【权威报告】WanaCrypt0r 勒索蠕虫完全分析报告

作者：360 追日团队

日期：2017-5-13

0x1 前言

360 互联网安全中心近日发现全球多个国家和地区的机构及个人电脑遭受到了一款新型勒索软件攻击，并于 5 月 12 日国内率先发布紧急预警，外媒和多家安全公司将该病毒命名为“WanaCrypt0r”（直译：“想哭勒索蠕虫”），常规的勒索病毒是一种趋利明显的恶意程序，它会使用加密算法加密受害者电脑内的重要文件，向受害者勒索赎金，除非受害者交出勒索赎金，否则加密文件无法被恢复，而新的“想哭勒索

蠕虫”尤其致命，它利用了窃取自美国国家安全局的黑客工具 EternalBlue（直译：“永恒之蓝”）实现了全球范围内的快速传播，在短时间内造成了巨大损失。360 追日团队对“想哭勒索蠕虫”国内首家进行了完全的技术分析，帮助大家深入了解此次攻击！

0x2 抽样分析样本信息

MD5: DB349B97C37D22F5EA1D1841E3C89EB4

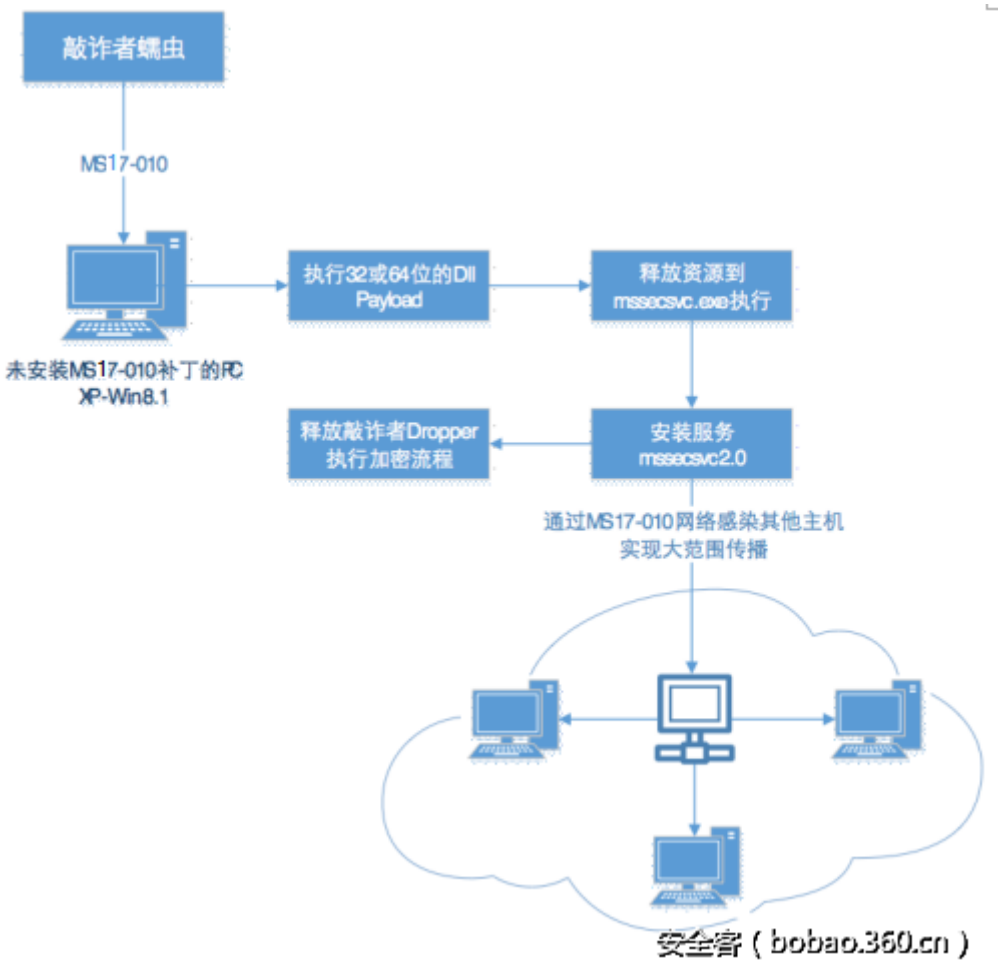
文件大小: 3,723,264

影响面：除 Windows 10 外，所有未打 MS-17-010 补丁的 Windows 系统都可能被攻击

功能: 释放加密程序，使用 RSA+AES 加密算法对电脑文件进行加密勒索，通过 MS17-010 漏洞实现自身的快速感染和扩散。

0x03 蠕虫的攻击流程

该蠕虫病毒使用了 ms17-010 漏洞进行了传播，一旦某台电脑中招，相邻的存在漏洞的网络主机都会被其主动攻击，整个网络都可能被感染该蠕虫病毒，受害感染主机数量最终将呈几何级的增长。其完整攻击流程如下



0x04 蠕虫启动逻辑分析

1.蠕虫启动时将连接固定 url: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

a)如果连接成功,则退出程序

b)连接失败则继续攻击

2.接下来蠕虫开始判断参数个数,小于 2 时,进入安装流程;大于等于 2 时,进入服务流程.

a)安装流程

i.创建服务,服务名称: mssecsvc2.0

参数为当前程序路径 –m security

ii.释放并启动 exe 程序

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

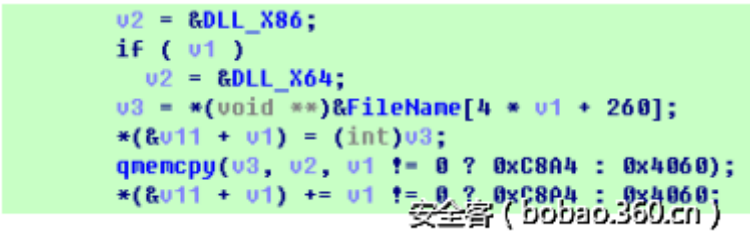
b)服务流程

