大家好，今天来为大家分享比特币病毒损失的一些知识点，和比特币病毒损失多少的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

#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！

全球爆发的比特币勒索病毒到底有多可怕？

现在这个事件感觉已经过的很远了，但是造成的恐慌是不言而喻的，在5月12日晚间，WannaCry（又称WannaDecryptor）蠕虫病毒在全球超过74个国家爆发，已有至少4.5万台机器受到感染，我国部分高校网络系统沦为重灾区，中石油加油站网络支付系统也受到影响。

而且当时据说只要是内网就有感染的可能，你想想如果银行、交通、通信系统被感染，没法预定火车票、机票，手机没法使用甚至你的银行存款被冻结是多么恐怖的事情，当然这种情况微乎其微，因为上述的系统基本都有备份服务器的。

如果把比特币病毒和熊猫烧香、冲击波、红色代码之类的老病毒放一起会怎么样？

这次勒索病毒其实不能算是一个真正意义上的病毒，更像是个小孩子搞的“恶作剧”，因为它本身并不破坏电脑系统，只是将某些文件，主要是一些文档，照片和视频等进行加密，而且还留有解密恢复正常的途径，就好像小孩子为了零花钱把你的重要的东西给藏起来了，然后你给钱他就还给你。但传统意义上的病毒则主要以破坏为目的，其过程是不可逆的，所以后果更严重！

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。

文章分享结束，比特币病毒损失和比特币病毒损失多少的答案你都知道了吗？欢迎再次光临本站哦！