题型有变化

计算分析题 4\*8

跟去年差不多

Ntfs考 data run 识别 簇号必考

结构

终止符

算

对着ppt做

Index 起始簇长度

Size 起始簇号

给 pe结构 属性 文件偏移 VA和FOA计算

VA算FOA

IDT表 比较难

多少dll 有多少个函数

栈结构

程序画结构

算字段在哪里

磁盘size \* 512

简答:

字写多一点

机制 课堂mooc问答题 填空题看下

勒索软件

堆，堆喷射

常规计算机病毒概念，分了很多类

病毒防御机制

漏洞类型，堆栈溢出 use after free

防御

（ 栈里放 cookies

GS DEP

Heap加校验什么的(记录)

Mooc里

）

8分题，起码三行

要点

综合题

两个代码题

12\*2

给汇编代码 恶意软件有关，分析功能属性，why

C代码 安全缺陷 怎么修补

最短最简单标准库函数

代码不超过四行0

极短

C++书上有

论述题

题干8行

针对国家软件监管 漏洞监管

中国漏洞管理条例

漏洞管理综述，自由发挥

要点

**0x00 Heap Spray（堆喷射）**

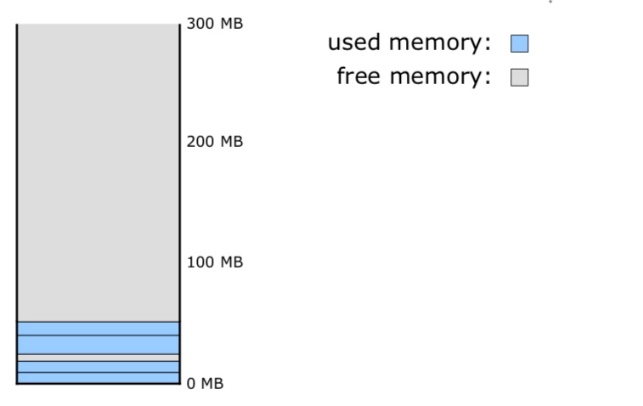
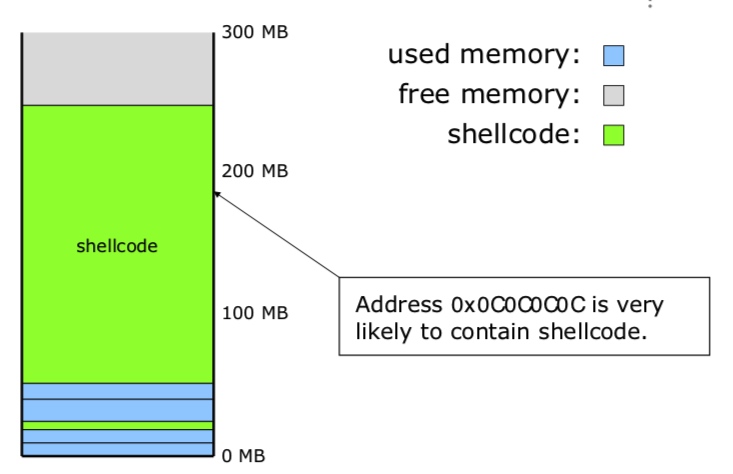
堆喷射是在 shellcode 的前面加上大量的slide code（跳板指令），组成一个注入代码段。然后向系统申请大量内存，并且反复用注入代码段来填充。这样就使得内存被大量的注入代码占据。然后通过结合其他漏洞控制程序流，使得程序执行到堆上，最终将导致shellcode的执行。

常见的slide code 有NOP指令，还有一些类NOP指令，比如0x0c,0x0d等。它们的共同特点都是不会影响shellcode的执行。

**0x01 Heap Spray原理**

**Q1 ： 为什么需要在shellcode前面加上silde code?**  
如果想要成功执行shellcode，必须要准确的跳转到shellcode的第一条指令开始执行，如果整个空间都被填充为shellcode，精确跳转到shellcode的第一条指令的几率反而很低。如果在shellcode前面加上很长一段slide code，那么只要跳转到slide code范围内的任意地址，最后都能执行shellcode。

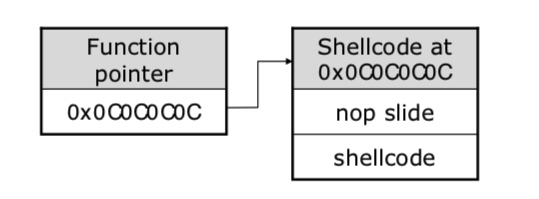
**Q2 ：为什么是 0x0c0c0c0c?**  
一是因为堆的分布不均衡（存在碎片），所以最先分配的一些堆块的地址可能是无规律的，但是如果大量的分配堆块的话，那么就会出现稳定的地址分布。也就是说内存中碎片过多，必须喷射到更高的地址才能使 exploit 更稳定。  
通常在申请的内存超过200M(0xc8000000 > 0x0c0c0c0c),0x0c0c0c0c被含有shellcode的内存片覆盖，只要slide code能够击中0x0c0c0c0c的位置，shellcode最后都能被执行。

正常情况下的堆布局：  
[](https://v1ckydxp.github.io/images/15637805830563.jpg)  
堆喷射后的堆布局：  
[](https://v1ckydxp.github.io/images/15637805995884.jpg)

**堆喷射攻击技术**

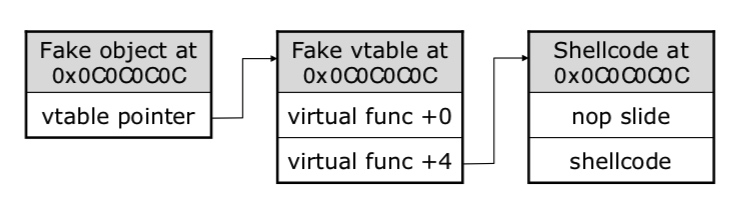
**1. 覆盖函数指针地址**

a. 申请200M内存，以sildecode+shellcode填充。  
b. 覆盖函数指针地址为0x0c0c0c0c  
c. 调用该函数的时候就会跳转到0x0c0c0c0c地址处，最后执行shellocde

[](https://v1ckydxp.github.io/images/15637811652656.jpg)

**2. 覆盖虚函数指针**

a. 申请200M内存，以sildecode+shellcode填充。这个时候选择的slidecode不能是0x90。如果用0x90来填充，则虚表里面全是0X90909090，程序会跳转到0X90909090处执行，会导致crash。  
b. 覆盖函数指针地址为0x0c0c0c0c  
c. 调用该函数的时候就会跳转到0x0c0c0c0c地址处，最后执行shellocde 。

