Malware Analysis Report

VirusTotal Report:

Harmless: 0
Malicious: 63
Suspicious: 0
Undetected: 9
Timeout: 0

File Metadata:

File Type: Win32 DLL
SHA256: 7f26bcad404867f92ee0f3de9257758132b2ea06884f436e7900e820ddd6646a
MD5: d98b63a319ad92b6c3a8347ade5a351a
SHA1: 698e02d1142d2c816511422aece03bfa10399e91
Reputation Score: -1
Popular Threat Label: trojan.idicaf/bckdr
First Submission Date: 2012-02-26 12:27:28
Last Analysis Date: 2025-04-25 22:41:19
Total Votes: Harmless: 1, Malicious: 2
Signature Info: product: Microsoft(R) Windows(R) Operating System, description: File Encryption Utility, copyright: (C) Microsoft Corporation. All rights reserved., file version: 5.1.2201.1329, internal name: X-doorc

Strings Analysis Summary:

IP Addresses: 1
URLs: 1
Executable Keywords: 9
Hex Encoded: 0
Base64 Strings: 38
Suspicious File Paths: 3
Registry Keys: 0
Email Addresses: 0
Embedded Powershell: 0

PE Analysis:

Entry Point: 0x1516d
Image Base: 0x10000000
Compilation Time: 2008-06-09 12:49:29
PE Header:
  Machine: 0x14c
  Number of Sections: 6
  Subsystem: 0x2
  DLL: True
File Size: 134160
Size of Image: 627880

Sections:

- {'Name': '.text', 'Entropy': 6.52, 'Size': 82944, 'Executable': True, 'Writable': False, 'Suspicious': False}
- {'Name': '.rdata', 'Entropy': 5.32, 'Size': 8704, 'Executable': False, 'Writable': False, 'Suspicious': False}
- {'Name': '.data', 'Entropy': 7.46, 'Size': 18944, 'Executable': False, 'Writable': True, 'Suspicious': True}
- {'Name': 'xdoors_d', 'Entropy': 5.09, 'Size': 11776, 'Executable': False, 'Writable': True, 'Suspicious': False}
- {'Name': '.rsrc', 'Entropy': 3.17, 'Size': 1024, 'Executable': False, 'Writable': False, 'Suspicious': False}
- {'Name': '.reloc', 'Entropy': 5.2, 'Size': 9728, 'Executable': False, 'Writable': False, 'Suspicious': False}

Suspicious APIs:

- recv
- send
- WSAStartup
- CreateRemoteThread
- TerminateProcess
- WriteProcessMemory
- GetProcAddress
- WinExec
- OpenProcess

Suspicious Sections:

Imports:

- {'GDI32.dll': ['DeleteDC', 'GetDIBits', 'CreateFontIndirectA', 'SetTextColor', 'SetBkMode', 'RealizePalette', 'SelectPalette', 'GetStockObject', 'GetObjectA', 'BitBlt', 'SelectObject', 'CreateCompatibleBitmap', 'CreateCompatibleDC', 'GetDeviceCaps', 'CreateDCA', 'DeleteObject', 'CreateDIBSection']}
- {'PSAPI.DLL': ['EnumProcessModules', 'GetModuleFileNameExA']}
- {'WS2_32.dll': ['select', 'inet_addr', 'gethostbyname', 'inet_ntoa', 'recv', 'send', 'connect', 'ntohs', 'htons', 'setsockopt', 'WSACleanup', 'WSAStartup', 'closesocket', 'socket', 'WSAGetLastError']}
- {'iphlpapi.dll': ['GetAdaptersInfo']}
- {'KERNEL32.dll': ['WriteFile', 'GetStdHandle', 'GetVersionExA', 'GetLastError', 'GetCurrentProcess', 'Process32Next', 'Process32First', 'CreateToolhelp32Snapshot', 'GetDiskFreeSpaceA', 'GetDriveTypeA', 'GetLogicalDrives', 'GetModuleHandleA', 'GlobalMemoryStatus', 'GetComputerNameA', 'CopyFileA', 'MoveFileExA', 'GetModuleFileNameA', 'SetCurrentDirectoryA', 'GetCurrentDirectoryA', 'GetCurrentThreadId', 'OutputDebugStringA', 'GetSystemDefaultLangID', 'WaitForSingleObject', 'CreateRemoteThread', 'GetVersion', 'GlobalFree', 'GlobalReAlloc', 'GlobalUnlock', 'GlobalLock', 'GlobalAlloc', 'GlobalSize', 'WideCharToMultiByte', 'Module32Next', 'Module32First', 'TerminateProcess', 'SetPriorityClass', 'SuspendThread', 'DeleteFileA', 'Thread32First', 'ResumeThread', 'LoadLibraryW', 'ProcessIdToSessionId', 'LeaveCriticalSection', 'EnterCriticalSection', 'InitializeCriticalSection', 'GetVolumeInformationA', 'FindClose', 'FindNextFileA', 'FindFirstFileA', 'SystemTimeToFileTime', 'GetLocalTime', 'CreateDirectoryA', 'SetFileAttributesA', 'GetFileAttributesA', 'RemoveDirectoryA', 'MoveFileA', 'GetFileTime', 'CreateFileA', 'SetFileTime', 'TerminateThread', 'LoadLibraryA', 'LocalFree', 'LocalAlloc', 'GetWindowsDirectoryA', 'GetSystemTime', 'GetSystemDirectoryA', 'CreateMutexA', 'FreeConsole', 'WriteProcessMemory', 'VirtualAllocEx', 'MultiByteToWideChar', 'SetLastError', 'ReadFile', 'CreateProcessA', 'GetStartupInfoA', 'CreatePipe', 'VirtualQuery', 'GetProcAddress', 'GetTickCount', 'CreateThread', 'CloseHandle', 'FreeLibrary', 'ExitThread', 'WinExec', 'Sleep', 'GetCurrentProcessId', 'Thread32Next', 'OpenProcess', 'GetExitCodeThread']}
- {'USER32.dll': ['BlockInput', 'ExitWindowsEx', 'CloseWindowStation', 'CloseDesktop', 'MessageBoxA', 'SetThreadDesktop', 'OpenDesktopA', 'SetProcessWindowStation', 'OpenWindowStationA', 'GetProcessWindowStation', 'GetDesktopWindow', 'GetThreadDesktop', 'SendMessageA', 'SystemParametersInfoA', 'PostMessageA', 'PostThreadMessageA', 'GetMessageA', 'RedrawWindow', 'DrawTextA', 'GetSystemMetrics', 'mouse_event', 'keybd_event', 'GetDC', 'ReleaseDC', 'OpenInputDesktop', 'GetUserObjectInformationA']}

