许多朋友不&#039；不了解勒索软件及其攻击方法。接下来，让&#039；让我们一起来看看Dadaqq.Com边肖对勒索软件的具体回答。

勒索病毒就是潜入别人&#039；美国电脑通过网络攻击。通过恶意破坏或窃取用户数据，主要以邮件、木马、网页等形式传播。这种病毒性质恶劣，危害极大。一旦感染，会给用户带来不可估量的损失。这种病毒使用各种加密算法来加密文件。感染者可以&#039；一般不能解密，只有他拿到解密的私钥才有可能破解。比如最近的WannaCry(也叫WannaCryptor)和&quot蠕虫状的&quot勒索软件就是最好的例子。

建议使用个人电脑或公司电脑。应部署安全防护软件，如红线防泄露系统、透明加密软件等，防止数据泄露，同时有目录保护功能。直接保护后，可以禁止任何非法篡改数据的行为，只有解除保护后才能查看。

勒索病毒是黑客劫持用户的恶意软件&#039；文件通过锁屏和加密文件，从而勒索用户&#039；钱。黑客利用系统漏洞或网络钓鱼将病毒植入受害者&#039；s电脑或服务器对硬盘甚至整个硬盘上的文件进行加密。之后在向受害人索要不同金额赎金后解密。

勒索病毒的形式

1。修改电脑开机密码、登录密码等。锁定计算机。

rip-off木马：通常伪装成外挂软件潜入用户&#039；的电脑。，修改用户登录名和密码并实施锁勒索，但一般不会破坏系统文件或用户文件。杀毒软件在正常运行情况下会拦截此类木马，这也是很多插件要求用户关闭或卸载杀毒软件的原因。

2。冒充安全机构恐吓用户。

雷富顿勒索病毒：根据用户&#039；的位置，它假装用户&#039；的电脑受到攻击，被用于非法活动，用户需要支付罚款才能解锁系统。。一位名叫约瑟夫爱德华兹(JosephEdwards)的17岁中学生自杀，原因是他的电脑感染了Reveton勒索病毒。

3。加密用户文件和数据。

WannaCry:计算机文档采用对称加密算法和非对称加密算法加密。一旦用户被招募，数据就无法恢复，除非黑客被支付赎金购买解密密钥。这次WannaCry利用了这个危险的漏洞&quot永恒的蓝色&quot被国安局泄露出去传播。，导致大面积电脑

用户被勒索病毒攻击。此外，CryptoLocker、VirLock、Locky等勒索病毒也是这一类型。

4。篡改磁盘MBR，加密整个电脑磁盘。

Petya勒索者病毒：感染电脑系统的MBR，覆盖整个硬盘，导致Windows崩溃，显示蓝屏。当用户重启电脑时，修改后的MBR会阻止Windows正常加载，并对整个磁盘进行加密。之后会显示一个ASCII骨架图像，提示你支付一定数量的比特币，否则你将失去访问文件和电脑的权限。

1中病毒的原因。垃圾邮件：犯罪分子通过伪造邮箱向目标发送邮件。，这些电子邮件将包含带有病毒的附件或在邮件正文中添加钓鱼URL链接。

2。坑式攻击：不法分子将恶意软件植入企业或个人经常访问的网站，一旦访问这些网站，恶意程序就会利用漏洞对其进行感染。。(网页挂马)[XY002][XY001]3。捆绑通信：捆绑正常软件或恶意软件进行通信，用户在下载安装这些软件的同时激活恶意软件，导致病毒感染。(尤其是游戏插件)

4。通过移动存储方式传播：通过感染u盘、移动硬盘、闪存卡等移动存储介质感染接入设备进行传播。(那&#039；伊朗如何&#039；美国核设施被招募。)

归根结底，大部分用户中病毒的原因是缺乏网络威胁防范意识。，轻易相信邮件信息、软件内容。很多犯罪分子只是利用用户&#039；贪小便宜伪装淘宝JD.COM发送打折邮件，诱骗用户点击。很多都是通过游戏外挂传播的。为了满足自己的虚荣心，他们在不知道自己已经被非法黑客所困的情况下使用插件。，造成敲诈勒索。如果你赢了，就有&#039；你无能为力。当密钥被破解或支付后，我可以告诉你如何防范

勒索病毒引起的恐慌。医院、加油站、学校、公安系统纷纷招人，it&#039它不是核心服务器。都是终端设备。似乎人们&#039；美国的安全目标也发生了变化。不加油还可以接受，取消操作就太戏剧化了。好了，中国人可以提高安全意识了。首先，杀毒软件可以有效防护，但是和发达国家一样，杀毒软件不是很强，所以还是中招。？备份是数据安全的最后一道防线，也是离线备份。传统上可以整个百度云备份文件，系统被破坏了重新敲打，至少损失减少了。不过我个人建议你可以用一个ghost或者更强的trueimage来保护图像级别。当然数据备份到哪里也很有讲究，本地备份的时候还是加密的。trueimage有安全区的概念。，即在本地磁盘上创建另一个专有格式的文件系统，没有病毒可以访问，用户可以备份和恢复数据，方便、快捷、安全，终端设备是首选。

