

# Shamoon or DistTrack.A samples

Archived: 2026-04-02 12:28:23 UTC



[Download all the files listed below](#) (New Link)

**d214c717a357fe3a455610b197c390aa**

**trksvr.exe**

12288:Xfz3ZXNPcwmGWdCCg98gJWGG2EbzXHlk3qBUb7UbXfzZdE5Ng98gJWb2Ebz3q

- <http://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Mdrop-ELD/detailed-analysis.aspx>

## PE info

UninitializedDataSize : 0  
InitializedDataSize : 913408  
ImageVersion : 0.0  
ProductName : Microsoft Windows Operating System  
FileVersionNumber : 5.2.3790.0  
LanguageCode : English (U.S.)  
FileFlagsMask : 0x003f  
FileDescription : Distributed Link Tracking Server  
CharacterSet : Unicode  
LinkerVersion : 10.0  
FileOS : Windows NT 32-bit  
MIMEType : application/octet-stream  
Subsystem : Windows command line  
FileVersion : 5.2.3790.0 (srv03\_rtm.030324-2048)  
TimeStamp : 2012:08:10 00:46:22+02:00  
FileType : Win32 EXE  
PEType : PE32  
InternalName : Distributed Link Tracking Server  
ProductVersion : 5.2.3790.0  
SubsystemVersion : 5.1  
OSVersion : 5.1  
OriginalFilename : trksvr  
LegalCopyright : Microsoft Corporation. All rights reserved.  
MachineType : Intel 386 or later, and compatibles

CompanyName : Microsoft Corporation  
CodeSize : 84480  
FileSubtype : 0  
ProductVersionNumber : 5.2.3790.0  
EntryPoint : 0x892b  
ObjectFileType : Executable application

PE Signature

=====

Publisher : Microsoft Corporation  
Product : Microsoft\_ Windows\_ Operating System  
Internal name : Distributed Link Tracking Server  
Copyright : (c) Microsoft Corporation. All rights reserved.  
Original name : trksvr  
File version : 5.2.3790.0 (srv03\_rtm.030324-2048)  
Description : Distributed Link Tracking Server

<https://www.securelist.com/en/blog?SSL=1#>

ASCI strings

File: D214C717A357FE3A455610B197C390AA  
MD5: d214c717a357fe3a455610b197c390aa  
Size: 989184

Wow64DisableWow64FsRedirection

Wow64RevertWow64FsRedirection

string too long

invalid string position

Schedule

JobAdd

vector<T> too long

ios\_base::eofbit set

ios\_base::failbit set

ios\_base::badbit set

bad locale name

bad cast

c:\windows\temp\out17626867.txt

kijjjnsnjbnnbknbkjadc

kjsdjbhjsdbhfcbsjkhdf jhg jkhg hjk hjk

slkdfjkhsbdfjbsdf

kljsdfjhsdkufskjdfh

generic

iostream  
system  
iostream stream error  
Unknown exception  
bad allocation  
CorExitProcess  
!"#\$%&'()\*+,-./0123456789;:<=>?@abcdefghijklmnopqrstuvwxyz[\]^\_`abcdefghijklmnopqrstuvwxyz{|}~  
!"#\$%&'()\*+,-./0123456789;:<=>?  
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~  
LC\_TIME  
LC\_NUMERIC  
LC\_MONETARY  
LC\_CTYPE  
LC\_COLLATE  
LC\_ALL  
!"#\$%&'()\*+,-./0123456789;:<=>?  
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_`abcdefghijklmnopqrstuvwxyz{|}~  
Visual C++ CRT: Not enough memory to complete call to strerror.  
bad exception  
FlsFree  
FlsSetValue  
FlsGetValue  
FlsAlloc  
HH:mm:ss  
dddd, MMMM dd, yyyy  
MM/dd/yy  
December  
November  
October  
September  
August  
July  
June  
April  
March  
February  
January  
Saturday  
Friday  
Thursday  
Wednesday  
Tuesday

