**勒索病毒防范指南**

**2020年5月26日星期二**

目录

[1. 前言 1](#_Toc41409145)

[1.1. 无法估量损失的新型电脑病毒 1](#_Toc41409146)

[1.2. 勒索病毒进程演变，动机始终为金钱变现 1](#_Toc41409147)

[1.3. 实际众多勒索事件难破解，解密不是万能药 3](#_Toc41409148)

[2. 病毒种类 4](#_Toc41409149)

[2.1. 文件加密勒索病毒 4](#_Toc41409150)

[2.2. 锁屏勒索病毒 4](#_Toc41409151)

[2.3. 主引导记录（MBR）勒索病毒 5](#_Toc41409152)

[2.4. 网络服务器加密勒索病毒 5](#_Toc41409153)

[2.5. 移动设备勒索软件（安卓） 5](#_Toc41409154)

[2.6. 另类的勒索攻击 5](#_Toc41409155)

[3. 病毒传播方式 7](#_Toc41409156)

[3.1. 远程桌面入侵 7](#_Toc41409157)

[3.2. 共享文件夹入侵 7](#_Toc41409158)

[3.3. 网站挂马 7](#_Toc41409159)

[3.4. 恶意软件 7](#_Toc41409160)

[3.5. 邮件传播 8](#_Toc41409161)

[3.6. 漏洞传播 8](#_Toc41409162)

[3.7. 捆绑传播 8](#_Toc41409163)

[3.8. 介质传播（如U盘蠕虫传播） 8](#_Toc41409164)

[4. 病毒传播特征 9](#_Toc41409165)

[4.1. 漏洞利用手段加持，勒索病毒传播更迅速 9](#_Toc41409166)

[4.2. 勒索病毒多平台扩散 9](#_Toc41409167)

[4.3. 安全软件对抗持久，勒索病毒持续变种 9](#_Toc41409168)

[4.4. 愈加复杂密码算法加码，受害者无奈妥协 9](#_Toc41409169)

[4.5. 勒索病毒蹭热点，诱导受害者点击中招 9](#_Toc41409170)

[4.6. 勒索软件即服务(RaaS)呈爆炸式发展，降低勒索门槛 10](#_Toc41409171)

[4.7. 攻击目标日益精准化，各行业需要加强重视 10](#_Toc41409172)

[4.8. 攻击以金钱驱动为主，转变以泄漏事件为辅 11](#_Toc41409173)

[4.9. 伪勒索，数据破坏意图明显 12](#_Toc41409174)

[4.10. 中文定制化，预警信息依然直观易懂 12](#_Toc41409175)

[4.11. 热衷于虚拟货币的支付方式，加大受害者支付成本 12](#_Toc41409176)

[4.12. 勒索赎金定制化，根据企业规模制定不同价格 13](#_Toc41409177)

[5. 勒索病毒带来的直观影响 14](#_Toc41409178)

[5.1. 业务停摆，常规业务无法进行 14](#_Toc41409179)

[5.2. 合规与数据之间的两难抉择 14](#_Toc41409180)

[5.3. 数据泄漏，企业数据成为黑客把柄 14](#_Toc41409181)

[5.4. 潜在隐患暴露，引发更多黑客攻击事件 15](#_Toc41409182)

[5.5. 企业/组织的公信力、声誉受影响 15](#_Toc41409183)

[5.6. 医疗行业严重者影响患者生命 15](#_Toc41409184)

[6. 中招后的应对措施 16](#_Toc41409185)

[6.1. 正确处置方法 16](#_Toc41409186)

[6.2. 错误的处置方法 17](#_Toc41409187)

[7. 具体防范措施 17](#_Toc41409188)

[7.1. 针对个人用户的安全建议 17](#_Toc41409189)

[7.2. 针对企业用户的安全建议 18](#_Toc41409190)

## 前言

2017年4月中旬，“永恒之蓝”攻击工具在网络盛传，5月不法分子通过改造此工具制作了WannaCry勒索病毒，一时间全球众多医院、高校、企业、政府及个人PC接连不断中招，受害者被要求支付高额赎金才可解密恢复文件，这是勒索病毒第一次以如此“亲民”的方式大规模渗透进各类网络。

2017年12月13日，“勒索病毒”入选国家语言资源监测与研究中心发布的“2017年度中国媒体十大新词语”。由于近年来数字加密币的流行，勒索病毒感染正处于愈演愈烈的态势。

