原文地址:http://drops.wooyun.org/papers/14149

Author: kangxiaopao

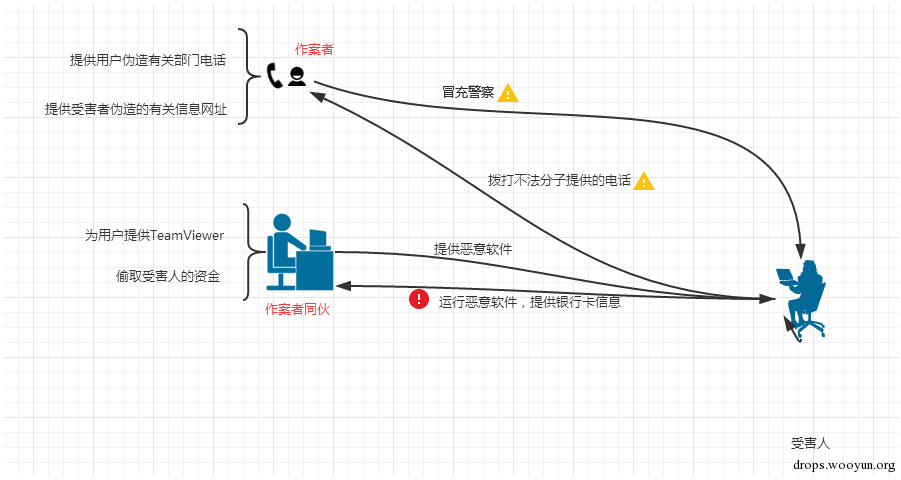
0x00 背景

TeanViewer是全球知名的合法远程控制，一般用于在线远程协助。它的一个定制版服务，已经不是第一次成为其他远控的帮凶了。在2014年的时候因为“小龙女”李若彤经纪人被骗100万轰动一时，现在又重新回到大众的视线。这次TeamViewer不再单单只是TeamViewer了，它变了。这次TeamViewer还携带着灰鸽子

0x01 变种前

变种前，不法分子主要通过广泛收集受害者信息，然后有针对性的进行欺骗。这样下来的每一单金额都相当的大。我们来看看他的主要手法，不法分子冒充警察告知用户的正涉及某项洗钱活动，把涉及金额说的相当的大，你不相信？不法分子非常贴心的为你准备了专门的热线以及网站供你查询。当你拨打不法分子为你提供的电话号码的时候，其实与你通话的就是那些对你钱包意图不轨的人。(为啥要打他给提供的电话号码呢╮(╯▽╰)╭)。它让你登录某个有关部门的网站去查看你自己的信息，一看信息什么的全对，哎哟妈呀，真的是自己啊。然后就掉进了圈套。开始对不法分子放松警惕，开始信任，并且乖乖的听话。然后我们的TeamViewer就上场了，一个定制版的TeamViewer就出现在了用户面前，你看它长的像下面这个样子。标题有没有很屌？图标有没有很吓人？

定制版的把用户名和密码都写死了的，只要你点击链接，你就自动上线了。然后在你输入你的银行卡相关信息后，你的钱钱就没了，没了，没了。是真的没了，找不回来了的那种。下面就是作案手法

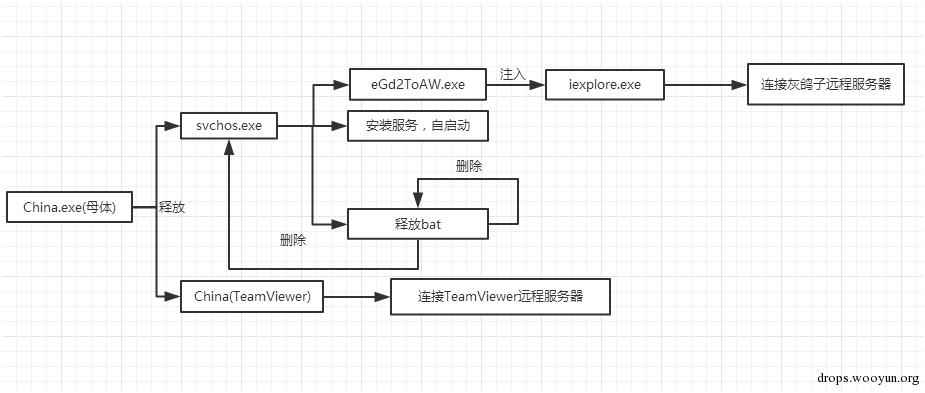


0x02 变种后

变种后的可变态了，不再是需要经过很久信息收集的对象了，而是把范围扩大了。虽然用的还是TeamViewer，可是它已不是当初的那个他了。它在原来的基础上升级了一下，在虚伪面纱背后，它还能释放出一个灰鸽子。变种前我们可以说，那都是针对有钱人的，我们看看就好，现在已经扩散开了，这就提醒了广大用户，不要轻信陌生人的电话，不要轻易点击不该点击的程序。下面我们就来探究一下新变种到底是个什么东西，从而采取预防措施。