Monday

Sunday

united-states

united-kingdom

trinidad & tobago

south-korea

south-africa

south korea

south africa

slovak

puerto-rico

pr-china

pr china

new-zealand

hong-kong

holland

great britain

england

czech

china

britain

america

swiss

swedish-finland

spanish-venezuela

spanish-uruguay

spanish-puerto rico

spanish-peru

spanish-paraguay

spanish-panama

spanish-nicaragua

spanish-modern

spanish-mexican

spanish-honduras

spanish-guatemala

spanish-el salvador

spanish-ecuador

spanish-dominican republic

spanish-costa rica

spanish-colombia

spanish-chile

spanish-bolivia

spanish-argentina  
portuguese-brazilian  
norwegian-nynorsk  
norwegian-bokmal  
norwegian  
italian-swiss  
irish-english  
german-swiss  
german-luxembourg  
german-lichtenstein  
german-austrian  
french-swiss  
french-luxembourg  
french-canadian  
french-belgian  
english-usa  
english-us  
english-uk  
english-trinidad y tobago  
english-south africa  
english-nz  
english-jamaica  
english-ire  
english-caribbean  
english-can  
english-belize  
english-aus  
english-american  
dutch-belgian  
chinese-traditional  
chinese-singapore  
chinese-simplified  
chinese-hongkong  
chinese  
canadian  
belgian  
australian  
american-english  
american english  
american  
Norwegian-Nynorsk  
Illegal byte sequence

Directory not empty  
Function not implemented  
No locks available  
Filename too long  
Resource deadlock avoided  
Result too large  
Domain error  
Broken pipe  
Too many links  
Read-only file system  
Invalid seek  
No space left on device  
File too large  
Inappropriate I/O control operation  
Too many open files  
Too many open files in system  
Invalid argument  
Is a directory  
Not a directory  
No such device  
Improper link  
File exists  
Resource device  
Unknown error  
Bad address  
Permission denied  
Not enough space  
Resource temporarily unavailable  
No child processes  
Bad file descriptor  
Exec format error  
Arg list too long  
No such device or address  
Input/output error  
Interrupted function call  
No such process  
No such file or directory  
Operation not permitted  
No error  
UTF-8  
UTF-16LE  
UNICODE

Complete Object Locator'  
Class Hierarchy Descriptor'  
Base Class Array'  
Base Class Descriptor at (  
Type Descriptor'  
'local static thread guard'  
'managed vector copy constructor iterator'  
'vector vbase copy constructor iterator'  
'vector copy constructor iterator'  
'dynamic atexit destructor for '  
'dynamic initializer for '  
'eh vector vbase copy constructor iterator'  
'eh vector copy constructor iterator'  
'managed vector destructor iterator'  
'managed vector constructor iterator'  
'placement delete[] closure'  
'placement delete closure'  
'omni callsig'  
delete[]  
new[]  
'local vftable constructor closure'  
'local vftable'  
'RTTI  
'udt re  
turning'  
'copy constructor closure'  
'eh vector vbase constructor iterator'  
'eh vector destructor iterator'  
'eh vector constructor iterator'  
'virtual displacement map'  
'vector vbase constructor iterator'  
'vector destructor iterator'  
'vector constructor iterator'  
'scalar deleting destructor'  
'default constructor closure'  
'vector deleting destructor'  
'vbase destructor'  
'string'  
'local static guard'  
'typeof'  
'vcall'  
'vtable'

`vftable'  
operator  
delete  
new  
\_\_unaligned  
\_\_restrict  
\_\_ptr64  
\_\_eabi  
\_\_clrcall  
\_\_fastcall  
\_\_thiscall  
\_\_stdcall  
\_\_pascal  
\_\_cdecl  
\_\_based(  
GetProcessWindowStation  
GetUserObjectInformationW  
GetLastActivePopup  
GetActiveWindow  
MessageBoxW  
NetScheduleJobDel  
NetApiBufferFree  
NetApiBufferAllocate  
NetRemoteTOD  
NETAPI32.dll  
WS2\_32.dll  
GetTickCount  
CloseHandle  
Process32NextW  
Process32FirstW  
CreateToolhelp32Snapshot  
OpenProcess  
GetCurrentProcess  
VirtualFree  
VirtualAlloc  
LocalFree  
Sleep  
LocalAlloc  
GetLastError  
MoveFileExW  
DeleteFileW  
GetProcAddress