### 无法估量损失的新型电脑病毒

勒索病毒（英：Ransomware），是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播，通过恐吓、绑架用户文件或破坏用户计算机等方式，向用户勒索钱财。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。由于原理是利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。

2018年3月，国家互联网应急中心通过自主监测和样本交换形式共发现23个锁屏勒索类恶意程序变种。该类病毒通过对用户手机锁屏，勒索用户付费解锁，对用户财产和手机安全均造成严重威胁。

### 勒索病毒进程演变，动机始终为金钱变现

事实上，WannaCry不是第一个在国内出现的勒索病毒。早期的勒索病毒通常是通过钓鱼邮件、社工等方式传播，通常传播规模量比较小，随着2017年NSA方程式工具泄露，“永恒之蓝”工具被大量利用，勒索病毒开始爆发式增长。

目前已知最早的勒索病毒雏形诞生于1989年，该木马程序以“艾滋病信息引导盘”的形式进入系统，采用替换DOS系统文件的方式，实现开机记数。一旦系统启动次数达到90次时，该木马将隐藏磁盘的多个目录，C盘的全部文件名也会被加密，从而导致系统无法启动。此时，屏幕显示信息，声称用户的软件许可已经过期，要求用户通过指定邮箱支付赎金以解锁系统。该病毒被称为艾滋病特洛伊木马或PC Cyborg病毒。

2006年出现的Redplus勒索木马是中国大陆首个勒索软件。该木马会隐藏用户文档和包裹文件，然后弹出窗口要求用户将赎金汇入指定银行账号。该木马程序运行时，还会试图终止除几个系统进程之外的所有正在运行的进程程序。如果计算机系统中装有反病毒软件和一些病毒分析工具，木马也会将其进程终止，以达到保护自己的目的。据国家计算机病毒应急处理中心统计，来自全国各地的该病毒及其变种的感染报告有581例。次年，出现的新型蠕虫病毒开始使用更复杂的RSA加密方案，同时密钥大小不断增加。

一些文字和图片的手机截图

描述已自动生成

图 1 Redplus勒索木马

后来，勒索病毒又有了另外一种表现形式，那就是“非法”设置开机密码。对于这一种“敲诈”方法，实际上进入PE后直接去掉开机密码就可以了，数据不会丢失。

手机屏幕截图

描述已自动生成

图 2 “非法”设置开机密码

2013年，随着比特币市场的疯狂兴起，勒索赎金的支付方式也产生的很大变化。早期的勒索软件采用传统的邮寄方式接收赎金，会要求受害者向指定的邮箱邮寄一定数量的赎金，或者向指定号码发送可以产生高额费用的短信。直到比特币这种虚拟货币出现，为勒索软件提供了更为隐蔽的赎金获取方式。2013年以来，勒索软件逐渐采用了比特币为代表的虚拟货币支付方式，不可溯源的赎金渠道加速了勒索软件的泛滥。

手机屏幕截图

描述已自动生成

图 3 如今人尽皆知的勒索病毒界面

### 实际众多勒索事件难破解，解密不是万能药

事实上，能够在勒索事件后成功解密的组织机构并不多，愈发复杂的加密方式给黑客带来了更大的信心，许多中招的客户经常为黑客的加密方式和密码的复杂性感到苦恼，总而言之，勒索病毒在多数情况下难以解密。

手机屏幕截图

描述已自动生成

图 4 常见的勒索病毒（GlobeImposter勒索病毒家族的最新变种）加密方式

与此同时，已有些许受害者会发现，即使乖乖交了赎金，黑客也有可能不信守承诺，不帮用户解密。

图片包含 游戏机

描述已自动生成

图 5 支付赎金后，黑客并未如期解密

## 病毒种类

常见的勒索病毒主要有以下几类：

### 文件加密勒索病毒

所有文件被加密（文件、图片、视频甚至是数据库），受感染的文件被加密后会被删除，用户通常会在文件夹中看到一个包含付款说明的文本文件。当用户尝试打开其中一个加密文件时，才可能会发现问题。最典型的案例就是WannaCry，该类型勒索病毒是目前最常见的勒索病毒。感染文件型勒索病毒后，病毒会更改系统桌面并展示勒索支付提示。

