大家好，关于比特币涨价很多朋友都还不太明白，今天小编就来为大家分享关于病毒是什么的知识，希望对各位有所帮助！

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

如何看待5月12号爆发在各高校电脑勒索比特币的病毒？

要想说清楚5月12日在部分高校爆发的勒索比特币的病毒，还要从2017年4月14日NSA旗下黑客团队方程式组织（EquationGroup）部分黑客武器被影子经纪（ShadowBrokers）组织公开外泄说起。那次外泄的黑客武器中，利用微软windows操作系统的SMB网络协议漏洞，可以远程攻破全球约70%的Windows计算机。好在微软公司在4月份这些漏洞利用工具外泄之前，提前得到消息，并在2017年3月份提前发布了MS17-010等补丁，避免了全球安装微软windows操作系统计算机的一次全军覆灭。

不过，全球仍然有大量计算机没有安装MS17-010等补丁，并且未安装有效的安全防护软件，导致利用这些SMB漏洞的病毒肆意扩散，感染了国内高校众多计算机无辜受害。

SMB是一个网络文件共享协议，它允许应用程序和终端用户从远端的文件服务器访问文件资源，用于在计算机之间共享文件、打印机、串口和邮槽等。我们平时使用的网络共享功能，就是通过SMB协议在445网络端口实现的。

5月12日在各高校爆发的勒索比特币蠕虫病毒的传播，利用的就是影子经纪（ShadowBrokers）组织公开的“永恒之蓝”（EternalBlue）黑客工具所利用的SMBv1和SMBv2漏洞。在2017年4月14日，“永恒之蓝”利用的SMB漏洞曝光后，勒索比特币蠕虫病毒及时添加了利用SMB漏洞进行网络自动传播感染的这种方式，从而导致近期勒索比特币蠕虫病毒的大爆发。

勒索比特币的蠕虫病毒自身具备自动扩散功能，它通过自动生成IP地址，对联入网络的计算机的445端口进行自动扫描，只要暴露在网络上的计算机，且445端口未防护并且未安装补丁的，就会被勒索蠕虫病毒自动扫描发现，之后蠕虫病毒即可利用445端口的SMB协议漏洞利用工具，马上入侵感染这台计算机。因此，造成短时间内大量高校的大量计算机被感染勒索蠕虫病毒。

对于这款病毒的防范措施，个人计算机最简单的防范方法有两种。一是打开微软的防火墙，在“控制面板”的“windows防火墙”中，点击“打开或关闭windows防火墙”，点击“启用windows防火墙”中的“组止所有传入连接”。这样，可通过windows防火墙关闭你自己计算机的445端口和其他所有网络端口，使勒索蠕虫病毒无法扫描到你的445端口，当然也就无法扩散到你的计算机了。二是抓紧升级微软补丁，或者从微软网站及时下载安装MS17-010补丁，或者及时运行微软的补丁自动更新，或者采用第三方杀毒软件或安全软件，及时更新MS17-010等补丁。

对于校园网络管理人员，应该及时配置校园网网络边界设备以及校园网内部的网络设备，通过添加访问控制列表规则或者网络安全防护规则，阻止对任意目标IP地址且目标端口为445端口的网络数据包的传播，从而阻止病毒从外网传入内网，同时对病毒在校园网内网的传播起到部分拦截作用。

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，“S

hadowBrokers”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。

比特币为什么会暴涨暴跌？

我肯定的告诉你，一定会暴涨，但也一定会暴跌。只有在暴涨暴跌之间，这才是比特币真正的价值所在，也是比特币的魅力所在。之所以出现这种情况，其原因如下。对不起。部分比特币是用于黑市中的。投机属性强。

另一部分人是投资人。

投资人为投资要获得极大利润，必须是在不断的暴涨暴跌的。这期间。如果总是跌。不用说了，这个币就没有价值了。这个很好理解，那为什么不可以一直涨呢。其实一直涨也会出现问题。

人家是越早加入的人，越赚钱，这样就需要不断的有人进来。

才能维持前面的人高收益，这其实就和旁氏骗局一样了。那世界上的人口是有限的，钱也是有限的。因此，必须在暴涨暴跌之中不断的收购韭菜。

无论是一起跌下去或者一起涨下去，这个游戏都玩不了多久，只有暴涨暴跌这个游戏。

如果你还想了解更多这方面的信息，记得收藏关注本站。