GetModuleHandleW  
WriteFile  
CreateFileW  
SizeofResource  
LockResource  
LoadResource  
FindResourceW  
GetCommandLineW  
GetFileTime  
GetWindowsDirectoryW  
SetFileTime  
CreateThread  
CreateProcessW  
CopyFileW  
MoveFileW  
ReadFile  
GetSystemTime  
LeaveCriticalSection  
EnterCriticalSection  
DeleteCriticalSection  
WaitForSingleObject  
InitializeCriticalSection  
KERNEL32.dll  
LoadImageW  
USER32.dll  
StartServiceW  
RegCloseKey  
RegDeleteValueW  
RegOpenKeyExW  
Chan  
geServiceConfig2W  
CreateServiceW  
CloseServiceHandle  
ChangeServiceConfigW  
QueryServiceConfigW  
OpenServiceW  
OpenSCManagerW  
RegQueryValueExW  
StartServiceCtrlDispatcherW  
SetServiceStatus  
RegisterServiceCtrlHandlerW  
ADVAPI32.dll

CommandLineToArgvW  
SHELL32.dll  
InterlockedIncrement  
InterlockedDecrement  
EncodePointer  
DecodePointer  
RaiseException  
RtlUnwind  
HeapFree  
ExitProcess  
HeapSetInformation  
WideCharToMultiByte  
LCMapStringW  
MultiByteToWideChar  
GetCPInfo  
HeapAlloc  
IsProcessorFeaturePresent  
TerminateProcess  
UnhandledExceptionFilter  
SetUnhandledExceptionFilter  
IsDebuggerPresent  
TlsAlloc  
TlsGetValue  
TlsSetValue  
TlsFree  
SetLastError  
GetCurrentThreadId  
HeapCreate  
SetHandleCount  
GetStdHandle  
InitializeCriticalSectionAndSpinCount  
GetFileType  
GetStartupInfoW  
GetConsoleCP  
GetConsoleMode  
FlushFileBuffers  
SetFilePointer  
LoadLibraryW  
GetLocaleInfoW  
GetModuleFileNameW  
FreeEnvironmentStringsW  
GetEnvironmentStringsW

QueryPerformanceCounter  
GetCurrentProcessId  
GetSystemTimeAsFileTime  
GetACP  
GetOEMCP  
IsValidCodePage  
GetStringTypeW  
HeapReAlloc  
HeapSize  
GetUserDefaultLCID  
GetLocaleInfoA  
EnumSystemLocalesA  
IsValidLocale  
WriteConsoleW  
SetStdHandle  
CreateFileA  
SetEndOfFile  
GetProcessHeap  
.?AVbad\_alloc@std@@  
.?AVexception@std@@  
.?AVruntime\_error@std@@  
.?AVfacet@locale@std@@  
.?AVcodecvt\_base@std@@  
.?AUctype\_base@std@@  
.?AVios\_base@std@@  
.?AV?\$\_Iosb@H@std@@  
.?AV?\$basic\_ostream@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$basic\_ios@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$basic\_istream@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$basic\_iostream@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$ctype@D@std@@  
.?AVsystem\_error@std@@  
.?AVfailure@ios\_base@std@@  
.?AV?\$basic\_streambuf@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$codecvt@DDH@std@@  
.?AVbad\_cast@std@@  
.?AV?\$basic\_filebuf@DU?\$char\_traits@D@std@@@std@@  
.?AV?\$basic\_fstream@DU?\$char\_traits@D@std@@@std@@  
.?AVlogic\_error@std@@  
.?AVlength\_error@std@@  
.?AVout\_of\_range@std@@  
.?AV\_Locimp@locale@std@@

?.?AVerror\_category@std@@

?.?AV\_Generic\_error\_category@std@@

?.?AV\_Iostream\_error\_category@std@@

?.?AV\_System\_error\_category@std@@

Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.

