Intercepting API

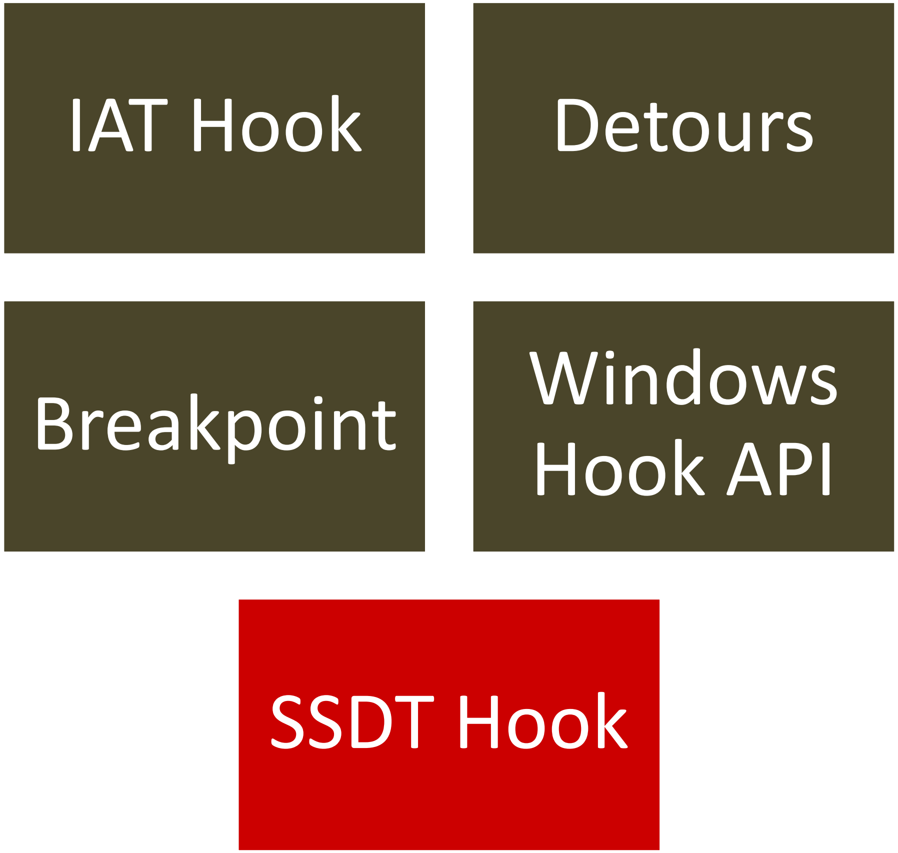
Win32 API Hooking

API Hooking

- API Hooking is the process of **intercepting** a given **API** by overwriting its entry point instruction or redirecting a call to it with the address of a **stub function**.

  The stub function usually returns control back to the original function after performing required operations.