i.服务函数中执行感染功能,执行完毕后等待 24 小时退出.

ii.感染功能

初始化网络和加密库,初始化 payload dll 内存.

a)Payload 包含 2 个版本,x86 和 x64



b)功能为释放资源到 c:\windows\mssecsvc.exe 并执行

启动线程,在循环中向局域网的随机 ip 发送 SMB 漏洞利用代码

```
mov     edi, 1
push    445             ; hostshort
mov     word ptr [esp+12Ch+name.sa_data+0Ch], ax
mov     [esp+12Ch+argp], edi
mov     dword ptr [esp+12Ch+name.sa_data+2], ecx
mov     [esp+12Ch+name.sa_family], 2
call    htons
push    IPPROTO_TCP     ; protocol
push    edi             ; type
push    AF_INET         ; af
mov     word ptr [esp+134h+name.sa_data], ax
call    socket
```



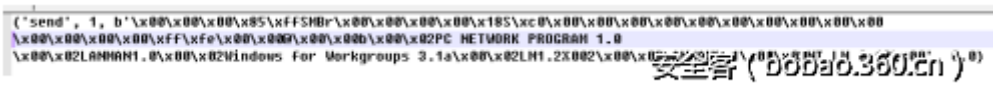
```
if ( q_Connect_445(a1) > 0 )
{
  v1 = (void *)beginthreadex(0, 0, q_MS17_010, a1, 0, 0);
  v2 = v1;
  if ( v1 )
  {
    if ( WaitForSingleObject(v1, 600000u) == WAIT_TIMEOUT )
      TerminateThread(v2, 0);
    CloseHandle(v2);
  }
}
InterlockedDecrement((volatile LONG *)&FileName[268]);
endthreadex(0);
return 0;
```


0x05 蠕虫利用漏洞确认

通过对其中的发送的 SMB 包进行分析，我们发现其使用漏洞攻击代码和 https://github.com/rapid7/metasploit-framework 近乎一致，为 Eternalblue 工具使用的攻击包。

蠕虫 SMB 数据包:

