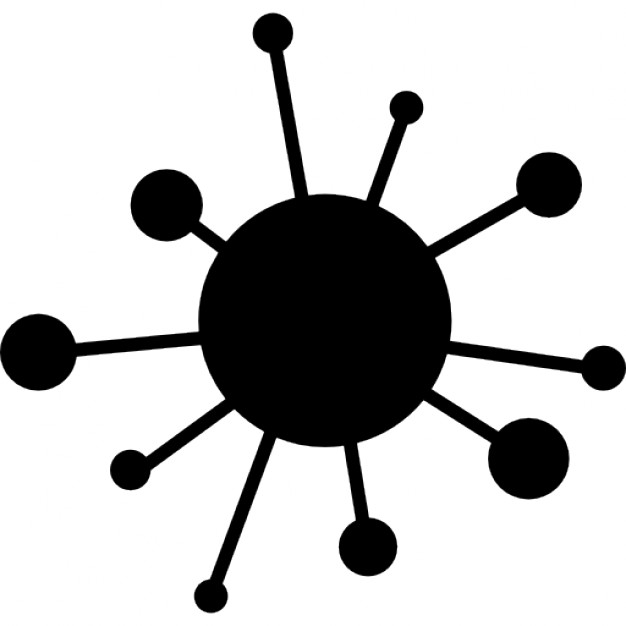
# 计算机病毒学

Wannycry勒索病毒分析案例

Copy\_from http://slab.qq.com/news/tech/1575.html



学号：0x091395

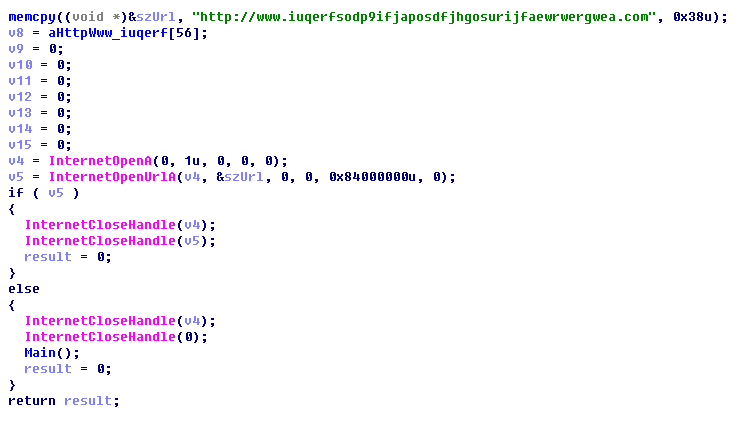
姓名：uknowho

WannCry病毒详细分析

mssecsvc.exe行为

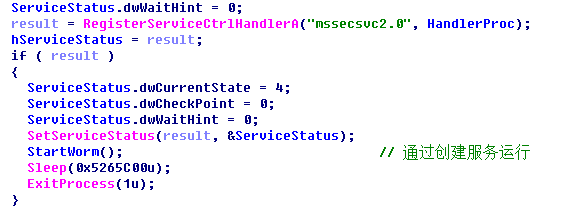
**1、开关：**

病毒在网络上设置了一个开关，当本地计算机能够成功访问http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com时，退出进程，不再进行传播感染。目前该域名已被安全公司接管。

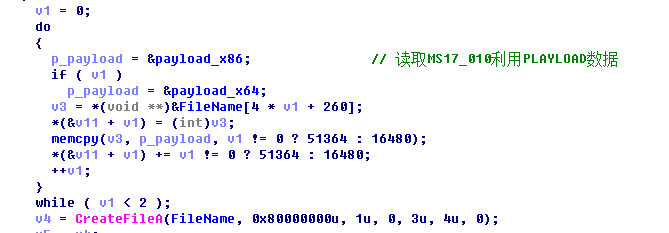


**2、蠕虫行为：**

通过创建服务启动，每次开机都会自启动



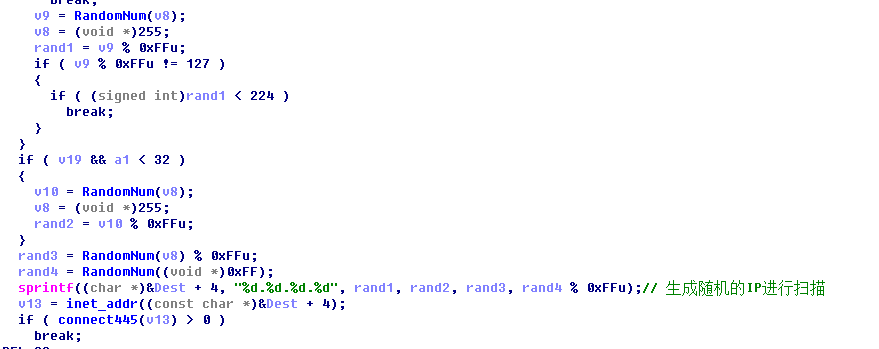
从病毒自身读取MS17\_010漏洞利用代码，playload分为x86和x64两个版本。