API Hooking: Techniques



IAT Hook

Detours

Breakpoint

Windows Hook API

SSDT Hook

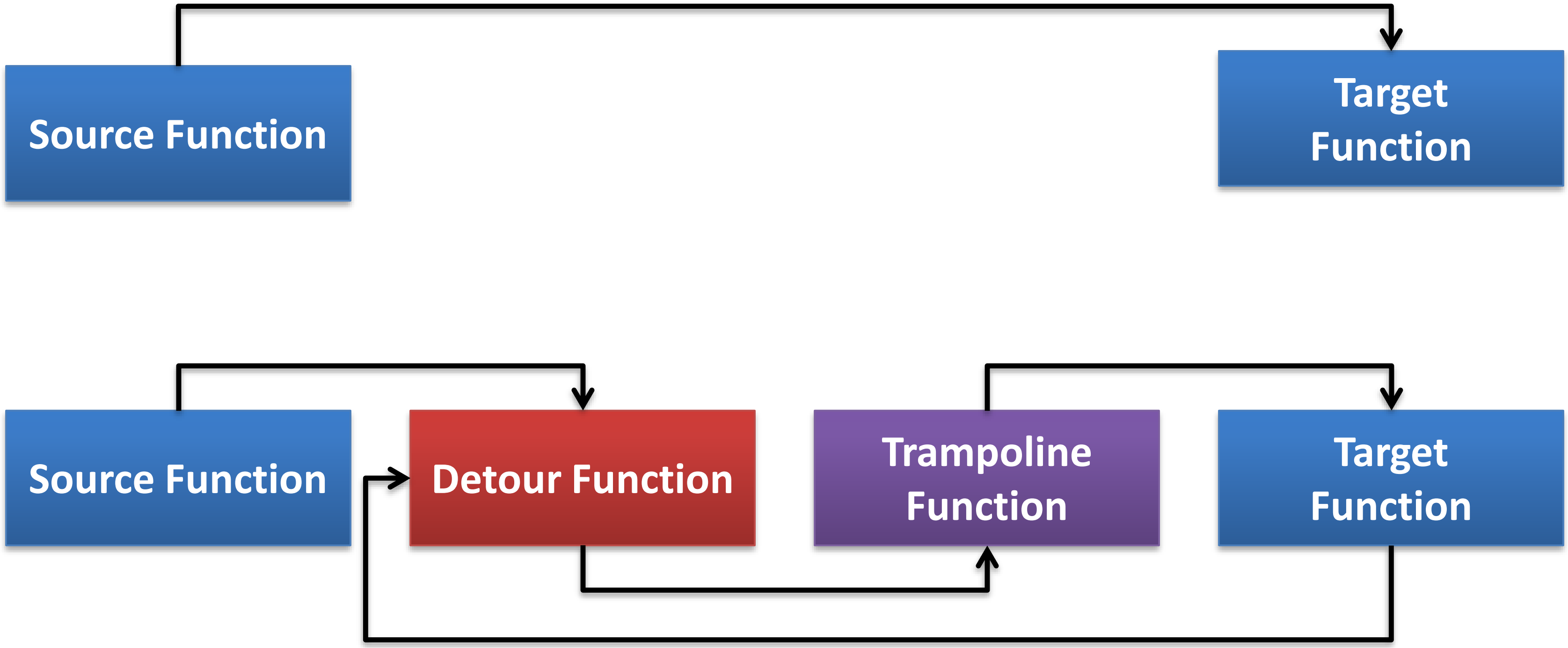
API Hooking Techniques

IAT/EAT Hook	Overwrite IAT/EAT entry for a given API with stub address
Detour	Microsoft Detour Library for API Interception
Breakpoint	Windows Debug API
Windows Hook API	*SetWindowsHookEx*(…) for MSG Interception. Can be per process or system wide.
SSDT Hook	System Service Dispatcher Table based Interception (Kernel Mode)