?.?AVtype\_info@@

?.?AVbad\_exception@std@@

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNPOQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNPOQRSTUVWXYZ

KG=]

>]H:

uD^5

\_D`j

^+'o

^#WkW+K

\_aFNZ-

kS3~

K^#s

K^aCN

^#WkW+K

\_aFNZ-

Unicode Strings:

-----  
jjjjj

@LanmanWorkstation

WOW64

SYSTEM\CurrentControlSet\Services\TrkSvr

Distributed Link Tracking Server

Enables the Distributed Link Tracking Client service within the same domain to provide more reliable and efficient maintenance of links within the domain. If this service is disabled, any services that explicitly depend on it will fail to start.

RpcSs

C:\Windows\system32\svchost.exe -k netsvcs

TrkSvr

.exe

kernel32.dll

amd64

AMD64

PROCESSOR\_ARCHITECTURE

SYSTEM\CurrentControlSet\Control\Session Manager\Environment

ntrksvr.exe

trksrv.exe

netinit

\system32\kernel32.dll

netapi32.dll

%SystemRoot%\System32\

\system32\

\system32\csrss.exe

E\$\WINDOWS

D\$\WINDOWS

C\$\WINDOWS

ADMIN\$

\inf\netft429.pnf

PKCS7

\System32\cmd.exe /c "ping -n 30 127.0.0.1 >nul && sc config TrkSvr binpath= system32\trksrv.exe && ping -n 10 127.0.0.1 >nul && sc start TrkSvr "

X509

myimage12767

PKCS12

wow32

mscoree.dll

((( H

h((( H

H

AKERNEL32.DLL

runtime error

TLOSS error

SING error

DOMAIN error

R6033

- Attempt to use MSIL code from this assembly during native code initialization

This indicates a bug in your application. It is most likely the result of calling an MSIL-compiled (/clr) function from a native constructor or from DllMain.

R6002

- floating point support not loaded

AMicrosoft Visual C++ Runtime Library

<program name unknown>

Runtime Error!

Program:

HH:mm:ss

dddd, MMMM dd, yyyy

MM/dd/yy

December

November

October

September

August

July

June

April

March

February

January

Saturday

Friday

Thursday

Wednesday

Tuesday

Monday

Sunday

Eccs

UTF-8

UTF-16LE

UNICODE

WUSER32.DLL

CONOUT\$

caclsr

certutil

clean

ctrl

dfrag

dnslookup

dvdquery

event

findfile

gpget

ipsecure

iissrv

msinit

ntfrsutil

ntdsutil

power

rdsadmin  
regsys  
sigver  
routeman  
rrasrv  
sacses  
sfmsc  
smbinit  
wscript  
ntnw  
netx  
fsutl  
extract  
\system32\  
test123  
test456  
test789  
testdomain.com  
123123  
456456  
789789  
PKCS12  
PKCS7  
X509  
VS\_VERSION\_INFO  
StringFileInfo  
040904b0  
CompanyName  
Microsoft Corporation  
FileDescription  
Distributed Link Tracking Server  
FileVersion  
5.2.3790.0 (srv03\_rtm.030324-2048)  
InternalName  
Distributed Link Tracking Server  
LegalCopyright  
Microsoft Corporation. All rights reserved.  
OriginalFilename  
trksvr  
ProductName  
Microsoft  
Windows

Operating System

ProductVersion

5.2.3790.0

VarFileInfo

Translation

<https://www.virustotal.com/file/f9d94c5de86aa170384f1e2e71d95ec373536899cb7985633d3ecfdb67af0f72/analysis/>

