WanaCrypt0r加密流程研究学习记录

原创

网糸隹 于 2018-11-12 10:59:32 发布
分类专栏： 密码 密码技术与应用 文章标签： WanaCrypt0r 加密 对称加密 非对称加密

摘要：本文档根据多家安全公司对新型勒索软件WanaCrypt0r的逆向分析结果和报告，记录该勒索软件的加密过程和密钥架构。

关键词：WanaCrypt0r、勒索软件、密钥、公钥、私钥、加密、RSA、AES、CryptGenRandom、CryptGenKey。

1. 前言

近日全球多个国家和地区的机构及个人电脑遭受到了新型勒索软件WanaCrypt0r（形象地直译为想哭）攻击。它利用了窃取自美国国家安全局的黑客工具永恒之蓝（EternalBlue）实现了全球范围内的快速传播，在短时间内造成了巨大损失。该勒索软件使用加密算法有选择性地加密受害者电脑内的重要文件向受害者勒索赎金，除非受害者交出勒索赎金否则加密文件无法恢复。被加密文件包含Office文档、邮件、PDF文档、图片、压缩包、虚拟机文件等。

本文从360、看雪、McAfee等公司对该勒索软件的逆向分析结果和报告中摘取勒索软件的加解密流程和密钥结构，将其作为一个学习样本，学习其加密过程和密钥架构。

2. 启动逻辑

原始样本会从资源中加载释放一个名为tasksche.exe的文件，并且以tasksche.exe /i的方式启动，tasksche.exe启动后首先会将自身拷贝到指定位置，接着创建服务，然后以服务的方式再启动自身。

以服务的方式启动后，tasksche.exe会以创建进程的方式执行用于修改文件属性相关的权限的命令。接着，会读取前期释放的一个名为t.wnry文件，并对其中的内容进行解密，解密后的内容为一个Dll文件，但是该Dll文件并不会被写入磁盘中，而是在内存中直接执行。分析者将该Dll从内存中dump，其取名为crypt.Dll，并作进一步分析。

crypt.Dll只有一个自定义的导出函数TaskStart，该导出函数是其行为展开的入口。进入TaskStart后该样本会先加载Kernel32，动态获取后续需要的API，然后加密部分文件而不是所有文件。猜测这么做的原因为：1）可能破坏系统导致系统无法启动；2）选择更有价值的文件；3）普遍撒网会延长加密时间）。要加密的文件以后缀名列表的形式放在程序中，主要是Office文档、邮件、PDF文档、图片、压缩包、虚拟机文件等。

3. 加密思路

加密思路如下。

1. 文件采用AES加密，而不是用RSA2048加密。原因很简单，效率！RSA和AES的效率有千倍的差距，比如，现在处理器执行AES加密的效率基本都可以达到Gbit/s（150兆字节每秒或更快）；如果它调用了AES-NI指令，那加速速度更加惊人。但RSA加密的速度基本上达不到1兆字节每秒。
2. 采用数字信封的方式加密，即AES加密文件数据，然后AES密钥被非对称算法RSA加密。AES加密效率高，适合加密大量数据；RSA虽然加密慢，但是加密的数据量少（只涉及密钥），且RSA便于密钥分发。
3. 采用三层密钥结构。详情参见4. 密钥层次。

4. 密钥层次

该勒索软件采用常见的三层密钥结构。

- 顶层密钥采用RSA 2048位密钥，公钥和私钥分别记为RPUBKEY和RPIVKEY；
- 中间层密钥是RSA 2048位密钥，公钥和私钥分别记为SPUBKEY和SPIVKEY；
- 底层文件加密密钥为AES密钥，记为FILEKEY。

表1 密钥结构表

密钥层次		类型	说明
顶层密钥	RPUBKEY	RSA2048	公钥，置于勒索软件中。
	RPIVKEY	RSA2048	对应私钥，作者自己持有。
二层密钥	SPUBKEY	RSA2048	受害用户的公钥，用于加密文件加密密钥FILEKEY。 导出到文件00000000.pky。 二层密钥调用API接口CryptGenKey生成公私钥对。
	SPIVKEY	RSA2048	SPIVKEY为受害用户对应私钥。 被置于勒索软件中的顶层密钥RPUBKEY加密后保存到文件00000000.eky。 二层密钥调用API接口CryptGenKey生成公私钥对。
文件加密密钥	FILEKEY	AES	AES128密钥，每个文件一个，一次一密。 被二层密钥的公钥SPUBKEY加密，记为ENCFILEKEY。 调用API接口 CryptGenRandom生成的随机数作为此密钥。

