大家好，关于比特币勒索病毒叫很多朋友都还不太明白，今天小编就来为大家分享关于比特币 勒索病毒的知识，希望对各位有所帮助！

本文目录

为什么国际刑警都对此次比特币勒索病毒的罪犯束手无策？

2016年2月的一天，好莱坞长老会医院的护士们发现电脑全都用不了了。所有的文件都加了个莫名其妙的后缀，根本打不开。所有电脑程序也都加了这个后缀，一个也启动不了。挂号只能用纸笔，病历都成了乱码，连手术都不能正常进行。当大家都束手无策的时候，院长阿兰·史蒂芬涅克（AllenStefanek）接到了一个陌生的通知：给我1万7千美元，不然你们的医院就得关张。

史蒂芬涅克院长犹豫了一个多星期，还是选择了交钱。好莱坞长老会医院所经历的勒索并不稀有。近年来，越来越多的用户报告自己的电脑曾被黑客锁住，只能交赎金了事。这种黑客攻击被人们叫做“网络勒索”，黑客们使用的软件也有一个名字，叫做Ransomware。

“面具脸”和“拼图”病毒

Ransomware的定义很枯燥，我们不如直接举一个例子：

小明在情人节收到了一名陌生人的邮件，邮件里一片空白只有一个叫做“拼图”的附件。小明兴高采烈地打开了这个“拼图”，然而这个叫做“拼图”的东西并不是节日礼物，而是一个Ransomware。

（“拼图”Ransomware的典型窗口)

上面就是大名鼎鼎的Ransomware----“拼图”（Jigsaw）。打开以后是一个黑色背景的窗口，窗口正中心是一个电影《电锯惊魂》里的面具脸。绿色的勒索信息会一个字一个字地打出来，它用《电锯惊魂》的口吻给小明写道：

“我想跟你玩一个游戏，我来解释一下游戏规则：你的文件正在被一个一个地删掉，照片、视频、文档……不过不要担心，只要你合作，它们就不会被删完。你的文

件都已经被加密了，你一个也看不了。每个小时我会删掉一些，删掉的速度越来越快。如果你关电脑，再次打开的时候我就删掉1000个文件，如果你关掉我，你的文件就会被永远加密。只有我能把文件还给你。现在，我们来玩这个游戏吧。”

小明赶紧打开自己硬盘里的电影文件夹，发现所有的片子都被加上了一个“.fun”的后缀，根本打不开。不仅是电影，自己写的日记，照的照片，玩的游戏，一个也打不开。

窗口的左下角是个倒计时，开始是一小时，每次归零就会删掉一些文件。每删一次，下一次删的数量就会增多。每小时被删的文件指数增长，用不了几天电脑就啥也不剩了。

当然黑客不是为了玩这个“删文件”的游戏，而是要钱。小明一开始还挺强硬，可文件都丢了怎么办？我这电脑花了几千块钱买的，这么着不就没法用了吗？红色的倒计时让小明的心脏一蹦一蹦的，而小明渐渐地陷入了绝望。过了几分钟，小明终于服软了。他按照黑客的指示，买了23美元的比特币，汇给这个陌生人。

小明事后报了警，可比特币无法追踪，警察根本抓不着凶手。小明回家打开电脑，发现面具脸的窗口终于没有了，可是自己的文件也全删没了。

(Ransomware“拼图”的各种变体)

这个名为“拼图”的勒索软件主要肆虐时间是2016年，它有很多不同的变体，比如被劫持文件的后缀不一定是”.fun”，还有.gefickt,.uk-dealer@sigaint.org,.paytounlock,.hush,.locked,.payrmts,.afd,.paybtcs,.fun,.kkk,.gws,和.btc.背景也不一定是《电锯惊魂》的面具脸，还有弄成一群头盔制服党的，还有搞出电影《V字仇杀队》的，还有扮成游戏“杀手47”的。“拼图”勒索软件要多少钱的都有，比较多的是要150块钱。“拼图”还走上了国际化道路，除了英语以外，还非常贴心地加上了西班牙语、法语、俄语等多国语言。好消息是这个臭名昭著的“拼图”终于被破解了，网上不仅有破解教程，还有一个破解软件“Jigsawdecrypter”。

