昨天抽风去了电子阅览室，刚插上U盘没多久，老师就突然大声说让大家把U盘拔下来，有学生发现U盘里的文件全部都打不开了，还多了两个要钱的文件。

于是大家都匆忙查看，只要U盘在学校电脑上插过的都中毒了，晚上出现大规模电脑中毒情况。

很多人的资料、毕业论文都在电脑中，真的觉得黑客这种行为太恶心了，为了钱，不管不顾学生的前途，老师毕生的科研成果……

希望尽早抓到犯罪分子，给予法律的严惩！

什么是比特币病毒？

据百度百科，比特币敲诈病毒（CTB-Locker）最早在2015年初传入中国，随后出现爆发式传播。该病毒通过远程加密用户电脑文件，从而向用户勒索赎金，用户只能在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，约合人民币6000余元。该病毒通过伪装成邮件附件，一旦受害者点击运行，就会弹出类似“订单详情”的英文文档。这时病毒已经在系统后台悄悄运行，并将在10分钟后开始发作。

病毒发行者是利用了去年被盗的美国国家安全局（NSA）自主设计的 Windows 系统黑客工具 Eternal Blue，把今年 2
月的一款勒索病毒进行升级后的产物，被称作 WannaCry。

这个病毒会扫描开放 445 文件共享端口的 Windows 设备，只要用户的设备处于开机上网状态，黑客就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

一些安全研究人员指出，这次大规模的网络袭击似乎是通过一个蠕虫病毒应用部署的，WannaCry 可以在计算机之间传播。更为可怕的是，与大部分恶意程序不同，这个程序可以自行在网络中进行复制传播，而当前的大多数病毒还需要依靠中招的用户来传播，方法则是通过欺骗他们点击附有攻击代码的附件。

这次袭击已经使得 99 个国家和多达 75,000 台电脑受到影响，但由于这种病毒使用匿名网络和比特币匿名交易获取赎金，想要追踪和定位病毒的始作俑者相当困难。

“比特币敲诈者”病毒再次变种 可盗取个人隐私

今年一月份首次现身中国的“比特币敲诈者”病毒如今呈指数级爆发，腾讯反病毒实验室日前发现，该病毒疯狂变种，仅5月7日当天新变种数就已达13万，不仅敲诈勒索用户，甚至还能盗取个人隐私。腾讯反病毒实验室分析，从攻击源来看，这是由黑客控制的僵尸网络以网络邮件为传播载体发起的一场风暴。

“比特币敲诈者” 呈指数级爆发

比特币是一种新兴的网络虚拟货币，因可兑换成大多数国家的货币而在全世界广受追捧。与此同时，一种名为“CTB-Locker”的“比特币敲诈者”病毒也肆虐全球，其通过远程加密用户电脑内的文档、图片等文件，向用户勒索赎金，否则这些加密的文档将在指定时间永久销毁。

僵尸网络助“比特币敲诈者”愈发猖狂

根据腾讯反病毒实验室监测，“比特币敲诈者”的攻击源大部分来自美国，其次是法国、土耳其等。从IP来看，这些攻击源来自一个黑客控制的僵尸网络，黑客利用这个僵尸网络发起邮件风暴。邮件内容大多是接收发票之类，诱导用户去点击下载附件。

“比特币敲诈者”攻击源分布

所谓僵尸网络（Botnet）是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指令，组成一个僵尸网络。

据了解，之所以用僵尸网络这个名字，是为了更形象地让人们认识到这类危害的特点：众多的计算机在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被人利用的一种工具。

僵尸网络助“比特币敲诈者”愈发猖狂

国家互联网应急中心监测的最新数据显示，仅2014年上半年，中国境内就有625万余台主机被黑客用作木马或僵尸网络受控端，1.5万个网站链接被用于传播恶意代码，2.5万余个网站被植入后门程序，捕获移动互联网恶意程序3.6万余个，新出现信息系统高危漏洞1243个。

