

SHA256: d6942ecdc29454fdd02a15846d95ce497c01e4b2f2db3d86b21eb6ab3854d5db

File name: msmunberb.dll

Detection ratio: 1 / 41

Analysis date: 2012-09-25 11:01:55 UTC (1 minuta ago)



[More details](#)

Antivirus	Result	Update
Agnitum	-	20120924
AntiVir	-	20120925
Antiy-AVL	-	20120924
Avast	-	20120925
AVG	-	20120925
BitDefender	-	20120925
CAT-QuickHeal	-	20120925
ClamAV	-	20120924
Commtouch	-	20120925
Comodo	-	20120925
DrWeb	-	20120925
Emsisoft	-	20120919
eSafe	-	20120924
ESET-NOD32	-	20120925
F-Prot	-	20120925
F-Secure	-	20120925
Fortinet	-	20120925
GData	-	20120925
Ikarus	-	20120925
Jiangmin	-	20120925
K7AntiVirus	-	20120924
Community Statistics Dokumentace FAQ About		Loger.gen Join our community Sign in
Kingsoft	-	20120925
McAfee	-	20120925
McAfee-GW-Edition	-	20120924
Microsoft	-	20120925
Norman	-	20120925
nProtect	-	20120925

Panda	-	20120924
PCTools	-	20120925
Rising	-	20120925
Sophos	-	20120925
SUPERAntiSpyware	-	20120911
Symantec	-	20120925
TheHacker	-	20120925
TotalDefense	-	20120925
TrendMicro	-	20120925
TrendMicro-HouseCall	-	20120925
VBA32	-	20120925
VIPRE	-	20120925
ViRobot	-	20120925

- Comments
- Votes
- Additional information

ssdeep
3072:cLlZLMRHBdw2mAhYoQootVsNBKo9oaE/:cRzLudVhYboztVJaE

TrID
Win32 Executable MS Visual C++ (generic) (65.2%)
Win32 Executable Generic (14.7%)
Win32 Dynamic Link Library (generic) (13.1%)
Generic Win/DOS Executable (3.4%)
DOS Executable Generic (3.4%)

PEiD packer identifier
Armadillo v1.xx - v2.xx

ExifTool

MIMEType.....: application/octet-stream
Subsystem.....: Windows GUI
MachineType.....: Intel 386 or later, and compatibles
TimeStamp.....: 2012:05:16 15:50:39-07:00
FileType.....: Win32 DLL
PEType.....: PE32
CodeSize.....: 122880
LinkerVersion.....: 6.0
EntryPoint.....: 0x14bda
InitializedDataSize.....: 49152
SubsystemVersion.....: 4.0
ImageVersion.....: 0.0
OSVersion.....: 4.0
UninitializedDataSize.....: 0

Portable Executable structural information

Compilation timedatestamp.....: 2012-05-16 22:50:39
Target machine.....: 0x14C (Intel 386 or later processors and compatible processors)
Entry point address.....: 0x00014BDA

PE Sections.....:

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	120954	122880	6.63	4513522fd0d0d7fac04d1585be5ec323
.rdata	126976	8812	12288	3.59	fe5f4fa6f10de689f8b0c85a71336a26
.data	139264	19308	16384	1.43	e0b6fd1ec366c5196cb7c8112cf461d3
.SYNCH	159744	3157	4096	0.00	620f0b67a91f7f74151bc5be745b7110
.reloc	163840	11208	12288	5.81	8aeaab30b3ef3d8cc6203b6b45f9fc1d

PE Imports.....:

```

[[ADVAPI32.dll]]
RevertToSelf, ImpersonateLoggedOnUser

[[KERNEL32.dll]]
GetStdHandle, WaitForSingleObject, HeapDestroy, GetLocalTime, FreeEnvironmentStringsA, DeleteCriticalSection, GetCurrentProcess,
FreeEnvironmentStringsW, SetStdHandle, GetFileTime, GetCPInfo, GetStringTypeA, WriteFile, HeapReAlloc, GetStringTypeW, GetOEMCP
, MoveFileA, GetThreadPriority, InitializeCriticalSection, FindClose, TlsGetValue, SetLastError, GetSystemTime, GetEnvironmentVa
riableA, HeapAlloc, FlushFileBuffers, GetModuleFileNameA, SetThreadPriority, InterlockedDecrement, MultiByteToWideChar, FlushIns
tructionCache, GetModuleHandleA, CreateThread, SetUnhandledExceptionFilter, SetEnvironmentVariableA, TerminateProcess, SetEndOff
ile, GetVersion, LeaveCriticalSection, HeapFree, EnterCriticalSection, SetHandleCount, GetExitCodeProcess, IsBadWritePtr, TlsAll

oc, VirtualProtect, GetVersionExA, LoadLibraryA, RtlUnwind, FreeLibrary, GetStartupInfoA, OpenProcess, SetEvent, WaitForMultiple
Objects, GetProcessHeap, GetComputerNameW, CompareStringW, lstrcmpA, FindFirstFileA, HeapValidate, CompareStringA, FindNextFileA
, GetProcAddress, GetTimeZoneInformation, CreateEventA, GetFileType, TlsSetValue, CreateFileA, ExitProcess, InterlockedIncrement
, GetLastError, LCMapStringW, lstrlenA, LCMapStringA, GetEnvironmentStringsW, lstrlenW, GetEnvironmentStrings, GetCurrentProcess
Id, WideCharToMultiByte, GetCommandLineA, GetCurrentThread, TlsFree, SetFilePointer, ReadFile, CloseHandle, GetACP, GetCurrentTh
readId, HeapCreate, VirtualFree, Sleep, IsBadReadPtr, IsBadCodePtr, VirtualAlloc

[[MPR.dll]]
WNetAddConnection2A, WNetCancelConnection2A

[[USER32.dll]]
GetWindowThreadProcessId, GetMessageA, GetForegroundWindow, GetKeyboardState, GetKeyboardLayout, GetActiveWindow, FindWindowA, M
apVirtualKeyExA, GetWindow

[[OLEAUT32.dll]]
Ord(411), Ord(23), Ord(6), Ord(4), Ord(24)

PE Exports.....:

, , , , , , , , , , , , , , ,

```

First seen by VirusTotal
2012-09-25 11:01:55 UTC (1 minuta ago)

Last seen by VirusTotal
2012-09-25 11:01:55 UTC (1 minuta ago)

File names (max. 25)
1. msmunberb.dll

[Blog](#) | [Twitter](#) | contact@virustotal.com | [Google groups](#) | [ToS](#) | [Privacy policy](#)