大家好，今天小编来为大家解答比特币病毒交易网站这个问题，比特币病毒交易网站官网很多人还不知道，现在让我们一起来看看吧！

本文目录

紧急求助！如何预防比特币病毒？

以支付比特币换取解密为特征的计算机病毒来势汹汹，世界多国计算机均已中毒，其中英国和中国尤为严重。昨天今天被该病毒的消息涮屏了，该病毒危害性不少，特别是面临毕业季，很多学生的论文存在丢失的巨大风险。

首先说如何预防，我的建议是，作为个人计算机用户，首先要关闭445端口，下载微软补丁完成修复，推荐下载360提供的NSA武器库免疫工具，完成该病毒的防护，下载地址连接http://dl.360safe.com/nsa/nsatool.exe

此次病毒于5月12日晚在我国校园网开始蔓延。据360分析分析，该病毒是由NSA泄漏的“永恒之蓝”黑客武器传播的。“永恒之蓝”可远程攻击Windows的445端口，该端口方便用户在局域网中轻松访问各种共享文件夹或共享打印机。

用户计算机如果之前安装的2017年3月的微软补丁，则不会中招。之前由于国内曾多次出现利用445端口传播的蠕虫病毒，中国电信等运营商对个人用户封掉了445端口，但教育网并无此限制，存在大量暴露着445端口的机器，因此成为不法分子使用NSA黑客武器攻击的重灾区。

根据360公司周鸿祎的说法，目前“永恒之蓝”传播的勒索病毒以ONION和WNCRY两个家族为主，受害机器的磁盘文件会被篡改为相应的后缀，图片、文档、视频、压缩包等各类资料都无法正常打开，只有支付赎金才能解密恢复。这两类勒索病毒，勒索金额分别是5个比特币和300美元，折合人民币分别为5万多元和2000多元。

根据360针对校园网勒索病毒事件的监测数据显示，国内首先出现的是ONION病毒，平均每小时攻击约200次，夜间高峰期达到每小时1000多次；WNCRY勒索病毒则是5月12日下午新出现的全球性攻击，并在中国的校园网迅速扩散，夜间高峰

期每小时攻击约4000次。

其实，针对NSA黑客武器利用的Windows系统漏洞，微软早在2017年3月已发布补丁修复。360公司也已推出NSA武器库免疫工具，能够一键检测修复NSA黑客武器攻击的漏洞，对WindowsXP、2003等已经停止更新的系统，免疫工具可以关闭漏洞利用的端口，防止电脑被NSA黑客武器植入勒索病毒等恶意程序。

我就想知道让各大高校瘫痪的比特币病毒到底是什么鬼？

这个病毒叫做“WanaCrypt0r2.0”（WanaCry直译过来，应该叫“想哭”），主要针对微软的Windows操作系统。

如果你不小心通过点开可疑邮件、未经扫描的附件等方式中招，那么等待你的将是：电脑所有文件会被加密锁定，制作病毒的黑客还会通过修改桌面壁纸和弹窗的方式，温馨提示被感染的机主（病毒提示内容甚至可因地区不同，而翻译成当地不同语言）。需要在指定时间内，支付价值300美元的比特币才能纾困，超时翻倍，拒绝的话，电脑中的文件可能会被彻底清空。

WannaCry病毒攻击的漏洞，是通过微软的Windows操作系统中的网络端口（如445、135、137、138、139端口等）以及网络共享等途径实现感染和攻击。这也解释了为什么中国成为此次病毒攻击的主要受害地区——在中国，教育网因为没有关闭445端口而成为感染重灾区。

对普通用户来说，如果你及时升级，事情没有那么可怕，升级地址：

https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

根据提示升级操作系统补丁就行了。

该病毒与美国国家安全局的黑客工具有关，或者最起码本次袭击借鉴了被泄露的NSA（美国国家安全局，好莱坞大片里经常见到）工具。去年起，一个自称为影子黑客（ShadowBrokers）的组织在网上公布了NSA针对Windows文件与打印机共享系统漏洞的黑客编程代码，但NSA从没有正面承认过。

近两天很火的比特币病毒到底是什么？

据媒体报道，这个病毒的“创造者”已经真相大白：居然是美国国家安全局（NSA），而且其手中还有大量的“网络战”武器。这种疯狂的举动，如果真是美国干的，说明美国已经消耗得查不多了！而且比特币也是日本鬼子弄的，二个无赖政府

正好狼狈为奸，坑害全世界！不过话说回来，这就是实力，这就是丛林法则！嘴上不承认没用，全方位增强实力吧！这是能站稳脚跟的唯一出路。中国芯，中国网，任重道远！

#比特币病毒#攻击我国大批高校也出现感染情况，周一上班后该如何应对？

近日，相信不少人让“永恒之蓝”比特币勒索病毒给刷屏了吧！也有不少用户担心自己的电脑是不是会中招，怕一不小心电脑上的资料都给废了。为此，不少厂商都给出了预防方案，因昨晚（5月14日），@ZEALER中国也给出了预防方案，教你如何预防比特币勒索病毒。

具体操作如下：1、开机前先拔掉网线、无线上网卡等联网设备；2、启用并打开“Windows防火墙”，进入“高级设置”，在入站规则里禁用“文件和打印机共享”相关规则。关闭UDP135、445、137、138、139端口，关闭网络文件共享。3、联网及时更新微软官方发布的MS17-010补丁：网页链接；4、尽快更新操作系统；5、做好重要数据备份，谨防新型变种病毒侵袭。

据介绍，此次比特币勒索病毒“永恒之蓝（WannaCry）”网络攻击事件已造成150多个国家、20多万台设备“中招”。即使是在周末，大部分公司不上班的情况下，中国也有约3万家机构受到了感染，如果还没进行系统更新升级的小伙伴，赶紧进行更新升级，同时也要做好数据备份！

关于比特币病毒交易网站的内容到此结束，希望对大家有所帮助。