信息安全前沿课堂讨论

陆皓喆 2211044 网络空间安全学院

2023 年 12 月 19 日

4 什么是勒索软件？介绍勒索软件的原理、危害和安全建议？

勒索软件又称勒索病毒，是一种特殊的恶意软件，又被归类为“阻断访问式攻击”（denial-of-access attack），与其他病毒最大的不同在于攻击手法以及中毒方式。勒索软件的攻击方式是将受害者的电脑锁起来或者系统性地加密受害者硬盘上的文件，以此来达到勒索的目的。所有的勒索软件都会要求受害者缴纳赎金以取回对电脑的控制权，或是取回受害者根本无从自行获取的解密密钥以便解密文件。勒索软件一般通过木马病毒的形式传播，将自身掩盖为看似无害的文件，通常假冒普通电子邮件等社会工程学方法欺骗受害者点击链接下载，但也有可能与许多其他蠕虫病毒一样利用软件的漏洞在互联网的电脑间传播。

下面简单的介绍一下一些常见的勒索软件的类型。

根据勒索软件对受害者系统采取的措施，主要可以分为以下几类：

绑架用户数据使用加密算法（如 AES、RSA 等）将用户的文件进行加密，用户在没有秘钥的情况下无法操作自己的文件。用户可以访问设备，但是对设备内的数据无法操作。

典型勒索软件有：WannaCry、GlobeImposter、CryptoLocker，TeslaCrypt 等。

锁定用户设备不加密用户的文件，但是通过修改一些配置或者系统文件，使得用户无法进入设备。

典型勒索软件有：NotPetya 等。

锁定用户设备和绑架数据既加密用户文件，又锁住用户设备。是 1 和 2 的结合体。

典型勒索软件有：BadRabbit 等。

见勒索软件之多，以至于它可能出现在我们的日常生活当中。

下面我们简要的了解一下**勒索软件的原理**。

1. 公开密钥密码体制要求密钥成对出现，一个用于加密，另一个用于解密，并且且不可能从其中一个推导出另一个。

2. 加密过程：

作者首先在自己电脑上生成的私钥 A 和公钥 A，目标电脑上病毒在会随机生成私钥 B 和公钥 B，目标电脑上的文件会被通过公钥 B 进行加密，目标电脑上的私钥 B 被公钥 A 加密，最后删除目标电脑上的私钥 B 、公钥 A、数据。

3. 解密过程：

通过作者私钥 A 解加密私钥解出私钥 B，通过私钥 B 解密用户数据。

需要注意的是：

1. 使用本地 RSA 算法将 AES 密钥加密；

2. 使用 RSA 等非对称加密算法，将受害者本地生成的 RSA 私钥进行了加密。通过这两步，只有作者使用自己私钥解密受害者 RSA 私钥后，受害者才能还原到本地 AES 密钥，从而使用 AES 算法解密文件。

当然，勒索软件，具有很多的危害。

一般被勒索病毒感染后，将导致重要文件无法读取、关键数据被损坏、计算机被锁死无法正常使用等情况；为了指引被感染者缴纳赎金，勒索病毒还会在桌面等明显位置生成勒索提示文件，被感染者需要通过缴纳高额赎金才能获取解密密钥恢复计算机系统和数据文件的正常使用，**多数情况即使缴纳了高额的赎金也未必能正常恢复数据**。因此，勒索病毒具有数据恢复代价大和数据恢复可能性极低的特点。

常见勒索病毒传播途径很多，它们可以通过各种形式进行传播。

1. **网站挂马**。用户浏览挂有木马病毒的网站，上网终端计算机系统极可能被植入木马并感染上勒索病毒。

2. **邮件传播**。邮件传播是目前互联网上常见的病毒传播方式。攻击者通过利用当前热门字样，在互联网上撒网式发送垃圾邮件、钓鱼邮件，一旦收件人点开带有勒索病毒的链接或附件，勒索病毒就会在计算机后台静默运行，实施勒索。

3. **漏洞传播**。通过计算机操作系统和应用软件的漏洞攻击并植入病毒是近年来流行的病毒传播方式。最典型的案例是 2017 年在国内泛滥的 WannaCry 大规模勒索事件，攻击者正是利用微软 445 端口协议漏洞，进行感染传播网内计算机。

4. **捆绑传播**。攻击者将勒索病毒与其他软件尤其是盗版软件、非法破解软件、激活工具进行捆绑，从而诱导用户点击下载安装，并随着宿主文件的捆绑安装进而感染用户的计算机系统。

5. **介质传播**。攻击者通过提前植入或通过交叉使用感染等方式将携有勒索病毒的 U 盘、光盘等介质进行勒索病毒的移动式传播。此种传播途径往往发生在文印店、公共办公区域等高频交叉使用可移动存储介质的场所，也可能通过广告活动派发、街区丢弃等方式实现诱导用户使用携带勒索病毒的 U 盘、光盘。携带勒索病毒的光盘、U 盘一旦接入计算机，勒索病毒即可能随着其自动运行或用户点击运行导致计算机被感染。

对于这些勒索软件，我们应该如何防范呢？下面我给出一些安全建议。

对于**企业**来说，勒索软件会造成生产链的数据丢失，会导致停工停产，所以企业要十分重视对勒索软件的防范。

我们可以：1. 针对网络安全加大投入，购买专业安全公司的安全产品和安全服务，对企业网络进行全面加固；

2. 加强企业工作人员的安全防护意识，适时进行网络安全攻防演习，将网络安全相关考核成绩纳入部门重要考核之一；

3. 企业重要 IT 系统上云，并购买专业云厂商的专业安全防护服务；

4. 同时对企业重要核心资产进行备份，防止因为被勒索导致企业生产停滞。

对于**个人**来说，勒索软件也会造成我们日常生活中使用电脑的不便性，所以我们也需要树立起一定的安全防范意识。

1. 及时给电脑打补丁，修复漏洞；

2. 谨慎打开来历不明的邮件，点击其中链接或下载附件，防止网络挂马和邮件附件攻击；

3. 尽量不要点击 office 宏运行提示，避免来自 office 组件的病毒感染；需要的软件从正规（官网）

途径下载，不要用双击方式打开.js、.vbs、.bat 等后缀名的脚本文件；

4. 升级防病毒软件到最新的防病毒库，阻止已知病毒样本的攻击；

5. 开启 Windows Update 自动更新设置，定期对系统进行升级；

6. 养成良好的备份习惯，对重要数据文件定期进行非本地备份，及时使用网盘或移动硬盘备份个人重要文件；

7. 更改账户密码，设置强密码，避免使用统一的密码，因为统一的密码会导致一台被攻破，多台遭殃，黑客会通过相同的弱密码攻击其它主机；

8. 如果业务上无需使用 RDP 的，建议关闭 RDP，以防被黑客 RDP 爆破攻击。