[反病毒] 小学生制作勒索病毒号称无人可破

MUSYIDA i春秋作家
发表于 2019-1-26 07:05:57

好久不见的敲竹杠以及迷之自信的作者

0x0 概况

近期，笔者捕获到了一个样本，并且作者放出话说没有人能够破解，我想探探虚实，没成想作者可能脑子坏掉了。

连壳都没加就说没有人能破解真是心大。

0x1 分析

查看编译时间戳

ExifTool File Metadata

CharacterSet	Unicode
CodeSize	573440
Comments	QQ
EntryPoint	0x69ad2
FileDescription	QQ
FileFlagsMask	0x0000
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
ImageVersion	0.0
InitializedDataSize	225280
LanguageCode	Chinese (Simplified)
LinkerVersion	7.1
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0
ObjectFileType	Executable application
PEType	PE32
ProductName	QQ
ProductVersion	1.0.0.0
ProductVersionNumber	1.0.0.0
Subsystem	Windows GUI
SubsystemVersion	4.0
TimeStamp	2018:01:21 09:06:47+01:00
UninitializedDataSize	0

查看杀软捕获时间

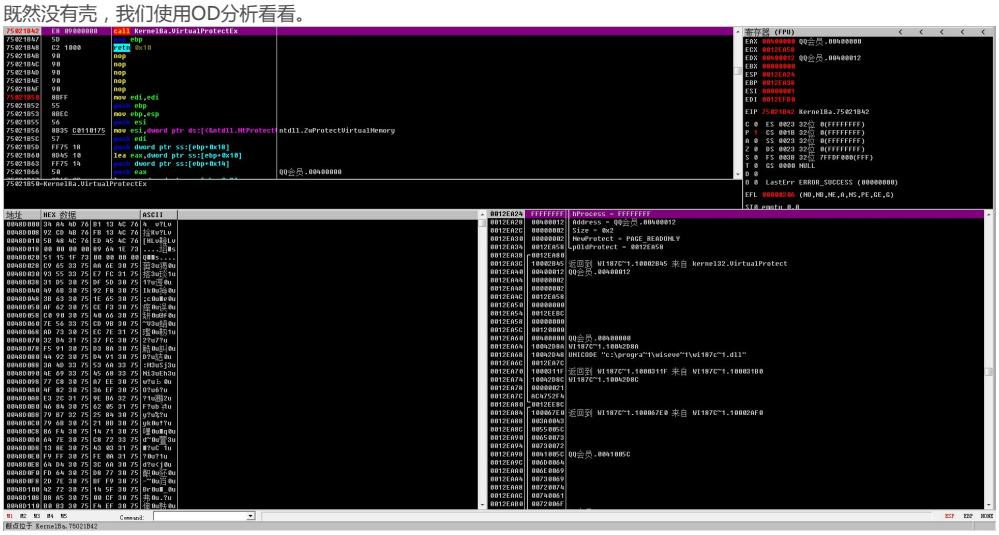
检测结果

是否恶意	是
恶意类型	Trojan
家族信息	Flystudio

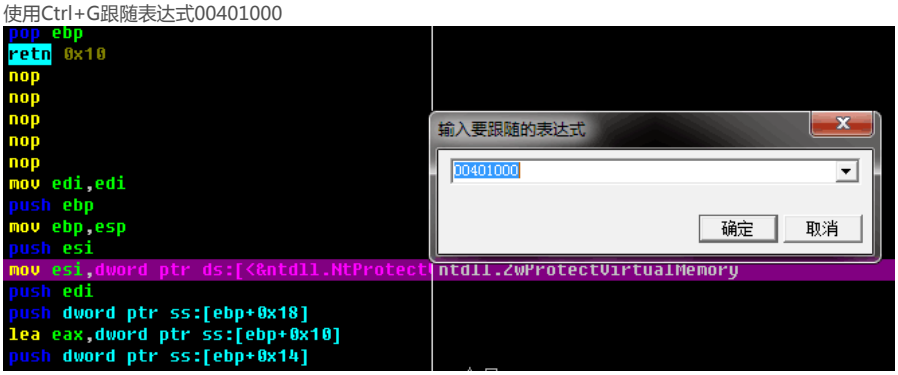
文件信息

MD5	85cc61951226b91d964dbd09e451e8cd
sha1	9b90186aaee1afbcf3313ae6dd560363ad1c42a5
sha256	066abc0299f82858460be6f5172842cd3294617f307c6833250319 44c7866da4
文件大小	784.0 KB
文件类型	Win32 EXE
文件名	85cc61951226b91d964dbd09e451e8cd.virus
发现时间	2019-01-23 06:11:42

