这篇文章给大家聊聊关于比特币勒索病毒的危害，以及比特币勒索病毒的危害有哪些对应的知识点，希望对各位有所帮助，不要忘了收藏本站哦。

本文目录

勒索病毒席卷全球，它为何如此凶猛？

勒索病毒又称"比特币"病毒是2017年5月12日开始在网上曝光的一种新型电脑病毒，主要以邮件，程序木马，网页挂马的形式进行传播，一旦电脑感染此病毒，电脑硬盘将被黑客加密，对硬盘数据会造成很大的危害。来电脑百事网关注勒索病毒是什么、中病毒如何解决、如何防止电脑中勒索比特币病毒以及勒索病毒最新消息。

比特币勒索病毒会导致手机损坏吗？怎么应对呢？

这个病毒确实有点强，被加密的文件大部分可以恢复，屏蔽455根本不是有效的方法，好多企业和家庭需要依赖455端口，455端口主要是用来共享设备的，比如打印机等设备，媒体在这里乱搅和真正懂得没几个，最有效的方法就是更新补丁，屏蔽455只会影响自己（民用运营商455被限死，病毒不可能从外网入侵）大家别屏蔽455端口，别做无用功，360不是有了杀毒补丁，可以试试。

据说比特币勒索病毒已经升级变异，如何避免手机感染，而造成手机支付瘫痪？

手机不会被感染啦，手机感染也不会造成手机支付瘫痪，但是和手机支付相关的服务器被感染了才可能造成瘫痪，但是也请放心，还没那么脆弱呢，手机支付安全做得很强，不会那么轻易被这种病毒感染。

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，“ShadowBrokers”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。

好了，关于比特币勒索病毒的危害和比特币勒索病毒的危害有哪些的问题到这里结束啦，希望可以解决您的问题哈！