

[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

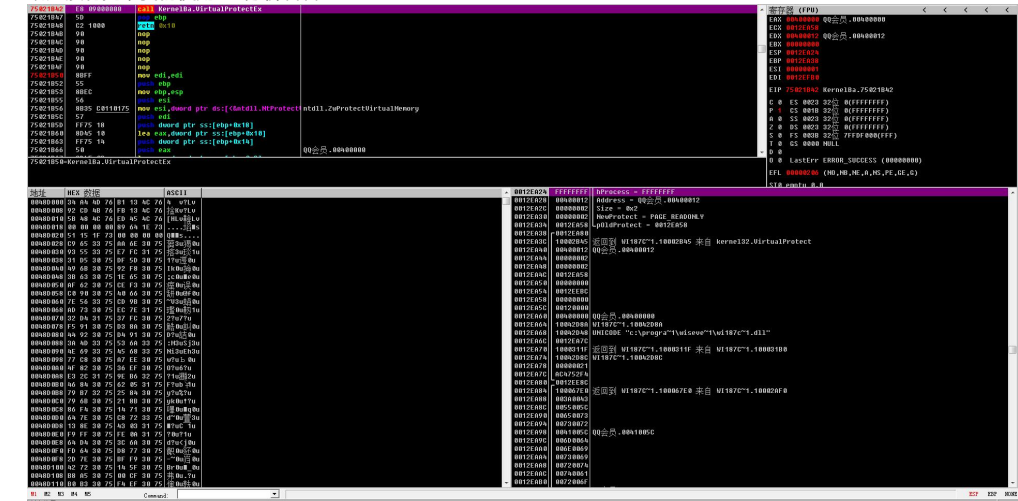
ExifTool File Metadata ⓘ	
CharacterSet	Unicode
CodeSize	573440
Comments	QQ
EntryPoint	0x69ad2
FileDescription	QQ
FileFlagsMask	0x0000
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	No relocs, Executable, No line 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

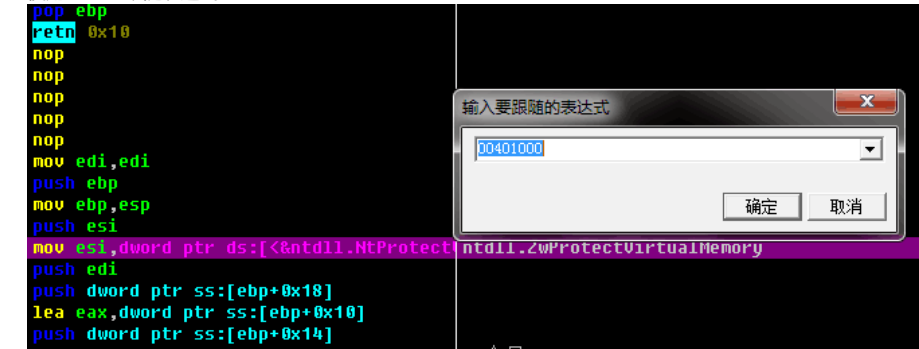
检测结果	
是否恶意	是
恶意类型	Trojan
家族信息	Flystudio

文件信息	
MD5	85cc61951226b91d964dbd09e451e8cd
sha1	9b90186aaee1afbcf3313ae6dd560363ad1c42a5
sha256	066abc0299f82858460be6f5172842cd3294617f307c683325031944c7866da4
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

00401000	- 33C0	xor eax,eax	QQ会员.00400000
00401002	- C3	ret 0	
00401003	- 90	nop	
00401004	- 55	push ebp	
00401005	- 8BEC	mov ebp,esp	
00401007	- 81EC 14000000	sub esp,0x14	
0040100D	- B8 24F34800	mov eax,QQ会员.0048F324	1277594771
00401012	- 8945 FC	mov [local.1],eax	QQ会员.00400000
00401015	- 8D45 FC	lea eax,[local.1]	
00401018	- 50	push eax	QQ会员.00400000
00401019	- B8 2FF34800	mov eax,QQ会员.0048F32F	1277594771@qq.com
0040101E	- 8945 F8	mov [local.2],eax	QQ会员.00400000
00401021	- 8D45 F8	lea eax,[local.2]	
00401024	- 50	push eax	QQ会员.00400000
00401025	- B8 49F34800	mov eax,QQ会员.0048F349	123456
0040102A	- 8945 F4	mov [local.3],eax	QQ会员.00400000
0040102D	- 8D45 F4	lea eax,[local.3]	
00401030	- 50	push eax	QQ会员.00400000

00401019- B8 2FF3482 ApiBreak32F12775947

0040101E- 8945 F83 API断点设置工具QQ会员.

