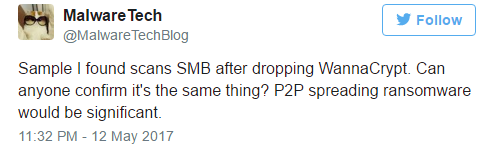
永恒之蓝（WannaCry）勒索蠕虫分析

## 事件时间线

1. **2017年5月12日**

Malware Tech在twitter上发布了一条通过SMB传播的勒索软件WannaCrypt，之后相关kill switch url被注册监管，之后该twitter作者编写了文章“How to Accidentally Stop a Global Cyber Attacks”，在该文章中记录了他是如何第一时间注意到这次攻击事件，并迅速做出相应的过程。



1. **2017年5月12日**

360发布紧急通告，对一种利用MS17-010进行传播勒索蠕虫进行了预警。



Malwarebytes发布相关分析的报告



思科talos intelligence发布相关的分析报告



同日英国大量医院感染WannaCry蠕虫。



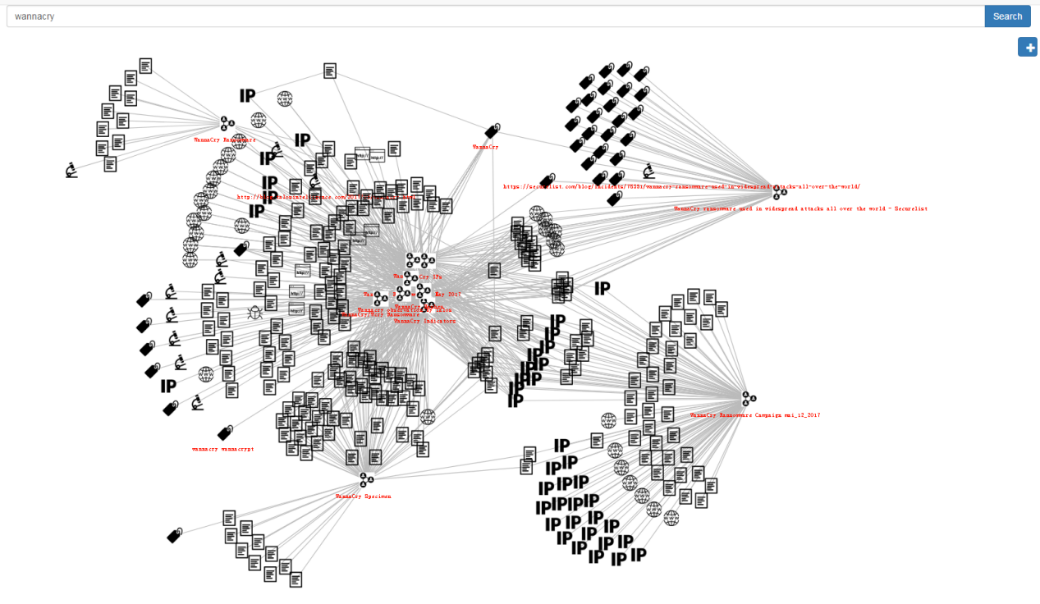
1. **2017年5月13日**

360发布对WannaCry勒索蠕虫的技术分析。



## 蠕虫变种监测

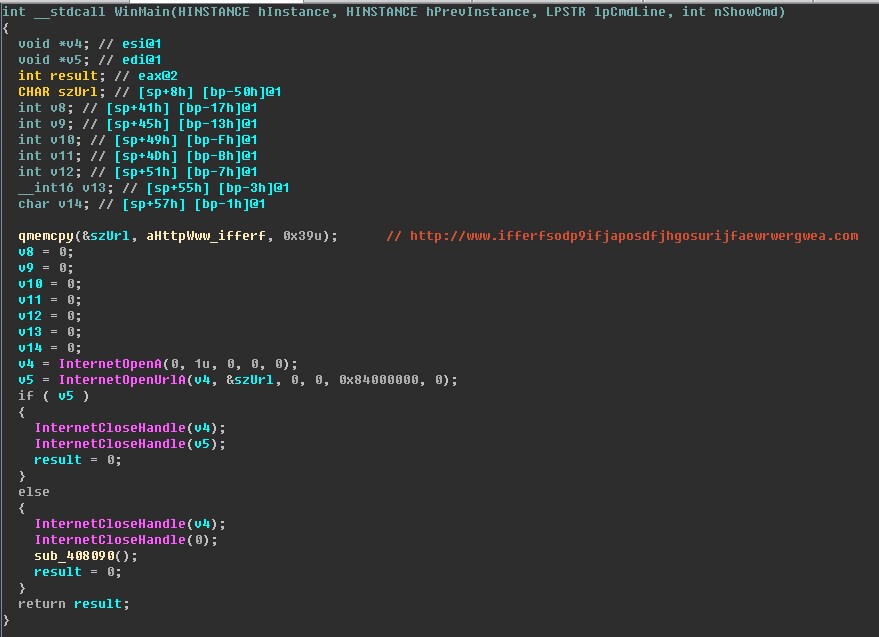
事件发生以来，包含360公司追日团队在内多家安全研究机构对蠕虫的技术细节做了详细分析，可见文后参考引用。在原始版本的蠕虫泛滥以后，360威胁情报中心观察到了大量基于修改的变种，数量达到数百个，在情报中心的图关联搜索中可以很直观地看到部分关联：



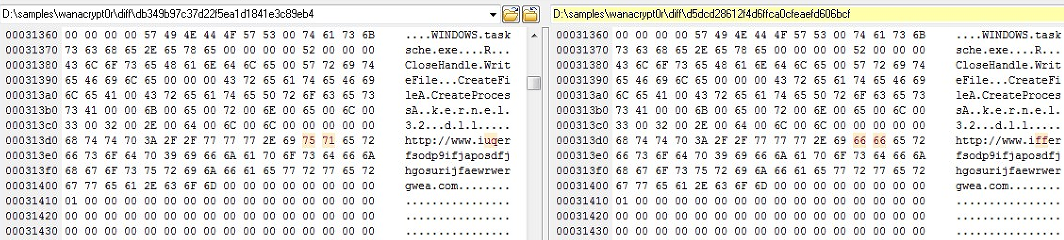
其中几个相对比较有特点的变种如下：

1. **d5dcd28612f4d6ffca0cfeaefd606bcf**

新版本变种和第一版差别不大，只是修改了一开始KILL SWITCH URL（修改为http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com），如下所示：