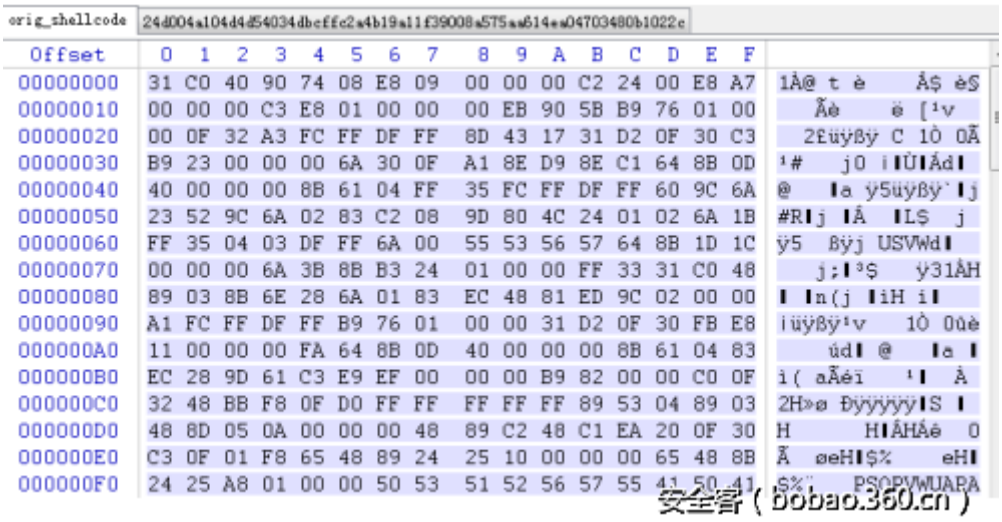
Eternalblue 工具使用的 MS17-010 SMB 数据包:



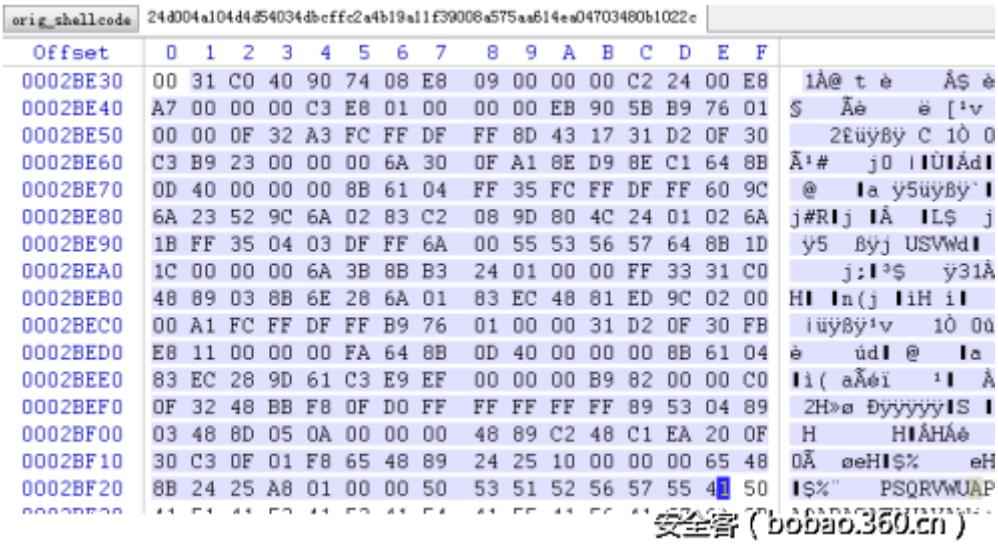
https://github.com/RiskSense-Ops/MS17-010/tree/master/exploits/eternalblue/orig_shellcode

文件内容在 DB349B97C37D22F5EA1D1841E3C89EB4 中出现

orig_shellcode 文件内容:

