WannaCry

1."Kill Switch"就是紧急开关的意思。WannaCry勒索病毒此前发作的时候会向某个域名发出请求，如果该域名存在就会退出，不存在则继续攻击.

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

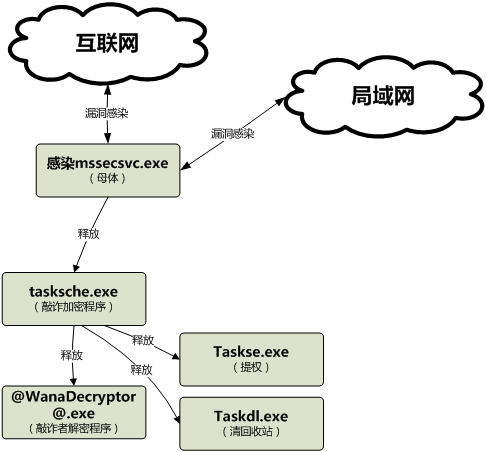
http://[www. ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com](http://www.freebuf.com/articles/system/134658.html)

2.ETERNALBLUE模块是SMB 漏洞利用程序，可以攻击开放了 445 端口的 Windows 机器，实现远程命令执行



3.当攻击者利用泄露的工具成功入侵目标机器后，会在目标机器对应的SMB端口植入一个名为DoublePulsar的后门程序。远程攻击者可以利用该后门向目标机器植入dll或者shellcode：

4.分析流程



(1)mssecsvc.exe

a、开关：

木马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](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。



(1)void \*memcpy(void\*dest, const void \*src, size\_t n);

功能

由src指向地址为起始地址的连续n个字节的数据复制到以dest指向地址为起始地址的空间内。

头文件

#include<string.h>

返回值

函数返回一个指向dest的指针。

(2)u是unsigned的意思，表示无符号数

(3)HINTERNET InternetOpen(   
　　\_In\_ LPCTSTR lpszAgent,   
　　\_In\_ DWORD dwAccessType,   
　　\_In\_ LPCTSTR lpszProxyName,   
　　\_In\_ LPCTSTR lpszProxyBypass,   
　　\_In\_ DWORD dwFlags   
　　);   
　　 lpszAgent   
　　指向一个 空结束的字符串，该字符串指定的应用程序或实体调用WinInet函数的名称。使用此名称作为用户代理的HTTP协议。   
　　 dwAccessType   
　　指定访问类型，参数可以是下列值之一：   
　　INTERNET\_OPEN\_TYPE\_DIRECT   
　　使用直接连接网络。   
　　INTERNET\_OPEN\_TYPE\_PRECONFIG   
　　获取代理或直接从注册表中的配置，使用代理连接网络。   
　　INTERNET\_OPEN\_TYPE\_PRECONFIG\_WITH\_NO\_AUTOPROXY   
　　获取代理或直接从注册表中的配置，并防止启动Microsoft JScript或Internet设置（INS）文件的使用。   
　　INTERNET\_OPEN\_TYPE\_PROXY   
　　通过代理的请求，除非代理旁路列表中提供的名称解析绕过代理,在这种情况下，该功能的使用。   
　　 lpszProxyName   
　　指针指向一个空结束的字符串，该字符串指定的代理服务器的名称，参数省略则为NULL。   
　　 lpszProxyBypass   
　　指向一个空结束的字符串，该字符串指定的可选列表的主机名或IP地址。如果 dwAccessType未设置为INTERNET\_OPEN\_TYPE\_PROXY的 ，参数省略则为NULL。   
　　 dwFlags   
　　参数可以是下列值之一：   
　　INTERNET\_FLAG\_ASYNC   
　　使异步请求处理的后裔从这个函数返回的句柄。   
　　INTERNET\_FLAG\_FROM\_CACHE   
　　不进行网络请求，从缓存返回的所有实体，如果请求的项目是不是在缓存中，一个合适的错误，如ERROR\_FILE\_NOT\_FOUND，则返回。   
　　INTERNET\_FLAG\_OFFLINE   
　　不进行网络请求，从缓存返回的所有实体，如果请求的项目是不是在缓存中，一个合适的错误，如ERROR\_FILE\_NOT\_FOUND，被返回。

