

Ascii Strings:

.exe
.dll
explorer.exe
%s%\%s.dll
\Windows NT
\Windows Media Player
\Internet Explorer
\Movie Maker
Software\Microsoft\Windows\CurrentVersion\Run
Windows Defender
WerSvc
ERSvc
BITS
wuauerv
WinDefend
wscsvc
-k NetworkService
-k netsvcs
svchost.exe
services.exe
rundll32.exe
Global\%u-%u
Global\%u-7
SeDebugPrivilege
p]A?
^A?`^A?o^A?
:@`RM@gRM@P]M@_JM@`
Q@FU@/FU@`QU@gQU@hQU@oQU@
D|@H
XA`)ZA
)ZA`
-#B0
EbC@HbC_HbC
C0<HD7<HD hXD'hXD
RYDH
ZD00{D70{D@O{DOO{DPO{D_O{D
~D@0
EP~,E_~,E
iEHq
vet.
sans.
nai.
msft.
msdn.
llnwd.
llnw.
kav.
gmer.
cert.
bit9.

avp.
avg.
windowsupdate
wilderssecurity
virus
virscan
trojan
trendmicro
threatexp
threat
technet
symantec
sunbelt
spyware
spamhaus
sophos
secureworks
securecomputing
safety.live
rootkit
rising
removal
quickheal
ptsecurity
prevx
pctools
panda
onecare
norton
norman
nod32
networkassociates
mtc.sri
msmvps
msftncsi
mirage
microsoft
mcafee
malware
kaspersky
k7computing
jotti
ikarus
hauri
hacksoft
hackerwatch
grisoft
gdata
freeav
free-av
fortinet
f-secure

f-prot
ewido
etrust
eset
esafe
emsisoft
dslreports
drweb
defender
cyber-ta
cpsecure
conficker
computerassociates
comodo
clamav
centralcommand
ccollomb
castleops
bothunter
avira
avgate
avast
arcabit
antivir
anti-
ahnlab
agnitum
wireshark
unlocker
tcpview
sysclean
sct_
regmon
procmon
procexp
ms08-06
mrtstub
mrt.
mbsa.
klwk
kido
kb958
kb890
hotfix
gmer
filemon
downad
confick
avenger
autoruns
c\V9
GX1[

L09n
Jknetapi32.dll
NetpwPathCanonicalize
ntdll.dll
NtQueryInformationProcess
Query_Main
DnsQuery_W
DnsQuery_UTF8
dnsapi.dll
DnsQuery_A
ws2_32.dll
sendto
dnssrvr.dll
wininet.dll
InternetGetConnectedState
kernel32.dll
S}LoadLibraryExA
NtQueueApcThread
LoadLibraryA
NtSetInformationProcess
SeTakeOwnershipPrivilege
ResetSR
srclient.dll
com.ve
com.uy
com.ua
com.tw
com.tt
com.tr
com.sv
com.py
com.pt
com.pr
com.pe
com.pa
com.ni
com.ng
com.mx
com.mt
com.lc
com.ki
com.jm
com.hn
com.gt
com.gl
com.gh
com.fj
com.do
com.co
com.bs
com.br
com.bo

com.ar
com.ai
com.ag
co.za
co.vi
co.uk
co.ug
co.nz
co.kr
co.ke
co.il
co.id
co.cr
rapidshare.com
imageshack.us
facebook.com
w3.org
ask.com
yahoo.com
google.com
baidu.com
http://www.%s
?http://%s
4d(2d
T1`m
c"5o
sMicrosoft Base Cryptographic Provider v1.0
t}9]
YY9]
uoSV
u)Sj
)9PP
SUVW3
PWWV
_^[
SVW3
Yv h
YYuBh
YYu(h
YYu+
UWj.S3
YYt]V3
jIY3
YYulSh
SV
jdY3
Q_R[3

jdRP
WVS3
i t0
PAb,

V;Az
glL(~5
0yJA
^)CW
>vb"R
y[nSp<
xiaonei.com
studiverzeichnis.com
InterlockedExchange
|alice.it
msn.com
(ebay.com
zedo.com
DVERSION
GetTempPathA
Documents
tuenti.com
metroflog.com
Collaboration
Service
Inter
conduit.com
ameba.jp
ning.com
Files
, application/x-ms-application
imdb.com
|\VarFileInfo\Translation
Debug
, application/x-shockwave-flash
Todnoklassniki.ru
Downloaded
memmove
fc2.com
LeaveCriticalSection
mediafire.com
Mail
FindClose
Build
mapquest.com
Fonts
socket
CreateDirectoryA
kernel32.dll
; .NET CLR
Internet
sourceforge.net
hgoogle.com
accept
Definitions
ucoz.ru
xhamster.com