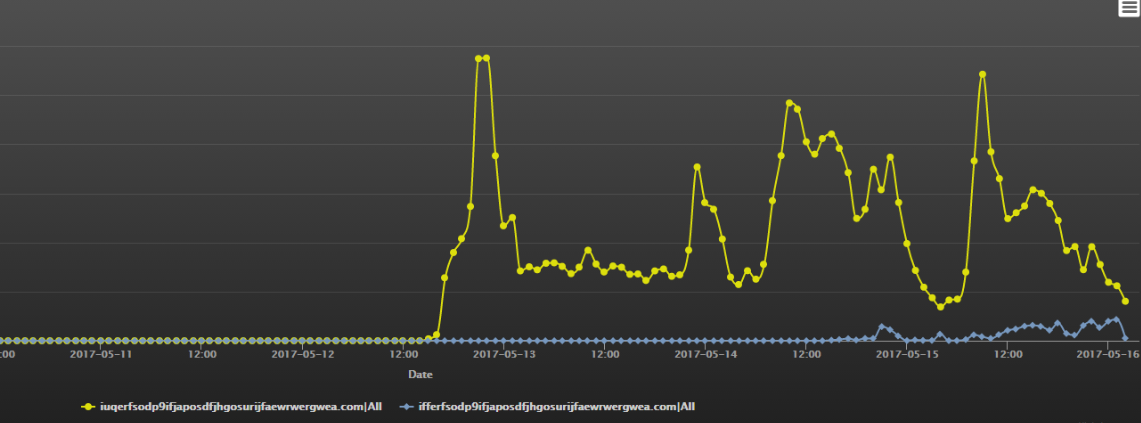
目前发现有多个变种采用了这种通过简单二进制Patch的方式修改开关域名，与原始版本相关，整个恶意代码只有域名部分的字节被修改：



我们看到部分样本及对应开关域名如下：

|  |  |  |
| --- | --- | --- |
| 样本 | Kill Switch | 备注 |
| 550ea639584fbf13a54eccdaa359d398 | http://www.udhridhfowhgibe9vheiviehfiehbfvieheifheih.com | 未监测到访问 |
| c2559b51cfd37bdbd5fdb978061c6c16 | http://www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com | 未监测到访问 |
| 0156edf6d8d35def2bf71f4d91a7dd22 | http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com |  |
| 61f75bb0c76fe332bccfb3383e5e0178 | http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com |  |
| 4287e15af6191f5cab1c92ff7be8dcc3 | http://www.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf.com | 未监测到访问 |
| dd7216f5cb34dcf9bd42879bd528eaf4 | http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.cum | 测试 |
| 6bb4ebf965016439ca452272ea8dcbf4 | https://twitter.com/msuiche/status/863730377642442752 | 测试 |
| 96dff36b5275c67e35097d77a120d0d4 | http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.testing | 测试 |

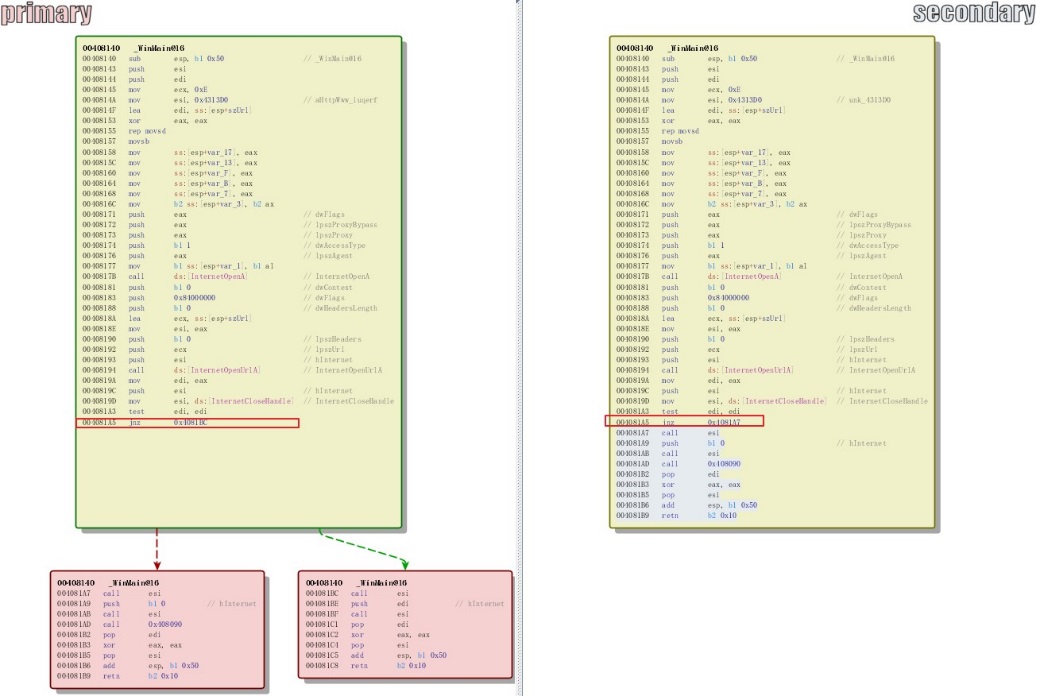
总体来说，由于随着系统漏洞的修补，这类样本对整体感染影响不大，下图是原始开关域名与其中一个修改后域名的解析量对比：



从上图还可以看到，开关域名对蠕虫的传播影响非常大，在域名被安全研究者注册形成有效解析和访问以后初始的指数级感染趋势很快被抑制，之后基本再也没有超过最早快速上升阶段形成的高峰。

1. **d724d8cc6420f06e8a48752f0da11c66**

样本通过对原始样本二进制Patch直接去除了检查开关域名以停止加密的功能，可以直接进入感染流程。下图为修改前后的比较：



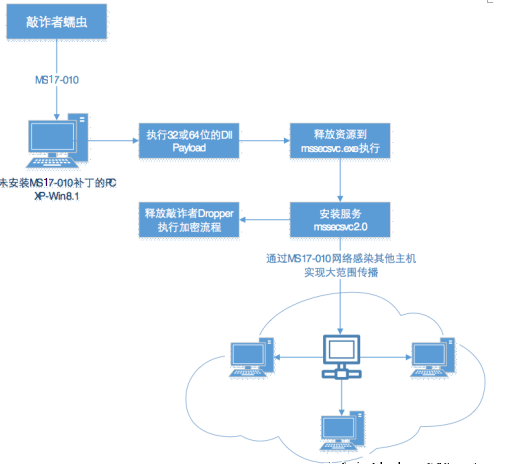
但是勒索的部分可能是由于作者疏忽，样本里硬编码的用于解压zip的密码还是WNcry@2ol7, 这个密码并不能解压成功，导致勒索流程被废掉了。接来下的变种可能会修复这个“Bug”，而使攻击的威胁程度大增。

360威胁情报中心会对出现的变种蠕虫做持续跟踪，更新进展。

## 原始蠕虫分析

作为补充，以下是360威胁情报中心对追日团队的技术分析报告基础上进行的分析确认，补充可能看到的一些细节。

样本为一个标准的网络蠕虫，通过MS17-010进行传播，不同于传统的蠕虫在于，该样本中附加了对应的勒索软件，以寻求利益的最大化，整体的感染流程如下所示：



样本运行之后会对内网，外网445端口进行扫描之后，通过MS17-010漏洞上传并执行payload进行传播，之后释放ransom样本，ransom执行初始化之后，再次释放对应的加密模块ransommodule对文件进行加密。

蠕虫整体分为三部分

Worm MD5：DB349B97C37D22F5EA1D1841E3C89EB4

Ransom MD5：84C82835A5D21BBCF75A61706D8AB549

RansomModule MD5：9849852166fe1d494496c1c5482498fd

**Worm**

**主体模块**

该部分为蠕虫的主体，样本运行之后会通过函数InternetOpenUrlA首先访问http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com这个地址，如果访问成功则放弃之后的运行，如下图所示，否则进入fun\_enterCry，即蠕虫的主流程，这个地方对于kill switch域名的作用，主要有以下两种解释：