返回值

　　成功：返回一个有效的句柄，该句柄将由应用程序传递给接下来的WinINet函数。   
　　失败：返回NULL。

(4)HINTERNET InternetOpenUrl

（ HINTERNET hInternet ，

LPCTSTR lpszUrl ，

LPCTSTR lpszHeaders ，

DWORD dwHeadersLength ，

DWORD dwFlags ，

DWORD\_PTR dwContext）

通过一个完整的FTP，[Gopher](http://baike.baidu.com/item/Gopher/611108" \t "http://baike.baidu.com/_blank)或HTTP网址打开一个资源。

hInternet

当前的 Internet 会话句柄。句柄必须由前期的 InternetOpen 调用返回。

lpszUrl

一个空[字符](http://baike.baidu.com/item/%E5%AD%97%E7%AC%A6" \t "http://baike.baidu.com/_blank)结束的字符串变量的[指针](http://baike.baidu.com/item/%E6%8C%87%E9%92%88" \t "http://baike.baidu.com/_blank)，指定读取的网址。只有以ftp:, gopher:, http:, 或者 https: 开头的网址被支持。

lpszHeaders

一个空字符结束的字符串变量的指针，指定发送到HTTP服务器的头信息。欲了解更多信息，请参阅[HttpSendRequest](http://baike.baidu.com/item/HttpSendRequest/8253338" \t "http://baike.baidu.com/_blank)函数里lpszHeaders参数的说明。

dwHeadersLength

dwFlags

此参数可为下列值之一。

数值 说明

INTERNET\_FLAG\_EXISTING\_CONNECT

如果使用相同的必须属性[创建会话](http://baike.baidu.com/item/%E5%88%9B%E5%BB%BA%E4%BC%9A%E8%AF%9D" \t "http://baike.baidu.com/_blank)，会尝试利用现有的InternetConnect对象。这只对FTP操作非常有用，因为FTP是唯一在同一会话中执行多种操作的协议。WinINet API 为每个由[InternetOpen](http://baike.baidu.com/item/InternetOpen/5138586" \t "http://baike.baidu.com/_blank)产生的HINTERNET句柄缓冲一个单独链接句柄。InternetOpenUrl使用此标志的HTTP和FTP连接。

INTERNET\_FLAG\_HYPERLINK

当决定何时从网络[重载](http://baike.baidu.com/item/%E9%87%8D%E8%BD%BD" \t "http://baike.baidu.com/_blank)时，如果服务器没有返回 Expires time 和 LastModified，那么强制重载。

INTERNET\_FLAG\_IGNORE\_CERT\_CN\_INVALID

停用检查从服务器对必须的[主机](http://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)名称返回的SSL/PCT-based证书。 WinINet函数使用简单的比较匹配主机名称和[通配符](http://baike.baidu.com/item/%E9%80%9A%E9%85%8D%E7%AC%A6" \t "http://baike.baidu.com/_blank)的规则检查证书。

INTERNET\_FLAG\_IGNORE\_CERT\_DATE\_INVALID

停用检查的SSL/PCT-based的证书的适当的有效日期。

INTERNET\_FLAG\_IGNORE\_REDIRECT\_TO\_HTTP

禁用检测这中特殊的[重定向](http://baike.baidu.com/item/%E9%87%8D%E5%AE%9A%E5%90%91/9064196" \t "http://baike.baidu.com/_blank)。当使用此标志， WinINet 透明允许从HTTPS到HTTP URL的重定向。

