ZeroAccess / Sirefef Rootkit - 5 fresh samples

Stocking stuffers.

ZeroAccess rootkit is far from new and exciting but but this is a fresh lot with still active C2 servers.

Although the dropper is detected by at least half of AV engines, post infection detection is another story. I tried Kaspersky TDSS Killer, Avast Rootkit utility and RootRepeal without any success. I used Gmer and LordPE to carve out the hidden file from the memory. You can use Redline or Volatility too.

You can download 5 files below together with pcaps from one of the files and the file dumped from memory. It appears that free videos and apps names are used as the lure in this case.

Download the 5 files below plus the file dumped from memory

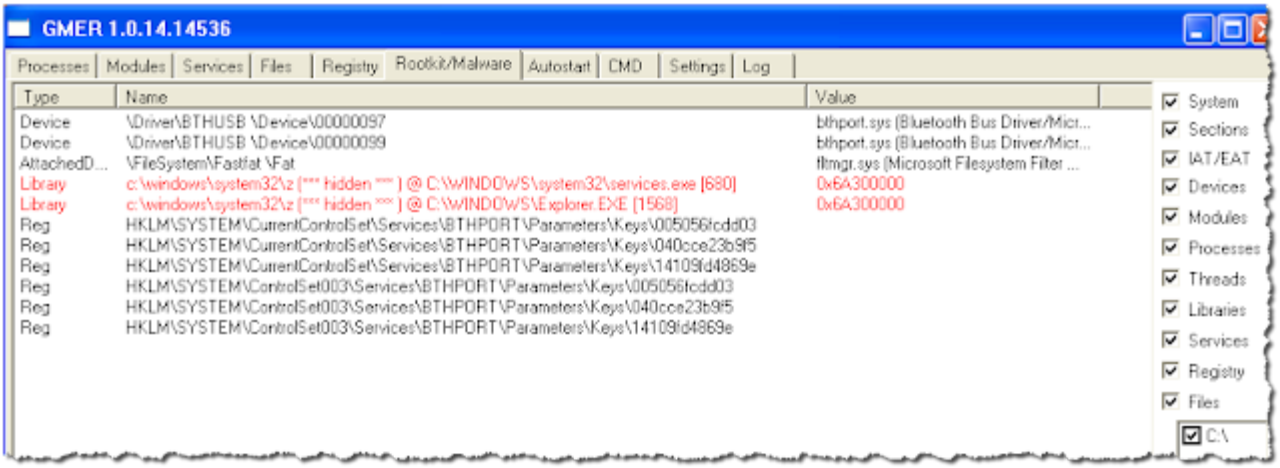
Download 2 pcap files from 2 runs of A2611095F689FADFFD3068E0D4E3E7ED