1. 作者用于控制样本的传播开关（但是不幸的是该域名之后被以为安全研究员注册并接管）
2. 该域名用于检测蜜罐的认证（部分蜜罐环境会接管样本的网络流量，如HTTP访问都返回成功，因此通过一个不存在的域名来校验是否运行在蜜罐环境下）



进入fun\_enterCry之后通过判断参数的个数来执行相应的流程。

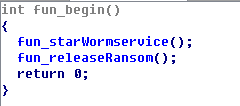
当参数<2，进入fun\_begin的安装流程。

当参数>=2，进入服务流程。



安装流程中通过函数fun\_starWormservice会创建一个服务mssecsvc2，参数为当前路径 –m security。

通过函数fun\_releaseRansom从资源中释放出Ramsom。

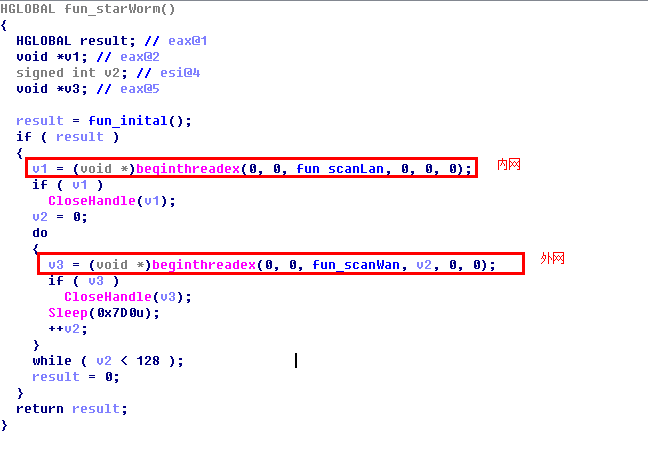


**扫描模块**

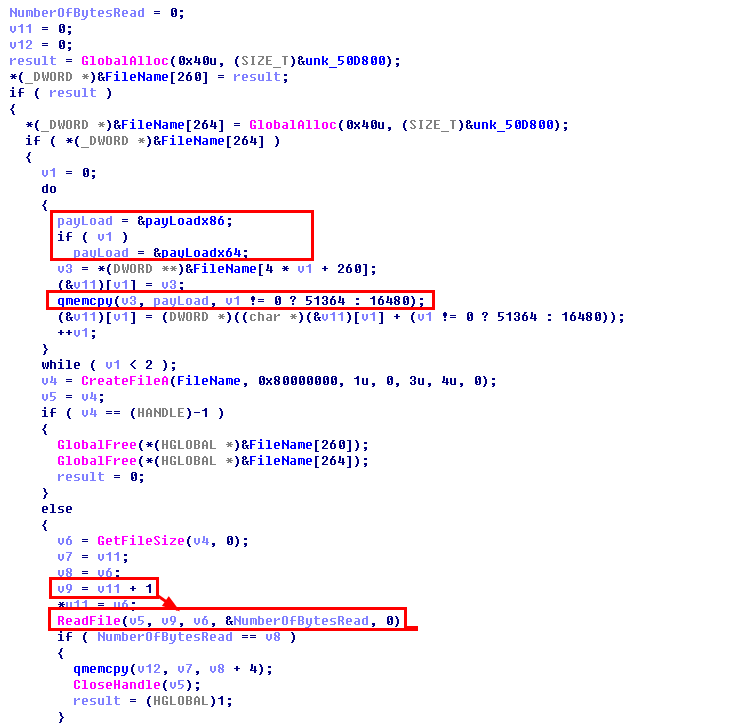
在服务流程中如下所示，首先在函数fun\_initial中实现初始化（网络和payload生成），之后生成线程对内外网进行扫描，

内网一个线程，扫描整个网段。

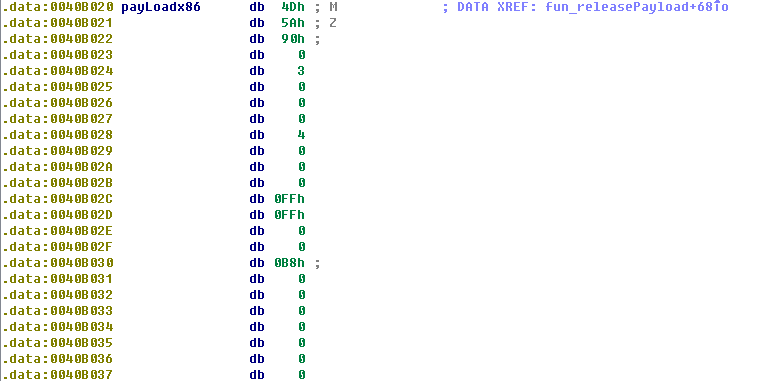
外网128个线程循环扫描随机生成的ip。



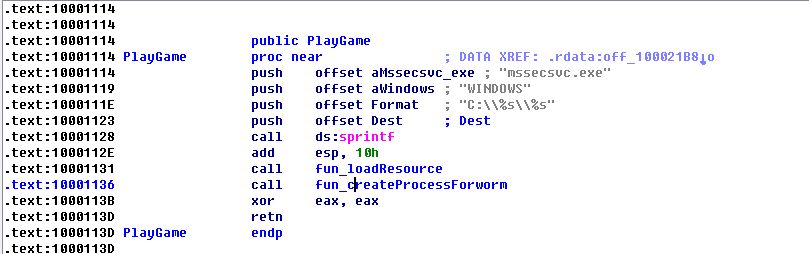
在fun\_initial中会调用函数用于生成对应的payload如下所示，分别在固定偏移根据平台获取x86或x64的payload，如下图所示实际上是拷贝到v11[]中，之后读取蠕虫本身并拷贝到payload后面因此整个载荷应该是payload+蠕虫的格式。