INTERNET\_FLAG\_IGNORE\_REDIRECT\_TO\_HTTPS

禁用检测这中特殊的重定向。当使用此标志， WinINet 透明的允许的HTTP到HTTPS URL的重定向。

INTERNET\_FLAG\_KEEP\_CONNECTION

如果可能的话，为连接使用保活语义。这个标志要求微软网络（ MSN ），[NTLM](http://baike.baidu.com/item/NTLM/6371298" \t "http://baike.baidu.com/_blank)和其他类型的身份验证。

INTERNET\_FLAG\_NEED\_FILE

如果要创建的文件不能被[缓存](http://baike.baidu.com/item/%E7%BC%93%E5%AD%98" \t "http://baike.baidu.com/_blank)，创建[临时文件](http://baike.baidu.com/item/%E4%B8%B4%E6%97%B6%E6%96%87%E4%BB%B6/3359209" \t "http://baike.baidu.com/_blank)。

INTERNET\_FLAG\_NO\_AUTH

不试图自动验证。

INTERNET\_FLAG\_NO\_AUTO\_REDIRECT

不自动处理[HttpSendRequest](http://baike.baidu.com/item/HttpSendRequest/8253338" \t "http://baike.baidu.com/_blank)中的[重定向](http://baike.baidu.com/item/%E9%87%8D%E5%AE%9A%E5%90%91/9064196" \t "http://baike.baidu.com/_blank)。

INTERNET\_FLAG\_NO\_CACHE\_WRITE

不添加返回实体到缓存。

INTERNET\_FLAG\_NO\_COOKIES

不会自动添加的Cookie头到请求，并且不自动添加返回的[cookie](http://baike.baidu.com/item/cookie/1119" \t "http://baike.baidu.com/_blank)到cookie数据库。

INTERNET\_FLAG\_NO\_UI

禁用Cookie的对话框。

INTERNET\_FLAG\_PASSIVE

使用被动FTP语义。InternetOpenUrl为FTP的文件和目录使用此标志。

INTERNET\_FLAG\_PRAGMA\_NOCACHE

即使代理中存在缓存副本，也强制要求由源服务器返回。

INTERNET\_FLAG\_RAW\_DATA

检索的[Gopher](http://baike.baidu.com/item/Gopher/611108" \t "http://baike.baidu.com/_blank)目录信息时，传回的数据作为GOPHER\_FIND\_DATA结构，如果检索的FTP目录信息时，作为一个[WIN32\_FIND\_DATA](http://baike.baidu.com/item/WIN32_FIND_DATA" \t "http://baike.baidu.com/_blank)结构。如果此标志没有指定，或者请求通过CERN代理创建， InternetOpenUrl返回的HTML版本的目录。

INTERNET\_FLAG\_RELOAD

从原服务器强制下载所要求的文件，对象，或目录列表，而不是从[缓存](http://baike.baidu.com/item/%E7%BC%93%E5%AD%98" \t "http://baike.baidu.com/_blank)下载。

INTERNET\_FLAG\_RESYNCHRONIZE

重新加载的HTTP资源，如果资源在最后一次下载后已被修改。所有FTP和Gopher资源将被[重载](http://baike.baidu.com/item/%E9%87%8D%E8%BD%BD" \t "http://baike.baidu.com/_blank)。