补充说明

1. RSA加密过程使用了微软的CryptAPI。
2. AES代码静态编译到Dll。

三层密钥相互关系及在加解密的数据流如下图所示（忽略二层公钥的导出）。

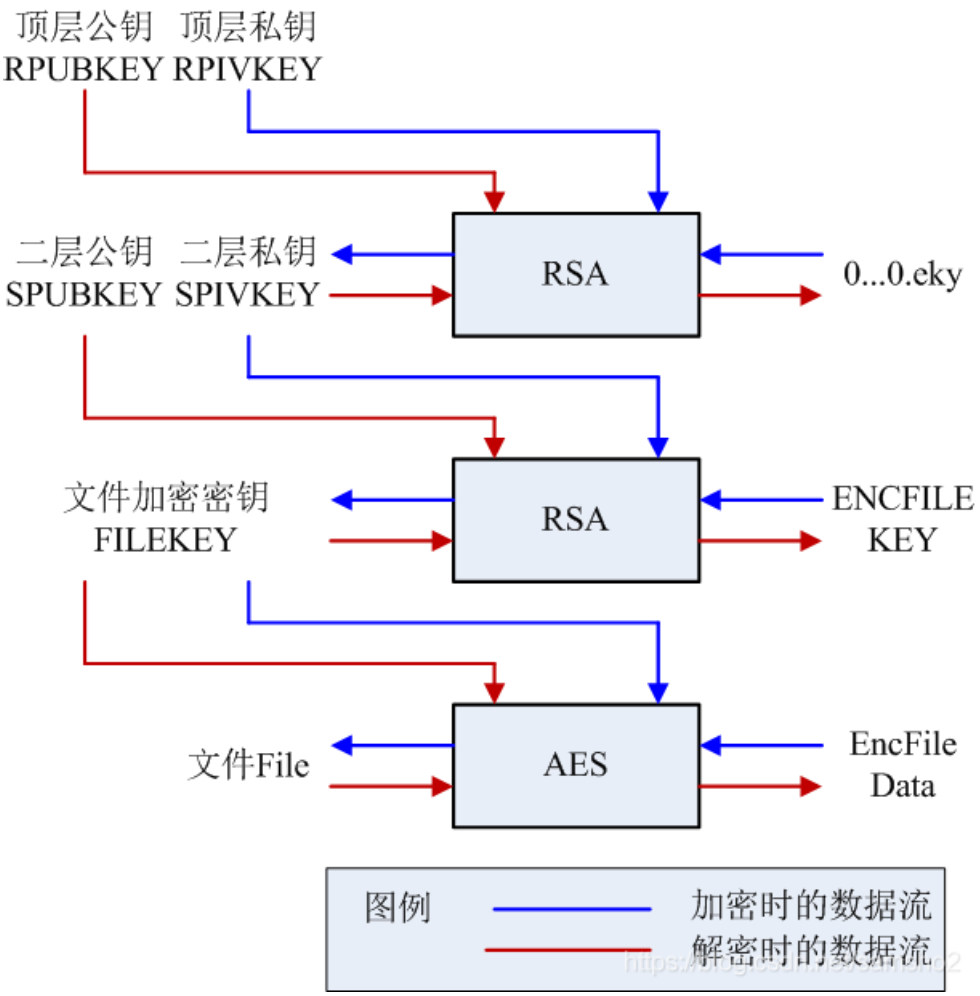

图1 加解密时的数据流和密钥流

5. 加密流程

5.1 勒索软件的加密流程

该勒索软件的加密流程按如下步骤执行。

步骤1：生成二级密钥。如果二级密钥没有生成，则生成二级密钥。否则执行下一步。

1.1 调用API接口CryptGenKey生成RSA 2048位公私钥对（SPUBKEY，SPIVKEY）。

1.2 公钥SPUBKEY导出到文件00000000.pky。

1.3 私钥SPIVKEY被主密钥中的公钥RPUBKEY加密后导出到文件00000000.pky。

步骤2：遍历文件后缀名在列表（需要加密文件的后缀名）中的文件并加密。

2.1 调用API接口 CryptGenRandom生成文件加密密钥（AES密钥）FILEKEY

2.2 用公钥SPUBKEY加密FILEKEY得到ENCFILEKEY。

2.3 使用AES密钥FILEKEY加密文件，并把ENCFILEKEY等信息写入文件。

补充说明

1. 加密文件时，勒索软件作者执行AES的步骤是：1）调用AES密钥扩展算法，把文件加密密钥扩展为扩展的子密钥，存于AES_CONTEXT；2）擦除文件加密密钥，保留扩展的子密钥AES_CONTEXT；3）利用扩展的子密钥AES_CONTEXT执行AES加密；4）加密完毕擦除扩展的子密钥AES_CONTEXT。

2. 第二步擦除文件加密密钥用保留扩展的子密钥加密。利用扩展的子密钥AES_CONTEXT可以恢复被擦除的文件加密密钥，不过此举毕竟会减少密钥直接暴露的时间。勒索软件作者为了安全，在加密完毕后擦除扩展的子密钥。
3. 勒索软件作者给加密后的文件定义了一套结构，详见6. 加密文件结构。

