Lấy địa chỉ kernel32.dll

Tính định chỉ ảo Exportable trên memory

Từ bảng Exportable tìm hàm GetProcessAddress

Sử dụng hàm GetProcAdress lấy địa chỉ các hàm LoadLibraryA, VirtualProtect, user32.dll, MessageBoxA, CreateFile, ReadFile, WriteFile, SetFilePoiter, CloseHandle, Lstrcmp, FindNextFileA, FindNextFileA

Lây nhiễm:

Hiển thị thong báo lây nhiễm thành công

Chỉnh sửa format vùng shellcode thành exe + readwrite

Tìm kiếm file

Inject

Display

Search()

findFirstFile

findNextFile

call infection

createfile

check MZ signature

unicode\_string(setfilepointer, readfile)

check PE

read section alignment, file alignment, entrypoint, sizeofimage, numberofSection

change:

read virtualsize

characteristics, rawsize, virtualsize

rawsize += shellcodesize = virtualsize

write entrypoint, sizeofimage

write virus

numofbytetofill

Đọc thông tin của file:

{

CreateFile(0,20,3,0,1,c000000h,namefile)

ReadFile(overlapped, numByteReaded, Buff save, hFile)

Edit header file

Check PE, signature by function readfile

Read number of Section, EntryPoint, ImageSize, Section Alignment, File Alignment

}

Thay đổi thông tin của file:

{

Đọc VirtualSize

Tính RawSize, VirtualSize, Characteristics

Sửa VitualSize

Sửa NewEntryPoint

Sửa Sizeofimage

Ghi shellcode vào cuối file

Lấp đầy các byte 0

Kí tên

}

Thay đổi thông tin

{

newVirtualSize = lastS->SizeOfRawData + 100 = newRawSize

Sizeofimage, VirtualSize, RawSize, Characteristics, SW

}

Fs:30h địa chỉ base address của PEB

PEB -> kernel32.dll đọc exportable kernel32.dll lấy LoadLibrary & GetProcessAddress

VA ImageBaseKernel in memory

VAPEsignatureinmem

RVA Exportableinfile = VA Pesignature + 78h

VAImageBaseKernelInFile = VA Pesignature +34h

ImageBase = VA ImageBaseKernelInmem – VAImageBasekernelinFile

* VAExportableinmem = RVA exportableinfile + VA imageinfile + offset imagebase