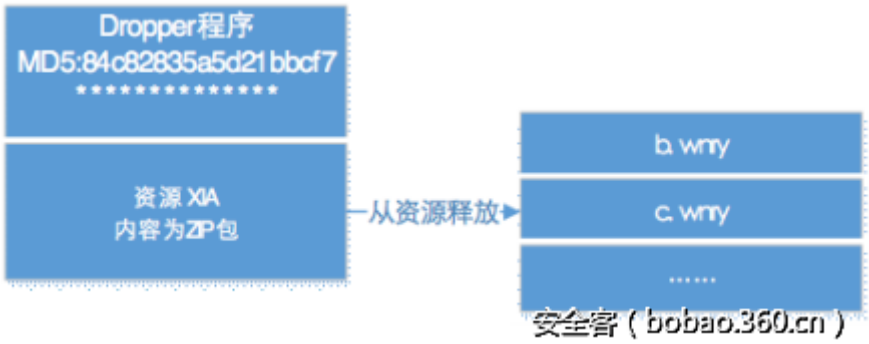


DB349B97C37D22F5EA1D1841E3C89EB4 文件:

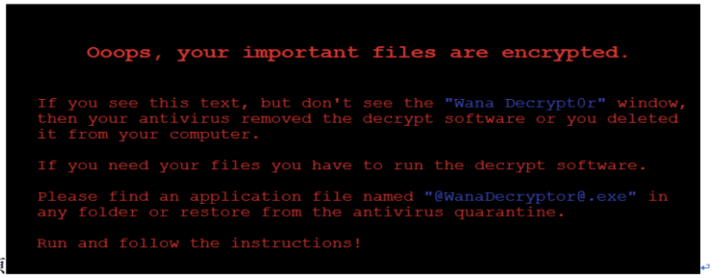


0x06 蠕虫释放文件分析

蠕虫成功启动后将开始释放文件，流程如下：



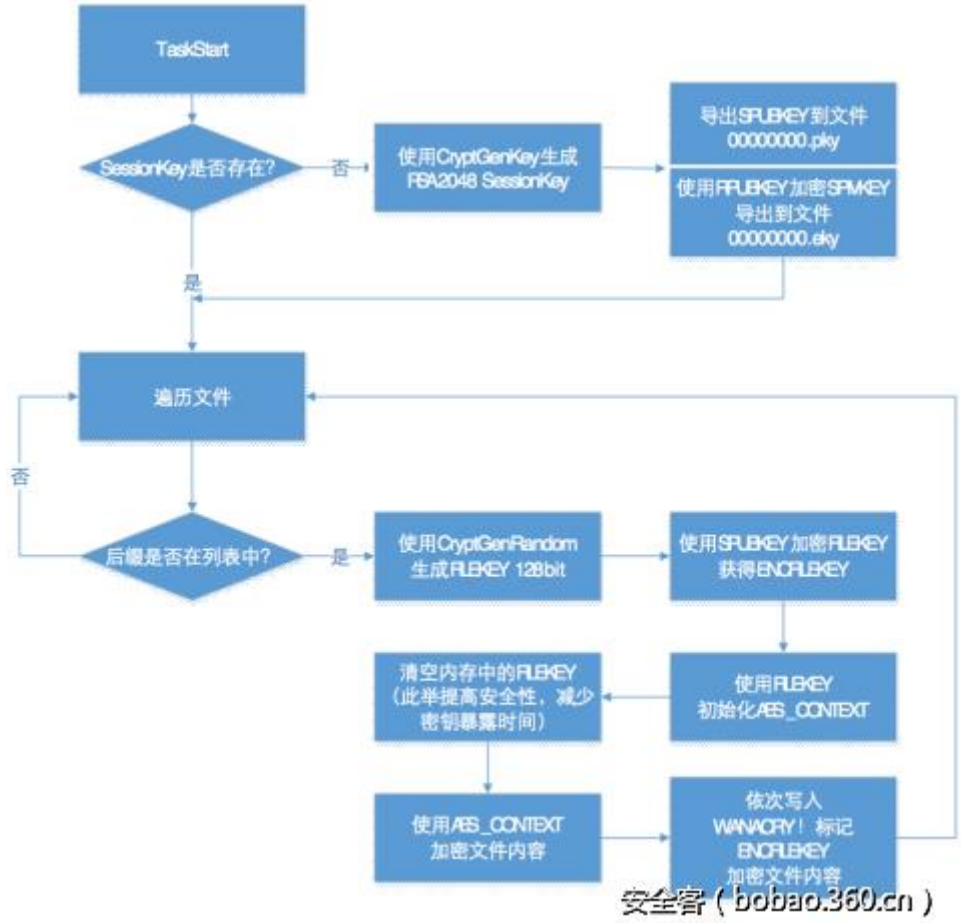
释放文件与功能列表，如下：

名称	作用
b.wnry	敲诈图片资源 
c.wnry	配置文件，包含钱包信息，tor 地址
r.wnry	Q&A
s.wnry	压缩包，包含 TOR 网络组件
t.wnry	加密的 PAYLOAD，用于加密文件
u.wnry	解密程序（@WanaDecryptor@.exe）
taskdl.exe	删除临时文件
taskse.exe	在任意的远程桌面的 session 中运行指定的程序
taskhsvc.exe	网络通讯组件

0x07 关键勒索加密过程分析

蠕虫会释放一个加密模块到内存，直接在内存加载该 DLL。DLL 导出一个函数 TaskStart 用于启动整个加密的流程。程序动态获取了文件系统和加密相关的 API 函数，以此来躲避静态查杀。