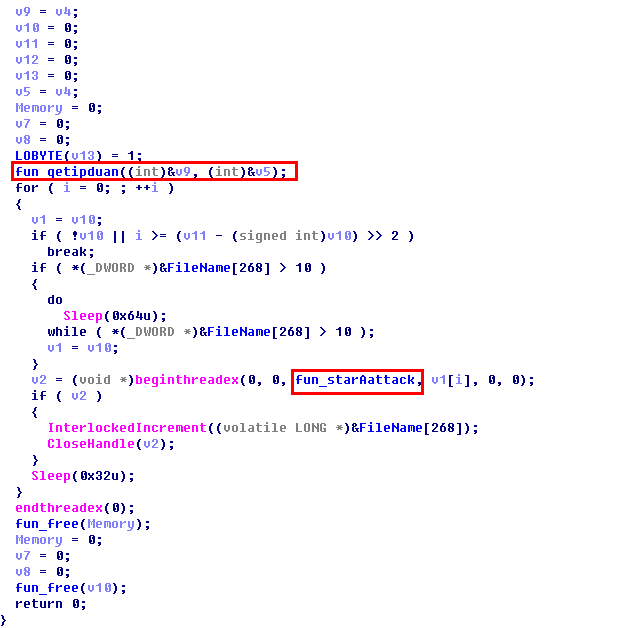
如下图所示为对应的payload的x86版本，可以看到这是一个pe文件。



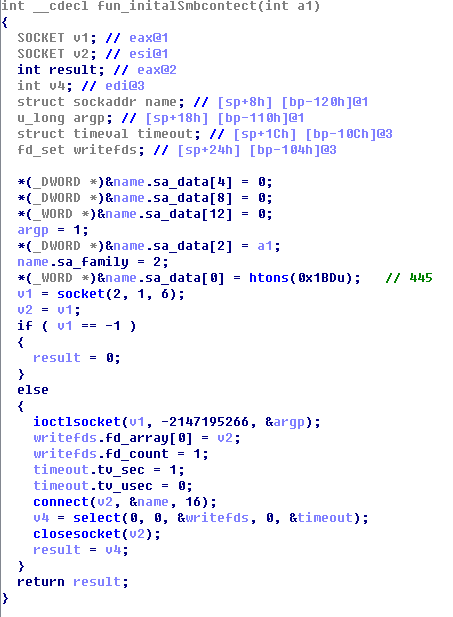
Dump出来可以看到该段代码就是一个单的loader，用于加载资源中的蠕虫。



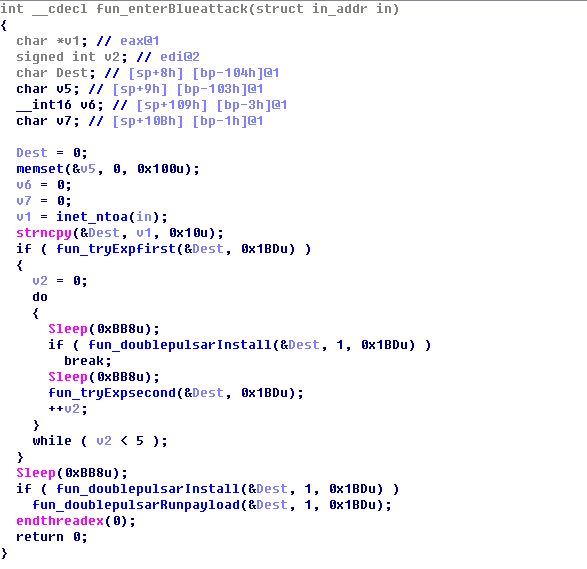
如下图所示为对应的内网感染代码的实现，通过函数fun\_getipduan获取当前ip段，针对每个ip通过函数fun\_starAttack发起一次攻击。



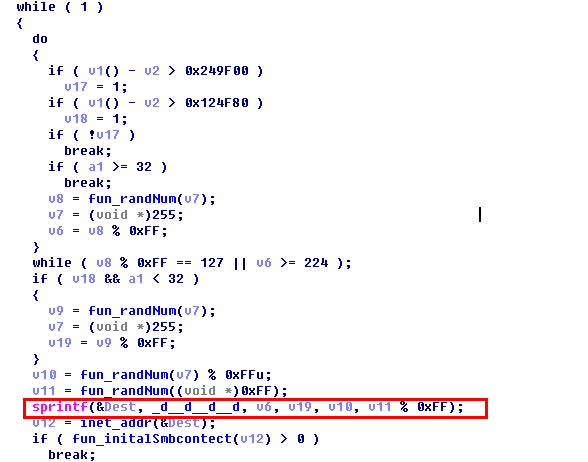
在fun\_starAttack中首先通过fun\_initalSmbcontect函数探测目标ip的445端口是否开启。



如果目标机器开启了445端口，则进入fun\_enterBlueattack，该函数中通过NSA泄露的enterblue实现远程攻击，并传播对应的蠕虫样本，如下所示通过fun\_tryExpfirst/second实现exploit，该次exploit之后会在目标机器中运行一段内核loader（接受来自doublespular上传的payload，并在user层运行），之后通过fun\_doublespularInstall，fun\_doubelspluarRunpayload将之前的payload上传并运行，这段payload被内核loader加载，并释放其中资源中的蠕虫运行。



下图为外网的情况下进行的扫描，此时通过随机生成ip进行攻击。



**Ransom释放**

扫描服务启动之后，样本中资源中先解压出对应的ransome，并移动当前 C:\WINDOWS\tasksche.exe到 C:\WINDOWS\qeriuwjhrf

释放自身的1831资源(MD5: 84C82835A5D21BBCF75A61706D8AB549),到C:\WINDOWS\tasksche.exe,并以 /i参数启动

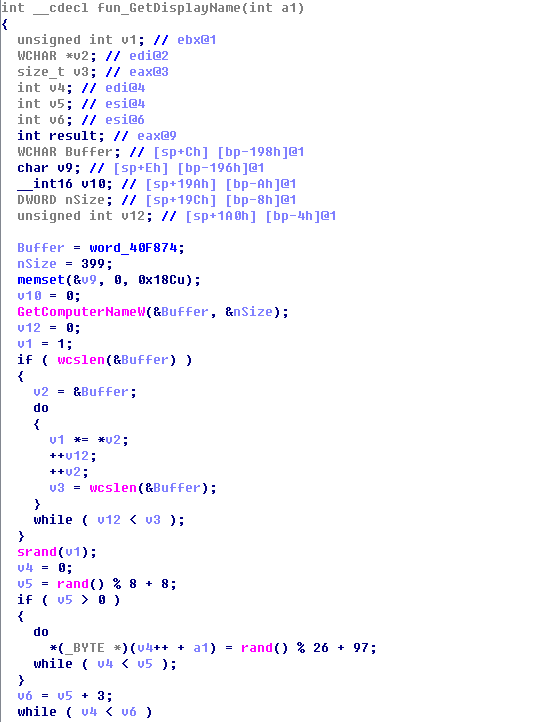


**Ransome**

Ransom整体流程如下：



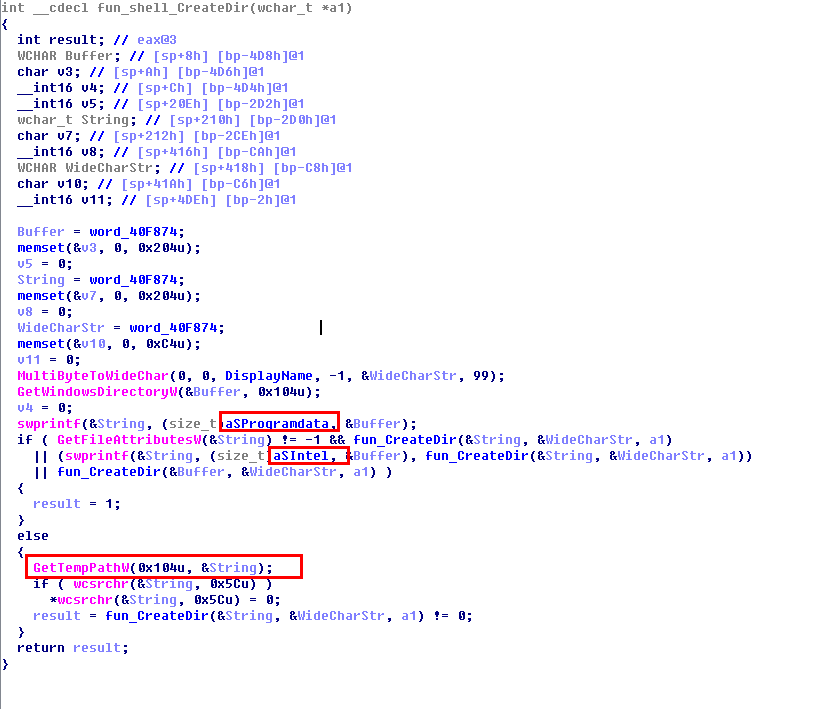
在函数fun\_GetDisplayName中通过username生成一个标识A。



