

PDF钓鱼木马

一、基本信息



HASH:

f42201b5d890a96302f90102b16d7c31cfcc3b67c801ba7c6f6be223f16d7011

流程很简单，使用的C2也感觉是拿CS生成的，使用针对CS的YARA规则可以被检查出来。免杀手法也只有白加黑，Python Loader，没有对某种杀软作专门的适配，没有对痕迹进行清理等操作，不像是针对性攻击。

二、执行流程

其包含一个隐藏文件夹，快捷方式指向的是vbs脚本

名称	大小	压缩后大小
 _image_	23 972 060	11 364 736
 中国人寿团体险.pdf.lnk	1 960	1 082

vbs脚本会获取当前路径，获取后执行白加黑

```
currentDirectory = objFSO.GetAbsolutePathName(".")
```

随后直接就是Loader执行了

```
wshShell.Run Chr(34) & programPath & Chr(34) & " " & Chr(34) & arguments &  
Chr(34), 0, False
```

白程序为之前LockBit使用过的VMwareXferlogs.exe，其Loader为Python程序，使用的RC4加密，并且shellcode使用的SMC技术，会先申请内存

```

seg000:0000000000028475      mov     rdx, r14
seg000:0000000000028478      mov     [rsp+48h], r14
seg000:000000000002847D      call    rsi
seg000:000000000002847F      mov     edx, [r15+50h]
seg000:0000000000028483      mov     r9d, 40h ; '@'
seg000:0000000000028489      mov     rcx, r14
seg000:000000000002848C      mov     r8d, 3000h
seg000:0000000000028492      call    rbx
seg000:0000000000028494      mov     rsi, rax
seg000:0000000000028497      test    rax, rax
seg000:000000000002849A      jnz     short loc_284BC
seg000:000000000002849C      mov     edx, [r15+50h]
seg000:00000000000284A0      mov     r9d, 40h ; '@'
seg000:00000000000284A6      mov     r8d, 3000h
seg000:00000000000284AC      xor     ecx, ecx
seg000:00000000000284AE      call    rbx
seg000:00000000000284B0      mov     rsi, rax
seg000:00000000000284B3      test    rax, rax
seg000:00000000000284B6      jz      loc_282F5
seg000:00000000000284B8

```

然后将数据写入申请的内存

```

seg000:00000000000284BC      mov     rbx, [rsp+30h]
seg000:00000000000284C1      mov     rdx, rdi
seg000:00000000000284C4      mov     rcx, rsi
seg000:00000000000284C7      xor     r15d, r15d
seg000:00000000000284CA      mov     [rbx+30h], rsi
seg000:00000000000284CE      mov     r8d, [rbx+54h]
seg000:00000000000284D2      call    r13

```

然后修复为PE文件执行，其远控感觉为CS生成的.....执行流程感觉差不多，都是先对IP地址解密，然后建立链接

00501FE1	E8 60 7F 00 00	call 509F46	
00501FE6	50	push eax	
00501FE7	6A 03	push 3	
00501FE9	FF 75 10	push dword ptr ss:[ebp+10]	[ebp+10]:Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.2;
00501FEC	FF 15 A4 62 52 00	call dword ptr ds:[<&InternetOpenA>]	
00501FF2	A3 84 5F 53 00	mov dword ptr ds:[335F84],eax	
00501FF7	8B 35 90 62 52 00	mov esi,dword ptr ds:[<&InternetSetOptionA>]	
00501FFD	6A 04	push 4	
00501FFF	8D 45 FC	lea eax,dword ptr ss:[ebp-4]	
00502002	50	push eax	
00502003	6A 05	push 5	
00502005	FF 35 84 5F 53 00	push dword ptr ds:[335F84]	esi:InternetSetOptionA
00502008	FF D6	call esi	
0050200D	6A 04	push 4	
0050200F	8D 45 FC	lea eax,dword ptr ss:[ebp-4]	
00502012	50	push eax	
00502013	6A 06	push 6	
00502015	FF 35 84 5F 53 00	push dword ptr ds:[335F84]	esi:InternetSetOptionA
00502018	FF D6	call esi	
0050201D	68 40 2C 53 00	push 532C40	
00502022	57	push edi	
00502023	6A 03	push 3	
00502025	57	push edi	
00502026	57	push edi	

dump出的内容拿检测CS的yara规则也能匹配上.....