[](https://v1ckydxp.github.io/images/15637811745883.jpg)

通过对数字签名进行篡改，可以使包含恶意代码的exe在被用户下载后成功安装并执行攻击。在程序安装到本地后，本次实验主要是通过对用户文件进行加密劫持。通过使用密码加密算法对用户文件进行加密以达到攻击目的。攻击时，扫描文件夹中的特定文件后缀，识别后对其进行加密。

现如今常见的勒索病毒经过几年的演变，勒索病毒攻击手法也有明显的变化，从最开始的单纯的“勒索”，发展到后面“勒索+窃密”，最近一些勒索病毒黑客组织还加入DDOS的方式，对受害者企业进行攻击，迫逼受害者交纳赎金。总结一些常见的勒索病毒攻击方式如下：

1、入侵：通过RDP爆破、SQL弱口令爆破、网络钓鱼、恶意电子邮件以及恶意附件投递，高危漏洞利用、无文件攻击等方式入侵。

2、扩散：黑客入侵一台主机后，会利用各种攻击手段，横向扩张，增加受控主机数量。

3、盗窃：黑客攻陷主机后，筛选最有价值的数据攻击对象，窃取数据，留置后门，安装远程控制软件，并将窃取到的数据上传到自己团队的服务器

4、勒索：下载一种或多种勒索病毒运行，瘫痪目标网络，留下勒索信件，在暗网发布失陷企业数据，实施勒索。

近期出现的勒索病毒主要攻击流程如下：

病毒作者自己生成一对椭圆曲线密钥对，分别称为主公钥（master public）和主私钥（master private），然后把主公钥写到病毒中，主私钥保存在作者自己的电脑上。病毒运行时，搜索硬盘中特定后缀名的文件（比如doc、xls、pdf等），每找到一个文件。首先采集文件创建时间、系统环境等信息，借助这些信息生成一个会话私钥（session private），然后根据会话私钥生成会话公钥（session public）。

使用会话私钥和主公钥，进行ECDH得到共享密钥（shared secret）；对共享密钥计算SHA-256摘要，得到AES密钥；使用AES密钥对文件进行加密并写回硬盘，同时向加密后的文件写入会话公钥；最后删掉原文件。

可以看到，硬盘上最后保存的只有病毒自带的主公钥，每一个文件的会话公钥，以及被加密的文件内容。想要解密，唯一的办法就是使用文件的会话公钥和病毒作者的主私钥进行ECDH，得到共享密钥。

**目录**

**1. 概述**

**2. 背景**

**3. 勒索软件发展历程**

3.1PC Cyborg(第一款勒索软件)

3.2 非对称加密

3.3 加密货币兴起

3.4 RaaS

3.5 双重破坏

**4.勒索软件TTPS**

4.1 传播

4.2 横向移动

4.3 扩大影响（上篇结束于此）

**5.常见勒索软件**

5.1 Sodinokibi/Revil（下篇开始于此）

5.2 Crysis/Dharma

5.3 Globelmposter

5.4 Buran

5.5 NetWalker

**6. 勒索软件的趋势**

**7. 勒索软件响应措施**

7.1 感染迹象

7.2 应急处理

7.3 加密数据处理

**8. 日常防范**

**9. 附录**

**1、概述**

信息安全 (Information Security)，意为保护信息及信息系统不受侵害。主要保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。从层面的概念来看，计算机硬件可以看作是物理层面，软件可以看做是运行层面，然后就是数据层面。从属性的概念来看，破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。随着当代网络技术的高速发展和人们对所面临问题理解程度的日益加深，信息安全已是当今众多互联网领域的突出问题之一。

在众多信息安全风险中，居首位者当属网络攻击。无论是公司还是组织，都随时可能成为网络攻击的对象。而每年网络犯罪所带来的经济损失也与日俱增。综合以往，我们从攻击对象和利益最大化的角度来看，影响最大也最恶劣的当属勒索软件攻击。一旦公司、企业的资产如数据库、服务器等被加密甚至被破坏，所造成的损失不可估量。如果是公共设施和服务被勒索，如医院、交通部门被窃密、勒索，不仅会对我们的生活造成影响，甚至可能威胁到我们的生命。

近期，我们整合流行的勒索家族、梳理历史上著名的攻击事件，对勒索软件的发展历史进行回顾，对勒索软件的加密流程和传播途径进行深入探讨，对勒索软件今后的发展趋势进行畅想，并对被勒索攻击后应急处置流程进行分享，使读者对勒索攻击事件有新的整体把握，更好地应对此类网络攻击。

**2、背景**

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）。勒索软件与其他病毒最大的不同在于攻击手法和中毒方式，部分勒索软件仅是单纯地将受害者的电脑锁起来，而也有部分勒索软件会系统性地加密受害者硬盘上的文件。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解密文件。

勒索软件通常透过木马病毒的形式传播，将自身伪装为看似无害的文件，如利用邮件等社会工程学方法欺骗受害者点击链接下载，另外也可能与许多其他蠕虫病毒一样利用软件的漏洞在联网的电脑间传播。

勒索攻击事件频繁发生，且在数量上逐年增多。勒索软件如此盛行的背后是巨大利益的驱动。2020年，全球因勒索软件造成的总损失高达25万亿美元，高额的收益让更多的犯罪者趋之若鹜，而以往诸如 GandCrab 勒索病毒，不仅高调宣布仅仅一年就获得超过20亿美元的赎金，并且已成功兑现。诸如此类事件的推波助澜，加剧了勒索事件的爆发。

另一方面，即使没有任何编程经验的人借助 RaaS 平台也可以制作分发勒索病毒，这也让更多犯罪者铤而走险。

另外，勒索软件一般采用加密货币进行交易，加密货币由于其本身的特殊性，很难被第三方监管，更难以追踪和溯源，导致执法人员很难抓到犯罪者。

从1989年历史上已知的第1款勒索软件 PC Cyborg 出现到现在的广泛流行，勒索软件经历了漫长的发展历程。从非对称加密算法的应用，加密货币的兴起，到勒索软件即服务（Raas， Ransomware as a service）概念和双重破坏技术的出现，勒索软件在技术和理论层面不断革新，使其在当前仍具有强劲的发展势头和极大的破坏力。

**3、勒索软件发展历程**

**3.1 PC Cyborg**（第一款勒索软件）

时间追溯到1989年，当时大多数人并没有接触过电脑，并且信息传输也是通过软盘进行传递。这时一位哈佛大学博士学位的生物学家约瑟夫·波普 （Joseph Popp） 开发了一款软件，并且他向世界卫生组织艾滋病会议的参加者分发了20,000张受到感染的磁盘，并且以"艾滋病信息-入门软盘"命名。当软盘被插入电脑，就会显示以下消息：



