# 一、定义

勒索病毒一种特殊的恶意软件，通过对系统文件或是锁定系统的方式要求受害者支付赎金来取回对电脑或是文档的控制权限。病毒的一般传播途径为通过邮件、网站、USB等方式欺骗受害者下载执行，或者结合一些漏洞的攻击在网络世界中传播。

# 二、病毒历史

最早的勒索病毒是1989年的"AIDS" Trojan病毒，由Joseph Popp制作。该病毒使得受害者的某個軟體已經結束了授权使用，並且加密磁碟上的档案，要求缴纳出189美元的费用給PC Cyborg Corporation以解除锁定。但是该病毒采用的是对称加密密钥，密钥保存在病毒样本中，所以通过获取密钥就可以解密文件。1996年由Adam L. Young和Moti Yung所提出的在Macintosh SE/30电脑上使用[RSA](https://zh.wikipedia.org/wiki/RSA%25E5%258A%25A0%25E5%25AF%2586%25E6%25BC%2594%25E7%25AE%2597%25E6%25B3%2595)及[TEA](https://zh.wikipedia.org/wiki/%25E5%25BE%25AE%25E5%259E%258B%25E5%258A%25A0%25E5%25AF%2586%25E7%25AE%2597%25E6%25B3%2595)演算法加密资料，通过对称密码和非对称密码的结合使用，保证了加密密钥的安全性，可以保证受害者必须支付赎金来解密文件。

"AIDS" Trojan

在2006年，勒索病毒开始运用更为复杂的RSA加密手段，加长密钥的長度，像是Gpcode、TROJ.RANSOM.A、Archiveus、Krotten、Cryzip、MayArchive等病毒。例如在2006年6月發現的Gpcode.AG使用了660位的RSA共钥。

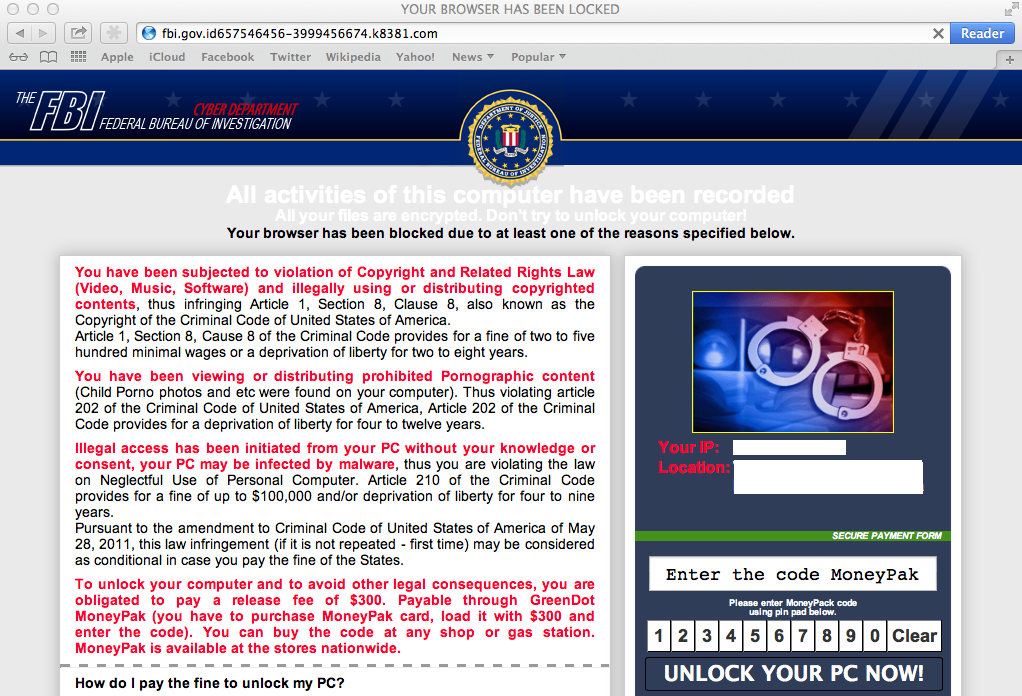
2008年6月，发现了该病毒的新变种Gpcode.AK。该变种使用了1024位元的RSA公钥，在不使用分散式计算的情況下，破解该密钥对单一的电脑来说是不可能的。