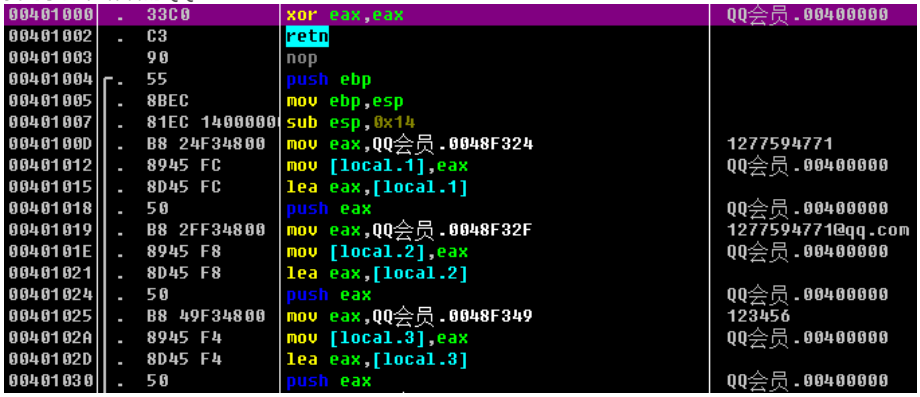
既然没有壳，我们使用OD分析看看。

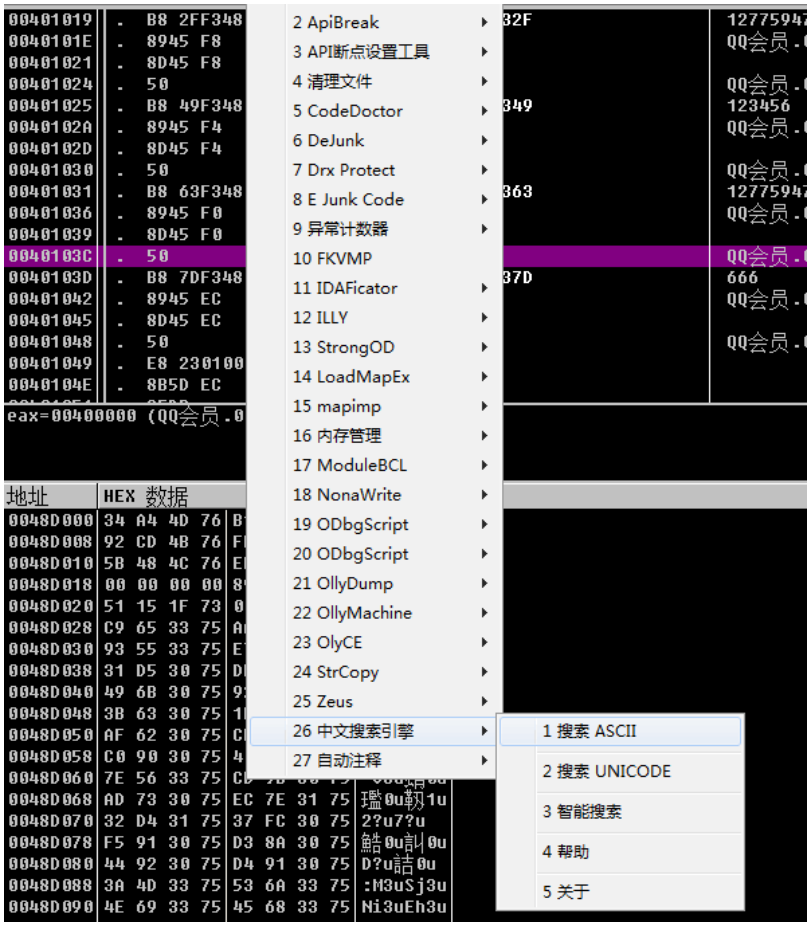


使用Ctrl+G跟随表达式00401000

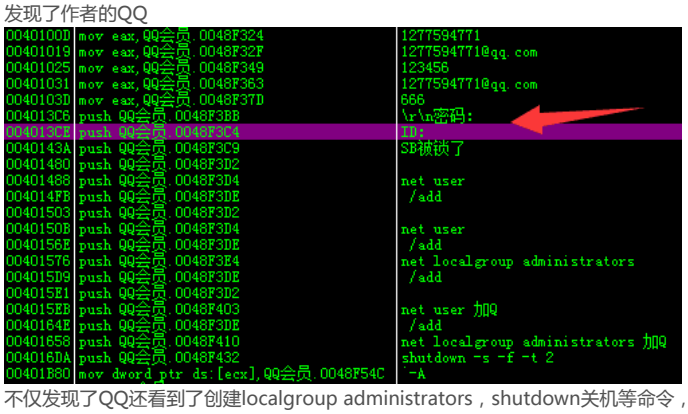


找到字符串-作者的QQ

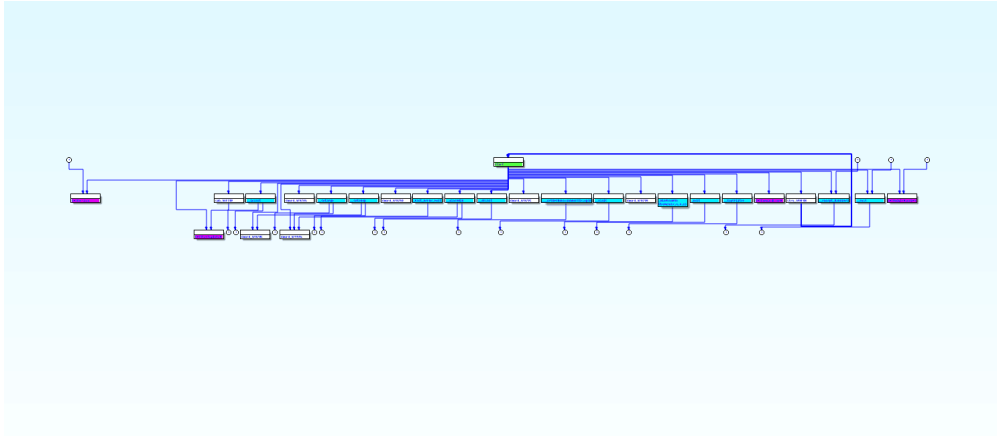




发现了作者的QQ



不仅发现了QQ还看到了创建localgroup administrators，shutdown关机等命令，在OD看让笔者眼花缭乱，所以笔者决定使用IDA分析。



通过IDA载入程序，直接跳转到刚才发现的位置。

```
; Attributes: bp-based frame

sub_401004 proc near

lpMem= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 14h
mov     eax, offset a1277594771 ; "1277594771"
mov     [ebp+var_4], eax
lea     eax, [ebp+var_4]
push    eax
mov     eax, offset a1277594771@qq_ ; "1277594771@qq.com"
mov     [ebp+var_8], eax
lea     eax, [ebp+var_8]
push    eax
mov     eax, offset a123456 ; "123456"
mov     [ebp+var_C], eax
lea     eax, [ebp+var_C]
push    eax
mov     eax, offset a1277594771@q_0 ; "1277594771@qq.com"
mov     [ebp+var_10], eax
lea     eax, [ebp+var_10]
push    eax
mov     eax, offset a666 ; "666"
mov     [ebp+lpMem], eax
lea     eax, [ebp+lpMem]
push    eax
call    sub_401171
mov     ebx, [ebp+lpMem]
test    ebx, ebx
jz      short loc_40105E
```

一阵乱点之后我们来到了想要的地方

```
.rdata:0048F39F                 db  73h ; s
.rdata:0048F3A0                 db  6Ah ; j
.rdata:0048F3A1                 db  69h ; i
.rdata:0048F3A2                 db  64h ; d
.rdata:0048F3A3 unk_48F3A3      db    1                 ; DATA XREF: sub_401171+12C↑o
.rdata:0048F3A4                 db    0
.rdata:0048F3A5                 db    0
.rdata:0048F3A6                 db    0
