文件勒索

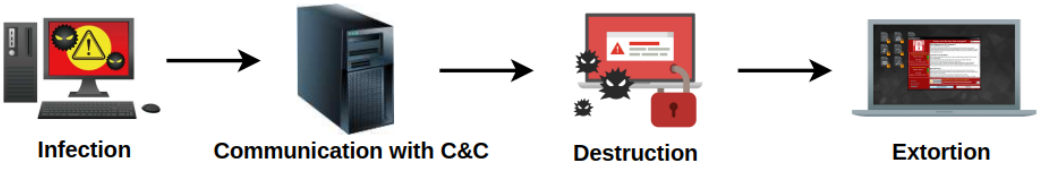
▼ 定义

勒索软件是恶意软件的一个子集，旨在限制对系统或数据的访问，直到攻击者请求的赎金金额得到满足。

▼ 打击勒索软件的挑战性

- 勒索软件通常依赖于强大的加密，由于多种开源实现，这种加密非常容易适应
- 受益于现代恶意软件所使用的常见规避技术（即代码混淆、加密通信、域生成算法（DGA）或快速通量以动态转移/生成域名等
- 经常使用受害者平台提供的应用程序编程接口（API）来执行恶意操作，这使得很难区分勒索软件和良性应用程序
- 使用 TOR（洋葱路由网络）等匿名通信以及加密货币等伪匿名和不受监管的支付技术，这些技术可以帮助攻击者在不轻易泄露其身份的情况下获得报酬

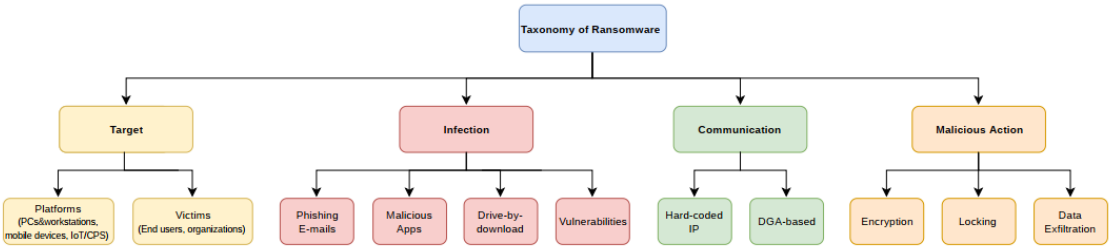
▼ 勒索软件攻击阶段



- **感染**：在此阶段，勒索软件被传递到受害者系统（例如 PC/工作站、移动设备、IoT/CPS）设备等）。恶意行为者利用多种感染媒介来实现勒索软件的传播。
- **与 C&C（Command and Control Server） 服务器通信：**感染后，勒索软件连接到命令与控制 (C&C) 服务器，与攻击者交换关键信息（即加密密钥、目标系统信息）。同时也存在一些不执行任何通信的勒索攻击。
- **破坏：**在此阶段，勒索软件会执行实际的恶意操作，例如加密文件或锁定系统，以防止受害者访问其文件或系统。
- **勒索：**最后，勒索软件通过显示勒索字条告知受害者有关攻击的信息。勒索信披露了攻击细节和付款说明。

▼ 勒索软件的分类

根据勒索软件的目标、感染方式、C&C 通信和恶意行为（破坏技术）对勒索软件进行分类



▼ 根据目标分类

根据受害者：

- 终端用户（个人设备）
- 组织（政府、医院、企业和学校）

根据平台：

- PCs/workstations（Windows、macOS、Linux）
- Mobile Devices
- IoT/CPS（物联网/网络物理系统） Devices

▼ 根据感染方式分类

- **恶意电子邮件：**攻击者向受害者发送垃圾邮件，其中的附件包含勒索软件。此类垃圾邮件活动可以使用僵尸网络进行分发。
- **短信或即时消息 (IM)：**通常是移动勒索，在此类感染中，攻击者会向受害者发送短信或即时消息，导致受害者浏览恶意网站，将勒索软件下载到其平台上
- **恶意应用程序：**开发和部署包含伪装成良性应用程序的勒索软件的移动应用程序
- **偷渡式下载：**当用户在不知情的情况下访问受感染的网站或点击恶意广告，然后在不知情的情况下下载并安装恶意软件
- **漏洞：**平台中的漏洞，例如操作系统、浏览器或软件中的漏洞

▼ 根据C&C Communication分类

命令与控制（C&C）服务器是攻击者域中的远程服务器。攻击者经常使用 C&C 服务器来通信和配置恶意软件。

在勒索软件中，C&C 服务器主要由加密勒索软件系列用来发送或接收用于加密受害者的文件和/应用程序的加密密钥。

勒索软件主要使用 HTTP 或 HTTPS 协议来连接到 C&C 服务器。

- **硬编码 IP/域：**勒索软件系列可以将硬编码 IP 地址或域嵌入到其二进制文件中，以设置与 C&C 服务器的连接。在这种方法中，IP 地址或域对于每次攻击都保持相同，并为攻击者提供可靠的通信。
- **动态域：**勒索软件系列使用域生成算法 (DGA) 来动态联系 C&C 服务器。这些算法通过快速变化/生成/转移域名，为每次通信的服务器提供唯一的域名。这种形式的通信有助于针对勒索软件进行更稳健的通信，并且防火墙无法轻松检测到它。