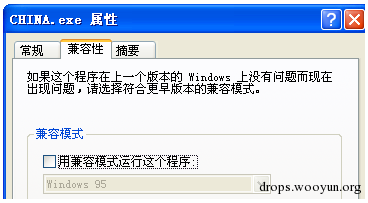
0x03 样本分析

样本执行流程

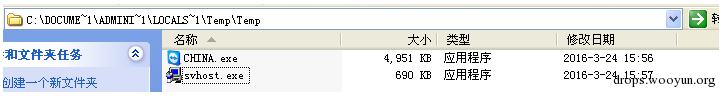


样本行为分析

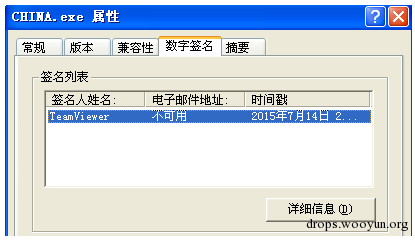
这个是母体程序，母体虽然也叫China.exe,但是他不具备TeamViewer的数字签名。它是一个恶意的程序



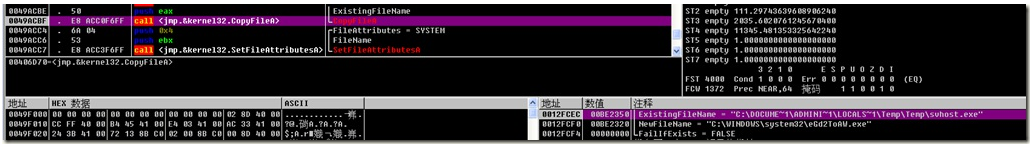
主体程序释放出两个程序，其中一个是合法的远控程序China(TeamViwer)，会连接到远程客服端，能对用户电脑进行远程控制。



看看看，这个China.exe是有签名的，这个才是正常的TeamViewer。



另外一个远控就是我们前面看到的svchost，这个远控是在背地里运行着的，所以这就降低了不法分子盗取用户资金的难度，以及使受害者范围更加的广。让我们看看他都在背后做了些什么诡异的操作。先判断在system32下是否能够找到自己的替身，没找到的话就将自己复制过去并替自己的替身将属性设置为系统文件。



