勒索病毒应急与响应手册

浙江大学网络与信息安全领导小组办公室

二〇一九年三月

前言

勒索病毒主要以邮件、程序木马、网页挂马的形式进行传播，利用各种非对称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。勒索病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。

勒索病毒文件一旦进入本地，就会自动运行。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密公钥，利用加密公钥对文件进行加密。除了拥有解密私钥的攻击者本人，其他人是几乎不可能解密。加密完成后，通常还会修改壁纸，在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。勒索病毒变种类型非常快，对常规的杀毒软件都具有免疫性。攻击的样本以 exe、js、wsf、vbe 等类型为主，对常规依靠特征检测的安全产品是一个极大的挑战。勒索过程如下：



本手册第1章详述如何判断是否已感染勒索病毒，是否已被加密；第2章详述当主机处于不同的中毒阶段时，应如何进行应急响应；第3章介绍对于已加密系统的五种处理方式，重要文件需要恢复应分别尝试备份还原、解密、数据恢复、支付解密，价值较低的文件可直接重装系统，并进行主机加固；第4章详述如何进行勒索病毒的基础防护措施及建议。

通过应用本手册，在不同阶段及时做出响应，尽可能避免或降低损失。

目录

第一章 判断当前状态 4

一 感染未加密 4

二 感染已加密 5

第二章 响应当前状态 7

一 隔离中毒主机 7

二 排查其他主机 7

三 主机加固 7

第三章 已加密系统的处理办法 9

一 备份还原 9

二 解密工具 9

三 数据恢复 9

四 支付解密 9

五 重装系统 10

第四章 基础防护措施及建议 11

一 增强安全意识 11

二 增加口令强度 11

三 修复系统漏洞 12

四 修复应用漏洞 12

五 端口管理 12

## 第一章 判断当前状态

### 一 感染未加密

从攻击者渗透进入内部网络的某一台主机到执行加密行为往往有一段时间，如果在这段时间能够做出响应，完全可以避免勒索事件的发生。如果有以下情况，可能是处于感染未加密状态：

1 监测设备告警

如果使用了监测系统进行流量分析、威胁监测，系统产生大量告警日志，例如“SMB 远程溢出攻击”、“弱口令爆破”等，可能是病毒在尝试扩散。



2 资源占用异常

病毒会伪装成系统程序，释放攻击包、扫描局域网络 445 端口等占用大量系统资源，当发现某个疑似系统进程的进程在长期占用 CPU 或内存，有可能是感染病毒。



### 二 感染已加密

勒索病毒的目的是索要赎金，所以会加密文件并在明显位置留下勒索信，通过这两点可以判断系统是否已经被加密。

1 统一的异常后缀

勒索病毒执行加密程序后会加密特定类型的文件，不同的勒索病毒会加密几十到几百种类型的文件，基本都会包括常见的文档、图片、数据库文件。当文件夹下文件变成如下统一异常不可用后缀时，就是已经被加密了。



2 勒索信或桌面被篡改

勒索病毒加密文件的最终目的是索要赎金，所以会在系统明显位置如桌面上留下文件提示，或将勒索图片更改为桌面。勒索信绝大多数为英文，引导被勒索的用户交赎金。





## 第二章 响应当前状态

某台主机在感染勒索病毒后，除了自身会被加密，勒索病毒往往还会利用这台主机去攻击同一局域网内的其他主机，所以当发现一台主机已被感染，应尽快采取响应措施，以下基础措施即使不是专业的人员也可以进行操作，以尽可能减少损失。

### 一 隔离中毒主机

1 物理隔离

断网，拔掉网线或禁用网卡，笔记本也要禁用无线网络。



2 逻辑隔离

访问控制、关闭端口、修改密码。访问控制可以由防火墙等设备来设置，禁止已感染主机与其他主机相互访问；视情况关闭 135、139、445、3389 等端口，避免漏洞或 RDP（远程桌面服务）被利用；尽快修改被感染主机与同一局域网内的其他主机的密码，尤其是管理员（Windows 下的 Administrator，Linux 下的 root）密码，密码长度不少于 8 个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

### 二 排查其他主机

隔离已感染主机后，应尽快排查业务系统与备份系统是否受到影响，确定病毒影响范围，准备事后恢复。如果存在备份系统且备份系统是安全的，就可以将损失降到最低，也可以最快的恢复业务。

### 三 主机加固

主机感染病毒一般都是由未修复的系统漏洞、未修复的应用漏洞或者弱口令导致，所以在已知局域网内已有主机感染并将之隔离后，应检测其他主机是否有上述的问题存在。

(1) 系统漏洞可以使用免费的安全软件检测并打补丁。

(2) 应用漏洞可以使用免费的漏扫产品（AWVS、APPScan等）检测并升级或采用其他方式修复。

(3) 弱口令应立即修改，密码长度不少于8个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

## 第三章 已加密系统的处理办法

### 一 备份还原

备份可以是本机、异机或异地（云端）备份，通常勒索病毒会遍历所有磁盘并加密文件，同时删除 Windows 的阴影卷，删除备份历史快照，所以本机备份恢复的可能性很低。异机备份如果是通过本地磁盘到共享磁盘进行文件或者数据拷贝的方式实现，勒索病毒同样有可能加密了备份文件。与感染病毒的主机不在同一局域网内的异地备份系统最能在此时发挥作用。