该勒索信息要求用户必须在巴拿马的邮政邮箱向 PC Cyborg Corporation 发送189美元，以解锁访问权限。这就是已知的历史上第一款勒索病毒，"AIDS" 木马，也被称为 PC Cyborg。

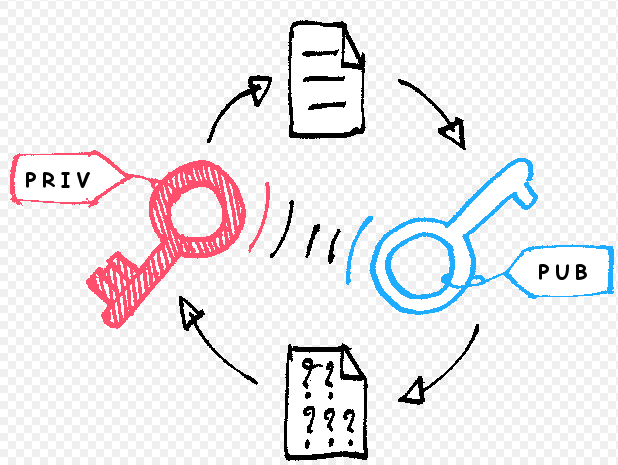
从原理上来讲，该病毒通过替换受害者计算机上的 Autoexec.bat 文件，在计算机每次启动时运行，一旦运行次数达到90，该病毒将会隐藏目录并利用简单的对称加密技术加密 C 盘的文件。虽然现在看来该软件无论是复杂程度还是加密算法都不值一提，但是它却象征着计算机犯罪的一个新分支——勒索软件的兴起。

**3.2 非对称加密**

All knowledge is, in the final analysis, history.  All sciences are, in the abstract,mathematics. All methods of acquiring knowledge are, essentially, throughstatistics.

—— C. R. Rao，数学家、统计学家（在终极的分析中，一切知识都是历史；在抽象的意义下，一切科学都是数学；在理性的基础上，所有的判断都是统计学）。

公开密钥密码学（英语：Public-key Cryptography）也称非对称式密码学（英语：Asymmetric Cryptography）是密码学的一种算法，它需要两个密钥：一个是公开密钥，另一个是私有密钥；公钥用作加密，私钥则用作解密。使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。公钥可以公开，可任意向外发布；私钥不可以公开，必须由用户自行严格秘密保管。



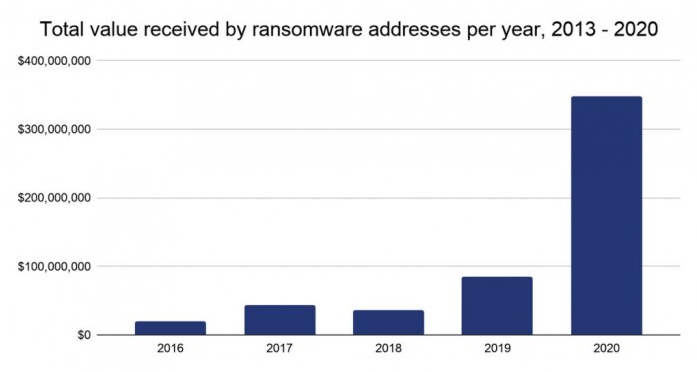
1996年，Adam L. Young 和 Moti M. Yung 两个密码学家发出警告，非对称加密算法将会用于勒索事件。十年之后，也就是2006年，做为第一个利用非对称加密(RSA)手法加密的恶意家族 Archiveus 发布。该病毒会对文档目录进行加密，并要求受害者必须在特定的 Web 站点上购买商品才能获得用于解密文件的密码。之后出现的 Krotten 、GPcode 和 Cryzip、等勒索软件也开始使用非对称加密算法进行文件加密。即使到了现在，假如受害者被一个使用2048位RSA加密算法的勒索软件加密文件，在不知道私钥的情况下，利用当前世界上最大、 最好的超级计算机进行暴力破解，需要的时间也长达80年。因此如果一旦文件被加密，在当前计算机计算能力有限的情况下，基本不可能无损解密数据。要么舍弃数据，要么交钱解密，无法自行解密的二选一窘境下，勒索的成功率大大提高。

**3.3 加密货币兴起**

2008年，以比特币为首的加密货币进入历史的舞台，因为其独特的特性引起攻击者的关注，例如比特币所具有的 POW 共识机制和双重的 sha256 区块哈希算法保证了绝对的去中心化、匿名和隐私等特性，另外根据 Coin Center 研究部主任 Peter Van Valkenburgh 的观点：作为一种电子货币，很容易开发出自动要求付款的软件。黑客能够轻松地查看公共区块链以验证受害者是否已经付款，并且可以在收到付款的同时自动执行将受害者所需要的文件或者密钥发送给受害者的操作，这些特性导致加密货币成为在勒索事件的首选货币。



2011年开始，使用加密货币进行交易的勒索软件开始疯狂增长，基本每个季度的勒索样本数量都在成倍的增加。截至到现在，根据区块链分析公司最新的统计报告，2020年勒索软件支付的赎金占加密货币总交易金额的7%左右。同比相较于2019年，这一比例增长了311%。



基于加密货币的匿名性和隐私性，导致很难被第三方进行监管，相关执法部门也几乎不太可能溯源到发动勒索攻击者的真实身份。在很长一段时间之内，勒索软件和加密货币还会保持紧密联系，并且不会有很大改善。

**3.4 RaaS**

2015年，为了寻求勒索软件收益的最大化，攻击者创建了一种全新的服务模式，勒索软件即服务 (RaaS) ，该模式借鉴软件即服务（SaaS）的模型。

勒索软件即服务是一个恶意软件销售商-客户通过订阅模式进行盈利的模型。首先犯罪分子编写完成勒索软件之后，通过类似会员的方式将其出售或出租给意图发动攻击的客户或者想要加盟进行分成的分销商，并且提供有关如何使用该软件发动勒索攻击的技术知识和相关步骤的教程，甚至提供可视化软件进行实时监控查看当前攻击状态。这种模型犯罪分子通过不同的"客户"可以轻松攻击那些自己无法接触到的新的受害者，扩大收益。一旦攻击成功，其赎金会按照一定比例分成给销售商、编码者、攻击者等各方。相比之前的单一模式的攻击，这种多层代理的攻击模型让勒索软件更容易传播。即使是攻击者自身没有高超的技术或者昂贵的设备，也可以通过低价购买和下载勒索软件，轻而易举的发起勒索攻击。