select
InternetGetConnectedState
pcpop.com
VirtualAlloc
Help
Mozilla/4.0 (compatible; MSIE
ameblo.jp
tinypic.com
Microsoft Base Cryptographic Provider v1.0
recv
Packages
\%d.tmp
#8HTTP/1.1
,\SystemTimeToFileTime
PPerformance
WSASocketA
yd__WSAFDIsSet
livejasmin.com
tianya.cn
MSVCRT
Intel
Journal
gougou.com
LWSAGetLastError
"\KERNEL32
reference.com
wikimedia.org
htonl
dpornhub.com
adultadworld.com
yahoo.com
Cursors
ebay.co.uk
Photo
ExitThread
Movie
imeem.com
,fr-FR;q=0.5
|co.cc
GetModuleFileNameA
Hkaixin001.com
naver.com
kooora.com
 registration
biglobe.ne.jp
Options
Profiles
xlivejournal.com
RegCloseKey
soso.com
answers.com
mail.ru

Video
xvideos.com
GetProcAddress
CryptReleaseContext
*XFindNextFileA
rapidshare.com
twain
Gallery
drambler.ru
Agent
RegSetValueExA
CreateFileA
xxSoftware\Microsoft\Windows\CurrentVersion\Explorer
tudou.com
Registered
Reference
,es-ES;q=0.5
FindFirstFileA
56.com
photobucket.com
Assemblies
URLMON
4tracing
Date:
narod.ru
foxnews.com
ReadFile
adsrevenue.net
assembly
awempire.com
; Windows
sonico.com
perfspot.com
; SV1
CryptAcquireContextA
myspace.com
craigslist.org
espn.go.com
pDigital
en-GB
ntdll.dll
pconline.com.cn
4ebay.it
metacafe.com
WriteFile
<SetEvent
bigpoint.com
ask.com
Software
VerQueryValueA
thepiratebay.org
taringa.net

GlobalAlloc
3705
download.com
sakura.ne.jp
Sleep
Speech
bbc.co.uk
ximagevenue.com
partypoker.com
IPlayer
seesaa.net
live.com
files.wordpress.com
21022
Security
send
paypopup.com
; Media Center PC 5.0
allegro.pl
clicksor.com
tribalfusion.com
mixi.jp
QIInitializeCriticalSection
bebo.com
Modem
T Distribution
Calendar
listen
xnxx.com
SetFilePointer
Works
zshare.net
NT 5.1
goo.ne.jp
Pages
aweber.com
geocities.com
megaporn.com
facebook.com
ObtainUserAgentString
GET %s HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg%s%s%s%s%s, */*
Accept-Language: %s%s
%sAccept-Encoding: gzip, deflate
User-Agent: %s
Host: %s
Connection: Keep-Alive
youtube.com
ioctlsocket
NT 6.0
GetSystemTime
Dtime

pogo.com
getsockname
digg.com
ADVAPI32
RegQueryValueExA
badongo.com
orange.fr
bind
ODGetTempFileNameA
System
getpeername
4shared.com
vkontakte.ru
Microsoft
googlesyndication.com
08seznam.cz
Content-Length:
:XWININET
DGetTickCount
baidu.com
megaclick.com
SetFileAttributesA
GetWindowsDirectoryA
RegCreateKeyExA
GetModuleHandleA
yandex.ru
40607
InternetTimeToSystemTime
Tasks
30729
imageshack.us
veoh.com
recvfrom
GetLastError
skyrock.com
closesocket
Policy
NT 4.0
Visual
'7.0
nicovideo.jp
winsxs
CloseHandle
cricinfo.com
htons
CryptGenRandom
Tfastclick.com
Prefetch
Resources
rediff.com
linkedin.com
flickr.com