腾讯反病毒实验室安全专家表示，僵尸网络构成了一个攻击平台，利用这个平台可以有效地发起各种各样的攻击行为，可以导致整个基础信息网络或者重要应用系统

瘫痪，也可以导致大量机密或个人隐私泄漏，还可以用来从事网络欺诈等其他违法犯罪活动。无论是对整个网络还是对用户自身，都造成了比较严重的危害。“比特币敲诈者”便是利用僵尸网络发起邮件风暴，进行各种各样的攻击。

“比特币敲诈者”疯狂变种 可窃取隐私

据了解，“比特币敲诈者”病毒敲诈过程具有高隐蔽性、高技术犯罪、敲诈金额高、攻击高端人士、中招危害高的“五高”特点。用户一旦中招，病毒将浏览所有文档（后缀为.txt、.doc、.zip等文件）和图片（后缀为.jpg、.png等文件），并将这些文件进行加密让用户无法打开，用户必须支付一定数量的“比特币”当做赎金才可以还原文件内容。

用户必须支付赎金才可解锁文件

腾讯反病毒实验室的监测数据显示，从今年4月开始，“比特币敲诈者”疫情最为严重，为了持久有效的攻击，躲避静态特征码的查杀，病毒也在不断地演变，图标多选用文档图标（如doc,pdf等），而自身的壳不断地变形变异。其中，5月7日新变种达到最高值，单天就高达13万个！

“比特币敲诈者”变异趋势

腾讯反病毒实验室安全专家表示，近期发现的“比特币敲诈者”病毒不仅敲诈用户，而且还新增了盗号的特性，会默默搜集用户电脑里的密码配置文件，如：电子邮箱、聊天工具、网银帐号、比特币钱包等等的密码，威胁用户财产安全。目前，腾讯安全团队已第一时间对该病毒进行了深入分析，并可完美查杀此类病毒以及所有变种。

赎回文件需数千元 安全专家支招防范技巧

据路透社报道，“比特币敲诈者”病毒出自俄罗斯的一名黑客，名字叫艾维盖尼耶·米哈伊洛维奇·波格契夫(Evgeniy Mikhailovich Bogachev)，曾凭借这类勒索木马病毒令12个国家超过一百万计算机感染，经济损失超过1亿美元。美国联邦调查局（FBI）官网显示，波格契夫在FBI通缉十大黑客名单中排名第二，是某网络犯罪团体的头目。FBI悬赏300万美元通缉波格契夫，这也是美国在打击网络犯罪案件中所提供的最高悬赏金。

专家强调，正因为危害较大，FBI才会悬赏如此高的奖金缉拿病毒作者。用户一旦中招，意味着电子版的合同，多年老照片，刚刚写好的企划案，刚刚做成的设计图，统统在病毒的加密下无法打开。病毒制造者主要利用用户急切恢复文件的心理实

施敲诈，成功率极高。据悉，比特币近期虽然行情低迷，但单个成交价也在1391元人民币左右（4月20日更新数据），所以，虽然是几个比特币的勒索，对于用户来说也不是小数目。

专家提醒，不要轻易下载来路不明的文件，尤其是后缀为.exe，.scr的可执行性文件，不要仅凭图标判断文件的安全性。另外，平时养成备份习惯，将一些重要文件备份到移动硬盘、网盘，一旦被木马感染，也可及时补救。


什么是勒索病毒？

1、WannaCry病毒与其他同类勒索病毒不同，它是一种可自动感染其他电脑进行传播的蠕虫病毒，因链式反应而迅猛爆发。

2、这种勒索病毒主要感染Windows系统，它会利用加密技术锁死文件，禁止用户访问，并以此勒索用户。

3、袭击者声称，索要价值300美元上述的比特币后方能解锁文件。实际上，即使支付赎金，也未必能解锁文件。

为什么会被感染？

该勒索蠕虫一旦攻击进入能连接公网的用户机器，则会扫描内网和公网的ip，若被

扫描到的ip打开了445端口，则会使用“EnternalBlue”（蓝之永恒）漏洞安装后门。一旦执行后门，则会释放一个名为Wana Crypt0r敲诈者病毒，从而加密用户机器上所有的文档文件，进行勒索。