SHA256: f9d94c5de86aa170384f1e2e71d95ec373536899cb7985633d3ecfdb67af0f72

SHA1: 502920a97e01c2d022ac401601a311818f336542

MD5: d214c717a357fe3a455610b197c390aa

File size: 966.0 KB ( 989184 bytes )

File name: str.exe

File type: Win32 EXE

Tags: peexe

Detection ratio: 22 / 42

Analysis date: 2012-08-16 13:57:43 UTC ( 16 hours, 25 minutes ago )

AntiVir TR/Crypt.FKM.Gen 20120816

Avast Win32:Malware-gen 20120816

AVG unknown virus Win32/DH{A2cI} 20120815

BitDefender Gen:Trojan.Heur.8u0@ILmUdSm 20120816

Commtouch W32/Dropper.gen8!Maximus 20120816

Comodo UnclassifiedMalware 20120816

Emsisoft Trojan.Win32.Spy!IK 20120816

F-Prot W32/Dropper.gen8!Maximus 20120815

F-Secure Gen:Trojan.Heur.8u0@ILmUdSm 20120816

GData Gen:Trojan.Heur.8u0@ILmUdSm 20120816

Ikarus Trojan.Win32.Spy 20120816

Jiangmin Trojan/Generic.aninx 20120816

K7AntiVirus Trojan 20120815

Kaspersky HEUR:Trojan.Win32.Generic 20120816

McAfee W32/DistTrack 20120816

McAfee-GW-Edition W32/DistTrack 20120816

Norman W32/Troj\_Generic.DKYIW 20120816

Sophos Troj/Mdrop-ELD 20120816

Symantec W32.DistTrack 20120816

TrendMicro TROJ\_DISTTRACK.A 20120816

TrendMicro-HouseCall TROJ\_DISTTRACK.A 20120816

VIPRE Trojan.Win32.Generic!BT 20120816

<https://www.virustotal.com/file/4f02a9fcd2deb3936ede8ff009bd08662bdb1f365c0f4a78b3757a98c2f40400/analysis/>

SHA256: 4f02a9fcd2deb3936ede8ff009bd08662bdb1f365c0f4a78b3757a98c2f40400

SHA1: 7c0dc6a8f4d2d762a07a523f19b7acd2258f7ecc

MD5: b14299fd4d1cbfb4cc7486d978398214  
File size: 966.0 KB ( 989184 bytes )  
File name: str.exe  
File type: Win32 EXE  
Tags: peexe  
Detection ratio: 21 / 42  
Analysis date: 2012-08-16 13:39:56 UTC ( 16 hours, 44 minutes ago )  
AntiVir TR/Crypt.FKM.Gen 20120816  
Avast Win32:Malware-gen 20120816  
AVG unknown virus Win32/DH{A2cI} 20120815  
BitDefender Gen:Trojan.Heur.8u0@ILmUdSm 20120816  
CommTouch W32/Dropper.gen8!Maximus 20120816  
Comodo UnclassifiedMalware 20120816  
Emsisoft Trojan.Win32.Spy!IK 20120816  
F-Prot W32/Dropper.gen8!Maximus 20120815  
F-Secure Gen:Trojan.Heur.8u0@ILmUdSm 20120816  
GData Gen:Trojan.Heur.8u0@ILmUdSm 20120816  
Ikarus Trojan.Win32.Spy 20120816  
K7AntiVirus Trojan 20120815  
Kaspersky HEUR:Trojan.Win32.Generic 20120816  
McAfee W32/DistTrack 20120816  
McAfee-GW-Edition W32/DistTrack 20120816  
Norman W32/Troj\_Generic.DLKSV 20120816  
Sophos Troj/Mdrop-ELD 20120816  
SUPERAntiSpyware - 20120816  
Symantec W32.DistTrack 20120816  
TrendMicro TROJ\_DISTTRACK.A 20120816  
TrendMicro-HouseCall TROJ\_DISTTRACK.A 20120816  
VIPRE Trojan.Win32.Generic!BT 20120816  
  
VirusBuster -

---

Source: <http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html>