昨天，我去了电子阅览室。我插上u盘没多久，老师突然大声说，大家把u盘拔了。有同学发现u盘里的文件都打不开了，还有两个文件需要钱。

于是大家都急着看。只要学校电脑里插的u盘中毒，晚上就会出现大规模的电脑中毒。许多人&#039；的资料和毕业论文都在电脑里，我真的觉得黑客这种行为很恶心。为了钱，不管学生&#039；未来，教师&#039；终身科研成果.

希望尽快抓到罪犯，让他们受到法律的严惩！

什么是比特币病毒？

根据百度百科，2015年初比特币勒索病毒(CTB-洛克人)首次传入中国，随后爆发式传播。。该病毒通过远程加密用户的电脑文件向用户勒索赎金，用户只有支付赎金后才能打开文件。

其最新变种勒索金额为3个比特币，约合6000元人民币。该病毒伪装成电子邮件附件一旦受害者点击运行，一个类似于&quot订单详情&quot会弹出来。此时病毒已经在系统后台悄悄运行，10分钟后会开始发作。

该病毒发布者利用去年被盗的美国国家安全局(NSA)设计的Windows黑客工具永恒之蓝(EternalBlue)，在今年2月升级了一款勒索软件。它叫做WannaCry。

该病毒将扫描打开445文件共享端口的Windows设备。只要用户&#039；设备在互联网上，黑客可以将勒索软件、远程控制木马、虚拟货币矿机等恶意程序植入电脑和服务器。

一些安全研究人员指出，这种大规模的网络攻击似乎是通过一个蠕虫应用程序部署的，WannaCry可以在计算机之间传播。更可怕的是，与大多数恶意程序不同，这种程序可以在网络中自我复制和传播。目前大部分病毒还是需要依靠被招募的用户，通过诱骗他们点击带有攻击代码的附件来传播。

这次攻击影响了99个国家和多达75，000台计算机。然而，由于这种病毒使用匿名网络和比特币匿名交易来获取赎金，因此追踪和定位病毒的发起者相当困难。

&quot；比特币勒索者&quot病毒再次变异窃取个人隐私

The&quot；比特币勒索者&quot今年1月首次在中国出现的病毒，已经呈指数级爆发。腾讯&#039；s反病毒实验室最近发现该病毒很疯狂，仅5月7日一天新变种数量就达到13万，不仅敲诈用户，还窃取个人隐私。。腾讯反病毒实验室分析认为

，从攻击源头来看，这是一场由黑客控制的僵尸网络以webmail为传播载体发起的风暴。

&quot；比特币勒索者&quot呈指数级爆炸

比特币是一种新型的网络虚拟货币。因为可以兑换成大多数国家的货币，所以在世界各地广受追捧。与此同时，一个&quot比特币勒索者&quot名为&quotCTB储物柜&quot也在世界各地肆虐，它通过远程加密用户电脑中的文档、图片和其他文件来勒索赎金。否则，这些加密文档将在指定时间被永久销毁。

僵尸网络帮助&quot比特币勒索者&quot越来越猖狂

根据腾讯&#039；的反病毒实验室，大多数攻击的来源&quot比特币勒索者&quot来自美国，其次是法国和土耳其。。从IP的角度来看，这些攻击来自黑客控制的一个僵尸网络，黑客利用这个僵尸网络发起邮件风暴。邮件内容多是收发票之类的，诱导用户点击下载附件。

&quot；比特币勒索者&quot攻击来源

所谓僵尸网络，是指通过一种或多种通信手段，使大量主机感染Bot病毒，在控制者和被感染主机之间形成的一对多的可控网络。。攻击者通过各种渠道传播僵尸程序，感染互联网上的大量主机，被感染的主机会收到攻击者&#039；s指令通过控制通道形成僵尸网络。

据了解，使用了僵尸网络这个名称。，以使人们更形象地认识到这种危害的特点：许多计算机像中国古代传说中的僵尸一样被驱动和指挥，成为人们使用的工具。

僵尸网络帮助&quot比特币勒索者&quot越来越猖狂

国家互联网应急中心监测的最新数据显示，仅2014年上半年，我国就有超过625万台主机被黑客用作木马或僵尸网络，1.5万个网站链接被用于传播恶意代码，2.5万多个网站被植入后门程序。已捕获移动互联网恶意程序36000余个，信息系统高危漏洞1243个。

