面对音讯化时期如果我们不&#039；不注意，我们会出轨，所以我们可以通过及时补充知识来与时俱进。明天，我们将为自己带来一篇关于比特币勒索病毒攻击原理和它是什么的文章。相信会给你带来很大的帮助！

a&quot；蠕虫状的&quot勒索软件，大小3.3MB，被NSA(美国国家安全局)不法分子利用。激进的风险缺陷&quot永恒的蓝色&quot(永恒之蓝)停止交流[1]。

恶意软件扫描计算机上的TCP445端口(服务器消息块/SMB)。以类似蠕虫病毒的方式进行通信，攻击主机并加密存储在主机上的文件，然后乞求用比特币支付赎金。勒索的金额是300到600美元。

2017年5月14日WannaCry勒索病毒有变种：WannaCry2.0，秒杀开关撤销或者更快。截至2017年5月15日，WannaCry在网络攻击下形成了至少150个国家。，一度波及金融、电力、医疗等行业，形成严酷的危机管理效应。国内部分Windows操作系统用户被感染，校园网用户首当其冲，受益严重，少量实验室数据和毕业想象被锁定加密。目前为

平安行业一直未能有效摒弃该勒索软件的恶意加密行为。微软总裁兼首席法律官布拉德史密斯(BradSmith)表示，美国国家安全局没有披露更多安全漏洞，这给了有功组织可乘之机，最终带来了这次攻击150个国家的勒索软件。

wanacry勒索病毒是由&quot影子经纪人&quot。

由于wanacry勒索软件利用Windows-445串口漏洞ms17-010来阻止攻击，掩盖了所有版本的Windows，受众特别多。。攻击电脑后，wanacry会对用户进行加密&#039；文件/数据/档案/照片等。并乞求比特币赎金来解锁。

目前Windows用户受到wanacry勒索软件攻击，处置方法如下：(任何情况下绝不支付赎金，有少量证据表明即使支付赎金文件也无法解密。)

Windows用户可以格式化所有硬盘，彻底清除设备上的wanacry勒索病毒。

集团用户可以联系国际、国外安全厂商，如奇虎360、金山毒霸、卡巴斯基、迈克菲等。腾讯安全管家等安全中心寻求协助恢复主数据。

应用&quot勒索病毒免疫工具&quot停止修理。用户下载腾讯电脑管家离线版&#039；s&quot赎金病毒免疫工具&quot通过其他电脑。，并将文件复制到安全无毒

的u盘；然后在屏蔽WiFi、拔掉网线、断开网络的条件下打开指定电脑，尽快备份主要文件；然后使用离线版本的&quot勒索病毒免疫工具&quot通过u盘一键停止修复漏洞；一般可以通过联网来使用电脑。

应用文件恢复停止工具停止恢复。已经感染病毒的用户可以使用电脑管家-文件恢复工具停止文件恢复，一定概率可以恢复你的文件。

注：也可以继续关注相关安全厂商的处置方式。，等待日益优越的完美解锁。

WannaCry利用Windows操作系统端口445的缺陷停止传播，具有自复制、自动传播的特性。

被这个勒索病毒入侵后，照片、图片、文档、音频和视频等各种文件几乎都在用户&#039；的主机系统将被加密，加密文件的后缀将被更正为。WNCRY，桌面上会弹出一个勒索对话框，恳求受益人向攻击者收取价值数百美元的比特币&#039；的比特币钱包。而且赎金数额会随着时间增加。

我明天去了电子阅览室。我插上u盘没多久，老师突然大声说要拔u盘。有同学发现u盘里的文件在本地打不开，又多了两个文件要钱。

于是我匆忙检查了一下自己，学校电脑里插的东西都中毒了，早上还出现了大规模的电脑中毒。许多人&#039；的资料和毕业论文都在电脑里，我真的觉得黑客的这种行为很恶心。为了钱，不管学生&#039；出路。教师的终身科研效应.

希望尽快抓到有功人员，给予法律严惩！

什么是比特币病毒？

根据百度百科，比特币勒索病毒(CTB-洛克人)于2015年底首次传入中国。，其次是生成式沟通。该病毒对用户进行加密&#039；电脑文件进行远程操作，从而向用户勒索赎金，用户支付赎金后才能打开文件。

其最新变种勒索金额为3个比特币，约合6000元人民币。。该病毒伪装成电子邮件附件，一旦受益人点击运行，一个类似&quot订单摘要&quot会弹出来。这时候病毒习惯在系统后台悄悄运行，10分钟结束就会发作。

病毒发布者应用了去年被美国国家安全局(NSA)窃取的Windows零碎黑客工具EternalBlue，并于去年2月停止升级了一款勒索软件，名为WannaCry。

该病毒会扫描打开445文件共享端口的Windows设备。只要用户&#039；s设备是以打开互联网的形态，黑客可以在电脑和服务器中植入勒索软件，远程掌握木马、虚拟货币矿机等恶意指令。

