比特币病毒通过135.137.138.445的端口入侵你的电脑。

感染比特币病毒后，他会锁定你电脑上的所有文件。如果你想打开它，你需要输入密码。你不&#039；我没有密码，所以他让你给他寄钱。，然后为您解锁。但是唐&#039；不要寄钱。自从他赢了&#039；不要松绑你，他只会要求更多。

我明天去了电子阅览室。我插上u盘没多久，老师突然大声说要我拔掉u盘。有同学发现u盘里的文件在本地打不开。又有两份文件要钱。

于是我匆忙检查了一下自己，学校电脑里插的东西都中毒了，早上还发生了大规模的电脑中毒。许多人&#039；s的资料和毕业论文都在电脑里，真的让黑客这么做很恶心。为了钱，不顾学生&#039；出路，教师&#039；终身科研效应.

希望尽快抓到有功人员，给予法律严惩！

什么是比特币病毒？

据百度百科，比特币勒索病毒(CTB-洛克)于2015年底首次传入中国，随后发生生成式传播。该病毒对用户进行加密&#039；电脑文件进行远程操作，从而向用户勒索赎金，用户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，对于群众来说约为6000元。该病毒伪装成电子邮件附件，一旦受益人点击运行，一个类似&quot订单摘要&quot会弹出来。这个时候，病毒习惯在系统后台悄悄运行并将在10分钟后发动攻击。

病毒发布者使用的是美国国家安全局(NSA)独立想象的Windows黑客工具永恒之蓝(EternalBlue)，该工具于去年被盗。去年2月暂停升级的一款勒索病毒的产品叫做WannaCry。

这种病毒会扫描封锁445文件共享端口的Windows设备，只要用户&#039；的设备已打开并联机。黑客可以在电脑和效应器中植入勒索软件，远程掌握木马、虚拟货币矿机等恶意指令。

有平安研究人员指出，这次大规模网络攻击似乎是由一个蠕虫病毒安排的。WannaCry可以在计算机之间进行通信。什么&#039；更可怕的是，与大多数恶意订单不同，这种订单可以自动停止在网络中的复制和传播，而未来大多数病毒都需要依靠被招募的用户来传播。规则是他们在诈骗后点击带有攻击代码的附件。

这次攻击曾经影响了99个国家，多达75000台电脑，但是由于这种病毒利用匿名网络和比特币进行匿名买卖，从而获得了赎金。追踪和定位病毒的始作俑者相当困难。

很多电脑用户发现自己的电脑操作系统失效，比如感染了电脑病毒的电脑，在电脑系统无法自动修复的情况下，风险非常大。而电脑病毒的结果是非常严酷的。自从计算机病毒诞生以来，网络安全人员就一直在向计算机病毒低头，但由于世界十大黑客的存在，以及世界上最安全的软件被禁，一些计算机病毒还是被传染了。，给电脑用户带来了非常严重的损失。

全球十大最强大的计算机病毒

10:闪回计算机病毒

？9:比特币病毒

？8。我的末日，我的爆炸

？7:地震台网

？6:Conficker蠕虫

？5.宙斯电脑病毒

？4:冲击波病毒。

？3.梅利莎

？2.红色电脑病毒代码

？1.伊洛维尤病毒

10。闪回电脑病毒

这种病毒的破坏力不如其他电脑病毒。它只会闪回存储在你电脑里的文件，让你的电脑恢复到以前的样子。这种病毒于2011年被发现，目前还没有找到一种方法来对付它。

9:比特币病毒

该病毒针对Windows系统的电脑。它主要通过电子邮件传播。一旦感染病毒，你的电脑将无法使用。你只能通过支付赎金来恢复电脑的使用。这种病毒已经造成了大约2000万美元的损失。

8:MyDoom？

这个病毒在2004年浮出水面，作者至今一无所知。这种病毒叫做&quot安迪，这种电脑病毒会让用户&#039；无法执行一般任务的计算机。据估计，该病毒曾造成3850万美元的损失。有些情况，明天还历历在目。

7:地震台网

据说这种病毒是美国政府和以色列国防军共同研发的，也就是说是为网络战制造的，这种病毒确实援助了两国政府。这样他们才能意识到伊朗可以停止对其他国家的核攻击。这种病毒可以以某种方式进入任何计算机，并完全扫描计算机外部的存储数据。

6:conficker蠕虫

这种病毒出现在2008年，它感染了900多万台计算机，造成了约90亿美元的损失。Conficker病毒在通过任何使用Windows的电脑接触Conficker病毒时都会受到影响。然后，它延迟设置的软件会把电脑变成僵尸网络来恐吓和骗取用户的财富。

5:宙斯电脑病毒

这是一种特洛伊木马制作的宙斯电脑病毒，影响Windows序列的电脑。这样他们就可以停止他们的功勋活动。据估计，已有100万台电脑被感染，大约7000万美元的被感染电脑用户被病毒制造者窃取。