腾讯反病毒实验室安全专家表示，僵尸网络构成了攻击平台，可以有效发起各种攻击。，可导致整个基础信息网络或重要应用系统瘫痪，也可导致大量机密或个人隐私泄露，还可用于从事网络诈骗等其他违法犯罪活动。无论对全网还是对用户本身，都造成了严重的危害。。"比特币勒索者&quot利用僵尸网络发动邮件风暴，实施各种攻击。

&quot；比特币勒索者&quot可以窃取隐私

据了解，&quot比特币勒索者&quot病毒具有高隐蔽性、高科技犯罪、高勒索金额、攻击高端人群、中招风险高等特点。一旦用户被招募，，病毒将浏览所有文档(后缀为。txt，doc，zip等。)和图片(后缀为。jpg，png等。)，并对这些文件进行加密，以便用户可以&#039；不要打开它们。用户必须支付一定数量的&quot比特币&quot作为恢复文件内容的赎金。。

用户需要支付赎金才能解锁文件

腾讯的监控数据&#039；美国反病毒实验室显示，自今年4月以来，流行的&quot比特币勒索者&quot一直是最严重的。为了有效攻击，避免检测到静态签名，病毒在不断进化。，图标多为文档图标(如doc、pdf等。)，而且它们的外壳不断变形变异。其中新品种在5月7日达到最高值，单日高达13万只！

&quot；比特币勒索者&quot

腾讯安全专家&#039；美国反病毒实验室表示，最近发现的&quot比特币勒索者&quot病毒不仅勒索用户，还增加了盗取号码的功能，在用户中默默收集密码配置文件&#039；电脑，比如邮箱的密码，聊天工具，网银账号，比特币钱包等等。，威胁用户的安全&#039；财产。目前，腾讯&#039；s安全团队第一时间对该病毒进行了深入分析，可以完美查杀此类病毒及所有变种。

安全专家采取防范措施赎回文件需要数千元

据路透社报道，&quot比特币勒索者&quot病毒来自一个名叫艾维盖尼耶米哈伊洛维奇波格契夫的俄罗斯黑客。有了这种勒索木马病毒，12个国家的100多万台电脑被感染，经济损失超过1亿美元。美国联邦调查局(FBI)官网显示，博格切夫在FBI排名第二&#039；他是一个网络犯罪集团的头目。。美国联邦调查局悬赏300万美元缉拿博格切夫，这也是美国在打击网络犯罪案件中悬赏的最高金额。

专家强调，正是因为危害巨大，FBI才会奖励抓到病毒作者这么高的奖金。用户一旦被招募，就意味着合同的电子版多年的老照片，刚刚写好的平面图，刚刚做好的设计图，都在病毒的加密下无法打开。病毒制造者主要利用用户&#039；急于恢复文件勒索，而且成功率极高。据悉，虽然比特币最近走势低迷，但单笔交易价格也在1391元左右(4月20日更新数据)，所以虽然是勒索几个比特币，但对用户来说也不是小数目。

专家提醒不要轻易下载来源不明的文件，尤其是带有后缀的文件。exe。,scr可执行

文件，don&#039不要仅仅通过图标来判断文件的安全性。另外，我平时养成了把一些重要文件备份到移动硬盘和网盘的习惯，一旦被木马感染，可以及时补救。

什么是勒索软件？

1。WannaCry病毒不同于其他类似的勒索病毒。它是一种可以自动感染其他电脑并传播的蠕虫病毒，由于连锁反应而迅速爆发。

2。这个勒索软件主要感染Windows系统。它会利用加密技术锁定文件，禁止用户访问，以此来勒索用户。

3。攻击者声称，只有索要上述价值300美元的比特币，才能解锁文件。实际上即使支付了赎金，文件也可能无法解锁。

为什么会感染？

勒索蠕虫一旦攻击一台可以连接公网的用户机器，就会扫描内网和公网的ip。如果被扫描的ip打开端口445。，您将使用&quotEnternalBlue&quot安装后门的漏洞。一旦后门实现，就会释放一个名为WanaCrypt0r的勒索病毒，从而加密用户身上的所有文档文件&#039；勒索的机器。