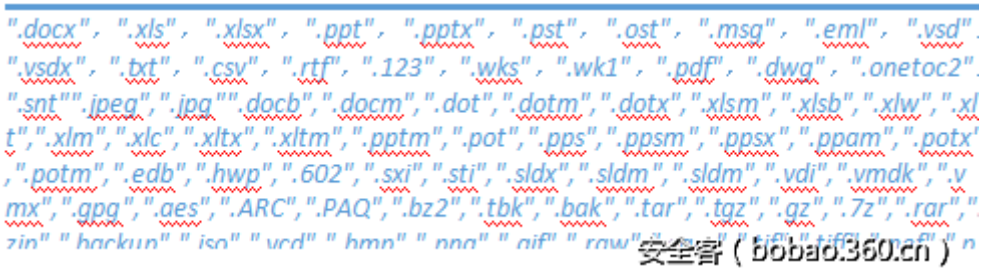
整个加密过程采用 RSA+AES 的方式完成，其中 RSA 加密过程使用了微软的 CryptAPI，AES 代码静态编译到 dll。加密流程如下图所示。



使用的密钥概述：

RPUBKEY	RSA 2048 Root Public Key，硬编码于程序中
RPIVKEY	RSA 2048 Root Private Key，作者持有，目前未公开
SPUBKEY	RSA 2048 Session Public Key, 每个受害用户唯一的会话密钥（公钥），用于加密 AES KEY，导出到文件 00000000.pky
SPIVKEY	RSA 2048 Session Private Key，每个受害用户唯一的会话密钥（私钥），用于解密 AES KEY，Encrypt（RPUBKEY，SPIVKEY），即用 RPUBKEY 加密后导出到文件 00000000.eky
FILEKEY	AES 128Bit KEY，每一个文件生成一个，通过 CryptGenRandom 生成
ENCFILEKEY	被 SPUBKEY 加密的 FILEKEY，存在于被加密的文件当中