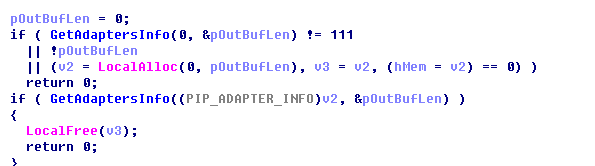
创建两个线程，分别扫描内网和外网的IP，开始进程蠕虫传播感染。



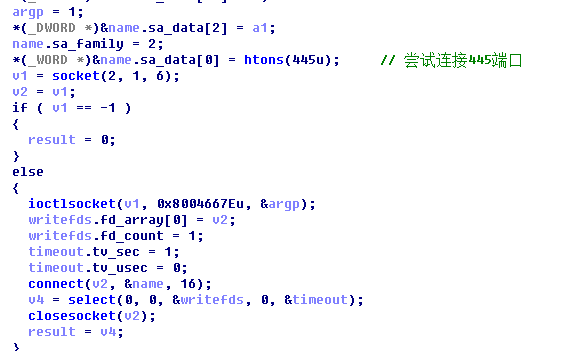
对公网随机ip地址445端口进行扫描感染



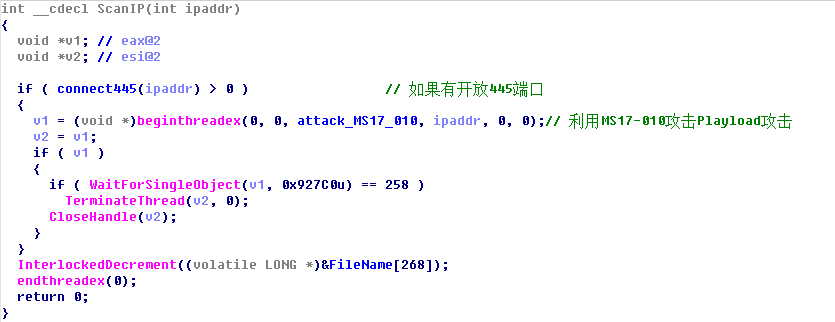
对于局域网，则直接扫描当前计算机所在的网段进行感染



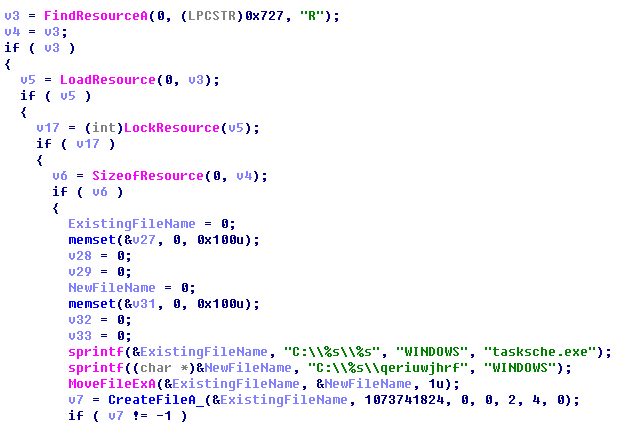
感染过程，尝试连接445端口



如果连接成功，则对该地址尝试进行漏洞攻击感染

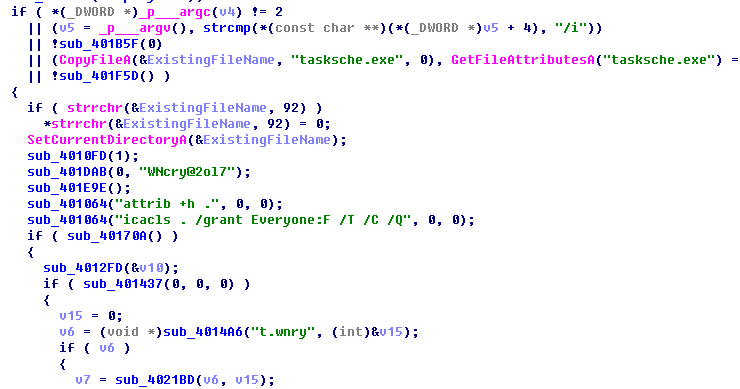


**3、释放敲诈者**

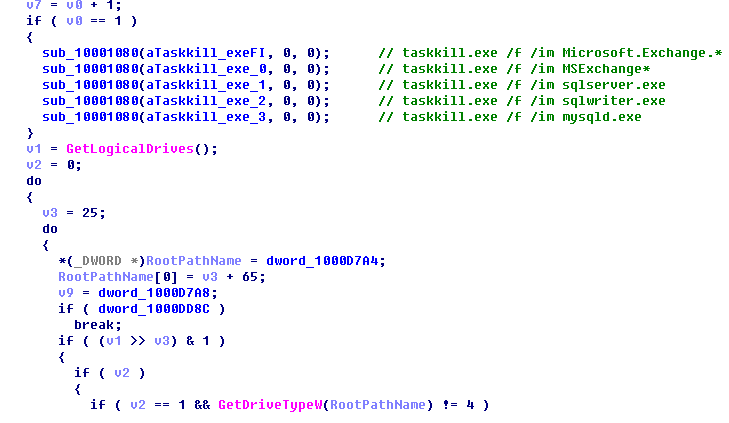


tasksche.exe行为（敲诈者）

解压释放大量敲诈者模块及配置文件，解压密码为WNcry@2ol7



首先关闭指定进程，避免某些重要文件因被占用而无法感染



遍历磁盘文件，避开含有以下字符的目录

\ProgramData

\Intel

\WINDOWS

\Program Files

\Program Files (x86)