进行备份还原前，要确保原主机上病毒已彻底清除，应进行磁盘格式化并重装系统。日常进行合理的数据备份，是最有效的灾难恢复方法。

### 二 解密工具

大部分勒索病毒使用 128 位密钥的 AES（对称加密算法）加密文件，再将 AES 的密钥使用 2048 位密钥的 RSA（非对称加密算法）加密，通过暴力破解来解密是不科学的，所以通常的解密工具是通过已公开的密钥来解密。而密钥来源有三种途径：

* 一是破解勒索程序得到，前提是勒索程序本身存在漏洞，但此概率极低。
* 二是勒索者对受害人感到愧疚、同情等极端情况而公开密钥。
* 三是执法机构获得勒索者的服务器，同时服务器上存储着密钥且执法机构选择公开。

除了付费解密的工具，还可尝试国际刑警组织反勒索病毒网站

（https://www.nomoreransom.org/zh/index.html）提供的解密工具。

### 三 数据恢复

一部分勒索病毒加密文件的时候直接加密原文件，还有一部分勒索病毒是加密原文件副本再删除原文件，而原文件有些会用随机数覆盖，有些并没有。原文件没有被覆盖的情况就可以通过数据恢复的方式进行恢复。

除了收费的专业数据恢复可以尝试使用 DiskGenius 等工具扫描磁盘进行数据恢复。

### 四 支付解密

在早期勒索病毒基本都是勒索不同数额的比特币，但是随着虚拟货币市场的发展，勒索病毒勒索的内容也不单单围绕比特币。例如 2018 年 1 月首次出现的 Gandcrab家族勒索的就是更能隐藏用户信息达世币。

注意：由于勒索病毒已呈现产业化，同时大量的实例表明，现阶段存在大量的变种病毒，支付赎金后，并不提供真实有效的密钥，实际解密成功率极低。同时，存在人为投毒后，冒以专家身份主动联系代付解密的情况，故不建议直接支付解密。但当数据十分重要且上述其他方法都无法恢复，最终经过综合评判，确定需要支付赎金以尝试解密时，也建议听取安全专家或警方人员的建议以及综合判断，谨慎处置。

### 五 重装系统

当使用上述方法恢复数据后或不需要解密文件，原本的中毒主机都需要重装系统后再使用。确保主机上没有可用数据后进行格式化并重装系统，格式化是保证不会有残余的病毒文件，当格式化之后将无法再进行数据恢复。重装系统后要打好补丁，软件应确保使用最新版本或打好补丁，避免漏洞被利用。口令也应符合上文中提到过的强口令要求。

## 第四章 基础防护措施及建议

很多勒索病毒的落地并不一定经过长时间复杂的攻击过程，可能就是源于一封垃圾邮件，所以一定不能忽略很多基础措施。

### 一 增强安全意识

除了漏洞利用与暴力破解外，最多的感染勒索病毒的原因就是利用网页挂马、垃圾电子邮件与捆绑恶意程序，所以日常使用网络时要有以下安全意识：

* 不访问色情、博彩等等不良信息网站，这些网站通常会引导访客下载病毒文件或发动钓鱼、挂马攻击。
* 不轻易下载陌生人发来的邮件附件，不点击陌生邮件中的链接。
* 不随意使用陌生 U 盘、移动硬盘等外设，使用时切勿关闭防护软件比如Windows 自带的 Windows defender，避免拷入恶意文件。
* 不轻易运行 bat、vbs、vbe、js、jse、wsh、wsf 等后缀的脚本文件和 exe可执行程序，不轻易解压不明压缩文件。陌生文件下载运行前可使用杀毒软件进行查杀，避免感染病毒。
* 定期查杀病毒，清理可疑文件，备份数据。

### 二 增加口令强度

勒索病毒最常用的攻击方式是利用永恒之蓝漏洞和爆破 RDP（远程桌面协议）等服务弱口令，为应对后者应立即修改系统和各应用（MySQL、SQLServer 等）的弱口令、空口令、多台服务器共用的重复口令。强密码长度不少于 8 个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名、邮箱名等。

可以通过密码策略让电脑使用者必须设置一个复杂密码，Windows 操作系统可以通过配置密码策略来实现。



### 三 修复系统漏洞

在微软发布高危漏洞公告后应尽快修复系统存在的漏洞，避免被恶意利用。可关注微软安全响应中心（https://docs.microsoft.com/zh-cn/security-updates/）或浙江大学信息技术中心（http://itc.zju.edu.cn/7943/list.htm）发布的漏洞预警公告。

如果不能及时关注响应这些漏洞信息，应借助安全软件完成漏洞修复。尤其当单位有庞大数量的主机需要管理时，应选择合适的安全管理系统完成修复漏洞的工作。

### 四 修复应用漏洞

勒索病毒利用的漏洞工具除了广为人知的永恒之蓝系列，新型的勒索病毒一般还携带许多 Web 应用漏洞利用工具，比如 JBoss 反序列化漏洞(CVE-2013-4810)、Tomcat任意文件上传漏洞（CVE-2017-12615）、Tomcat web 管理后台弱口令爆破、ApacheStruts2 远程代码执行漏洞 S2-045 等。所以应定期检测并修复漏洞，最好是能够及时更新版本。

### 五 端口管理

除了必要的业务需求应关闭 135、139、445、3389 等端口，即使需要对部分机器开放，也应通过防火墙配置、安全软件隔离、准入管理等手段，仅限部分机器可访问。

感谢杭州安恒信息技术股份有限公司的支持