登录

Encryption 101系列：恶意软件分析人员加密知识入门

mss**** / 2018-03-12 11:46:39 / 浏览数 11742 技术文章 技术文章 顶(0) 踩(0)

原文：https://blog.malwarebytes.com/threat-analysis/2018/02/encryption-101-malware-analysts-primer/

0x00 简介

虽然大部分安全业内人士对于加密技术并不陌生，但是，仍有许多人对加密技术在恶意软件（特别是勒索软件）中的应用方式缺乏基本的了解。鉴于此，本文将会为大家介绍

首先，我们将介绍什么是加密技术，然后，讲解勒索软件加密文件时所用的主要方法。在本系列的第二篇文章中，我们将以勒索软件Ransom.ShiOne的最新变体为例，展示

0x01 什么是加密？

简单来说，加密就是对信息进行编码处理，使得只有授权方才可以访问明文信息，而未授权方则无法访问这些信息。从计算的角度来看，加密就是将数据从可读形式（明文）

不幸的是，加密也被用于恶意目的，例如勒索软件就属于这种情况。

0x02 分析加密算法

对于恶意软件分析人员来说，为了有效分析用于恶意目的的加密算法，需要在创建或接收加密数据的计算机上对其进行深入考察。如果他们可以在数据加密之前访问系统上的

要想在无需破解加密的情况下恢复文件的话，成为观察者是唯一的机会。但是，对于勒索软件攻击情形来说，成为观察者通常是不可能的。这是因为，当恶意软件运行结束并

那么，成为解密和加密的观察者究竟意味着什么呢？有人曾问我：

■■■■■■■■■■■■■C2■■■■■■■■■■■■■■■

我的回答是，因为恶意软件是可以公开获取的，毕竟它可能运行于世界各个角落的受害者系统上。作为逆向工程师，我们能够访问二进制文件，并可以在最低、最详细的级别

在客户端（受害者计算机）上接收到的SSL或https通信流量，需要在内存中进行解密，以便提取出符合恶意软件要求的数据。而在这个过程中，如果我们有机会“窥视”内存，

前面的逻辑同样适用于勒索软件和文件加密的情形。如果我们在“窥视”勒索软件的过程中，它在本地生成了加密密钥，那么，我们就可以在内存中看到该密钥，并将其保存下

在勒索软件运行和加密文件的时候，如果用户转储了其内存的话，就有机会成为观察者并恢复文件。不幸的是，事情并不总是如我们所愿，因为受害者的第一本能并不是在创

0x03 勒索软件使用的算法

近几年来，我们遇到过许多“绑架”受害者文件的算法，其中大部分都与标准、公开和经过验证的非对称加密算法有关。但是，偶尔也会遇到自定义加密算法（可能会更弱），

多年前，当我刚开始接触勒索恶意软件时，它们通常会使用其他方法“绑架”受害者计算机来从事勒索，而不是加密驱动器上的所有文件。现在，他们的勒索手段已经变得五花

0x04 文件混淆

就文件混淆方式来说，勒索软件只是移动或隐藏目标文件（文档及其认为受害者在意的其他文件），然后要求受害者支付赎金以恢复文件。在这种情况下，恢复方法其实非常

下面给出一个示例：弹出窗口声称硬盘驱动器已损坏，并要求受害者回电咨询，这时他们就要求支付“支持”费用以恢复文件。在某些恶意软件中，会显示一个弹出窗口（如下

0x05 自定义加密算法

对于自定义加密算法来说，最常见的情形就是通过一种标准方式修改文件中的所有内容。一个简单的例子就是，利用常量或循环字节组对文件进行逐字节异或运算。在这些情

0x06 MBR重写

在第三种情况下，MBR会被一个需要输入密码或序列号才能访问的小程序所重写。然后，恶意软件会强制重启计算机，并在系统加载Windows之前，提示用户需支付赎金才

除了逆向算法之外，剩下的难点就是需要了解如何重写MBR，以将原始代码恢复到驱动器的引导区中。

以下是一个MBR锁的示例代码。需要注意的是，它没有要求输入任何ID，这意味着锁定过程无需特定的数据，并且可能需要静态解锁代码。

实际上，上面介绍的这些方法并非标准意义上的加密技术，之所以在此介绍它们，是为了说明有时自定义的、闭源的混淆算法破解起来非常容易。现实中，大多数犯罪分子都

为什么要强调这一点呢？因为有些使用标准算法的开源加密算法，其安全性是建立在加密密钥之间特定关系之上的。例如，有的算法会导出两个既相互关联又相互独立密钥。

0x07 非对称密码加密

非对称加密通常会生成两个完全不同的密钥；然而，它们之间的关系是密不可分的。一个密钥（公钥）用于将数据加密为密文，而其另一个密钥（私钥）用于将密文解密为原

对基于非对称密码算法的加密通信来说，两个密钥都是在本地生成的——无论公钥还是私钥。公钥可向所有人公开。如果我们想给Bob发送一则只有他才能阅读的消息，这时

下面给出了一些示意图，可以帮助读者加深理解。

这里的加密算法与勒索软件作者用于文件加密的方法是相同的，具体过程如下：

首先，生成一个随机数组。在进行第一轮文件加密操作前，将会用到这个字节序列。通常，算法会对公钥进行一系列的数学运算，实际上就是通过随机初始化操作，根据初始

最初，算法会使用随机数作为IV，然后，将生成的密文用于下一轮加密。

实际上，密钥本身的生成也依赖于随机数生成器。因此，拥有一个可靠的、“尽可能随机”的随机数生成器是非常非常重要的。

0x08 勒索软件常用的文件加密算法

现代勒索软件通常会在本地动态生成密钥，然后将它们发送至对应于客户端ID的C2服务器上，或者由作者生成密钥并提前植入到勒索软件本身之中。

虽然后一种做法要更安全一些，但其缺点是，需要为每个受害者生成一个全新的二进制文件，所以需要大量额外工作；或者可以退一步，在每次攻击活动中，让同一版本的恶

如果密钥是动态生成的，那么就存在使用内存转储来恢复文件的可能性（尽管这个可能性很小），以及分析师可以在加密代码中找到漏洞的可能性（尽管这个可能性也很小）

现代勒索软件作者通常使用AES，RSA，Blowfish等标准加密算法，以试图达到没有解密密钥的情况下，受害者无法恢复加密文件的目的。之所以加了“试图”这两个字，是因

不对称密码加密算法几乎是无法破译的，但这并不意味着毫无希望。为了了解加密的破解之道，请阅读本系列的下面一篇文章，届时，我们将以ShiOne勒索软件为例，为恶

上一篇：Web日志安全分析系统实践 下一篇：知识图谱系列（1）基础知识简介

1. 0 条回复

- 动动手指，沙发就是你的了！