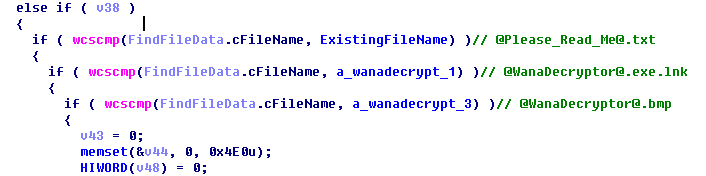
\AppData\Local\Temp

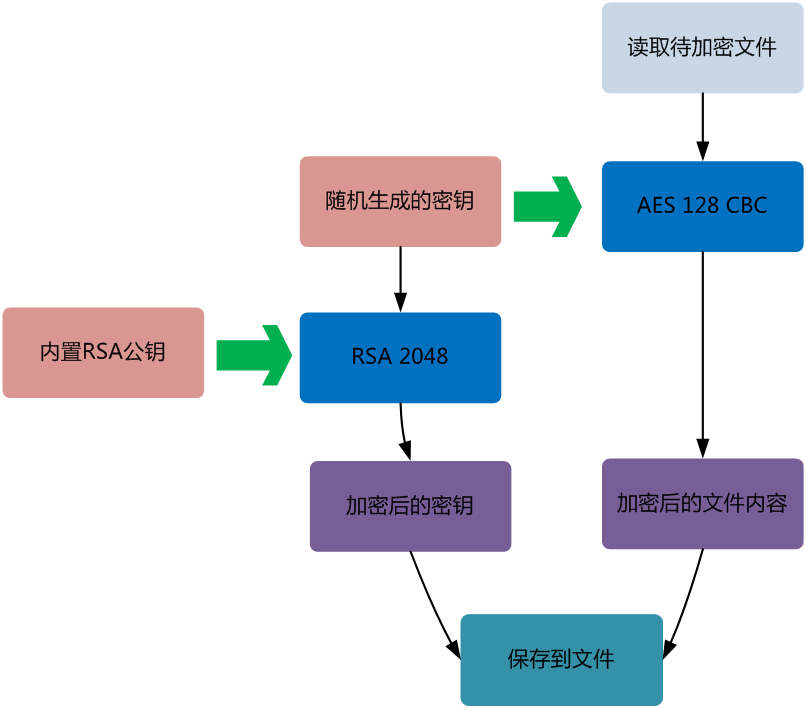
\Local Settings\Temp

This folder protects against ransomware. Modifying it will reduce protection



同时，也避免感染病毒释放出来的说明文档



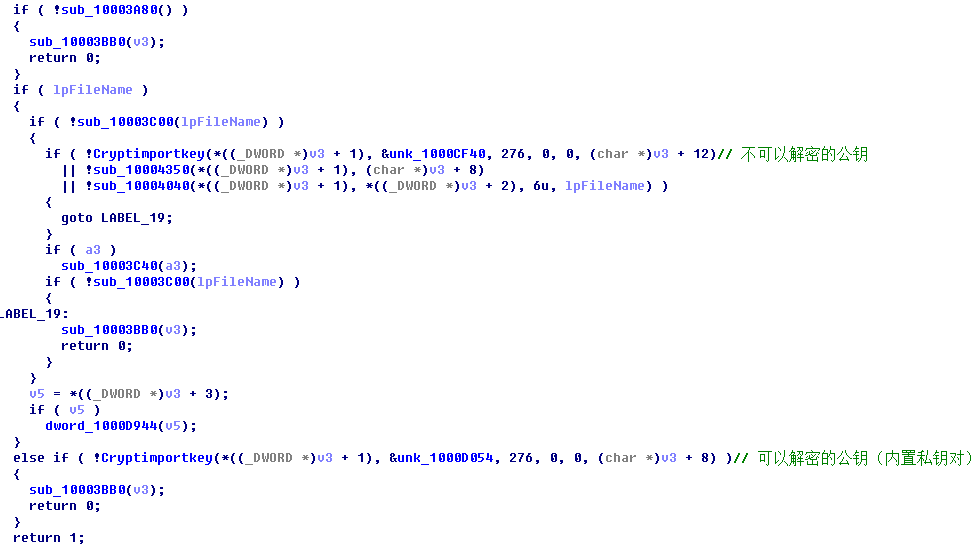


病毒加密流程图

遍历磁盘文件，加密以下178种扩展名文件。

.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der

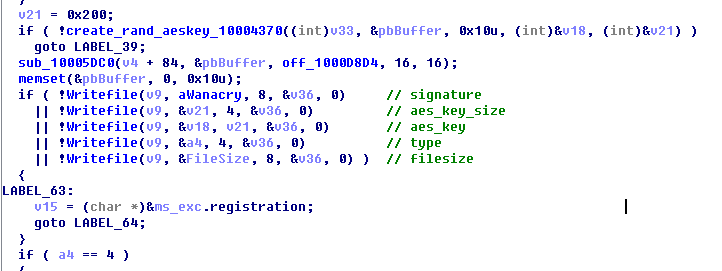
程序中内置两个RSA 2048公钥，用于加密，其中一个含有配对的私钥，用于演示能够解密的文件，另一个则是真正的加密用的密钥，程序中没有相配对的私钥



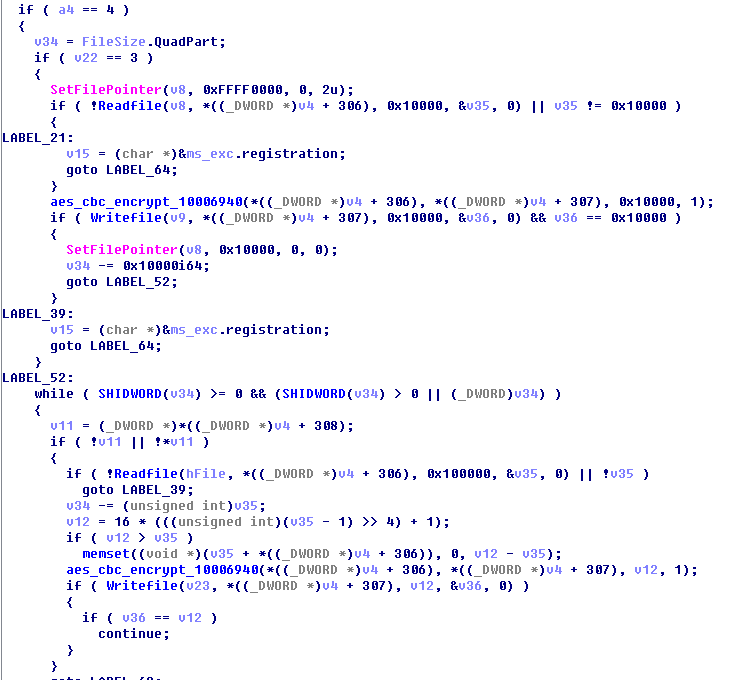
病毒随机生成一个256字节的密钥，并拷贝一份用RSA2048加密，RSA公钥内置于程序中



构造文件头，文件头中包含有标志、密钥大小、RSA加密过的密钥、文件大小等信息



使用CBC模式AES加密文件内容，并将文件内容写入到构造好的文件头后，保存成扩展名为.WNCRY的文件，并用随机数填充原始文件后再删除，防止数据恢复



完成所有文件加密后释放说明文档，弹出勒索界面，需支付价值数百美元不等的比特比到指定的比特比钱包地址，三个比特币钱包地址硬编码于程序中

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

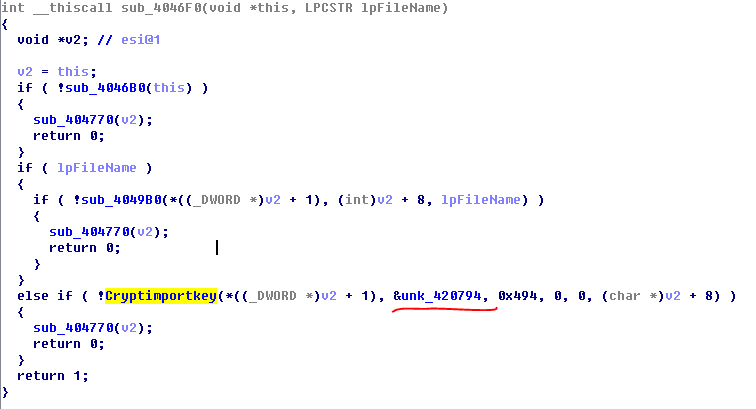
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

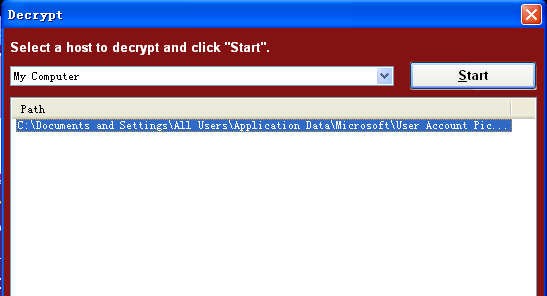
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94