像“拼图”这样的Ransomware还有很多很多，长相也各不相同，但行为都是一样的。它通过木马的形式在邮件、U盘、下载网站里传播，它自动锁住你的电脑，把所有文件加密，并威胁要删掉它们。受害者必须通过比特币支付给发布者，然后发布者根据心情好坏选择是否把文件交还。像小明这样的受害者，近来一年比一年多。

为什么Ransomware突然肆虐了起来

Ransomware已经存在了至少十年了，最早只泛滥在“黑客之乡”俄罗斯。可最近三年Ransomware突然异军突起，全世界流行起来。IBM曾经在美国做过一次调研，仅在2016年，已知的网络勒索涉案金额总额近10亿美元，40%的垃圾邮件里都有Ransomware。一半的受害者拒绝交钱，“鱼死网破”，另一半的受害者束手无策，乖乖交钱。

受害者往往对于一百美元以下的赎金能够接受，这也是为什么Ransomware每次涉案金额较小，但传播极其广泛。企业用户往往比个人用户更倒霉，因为他们要交的赎金往往更多，而且他们会迫于公司压力选择交钱。70%的企业受害者交了赎金，这些交了赎金的人里面，一半的人交了至少一万美元，20%的人交了至少四万美元。

2016年，欧洲刑警组织（Europol）把Ransomware列为“危害性最高的网络攻击”，排在它后面的才是数据盗窃（偷文件）和银行木马（偷银行卡）。欧洲刑警组织对网络犯罪做了一个执法优先级排名，排名前五的病毒里，三个都是Ransomware。

(欧洲刑警组织对网络病毒的执法优先级排名)

互联网初期的病毒，大多数是“损人不利己”的。黑客们搞出个病毒，不为赚钱，就为炫耀一下自己的才华。2006年的病毒“熊猫烧香”，中病毒以后所有.exe结尾的文件无法运行，图标变成一个熊猫举着三炷香。2003年的“冲击波”（Worm.Blaster）病毒，中病毒以后，电脑会一分钟自动重启一次。“冲击波”的源代码里，还有一行嘲讽比尔·盖茨的话：

“比尔盖茨啊，你怎么能让这种事情发生？少挣点儿钱吧，多修修漏洞。”

(被“熊猫烧香”感染的文件，图标全变成了熊猫)

早期的黑客往往都是软件爱好者，业余时间搞出个病毒宣传一下自己，并不拿它赚钱。可随着互联网的普及，病毒不再是“恶作剧”，越来越多的职业犯罪者用它来大发横财。

Ransomware是个很特别的攻击手段。过去的黑客往往喜欢“黑进”你的电脑，手里拿着一个“万能钥匙”（解密算法），撬开你的锁（加密文件）。而网络勒索正相反，黑客并不在乎你电脑里有什么，他们手里拿的是个“万能锁”（Ransomware），逼你交钱以后才把这个“万能锁”打开。上锁比开锁容易，加密也比解密要简单。所以网络敲诈犯，不需要学太多计算机知识。只要拿到了Ransomware，小学生都可以搞勒索。

管病毒管受害者直接要钱，在过去是行不通的。警方可以通过查找银行的交易记录，迅速追捕到罪犯。可在比特币发明出来以后，形势一下子就变了。比特币随处可买，线上流通。它不需要身份证验证，也不需要去银行管理。比特币是个“去中心化”的金融体系，警察对比特币交易无法追踪。有了这么一个“地下交易”网，黑客们拿完钱后轻松逍遥法外。已报告的网络勒索案，绝大多数都是通过比特币支付的赎金。

(比特币无法追踪，所以成了黑客的“通用货币”)

互联网创业就像赛跑，谁发布的早，谁就容易占掉市场份额。这就导致创业者们养成了一种陋习：先发布一个差不多能用的软件，以后再慢慢修漏洞。正是这些漏洞，让黑客们一下子有隙可乘。

一个典型的例子就是MongoDB。MongoDB是一个非常好用的“非关系型数据库”（至于什么是“非关系型数据库”，我们以后有机会再讲）。MongoDB刚刚发布的时候，它的默认设置非常不合理：任何人都可以访问这个数据库（没有Access Control），而且不做自动备份。很多人不会改MongoDB的默认设置，于是黑客们纷纷前去盗取这些没有任何保护的数据库，然后敲诈管理员。

