

TREE Case Study - Sage

Sage

Application Mode: User Mode

Target: Windows

Sample ran on:

Windows 7 32-bit for IDA 6.4 environment

Description

Sage example. Branch Condition propagation for input file.

Sage.c

```
#include "windows.h"
#include <stdio.h>

HANDLE hFile = NULL;

int main(int argc, char** argv)
{
    int j = 0;
    DWORD dwBytesRead=0;
    char input[4];

    hFile = CreateFile("mytaint.txt",          // Open One.txt
        GENERIC_READ,                        // Open for reading
        0,                                    // Do not share
        NULL,                                // No security
        OPEN_EXISTING,                       // Existing file only
        FILE_ATTRIBUTE_NORMAL,               // Normal file
        NULL);                               // No template file

    if (hFile == INVALID_HANDLE_VALUE)
    {
        return 1;
    }

    ReadFile(hFile, input, 4, &dwBytesRead, NULL);




    CloseHandle(hFile);

    if (input[0] == 'b') j++;
    if (input[1] == 'a') j++;
    if (input[2] == 'd') j++;
    if (input[3] == '!') j++;
    if (j == 4) printf("bad!");
    else printf("ok!");
    return 0;
}
```

Configuring the Tracer

Indicate mytaint.txt file content

Configuring the Tracer



Configurable Parameters

☐ Interactive Mode

Application:

Path:

Arguments:

☐ Remote ☐ PIN

Host: Password: Port:

Application: Sage.exe

Path: ...\\Sage.exe

Filters: mytaint.txt

Taint Propagation Policy - Taint Branch

Taint Propagation Policy

☐ Taint_DATA

☒ Taint_BRANCH

☐ Taint_COUNTER

☐ Taint_ADDRESS

Instruction Set Architecture

☒ x86

☐ x86_64

☐ ARM

☐ PPC

☐ MIPS

Taint Branch

Image Load Table			Taint Source Table		
Name	Address	Size	Input Address	Size	Input Bytes
["sage.exe"]	0x13c0000	0xf000	0x43fe04	4	676f6f64
ntdll.dll	0x778c0000	0x180000			
kernel32.dll	0x761f0000	0x110000			
kernel32.dll	0x761f0000	0x110000			
KernelBase.dll	0x76400000	0x47000			

Taint Table

UUID	Type	Name	Start Sequence	End Sequence	Transformation Instruction
499	branch	0x30	0x30		jnz 0x9
506	register	ecx_0_9412	0x37	0x44	movsb -0x1(%ebp), %ecx
493	input	0x3fe04	0x0		0xd3c105d
508	branch	0x39	0x39		jnz 0x9
494	input	0x3fe05	0x0		0xd3c105d
500	register	eax_0_9412	0x21	0x43	movsb -0x2(%ebp), %eax
495	input	0x3fe06	0x0		0xd3c105d
507	register	eflags_9412	0x38		cmp 0x21, %ecx
497	register	ecx_0_9412	0x2e	0x37	movsb -0x4(%ebp), %ecx
503	register	edx_0_9412	0x34	0x109	movsb -0x2(%ebp), %edx
502	branch	0x33	0x33		jnz 0x9
505	branch	0x36	0x36		jnz 0x9
496	input	0x3fe07	0x0		0xd3c105d
498	register	eflags_9412	0x2f	0x32	cmp 0x62, %ecx
504	register	eflags_9412	0x35	0x38	cmp 0x64, %edx
501	register	eflags_9412	0x32	0x35	cmp 0x63, %eax

Taint Graph

