

[Srpski](#) | [Македонски](#) | [العربية](#) | [Suomi](#) | [ihMdl](#) | [한국어](#) | [עברית](#) | [日本語](#) | [Slovenščina](#) | [Dansk](#) | [Русский](#) | [Română](#) | [Türkçe](#)
| [Nederlands](#) | [Ελληνικά](#) | [Français](#) | [Svenska](#) | [Português](#) | [Italiano](#) | [繁體中文](#) | [简体中文](#) | [Magyar](#) | [Deutsch](#) | [Polski](#) |
[Español](#) | [English](#)



Virustotal je služba, **která analyzuje podezřelé soubory** na přítomnost virů, červů, trojanů a dalšího malware, pomocí detekčního jádra mnoha antivirů. [Více informací...](#)

[Analýza](#)[Hledání součtů](#)[Statistiky](#)[Email/Uploader](#)[O VT](#)

Soubor **services.exe** přijatý **2010.03.25 07:28:05 (UTC)**

Současný stav: **Dokončeno**

Výsledek: **1/42 (2.39%)**

[Formátované](#)[Vytisknout výsledky](#)

Antivirus	Verze	Poslední aktualizace	Výsledek
a-squared	4.5.0.50	2010.03.25	-
AhnLab-V3	5.0.0.2	2010.03.25	-
AntiVir	8.2.1.196	2010.03.24	-
Antiy-AVL	2.0.3.7	2010.03.24	-
Authentium	5.2.0.5	2010.03.25	-
Avast	4.8.1351.0	2010.03.24	-
Avast5	5.0.332.0	2010.03.24	-
AVG	9.0.0.787	2010.03.25	-
BitDefender	7.2	2010.03.25	-

CAT-QuickHeal	10.00	2010.03.25	-
ClamAV	0.96.0.0-git	2010.03.25	-
Comodo	4377	2010.03.25	-
DrWeb	5.0.1.12222	2010.03.25	-
eSafe	7.0.17.0	2010.03.24	-
eTrust-Vet	35.2.7387	2010.03.25	-
F-Prot	4.5.1.85	2010.03.24	-
F-Secure	9.0.15370.0	2010.03.25	-
Fortinet	4.0.14.0	2010.03.24	-
GData	19	2010.03.25	-
Ikarus	T3.1.1.80.0	2010.03.25	-
Jiangmin	13.0.900	2010.03.25	-
K7AntiVirus	7.10.1004	2010.03.22	-
Kaspersky	7.0.0.125	2010.03.25	-
McAfee	5930	2010.03.24	-
McAfee+Artemis	5930	2010.03.24	-
McAfee-GW-Edition	6.8.5	2010.03.25	Heuristic.LooksLike.Win32.Suspicious.H
Microsoft	1.5605	2010.03.25	-
NOD32	4972	2010.03.24	-
Norman	6.04.10	2010.03.24	-
nProtect	2009.1.8.0	2010.03.24	-
Panda	10.0.2.2	2010.03.24	-
PCTools	7.0.3.5	2010.03.25	-
Prevx	3.0	2010.03.25	-
Rising	22.40.03.03	2010.03.25	-
Sophos	4.52.0	2010.03.25	-
Sunbelt	6075	2010.03.25	-

Symantec	20091.2.0.41	2010.03.25	-
TheHacker	6.5.2.0.242	2010.03.24	-
TrendMicro	9.120.0.1004	2010.03.25	-
VBA32	3.12.12.2	2010.03.24	-
ViRobot	2010.3.25.2243	2010.03.25	-
VirusBuster	5.0.27.0	2010.03.24	-

Rozšiřující informace

File size: 111104 bytes

MD5...: 9ef697af07bb8dd82c3b02ca953a95b7

SHA1...: 7f9ec136746a6d49ca34d6e6909222076b074cc0

SHA256: f26033e660b8ff1bdb9e88cda205ce128c03138af6bec05db3cf2d95c16d86c6

ssdeep: 1536:Hyj12id0hKy+k1DQ+7Gpj3r4M7TGfwG1K9IJvydlnk4pCxvZbD:HyG1DQgG
pj3Cf1K9IBydlk+cvFD

PEid...: -

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0xbf63

timedatestamp.....: 0x498c1ac8 (Fri Feb 06 11:11:04 2009)

machinetype.....: 0x14c (I386)

(3 sections)

name viradd virsiz rawdsiz ntrpy md5

.text 0x1000 0x196a5 0x19800 6.23 bf32e1a6f4363e9fffea31d970bdebf2

.data 0x1b000 0xa38 0xc00 1.78 817a9a6979796d656eb64e994df5db0a

.rsrc 0x1c000 0x810 0xa00 4.03 9c077f09c85c35a0f56507998053e0a0

(10 imports)