INTERNET\_FLAG\_SECURE

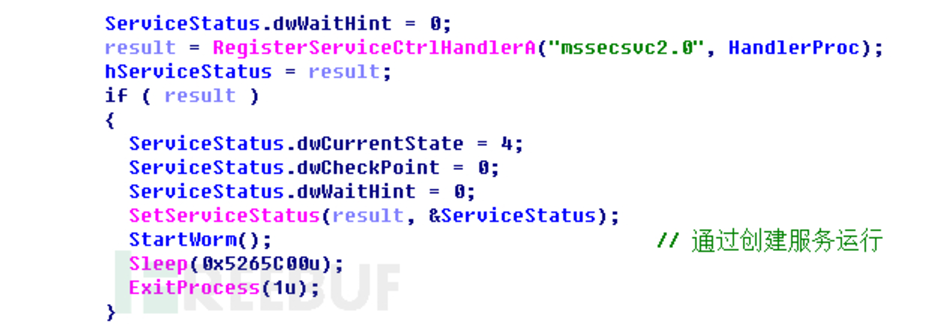
使用安全传输语义。这次传输使用安全套[字节](http://baike.baidu.com/item/%E5%AD%97%E8%8A%82" \t "http://baike.baidu.com/_blank)层/专用通信技术（的SSL / PCT ），这只有在[HTTP请求](http://baike.baidu.com/item/HTTP%E8%AF%B7%E6%B1%82/10882159" \t "http://baike.baidu.com/_blank)时有意义。

dwContext

一个指向一个应用程序定义的值，将随着返回的句柄，一起传递给[回调函数](http://baike.baidu.com/item/%E5%9B%9E%E8%B0%83%E5%87%BD%E6%95%B0" \t "http://baike.baidu.com/_blank)。

b、蠕虫行为：

通过创建服务启动，每次开机都会自启动。



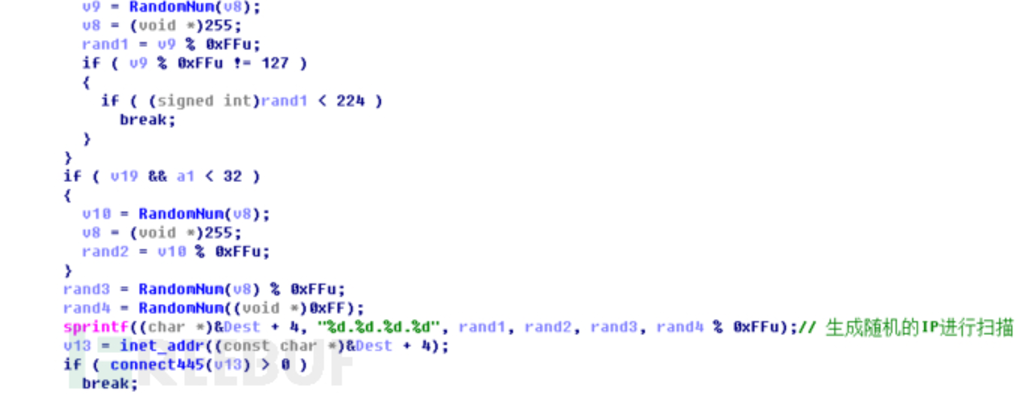
从木马自身读取MS17\_010漏洞利用代码，playload分为x86和x64两个版本。