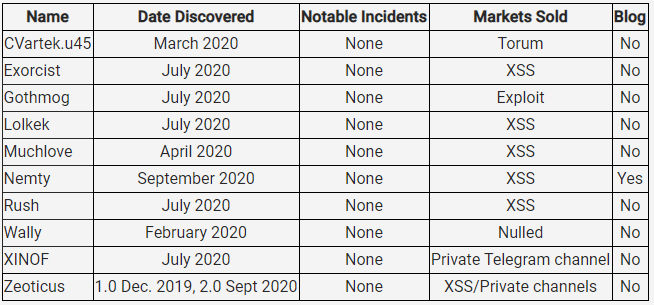
2015年中期，第一个 RaaS 服务在暗网中悄然诞生：



Tox 勒索软件套件作为 RaaS 服务开始投入销售，该工具包提供各种反分析反检测功能。攻击者只需要提供几个自定义字段就可以开发出一个自定义的勒索软件，其易用性之高，让不同水平的攻击者瞬间涌入勒索事件的行列。

虽然 Tox 勒索软件套件不久就被封禁，但是不同的 RaaS 服务如雨后春笋般层出不穷，勒索攻击的事件进一步增多。

2020年新型Raas平台：

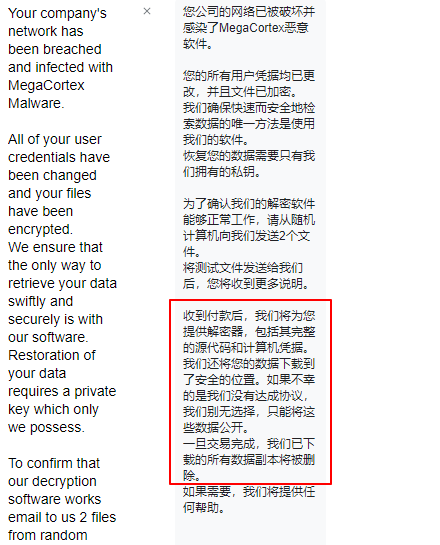


**3.5 双重破坏**

窃密软件一般具有隐匿性，通过执行窃取受害者密码或者文件信息。而勒索软件具有暴力性，会直接加密用户文件。当这两种不同类型家族发生碰撞，会发生什么样的火花。

当前，勒索软件日益猖狂的同时，人们的防范意识也越来越强。即时备份成为越来越多的企业、公司的标准操作。即使被勒索，只要恢复备份即可。当用户认为备份数据之后就可以高枕无忧时，一种新的勒索形式让人们再次陷入被动泥潭。

2019年初， Megacortex 勒索病毒借助 Emotet 僵尸网络进行传播。在留下的勒索信中，不仅加密用户文件，同时还窃取了用户信息，如果不缴纳赎金，则公开用户文件。



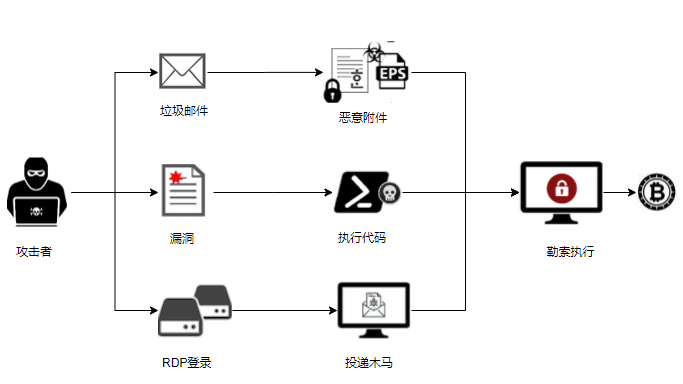
紧接2019下半年开始，针对政企的勒索病毒大量增加，勒索的同时窃取了受害者信息，这不仅对企业经济造成损失，而且对企业声誉和用户隐私的造成更大影响。基于双重的压力之下，受害企业往往只能缴纳赎金，即时止损。

**4、勒索软件 TTPs**

勒索软件不同于其他蠕虫或者木马等恶意软件，大部分勒索软件具有暴力性，不需要考虑隐藏自身等行为，但危害程度相对与其他恶意软件有过之而无不及。我们对恶意软件的讨论，主要集中在投递、横向传播以及攻击特点方面。对于那些我们目前还无法无损解密的情况，我们着重讲解其传播特性，为以后的预防打下基础。