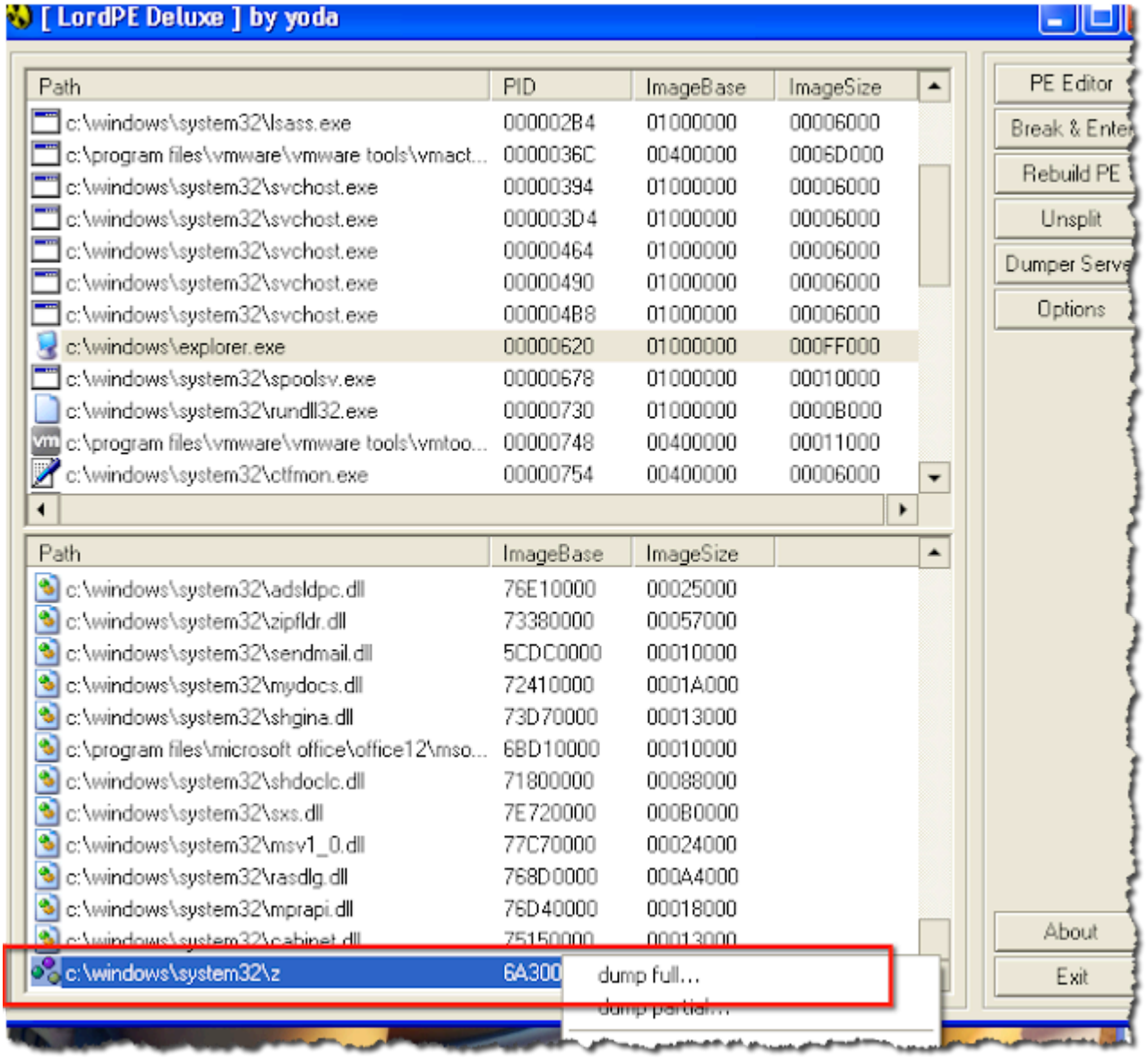
File information

- **251a2c7eff890c58a9d9eda5b1391082 160 KB 622.exe_**
- **1a12137bd701bd9ed607671ce1b7806a 160 KB animal-sex-free.avi.exe_**
- **59b247f0266b107451104243261a7ecf 159 KB FlashPlayer_11_4_update_for_Win.exe_**
- **98a993d62d367682048ec70df109e7d8 161 KB readme.exe_**
- **a2611095f689fadffd3068e0d4e3e7ed 160 KB ZeroAccess_xxx-porn-movie.avi.exe_**

A2611095F689FADFFD3068E0D4E3E7ED

hidden library - injected in Explorer.exe





Strings from the dumped z binary

File: dumped.dll

MD5: fe756584b159fd24dc4b6a572917354c

Size: 73728

Ascii Strings:

!This program cannot be run in DOS mode.
RichK6
t#cP[LordPE]
SPC3
.text
`.rdata
@.data
RtlImageNtHeader
RtlImageDirectoryEntryToData
LdrProcessRelocationBlock

---snip---

RtlExitUserThread
wcslen
swprintf
LdrGetProcedureAddress
wcsrchr
wcscpy
wcscat
ZwOpenFile
RtlInitUnicodeString
ZwReadFile
ZwClose
ZwWriteFile
ZwOpenEvent
ZwQueryVolumeInformationFile
memcpy
RtlAppendUnicodeToString
RtlConvertSidToUnicodeString
ZwOpenProcessToken
ZwQueryInformationToken
ZwCreateEvent
LdrFindEntryForAddress
ZwCreateEventPair
ZwSetHighWaitLowEventPair
ZwWaitHighEventPair
ZwSetLowEventPair
memset
RtlInterlockedPushEntrySList

RtlInterlockedPopEntrySList
RtlNtStatusToDosError
ZwCreateSection
ZwMapViewOfSection
ZwUnmapViewOfSection
RtlTimeToSecondsSince1980
qsort
ZwQueryEaFile
ZwQueryDirectoryFile
wcstoul
ZwDeleteFile
ZwCreateFile
ZwSetEaFile
ZwSetInformationFile
RtlAddressInSectionTable
RtlComputeCrc32
ntdll.dll
VirtualAlloc
LoadLibraryA
EnterCriticalSection
LeaveCriticalSection
VirtualFree
LoadLibraryW
FreeLibrary
Sleep
SleepEx
InitializeCriticalSection
DeleteCriticalSection
GetProcAddress
DisableThreadLibraryCalls
CreateThread
CreateTimerQueueTimer
DeleteTimerQueueTimer
LocalAlloc
LocalFree
BindIoCompletionCallback
GetLastError
GetSystemTimeAsFileTime
KERNEL32.dll
MD5Init
MD5Update
MD5Final