为什么使用比特币？

比特币是一种点对点网络支付系统和虚拟计价工具，通俗的说法是数字货币。比特币在网络犯罪分子之中很受欢迎，因为它是分散的、不受管制的，而且几乎难以追踪。

传播感染背景

本轮敲诈者蠕虫病毒传播主要包括Onion、WNCRY两大家族变种，首先在英国、俄罗斯等多个国家爆发，有多家企业、医疗机构的系统中招，损失非常惨重。

安全机构全球监测已经发现目前多达74个国家遭遇本次敲诈者蠕虫攻击。

从5月12日开始，国内的感染传播量也开始急剧增加，在多个高校和企业内部集中爆发并且愈演愈烈。

WannaCry勒索病毒预防方法：

1、为计算机安装最新的安全补丁，微软已发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞，请尽快安装此安全补丁；对于windowsXP、2003等微软已不再提供安全更新的机器，可使用360“NSA武器库免疫工具”检测系统是否存在漏洞，并关闭受到漏洞影响的端口，可以避免遭到勒索软件等病毒的侵害。

2、关闭445、135、137、138、139端口，关闭网络共享。

3、强化网络安全意识：不明链接不要点击，不明文件不要下载，不明邮件不要打开……

4、尽快（今后定期）备份自己电脑中的重要文件资料到移动硬盘、U盘，备份完后脱机保存该磁盘。

5、建议仍在使用windowsxp，windows2003操作系统的用户尽快升级到windows7/windows10，或windows2008/2012/2016操作系统。

一旦电脑中了这种比特币勒索病毒，电脑上的所有文件数据就会被强行加密，如果

不向病毒制作者以比特币的形式交付“赎金”，那么这些文件就别想解密找回来了，而即便这次交了赎金解了密了，下次可能还会被“光顾”——也就是说，这种病毒对于“重视数据”的用户、尤其是企业用户来说，所能造成的危害之大是难以估量的。

一、为什么会叫比特币勒索病毒？

所谓的比特币勒索病毒，其实是一种“非对称文件加密”病毒。

感染了这种病毒的电脑其硬盘里的文件，会被以特殊方式进行加密，除非从病毒制作者那里得到对应的密钥，否则永远不可能解密，就算采用重装系统、数据恢复软件等手段也无济于事，也就是说，无法解密就意味着文件被病毒摧毁了。

而唯一的解密方式就是，用比特币向病毒制造者交付“赎金”，但是即便你真的交了这笔钱，对方也不一定就真的会帮你解密，因为比特币的交易是无法追查的——也就是说，如果真的向其妥协交了钱，那么你很可能面临既丢了钱、又被毁掉了数据、还偏偏拿勒索者一点办法都没有的窘境。

这种“撕票”的情况在比特币病毒勒索案件中，可不是什么极个别的个例，而是比比皆是。

所以如果真的遭遇了比特币勒索病毒，一定不要交钱，妥协只会加重你的损失、扩大你所受的伤害，除此之外毫无意义。

二、如何规避比特币勒索病毒的危害？

比特币勒索病毒始一现世，立刻就在全球范围引起了轩然大波，各大网络安全机构、知名杀毒软件都开始重视这个问题。

网络上有不少关于“手动设置防火墙来关闭电脑的敏感端口，从而抵御比特币勒索病毒”的教程帖子，但是这类方法更适用于比较懂电脑的“非小白人士”，就比如我这样的三流程序员，这种方法就比较适合我，我连杀毒软件都用不上。

但是对于普通大众而言，可能就需要换一个更简单的方式去应对了。

如今距离比特币勒索病毒现世已是几年过去，为了帮助用户的电脑对抗比特币勒索病毒攻击，很多杀毒软件都已经有了一定的防御机制，就比如360就推出了一个“反勒索服务”，如果你的电脑在安装了360的情况下你的数据还被比特币勒索病毒给加密了，那么360会为你代偿赎金并为你恢复数据。

不懂电脑的用户可以选择安装杀毒软件来为你防御这类病毒，但是具体选哪种杀软，就看个人的爱好了。