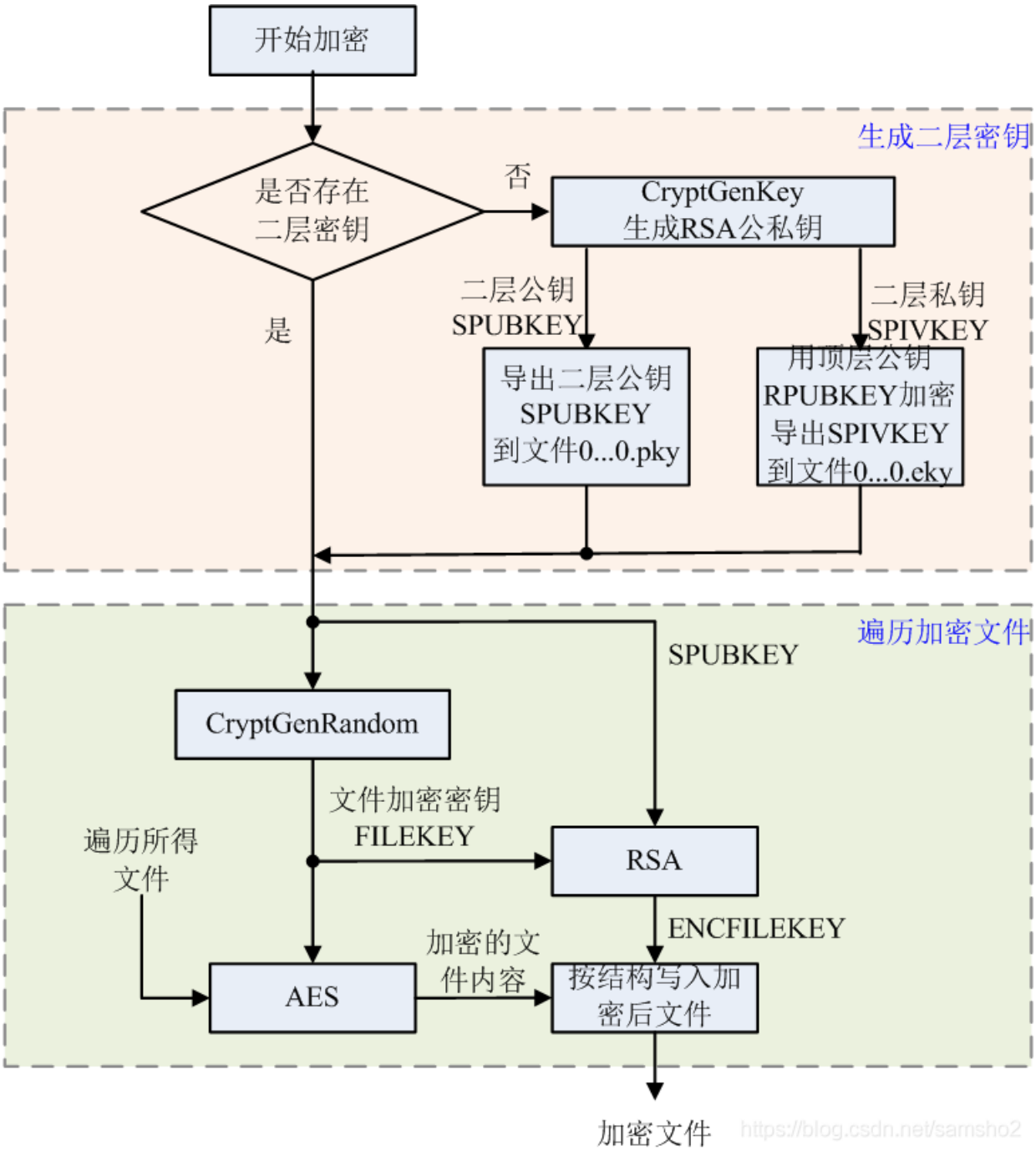

图2 加密流程图

5.2 单个文件的加密流程

单个文件的加密流程按如下步骤执行。

步骤1：加密前。新建一个文件，新文件名=原始文件名.WANACRYT，末尾的T表示临时文件，待加密完毕后会重命名，删除T。

步骤2：加密中。对新文件加密，并写入相关结构化字段（详情参见6. 加密文件结构）。

步骤3：加密后。

3.1把新文件的文件时间修改为原始文件的时间。

3.2 删除原文件。

3.3 并将新文件重命名为WANACRY，即删除文件名中的那个“T”。

3.4 若文件为可免费解密文件，则将文件名记录到f.wnry文件中。

补充说明

1. 从多个分析报告看，目前AES采用128比特密钥加密，但不排除作者将之变种为采用AES256加密。AES128用10轮变换加密128比特数据，而AES256用14轮变换加密128比特数据，效率下降不少。
2. AES算法加密原文件时采用的是哪个工作模式，目前没有从相关分析报告中查到。
3. 由于文件加密是在新建的文件中进行，然后删除原文件，所有360出了一个工具用文件恢复的思想来恢复被删除的原文件。可惜实测效果并不理想。
4. 在加密过程中程序会随机选取一部分文件使用内置的RSA公钥来进行加密，其目的是解密程序提供的免费解密部分文件的功能。能免费解密的文件路径保存在文件f.wnry中

6. 加密文件结构

加密文件的结构以及各部分含义如下。

表2 加密文件的结构

字段	长度(字节)	含义
加密标识	8	加密标志“WANACRY!”
文件加密密钥长度	4	AES加密密钥长度
被加密的文件加密密钥	256	文件加密密钥被第二层密钥（采用RSA2048密钥）加密。 RSA解密还原后实际长度为字段“文件加密密钥长度”定义的长度。
特定类型	4	不为4则表示此为可免费解密文件。
原始文件长度	8	记录原文件（未加密前）的长度。
被加密的原文件内容	原始文件长度	被AES算法加密的原文件内容。

7. 解密过程

二层私钥SPIVKEY获取流程

步骤1：解密程序通过释放的taskhsvc.exe向服务器查询付款信息。若用户已支付，则将eky文件发送给勒索软件作者，eky记录二层私钥SPIVKEY被顶层密钥RPUBKEY加密后的密文（见下图）。