**4.1 传播**

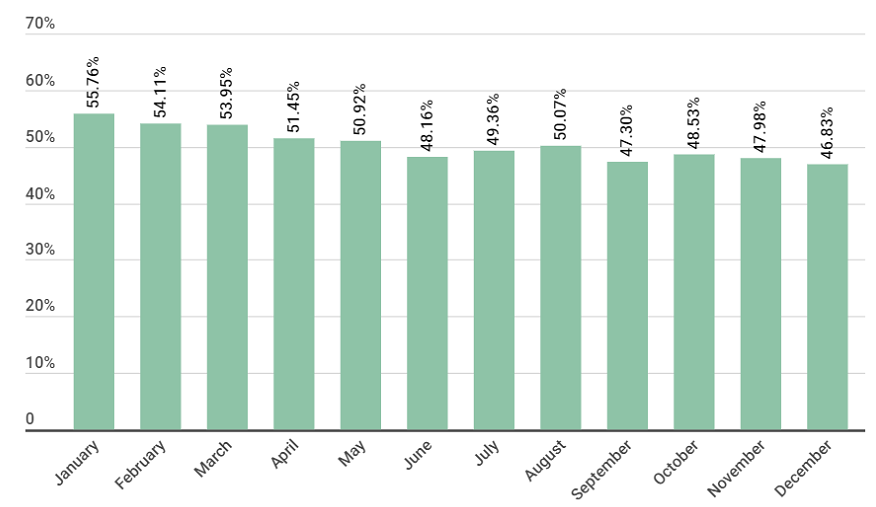
勒索软件的传播其主要方式为垃圾邮件、漏洞利用、RDP 弱口令，如下图：



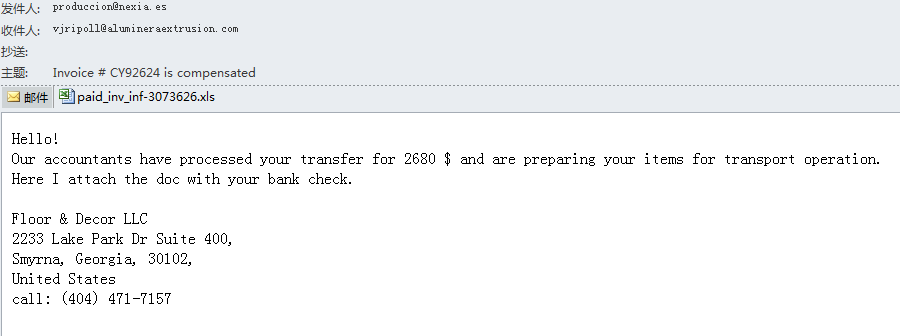
**4.1.1 垃圾邮件**

垃圾邮件 ( junk Mail 或 Email spam ) 是滥发电子消息中最常见的一种，指的就是不请自来，未经用户许可就塞入信箱的电子邮件。

垃圾邮件也是恶意软件(无论是勒索病毒还是蠕虫木马)最主要的传播方式之一。攻击者为了提高恶意软件的传播率和提高自身隐秘性，通常会通过 Necurs 、 Rustock等大型僵尸网络进行邮件的分发，全球计算机网络中每天都会有数以万计的垃圾邮件在用户之间传播。其中大部分都包含恶意软件附件或者有害的钓鱼链接。这不仅浪费用户正常的工作时间，还大大增加了网络资源的浪费。



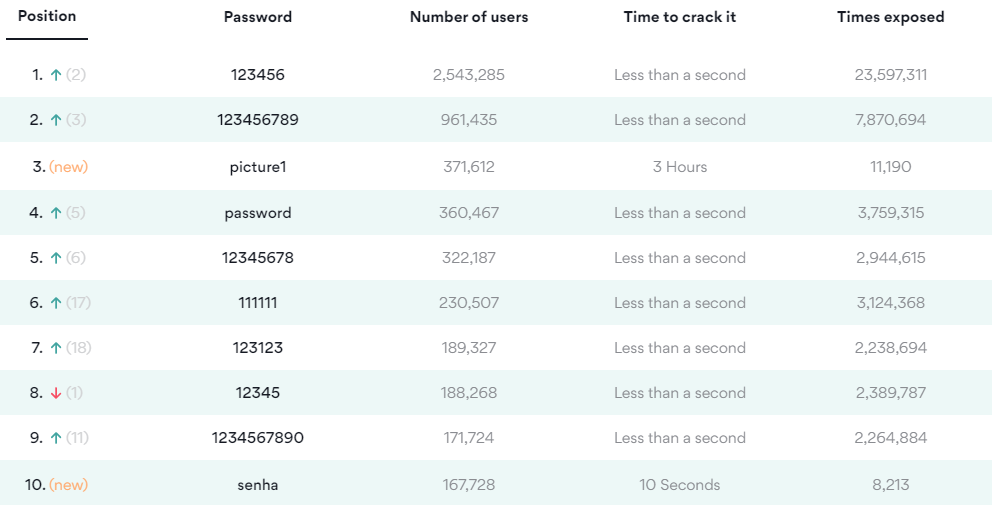
垃圾邮件结构多为一封携带附件的电子邮件，邮件内容多为交货收据、退税单或票证发票，然后提示受害者必须打开附件才能收到货物或收取款项，诱惑受害者运行附件内容，其附件多为 Word文档、 JavaScript 脚本文件或者伪装后的可执行文件。如果受害者没有一定的计算机知识，很容易误认为这个文件是正常的，直接运行后导致计算机文件被勒索或者被攻击者远程控制。除了垃圾邮件之外，如果对指定政企单位进行勒索攻击，通常会采用发送钓鱼邮件，其内容相比垃圾邮件多为实时消息或者与其单位相关的话题，如利用2020新冠等话题进行定向攻击，如下就是一个典型的垃圾邮件。



**4.1.2 RDP/弱口令**

远程桌面协议 (RDP: Remote Desktop Protocol) 主要用于用户远程连接并控制计算机，通常使用3389端口进行通信。当用户输入正确的用户密码，则可以直接对其远程电脑进行操作，这为攻击者提供了新的攻击面。只要拥有正确的凭证，任何人都可以登录该电脑。故攻击者可以通过工具对攻击目标进行端口扫描，如果用户开启了3389端口，并且没有相关的防范意识，使用弱密码如123456，攻击者可以进行远程连接并通过字典尝试多种方式组合，暴力破解用户名密码。一旦拥有登录权限，就可以直接投放勒索病毒并进一步横向渗透扩大影响面。

下图展示了2020年度最新排名前十的弱密码:



**4.1.3 漏洞利用**

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未被授权的情况下访问或破坏系统。

漏洞利用与时间息息相关，如果攻击者利用 0day 进行攻击，那么相关的系统或者组件是极其危险的。但是在以往的勒索事件中，大多数攻击者一般采用成熟的漏洞利用工具进行攻击，如永恒之蓝、RIG 、GrandSoft 等漏洞攻击包等。如果用户没有及时修复相关漏洞，很可能遭受攻击。

在过去的一年里，受疫情影响，很多人开始居家办公，由于工作方式的转化促进了远程办公工具的兴起，进而导致了远程工具相关漏洞利用攻击事件的显著增加，除了传统的 office 漏洞（如 CVE 2012-0158、CVE 2017-11882 等），一些新的漏洞利用攻击也频繁出现，如 CVE-2019-19781、CVE-2019-11510 等。

**4.2 横向移动**

一旦勒索软件进入用户环境，为了尽可能扩大影响，很可能不会直接进行加密，而是通过感染机进行渗透其他机器、权限提升或者窃取更有价值的凭证。通过横向移动攻击如果可以拿到域控权限，从而获取控制域环境下的全部机器。无论是赎金额度还是勒索成功率都会大大提高。

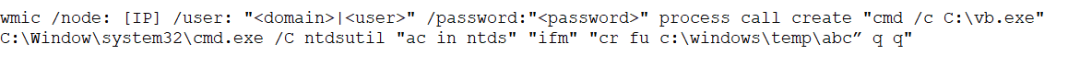
其主要方式包括:

**1. 使用如 PsExec 等工具**

如 WastedLocker 勒索软件通过入侵系统后，会通过 psexec 等命令进行横向渗透，寻找价值较高的系统并进行加密

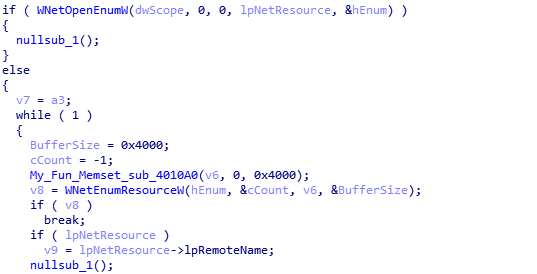
psexec -s \\<HOSTNAME>|<IP\_ADDRESS> cmd