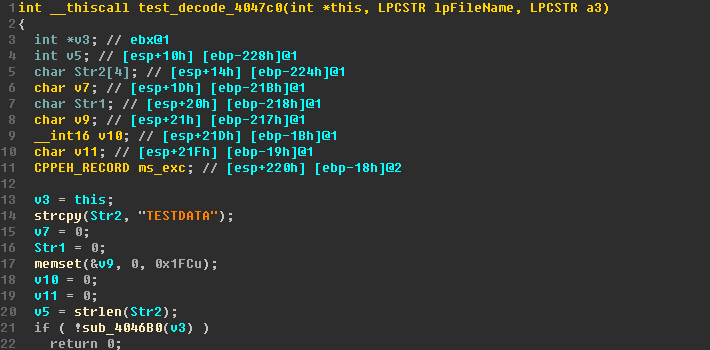
解密程序

病毒解密程序中内置了其中一个公钥的配对私钥，可以用于解密使用该公钥加密的几个文件，用于向用户“证明”程序能够解密文件，诱导用户支付比特币。

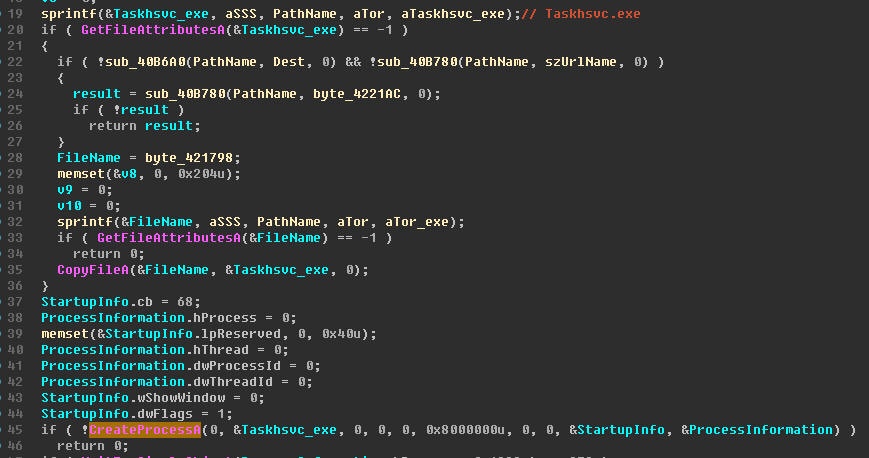




此后，程序判断本地是否存在“00000000.dky”文件，该文件为真实解密所需私钥文件。若存在，则通过解密测试文件来检测密钥文件是否正确。

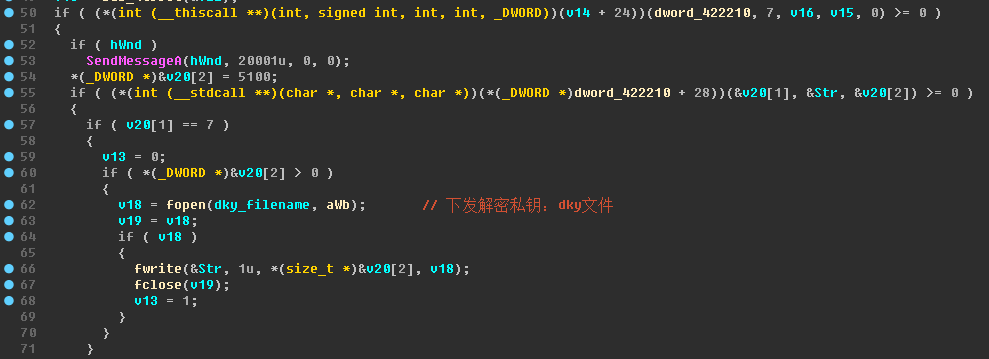


若正确，则解密，若错误或不存在，病毒将程判断解压后的Tor目录下是否存在taskhsvc.exe，若不存在，则生成该文件，并且调用CreateProcessA拉起该进程：



该程序主要为tor匿名代理工具，该工具启动后会监听本地9050端口，病毒通过本地代理通信实现与服务器连接。

在点击“Check Payment”按钮后，由服务端判断是否下发解密所需私钥。若私钥下发，则会在本地生成解密所需要的dky文件。



而后，程序便可利用该dky文件进行解密。不过，到目前为止，未曾有解密成功的案例。

文件列表及作用

b.wnry: 中招敲诈者后桌面壁纸

c.wnry: 配置文件，包含洋葱域名、比特币地址、tor下载地址等

r.wnry: 提示文件，包含中招提示信息

s.wnry: zip文件，包含Tor客户端

t.wnry: 解密后得到加密程序所需的dll文件

u.wnry: 解密程序（敲诈者主界面）

f.wnry: 可免支付解密的文件列表

WNCYRT：加密过程中生成的，有的被随机擦写过、有的是原文件、有的只对文件头进行了处理

WNCRY：加密后的文件

Wanacry加解密过程深入分析

勒索软件一个核心重点是其加解密过程，接下来我们对加解密和擦写逻辑进行详细分析。

文件加密

A. 文件是使用AES进行加密的。   
B. 加密文件所使用的AES密钥（AESKEY）是随机生成的，即每个文件所使用的密钥都是不同的。   
C. AESKEY通过RSA加密后，保存在加密后文件的文件头中。   
D. 敲诈者会根据文件类型、大小、路径等来判断文件对用户的重要性，进而选择对重要文件的先行进行加密并擦写原文件，对认为不太重要的文件，仅作删除处理。

文件删除及擦写逻辑

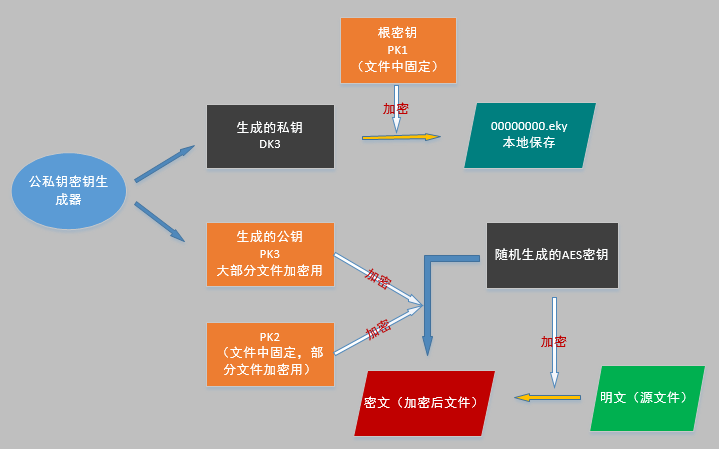
A. 对于桌面、文档、所有人\桌面、所有人\文档四个文件夹下小于200M的文件，均进行加密后擦写原文件。   
B. 对于其他目录下小于200M的文件，不会进行擦写，而是直接删除，或者移动到back目录（C盘下的“%TEMP%”文件夹，以及其他盘符根目录下的“$RECYCLE”文件夹）中。   
C. 移动到back后，的文件重命名为%d.WNCRYT，加密程序每30秒调用taskdl.exe对back目录下的这些文件定时删除。   
D. 对于大于200M的文件，在原文件的基础上将文件头部64KB移动到尾部，并生成加密文件头，保存为“WNCRYT”文件。而后，创建“WNCRY”文件，将文件头写入，进而按照原文件大小，对该“WNCRY”文件进行填充。

