站。