**2. 通过 WMI 命令完成**



如 Conti 勒索软件在通过 wmic 远程执行命令，收集域密码哈希，进行横向渗透，利用 IPC$ 或者默认共享如 makop 通过遍历共享资源进行加密

**3. 利用永恒之蓝等漏洞**



如著名的 WanaCry 勒索病毒通过永恒之蓝漏洞和445端口进行内网传播。

**4.3 扩大影响**

正如之前所说，当前的勒索软件不在是功能单一的勒索，而是联合其他恶意软件如僵尸网络、窃密木马等一起发动攻击。通过对用户敏感数据进行窃取，从而进行勒索。而且对目标的攻击更加具有针对性，所利用的工具也大都为定制化工具。如 Nozelesn 勒索软件利用 Emotet 僵尸网络进行传播、Locky 勒索软件通过 Necurs 僵尸网络传播垃圾邮件进行分发、Ruyk 利用 Trickbot 木马进行传播并窃取用户信息。

**5、常见勒索软件**

**5.1 Sodinokibi/Revil**

**5.1.1 概述**

Sodinokibi 于2019年4月被发现，与之前 GandCrab 勒索软件相关，并与其采用相同的传播策略，被称为 GandCrab 勒索病毒的接班人，之后在全球进行大范围传播，其变种数量众多。

**5.1.2 常见后缀**

随机

**5.1.3 传播方式**

* Oracle Weblogic Server漏洞
* RDP攻击
* 垃圾邮件
* APT水坑攻击方式
* 漏洞利用工具包和恶意广告下载

**5.1.4 特征**

替换桌面背景图片

内存解密配置文件

{

"pk": "",

"pid": "",

"sub": "",

"dbg": ,

"fast": ,

"wipe": ,

"wht": {

"fld": [],

"fls": [],

"ext": []

},

"wfld": [],

"prc": [],

"dmn": "",

"net": ,

"nbody": "",

"nname": "",

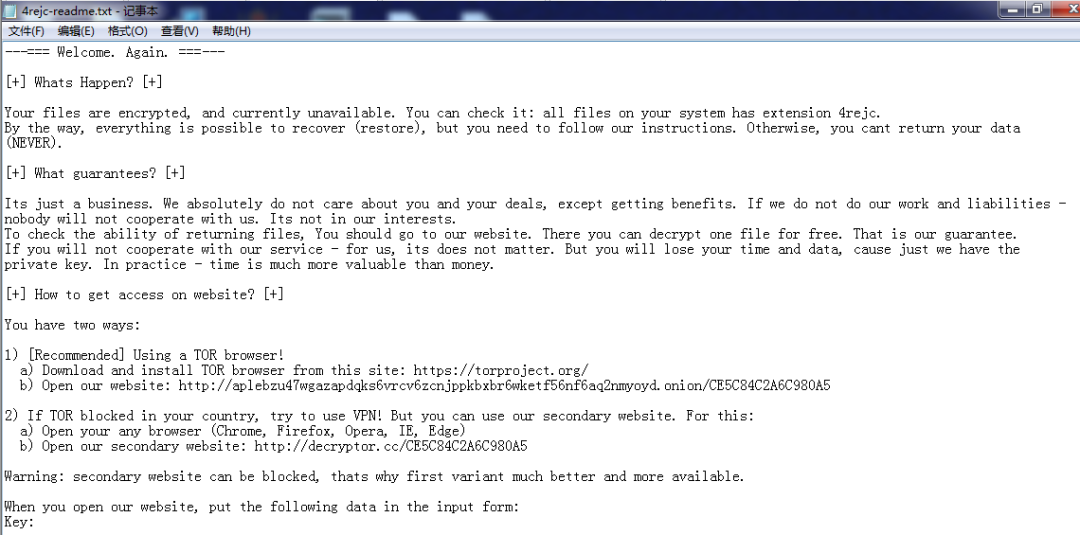
"exp": ,

"img": ""

}

**5.1.5 勒索信**

<random>-readme.txt



**5.2 Stop**

**5.2.1 概述**

Stop主要通过软件捆绑进行传播，并且部分软件会通过远程下载 Azorult 密码窃取木马到本地，窃取受害者信息。

**5.2.2 常见后缀**

* stop
* puma
* djvu
* tro
* kroput
* promo
* grovas
* nols

**5.2.3 传播方式**

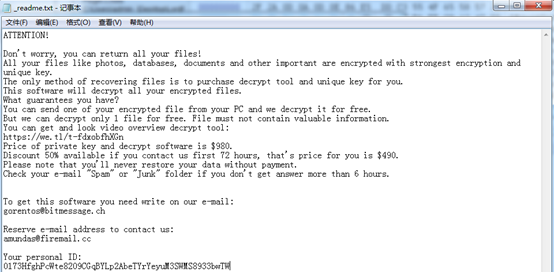
* 软件捆绑
* 垃圾邮件

**5.2.4 特征**

复制自身并连接网络下载文件到 %appdata%\\GUID 目录

**5.2.5 勒索信**

\_readme.txt



**5.3 Crysis/Dharma**

**5.3.1 概述**

Crysis勒索病毒，又称Dharma。2016年首次被发现，在2017年5月万能密钥被公布，2017年6月之后继续更新，主要采用RDP爆破进行攻击，最新版采用AES+RSA进行加密，不能解密。

**5.3.2 常见后缀**

{id}+勒索邮箱+特定后缀(如.crysis，.xtbl,.java，.crysis，.dharma，.wallet)