00401021- 8D45 F84 清理文件QQ会员.

00401024- 505 CodeDoctor123456

00401025- B8 49F3486 DeJunkQQ会员.

0040102A- 8945 F47 E Junk Code12775947

0040102D- 8D45 F49 异常计数器QQ会员.

00401030- 5010 FKVMPQQ会员.

0040103D- B8 7DF34811 IDAFicator666

00401042- 8945 EC12 ILLYQQ会员.

00401045- 8D45 EC13 StrongODQQ会员.

00401048- 5014 LoadMapEx

00401049- E8 23010015 mapimp

0040104E- 8B5D EC16 内存管理

eax=00400000 (QQ会员.017 ModuleBCL

18 NonaWrite

19 ODbgScript

20 ODbgScript

21 OllyDump

22 OllyMachine

23 OlyCE

24 StrCopy

25 Zeus

26 中文搜索引擎1 搜索 ASCII

27 自动注释2 搜索 UNICODE

3 智能搜索

4 帮助

5 关于

地址	HEX 数据
0048D000	34 A4 4D 76 B
0048D008	92 CD 4B 76 F
0048D010	5B 48 4C 76 E
0048D018	00 00 00 00 8
0048D020	51 15 1F 73 0
0048D028	C9 65 33 75 A
0048D030	93 55 33 75 E
0048D038	31 D5 30 75 D
0048D040	49 6B 30 75 9
0048D048	3B 63 30 75 1
0048D050	AF 62 30 75 C
0048D058	C0 90 30 75 4
0048D060	7E 56 33 75 C
0048D068	AD 73 30 75 EC 7E 31 75
0048D070	32 D4 31 75 37 FC 30 75
0048D078	F5 91 30 75 D3 8A 30 75
0048D080	44 92 30 75 D4 91 30 75
0048D088	3A 4D 33 75 53 6A 33 75
0048D090	4E 69 33 75 45 68 33 75

发现了作者的QQ

0040100Bmov eax, QQ会员0048F3241277594771

00401019mov eax, QQ会员0048F32F1277594771@qq.com

00401025mov eax, QQ会员0048F349123456

00401031mov eax, QQ会员0048F3631277594771@qq.com

0040103Dmov eax, QQ会员0048F37D666

004013C6push QQ会员0048F3BB\r\n密码:

004013C7push QQ会员0048F3C4IP:

0040143Apush QQ会员0048F3C9SB解锁了

00401480push QQ会员0048F3D2

00401488push QQ会员0048F3D4net user

004014FEpush QQ会员0048F3DE/add

00401503push QQ会员0048F3D2

0040150Fpush QQ会员0048F3D4net user

0040156Fpush QQ会员0048F3DE/add

00401576push QQ会员0048F3E4net localgroup administrators

004015D9push QQ会员0048F3DE/add

004015E1push QQ会员0048F3D2

004015EFpush QQ会员0048F403net user 加QQ

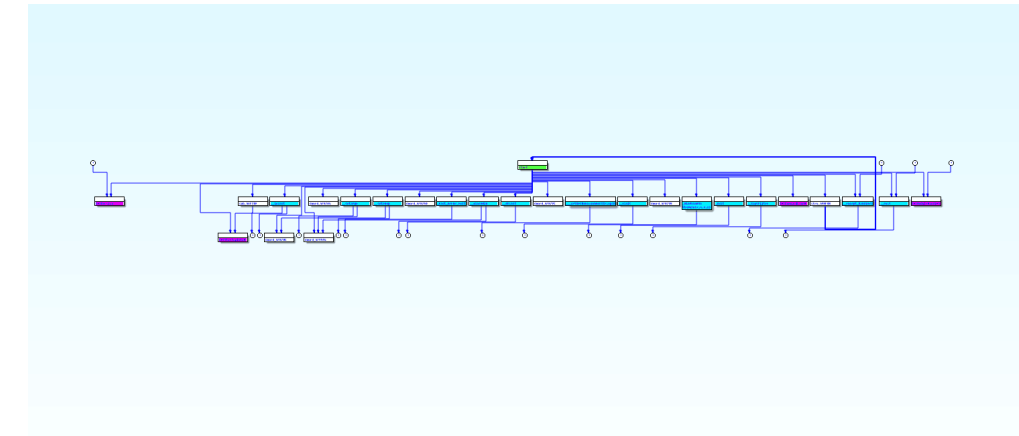
0040164Fpush QQ会员0048F3DE/add

00401658push QQ会员0048F410net localgroup administrators 加QQ

004016DApush QQ会员0048F432shutdown -s -f -t 2

00401E80mov dword ptr ds:[ecx], QQ会员0048F54C-A

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:0040F39F      db 73h ; s
.rdata:0040F3A0      db 6Ah ; j
.rdata:0040F3A1      db 69h ; i
.rdata:0040F3A2      db 64h ; d
.rdata:0040F3A3      unk_48F3A3      db 1 ; DATA XREF: sub_401171+12C70
.rdata:0040F3A4      db 0
.rdata:0040F3A5      db 0
.rdata:0040F3A6      db 0
.rdata:0040F3A7      db 3
.rdata:0040F3A8      db 0
.rdata:0040F3A9      db 0
.rdata:0040F3AA      db 0
.rdata:0040F3AB      db 77h ; w
.rdata:0040F3AC      db 79h ; y
.rdata:0040F3AD      db 63h ; c
.rdata:0040F3AE      unk_48F3AE      db 1 ; DATA XREF: sub_401171+16C70
.rdata:0040F3AF      db 0
.rdata:0040F3B0      db 0
.rdata:0040F3B1      db 0
.rdata:0040F3B2      db 4
.rdata:0040F3B3      db 0
.rdata:0040F3B4      db 0
.rdata:0040F3B5      db 0
.rdata:0040F3B6      db 79h ; y
.rdata:0040F3B7      db 73h ; s
.rdata:0040F3B8      db 79h ; y
.rdata:0040F3B9      db 73h ; s
.rdata:0040F3BA      unk_48F3BA      db 0 ; DATA XREF: sub_401171+1FD70
.rdata:0040F3BB      db 0 ; sub_401171+21370 ...
.rdata:0040F3BB      aIg      db 00h,0Ah ; DATA XREF: sub_401171+25570
.rdata:0040F3BB      db '密码:',0
.rdata:0040F3C4      aIdg     db 'ID:',0 ; DATA XREF: sub_401171+25D70
.rdata:0040F3C9      aSb      db 'SB被锁了',0 ; DATA XREF: sub_401171+2C970
.rdata:0040F3D2      asc_48F3D2      db ' ',0 ; DATA XREF: sub_401171+30F70