步骤2：勒索者解密获得dky文件（二层私钥SPIVKEY）发送给用户。

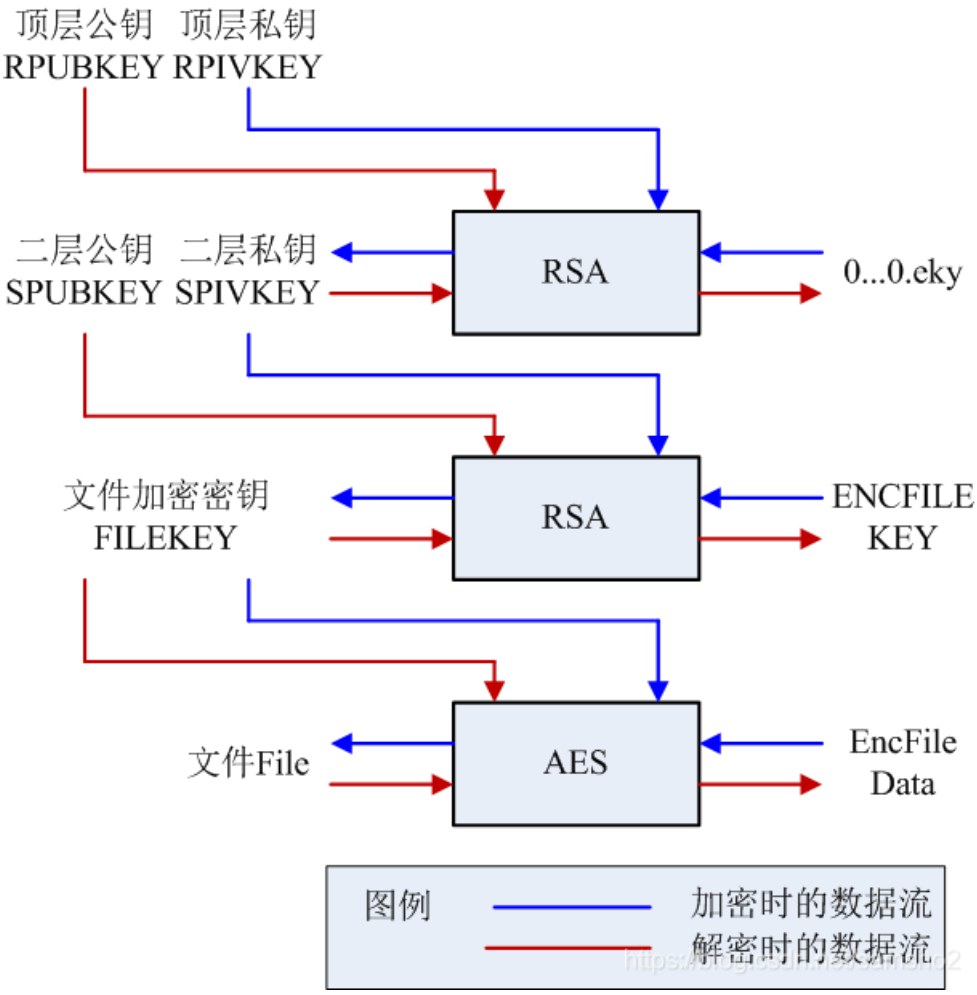

图3 加解密时的数据流和密钥流

文件解密流程

步骤1：解密程序将从服务器获取的dky文件（二层私钥SPIVKEY）导入。当不存在dky文件时使用内置密钥免费解密文件。

步骤2：解密程序从被加密文件的文件头读取被加密的文件加密密钥，使用导入的二层私钥SPIVKEY，调用函数CryptDecrypt解密得到文件加密密钥。

步骤3：使用文件加密密钥对被加密的文件执行AES解密，恢复原文。

8. 总结

从以上分析流程看，这个勒索软件可作为密码应用的一个很好的素材，可以从中获得很多可以借鉴学习的地方。

1. 可以感受到对称加密（AES）和非对称加密（RSA）速度的显著差异，完全不在一个量级。
2. 数字信封技术的应用，很好地结合了对称加密执行效率高和非对称加密便于密钥分发管理的优点。
3. 三层密钥体系在实际应用中的使用，根密钥对下层密钥保护，会话密钥直接对大量数据加密，以及密钥的层层保护措施。

后续跟进

1. 学习其反汇编后的对称加密代码。比如是否调用AES-NI指令等。
2. 了解AES加密采用的工作模式。个人猜测应该为CBC、CTR等模式，这些模式需要的IV存在哪里呢，猜测可能在加密文件文件头中，那个256字节的“被加密的文件加密密钥”字段。

进一步研究

1. Global WannaCry ransomware outbreak uses known NSA exploits

http://blog.emsisoft.com/2017/05/12/wcry-ransomware-outbreak/

1. The worm that spreads WanaCrypt0r

https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/

1. WannaCrypt ransomware worm targets out-of-date systems

https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

1. WannaCry Ransomware的进一步分析

https://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/