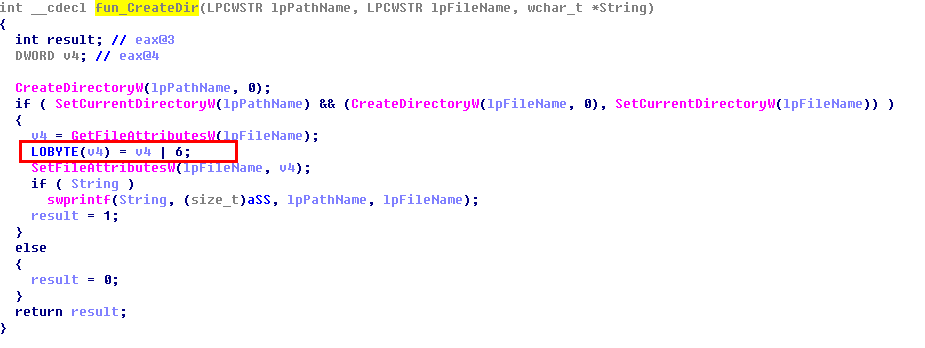
该勒索样本其中之后，首先会判断参数是否为2，是否包含i



通过该标识尝试在ProgramData目录/Intel目录/Temp系统临时目录生成一个标识A的目录



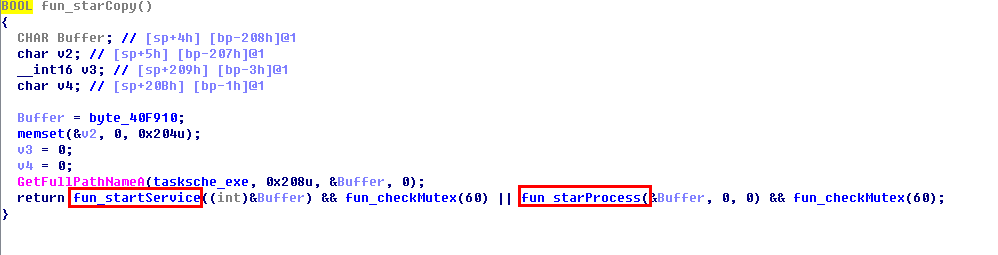
并将这个这个目录的属性设置为隐藏不可见。



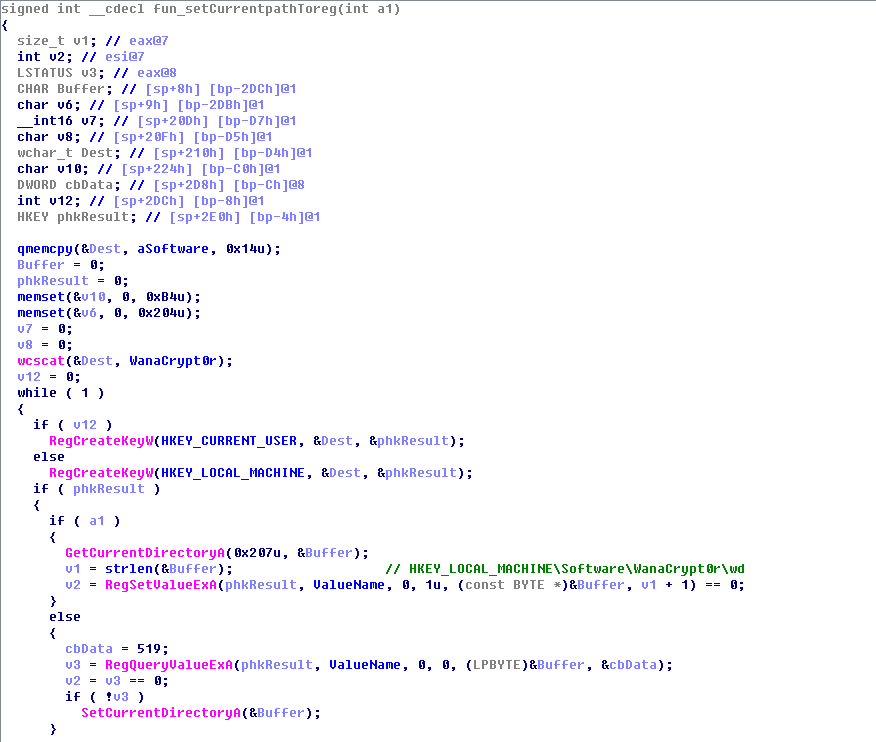
将自身拷贝创建副本。



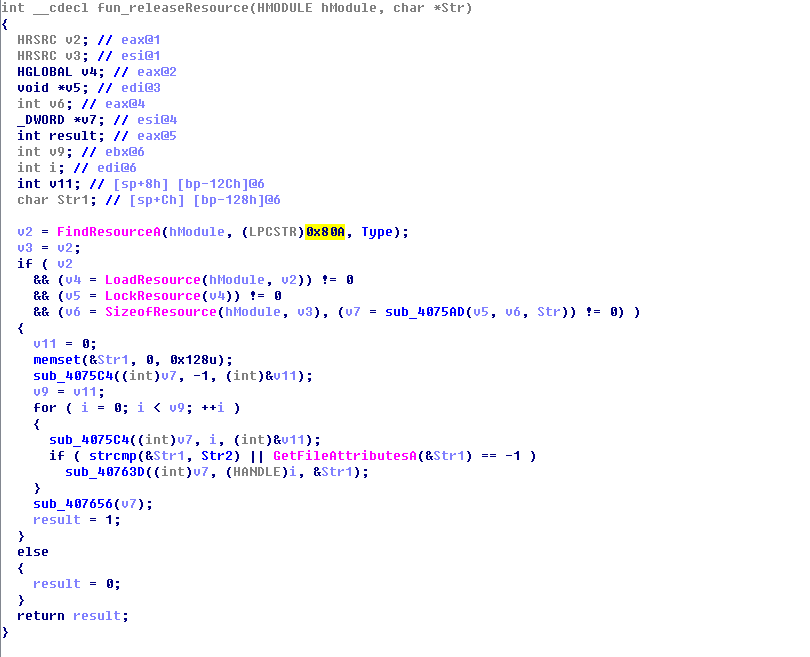
运行副本，优先通过服务的模式启动，否则以进程的方式启动，在函数fun\_checkMutex中通过检测互斥体Global\MsWinZonesCacheCounterMutexA来判断是否运行成功。