Win32 MSG Hooks

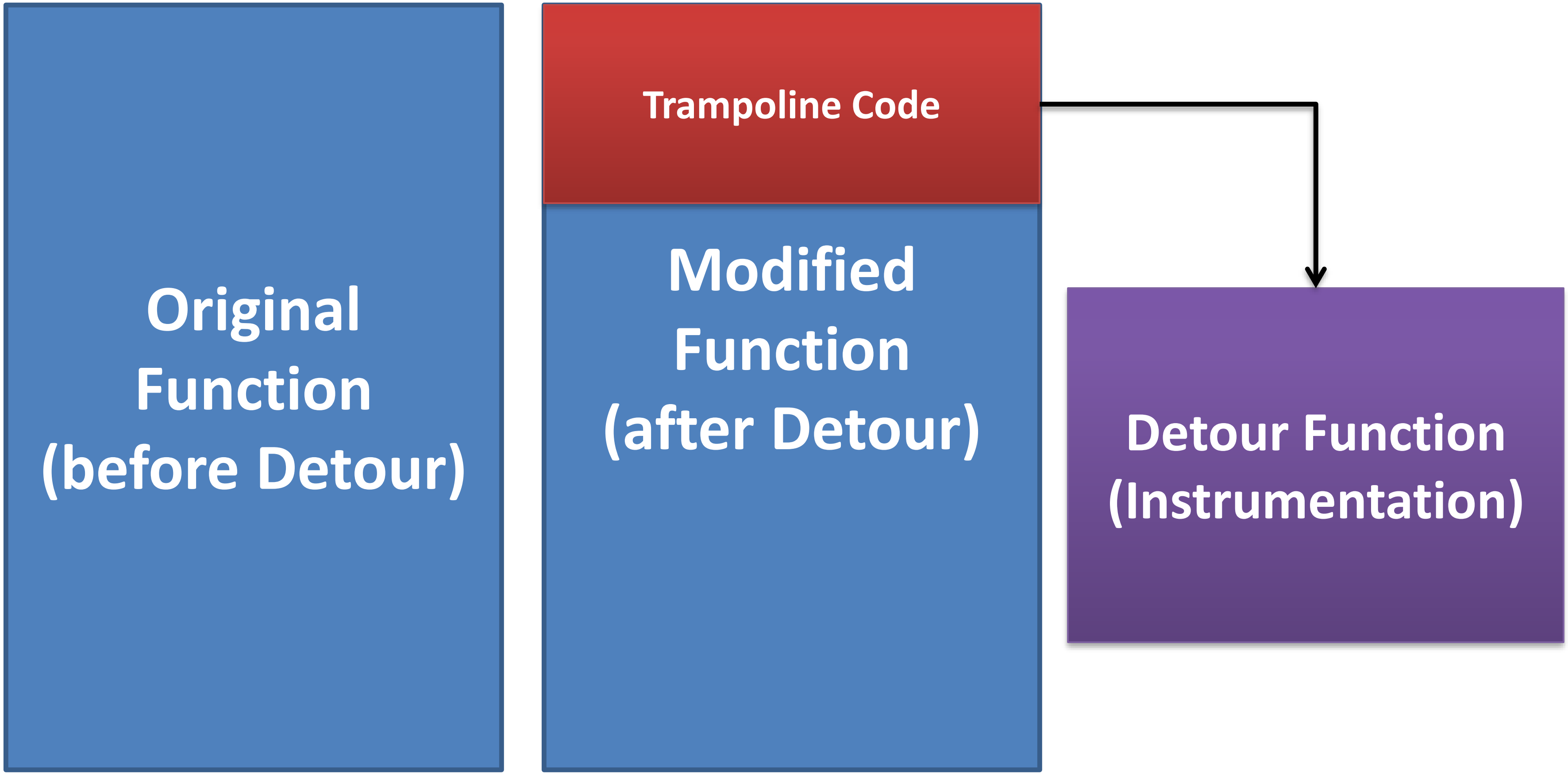
- WH_CALLWNDPROC
- WH_CBT
- WH_FOREGROUNDIDLE
- WH_GETMESSAGE
- WH_JOURNALRECORD
- WH_JOURNALPLAYBACK
- WH_KEYBOARD
- WH_MOUSE
- […]

API Hooking: Microsoft Detours Way



http://research.microsoft.com/en-us/projects/detours/

API Hooking: Microsoft Detours Way


Original Function (before Detour)
Trampoline Code
Modified Function (after Detour)
Detour Function (Instrumentation)

Microsoft Detours: HOW TO

Original Function →

```
BOOL (WINAPI *) Real_ExitWindowsEx(UINT a1,
DWORD a2) = &ExitWindowsEx
```

Begin Update →

```
DetourTransactionBegin();
DetourUpdateThread(GetCurrentThread());
```

Attach Detour →

```
DetourAttach(
        (LPVOID*)  &Real_ExitWindowsEx,
        (LPVOID)   &My_ExitWindowsEx
);
```