.rdata:0048F3A7                 db    3
.rdata:0048F3A8                 db    0
.rdata:0048F3A9                 db    0
.rdata:0048F3AA                 db    0
.rdata:0048F3AB                 db  77h ; w
.rdata:0048F3AC                 db  79h ; y
.rdata:0048F3AD                 db  63h ; c
.rdata:0048F3AE unk_48F3AE      db    1                 ; DATA XREF: sub_401171+16C↑o
.rdata:0048F3AF                 db    0
.rdata:0048F3B0                 db    0
.rdata:0048F3B1                 db    0
.rdata:0048F3B2                 db    4
.rdata:0048F3B3                 db    0
.rdata:0048F3B4                 db    0
.rdata:0048F3B5                 db    0
.rdata:0048F3B6                 db  79h ; y
.rdata:0048F3B7                 db  73h ; s
.rdata:0048F3B8                 db  79h ; y
.rdata:0048F3B9                 db  73h ; s
.rdata:0048F3BA unk_48F3BA      db    0                 ; DATA XREF: sub_401171+1FD↑o
.rdata:0048F3BA                                         ; sub_401171+213↑o ...
.rdata:0048F3BB aIg             db 0Dh,0Ah              ; DATA XREF: sub_401171+255↑o
.rdata:0048F3BB                 db '密码：',0
.rdata:0048F3C4 aIdg            db 'ID：',0              ; DATA XREF: sub_401171+25D↑o
.rdata:0048F3C9 aSb             db 'SB被锁了',0            ; DATA XREF: sub_401171+2C9↑o
.rdata:0048F3D2 asc_48F3D2      db ' ',0                ; DATA XREF: sub_401171+30F↑o
.rdata:0048F3D2                                         ; sub_401171+392↑o ...
```

