大家好，今天来为大家分享比特币勒索病毒攻击的一些知识点，和比特币勒索病毒攻击原理的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

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

什么是比特币？比特币如何产生的？

首先我们要知道，比特市不是政府发行的，不是由中国人民银行发行的，它是从2009年才开始有的，它通过P2P分布式网络来核查重复消费，比特币通过下载客户端可以制造比特币，不存在伪造行为，它是通过一套密码编码通过复杂的算法产生的，每四年比特币的数量会减半，所以比特币很值钱。

2/6

其实比特币在现实生活中也在应用，如：四川芦山地震时中国第一次允许用比特币作为捐赠物，其实也就是从那时起比特币才开始火热起来，大家很好奇比特币是什么东西，才开始认识这个东西。

3/6

我们如何得到比特币呢？其实大家也知道有两种方法：

一种方法就是到网络市场上去买，根据与人民币的换算去购买，现在差不多，一比特币要换5000多元人币吧。

另外一种方法就是通过下载客户端进行计算特定数量的数学问题来获得比特币。

其实第二种方法也并不是这么容易就能够获得的，也需要很大的成本才能赚到，我的一个朋友运行了几天才赚到0.0016比特币，很难，可能与方法，电脑也有一定的关系。

4/6

现在有很多人用比特币进行投资，其实说实话也在用这个东西投资还有一定的风险的，国家现在还没有承认这个东西的合法性，现在很大程度上只是在网络上进行交易，也有一部分人用于黑市交易，最近一段时间内比特币肯定会升值，但是就要看下一步政府怎样对网络进行监管，因为现在网络监管很滞后，网络上产生的很多问题，现实中没有人去解决，可能政府现在也是心有余力不足，没有找到合适的方法，

5/6

想象一下，目前全球没有一个统一的货币在运行，也都通过兑换的形式进行操作的，如果比特币能够担当这个重任的话，势必是个好事情，现在通过虚拟的形式比特币已经可以买到现实生活中的所有的东西了，尽管政府现在还不承认，但是它已经很现实的存在了。但是很多人认为比特币是一个阴谋，是用后人的精力或财力为前人做事。也就是说现在我们对比特币这么热衷其实钱早被最早的人赚去了。

6/6

比特币与QQ币的区别：

比特币不属于任何一个国家或公司或团体，它广泛的存在于网络当中，目前可以和任何一个国家的货币进行兑换，现在各个国家对它都很重视，虽然没有成为法定货币。

QQ币属于腾讯公司，现在腾讯公司大力推广这个QQ币，其它团体或公司很少有推广这个东西，因为这样不会给它带来任何利益。

黑客明知勒索比特币不会有什么效果，是为了炒作比特币吗？

如果从更深层次来说，这次攻击是网络战的一次试探，因为病毒的源头是FBI，勒索不在多少，比特币只是个掩护，替罪羊罢了。中美战争不会发生实战的，经济战、贸易战、网络战、太空战也是摧毁对方的手段。

比特币勒索病毒怎么回事？

比特币勒索病毒比起多年前的熊猫烧香，显得更凶猛。

中招的吃瓜群众感到好奇也是不奇怪的，那就简单的介绍一下吧。

这款病毒通常被称做“WannaCry”，中文意思即“想哭”。不过也有人指出，病毒的真正名字是WannaDecrypt0r2.0，含义是交钱解锁。

中毒之后，该病毒将会加密计算机硬盘中的大量文件，并修改文件的后缀名。随后弹出勒索窗口，要求在指定时间内支付约合300美元的比特币到给出的账户，否则将不能解密。勒索病毒很贴心地提供了28国语言。其勒索界面还郑重承诺：

“请您放心，我是绝不会骗你的。”“对于半年以上没钱付款的穷人，会有活动免费恢复。”

想必这也不是一个普通的勒索团伙，是一个渴望发展成连锁加盟级别的病毒运营团队也说不定。

这次涉及范围可谓是很随意，下至WinXP小屁民，上至官方机构，丝毫不介意感染对象。

放眼全世界，英国、俄罗斯、西班牙、台湾、德国才叫损失惨重。英国多家公立医院的医疗设备也都沦陷，甚至导致X光机都无法工作。德国更是悲惨，连火车站的电子看板都惨遭勒索。

如此庞大的感染情况其实也没有引起太多惊慌，感染五天时，该病毒收到了45笔勒索资金，共获利8个多比特币，约合人民币10万元。

平摊到“病毒官方”提供的三个账号后，几乎是扫一眼就看完了付款人。

官方提供的三个账号：

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn；

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw；

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

但可不要因此小看这次的勒索病毒，它的来头可不小。

一位不愿意透露姓名的美国前官员表示，WannaDecrypt0r2.0勒索病毒可能就是利用NSA武器库中的“EternalBlue”制作的。这也是一些媒体称该病毒为永恒之蓝的原因。

这次的WannaDecrypt0r2.0病毒，其传播方式是利用了一个Windows系统中445端口的一个漏洞。这个漏洞正是来自于美国国安局。而这个445端口的漏洞是NSA精心准备的“武器库”当中的一员。

原本依靠这个漏洞，可以进行强有力的打击。不仅如此，NSA拥有多种武器，足以入侵包括iPhone、Android、Windows、Mac各种系统，甚至连智能家居等物联网系统也难逃魔掌。

NSA的行为令人发指。

在去年的4月份，一个自称“ShadowBrokers”的黑客组织盗取了NSA的这款大杀器。

本打算高价竞拍这个漏洞豪赚一笔，但最终据说是因为对新总统川普的抗议，“ShadowBrokers”选择免费在网络上公开了这个漏洞。

WannaDecrypt0r2.0的作者拿到了这个永恒之蓝漏洞，针对性地制作出了这款传播力极强的勒索病毒。

永恒之蓝几乎让全世界都中了招，可以说唯一没有受到伤害恐怕只有网络封闭的朝鲜。

估计朝鲜也没想到会以这种形式成为这场网络战争的最后赢家。

文章到此结束，如果本次分享的比特币勒索病毒攻击和比特币勒索病毒攻击原理的问题解决了您的问题，那么我们由衷的感到高兴！