▼ 按恶意行为分类

按恶意行为分类可分为加密勒索软件和Locker 勒索软件

加密（Encrypting）：

- **加密勒索软件：**此类勒索软件会对受害者文件进行加密，删除或覆盖原始文件，并要求支付赎金才能解密文件。

▼ **加密技术：**勒索软件可以采用对称、非对称或混合加密技术。

- **对称密钥加密：**

对称密钥加密仅使用一个密钥来加密和解密文件。与非对称密钥加密相比，它需要更少的资源来加密大量文件，因此勒索软件可以更快地加密受害者文件。加密密钥要么在目标系统上生成，要么嵌入到勒索软件二进制文件中。加密后，勒索软件通过C&C通信将加密密钥发送给攻击者。、

- **非对称密钥加密**

在这种方法中，勒索软件利用一对密钥（即公钥和私钥）来加密和解密文件。虽然加密大量文件的效率不高，但非对称密钥加密解决了密钥保护问题，因为加密和解密需要单独的密钥。RSA (Rivest–Shamir–Adleman) 是最常用的非对称密钥算法。

- **混合加密：**

攻击者在混合加密中结合了两种加密技术的优点。在这方面，勒索软件首先使用对称密钥加密来快速加密受害者的文件。之后用攻击者的公钥加密所使用的对称密钥。通常，攻击者的公钥嵌入在勒索软件二进制文件中，因此这些变体在攻击过程中**不需要连接到 C&C 服务器。**

▼ **破坏行为：**

- 就地加密文件，用加密版本覆盖原始文件
- 修改主文件表（MFT）删除受害者的原始文件，并创建包含原始文件加密版本的新文件
- 删除 Windows 卷影副本，消除从文件系统快照恢复文件的机会，

锁定（Locking）：

- **Locker 勒索软件：**此类勒索软件通过锁定屏幕或浏览器来阻止受害者访问其系统，并要求支付赎金来解锁系统。与加密勒索软件不同，它不会加密系统或用户数据

Locker 勒索软件系列锁定系统组件以防止受害者访问。根据锁定目标，锁定勒索软件可分为三类：**屏幕锁定**、**浏览器锁定**和**主引导记录（MBR）锁定**。

数据泄露

窃取受害者的有价值信息（例如信用卡信息、公司文档、个人文件等）。事实上，一些勒索软件家族要求支付两笔赎金：其中一笔付款用于发送解密文件的密钥，另一笔付款用于防止发布被盗信息。

勒索软件防御研究

▼ 勒索软件分析：包括了解勒索软件的行为和/或特征的活动

- 静态分析：旨在通过从样本中提取结构信息而不实际运行。分解样本二进制文件并提取有关样本结构/内容的信息。由于不运行样品，静态分析通常快速且安全。然而，恶意软件作者采用隐藏（即混淆、多态性、加密）和反反汇编技术来使静态分析工作变得更加困难，并规避使用通过静态分析获得的结构特征的防御方案。
- 动态分析：包括运行样本并观察行为以确定样本是否是勒索软件。动态分析是通过在隔离环境（即沙箱）内运行样本来执行的，以避免分析样本可能造成的损坏，因此在时间和资源方面成本高昂。
- 静态分析和动态分析各有优缺点，通常在混合分析中使用这两种方法

▼ 勒索软件检测

- **基于黑名单：**系统使用已知勒索软件系列使用的**恶意域名或 IP 地址列表**来检测勒索软件。
- **基于规则：**系统**使用分析功能构建的规则**来检测勒索软件。规则可以是与恶意软件检测引擎兼容的规则、恶意分数或阈值。

- **基于统计：**系统使用表明样本是勒索软件的**特征统计**来检测勒索软件。
- **基于形式化方法：**系统使用可以区分恶意和良性模式的**形式化模型**来检测勒索软件。
- **基于信息论：**系统使用**信息论方法（例如熵）**检测勒索软件。
- **基于机器学习：**系统通过使用一组分析功能构建的**机器学习模型**来检测勒索软件。基于机器学习的勒索软件检测系统使用**结构特征/行为特征**。研究人员通过对勒索软件二进制文件进行静态分析来获得结构特征来检测勒索软件二进制结构中的模式。另一方面，通过勒索软件二进制文件的动态分析获得行为特征来检测勒索软件二进制文件的行为模式。

▼ 勒索软件恢复

勒索软件造成的破坏可以通过三种不同的方式恢复：恢复密钥、通过硬件恢复文件或通过云备份恢复文件。

- **密钥恢复：**通过挂钩加密 API 来捕获加密密钥并解密受害者文件。仅对调用相应加密API进行加密的勒索软件家族有效。
- **通过硬件恢复文件：**利用存储硬件（即SSD）的特性来恢复受害者的加密文件。基于 NAND 的 SSD 具有异地更新功能，可以保留已删除数据的先前版本，直到垃圾收集器将其删除。
- **通过云备份恢复文件：**利用云环境进行备份恢复文件。它允许管理员在勒索软件事件发生后通过分析日志来恢复文件。它还旨在通过使用秘密共享密钥进行加密来保护存储在客户端的用户的云访问凭据。