文件擦写方案

A. 先重写尾部1k。   
B. 判断大小后重写尾部4k。   
C. 从文件头开始每256k填充一次。   
D. 填写的内容为随机数或0x55。

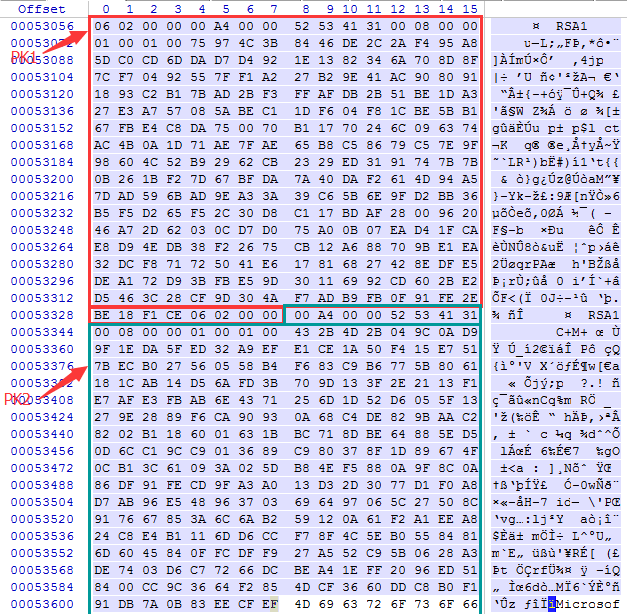
详细加密流程

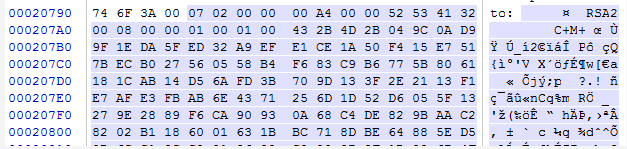
  总结密钥及加密关系大致如下：



A. 程序加密过程中，动态加载的dll里含有两个公钥（KEYBLOB格式），这里分别记为PK1和PK2。

其中PK2用于加密部分文件的AESKEY，并将该部分加密文件的路径存放在f.wnry中，这些文件是可以直接解密的（DK2也存在与可执行文件中）。

而PK1用于加密DK3（见后文介绍）。   


B. 解密程序u.wnry（即界面程序@WanaDecryptor@.exe）中包含有一个私钥（KEYBLOB格式），该私钥与PK2配对，记为DK2。该DK2用于解密f.wnry中记录的文件。   


C. 程序在每次运行时，会随机生成一组公私钥，用于。记为PK3、DK3。其中PK3保存在本地，主要用于加密各文件加密时随机生成的AESKEY。而DK3则由PK1加密后保存在本地，文件名为00000000.eky。

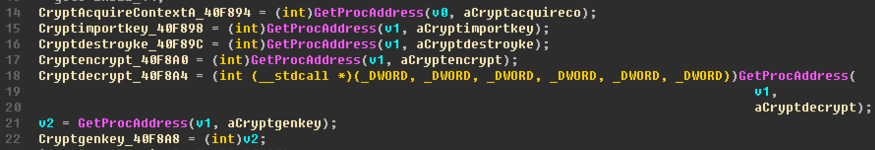
解密过程

A. f.wnry中记录的文件，主要使用DK2完成解密。   
B. 其余文件若需要解密，则需点击check payment后，通过Tor将本地00000000.eky、00000000.res文件信息上传到服务端，由服务端使用作者自己保存的DK1解密后，下发得到DK3，本地保存为00000000.dky。