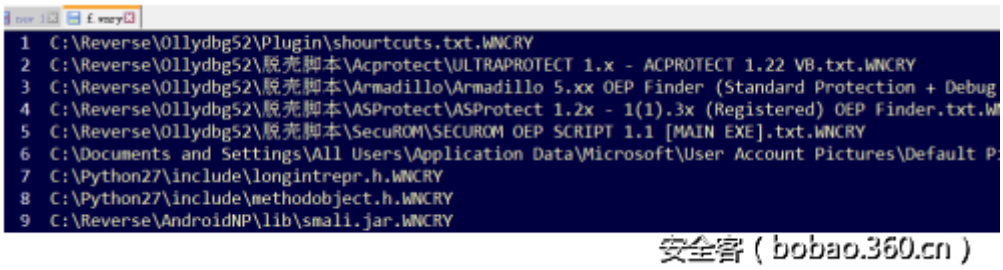
目前加密的文件后缀名列表：



值得注意的是，在加密过程中，程序会随机选取一部分文件使用内置的 RSA 公钥来进行加密，这里的目的是解密程序提供的免费解密部分文件功能。

```
62 LABEL_29:
63   if ( a4 == 4 && FileSize.HighPart <= 0 && FileSize.LowPart < 0xC800000 )
64   {
65     if ( *((_DWORD *)v4 + 582) )
66     {
67       if ( !((unsigned int)rand() % *((_DWORD *)v4 + 582)) )
68       {
69         v10 = *((_DWORD *)v4 + 584);
70         if ( v10 < *((_DWORD *)v4 + 583) )
71         {
72           v62 = 1;
73           v64 = v4 + 44;
74           *((_DWORD *)v4 + 584) = v10 + 1;
75         }
76       }
77     }
78   }
79   v52 = 512;
80   if ( !q_init_key((int)v64, &pbBuffer, 0x10u, (int)&v49, (int)&v52) )
81     goto LABEL_62;
```


能免费解密的文件路径在文件 f.wnry 中



0x08 蠕虫赎金解密过程分析

首先，解密程序通过释放的 taskhsvc.exe 向服务器查询付款信息，若用户已经支付过，则将 eky 文件发送给作者，作者解密后获得 dky 文件，这就是解密之后的 Key

解密流程与加密流程相反，解密程序将从服务器获取的 dky 文件中导入 Key

```
push    offset a08x_dky ; "%08X.dky"
push    ecx             ; Dest
call    edi ; __imp_sprintf
```



```
v2 = this;
if ( !q_CryptAcquireContext() )
{
  q_DestroyKey(v2);
  return 0;
}
if ( lpFileName )
{
  if ( !q_ImportKeyFromFile(*((_DWORD *)v2 + 1), (int)((char *)v2 + 8), lpFileName) )
  {
    q_DestroyKey(v2);
    return 0;
  }
}
else if ( !g_CryptImportKey(*((_DWORD *)v2 + 1), &g_InsideKey, 1172, 0, 0, (char *)v2 + 8) )
{
  q_DestroyKey(v2);
  return 0;
}
return 1;
```


可以看到，当不存在 dky 文件名的时候，使用的是内置的 Key，此时是用来解密免费解密的文件使用的。

```
85C0          test eax,eax
75 0D         jnz X@WanaDec.00404709
8BCE          mov ecx,esi
E8 6D000000   call @WanaDec.00404770
33C0          xor eax,eax
5E            pop esi
C2 0400       retn 0x4
8B4424 08     mov eax,dword ptr ss:[esp+0x8]
85C0          test eax,eax
75 2D         jnz X@WanaDec.0040473E
8B4E 04       mov ecx,dword ptr ds:[esi+0x4]
8D46 08       lea eax,dword ptr ds:[esi+0x8]
50            push eax
6A 00         push 0x0
6A 00         push 0x0
68 94040000   push 0x494
68 94074200   push @WanaDec.00420794
51            push ecx
FF15 C4174200 call dword ptr ds:[0x4217C4]
```

```
mov     esi, [esp+0Ch+arg_0]
mov     ecx, [ebx+8]
lea     eax, [esp+0Ch+arg_4]
push    eax
push    esi
push    0
push    1
push    0
push    ecx
call    q_CryptDecrypt
```


之后解密程序从文件头读取加密的数据，使用导入的 Key 调用函数 CryptDecrypt 解密，解密出的数据作为 AES 的 Key 再次解密得到原文件。

```
    v24 -= (unsigned int)v25;
    q_AES_Decrypt(*((_DWORD *)v10 + 306), *((_DWORD *)v10 + 307), v25, 1);
    if ( !g_WriteFile(v5, *((_DWORD *)v10 + 307), v25, &v26, 0) || v26 != v25 )
      goto LABEL_33;
  }
  SetFilePointerEx(v5, liDistanceToMove, 0, 0);
```


总结

该蠕虫在勒索类病毒中全球首例使用了远程高危漏洞进行自我传播复制，危害不小于冲击波和震荡波蠕虫，并且该敲诈者在文件加密方面的编程较为规范，流程符合密码学标准，因此在作者不公开私钥的情况下，很难通过其他手段对勒索文件进行解密，同时微软已对停止安全更新的 xp 和 2003 操作系统紧急发布了漏洞补丁，请大家通过更新 MS17-010 漏洞补丁来及时防御蠕虫攻击。