为什么要用比特币？

比特币是一种点对点的网络支付系统，也是一种虚拟的定价工具，俗称数字货币。比特币非常受网络犯罪分子的欢迎，因为它是分散的，不受监管的，几乎难以追踪。

传播感染背景

此轮勒索蠕虫病毒传播主要包括洋葱和WNCRY两个家族变种。一是在英国、俄罗斯等国爆发，很多企业、医疗机构在体制内中招，损失非常惨重。

安全机构的全球监测发现，多达74个国家受到了这种勒索蠕虫的攻击。

从5月12日开始，我国的感染传播也开始急剧增加，多所高校和企业的集中爆发愈演愈烈。

wannacry勒索病毒的防范方法：

1。为计算机安装最新的安全补丁。Microsoft已发布修补程序MS17-010来修复&quot永恒的蓝色&quot进攻。，请尽快安装此安全补丁；对于windowsXP、2003等微软不再提供安全更新的机器，我们可以使用360“NSA武器库免疫工具&quot检测系统是否存在漏洞，关闭受漏洞影响的端口。，可以避免被勒索软件等病毒入侵。

2。关闭端口445、135、137、138和139，并关闭网络共享。

3。加强网络安全意识：don&#039不要点击未知链接，也不要&#039；不要下载未知文件。唐&#039；不要打开未知的电子邮件.

4。尽快(以后定期)将电脑中的重要文件备份到移动硬盘和u盘上，备份后离线保存磁盘。

5。建议还是用windowsxp。，windows2003操作系统的用户应尽快升级到windows7/windows10或windows2008/2012/2016操作系统。

这种比特币勒索病毒一旦安装到电脑中，计算机上的所有文件数据都将被强制加密。如果你不&#039；不要付&quot赎金&quot以比特币的形式交给病毒制作者，那么这些文件就不会被解密和检索。即使这次你付了赎金，你也可能&quot光顾&quot下次吧。也就是说，这种病毒会对重视数据的用户，尤其是企业用户造成不可估量的伤害。

1。为什么叫比特币勒索软件？

所谓的比特币勒索病毒其实是一种&quot不对称文件加密&quot病毒。

感染此病毒的电脑硬盘中的文件会被以特殊方式加密。除非从病毒制造者处获得相应的密钥，否则永远无法解密，即使重装系统，使用数据恢复软件，也就是说，解密失败意味着文件已被病毒破坏。

解密的唯一方法是支付&quot赎金&quot给有比特币的病毒制造者，但即使你真的付了钱，对方也未必真的帮你解密。因为比特币的交易是不可追踪的，也就是说，如果你真的妥协了，向它交了钱，那么你很有可能面临着赔钱、销毁数据、根本拿不到勒索者的窘境。

这种&quot杀票&quot就是在比特币病毒勒索的情况下。，不是很个别的案例，而是无处不在。

所以如果真的遇到比特币勒索病毒，一定不要支付。妥协只会加重你的损失，扩大你的伤害，毫无意义。

二、如何避免比特币勒索病毒的危害？

比特币勒索病毒立即在全球引起轩然大波，各大网络安全机构和知名杀毒软件开始关注这个问题。

有许多关于&quot手动设置防火墙关闭电脑的敏感端口，以抵御比特币勒索病毒&quot，但这种方法更适合&quot非白人&quot对计算机比较了解的人，比如我这种三流程序员，这种方法比较适合我。我可以&#039；甚至不用杀毒软件。

但是对于普通大众来说，可能需要换一种更简单的方式来处理。

It&#039；比特币勒索软件已经出现好几年了，为了帮助用户&#039；电脑对抗比特币勒索病毒攻击。很多杀毒软件已经有了一定的防御机制。例如，360已经推出了一个&quot反勒索服务&quot。如果你的电脑在安装360的时候被比特币勒索病毒加密了，那么360会赔偿你赎金，并恢复你的数据。

没有&#039；t不懂电脑可以选择安装杀毒软件来为你防御这类病毒，但具体选择查杀软件还是要看个人爱好。