C. 得到DK3后，即可完成对磁盘中其余文件的解密。

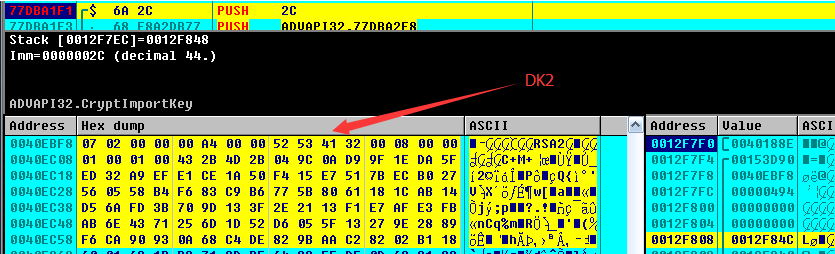
分析及调试验证

  将tasksche.exe拖到ida里可以发现，其加解密用到的是系统自带API，通过GetProcAddress来获取地址动态调用的。

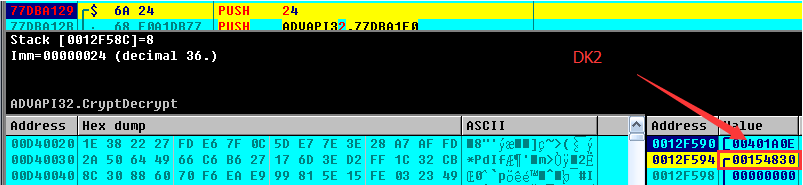
  
  于是，就可以以此为突破口来进行分析。

密钥分发过程

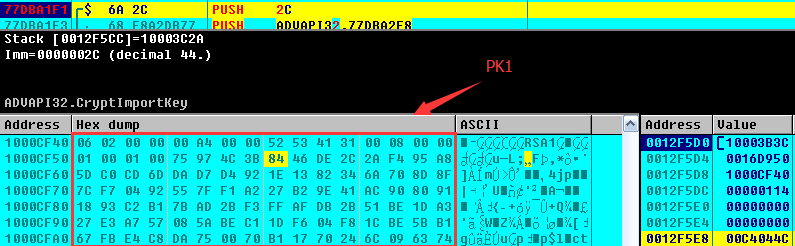
1、导入密钥DK2，存放于00154830



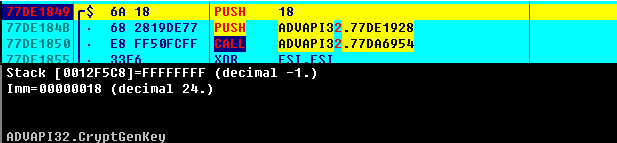
2、解密t.wnry

  
解密得到的t.wnry实则为一个DLL文件，该文件负责文件加密操作。

3、DLL线程导入PK1，存放于0016BE18

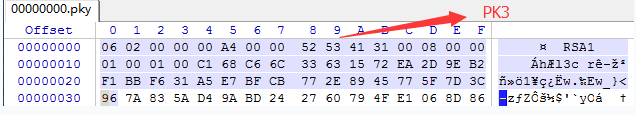


4、生成PK3、DK3

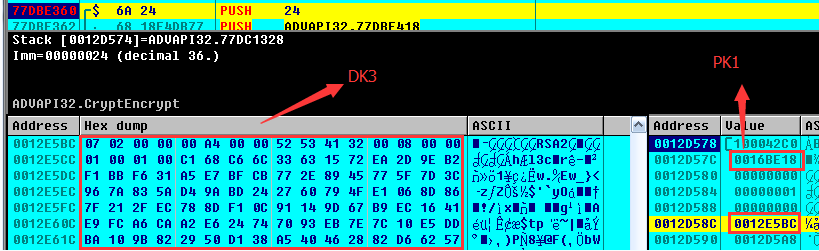


5、导出PK3

  
导出后，会调用writefile在本地生成00000000.pky。

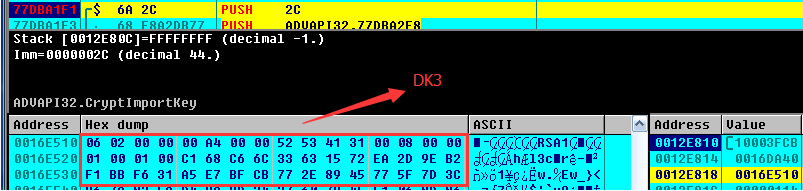


6、使用PK1加密DK3

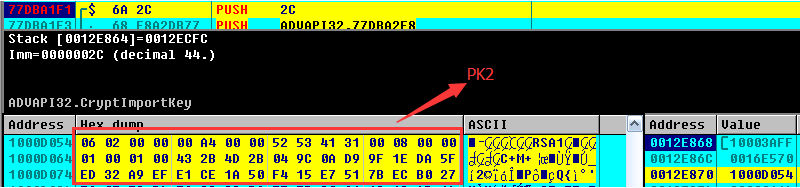
  
由上图可以匹配PK3和DK3。加密后，会调用writefile在本地生成00000000.eky。   
  至此，验证了密钥生成关系。

文件加密

1、导入PK3，放到0016D950

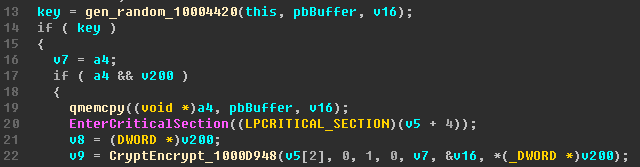


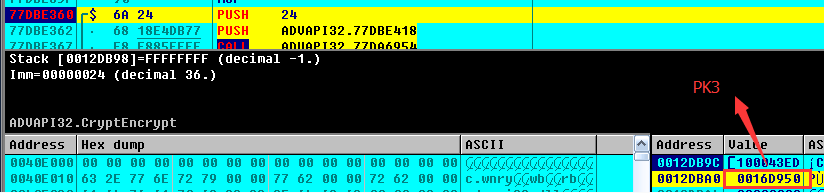
2、导入PK2，放到0016E510



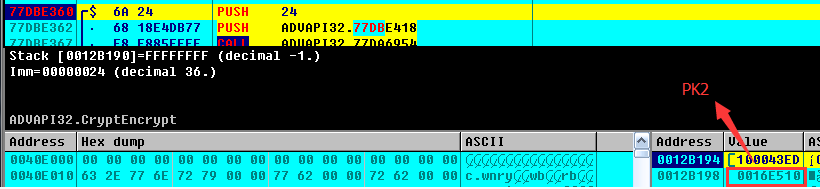
3、生成AESKEY，并使用PK3加密

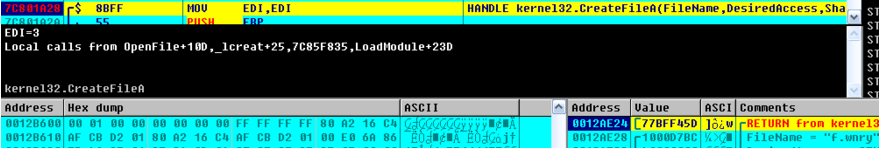
生成随机AESKEY：

  
使用PK3加密：

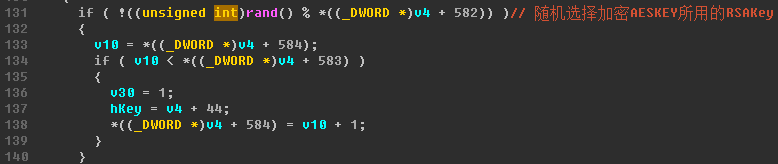


4、使用PK2加密

  
使用PK2加密后的文件，会写入f.wnry中：

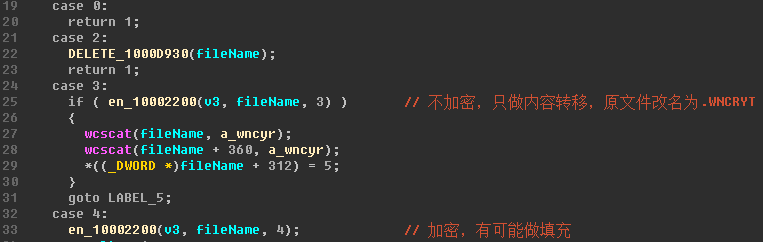


选择使用PK2还是PK3，是随机的：



文件删除和擦写条件

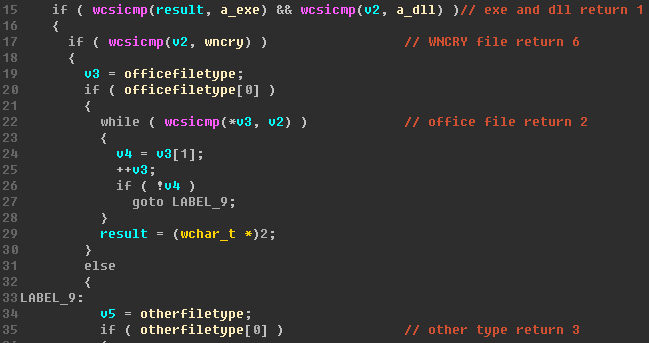
  调试时发现，敲诈者会对一些特定的文件再加密后对原文件进行擦写（填充随机数，为了防止数据回复）。操作首先找到擦写文件的逻辑，可以知道要擦写文件，有两个必要条件：

1、传入的this+902即back目录必须不为空。   
http://slab.qq.com/uploads/image/20170519/20170519120257_42053.png  
2、传入给上层函数的参数a4，需要等于4。   
http://slab.qq.com/uploads/image/20170519/20170519120314_54736.png  
往上层函数追溯，发现，该参数来自于函数10002940。   
分别有3和4，两个参数：   