- {'ADVAPI32.dll': ['LookupPrivilegeValueA', 'OpenProcessToken', 'RegCloseKey', 'RegQueryValueExA', 'RegOpenKeyExA', 'CreateProcessAsUserA', 'RegSetValueExA', 'RegDeleteValueA', 'RegEnumKeyA', 'RegOpenKeyA', 'SetTokenInformation', 'DuplicateTokenEx', 'RegEnumValueA', 'AdjustTokenPrivileges', 'RegCreateKeyA', 'RegDeleteKeyA', 'CloseServiceHandle', 'QueryServiceConfigA', 'RegisterServiceCtrlHandlerA', 'SetServiceStatus', 'CreateServiceA', 'ChangeServiceConfig2A', 'QueryServiceStatusEx', 'ChangeServiceConfigA', 'StartServiceA', 'QueryServiceStatus', 'ControlService', 'DeleteService', 'OpenSCManagerA', 'EnumServicesStatusExA', 'QueryServiceConfig2A', 'OpenServiceA']}
- {'ole32.dll': ['CoTaskMemFree', 'CoInitialize', 'CoInitializeEx', 'CoCreateInstance', 'CoUninitialize']}
- {'OLEAUT32.dll': ['SysFreeString', 'VariantClear']}
- {'MSVFW32.dll': ['ICCompress', 'ICClose', 'ICSendMessage', 'ICOpen', 'ICImageCompress']}
- {'WINMM.dll': ['waveInReset', 'waveInOpen', 'waveInClose', 'waveInUnprepareHeader', 'waveInPrepareHeader', 'waveInAddBuffer', 'waveInStart']}
- {'MSVCRT.dll': ['fread', '_ftol', '_except_handler3', '__CxxFrameHandler', '??2@YAPAXI@Z', '??3@YAXPAX@Z', 'isdigit', 'strtoul', 'strncat', '_strupr', 'strcmp', 'strtok', 'malloc', 'abs', 'wcstombs', '_CxxThrowException', 'fopen', 'ftell', 'wcslen', '_CIacos', '_CIpow', '_strrev', '__dllonexit', '_onexit', '??1type_info@@UAE@XZ', '_initterm', '_adjust_fdiv', 'fwrite', 'fclose', 'printf', 'memcmp', 'strncmp', 'atoi', 'strncpy', '_stricmp', '_strnicmp', '_strlwr', 'memcpy', 'strcpy', 'strlen', 'memset', 'fseek', 'free', '_vsnprintf', 'fprintf', '_strtime', '_strdate', 'strcat', 'sprintf', 'strrchr', 'strstr', 'strchr']}

Exports:

- {'Name': 'InstallRT', 'Ordinal': 1, 'Address': '0xd847', 'Forwarded': False}
- {'Name': 'InstallSA', 'Ordinal': 2, 'Address': '0xdec1', 'Forwarded': False}
- {'Name': 'InstallSB', 'Ordinal': 3, 'Address': '0xe892', 'Forwarded': False}
- {'Name': 'PSLIST', 'Ordinal': 4, 'Address': '0x7025', 'Forwarded': False}
- {'Name': 'ServiceMain', 'Ordinal': 5, 'Address': '0xcf30', 'Forwarded': False}
- {'Name': 'StartEXS', 'Ordinal': 6, 'Address': '0x7ecb', 'Forwarded': False}
- {'Name': 'UninstallRT', 'Ordinal': 7, 'Address': '0xf405', 'Forwarded': False}
- {'Name': 'UninstallSA', 'Ordinal': 8, 'Address': '0xea05', 'Forwarded': False}
- {'Name': 'UninstallSB', 'Ordinal': 9, 'Address': '0xf138', 'Forwarded': False}

Packer Indicators:

detected: True
reasons: ['Unusual file size vs image size']