Supplementary Materials for Open Source Intelligence for Malicious Behavior Discovery and Interpretation

Yi-Ting Huang, Chi Yu Lin, Ying-Ren Guo, Kai-Chieh Lo,
Yeali S. Sun, and Meng Chang Chen

SUPPLEMENTARY A. WINDOWS API CALLS

TABLE SI
THE API CALLS RELATED TO DISCOVER TTPS ARE USED IN THIS STUDY.

Category	API Function Name	Argument Name
File	NtCreateFile, NtOpenFile, NtReadFile, CopyFile, NtWriteFile, NtDeleteFile, GetFileAttributes, SetFileAttributesW, DeleteFile, GetSystemDirectory, CreateDirectoryW, RemoveDirectory, GetSystemWindowsDirectory	filepath, dirpath, oldfilepath, newfilepath
Service	CreateService, OpenService, StartService, DeleteService, ControlService	display_name, service_name, filepath
System	LdrLoadDll, LdrGetDllHandle, LdrGetProcedureAddress, SetWindowsHookEx	module_name, module_address, module
Process	NtProtectVirtualMemory, AssignProcessToJobObject, CreateRemoteThread, CreateProcessInternalW, CreateToolhelp32Snapshot, NtFreeVirtualMemory, NtAllocateVirtualMemory, CreateThread, Module32FirstW, Module32NextW, NtCreateProcessEx, CreateJobObjectW, NtCreateThread, ShellExecuteExW, NtGetContextThread, NtMapViewOfSection, NtOpenProcess, NtOpenSection, NtUnmapViewOfSection, NtSuspendThread, NtResumeThread, NtOpenThread, NtWriteVirtualMemory, RtlCreateUserThread, NtReadVirtualMemory, NtCreateSection, NtSetContextThread, Process32FirstW, Process32NextW, ReadProcessMemory, NtCreateSection, NtQueueApcThread, NtTerminateProcess, NtTerminateThread, WriteProcessMemory	previous_suspend_count, process_identifier, stack_dep_bypass, heap_dep_bypass, access, snapshot_handle, process_handle, parameter, section_handle, desired_access, job_handle, win32_protect, ThreadHandle, thread_handle, suspend_count, process_name, section_name, base_address, stack_pivoted, region_size, status_code, protection, free_type, flags, view_size, suspended, filepath, parameters command_line, size
Registry	NtCreateKey, RegCreateKey, NtOpenKey, RegOpenKey, NtQueryKey, NtSaveKey, RegDeleteValue, NtQueryValueKey, RegQueryInfoKey, RegQueryValueEx, NtEnumerateKey, NtEnumerateValueKey, RegEnumKey, RegEnumValue, RegSetValue, NtQueryMultipleValueKey, NtSetValueKey, NtDeleteKey, RegDeleteKey, NtDeleteValueKey	regkey, value, filepath
Network	URLDownloadToFileW, InternetConnect, gethostbyname, shutdown, connect, accept, recv, send, recvfrom, sendto, listen, select, bind, socket, closesocket, WSAAccept, WSAConnect, WSARecv, WSARecvFrom, WSASend, WSASendTo, WSASocket, getsockname, GetAddrInfoW, DnsQuery	filepath, hostname, ip_address, port, protocol, s, service, socket, url