  而再往上层，该参数取决于函数10002E70。  
通过分析，得知该函数逻辑如下，会对文件列表做四部处理：

第一步：对文件类型为类型一（见后文）进行处理，做大小判断，大于200M返回3，小于1k返回1，其余大小则返回4。类型二的文件，均返回1。   
第二步：对剩余文件中，所有类型一的文件均返回1。而对其他类型文件，做大小判断，大于200M的文件返回3，大于1k小于200M的文件返回4，小于1k的文件返回1。   
第三步：对剩余文件，返回4。   
第四步：对wncryt文件，返回2，wncyr、exe、dll文件，返回1。

至于为什么要这么做，可能是考虑擦写效率问题，为了尽可能多的加密、擦写文件，耗时的文件、小于1k不重要的文件最后处理。其中，返回为1的，不做处理；返回为2的，做删除处理；返回为3的：生成加密文件头，而后做文件头转移处理，创建为“WNCRYT”文件，而后生成假的加密文件“WNCRY”，往里填充随机数；返回为4的，做完整文件加密处理。   
  其中判断文件类型的代码在：

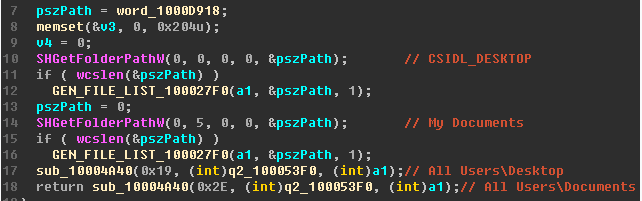
  
类型一：

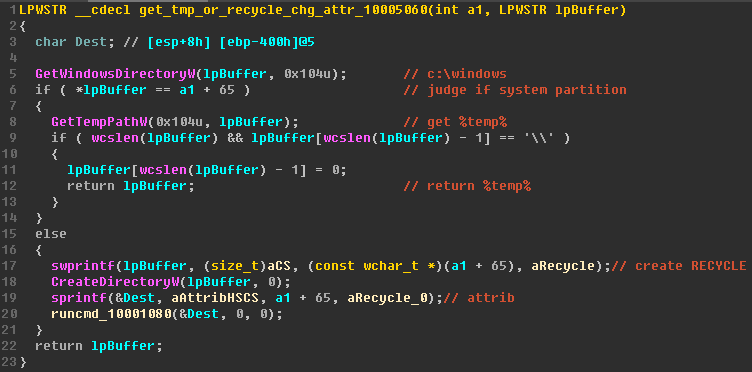
doc、docx、xls、xlsx、ppt、pptx、pst、msg、、vsd、vsdx、txt、csv、rtf、123、wks、wk1、pdf、dwg、onetoc2、snt、jpeg、jpg

类型二：

docb、docm、dot、dotm、dotx、xlsm、xlsb、xlw、xlt、xlm、xlc、xltx、xltm、pptm、pot、pps、ppsm、ppsx、ppam、potx、potm、edb、hwp、602、sxi、sti、sldx、sldm、sldm、vdi、vmdk、vmx、gpg、aes、arc、paq、bz2、tbk、bak、tar、tgz、gz、7z、rar、zip、backup、iso、vcd、bmp、png、gif、raw、cgm、tif、tiff、nef、psd、ai、svg、djvu、m4u、m3u、mid、wma、flv、3g2、mkv、3gp、mp4、mov、avi、asf、mpeg、vob、mpg、wmv、fla、swf、wav、mp3、sh、class、jar、java、rb、asp、php、jsp、brd、sch、dch、dip、pl、vb、vbs、ps1、bat、cmd、js、asm、h、pas、cpp、c、cs、suo、sln、ldf、mdf、ibd、myi、myd、frm、odb、dbf、db、mdb、accdb、sql、sqlitedb、sqlite3、asc、lay6、lay、mml、sxm、otg、odg、uop、std、sxd、otp、odp、wb2、slk、dif、stc、sxc、ots、ods、3dm、max、3ds、uot、stw、sxw、ott、odt、pem、p12、csr、crt、key、pfx、der

  如此，第二个条件已理清楚，剩下第一个，在分析时发现：程序运行后，首先对桌面、文档、所有人\桌面、所有人\文档四个文件夹进行处理。

  
  而对这几个文件夹处理的时候，back目录为空。对其他目录进行处理的时候，会进行判定：

  
即：

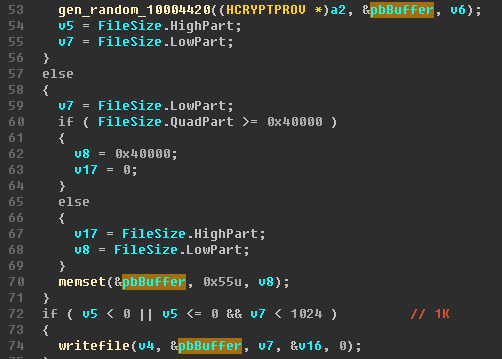
1、处理C盘其他目录时，back目录为%temp%   
2、处理其他盘符时，back目录为各盘符下的回收站目录，若回收站不存在，则创建

  由此，可以得到整体逻辑如下：

1、对于桌面、文档、所有人\桌面、所有人\文档四个文件夹下的文件，文件类型为类型一、类型二的文件，大小小于200M的，均进行加密后擦写原文件，大于200M的文件不做加密也不做擦写操作，仅作转移文件头处理，后生成随机数填充的WNCRY文件。   
2、对于其他目录下文件：由于back目录不为空，不会对原文件进行擦写，而是直接删除，或者移动到back目录中。移动到back后，的文件命名为%d.WNCRYT，程序taskdl.ext会对back目录下的这些文件定时删除。同样，大于200M的文件不做加密也不做擦写操作，仅作转移文件头处理。

文件擦写方式

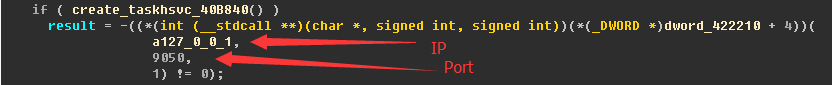
  擦写方式主要是对加密后的原文件进行重写。根据代码可知，其主要填充数据有两种：随机数、0x55。