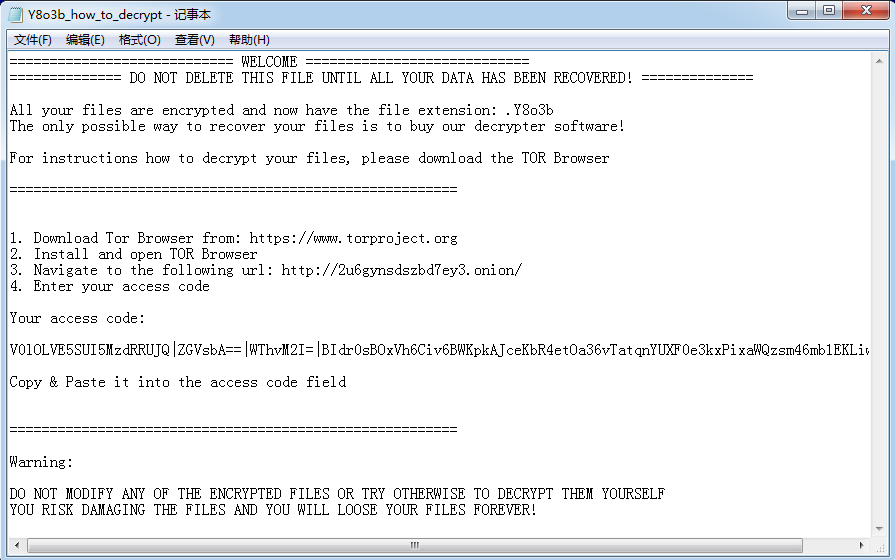


图 6 受害者桌面的警示文件

### 锁屏勒索病毒

锁屏病毒会锁定电脑屏幕并要求付款。它会呈现一个全屏图像并阻止所有其它窗口开启。幸运的是，这种类型的勒索病毒并不会加密用户的数据文件，数据有挽回的可能。

手机屏幕截图

描述已自动生成

图 7 锁屏病毒示例

### 主引导记录（MBR）勒索病毒

主引导记录（MBR）是电脑硬盘驱动器的一部份，影响操作系统的启动功能。主引导记录勒索病毒会更改电脑的主引导记录，中断电脑的正常启动，然后在屏幕上显示要求赎金的内容，最流行的Petya就属于这类病毒。这类病毒不同于文件型勒索病毒，感染后病毒可能采用磁盘级加密技术覆写磁盘，数据基本无挽回可能。

电脑屏幕的照片上写着字

描述已自动生成

图 8 Petya变种病毒页面

### 网络服务器加密勒索病毒

这类病毒专门针对网络服务器上的文件进行加密。它通常使用内容管理系统中的已知漏洞，在网络服务上释放和安装勒索病毒，例如最近经常碰到的master勒索病毒。

### 移动设备勒索软件（安卓）

目前针对移动设备的勒索病毒主要存在于安卓系统上（iOS系统安全性要高一些，但也要注意及时升级），用户遭受感染的方式一般为下载、浏览不信任程序以及网站或伪装程序。

### 另类的勒索攻击

1. **DDoS攻击**

通过DDoS攻击来堵塞服务器通道。万幸的是这样的攻击不会影响到企业的数据安全。目前，国内市场中常常出现的DDoS一般分为四种：ARP攻击、ICMP攻击、TCP攻击、应用层攻击。DDoS攻击日渐猖獗，大量实践数据表明，DDoS特别青睐于安全管理等级不高的服务器。

1. **针对知识产权的攻击**

目前，使用盗版数据库、操作系统等不合规经营问题普遍存在。对政府部门和大型上市公司而言，黑客收集相关证据后可以此为把柄勒索赎金，并向Microsoft、Oracle等公司举报。类似事件可能将机构卷入复杂的知识产权诉讼案件中。

1. **其它衍伸的胁迫事件**

受害者数据、军事机密、刑事调查文件、设计图纸、企业核心技术及产品等，都是组织机构的核心命脉，近年来这类文件已成为黑客觊觎的攻击对象，只要获取到这些文件，黑客可以做加密之外的任何事情，因此除了面对高额的赎金，组织机构还可能面临长期的数据胁迫，毕竟已经泄漏的数据很大程度上难以收回。

## 病毒传播方式

勒索病毒的主要攻击方式依然以远程桌面入侵为主，其次为通过海量的垃圾邮件传播，或利用网站挂马和高危漏洞等方式传播，整体攻击方式呈现多元化的特征。

### 远程桌面入侵

攻击者大多利用弱口令漏洞、系统漏洞等方式获得远程登录用户名和密码，之后通过RDP（远程桌面协议）远程登录目标服务器并运行勒索病毒程序。“黑客”一旦能够成功登录服务器，就可以在服务器上为所欲为。即使服务器上安装了安全软件，也有可能会被黑客第一时间手动退出，以便于后续投毒勒索。

