勒索病毒 防范科普手册

勒索病毒全产业链图

您遭遇的勒索攻击一定不是偶然

勒索产业链的发展会使得黑客团伙活动
更加频繁、更加组织化和目标化

第一步：
勒索病毒制作

第二步：
勒索病毒买卖

第三步：
勒索病毒传播

第四步：
勒索病毒攻击

第五步：
勒索病毒解密

目录
contents

勒索病毒简介 1

勒索产业链RaaS 4

勒索病毒攻击趋势 5

典型勒索组织 6

勒索病毒防范16个小技巧 8

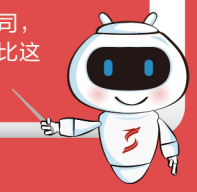
勒索病毒简介

什么是勒索病毒?

简单来说

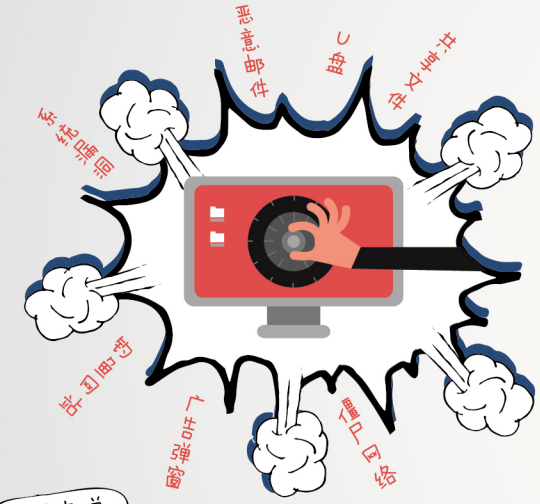
勒索病毒就像是把你家的门窗全部锁住，然后在门上堂而皇之地贴上告示，告诉你如果不交钱拿到钥匙，就回不了自己的家。

不一样的是，如果你家被锁住了，你可以找开锁公司，或者直接破门而入，很轻松，而破解勒索病毒，要比这难上千万倍。



勒索病毒是怎样运行的?

勒索病毒的运行，主要分为下面三个步骤:

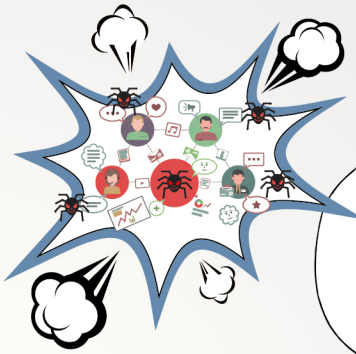


第1步：攻击！

简单来说

攻击的手法五花八门，系统漏洞、恶意邮件、U盘、共享文件、钓鱼网站、广告弹窗、僵尸网络等都可能成为病毒传播的载体。目前，勒索病毒的主要入侵方式是远程桌面入侵，其次是共享文件夹被加密。主要攻击手段有弱口令攻击、横向渗透、钓鱼邮件、利用系统漏洞或应用软件漏洞攻击、网站挂马攻击、破解软件与激活工具、僵尸网络和供应链攻击等。

在这些攻击手段中，利用系统漏洞是最为常见的，它的最大特点是被动性。病毒会自动扫描网络中存在系统漏洞的主机，只要没有安装补丁，即使没有点开邮件、没有访问恶意网站，也可能被攻击。



第2步：扩散！

简单来说

在感染某一台主机后，病毒往往不急着开始“工作”，而是尽可能利用各种手法来自我复制，进行不同文件、不同主机间的相互感染，最终将病毒扩散到整个局域网。等病毒爆发时，往往就是整个单位、整个企业的电脑全部被锁。

第3步：窃取！

简单来说

完成了“热身”，病毒开始“大显身手”。一方面，它会通过格式篡改的方式，加密电脑中的文档、图片等文件；另一方面，它会将感染电脑上的机密文件上传到黑客服务器上。

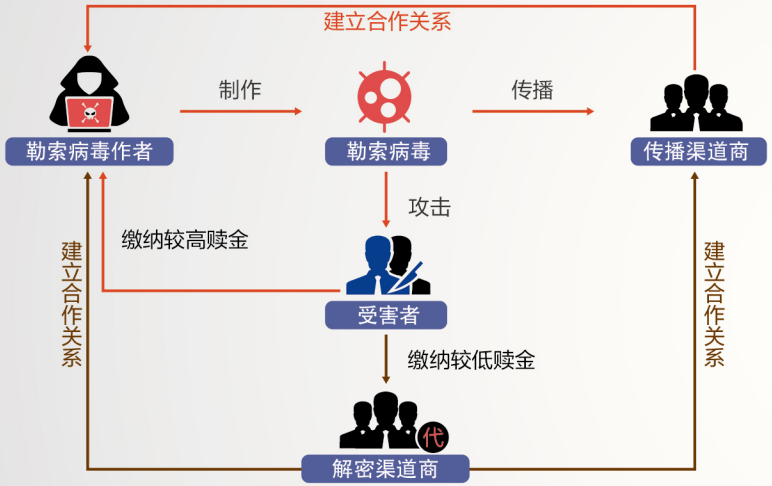
第4步：勒索！

简单来说

在成功加密、窃取文件之后，病毒会在桌面或醒目位置生成一个提醒用户文件已被锁定/窃取，指引其交赎金的文件。

对于一些知名企业，如果不及时交赎金，黑客会在暗网陆续公开窃得的机密文件，以实现施压的目的。

勒索产业链RaaS



勒索软件即服务（RaaS）借鉴了软件即服务（SaaS）模型，黑客为网络攻击者提供工具和基础设施，从他们以盗取的文件为质押所获取的利益中分成。

这种基于订阅的恶意模型使新手网络犯罪分子也能够毫不费力地发起勒索软件攻击。您可以在市场上找到各种RaaS软件包，这些软件包可减少对恶意软件进行编码的需求。

因此，网络犯罪分子即便不了解如何创建勒索软件，也能够轻松地使用它。一旦攻击成功，就将赎金分配给服务提供商、编码者和入侵网络的黑客以及勒索软件会员。

勒索病毒 防范科普手册

勒索病毒攻击趋势

典型勒索组织

REvil

REvil是目前最老练的勒索组织，于2019年5月24日首次被发现，具有成熟的攻击与运营能力，曾声称可以控制导弹发射系统，并攻击了如核设施合作商等多个重要的机构和组织。REvil被称为是GandCrab的“接班人”，是目前最大的RaaS勒索软件运营商之一。

