MalwareAnalysis.co

HUNTING PROCESS INJECTION BY WINDOWS API CALLS

BY NIR YEHOSHUA (@NIRYEHO) AND URIEL KOSAYEV (@MALFUZZER)

Thanks to Adam (@hexacorn): http://www.hexacorn.com/blog/ and
Odzhan: https://modexp.wordpress.com/author/odzhan/

CLASSIC DLL INJECTION	OpenProcess,VirtualAllocEx, WriteProcessMemory, CreateRemoteThread
DLL INJECTION USING SETWINDOWSHOOKEX	LoadLibrary / LoadLibraryEx, GetProcAddress, SetWindowsHookEx.
APC INJECTION	CreateToolhelp32Snapshot, Process32First, Thread32First, Thread32Next, Process32Next, OpenProcess, VirtualAllocEx, WriteProcessMemory, QueueUserAPC / NtQueueApcThread, VirtualFreeEx, CloseHandle.
ATOM BOMBING	CreateToolhelp32Snapshot, Thread32First, Thread32Next, OpenThread, CreateEvent, DuplicateHandle, NtQueueApcThread, QueueUserAPC, GetModuleHandle, GetProcAddress, SetEvent, GetCurrentProcess, SleepEx WaitForMultipleObjectsEx MsgWaitForMultipleObjectsEx, CloseHandle.
ALPC INJECTION	NtQuerySystemInformation, NtDuplicateObject / ZwDuplicateObject, GetCurrentProcess, NtQueryObject, NtClose, RtlInitUnicodeString, NtConnectPort, VirtualAllocEx, WriteProcessMemory, CopyMemory, ReadProcessMemory, VirtualFreeEx, VirtualQueryEx, GetMappedFileName, OpenProcess, CloseHandle, GetSystemInfo.
LOCKPOS	CreateFileMappingW, MapViewOfFile, RtlAllocateHeap, NtCreateSection, NtMapViewOfSection, NtCreateThreadEx.
PROCESS HOLLOWING	CreateProcess("CREATE_SUSPENDED"),NtQueryProcessInformation, ReadProcessMemory, GetModuleHandle, GetProcAddress, ZwUnmapViewOfSection / NtUnmapViewOfSection, VirtualAllocEx, WriteProcessMemory, VirtualProtectEx, SetThreadContext, ResumeThread.
PROCESS DOPPELGÄNGING	CreateFileTransacted, WriteFile, NtCreateSection, RollbackTransaction, NtCreateProcessEx, RtlCreateProcessParametersEx, VirtualAllocEx, WriteProcessMemory, NtCreateThreadEx, NtResumeThread.

REFLECTIVE PE INJECTION	CreateFileA, HeapAlloc, OpenProcessToken, OpenProcess, VirtualAlloc, GetProcAddress LoadRemoteLibraryR / LoadLibrary, HeapFree, CloseHandle.
THREAD EXECUTION HIJACKING	RtlAdjustPrivilege, OpenProcess, CreateToolhelp32Snapshot, Thread32First, Thread32Next, CloseHandle, VirtualAllocEx, OpenThread, VirtualFree / VirtualFreeEx, SuspendThread, GetThreadContext, VirtualAlloc, WriteProcessMemory, SetThreadContext, ResumeThread.
KERNEL CALLBACK TABLE	FindWindowA, GetWindowThreadProcessId OpenProcess, NtQueryInformationProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, SendMessage, VirtualFreeEx
CLIPBRDWNDCLASS	FindWindowEx("CLIPBRDWNDCLASS"), OpenProcess, VirtualAllocEx, WriteProcessMemory, SetProp("ClipboardDataObjectInterface"), VirtualFreeEx.
PROPAGATE	FindWindow("Progman"), FindWindowEx("SHELLDLL_DefView"), GetProp("UxSubclassInfo"), GetWindowThreadProcessId, OpenProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, SetProp("UxSubclassInfo"), PostMessage, VirtualFreeEx.
EARLY BIRD	CreateProcessA, VirtualAllocEx, WriteProcessMemory, QueueUserAPC, ResumeThread.
CONSOLEWINDOWCLASS	FindWindow("ConsoleWindowClass"), GetWindowThreadProcessId, OpenProcess, ReadProcessMemory, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx.
TOOLTIP PROCESS INJECTION	FindWindow("tooltips_class32"), OpenProcess, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx, CloseHandle.
DNS API	GetWindowThreadProcessId, CreateThread, GetTickCount, OpenProcess, VirtualAllocEx, WriteProcessMemory, VirtualFreeEx, TerminateThread.