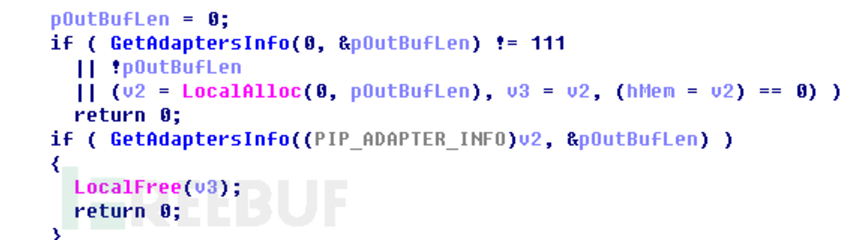
创建两个线程，分别扫描内网和外网的IP，开始进程蠕虫传播感染。



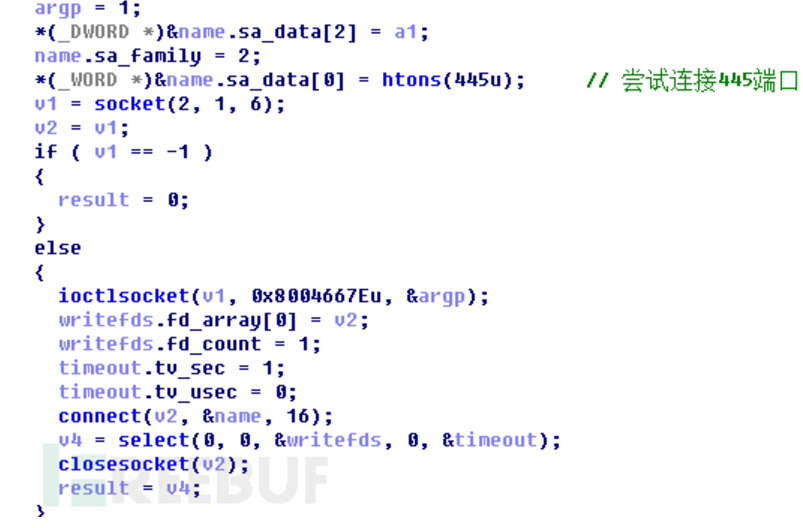
对公网随机ip地址445端口进行扫描感染。



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。



释放敲诈者

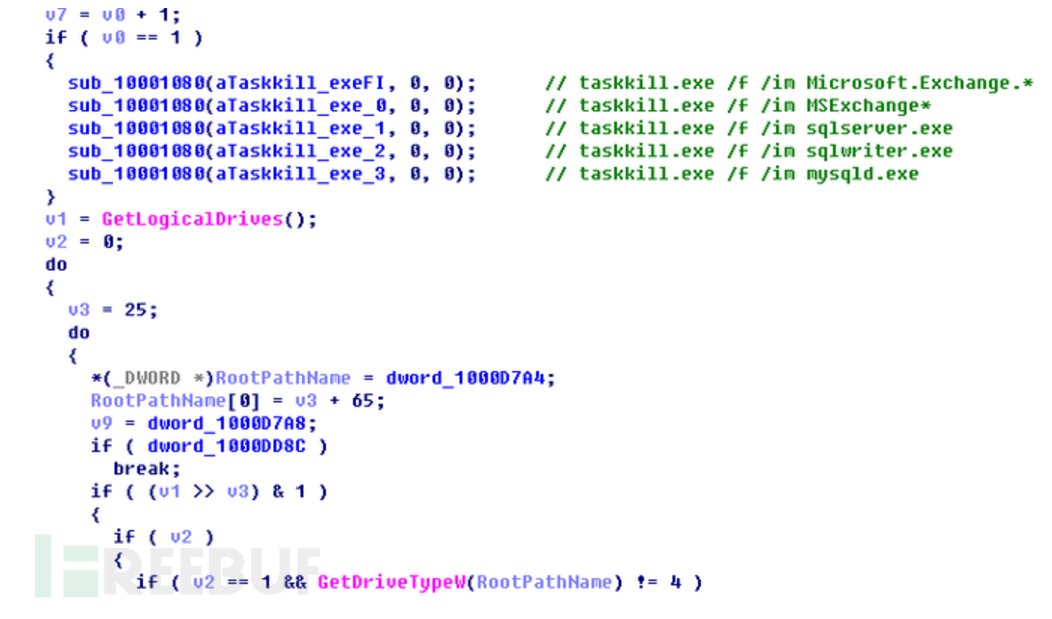


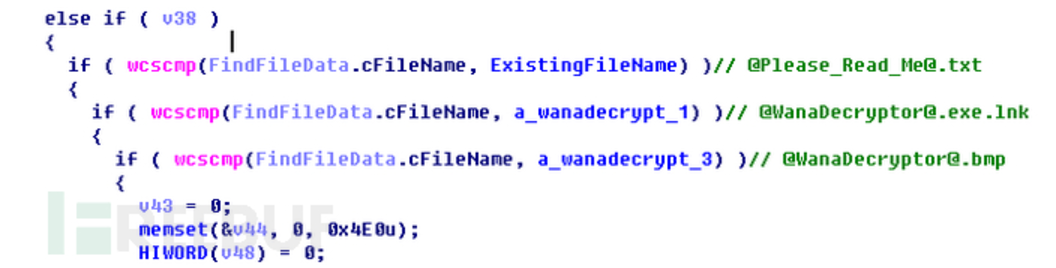