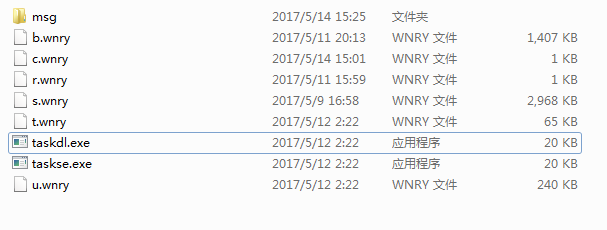
设置对应的注册表项



之后在函数fun\_releaseResource中通过再次解压出真正的ransome模块，解压的时候资源为对应80A，需要是使用到解压码WNcry@2ol7。



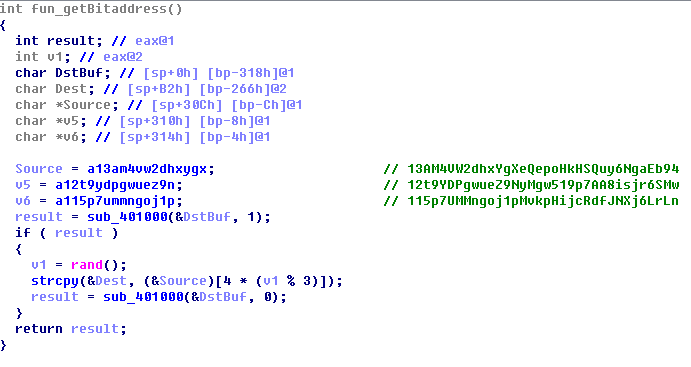
解压出的文档如下所示：其中msg中包含各国的敲诈说明版本



详细的功能列表

|  |  |
| --- | --- |
| 名称 | 作用 |
| b.wnry | 敲诈图片资源 |
| c.wnry | 配置文件，钱包地址，Tor地址 |
| r.wnry | Q&A |
| s.wnry | 压缩包，用于TOR的网络组建 |
| t.wnry | 真正的ransom模块，被加密 |
| u.wnry | 解密程序，之后被改名为@WanaDecryptor@.exe |
| taskdl.exe | 用于删除临时文件 |
| taskse.exe | 在任意的远程桌面session中运行指定程序 |
| taskhsvc.exe | 网络通信组建 |

之后在函数fun\_getBitaddress中获取对应的比特币付款地址，受害者通过该地址可以进行支付解锁。



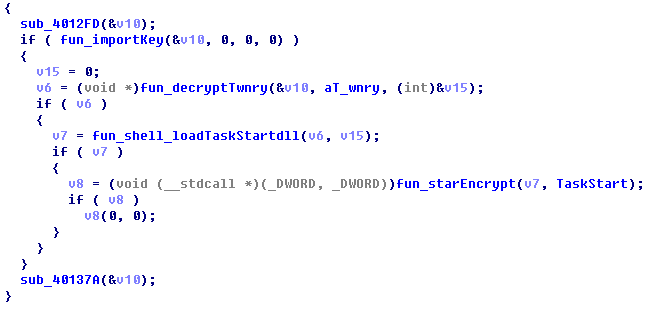
运行命令再次设置该工作目录。



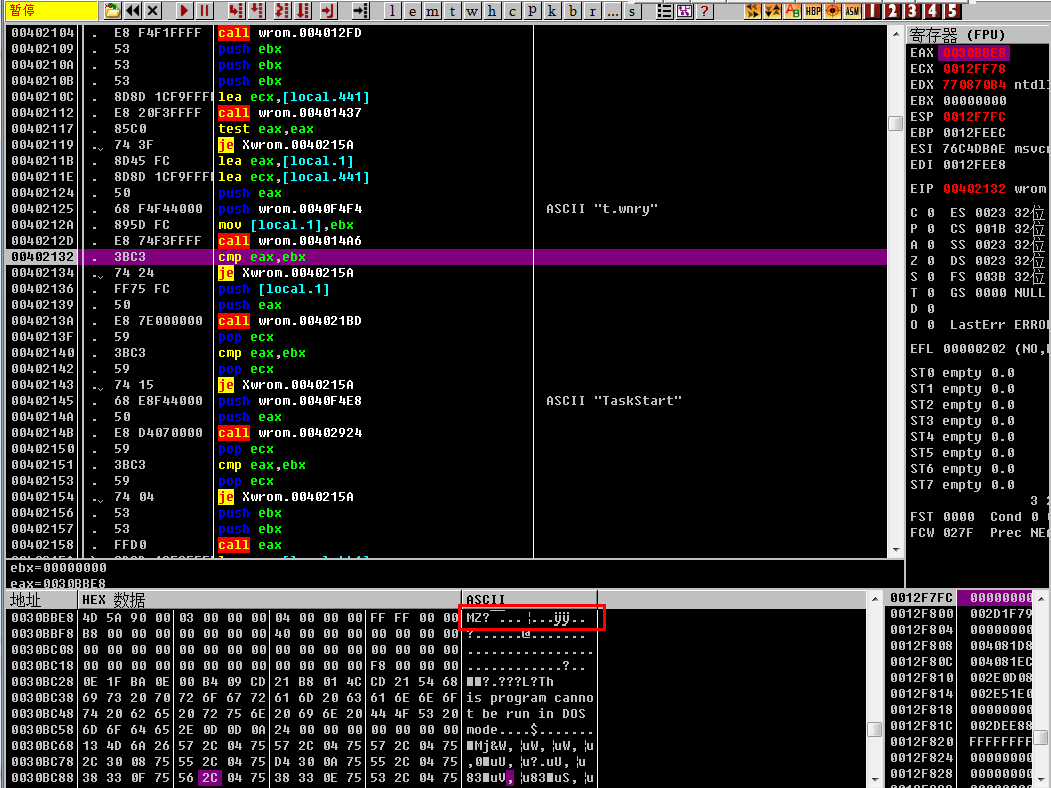
之后动态获取文件类api，crypt解密类api。



之后通过内置的RSA公钥解密对应的t.wnry，该模块为对应的RansomModule，用于实现真正的文件加密功能，如下所示，解密之后通过fun\_shell\_loadTaskStardll加载该dll到内存中，并调用TaskStart函数开始进行加密流程。