Maker
5.01
ebay.de
HTTP/1.0
typepad.com
linkbucks.com
Offline
multiply.com
tblogfa.com
Shell
terra.com.br
UA-CPU: x86
_memicmp
5@msdownld
4322
badoo.com
Globalization
Games
GlobalFree
wordpress.com
ntohl
aim.com
lCommon
mininova.org
Logs
netflix.com
LoadLibraryA
GetFileAttributesA
youporn.com
tagged.com
, application/xaml+xml
,fr-CA;q=0.5
dell.com
WS2_32
miniclip.com
m ?2
\4<,
TmW~
LQv5I
#:Lb
r^m)
xNIk
T0K0
szn-US
Explorer
Patch
comcast.net
sendto
icq.com
adobe.com
QHhyves.nl
CreateEventA

Reports
WSAIoctl
Google
4325
Kernel
WaitForSingleObject
04506
CreateThread
,es-US;q=0.5
gethostbyname
fotolog.net
Installer
DeleteFileA
GetFileVersionInfoSizeA
wikipedia.org
NT 5.0
connect
Publish
Java
Components
hi5.com
Mobile
RegOpenKeyExA
mywebsearch.com
GetVersionExA
disney.go.com
, application/vnd.ms-xpsdocument
ntohs
\Temp
Live
RegDeleteValueA
megaupload.com
,de-DE;q=0.5
PMedia
depositfiles.com
GetFileVersionInfoA
verizon.net
2ch.net
Office
Adobe
GetVersion
netlog.com
apple.com
adultfriendfinder.com
doubleclick.com
yahoo.co.jp
|vnexpress.net
50727
2914
torrentz.com
, application/x-ms-xbap
Program

friendster.com
go.com
livedoor.com
P0Defender
schemas
{%08X-%04X-%04X-%04X-%08X%04X}
Boot
tube8.com
inet_ntoa
nba.com
ziddu.com
XEnterCriticalSection
Setup
MoveFileA
DeleteFileA
GetTempPathA
GetSystemDirectoryA
Sleep
CloseHandle
CreateThread
LockFile
GetFileSize
CreateFileA
GetLocalTime
GetVersion
SetErrorMode
ExitProcess
GetCommandLineA
GetLastError
CreateMutexA
GetComputerNameA
GetCurrentProcessId
DisableThreadLibraryCalls
MoveFileExA
Process32First
CreateToolhelp32Snapshot
ReadFile
CreateFileW
MoveFileExW
DeleteFileW
WideCharToMultiByte
ExpandEnvironmentStringsW
GlobalAlloc
MultiByteToWideChar
TerminateThread
GetExitCodeThread
GetCurrentThreadId
GetVersionExA
WaitForSingleObject
SetLastError
Module32Next
Module32First

ExitThread
SetThreadPriority
VirtualProtect
GetThreadPriority
GetCurrentThread
VirtualFree
VirtualAlloc
GetProcAddress
LoadLibraryA
GetModuleHandleA
GetVolumeInformationA
GetTickCount
QueryPerformanceCounter
GetCurrentProcess
SetFileTime
GetFileAttributesA
GetFileTime
WriteFile
SetEndOfFile
TerminateProcess
OpenProcess
Thread32Next
SuspendThread
OpenThread
GlobalFree
CreateRemoteThread
WriteProcessMemory
VirtualAllocEx
ReadProcessMemory
SetFileAttributesA
CreateProcessA
LocalFree
VirtualQuery
GetTempFileNameA
FreeLibrary
SystemTimeToFileTime
GetSystemTime
GetSystemTimeAsFileTime
RtlUnwind
GetModuleFileNameA
Process32Next
Thread32First
RegCreateKeyExW
RegFlushKey
OpenSCManagerW
EnumServicesStatusW
QueryServiceConfigW
QueryServiceConfig2W
GetNamedSecurityInfoW
SetEntriesInAclW
SetNamedSecurityInfoW
RegEnumKeyExW