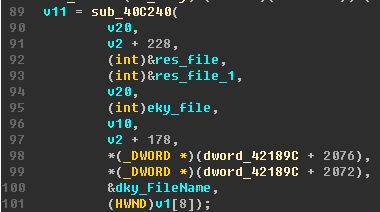
  
  而擦写过程为：

1、先重写尾部1k   
2、判断大小后重写尾部4k   
3、从文件头开始每256k填充一次

解密通信

  敲诈者会在Tor目录下释放并拉起taskhsvc.exe，该工具启动后会监听本地9050端口，病毒通过本地代理连接实现与Tor服务器的通信。

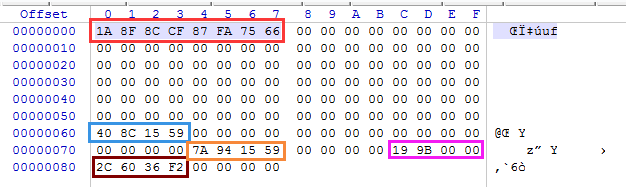
  
  在点击“Check Payment”按钮后，上传本地res和eky文件。

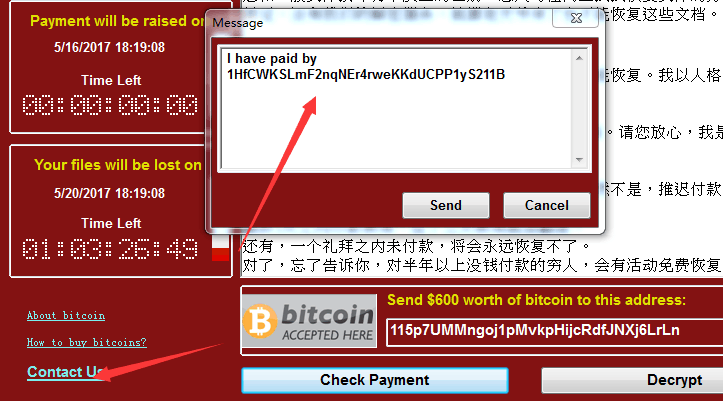
  
  若私钥下发，则会在本地生成解密所需要的dky文件。



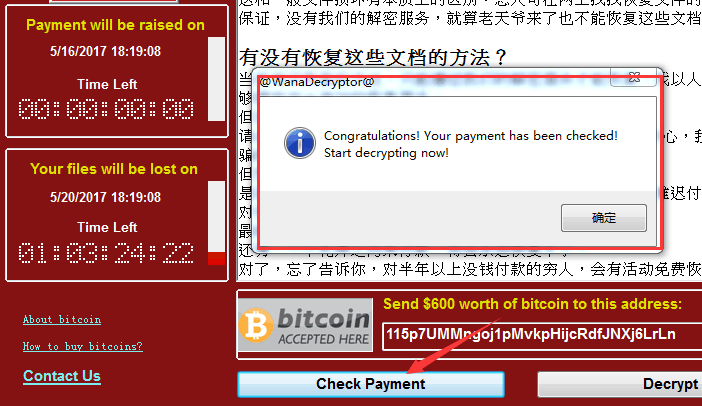
RES文件解析

  解密同时需要res文件和eky，就来分析一下res文件格式。通过分析，可得其格式大致如下：

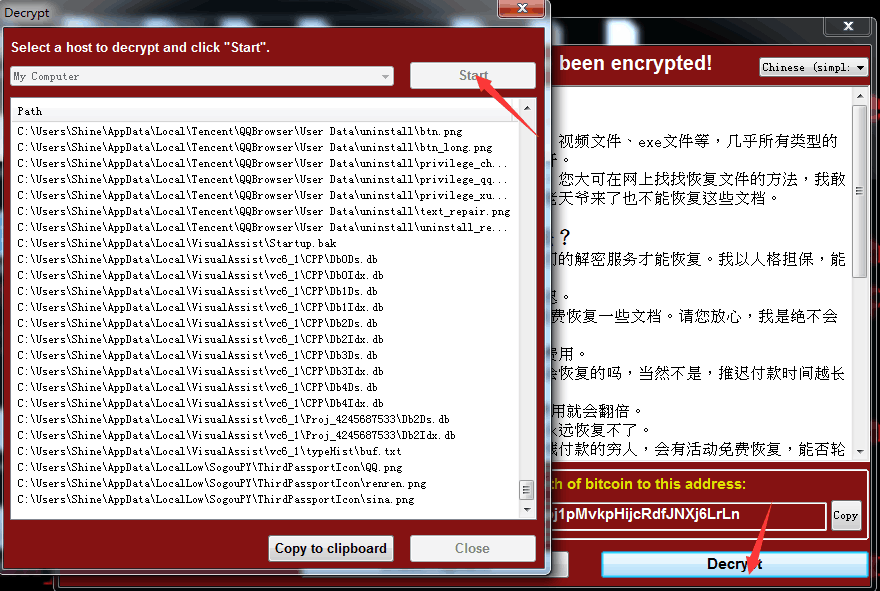
  
  红色框为八字节随机生成，应该是用于唯一性判定；蓝色框中为敲诈者首次运行时间，即首个文件加密时间；橘色框中为最后一个文件加密时间；紫色框中为加密文件总数；褐色框中记录的是加密文件总大小。   
  有这些信息后，作者应该可以初步对非正常用户进行排除。当然，具体如何判定，还不得而知。

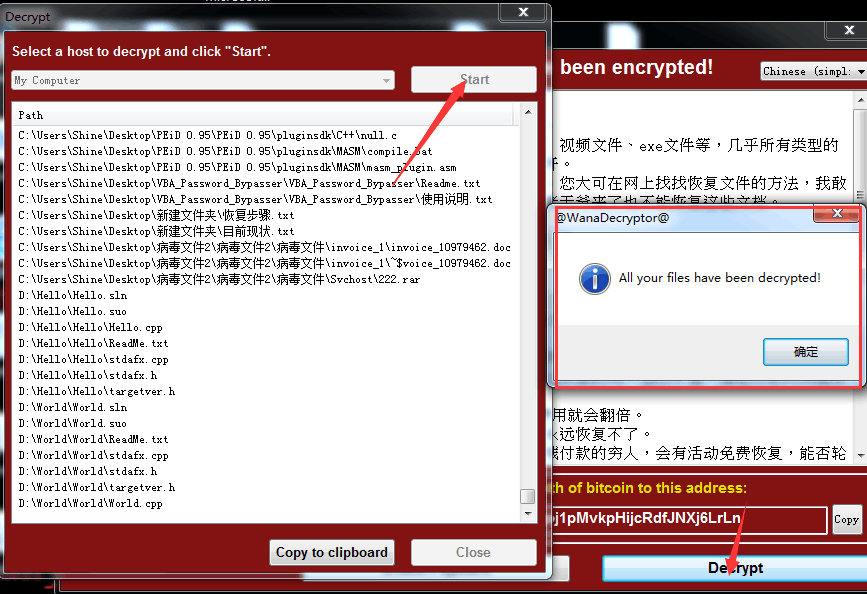


4，作者如果匿名网络在线，点击“check payment”会收到回复的确认消息，这个时候用于解密的密钥会通过匿名网络发送回来。



5，然后选择解密就可以解密文件了





6，解密完成后是仍然有可能重新中毒的，病毒并没有标签解密过的机器。