我亲自测试过，效果不错。安全区域中的备份文件没有加密。

赎金病毒属于勒索木马病毒，目前wanacry赎金病毒已经席卷全球。

WannaCry(也称为WannaDecryptor)，a&quot蠕虫状的&quot3.3MB大小的勒索软件。，被不法分子利用危险的漏洞&quot永恒的蓝色&quotNSA(美国国家安全局)泄露的。

该恶意软件扫描电脑上的TCP445端口(服务器消息块/SMB)，以类似蠕虫病毒的方式传播，攻击主机并加密存储在主机上的文件，然后要求以比特币的形式支付赎金。。勒索的金额是300到600美元。

2017年5月14日WannaCry勒索软件出现变种：WannaCry2.0，传播速度取消或更快。截至2017年5月15日WannaCry已经导致至少150个国家遭到网络攻击，影响了金融、能源、医疗等行业，引发了严重的危机管理问题。国内部分Window操作系统用户被感染，首当其冲的是校园网用户。，大量的实验室数据和毕业设计都被锁定加密。

目前安全行业还未能有效破解这种勒索病毒的恶意加密行为。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。，给了犯罪组织可乘之机，最后带来了这次袭击150个国家的勒索病毒。

勒索软件的工作原理：

勒索软件是黑客劫持用户的恶意软件&#039；设备或文件，并向用户勒索金钱。。黑客利用系统漏洞或网络钓鱼将病毒植入受害者&#039；的电脑或服务器，对硬盘甚至整个硬盘上的文件进行加密，然后在解密之前向受害者索要赎金。如果用户未能在指定时间支付黑客要求的金额，锁定的文件将无法恢复。。

1。针对个人用户常见的攻击方式

，用户通过浏览网页下载勒索病毒。攻击者将病毒伪装成盗版软件、外挂软件、色情播放器等。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。针对个人用户的攻击流程如下图所示：

攻击流程

2。企业用户常见的攻击方法

Lesu病毒对企业用户常见的攻击方式有系统漏洞攻击、远程访问弱密码攻击、钓鱼邮件攻击、web服务漏洞和弱密码攻击、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office、PDF图标等exe程序。

1)系统漏洞攻击

系统漏洞是指操作系统逻辑设计中的缺陷或错误。不法分子通过网络植入木马和病毒攻击或控制整台计算机，窃取计算机中的重要数据和信息，甚至破坏系统。和个人用户一样，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较多，更新补丁费时费力，有时需要中断业务，所以企业用户不及时更新补丁，对系统造成严重威胁。攻击者可以通过漏洞植入病毒，并快速传播。。席卷全球的Wannacry勒索病毒利用了永恒之蓝的漏洞，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、弱密码等手段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被绝对隔离，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

互联网上有大量的漏洞攻击工具。特别是武器级NSA方程组织工具的泄露，对网络安全造成了巨大影响，并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，所以很多机器都开启了远程访问功能。如果密码太简单，就会给攻击者可乘之机。很多用户心存侥幸，总觉得网络上那么多机器。被攻击的概率很低，但事实上，在世界各地，成千上万的攻击者不断使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。与个人用户相比，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勒索病毒综合分析报告

北京时间2017年5月13日上午，本周五，全球近百个国家遭遇勒索病毒攻击。

目前，勒索软件已经肆虐国内多所高校。国家网络与信息安全中心也发布了反勒索补丁的地址。

这种勒索病毒的攻击具有威胁性，就像一场前所未有的大灾难，许多媒体都利用了&quot坠落&quot！"诸如此类。。但其实只要我们的电脑系统经常更新，是不会被这种病毒攻击的。在微软&#039；今年3月的s安全更新中，有针对该勒索软件利用的漏洞的安全补丁。

安装补丁

此次爆发的勒索病毒WannaCry依托的是Windows10代码的漏洞，微软在3月14日发布了该漏洞的补丁。Windows用户开启自动补丁安装功能非常重要。这样可以保证第一时间安装微软发布的补丁。打了补丁的系统被攻击的风险很低。

数据备份

定期对操作系统进行完整备份。这样，即使电脑被勒索软件攻击。您也可以从其他地方恢复所有文件。请注意，这意味着备份不应该在同一台电脑上进行，而是通过云存储系统或外置硬盘进行。

以上文章内容均为&quot勒索软件&quot和&quot勒索软件攻击方法&quot。