> ADVAPI32.dll: AllocateLocallyUniqueId, RegOpenKeyW,
ConvertSidToStringSidW, AllocateAndInitializeSid, FreeSid, LogonUserExW,
LsaStorePrivateData, LsaLookupNames, AddAccessAllowedAce,
SetTokenInformation, StartServiceCtrlDispatcherW,
RegisterServiceCtrlHandlerW, SetServiceStatus, SystemFunction029,
SystemFunction005, CheckTokenMembership, LsaQueryInformationPolicy,

```
OpenThreadToken, RegNotifyChangeKeyValue, InitializeSecurityDescriptor,
SetSecurityDescriptorOwner, GetSecurityDescriptorDacl, GetLengthSid,
CopySid, InitializeAcl, AddAce, SetSecurityDescriptorDacl, LsaOpenPolicy,
LsaLookupSids, LsaFreeMemory, LsaClose, GetTokenInformation, RegCloseKey,
RegQueryValueExW, RegOpenKeyExW, InitiateSystemShutdownW, RevertToSelf,
CreateProcessAsUserW, ImpersonateLoggedOnUser
> KERNEL32.dll: GetCurrentThread, CreateMutexW, ReleaseMutex, ExitThread,
FormatMessageW, lstrcmpiW, SetProcessShutdownParameters,
DelayLoadFailureHook, RaiseException, GetExitCodeThread,
SetConsoleCtrlHandler, SetErrorMode, SetUnhandledExceptionFilter,
LoadLibraryA, QueryPerformanceCounter, GetCurrentThreadId,
GetCurrentProcess, UnhandledExceptionFilter, GetModuleHandleA,
OpenEventW, LocalAlloc, LocalFree, Sleep, LeaveCriticalSection,
EnterCriticalSection, SetLastError, CloseHandle, CreateThread,
GetLastError, CreateProcessW, ExpandEnvironmentStringsW,
InitializeCriticalSection, HeapAlloc, HeapFree, TerminateProcess,
WaitForSingleObject, HeapCreate, FreeLibrary, GetProcAddress,
GetModuleHandleExW, InterlockedCompareExchange, CreateNamedPipeW,
ReadFile, CancelIo, GetOverlappedResult, WaitForMultipleObjects,
ConnectNamedPipe, TransactNamedPipe, WriteFile, GetTickCount,
GetSystemTimeAsFileTime, GetModuleHandleW, GetComputerNameW,
CreateEventW, SetEvent, ResetEvent, DeviceIoControl, CreateFileW,
ResumeThread, GetCurrentProcessId, LoadLibraryW, GetDriveTypeW
> msvcrt.dll: _itow, wcsrchr, time, _except_handler3, memmove, wcschr,
_c_exit, _exit, wcsncmp, _XcptFilter, _cexit, exit, _wcsnicmp,
__getmainargs, _initterm, __setusermatherr, _adjust_fdiv, __p__commode,
__p__fmode, __set_app_type, _controlfp, _wtol, wcscpy, wscat, wcsncpy,
_wcsicmp, __initenv, wcslen, wcscspn, _ultow
> NCOBJAPI.DLL: WmiCreateObjectWithFormat, WmiEventSourceConnect,
WmiSetAndCommitObject
> ntdll.dll: RtlCreateSecurityDescriptor, RtlAddAccessAllowedAce,
RtlCreateAcl, NtCreateKey, NtQueryValueKey, NtSetValueKey,
NtDeleteValueKey, NtEnumerateKey, NtQuerySecurityObject, RtlFreeHeap,
NtOpenKey, NtDeleteKey, RtlSetControlSecurityDescriptor,
RtlValidSecurityDescriptor, RtlLengthSecurityDescriptor,
NtPrivilegeObjectAuditAlarm, NtPrivilegeCheck, NtOpenThreadToken,
NtAccessCheckAndAuditAlarm, NtSetInformationThread,
NtAdjustPrivilegesToken, NtDuplicateToken, NtOpenProcessToken,
RtlSetDaclSecurityDescriptor, RtlQuerySecurityObject,
RtlSetSecurityObject, RtlValidRelativeSecurityDescriptor,
RtlMapGenericMask, RtlCopyUnicodeString, NtSetInformationFile,
NtQueryInformationFile, RtlAppendUnicodeStringToString,
```

```
RtlAppendUnicodeToString, NtWaitForSingleObject, NtQueryDirectoryFile,
NtDeleteFile, NtSetInformationProcess, RtlUnhandledExceptionFilter,
NtSetEvent, RtlGetAce, RtlQueryInformationAcl,
RtlGetDaclSecurityDescriptor, RtlAllocateHeap,
RtlConvertSharedToExclusive, RtlConvertExclusiveToShared,
RtlRegisterWait, RtlGetNtProductType, RtlEqualUnicodeString,