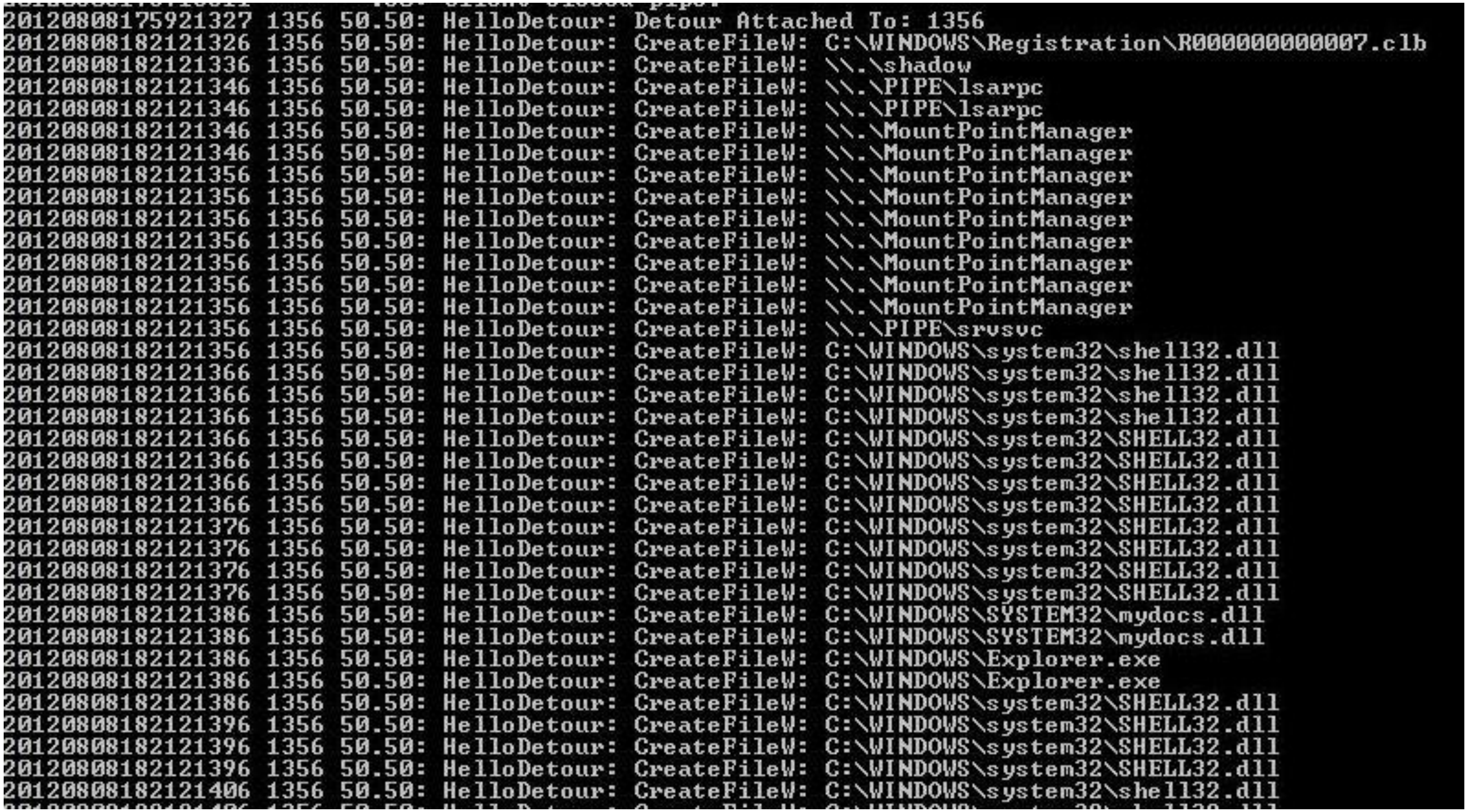
Commit Update →

```
DetourTransactionCommit();
```

API Hooking: Common Applications

- Process Instrumentation
- Dynamic Program Analysis
  - Automatic Malware Analysis
- Vulnerability Analysis
- Exploit Development
- Hot Patching
- Etc.

API Hooking: Detours in Action



```
20120808175921327 1356 50.50: HelloDetour: Detour Attached To: 1356
20120808182121326 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\Registration\R000000000007.clb
20120808182121336 1356 50.50: HelloDetour: CreateFileW: \\.\shadow
20120808182121346 1356 50.50: HelloDetour: CreateFileW: \\.\PIPE\lsarpc
20120808182121346 1356 50.50: HelloDetour: CreateFileW: \\.\PIPE\lsarpc
20120808182121346 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121346 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\MountPointManager
20120808182121356 1356 50.50: HelloDetour: CreateFileW: \\.\PIPE\srvsvc
20120808182121356 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\shell32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\shell32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\shell32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\shell32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121366 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121376 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121376 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121376 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121376 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121386 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\SYSTEM32\mydocs.dll
20120808182121386 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\SYSTEM32\mydocs.dll
20120808182121386 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\Explorer.exe
20120808182121386 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\Explorer.exe
20120808182121386 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121396 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121396 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121396 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\SHELL32.dll
20120808182121406 1356 50.50: HelloDetour: CreateFileW: C:\WINDOWS\system32\shell32.dll
```

Time to look into the CODE