4:冲击波病毒

这种病毒在2004年首次被发现。这个病毒是一个名叫斯文贾森的学生写的计算机迷信。它是世界上第四大病毒。它不仅影响数百万台计算机，还会破坏主要的基础设施。梅利莎

这种计算机病毒是以佛罗里达州的一名脱衣舞女命名的，由一个名叫大卫史密斯的人于1999年创建。病毒的载体是一个被电脑病毒感染的Word文档。据报道该病毒造成了高达8000万美元的损失。制造病毒的人被指控并被判10年监禁。释放，但最终他在支付5000美元保释金后，仅在监狱服刑20个月后被释放。2:红色计算机病

毒代码

红色代码病毒于2001年首次出现。发现病毒的人是两名网络安全工程师。这种病毒被命名为&quot红色病毒代码&quot因为两名工程师在喝红酒时发现了病毒。这种病毒已经袭击了许多主要的中心。例如美利坚合众国的白宫。该病毒造成了高达20亿美元的损失。

1:iloveyou病毒

这种病毒被认为是迄今为止已知的最危险的计算机病毒之一。据说是两个菲律宾人依次发明的。该病毒利用社交媒体平台，它会弹出一个弹窗通知用户点击链接，提示这是一个关于爱情的效果。用户往往不了解这些链接中包含病毒，点击后电脑就会被病毒感染。目前，病毒造成的损失高达100亿美元。

比特币勒索软件wanacry介绍：[XY002][XY001]WANACry(也叫WannaDecryptor)，一种蠕虫状勒索软件，大小为3.3MB。犯罪分子利用激进的风险漏洞&quot永恒的蓝色&quotNSA(美国国家安全局)停止通信。

该恶意软件会扫描电脑上的TCP445端口(服务器消息块/SMB)，以类似蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后乞求以比特币支付赎金。。勒索的金额是300到600美元。

2017年5月14日，WannaCry勒索软件出现变种：WannaCry2.0，KillSwitch被撤销，传播速度更快。截至2017年5月15日WannaCry造成了至少150个国家的网络攻击，影响了金融、电力、医疗等行业，造成了严重的危机管理效应。国内部分Windows操作系统用户被感染，校园网用户首当其冲，受益严重。大量的实验室数据和毕业想象被锁定加密。

目前安全行业还未能有效摒弃这种勒索病毒的恶意加密行为。微软总裁兼首席法律官布拉德史密斯(BradSmith)表示，国家安全局没有披露更多安全漏洞。，给了有功组织可乘之机，最后带来了这次攻击150个国家的勒索病毒。

数据引用：百度百科

2017年，从5月12日开始，一种具有勒索本质的比特币病毒在全球范围内传播。。目前，许多国家已被攻击：中国，澳大利亚，美国，英国，俄罗斯，西班牙和其他超过99个国家。医院、学校、企业等社会机构的20万台电脑被攻破，病毒以每小时500万封邮件的速度传播。，拉开了世界&#039；史上最大的病毒入侵。

首先，可以选择比特币作为这次入侵的交易方式，因为它的便捷性和隐蔽性。作为一种网络虚拟货币，它是非国有化的产物，是货币规律安排的。在网络音频时期，梦想和生活是相互联系的，越来越多的人进入虚拟世界并相互交流。可以在死亡世界的任何中心兑换，不受地域限制，难以追踪。从2014年开始，比特币在西方国家末期开始流行，并逐渐获得了极佳的口碑。依托比特币的洗钱、敲诈等非法交易愈演愈烈。这一次，黑客以危害国家公共安全罪为代价，利用比特币赚黑费。

其次，美国攻击力弱。。比特币病毒是一种病毒攻击软件，由犯罪分子利用激进的&quot永恒的蓝色&quotNSA(国家安全局)黑客武器库。永恒之蓝(EternalBlue)是美国情报机构发现Windows系统电脑漏洞并针对漏洞开发多种攻击软件的工具。。通常是一些软件泄露，被黑客利用，与勒索病毒区分为比特币病毒，可以入侵你的电脑，自行实施勒索。这一次生成的规模暗示了美国潜在目标的范围。

同样，由于依赖，所以更安全。科学技术的传播导致了我们比以往任何时候都更加依赖的网络时代。黑客是伴随着网络的，要多注意自己的维护，要有足够的音频安全洞察。"我迫切需要大规模杀伤性武器。但我认为核战争的可能性低于生化武器和网络攻击。"巴菲特一倒下，比特币病毒就在生成。国内很多高校之所以招人，是因为学校里的网络基本上是大范围互联的，线路没有按照特殊岗位划分区域说深一点，任何一台电脑都可以连接到学生系统，一直到教务系统。没有合理细化的软件，一旦病毒攻击校园计算机网络共享，音频安全不堪重负。IP组的大多数病毒都是通过邮件和未知链接入侵的。我们没有建立警惕心的习惯，给了病毒可乘之机。一个敌人说：&quot我以前防范过电脑提供的这些共享功能，然后这次没有被攻击，没有连接。"而win10在3月份修补了这个效果。生成是在五月。也就是微软&#039；的父亲会说，&quot哇，我可以&#039；也不是。如果分发针头，没有人想打。""所以为了大众的利益，我们应该深入思考我们是否能理解我们正在使用的工具。预防会没用吗？

最后，我要通知自己。假设已经被攻击了，付费可能不可行。我希望我们都能信任我们的国家政府，不要害怕病毒。