(2)tasksche.exe行为：（敲诈者）

解压释放大量敲诈者模块及配置文件，解压密码为WNcry@2ol7

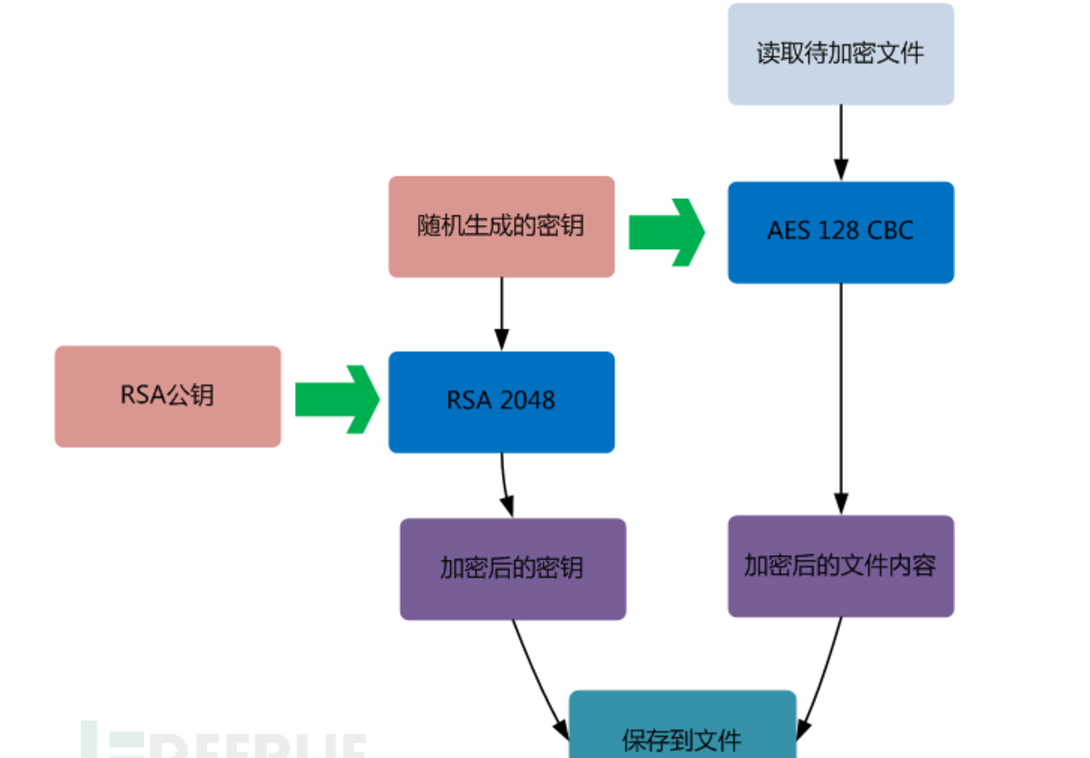


首先关闭指定进程，避免某些重要文件因被占用而无法感染。



遍历磁盘文件，避开含有以下字符的目录。同时，也避免感染木马释放出来的说明文档。

木马加密流程图：



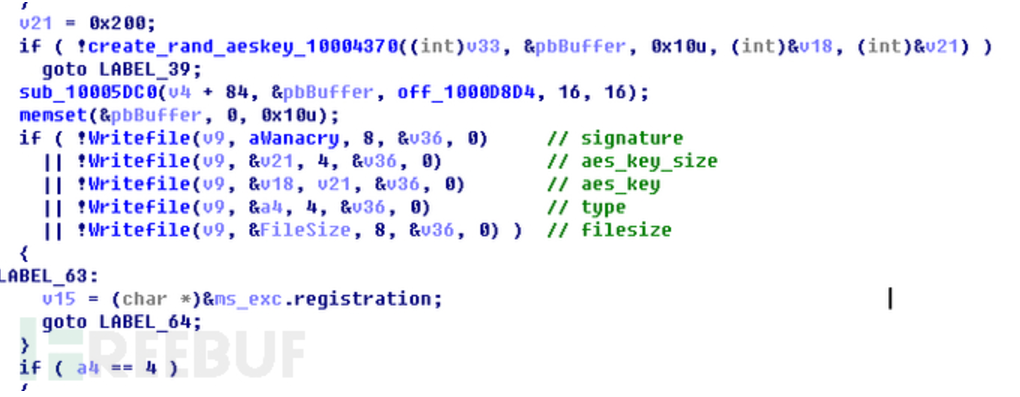
程序中内置两个RSA 2048公钥，用于加密，其中一个含有配对的私钥，用于演示能够解密的文件，另一个则是真正的加密用的密钥，程序中没有相配对的私钥。