如常见的GlobeImposter勒索病毒，主要是开启远程桌面服务的服务器，攻击者通过暴力破解服务器密码，对内网服务器发起扫描并人工投放病毒加密文件进行勒索，多家医院被入侵，致使医院系统瘫痪，患者无法正常接受治疗。

### 共享文件夹入侵

此类病毒通常会结合远程桌面入侵，对本地磁盘与共享文件夹的所有文件进行加密，导致系统、数据库文件被加密破坏。

### 网站挂马

黑客通过在色情网站某些页面中嵌入恶意代码文件，当网民、企业员工访问色情网站时，触发恶意代码，导致电脑被勒索病毒感染，严重者甚至会感染整个组织机构/企业的网络。

### 恶意软件

黑客利用恶意软件试图获取计算机系统和网络的资源以及在未获得用户的许可时得到其私人的敏感信息，如个人信息凭证，并以此进一步入侵网络，实施勒索病毒入侵。

图片包含 游戏机, 钟表, 画

描述已自动生成

图 9 下载恶意软件容易引起勒索事件

### 邮件传播

这种传播方式也是病毒界老套路的传播方式。病毒执行体附着于邮件附件的docx、XLS、TXT等文件中，攻击者以广撒网的方式大量传播垃圾邮件、钓鱼邮件，一旦收件人打开邮件附件或者点击邮件中的链接地址，勒索软件会以用户看不见的形式在后台静默安装，实施勒索。

手机截图图社交软件的信息

描述已自动生成

图 10 伪装为发票的勒索病毒

### 漏洞传播

这种传播方式是这几年非常流行的病毒传播方式。通过网络、系统、应用程序的漏洞攻击用户。例如国内曾经泛滥的WannaCry就是这样的典型：利用微软445端口协议漏洞，感染传播网内计算机。

### 捆绑传播

与其他恶意软件捆绑传播，这种传播方式这两年有所变化。有用户使用P2P下载例如Bt、迅雷、电驴等下载工具下载文件后，勒索病毒体同下载文件进行捆绑导致用户感染。

### 介质传播（如U盘蠕虫传播）

可移动存储介质、本地和远程的驱动器以及网络共享传播、社交媒体传播。

## 病毒传播特征

### 漏洞利用手段加持，勒索病毒传播更迅速

我们能够看到，在过去几次大规模爆发的勒索病毒事件中，黑客主要利用钓鱼邮件、恶意链接、RDP口令爆破等传播渠道为主，诱导用户点击运行相应的程序。而随着各类漏洞信息的披露、信息系统的普及、复杂的网络环境、难以区分的网络边界，勒索病毒更多利用了高危漏洞、鱼叉式攻击，或水坑攻击等非常专业的黑客攻击方式传播，乃至通过软件供应链传播，大大提高了入侵成功率和病毒影响面。

### 勒索病毒多平台扩散

目前受到的勒索病毒攻击主要是windows系统，但也陆续出现了针对MacOS、Linux等平台的勒索病毒，随着windows的防范措施完善和攻击者永不满足的贪欲，未来勒索病毒在其他平台的影响力也会逐步增加。

### 安全软件对抗持久，勒索病毒持续变种

目前仅国内来看，已有众多杀毒软件、病毒防护软件与勒索病毒进行抗衡，原理多基于病毒库、沙箱、文件备份、诱捕等方式，随着各类安全软件对于勒索病毒的免疫能力持续升级，基于原有特征的入侵已相对较难，因此勒索病毒需要不断演变，即演变成我们常说的变种病毒，才能够提高感染的成功率，这也是当前勒索病毒常见的手段。

### 愈加复杂密码算法加码，受害者无奈妥协

如今，虽然已有部分厂商能够对数据进行恢复，但大多依赖已公开的密钥和解密方式，如果为了降低厂商的破解效率和能力，狠心的黑客很有可能大范围使用诸如4096的RSA等加密算法，可以用“太阳系爆炸了都无法破解来形容了”，因此做好事前防范才是关键。

### 勒索病毒蹭热点，诱导受害者点击中招

勒索病毒在不断演变的过程中，本身也增加了许多带有社会事件话题的影子，如2020年新出现的“新冠肺炎”勒索病毒，人们对“新冠肺炎”的关注促使了恶意木马作者也打起了主意，以疫情有关词汇或信息为诱饵，通过社交网络、钓鱼邮件等渠道传播计算机勒索病毒，进行网络攻击。黑客大肆传播的这一系列勒索病毒均带有“冠状病毒”、“疫情”、“武汉”等诱饵词汇。这些勒索病毒将会使得绝大多数文件被加密算法修改，并添加一个特殊的后缀，且用户无法读取原本正常的文件，对用户造成无法估量的损失。