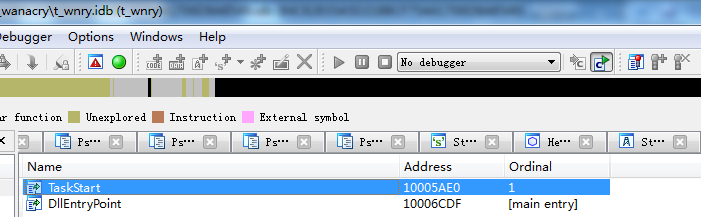


如下图示可以看到对fun\_decryptTwnry函数下断，函数运行结束之后，内存中已经解密出了RansomModule，可以直接进行dump。

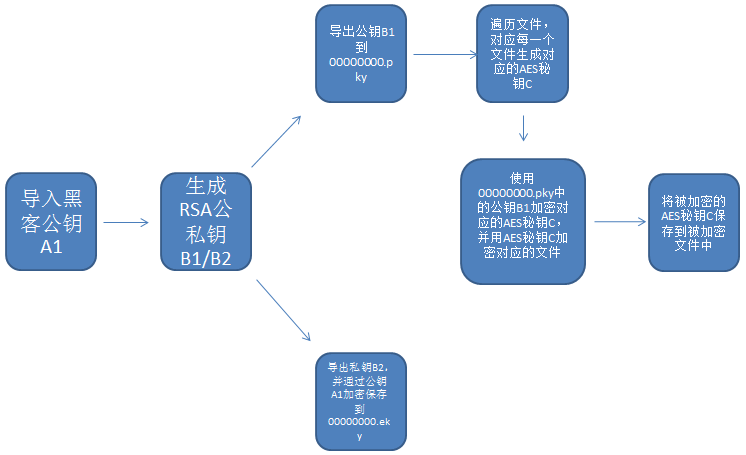


**RansomeModule**

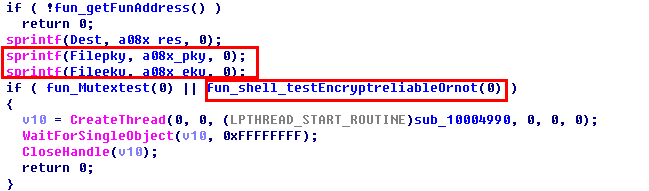
如下图所示dump出的RansomModule的导出函数如下所示，通过TaskStart开始加密任务。



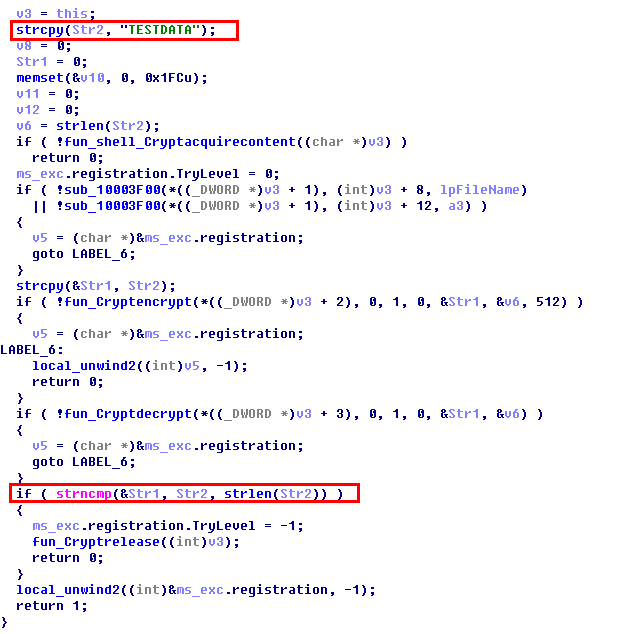
该RansomeModule的加密流程如下，黑客掌握一对公私钥A1/A2，A1公钥在样本中，A2私钥为黑客持有，RansomModule通过该公钥A1生成一对新的RSA公私钥B1/B2，公钥B1保存到文件00000000.pky中，私钥B2通过公钥A1加密保存到00000000.eky中，遍历文件并对每一个文件生成随机的AES128位秘钥C，通过公钥B1加密AES秘钥C，并用C对文件进行加密，之后将被加密AES秘钥C附加在文件内容中。



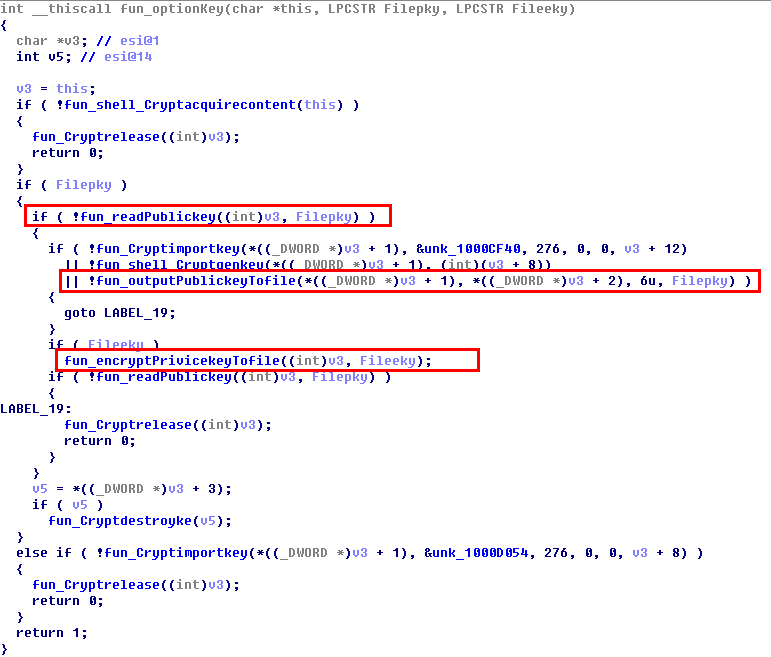
如下所示样本首先获取file/crypt类函数，之后分别生成两个用于保存公私钥的文件名，之后通过函数fun\_shell\_testEncryptreliableOrnot测试内置公钥的的可靠性。



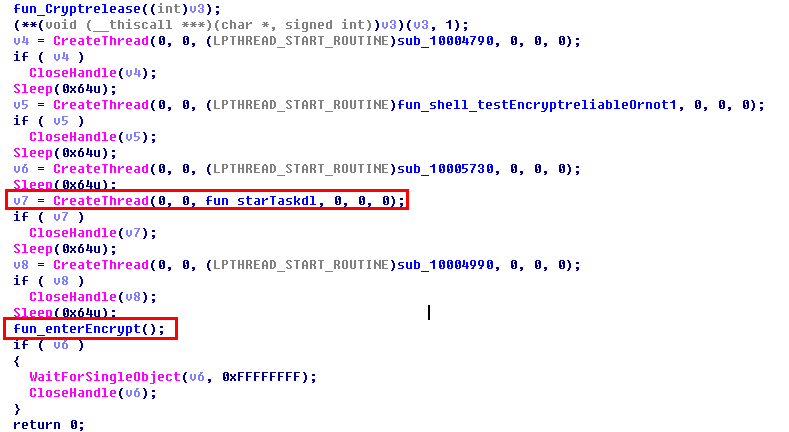
如下所示对首先通过加密TESTDATA字符测试该公钥的加密可行性。



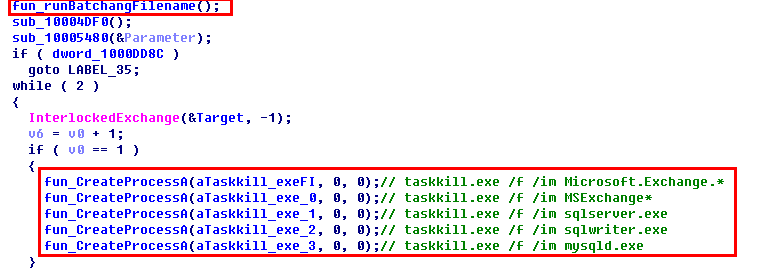
之后在函数fun\_optionKey中通过该内置的公钥生成一对RSA公私钥A1/A2，并保存到对应的文件00000000.pky，00000000eky中。



之后运行一系列线程初始化运行环境，如下图中fun\_starTaskdl用于调用Taskdl.exe删除临时文件，最后进行fun\_enterEncrypt开始加密流程。