2017年5月，勒索软件[WannaCry](https://zh.wikipedia.org/wiki/WannaCry)大规模爆发，据报道，至少有99个国家的其他目标在同一时间遭到WanaCrypt0r 2.0的攻击。[俄罗斯联邦内务部](https://zh.wikipedia.org/wiki/%25E4%25BF%2584%25E7%25BD%2597%25E6%2596%25AF%25E8%2581%2594%25E9%2582%25A6%25E5%2586%2585%25E5%258A%25A1%25E9%2583%25A8)、俄罗斯电信公司MegaFon共有超过1000台计算机受到感染。中国教育网相连的中国大陆高校也出现大规模的感染，感染甚至波及到了[公安机关](https://zh.wikipedia.org/wiki/%25E5%2585%25AC%25E5%25AE%2589%25E6%259C%25BA%25E5%2585%25B3)使用的内网，使得河南省洛阳市的公安系统遭到破坏。国家互联网应急中心亦发布通报。

# 三、案例

## 3.1 Reveton

2012年，一款叫做Reveton的勒索病毒开始发布。该病毒基于Citadel木马病毒，而病毒的有效数据会显示成來自执法机关的讯息（因此，此类病毒又被称为police Trojan或cop Trojan）。该病毒会宣称在计算机上查获非法活动，例如盗版软件和色情视频，並且提示受害者使用Ukash 或Paysafecard等匿名货币进行缴纳解锁。



Reveton

## 3.2 CryptoLocker

2013年9月，加密性勒索病毒以CryptoLocker名称出现。该病毒使用2048位元的RSA加密密钥，並將其回传至主控病毒行动的服务器。CryptoLocker威胁受害者，若不以[比特币](https://zh.wikipedia.org/wiki/%25E6%25AF%2594%25E7%2589%25B9%25E5%25B8%2581)或付费卡在三天內缴款，就会将加密文档删除。由于运用了超长的加密密钥，因此一般认为对加密的文档无法进行复原，除非获取私钥。

## CryptoLocker

## 3.3 RSA4096

最初出现于2015年，该病毒使用公钥加密，付款要求受害者利用比特币向暗网內的代理人购买，却不保证一定能给予私钥。该病毒有数种变种，大部分都尚未找到解決办法。某些变种会将档案的格式名称改变。唯一从攻击种得到恢复的方法，除了支付费用获取私钥，只有数据备份一种方式。

## RSA4096

## 3.4 WannaCrypt

# WannaCrypt是利用Windows系统漏洞进行侵入的一款勒索病毒，在2017年5月12日后全球超过230,000台计算机皆遭此病毒侵害，此病毒要求支付价值等同于300美元的比特币才可解密所有遭加密文件。受害者电脑大多数皆装载Windows 7系统，微软对此也发布了更新补丁。

# WannaCrypt

# 四、病毒原理分析

## 4.1 勒索病毒加密原理

# 要了解整个勒索病毒的原理，必须需要了解整个勒索病毒的加密过程，通过了解学习过程就可以解决为什么加密的方式几乎无法被破解，也可以让我们对核心数据的安全备份有更清晰的认识。

# 

# 

# 上图是勒索病毒的加密流程，一共分为三个方面：

# 1）客户端中了勒索病毒之后，通过RSA非对称加密算法生成共钥和私钥，私钥会传输给黑客的服务器端，为了防止网络数据包中被捕获私钥，因此在病毒中引入了内置公钥对生成的私钥进行了加密，这样保证了私钥可以安全的发送到服务器端，并通过RSA私钥进行解密。

# 2）受害者电脑端用AES对称加密生产密钥，对文档内容进行加密。

# 3）为了防止对称密钥被识别，用本地的随机的RSA共钥对AES密钥进行加密，结合加密后的密钥和加密后的文件生成一个加密文件。

## 4.2 演示勒索加解密过程

加密过程：

<https://github.com/leadsino/zl/blob/master/image/file_encrypt.gif> 演示

<https://github.com/leadsino/zl/blob/master/randsome/RSA%2BAES_encrypt.py> 加密脚本地址

解密过程：

<https://github.com/leadsino/zl/blob/master/image/file_decrypt.gif> 演示

<https://github.com/leadsino/zl/blob/master/randsome/RSA%2BAES_decrypt.py> 解密脚本地址

注意：脚本只能用于安全学习使用。

# 五、防御思路

1）根据勒索病毒的特性，对核心数据文件进行备份是最重要的事情，这样可以减少损失；

2）对于运维人员的接入端的控制，使用安全的客户端接入数据库，可以使用堡垒家做统一的接入。譬如去年11月发生的关于Oracle RushQL勒索病毒，就是破解的PLSQL工具中包含自动知行的存储过程导致的数据被加密；

3）禁止安装来路不明的软件，尤其是企业内部安全运维工程师的PC；

4）企业内部加强安全意识的培训，最好能演示中毒的过程以及危害，让员工提高安全意识。