Malware Analysis Report

VirusTotal Report

Malicious: 0

Suspicious: 0

Undetected: 71

Strings Analysis

IP Addresses: 2

URLs: 1

Executable Keywords: 4

Hex Encoded: 0

PE Analysis

Entry Point: 0x23bc0

Image Base: 0x140000000

Sections: .text, .rdata, .data, .pdata, .didat, .rsrc, .reloc

Imports: {'KERNEL32.dll': ['GetProcAddress', 'CreateMutexExW', 'AcquireSRWLockShared', 'DeleteCriticalSection', 'GetCurrentProcessId', 'GetProcessHeap', 'GetModuleHandleW', 'DebugBreak', 'IsDebuggerPresent', 'GlobalFree', 'GetLocaleInfoW', 'CreateFileW', 'ReadFile', 'GetACP', 'MulDiv', 'GetCurrentProcess', 'GetCommandLineW', 'HeapSetInformation', 'FreeLibrary', 'LocalFree', 'LocalAlloc', 'FindFirstFileW', 'FindClose', 'FoldStringW', 'GetModuleFileNameW', 'GetUserDefaultUILanguage', 'HeapFree', 'HeapAlloc', 'GetTimeFormatW', 'WideCharToMultiByte', 'WriteFile', 'GetFileAttributesW', 'LocalLock', 'LocalUnlock', 'DeleteFileW', 'SetEndOfFile', 'GetFileAttributesExW', 'GetFileInformationByHandle', 'CreateFileMappingW', 'MapViewOfFile', 'MultiByteToWideChar', 'LocalReAlloc', 'UnmapViewOfFile', 'GetFullPathNameW', 'LocalSize', 'GetStartupInfoW', 'lstrcmpiW', 'FindNLSString', 'GlobalLock', 'GlobalUnlock', 'GlobalAlloc', 'GetDiskFreeSpaceExW', 'CreateDirectoryW', 'RegisterApplicationRestart',

'CreateSemaphoreExW', 'CreateThreadpoolTimer', 'ReleaseSRWLockShared', 'SetThreadpoolTimer', 'CloseHandle', 'OpenSemaphoreW', 'WaitForSingleObjectEx', 'AcquireSRWLockExclusive', 'CloseThreadpoolTimer', 'OutputDebugStringW', 'ReleaseSRWLockExclusive', 'GetLastError', 'FormatMessageW', 'ReleaseMutex', 'GetCurrentThreadId', 'WaitForSingleObject', 'WaitForThreadpoolTimerCallbacks', 'InitializeCriticalSectionEx', 'LeaveCriticalSection', 'GetModuleHandleExW', 'ReleaseSemaphore', 'EnterCriticalSection', 'GetDateFormatW', 'SetLastError', 'GetLocalTime', 'ResolveDelayLoadedAPI', 'DelayLoadFailureHook', 'GetModuleFileNameA']}, {'GDI32.dll': ['CreateDCW', 'StartPage', 'StartDocW', 'SetAbortProc', 'DeleteDC', 'EndDoc', 'AbortDoc', 'EndPage', 'GetTextMetricsW', 'SetBkMode', 'LPtoDP', 'SetWindowExtEx', 'SetViewportExtEx', 'SetMapMode', 'GetTextExtentPoint32W', 'TextOutW', 'EnumFontsW', 'GetTextFaceW', 'SelectObject', 'DeleteObject', 'CreateFontIndirectW', 'GetDeviceCaps']}, {'USER32.dll': ['PostMessageW', 'MessageBoxW', 'GetMenu', 'CheckMenuItem', 'GetSubMenu', 'EnableMenuItem', 'ShowWindow', 'GetDC', 'ReleaseDC', 'SetCursor', 'GetDpiForWindow', 'SetActiveWindow', 'LoadStringW', 'DefWindowProcW', 'IsIconic', 'SetFocus', 'PostQuitMessage', 'DestroyWindow', 'MessageBeep', 'GetForegroundWindow', 'GetDlgCtrlID', 'SetWindowPos', 'RedrawWindow', 'GetKeyboardLayout', 'CharNextW', 'SetWinEventHook', 'GetMessageW', 'TranslateAcceleratorW', 'IsDialogMessageW', 'TranslateMessage', 'DispatchMessageW', 'UnhookWinEvent', 'SetWindowTextW', 'OpenClipboard', 'IsClipboardFormatAvailable', 'CloseClipboard', 'SetDlgItemTextW', 'GetDlgItemTextW', 'EndDialog', 'SendDlgItemMessageW', 'SetScrollPos', 'InvalidateRect', 'UpdateWindow', 'GetWindowPlacement', 'SetWindowPlacement', 'CharUpperW', 'GetSystemMenu', 'LoadAcceleratorsW', 'SetWindowLongW', 'CreateWindowExW', 'MonitorFromWindow', 'RegisterWindowMessageW', 'LoadCursorW', 'RegisterClassExW', 'GetWindowTextLengthW', 'GetWindowLongW', 'PeekMessageW', 'GetWindowTextW', 'EnableWindow', 'CreateDialogParamW', 'DrawTextExW', 'LoadIconW', 'LoadImageW', 'DialogBoxParamW', 'SetThreadDpiAwarenessContext', 'SendMessageW', 'MoveWindow', 'GetClientRect', 'GetFocus']}, {'api-ms-win-crt-string-l1-1-0.dll': ['memset', 'wcsnlen', 'wcscmp']}, {'api-ms-win-crt-runtime-l1-1-0.dll': ['_c_exit', '_register_thread_local_exe_atexit_callback', '_initterm_e', '_initterm']}, {'api-ms-win-crt-private-l1-1-0.dll': ['_o__callnewh', '_o__cexit', '_o__configthreadlocale', '_o__configure_wide_argv', '_o__crt_atexit', '_o__errno', '_o__exit', '_o__get_wide_winmain_command_line', '_o__initialize_onexit_table', '_o__initialize_wide_environment',