**5.3.3 传播方式**

RDP

**5.3.4 特征**

在%Startup%、%AppData%和%windir%系统目录存在样本备份

勒索信放于%Startup%和%windir%目录

**5.3.5 勒索信**

邮箱.hta



**5.4 Ryuk**

**5.4.1 概述**

Ryuk勒索病毒于2018年由国外安全公司披露。相对于其他勒索软件，该家族更倾向于一种定制化的攻击，通过加密网络中的重要资产和资源来勒索赎金。

**5.4.2 常见后缀**

.RYK

**5.4.3 传播方式**

钓鱼邮件

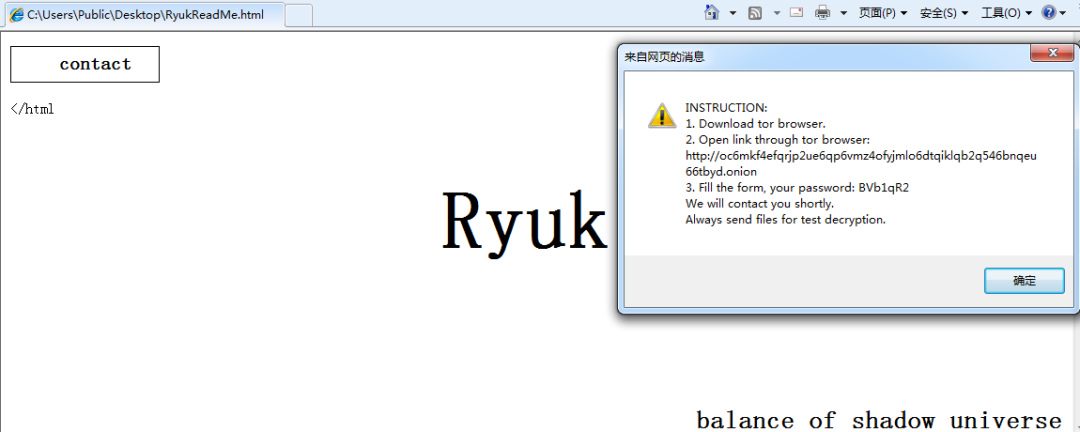
**5.4.4 特征**

横向传播样本，样本放于%Public%目录，文件名随机

在相同目录创建多个隐藏属性文件名随机的副本

**5.4.5 勒索信**

RyukReadMe.html



**5.5 Globelmposter**

**5.5.1 概述**

Globelmposter 勒索病毒首次出现是在2017年5月份，在过去的几年中，对医院以及政企单位发起了大规模勒索攻击，其主要通过钓鱼邮件、RDP爆破进行传播，变种数量众多。每年都会有版本更新，截至目前已经存在1.0、2.0、3.0、4.0、5.0等版本，最近友商披露5.1版本正在传播。

**5.5.2 常见后缀**

TRUE、FREEMAN、CHAK、TECHNO、DOC、ALC0、ALC02、ALC03、RESERVE、GRANNY、BUNNY+、BIG、ARA、WALKER、XX、BONUM、DONALD、FOST、GLAD、GORO、MIXI、RECT、SKUNK、SCORP、TRUMP、PLIN

Ox4444、Snake4444、Rat4444、Tiger4444、Rabbit4444、Dragon4444、Horse4444、Goat4444 、onkey4444 、Rooster4444 、Dog4444 、Pig4444

auchentoshan、makkonahi

Ares666、Zeus666、Aphrodite666、Apollon666、Poseidon666、Artemis666、Dionysus666、Hades666、Persephone666、Hephaestus666、Hestia666、Athena666

C4H、.IQ0005、lockfiles

**5.5.3 传播方式**

钓鱼邮件

RDP

**5.5.4 特征**

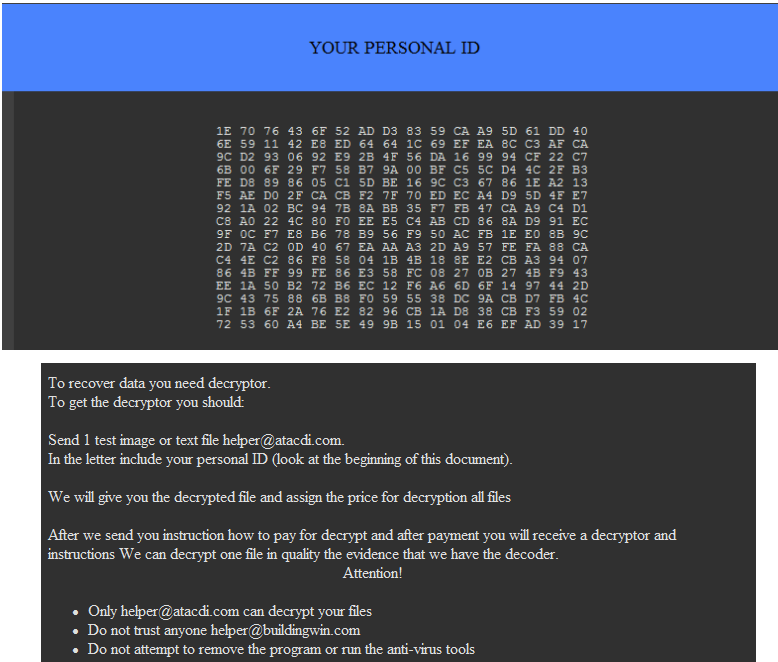
在%LOCALAPPDATA%或者%APPDATA%存在样本备份，并通过注册实现自启动;

在%public%存在用户ID以及rsa公钥文件;

在%temp%存在bat脚本文件用于环境清理;

**5.5.5 勒索信**

how\_to\_back\_files.html



**5.6 Buran**

**5.6.1 概述**

Buran 勒索病毒自2019年9月开始传入我国。早期该勒索病毒会在注册表和加密文件中写入 “buran” 字符串，故命名为 Buran 勒索病毒。

**5.6.2 常见后缀**

.Buran、.{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}、.xxx-xxx-xxx等

**5.6.3 传播方式**

垃圾邮件

RDP

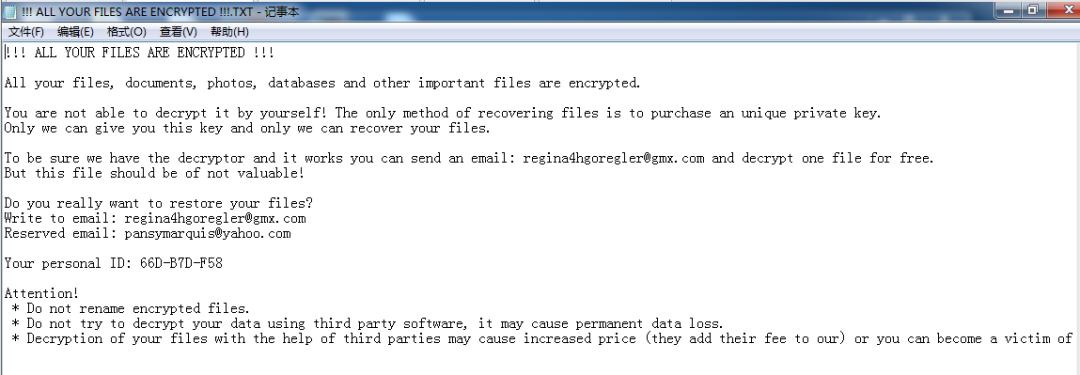
**5.6.4 特征**

进程可带参数启动，参数为 -agent 0、-start;