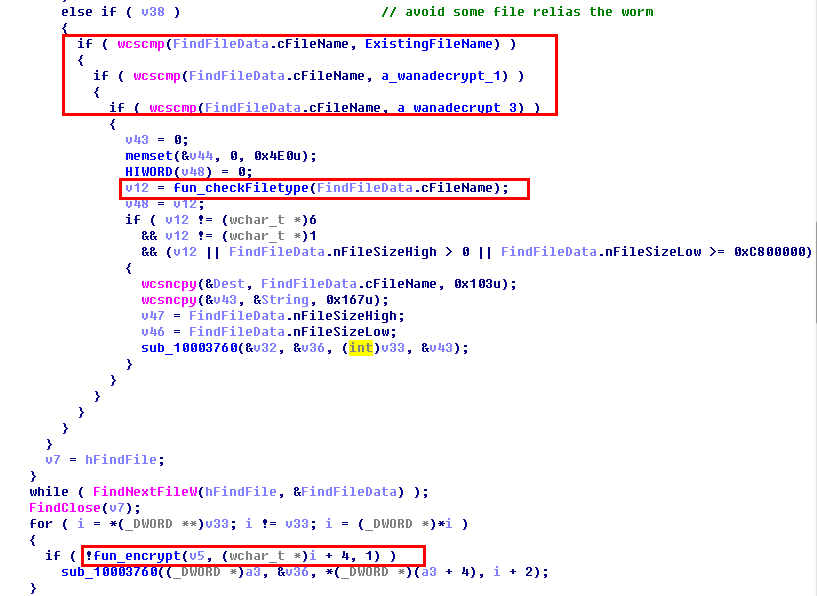
进入fun\_enterEncrypt后，首先调用fun\_runBatchangFilename，之后通过命令行关闭一些重要进程，以保证对应的文件能成功被加密。



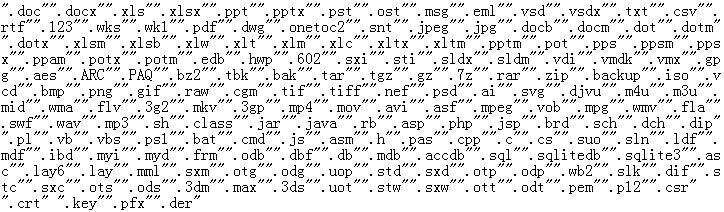
fun\_runBatchangFilename中运行通过一个脚本设置一个link，将u.wnry重命名为@WanaDecryptor@.exe，该exe即为受害者能看到的勒索展示程序。



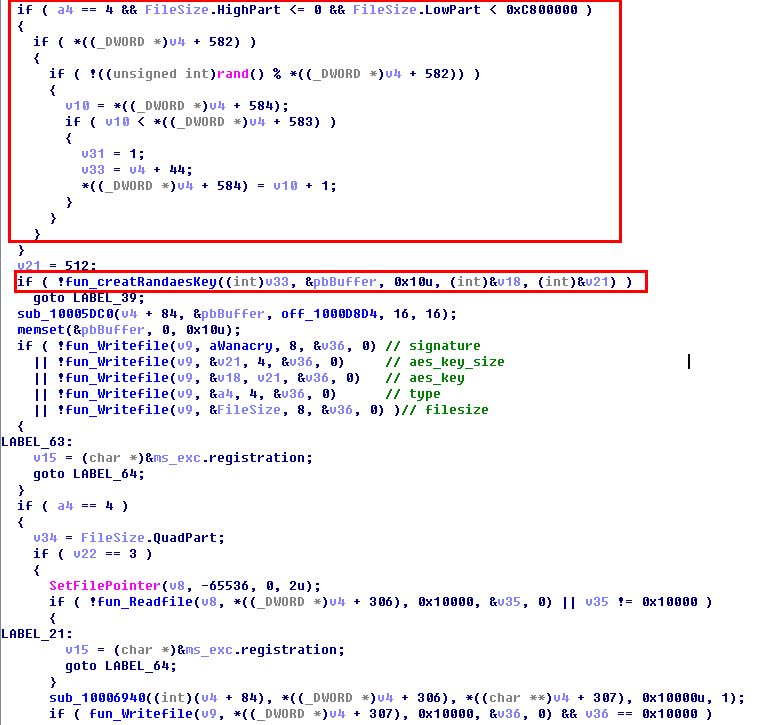
之后开始遍历文件，如下所示过滤掉ransom自己的文件，然后对比文件后缀是否为内置需要加密的文件类型。



支持的加密文件如下所示：



之后创建AES秘钥并开始加密，注意此处会随机挑选几个文件使用内置的RSA公钥来进行加密，这里的目的是为解密程序提供的免费解密部分文件功能演示。



## 一些思考

蠕虫样本的分析显示其结构和功能并不复杂，也没有做什么技术上的对抗。为什么在全球范围内形成了如此大的危害，其核心还是在于其所依赖的蠕虫式传播手段。蠕虫攻击传播所利用的漏洞微软在2017年3月已经修补，而在4月Shadow Brokers公开了蠕虫所基于的NSA黑客工具以后，安全业界对于可能出现蠕虫其实已经有所警觉，并再次提醒更新系统，但似乎并没什么用。

这回的蠕虫事件本质上是对企业机构的内部网络安全运维一次大考，如果企业有比较完善的IT运维策略并得以有效地落地执行，安全补丁能被及时打上，在本次勒索大潮中可安然度过，反之，则必然经历一场伤痛。

## 参考引用

[1] WanaCrypt0r勒索蠕虫完全分析报告

http://bobao.360.cn/learning/detail/3853.html

[2] Wannacry勒索软件母体主程序逆向分析

http://www.freebuf.com/vuls/134602.html

[3] WannaCry蠕虫详细分析

http://www.freebuf.com/articles/system/134578.html

[4] Wannacry 勒索软件分析

https://mp.weixin.qq.com/s/CTPvdIcryGYiGHKQyNROyA

[5] 关于“魔窟”（WannaCry）勒索蠕虫变种情况的进一步分析

http://www.antiy.com/response/Antiy\_Wannacry\_Explanation.html?from=groupmessage&isappinstalled=0

[6] WannaCry and Lazarus Group – the missing link?

https://securelist.com/blog/research/78431/wannacry-and-lazarus-group-the-missing-link/

[7] the-worm-that-spreads-wanacrypt0r

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

[8] how-to-accidentally-stop-a-global-cyber-attacks

https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

[9] WanaCry Ransomware：Potential Link to North Korea

http://www.intezer.com/wp-content/uploads/2017/05/Intezer\_WannaCry.pdf

[10] Player 3 Has Entered the Game: Say Hello to 'WannaCry'

http://blog.talosintelligence.com/2017/05/wannacry.html?m=1&nsukey=0iYxeUP%2BZU1uMlAkxW%2FksDg0RiWTLnUGIC2KF597siLZgc3qDVK7XZMWKuhZ4RZhlW3%2BujNrSiujH1ZxR0awd6vxNsLbR61jXdVlJT7hMX3pH7gkSrhVA%2B6w%2BvT8T0bXgAmQGZOAtHfWkNjeW9lY68RaTM7fIaoNjQvQus3P0kgxvXqOZp4NSwqmsHFZTTSm