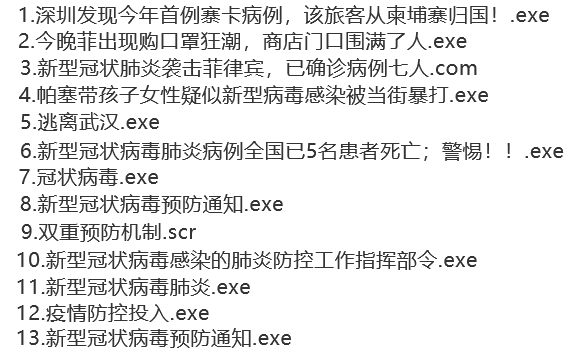


图 11 借“新冠肺炎”热点事件传播的相关病毒

如Petya勒索病毒，Petya一词本身取自007系列电影《黄金眼》​中的武器卫星名。由此可以看到勒索病毒并非以一贯严肃的风格出现，反而通常会借势节日热点和社会热点等来造势，试图引起受害者的关注。

### 勒索软件即服务(RaaS)呈爆炸式发展，降低勒索门槛

暗网和地下黑客论坛一直是恶意软件推广和销售的地方，一些恶意软件的开发者会利用暗网来发布和销售自己的勒索病毒软件。这些勒索病毒大多数是采用RAAS(勒索软件即服务)模式进行分发，比方之前已知的几大流行勒索病毒家族：GandCrab、CrySiS、Globelmposter、Sodinokibi等。想象一下这样的广告：

“相信我，你也可以成为成功的网络罪犯!简单!低成本!一夜暴富!不需要花多年时间浸淫代码编写或软件开发技艺。只需要下载我们简单的勒索软件工具包，就能让您坐等钱财源源而来——享受在家办公的舒适与弹指坐听比特币落袋声的双重快乐。”

你是否也会蠢蠢欲动，可以说，RAAS使得任何人，包括几乎没有IT经验的那些人，都可以成为成功的网络罪犯。

### 攻击目标日益精准化，各行业需要加强重视

根据美国Verizon最新的《2020年数据泄漏研究报告》来看，相比于需要长期潜伏在受害者的网络中进行持续攻击、传播病毒，黑客通过部署勒索软件会更能够快速地获得金钱变现，尤其在支付数据、个人数据、业务数据十分重要的行业，如零售行业、医疗行业、制造业，黑客的野心会更大。

结合实际经验来看，如今的勒索病毒，从广泛而浅层的普通用户，明显转向了中大型政企机构、行业组织。很多企业系统因为管理的原因，或系统版本较低，不能及时安装补丁等客观因素，导致企业网络更容易被入侵，而企业数据的高价值，这便导致企业受害者倾向于支付赎金挽回数据。

### 攻击以金钱驱动为主，转变以泄漏事件为辅

数据泄漏在勒索病毒事件中常常会被忽视，但始终是绕不开的话题，我们认为在未来，部分勒索病毒事件的性质会逐渐转变为数据泄露，即黑客已在原有的基础上进行了事件的加码，如几家著名的勒索软件供应商已经表示，他们计划开始发布拒绝付款的受害者所窃取的数据。

当企业有完善的数据备份方案，拒绝缴纳赎金时，勒索团伙则采取另一种手段：威胁公开受害者的机密文件来勒索。更糟的是，一个勒索软件团伙现在已经创建了一个公共网站，用于发布一些不合作的受害公司，不合作的受害公司中了勒索病毒，选择重建其业务，而不是悄悄地交赎金。网站专门发布不合作公司的名单。下图为Maze病毒团伙在数据加密勒索企业失败后，公开放出了被攻击企业2GB私密数据。

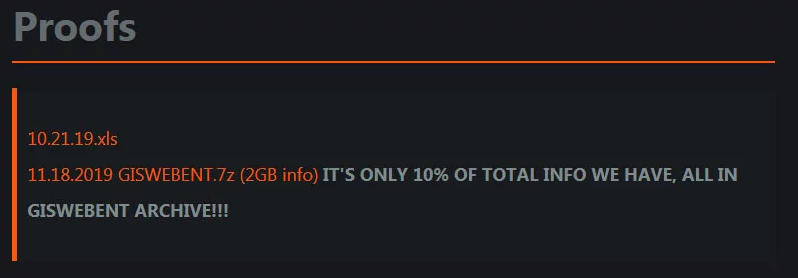


图 12 拒绝支付赎金的企业数据被公开至互联网

该网站用服务英语写道：在这网站发布的公司，都是那些不打算交钱，不合作的公司名单，并试图隐瞒黑客已经成功入侵并下载其重要资源的公司。不合作公司的数据还有重要文件资源，将会发布这网站上。