RegSetKeySecurity
GetTokenInformation
EqualSid
InitializeSecurityDescriptor
AllocateAndInitializeSid
GetLengthSid
InitializeAcl
AddAccessAllowedAce
SetSecurityDescriptorDacl
SetFileSecurityA
FreeSid
OpenProcessToken
LookupPrivilegeValueA
AdjustTokenPrivileges
OpenServiceA
ControlService
ChangeServiceConfigA
RegSetValueExW
RegOpenKeyExW
RegQueryValueExW
RegCloseKey
OpenSCManagerA
OpenServiceW
CloseServiceHandle
QueryServiceStatus
QueryServiceConfigA
CryptReleaseContext
CryptGenRandom
CryptAcquireContextA
_adjust_fdiv
_initterm
calloc
memcmp
strcat
strtok
atoi
wcscpy
wscat
_wcsdup
malloc
free
memcpy
memset
wcsstr
_snwprintf
wcsncmp
wcsncpy
_wcsnicmp
wcsncat
wcslen
_wcsicmp
_strlwr

strstr
_strnicmp
srand
rand
_snprintf
strchr
strncpy
strlen
_stricmp
strncat
CoInitializeEx
CoCreateInstance
CoUninitialize
CoInitializeSecurity
SHGetSpecialFolderPathA
SHDeleteValueA
StrStrIW
StrStrIA
SHDeleteKeyW
ObtainUserAgentString
EnumThreadWindows
GetDlgItem
PostMessageA
InternetGetConnectedState
InternetOpenA
InternetOpenUrlA
HttpQueryInfoA
InternetReadFile
InternetCloseHandle
1Dc"
,A*--O4
5q#&!
)N#R
#K O"N
}0hZ
"9I;&
?p"E
9!O"
0"&+
9(\$.
EGDA
[%#D0
NDzO
%^S1(
.text
`.data
.reloc
68WpPe
zJ(E
6`Q-
T[^
S|=E=

B&2:
Yg[C
LBK 5
42XVx
,J32
LPOh
=%b{
[9jL
@E~'%
%E}uUt
O7k[l
m)&6
nF^1
9gx1bS
m\$~&+
hk!]d4
]gQK
g\vj:veUl
JT=7
ihKD
FFSh
UWVS
9L\$ts
D\$xf
T\$L1
;\\$L
9L\$t
t\$t#t\$l
;\\$L
D\$Hf
T\$sf
D\$t#D\$h
+L\$d
D\$t+D\$\
;\\$L
D\$Hf
)D\$H)
;\\$L
D\$Hf
)D\$H)
L\$H)
t\$`)
t\$8w
;\\$L
L\$xf
D\$X1
L\$8f)
;\\$L
L\$8f
;\\$L
s`)L\$4
D\$t+D\$\

I\$8f)
;\\$L
;\\$L
D\$8f
I\$X1
;\\$L
;\\$L
T\$Df
t\$Hf
;\\$L
D\$Hf
)D\$H)
t\$(N
t\$(u
;\\$L
D\$Hf
)D\$H)
I\$SM
I\$\$u
;\\$L
;|\$Hr
+|\$H
;\\$L
D\$Hf
)D\$H)
t\$\tY
9I\$\w_
+D\$\
D\$tIt
9I\$tr
9D\$t
;\\$L
|[^_]
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
ole32.dll
OLEAUT32.dll
SHELL32.dll
SHLWAPI.dll
urlmon.dll
USER32.dll
WININET.dll
WS2_32.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
FreeSid
CoInitializeEx

SHGetSpecialFolderPathA
StrStrIW
ObtainUserAgentString
GetDlgItem
InternetOpenA

Unicode Strings:

svchost.exe -k netsvcs
netsvcs
SYSTEM\CurrentControlSet\Control\SafeBoot
Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-
41F1-9A6F-135D9C6622CC}
SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
.dll
SYSTEM\CurrentControlSet\Services\
ServiceDll
\Parameters
%S %S
\.
svchost.exe -k NetworkService
%s\%s
USERS
MACHINE
CURRENT_USER
CLASSES_ROOT
Policy
Discovery
Storage
Power
Logon
Machine
Browser
Management
Framework
Component
Trusted
Backup
Notify
Audit
Control
Hardware
Windows
Update
Universal
Task
Support
Shell
Security
Network
Monitor
Microsoft

Manager
Installer
Image
Helper
Driver
Config
Center
Boot
Time
System
Service
Server
serv
prov
mgmt
logon
auto
agent
access
wuau
Wmdm
Tapi
Remote
Ntms
Lanman
help
Event
Audio
SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
Parameters
Description
ObjectName
LocalSystem
ImagePath
ErrorControl
Start
Type
DisplayName
SYSTEM\CurrentControlSet\Services
%SystemRoot%\system32\svchost.exe -k
Software\Microsoft\Windows\CurrentVersion\Run
rundll32.exe "%s",%S
Ijjjj
jjjj
jjj
jjjj
jjj
jjj