然后通过调用GetVersion函数来判断程序当前运行的环境是什么系统，根据判断结果选择是否对程序的权限进行提升。为了不让操作系统 弹框框ヽ(ﾍ ▽ ﾚ)ノ

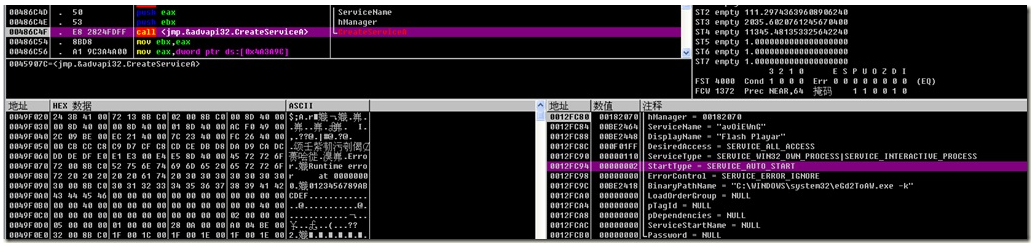
```
0045FF28  .v E9 40010000  jmp svhost.0046006D                    
0045FF2D  >  8BC3         mov eax,ebx                            Case 0 of switch 0045FF1C
0045FF2F  .  BA A8004600  mov edx,svhost.004600A8                ASCII "Win95"
0045FF34  .  E8 FB47FAFF  call svhost.00404734
0045FF39  .v E9 2F010000  jmp svhost.0046006D
0045FF3E  >  8BC3         mov eax,ebx                            Case 1 of switch 0045FF1C
0045FF40  .  BA B8004600  mov edx,svhost.004600B8                ASCII "Win98"
0045FF45  .  E8 EA47FAFF  call svhost.00404734
0045FF4A  .v E9 1E010000  jmp svhost.0046006D
0045FF4F  >  8BC3         mov eax,ebx                            Case 9 of switch 0045FF1C
0045FF51  .  BA C8004600  mov edx,svhost.004600C8                ASCII "WinMe"
0045FF56  .  E8 D947FAFF  call svhost.00404734
0045FF5B  .v E9 0D010000  jmp svhost.0046006D
0045FF60  >  8B85 6CFFFFFF mov eax,dword ptr ss:[ebp-0x94]       Case 5 of switch 0045FF02
0045FF66  .  83E8 01      sub eax,0x1                            Switch (cases 0..2)
0045FF69  .v 72 0A        jb Xsvhost.0045FF75
0045FF6B  .v 74 30        je Xsvhost.0045FF9D
0045FF6D  .  48           dec eax
0045FF6E  .v 74 3E        je Xsvhost.0045FFAE
0045FF70  .v E9 F8000000  jmp svhost.0046006D
0045FF75  >  807D FE 01   cmp byte ptr ss:[ebp-0x2],0x1          Case 0 of switch 0045FF66
0045FF79  .v 75 11        jnz Xsvhost.0045FF8C
0045FF7B  .  8BC3         mov eax,ebx
0045FF7D  .  BA D8004600  mov edx,svhost.004600D8                ASCII "Win2000"
0045FF82  .  E8 AD47FAFF  call svhost.00404734
0045FF87  .v E9 E1000000  jmp svhost.0046006D
0045FF8C  >  8BC3         mov eax,ebx
```

提升进程运行权限的地方。是不是很眼熟，大部分木马病毒程序中差不多都会看到这个代码。o(╯□╰)o

```
10  v0 = GetCurrentProcess();
11  OpenProcessToken(v0, 0xF00FFu, &TokenHandle);
12  if ( LookupPrivilegeValueA(0, "SeDebugPrivilege", &Luid) )
13  {
14    NewState.PrivilegeCount = 1;
15    NewState.Privileges[0].Attributes = 2;
16    NewState.Privileges[0].Luid = Luid;
17    AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, &PreviousState, &ReturnLength);
18  }
```

drops.wooyun.org

程序通过写入一个服务，从而让背后的远控长期驻扎在用户的系统中，而且在调用CreatService的时候，为参数StartType指定的SERVICE_AUTO_START。该远控就会在系统启动的时候，随着服务控制管理器的启动而自动启动



运行自己的替身的同时还会释放出一个bat文件，来替自己处理后事。消尸灭迹。

```
#!bash
:Repeat
del "C:\Documents and Settings\Administrator\Local Settings\Temp\Temp\svhost.exe"
 If Exist "C:\Documents and Settings\Administrator\Local Settings\Temp\Temp\svhost.exe" Goto Repeat
 del %0
```

新启动的替身会打开iexplore，并将自身注入到了iexplore进程中，让iexplore做在自己的傀儡。

```
0049DB21  .  8D45 A4      lea eax,[local.23]                     ┌pProcessInfo
0049DB24  .  50           push eax                               │
0049DB25  .  8D45 B4      lea eax,[local.19]                     │
0049DB28  .  50           push eax                               pStartupInfo
0049DB29  .  6A 00        push 0x0                               CurrentDir = NULL
0049DB2B  .  6A 00        push 0x0                               pEnvironment = NULL
0049DB2D  .  6A 04        push 0x4                               CreationFlags = CREATE_SUSPENDED
0049DB2F  .  6A 00        push 0x0                               InheritHandles = FALSE
0049DB31  .  6A 00        push 0x0                               pThreadSecurity = NULL
0049DB33  .  6A 00        push 0x0                               pProcessSecurity = NULL
0049DB35  .  68 185B4A00  push eGd2ToAW.004A5B18                 CommandLine = "C:\Program Files\Internet Explorer\iexplore.exe"
0049DB3A  .  6A 00        push 0x0                               ModuleFileName = NULL
0049DB3C  .  E8 8792F6FF  call <jmp.&kernel32.CreateProcessA>    └CreateProcessA
```