甚至还有名为Sodinokibi勒索团伙也在黑客论坛发声，称如果被攻击者拒绝缴纳赎金，则会将其商业信息出售给其竞争对手。数据泄露对大型企业而言，带来的损失可能更加严重，不仅会造成严重的经济损失，还会使企业形象受损，造成严重的负面影响。

2020年，Verizon机构已经意识到这一点，并将数据泄漏与勒索病毒事件关联。

### 伪勒索，数据破坏意图明显

有些勒索家族在感染目标中不断搜寻敏感信息，包括军事机密、银行信息、欺诈、刑事调查文件，行动举止完全不像为了图财。此外，有些“勒索病毒”会对文件玩了命似的多次加密，甚至对文件进行无法修复的破坏，完全断了收赎金的后路。

### 中文定制化，预警信息依然直观易懂

勒索事件热衷于使用“英文”、或受害者的母语来提醒用户。因此对国内用户“量身打造”的勒索病毒，会非常“贴心”的使用全中文的勒索提示界面，个别会要求直接通过微信、支付宝来缴纳赎金（当然是极少数，大多数还是要求用比特币等虚拟货币来支付）。

中国作为拥有10亿多网民的网络应用大国，毫无疑问成为勒索病毒攻击的重要目标，一部分勒索病毒运营者开始在勒索信、暗网服务页面提供中文语言界面。

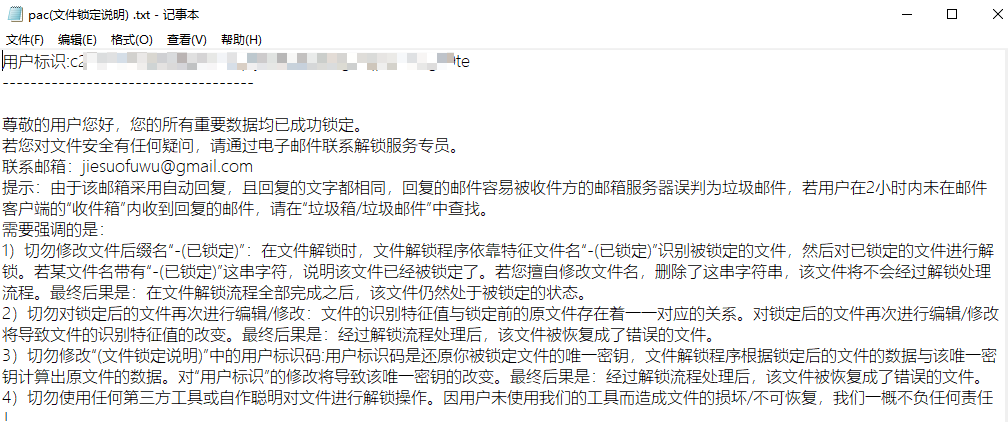


图 13 中文定制化勒索警示信息界面

### 热衷于虚拟货币的支付方式，加大受害者支付成本

由于比特币有一定的匿名性，便于黑客隐藏身份；其次，它不受地域限制，可以全球范围收款；同时，还有“去中心化”的特点，可以让黑客通过程序自动处理受害者赎金。相比于其他数字货币，比特币目前占有最大的市场份额，具有最好的流动性，所以成为黑客的选择。

当然，为了让身份难以追踪，黑客往往不会选择以银行、支付宝、微信等有严格监管、追溯机制的方式收款，转而选择其它复杂的虚拟货币，无意中加大了受害者的支付成本，试想一下，如果黑客要求你使用一种从未听过的虚拟货币进行支付，也许我们会先被虚拟货币本身搞得崩溃。

手机屏幕截图

描述已自动生成

图 14 要求受害者联系电子邮件并支付高额的勒索费以恢复其加密文件

### 勒索赎金定制化，根据企业规模制定不同价格

随着用户安全意识提高、安全软件防御能力提升，勒索病毒入侵成本越来越高，攻击者更偏向于向不同企业开出不同价格的勒索赎金，定制化的赎金方案能有效提升勒索成功率，直接提升勒索收益。