.rdata:0040F3D2      db 0 ; sub_401171+39270 ...

```

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 wyc8953sysys
- 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 wyc8953sysys /add
ImagePath = , CmdLine = net user 加Q1277594771 wyc8953sysys /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 wyc9258sysys
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 wyc9258sysys /add
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdline:net user 加Q1277594771 wy c9258sysys /add
类型:	ioc
类别:	cmdline
入侵指标:	C:\Windows\System32\net.exe creator:85cc61951226b91d964dbd09e451e8cd.exe cmdline:net user Administrator wyc9258sysys
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 wyc7905sysys /add
- net1.exe (PID:2596)
C:\Windows\system32\net1 user ¼ÓQ1277594771 wyc7905sysys /add
- shutdown.exe (PID:2360)
shutdown -s -f -t 2
- net.exe (PID:2708)
net user vbccsb wyc7905sysys
- net1.exe (PID:3048)
C:\Windows\system32\net1 user vbccsb wyc7905sysys
- net.exe (PID:2780)
net user 3998sjid wyc7905sysys /add
- net1.exe (PID:1532)
C:\Windows\system32\net1 user 3998sjid wyc7905sysys /add

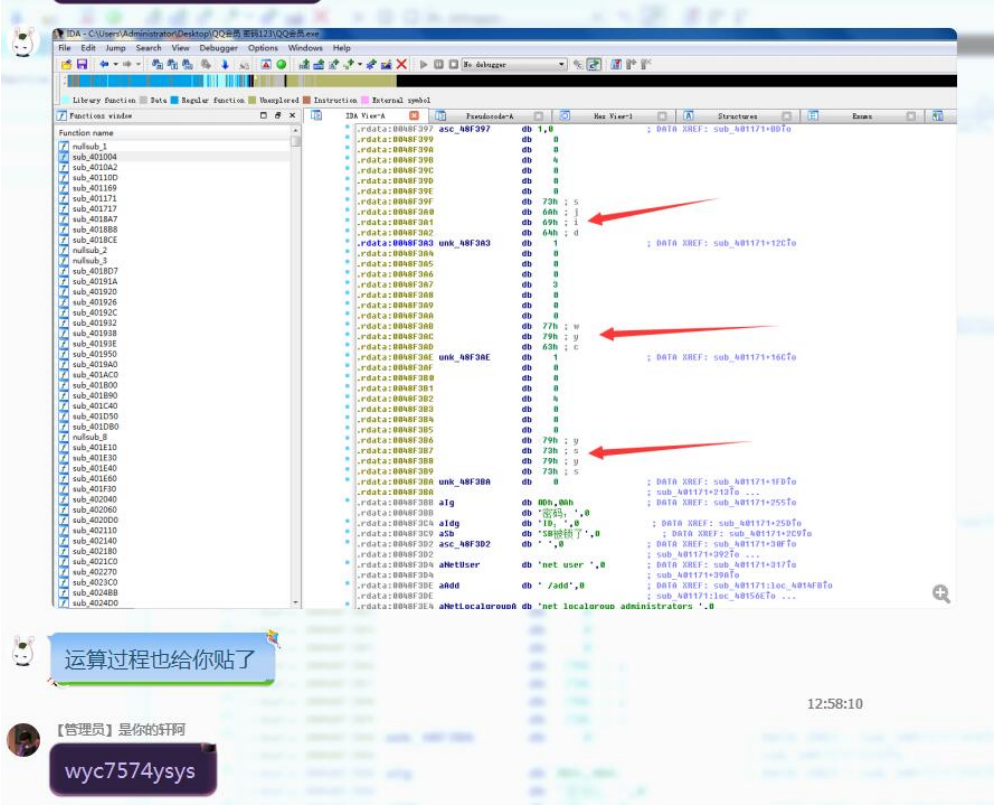
好的，的确都是wyc+4个数字+sysy的密码。说明笔者的分析是正确的。

```
IDA View-A Pseudocode-A Hex
1 int sub_401004()
2 {
3     int result; // eax@1
4     LPVOID lpMem; // [sp+0h] [bp-14h]@1
5     LPVOID v2; // [sp+4h] [bp-10h]@1
6     LPVOID v3; // [sp+8h] [bp-Ch]@1
7     LPVOID v4; // [sp+Ch] [bp-8h]@1
8     LPVOID v5; // [sp+10h] [bp-4h]@1
9
10    v5 = "1277594771";
11    v4 = "1277594771@qq.com";
12    v3 = "123456";
13    v2 = "1277594771@qq.com";
14    lpMem = "666";
15    result = sub_401171(&lpMem, &v2, &v3, &v4, &v5);
16    if ( lpMem )
17        result = sub_40192C(lpMem);
18    if ( v2 )
19        result = sub_40192C(v2);
20    if ( v3 )
21        result = sub_40192C(v3);
22    if ( v4 )
23        result = sub_40192C(v4);
24    if ( v5 )
25        result = sub_40192C(v5);
26    return result;
27 }
```

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](#)