拷贝自身到 %Appdata%\Microsoft\Windows 文件下，并随机命名;

**5.6.5 勒索信**

!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT



**5.7 NetWalker**

**5.7.1 概述**

NetWalker 于2019年9月出现，其幕后创建者为以俄语为母语的的团体组织，以 Circus Spider 名称提供 RaaS 服务，隶属 Mummy Spider 成员。

**5.7.2 常见后缀**

随机

**5.7.3 传播方式**

钓鱼邮件

**5.7.5 勒索信**

USERID-Readme.txt

**6、勒索软件的趋势**

从第一起勒索事件被披露，经过时间的洗礼，勒索软件正在一步步进化。当前的勒索事件背后从开发、销售到攻击，早已成为一个供销分明的产业链，虽然人们一直在想方设法遏制其发展，但是不可否认的是这条产业链规模不仅没有缩小反而越来越流行。随着勒索软件的形式越来越多样，其在今后的发展将何去何从？

对于政企单位来说，由于其数据价值高，影响广泛，依旧会被勒索软件针对，其勒索事件日后也会只增不减，并且赎金价值也会越来越大。在最近一年，披露了一大批漏洞工具包、渗透攻击工具，这让攻击者在对指定目标攻击时更加隐蔽，手法也会更加高明。其精准化、复杂化、定制化、流程化将会是针对政企单位攻击的一大特点。如果公司内部没有及时更新并且做好相应的防范措施，可能会遭到攻击。

除了基于个人电脑的传统企业外，IOT设备的勒索攻击很可能成为下一个主流攻击面。虽然IOT设备的勒索攻击在2016年已经被提及，这几年勒索事件频发，但针对IOT设备的勒索攻击还是相对来说比较少的。如今，随着5G技术的普及，万物互联的时代也一步步改变我们的生活。智能摄像头、智能冰箱、电灯等物联网设备越来越多，占据人们生活比重越来越大。相信在不久的将来，物联网勒索也会成为一个重要的攻击面。

如上文所说，勒索的同时很可能会造成数据的泄露，虽然攻击者保证缴纳赎金会销毁数据，但是随着勒索事件越来越多，当这块蛋糕变的越来越小时，即使受害者缴纳赎金，其勒索得到的数据也很可能会变成在线商品进行出售，从而牟取利益最大化。

在针对个人勒索，相较于企业、公司而言，针对个人及其勒索数据价值相对较小，勒索成功率较低。但是近期勒索软件针对个人的勒索形式也不在局限于数据的勒索，对于个人隐私的勒索也越来越多，通过裸聊软件进行录屏等形式进行隐私勒索，此类勒索事件越来越多，相比于数据勒索该种形式的勒索成功率要高得多，并且很可能让犯罪者进行持续勒索。

**7、勒索软件响应措施**

**7.1 感染迹象**

勒索软件具有强破坏性。一旦运行起来，用户很快就会发现其特征，如部分进程突然结束、文件不能打开、文件后缀被篡改、屏保壁纸被更换等。

**7.2 应急处理**

**7.2.1 物理隔离**

强制关机和关闭网络（关闭网络包括拔网线、禁网卡，笔记本禁用无线网络）

**7.2.2 访问控制**

加策略防止其他主机接入，关闭感染主机开放端口如445、3389等，修改感染主机及同局域网下所有主机密码，密码采用大小写字母、数字、特殊符号混合的长密码。

**7.2.3 确认损失**

查看感染主机数量，根据感染特征，排查未感染主机，统计受损情况并列出清单。

**7.2.4 主机加固**

对未受感染主机进行加固处理，包括：

1. 登录密码采用强密码(大小写字母、数字、特殊符号混合，长度为15+)

2. 更新系统补丁，更新应用软件到最新版本

**7.2.5 保护现场**

当以上措施结束之后，尽量不要再操作受感染主机，等待相关专业人员进行处理。

**7.3 加密数据处理**

当数据被加密，如何对数据进行恢复。一般情况数据恢复有以下途径。

**7.3.1 备份恢复**

利用备份数据恢复是当前数据恢复途径中最有效成本最低的恢复方式，所以如果在固定的工作周期及时进行备份，这时就可以轻松应对。但是在恢复时一定要注意将被感染机器的勒索病毒清除干净，最好是格式化磁盘或者重装系统并及时修复系统漏洞，保证安全之后在恢复备份，防止二次感染。

**7.3.2 解密工具**

利用网上提供的解密工具进行修复，在一些特定情况下，如勒索软件通过读取文件副本加密然后删除原文件的方式，如果原文件内存未被覆盖，或者勒索软件尚未加密完成，及时发现后强制关机。部分文件未加密，这些情况都有几率成功恢复。

也可以使用很多在线解密网站的解密工具。通过公开的密钥进行解密，其密钥获取主要的方法为以下四种方法：

1.勒索软件本身算法存在缺陷，内存中可找到密钥；

2.攻击者服务器比较脆弱，通过攻陷服务器，获取解密密钥；

3.多国联合执法，通力合作，抓捕攻击者获取密钥并公开发布；

4.攻击者自己良心发现，公开密钥。

**7.3.3 支付赎金**

如果加密数据过于重要且无法免费解密，不得不缴纳赎金时，也需要注意，因为有部分勒索软件本身存在缺陷无法进行解密，即使缴纳赎金也无法恢复。另外一般赎金的类型为加密货币如比特币、达世币等，与法币交易不同，最好是找相关的安全专家进行综合判断之后，在确定是否缴纳赎金。不然如果盲目交钱，很可能最后人财两空。

**7.3.4 重装系统**

如果数据不重要或者通过上述方法解密成功之后并对数据做好备份之后，一定要重装主机系统，及时更新补丁等，防止二次勒索。

**8、日常防范**

现在勒索病毒的勒索形式不断变化，一旦中招，想要无损解密相对来说比较困难。所以，勒索病毒主要还是预防为主，通过周期性的安全培训，增强人们的安全意识。做到未雨而绸缪，防止临渴而掘井。

1.使用大小写字母、数字、特殊符号混合长度15+的强密码作为登录密码，并定期进行修改；

2.及时更新系统补丁，及时更新应用软件到最新版本；

3.对重要文件及时备份；

4.适当安装反病毒软件，及时更新病毒库；

5.不随便运行邮件附件、未知可执行程序，对于不确定文件，可放入沙箱如s.threatbook.cn 或 any.run 等；

6.不访问不安全连接；

7.无特别需求，应尽量关闭3389、445等端口。