## 勒索病毒带来的直观影响

### 业务停摆，常规业务无法进行

2020年，根据法院文书网显示，郑大一附院因第三方运维人员在2018年年底的一个误操作，导致郑东院区、惠济院区、医学院院区所有门诊、临床计算机业务受到恶意语句攻击，门急诊挂号、门急诊叫号、门急诊支付、门急诊药房、门急诊检查、门急诊检验等业务系统均无法正常操作，所有门诊相关业务停止服务，造成该医院三个院区门诊业务停滞近两个小时，造成大量患者积压在门诊无法就诊，严重影响医院的正常医疗工作，院方直接损失200万元。

尽管本次事件的并不是由勒索病毒引起，但院方业务停摆造成的损失给各个对业务实时性有高要求的行业敲响了警钟，勒索病毒作为以加密关键文件（如服务器中的数据库、系统文件等）为主要手段的病毒，已然成为造成业务中断的主要威胁之一。

### 合规与数据之间的两难抉择

根据接触的客户来看，在众多遭受勒索病毒攻击的行业中，医院、企业类客户占比最大，这些往往会选择第三方解密（即使解密成功率低，但迫于数据的重要性，也会义无反顾尝试）、数据恢复、安全设备防护等方案。

而医疗行业的核心HIS系统存储着大量患者信息，其作为“数据不可丢失”的重要行业，很有可能会在业务连续性和支付赎金之间徘徊，最终屈服于黑客，选择支付赎金。

目前根据我们获得的消息，包括上海、江苏、安徽等在内的30多个省份的医院都存在被勒索病毒入侵的案例，部分省份地区的医院在无奈之下，甚至选择支付上百万的赎金/支付上百万请第三方厂商进行数据恢复（毕竟一台服务器的数据恢复价格也不低）。

然而根据《网络安全法》第二十七条规定，“明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。”这也意味着，支付赎金是不合规的手段，那么组织机构面临勒索病毒事件，可选的只有事前做好防护，事中及时响应了。

### 数据泄漏，企业数据成为黑客把柄

如上所述，目前有众多受害者选择不支付赎金，黑客转而以资产泄漏为把柄，威胁受害者支付比特币，这也是未来病毒的发展趋势之一，没有黑客做不到的，只有我们想不到的。

### 潜在隐患暴露，引发更多黑客攻击事件

结合勒索事件的传播方式和传播特征，我们能够看到，黑客通常借助系统漏洞、获得远程桌面RDP凭证等方式进行勒索病毒的植入，被感染的主要原因有：

1. 由于医疗设备的特殊性，几乎不大可能停机，因此很难保持软件基础结构的更新；
2. 仅在特定操作系统或驱动版本中运行的旧版软件很容易成为攻击目标。这些无法更新的设备从某种程度上来说，为恶意软件在网络中的扩散提供了条件

这也意味着，勒索病毒只是黑客攻击的手段之一，事实上，他们可以利用这些漏洞进行诸如DDOS、SQL注入等具有极大危害的攻击，如长期潜伏在信息系统中，获取用户数据、数据库，以进一步破坏企业或组织的数据隐私。

### 企业/组织的公信力、声誉受影响

如今，我们很难在媒体、社交网站上寻找到医疗、政府行业遭受勒索病毒侵害的准确单位，这类客户往往不愿意声张，因为他们意识到一旦勒索病毒事件被大众知晓，单位的公信力和声誉都会遭受影响，其客户常常不会认为勒索病毒太厉害，而是把责任归于单位薄弱的信息系统建设。再试想一下，如果你最近去一家医院就诊，得知医院信息系统被勒索，心里会不会为就医的便利性、个人的数据隐私感到恐慌？

### 医疗行业严重者影响患者生命

区别于其它行业，在医疗组织机构中，IT系统之间紧密相连、系统没有发生服务中断的时候很难独立隔离，为恶意软件创造了合适的环境。如超声波设备、EKG、除颤器、输液泵或生命体征监护仪等设备，一旦遭受勒索病毒袭击，可能直接对患者造成生命威胁。

## 中招后的应对措施

当我们已经确认感染勒索病毒后，应当及时采取必要的自救措施。之所以要进行自救，主要是因为：等待专业人员的救助往往需要一定的时间，采取必要的自救措施，可以减少等待过程中，损失的进一步扩大。例如：与被感染主机相连的其他服务器也存在漏洞或是有缺陷，将有可能也被感染。所以，采取自救措施的目的是为了及时止损，将损失降到最低。