从这里可以看出id是随机的，因为（suiji-ID），所以笔者使用了3个云沙箱来验证一下。

基本信息

文件名称：	QQ会员.exe
MD5：	85cc61951226b91d964dbd09e451e8cd
文件类型：	EXE
上传时间：	2019-01-26 14:40:14
出品公司：	N/A
版本：	1.0.0.0---1.0.0.0
壳或编译器信息：	COMPILER:Elan

关键行为

行为描述：修改用户密码

详情信息：ImagePath = , CmdLine = net user Administrator wyc8953ysys

行为描述：关机或重启

详情信息：InitiateSystemShutdownExW

行为描述：连接邮件服务器

详情信息：EHLO: SOCKET = 0x0000012c, IP: 0.0.2.154:25

行为描述：添加管理员权限

详情信息：ImagePath = , CmdLine = net localgroup administrators 5395sjid /add

ImagePath = , CmdLine = net localgroup administrators 加Q1277594771 /add

行为描述：添加新用户帐号

详情信息：ImagePath = , CmdLine = net user 5395sjid wyc8953ysys /add

ImagePath = , CmdLine = net user 加Q1277594771 wyc8953ysys /add

威胁分析

行为异常分析 全部展开

使用shutdown.exe来关闭或重启系统

类别:	cmdline
入侵指标:	C:\Windows\System32\shutdown.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdLine:shutdown -s -f -t 2
类型:	ioc

执行net.exe来查找Windows服务相关的信息

类别:	cmdline
入侵指标:	C:\Windows\System32\net1.exe creator:net.exe cmdLine:C:\Windows\system32\net1 user Administrator wyc9258ysys
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdLine:net localgroup administrators 加Q1277594771 /add
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net1.exe creator:net.exe cmdLine:C:\Windows\system32\net1 user 加Q1277594771 wyc9258ysys /add
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdLine:net user 加Q1277594771 wyc9258ysys /add
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdLine:net user Administrator wyc9258ysys
类型:	ioc

- **066abc0299f82858460be6f5172842cd3294617f307c683325031944c7866da4.exe (PID:2616)**
  "C:\Users\vbccsb\AppData\Local\Temp\066abc0299f82858460be6f5172842cd3294617f307c683325031944c7866da4.exe"
  - **net.exe (PID:2112)**
    net localgroup administrators ¼ÓQ1277594771 /add
    - **net1.exe (PID:2816)**
      C:\Windows\system32\net1 localgroup administrators ¼ÓQ1277594771 /add
  - **net.exe (PID:2876)**
    net localgroup administrators 3998sjid /add
    - **net1.exe (PID:2260)**
      C:\Windows\system32\net1 localgroup administrators 3998sjid /add
  - **net.exe (PID:2972)**
    net user ¼ÓQ1277594771 wyc7905ysys /add
    - **net1.exe (PID:2596)**
      C:\Windows\system32\net1 user ¼ÓQ1277594771 wyc7905ysys /add
  - **shutdown.exe (PID:2360)**
    shutdown -s -f -t 2
  - **net.exe (PID:2708)**
    net user vbccsb wyc7905ysys
    - **net1.exe (PID:3048)**
      C:\Windows\system32\net1 user vbccsb wyc7905ysys
  - **net.exe (PID:2780)**
    net user 3998sjid wyc7905ysys /add
    - **net1.exe (PID:1532)**
      C:\Windows\system32\net1 user 3998sjid wyc7905ysys /add