'_o__invalid_parameter_noinfo', '_o__purecall', '_o__register_onexit_function', '_o__seh_filter_exe', '_o__set_app_type', '_o__set_fmode', '_o__set_new_mode', '_o__wcsicmp', '_o__wtol', '_o_exit', '_o_free', '_o_iswdigit', '_o_malloc', '_o_terminate', '_o_toupper', '__CxxFrameHandler3', '_CxxThrowException', '_o___std_exception_destroy', '_o___std_exception_copy', '_o___p__commode', '_o___stdio_common_vswprintf', '__C_specific_handler', 'memcmp', 'memcpy', 'memmove']}, {'api-ms-win-core-com-l1-1-0.dll': ['CoWaitForMultipleHandles', 'CoUninitialize', 'PropVariantClear', 'CoTaskMemFree', 'CoTaskMemAlloc', 'CoCreateFreeThreadedMarshaler', 'CoCreateInstance', 'CoInitializeEx', 'CoCreateGuid']}, {'api-ms-win-core-shlwapi-legacy-l1-1-0.dll': ['PathIsFileSpecW', 'PathFindExtensionW', 'PathFileExistsW']}, {'api-ms-win-shcore-obsolete-l1-1-0.dll': ['SHStrDupW']}, {'api-ms-win-shcore-path-l1-1-0.dll': ['None']}, {'api-ms-win-shcore-scaling-l1-1-1.dll': ['GetDpiForMonitor']}, {'api-ms-win-core-rtlsupport-l1-1-0.dll': ['RtlLookupFunctionEntry', 'RtlCaptureContext', 'RtlVirtualUnwind']}, {'api-ms-win-core-errorhandling-l1-1-0.dll': ['SetUnhandledExceptionFilter', 'UnhandledExceptionFilter', 'RaiseException']}, {'api-ms-win-core-processthreads-l1-1-0.dll': ['TerminateProcess']}, {'api-ms-win-core-processthreads-l1-1-1.dll': ['GetProcessMitigationPolicy', 'IsProcessorFeaturePresent']}, {'api-ms-win-core-profile-l1-1-0.dll': ['QueryPerformanceCounter']}, {'api-ms-win-core-sysinfo-l1-1-0.dll': ['GetTickCount', 'GetSystemTimeAsFileTime']}, {'api-ms-win-core-interlocked-l1-1-0.dll': ['InitializeSListHead']}, {'api-ms-win-core-libraryloader-l1-2-0.dll': ['LoadLibraryExW']}, {'api-ms-win-core-winrt-string-l1-1-0.dll': ['WindowsCreateString', 'WindowsDeleteString', 'WindowsGetStringRawBuffer', 'WindowsCreateStringReference']}, {'api-ms-win-core-synch-l1-1-0.dll': ['SetEvent', 'CreateEventExW']}, {'api-ms-win-core-winrt-error-l1-1-0.dll': ['SetRestrictedErrorInfo']}, {'api-ms-win-core-string-l1-1-0.dll': ['CompareStringOrdinal']}, {'api-ms-win-core-winrt-l1-1-0.dll': ['RoInitialize', 'RoUninitialize', 'RoGetActivationFactory']}, {'api-ms-win-core-winrt-error-l1-1-1.dll': ['RoGetMatchingRestrictedErrorInfo']}, {'api-ms-win-eventing-provider-l1-1-0.dll': ['EventProviderEnabled']}, {'api-ms-win-core-synch-l1-2-0.dll': ['Sleep']}, {'COMCTL32.dll': ['CreateStatusWindowW', 'None']}