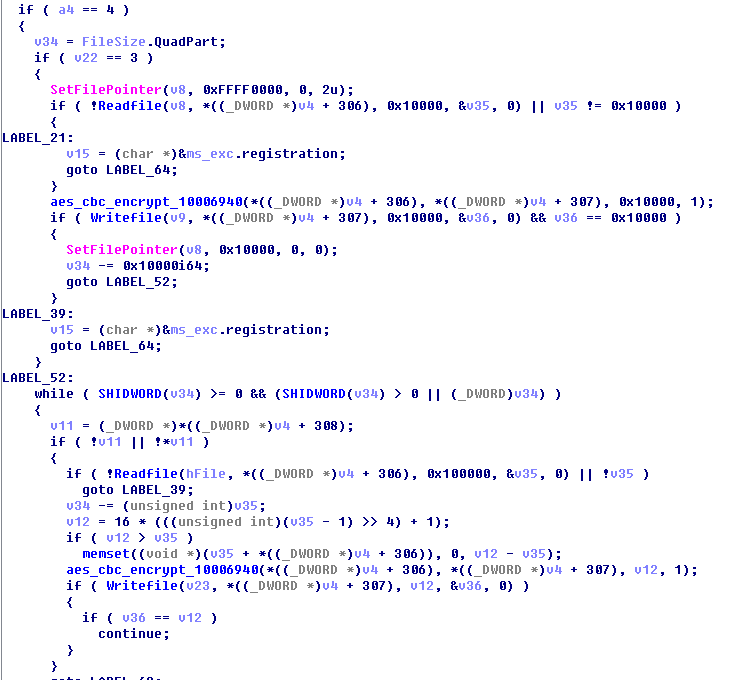
木马随机生成一个256字节的密钥，并拷贝一份用RSA2048加密，RSA公钥内置于程序中。



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

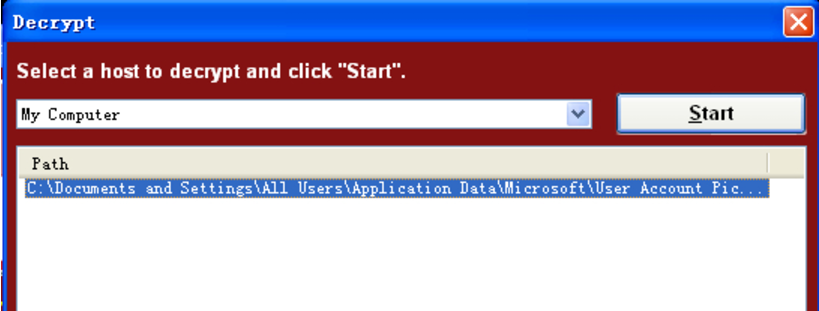
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