好的，的确都是wyc+4个数字+ysys的密码。说明笔者的分析是正确的。

IDA View-A | Pseudocode-A | Hex

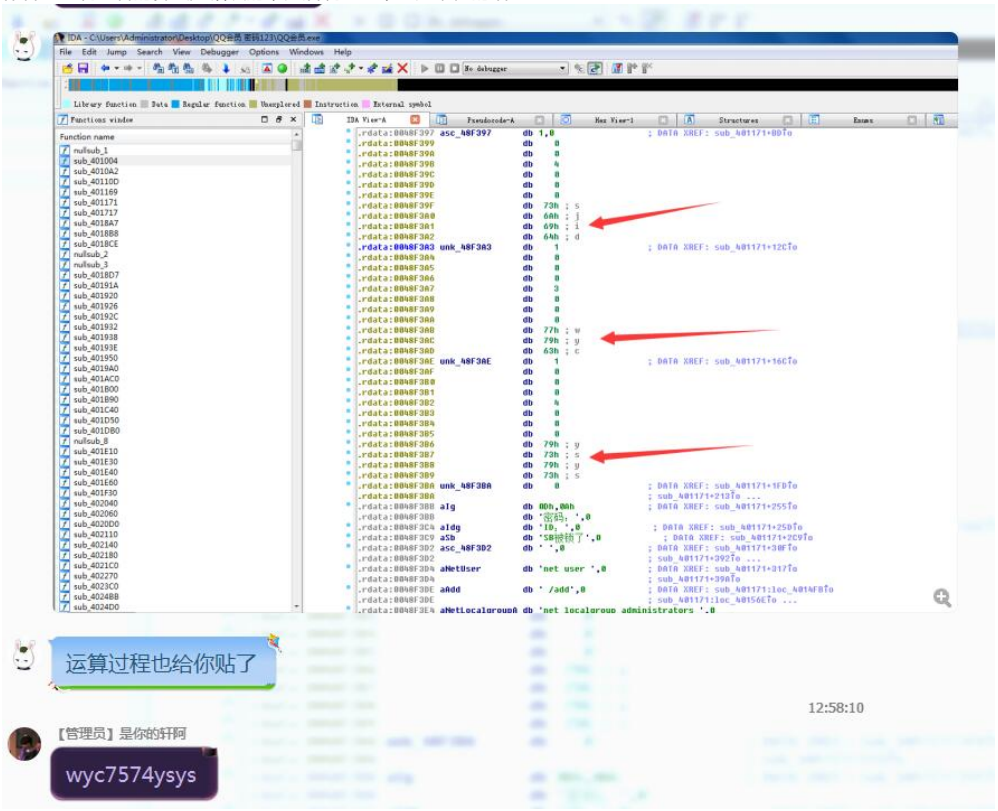
```
int sub_401004()
{
  int result; // eax@1
  LPVOID lpMem; // [sp+0h] [bp-14h]@1
  LPVOID v2; // [sp+4h] [bp-10h]@1
  LPVOID v3; // [sp+8h] [bp-Ch]@1
  LPVOID v4; // [sp+Ch] [bp-8h]@1
  LPVOID v5; // [sp+10h] [bp-4h]@1

  v5 = "1277594771";
  v4 = "1277594771@qq.com";
  v3 = "123456";
  v2 = "1277594771@qq.com";
  lpMem = "666";
  result = sub_401171(&lpMem, &v2, &v3, &v4, &v5);
  if ( lpMem )
    result = sub_40192C(lpMem);
  if ( v2 )
    result = sub_40192C(v2);
  if ( v3 )
    result = sub_40192C(v3);
  if ( v4 )
    result = sub_40192C(v4);
  if ( v5 )
    result = sub_40192C(v5);
  return result;
}
```

就可以F5查看伪代码看算法咯。

0x2 故事

作者一直说笔者的算法是错误的，然后说了一堆让人难懂的话。



我已经把算法给他了，但是他又去拿“一个高手”破解出的对应随机密码出来挑衅。

我只想说，汇编看不懂的也没什么好讲的，还有那个所谓的“一个高手”别丢人现眼了，行为分析的密码拿出来说是自己破解的.....

0x3 总结

敲竹杠已经流行几年了，经久不衰，甚至还更新迭代，但是作者一般都是小学生水平的，编译成功后以为加个强壳就万事大吉了。人外有人，天外有天。笔者也算是从2013年就开始研究敲竹杠，见过无数敲竹杠，这个已经算是低级的了，但是这个作者连逆向出来的算法都不肯承认，那笔者也是无语了。

本主题由 小i 于 2019-1-27 02:47 生成文章

使用道具 举报 回复