有安全研究人员指出，这种大规模的网络攻击似乎是由一种蠕虫病毒安排的，WannaCry可以在计算机之间传播。更可怕的是，与大多数的邪念不同，这种邪念是可以自行复制并在网络中传播的。以后大部分病毒还是要靠招商的用户来传播，规则是骗他们点击带有攻击代码的附件。

这次攻击影响了99个国家和多达75，000台计算机。然而，由于这种病毒使用匿名网络和比特币匿名买卖赎金，因此追踪和定位病毒的发起者相当困难。

勒索软件的义务原则：

勒索软件是黑客劫持用户&#039；通过屏幕锁定和加密的方式来保护用户的设备或文件。利用这一点来勒索用户的恶意软件&#039；钱。黑客利用系统漏洞或钓鱼方式，将病毒植入受益电脑或服务器，对硬盘甚至整个硬盘上的文件进行加密，然后向受害者索要不同金额的赎金后再解密。假设用户未能在规定时间内支付黑客要求的金额，锁定的文件将无法恢复。

1。一种罕见的针对集团用户的攻击方式

通过用户浏览网页下载勒索病毒，攻击者将病毒伪装成盗版软件、插件和色情播放器。，诱导受害者下载运行病毒，对受害者进行加密&#039；s机器运行后。此外，勒索软件还会通过钓鱼邮件和系统漏洞进行传播。针对集团用户的攻击流程如下图所示：

攻击流程

2。企业用户罕见的攻击手段。

Lesu病毒针对企业用户的罕见攻击方式包括系统漏洞攻击、远程访问弱密码攻击、钓鱼邮件攻击、web漏洞和弱密码攻击、数据库漏洞和弱密码攻击。在...之中钓鱼邮件攻击包括通过漏洞下载运行病毒、通过office机制下载运行病毒、伪装成office和PDF图标的exe序列等。

1)系统漏洞攻击

系统漏洞是指操作系统在逻辑假设上的缺陷或疏忽。不法分子通过网络植入木马和

病毒，攻击或掌握整台电脑，攫取电脑中的主要数据和音频，甚至破坏系统。和集团用户一样，企业用户也会受到系统漏洞的攻击。由于企业局域网内机器数量众多，更新补丁费时费力，有时还需要中间件服务，企业用户不及时更新补丁，对系统构成严重威胁。攻击者可以通过漏洞植入病毒，并快速传播。。席卷全球的Wannacry勒索病毒利用永恒之蓝的漏洞在网络中迅速传播。

攻击者利用系统漏洞的方式主要有两种。一种是通过系统漏洞扫描互联网中的机器，发送漏洞攻击包。，入侵机器，植入后门，然后上传运行勒索软件。

通过系统漏洞扫描网络中的电脑

另一种方式是通过钓鱼邮件、弱密码等方式入侵一台连接互联网的机器。然后利用漏洞局域网进行横向传播。。大多数企业的网络可以&#039；t相对隔离，一台连接外网的机器被入侵，内网有漏洞的机器也会受到影响。

入侵一台机器后，通过漏洞局域网进行横向传播

网上有少数漏洞攻击工具。特别是武器级NSA方程组织工具的激进化，对网络安全产生了巨大影响，被广泛用于传播勒索软件、挖矿病毒、木马等。一些攻击者将这些工具包装成图形化的一键自动攻击工具，进一步降低了攻击门槛。

2)远程访问弱密码攻击

因为很多企业机器需要远程维护，所以很多机器都屏蔽了远程访问功能。假设密码太复杂，会给攻击者可乘之机。很多用户抱有侥幸心理，总觉得网络上的机器那么多。，被攻击的概率很低，但在梦里，在世界各地，无数的攻击者不断地用工具扫描网络中密码较弱的机器。有些机器因为弱密码的存在，被不同的攻击者攻击，植入多种病毒。此病毒未被删除，但已感染新病毒。，导致机器卡死，文件被加密。

弱密码攻击类似于漏洞攻击，只是弱密码攻击采用暴力破解，试图用字典中的账号密码扫描互联网中的设备。

弱密码扫描网络中的计算机

还有一种通过弱密码进行攻击的方法。一台连接外网的机器被入侵，内网的机器通过弱密码被攻击。

入侵一台机器然后用弱密码爆破局域网机器

3)钓鱼邮件攻击

企业用户也会受到钓鱼邮件的攻击。与集团用户相比，由于企业用户使用邮件频繁，业务需求不得不打开很多邮件，一旦打开的附件含有病毒，企业的整个网络都会受到攻击。钓鱼邮件攻击逻辑图：

钓鱼邮件攻击逻辑

文章转载至：2018勒索病毒一边倒分析演讲

比特币勒索病毒的攻击原理介绍以及什么是比特币勒索病毒的攻击原理介绍完毕。不知道你有没有从中找到你需要的音频？