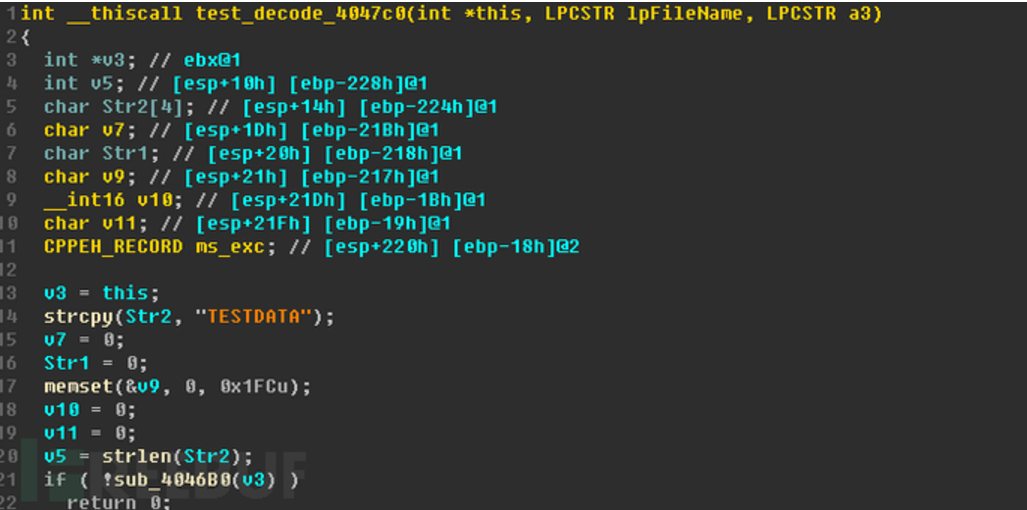
(3)解密程序：

木马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。

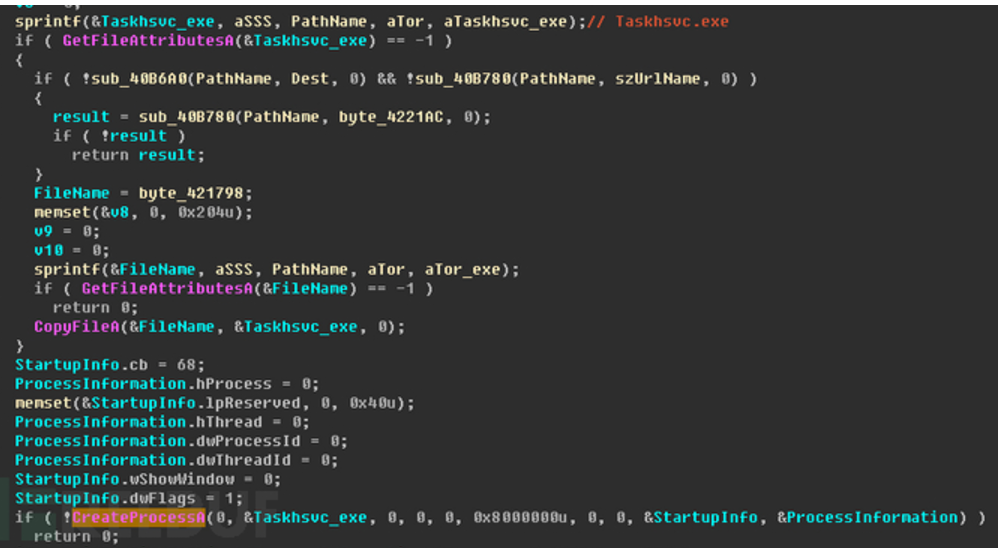




此后，程序判断本地是否存在“00000000.dky”文件，该文件为真实解密所需私钥文件。若存在，则通过解密测试文件来检测密钥文件是否正确。



若正确，则解密，若错误或不存在，木马将程判断解压后的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，木马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。