BlackMatter

BlackMatter成立于2021年7月，是目前最受关注的新兴勒索团伙，被认为是Darkside和REvil的继任者。Black-Matter将瞄准符合以下要求的目标：
1.收入超过1亿美元
2.网络中有500-15000台主机
3.位于美国、英国、加拿大或澳大利亚

Darkside

Darkside于2020年8月以勒索软件即服务（RaaS）形式开始运营，是美国管道勒索事件的罪魁祸首。该组织会在攻击前对目标进行信息收集，以评估企业的财力制定具体的赎金数额。Darkside在成立不到一年的时间里感染了上百个组织，收到的平均赎金为190万美元，总收入高达9000万美元。

Avaddon

Avaddon勒索软件团伙是来自俄罗斯的黑客组织，在2020年6月2日首现于俄罗斯黑客论坛，所开发的Avaddon勒索软件除了供自身使用之外，也通过提供勒索即服务（RaaS）谋求外部合作以获取更大的利益，例如与Phorpiex僵尸网络合作进行大范围感染传播，勒索的平均赎金要求约为60万美元。

Babuk

2021年加入的新兴勒索团伙，目标是窃取高级机密类文件。其使用的勒索软件Babuk Locker于2021年1月被首次披露，作为今年新出现的勒索软件，该运营商不断地对Babuk Locker进行版本更新，并增加了针对敲诈勒索而设计的数据提取功能。Babuk勒索软件曾多次攻击国外著名的组织或企业。

Conti

Conti勒索软件在2019年12月首次被发现，并在2020年7月作为个人的勒索软件即服务（RaaS）开始运营，是目前攻击事件最多产的勒索软件团伙，被认为是流行的Ryuk勒索软件家族的变种。Conti勒索软件团伙通过多种流行的恶意软件传播，包括Trickbot/Emotet和BazarLoader。

勒索病毒防范16个小技巧

增强安全意识

1. 不访问色情、博彩等不良信息网站，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。
2. 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。
3. 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。
4. 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文件威胁分析平台进行检测（http://ti.dbappsecurity.com.cn:8080/），避免感染病毒。
5. 定期查杀病毒，清理可疑文件，备份数据。

增加口令强度

6. 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。
7. 设置强密码，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。
8. Windows操作系统可以通过配置密码策略来实现。

修复漏洞

9. 及时修复系统漏洞或借助EDR等安全软件完成漏洞修复，避免被恶意利用。
10. 当需要管理庞大数量的主机时，应选择合适的安全管理系统完成漏洞修复工作。
11. 应定期检测并修复应用漏洞，最好是能够及时更新版本。

端口管理

12. 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，也应做出配置仅限部分机器可访问。
13. 通过防火墙配置、安全软件隔离或准入管理。

应急方法

14. 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。
15. 逻辑隔离：访问控制、关闭端口、修改密码。
16. 排查其他主机：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。

无论是个人还是企业，一旦被勒索软件敲诈，都不建议支付赎金！首先，支付赎金变相鼓励了勒索攻击行为，其次，支付赎金也可能会留下后遗症，甚至根本解决不了问题。建议优先尝试通过备份、数据恢复、数据修复等手段挽回部分损失，比如部分勒索病毒只加密文件头部数据，对于某些类型的文件（如数据库文件），就可以尝试通过数据修复手段来修复被加密文件。总的来说，勒索病毒重在防范，建议部署安恒edr等相关安全防护产品。

事后恢复

备份还原

通常来说，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。

解密工具恢复

通常的解密工具是通过已公开的密钥来解密，来源途径包括破解勒索程序得到，勒索者对受害人感到愧疚、同情等极端情况而公开密钥，执法机构获得勒索者的服务器上存储着密钥且执法机构选择公开。此外，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。

需要注意的是：使用解密工具之前，务必要备份加密的文件，防止解密不成功导致无法恢复数据。

随堂小测试

火眼金睛，小心上当

1. 勒索病毒是恶意程序吗？
   A. 是　B. 不是
2. 勒索病毒的攻击方式有哪些？
   A. 弱口令攻击　B. 钓鱼邮件　C. 利用系统漏洞攻击
   D. 网站挂马攻击　E. 以上都是
3. 勒索病毒只针对企业？
   A. 是　B. 不是
4. 勒索攻击是不是离我们很遥远？
   A. 是　B. 不是
5. 当被勒索了，断网就行了？
   A. 是　B. 不是
6. 被勒索了第一件事，交赎金？
   A. 是　B. 不是
7. 如何防范被勒索病毒入侵？
   A. 提高安全意识　B. 增强密码安全　C. 及时修复漏洞
   D. 端口管理　E. 部署安恒edr产品　F. 以上都是
8. 如何理解RaaS？
   A. 勒索软件即服务
   B. 黑客为网络攻击者提供工具和基础设施，从他们以盗取的文件为质押所获取的利益中分成
   C. 以上都是

答案：AEBBBBFC