RtlLengthSid, RtlCopySid, NtOpenDirectoryObject, NtQueryDirectoryObject,
RtlUnicodeStringToAnsiString, RtlInitAnsiString,
RtlAnsiStringToUnicodeString, RtlNewSecurityObject, RtlAddAce,
RtlSetOwnerSecurityDescriptor, RtlSetGroupSecurityDescriptor,
RtlSetSaclSecurityDescriptor, RtlSubAuthorityCountSid,
RtlCompareUnicodeString, NtLoadDriver, NtUnloadDriver,
RtlExpandEnvironmentStrings_U, RtlAdjustPrivilege, NtFlushKey,
NtOpenFile, RtlDosPathNameToNtPathName_U, NtOpenSymbolicLinkObject,
NtQuerySymbolicLinkObject, RtlFreeUnicodeString,
RtlAreAllAccessesGranted, NtDeleteObjectAuditAlarm,
NtCloseObjectAuditAlarm, RtlQueueWorkItem, RtlCopyLuid,
RtlDeregisterWait, RtlReleaseResource, RtlAcquireResourceExclusive,
RtlAcquireResourceShared, RtlInitializeResource, RtlDeleteSecurityObject,
RtlLockBootStatusData, RtlGetSetBootStatusData, RtlUnlockBootStatusData,
NtInitializeRegistry, NtQueryKey, NtClose, RtlInitUnicodeString,
NtSetSystemEnvironmentValue, RtlNtStatusToDosError, NtShutdownSystem,
NtQueryInformationToken, RtlMakeSelfRelativeSD, RtlInitializeSid,
RtlLengthRequiredSid, RtlSubAuthoritySid, NtSetSecurityObject
> RPCRT4.dll: RpcServerRegisterAuthInfoW, RpcBindingFree,
RpcEpResolveBinding, RpcBindingFromStringBindingW,
RpcStringBindingComposeW, NdrClientCall2, RpcAsyncCompleteCall,
RpcAsyncInitializeHandle, NdrAsyncServerCall, RpcServerListen,
RpcMgmtStopServerListening, RpcMgmtWaitServerListen,
RpcServerUnregisterIf, NdrAsyncClientCall, NdrServerCall2,
I_RpcBindingIsClientLocal, RpcRevertToSelf, I_RpcMapWin32Status,
RpcImpersonateClient, RpcStringBindingParseW, RpcStringFreeW,
RpcBindingToStringBindingW, RpcServerRegisterIfEx,
RpcServerUseProtseqEpW, RpcServerRegisterIf
> SCESRV.dll: ScesrvInitializeServer, ScesrvTerminateServer
> umpnpmgr.dll: RegisterScmCallback, PNP_SetActiveService,
PNP_GetDeviceRegProp, PNP_GetDeviceListSize, PNP_GetDeviceList,
PNP_HwProfFlags, RegisterServiceNotification,
DeleteServicePlugPlayRegKeys
> USER32.dll: LoadStringW, wsprintfW, BroadcastSystemMessageW,
MessageBoxW, RegisterServicesProcess
> USERENV.dll: UnloadUserProfile, CreateEnvironmentBlock,
```

```
LoadUserProfileW, DestroyEnvironmentBlock
```

```
( 0 exports )
```

```
RDS...: NSRL Reference Data Set
```

```
-
```

```
pdfid.: -
```

```
trid...: Win32 Executable Generic (42.3%)
```

```
Win32 Dynamic Link Library (generic) (37.6%)
```

```
Generic Win/DOS Executable (9.9%)
```

```
DOS Executable Generic (9.9%)
```

```
Autodesk FLIC Image File (extensions: flc, fli, cel) (0.0%)
```

```
sigcheck:
```

```
publisher....: Microsoft Corporation
```

```
copyright....: (c) Microsoft Corporation. V_echna pr_va vyhrazena.
```

```
product.....: Opera_n_ syst_m Microsoft_ Windows_
```

```
description...: Services and Controller app
```

```
original name: services.exe
```

```
internal name: services.exe
```


```
file version.: 5.1.2600.5755 (xpsp_sp3_gdr.090206-1234)
```

```
comments.....: n/a
```

```
signers.....: -
```

```
signing date.: -
```

```
verified.....: Unsigned
```

 **VAROVÁNÍ:** VirusTotal je služba poskytovaná zdarma společností Hispasec Sistemas. Kvalita výsledků není nijak zaručena. Výsledky jsou závislé na tvůrci daného produktu. Výsledky testů nemusí být 100% správné. **Tyto výsledky nemusí znamenat**, že daný soubor je infikován, nebo čistý!

Další soubor