### 正确处置方法

1. **隔离中招主机**

当确认服务器已经被感染勒索病毒后，应立即隔离被感染主机。

隔离的目的，一方面是为了防止感染主机自动通过连接的网络继续感染其他服务器；另一方面是为了防止黑客通过感染主机继续操控其他服务器。

有一类勒索病毒会通过系统漏洞或弱密码向其他主机进行传播，如WannaCry勒索病毒，一旦有一台主机感染，会迅速感染与其在同一网络的其他电脑，且每台电脑的感染时间约为1-2分钟左右。所以，如果不及时进行隔离，可能会导致整个局域网主机的瘫痪，造成无法估量的损失。

隔离主要包括物理隔离和访问控制两种手段。

**①物理隔离**

物理隔离常用的操作方法是断网和关机。断网主要操作步骤包括：拔掉网线、禁用网卡，如果是笔记本电脑还需关闭无线网络。

**②访问控制**

a.避免将远程桌面服务（RDP，默认端口为3389）暴露在公网上，并关闭445、139、135等不必要的端口。

b.将服务器密码修改为高强度的复杂密码。

1. **排查业务系统**

在已经隔离被感染主机后，应对局域网内的其他机器进行排查，检查核心业务系统是否受到影响，生产线是否受到影响，并检查备份系统是否被加密等，以确定感染的范围。

另外，备份系统如果是安全的，就可以避免支付赎金，顺利的恢复文件。

所以，当确认服务器已经被感染勒索病毒后，并确认已经隔离被感染主机的情况下，应立即对核心业务系统和备份系统进行排查。

### 错误的处置方法

1. **使用移动存储设备**

当确认服务器已经被感染勒索病毒后，在中毒电脑上使用U盘、移动硬盘等移动存储设备。当电脑感染病毒时，病毒也可能通过U盘等移动存储介质进行传播。所以，当确认服务器已经被感染勒索病毒后，切勿在中毒电脑上使用U盘、移动硬盘等设备。

1. **读写中毒主机上的磁盘文件**

当确认服务器已经被感染勒索病毒后，反复读取磁盘上的文件可能会而降低数据正确恢复的概率。

## 具体防范措施

面对严峻的勒索病毒威胁态势，安全实验室提醒广大用户，勒索病毒以防为主，注意日常防范措施，以尽可能免受勒索病毒感染。

### 针对个人用户的安全建议

1. **养成良好的安全习惯**
2. 使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。
3. 重要的文档、数据定期进行非本地备份，一旦文件损坏或丢失，也可以及时找回。
4. 使用高强度且无规律的密码，要求包括数字、大小写字母、符号，且长度至少为8位的密码。不使用弱口令，以防止攻击者破解。
5. 安装具有主动防御的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易才去放行操作。
6. 及时给电脑打补丁，修复漏洞，防止攻击者通过漏洞入侵系统。
7. 尽量关闭不必要的端口，如139、445、3389等端口。如果不使用，可直接关闭高危端口，降低被攻击的风险。
8. **减少危险的上网操作**
9. 浏览网页时提高警惕，不浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。
10. 不要点击来源不明的邮件附件，不从不明网站下载软件，警惕伪装为浏览器更新或者flash更新的病毒。
11. 电脑连接移动存储设备（如U盘、移动硬盘）时，应首先使用安全软件检测其安全性。

### 针对企业用户的安全建议

1. 及时给办公终端和服务器打补丁，修复漏洞，包括操作系统以及第三方应用的补丁，防止攻击者通过漏洞入侵系统。
2. 尽量关闭不必要的端口，如139、445、3389等端口。如果不使用，可直接关闭高危端口，降低被漏洞攻击的风险。
3. 不对外提供服务的设备不要暴露于公网之上，对外提供服务的系统，应保持较低权限。
4. 企业用户应采用高强度且无规律的密码来登录办公系统或服务器，要求包括数字、大小写字母、符号，且长度至少为8位的密码，并定期更换口令。对于各类系统和软件中的默认账户，应该及时修改默认密码，同时清理不再使用的账户。
5. 对重要的数据文件定期进行非本地备份，一旦文件损坏或丢失，也可以及时找回。
6. 尽量关闭不必要的文件共享。
7. 提高安全运维人员职业素养，定期进行木马病毒查杀。
8. 安装诺亚防勒索软件，防御未知勒索病毒。
9. 按照《国家网络安全事件应急演练指南》开展勒索病毒入侵应急演练。

本指南由浙江省委网信办指导、杭州美创科技有限公司编撰。