在MongoDB的官方博客透露，2万5千个数据库中，2000个受到了黑客的勒索。勒索者偷走了所有数据，然后在数据库里留下一句话：“通过比特币给我XXX美元，不然我就删掉你的数据。”攻击MongoDB的黑客实在太多了，以至于一个黑客刚刚在数据库里留下勒索的“纸条”，另一个黑客立刻把“纸条”的收款人抹掉，改成自己的比特币账户。如今MongoDB已经修复了这个漏洞，然而大量用户并没有升级，还处在被勒索的风险之下。

综上所述，职业罪犯的加入、极低的技术门槛、无法追踪的交易模式、漏洞百出的软件，这些就是Ransomware肆虐的原因。

那么，我们拿这些敲诈犯没有办法了吗？

对抗网络勒索的手段

2016年6月，美国加利福尼亚州参议院通过了一项法律：网络勒索，视同勒索罪处理。这个编号为SB-1137的法律由加州参议员鲍勃·赫兹伯格（BobHertzberg）提出，在州参议院全票通过，最后由加州州长杰瑞·布朗（JerryBrown）签署。它不仅给出了网络勒索的法律定义，还规定：就算这个黑客没有收到赎金，罪行也按照收到赎金判决。作案者最高可以被判4年监禁，另外还有1万美元的罚款。这个法案在讨论的时候，好莱坞长老会医院作为受害者还曾发表过证词。医院院长终于可以

放下心来，不再担心医院电脑被黑客给“锁住”了。

可事情就这么结束了吗？

法案通过仅仅一天后，法案提出者赫兹伯格的电脑就被黑客给加密了。赫兹伯格无奈地发了一条推文，还发了个截图：“这就是我在州议会的办公室电脑截图，它被Ransomware攻击了。”

(网络勒索法案的提出者赫兹伯格反而被勒索)

直到今日，这些网络勒索的罪犯们还在频频作案，因为虽然立法有了，执法手段上还有很长一段路要走。今天被成功逮捕的黑客少之又少，大多数勒索者还在逍遥法外。如果事后抓不到，我们就只能事前预防。

防范网络敲诈的方法有很多，最重要的就是养成良好的上网习惯：不要点开不认识的邮件附件，不要在不安全的网站下载软件，勤杀毒，勤升级，多用云存储，定期做硬盘备份。

如果上面的都没有做到，自己还是被攻击了，不要慌，有不少网站可以把你的文件找回来。比如http://nomoreransom.org，它不仅可以用多种算法尝试解密被“锁住”的文件，还会指导你如何报警。不少Ransomware已经被破解了（比如“拼图”），去一些值得信任的论坛，也能下载到正确的解密工具。

最后，在付赎金之前一定要再三考虑，因为黑客可能会在要了一次钱以后得寸进尺，不断地骚扰你。而且黑客不一定会在最后把文件还给你，你的钱最后也拿不回来。况且，如果交赎金的人少了，黑客们就赚不到钱，类似的攻击就会变少。你如果交了赎金，这可能是一种对这种犯罪行为的鼓励。

万一自己电脑中了勒索比特币的病毒怎么办？第一时间应采取什么措施？

1、不要给钱。即使交了之后未必能恢复数据。

2、迅速多次备份数据。已中毒的，重装系统前把硬盘低格

3、安装反勒索防护工具，不要访问可以网站、不打开可疑邮件和文件

4、关闭电脑包括TCP和UDP协议135和445端口

5、win7系统格外注意，不要使用校园网落，cmcc也不行

6、还不懂的，把网掐了。

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。

比特币勒索病毒的黑客被抓了吗

目前还没有呢，勒索病毒勒索的是比特币，比特币是匿名交易的，黑客不勒索现金，就不通过银行，所以不好追踪，黑客也正是看到了这点。

比特币勒索病毒叫的介绍就聊到这里吧，感谢你花时间阅读本站内容，更多关于比特币 勒索病毒、比特币勒索病毒叫的信息别忘了在本站进行查找哦。