drops.wooyun.org

读取进程自己的数据到内存候中，为待会儿注入iexplore做准备

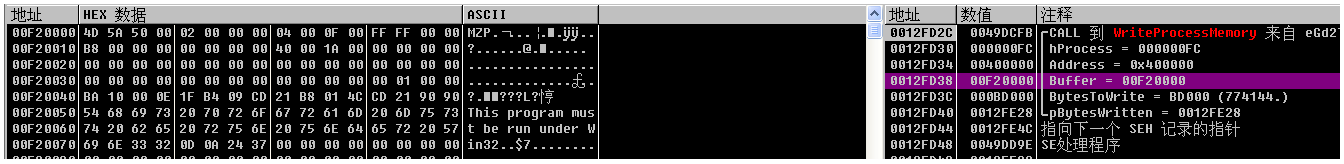
```
0049DB75  .  50           push eax                               ┌pBytesRead
0049DB76  .  6A 04        push 0x4                               BytesToRead = 0x4
0049DB78  .  8B45 0C      mov eax,[arg.2]                        │
0049DB7B  .  50           push eax                               Buffer
0049DB7C  .  8B87 A4000000 mov eax,dword ptr ds:[edi+0xA4]       │
0049DB82  .  83C0 08      add eax,0x8                            │
0049DB85  .  50           push eax                               pBaseAddress
0049DB86  .  8B06         mov eax,dword ptr ds:[esi]             │
0049DB88  .  50           push eax                               hProcess
0049DB89  .  E8 BA94F6FF  call <jmp.&kernel32.ReadProcessMemory> └ReadProcessMemory
```

drops.wooyun.org

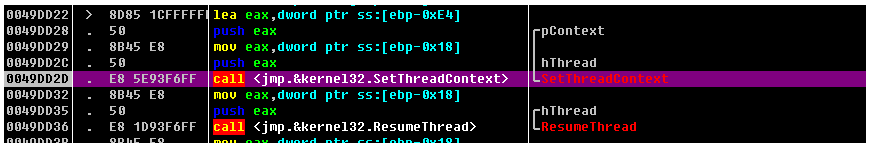
动态获取到ZwUnmapViewOfSection函数的地址，用来卸载iexplore的内存数据。同是为待会儿注入做准备。也就是跟古代小说一样，被坏人给洗脑了，什么都忘记了。

```
0049DA88  .  8BE8         mov ebp,eax
0049DA8A  .  33DB         xor ebx,ebx
0049DA8C  .  68 C8DA4900  push eGd2ToAW.0049DAC8                 ┌FileName = "ntdll.dll"
0049DA91  .  E8 6A95F6FF  call <jmp.&kernel32.LoadLibraryA>      └LoadLibraryA
0049DA96  .  8BF8         mov edi,eax
0049DA98  .  85FF         test edi,edi
0049DA9A  .v 74 23        je XeGd2ToAW.0049DABF
0049DA9C  .  68 D4DA4900  push eGd2ToAW.0049DAD4                 ┌ProcNameOrOrdinal = "ZwUnmapViewOfSection"
0049DAA1  .  57           push edi                               hModule
0049DAA2  .  E8 8194F6FF  call <jmp.&kernel32.GetProcAddress>    └GetProcAddress
0049DAA7  .  8BF0         mov esi,eax
```

然后坏人们就会开始往你的脑子里灌输一些黑暗的，反动的思想，然后我们的iexplore也就成了这个样子。ヽ(╯▽╰)ノ

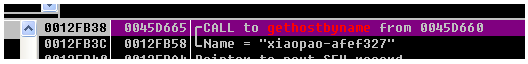


傀儡开始要做坏事了。想找到了目标，然后开始出击。调用ResumeThread会回复了线程，然后我们的傀儡进程就跑起来了



通过对域名解析，获取到ip地址，这里木马制作者用的是花生壳提供的动态域名，所以跟踪不到作者的私人信息。作者有很强的私人信息保护意识，虽然利用了两款远控软件但是两款都是都很难追踪到作者背后的信息。

获取到受害者的主机名，还有主机地址



从这里就可以很清晰的看出发送的数据

还获取了大量文件信息，然后就会进入一个长期监控的状态。等待不法分子发送远程命令。

0x04 温馨提示

为防上当受骗，提醒广大市民在接到自称“公检法”机关的来电时，一定要认真核实对方身份，切勿轻信对方发来的网址。如果遇到电脑鼠标被他人控制、显示器忽然黑屏等异常情况，应立即拔掉网线，重启电脑后使用安全软件全盘扫描杀。