CryptAcquireContextW
CryptImportKey
CryptGenRandom
CryptDestroyKey
CryptReleaseContext
CryptCreateHash
CryptSetHashParam
CryptVerifySignatureW
CryptDestroyHash
ADVAPI32.dll
AcceptEx
MSWSOCK.dll
WSASocketW
WSAIoctl
WSARecv
WSASend
WSASendTo
WSARecvFrom
WS2_32.dll
RtlUnwind
NtQueryVirtualMemory
t#cP
p2p.32.dll
DllGetClassObject
@S0j
@p0j
@p0j
T0j@
U0j@
0*0k0
1&101B1J1[1b1p1v1
2#2(2?2H2g2y2
2H3Q3m3s3
41484`4r4x4
546;6B6]6b6n6
7&757;7U7h7q7
8+888=8H8M8X8]8j8p8
9#90969@9J9P9W9^9e9j9o9
9F:M:T:Z:b:
;%;2;
=$=2=<=s= >q?{?
3*3s3~3R4m4z4

545Y5z5
6E6J6
6O7t7
9,9C9i9
9$:/:G:i:
;%;,;M;];
;3<: data-blogger-escaped-i="i" data-blogger-escaped-j="j" data-blogger-escaped-z="z">q>
?.?>?P?^?p?
0(0:0F0W0h0
1#121R1
313R3Y3_3q3v3
4!4t4z4
5?5|5
9+9A9K9
;,;R;[;t;
<$<*<0 data-blogger-escaped-00080="00080" data-blogger-escaped-1.141="1.141" data-blogger-escaped-6="6" data-blogger-escaped-al="al" data-blogger-escaped-b="b" data-blogger-escaped-d0t0="d0t0" data-blogger-escaped-ddev="ddev" data-blogger-escaped-h="h" data-blogger-escaped-iy="iy" data-blogger-escaped-m="m" data-blogger-escaped-ur="ur">2i1FQ
q'.C
)5Rb
!Q[#\
5L@0
5e{u
-~G5
iV:RE
Scwn=
/dq_
m|XK
vT{!
g]a%Ph
Z,Jn
gf[G:C0!
>Ze\#
b'fg
(m9/
"0Gk_
@Vc}X
J+[YR~m
Ol"`o
L*s~t6L
(-w^

RdHQ
is*X
Lclu)
[TRg"
k#lhK&
2)\a
N3?2t-%
}vX}
=0^FBO
Jfjo
hNHWF
Eub!
%h:A
Zn=p
#`N$
%JQ3
CVy\
n_"/?
AYQD
_pB0
@-S
WQ<6 data-blogger-escaped-3cbi="3cbi" data-blogger-escaped-fdrtg="fdrtg" data-blogger-escaped-gj="gj" data-blogger-escaped-vb="e" data-blogger-escaped-y="y">
Kz!81
)v L
X-vy
YgB\
\Y82aM"
==.yf
2z"-{
^guA
,~qw)
7z2F
-IR4j;z1|
>!Nh
OZWG
s&h!\
rKhi/
iVrOhi
7']lM
K64}
ivYi

|fpK
Jd$< 9CX? .t'TR O6qa |-De mTB` \BL\* m`Wo mB"XpH 2C|d X\,j /"JE VW>b
gP,.-
%m|SXG
aOBY
A`3"kr9 D
dRIT
PgBeb
~pi2C
USER32.dll
CreateWindowExW
InvalidateRgn
PostMessageW
UpdateWindow
SetTimer
IsIconic
GetSystemMetrics
GetClientRect
DrawIcon
EnableWindow
PostQuitMessage
SetWindowPos
MapDialogRect
KERNEL32.dll
GetVersionExW
SetUnhandledExceptionFilter
QueryPerformanceCounter
GetSystemTimeAsFileTime
GetModuleHandleW
FreeEnvironmentStringsA
GetEnvironmentStrings
FreeEnvironmentStringsW
GetEnvironmentStringsW
GetCommandLineA
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
GetModuleFileNameA

TerminateProcess
UnhandledExceptionFilter
GetACP
GetOEMCP
GetCPInfo
IsValidCodePage
HeapReAlloc
GetTimeZoneInformation
DebugBreak
OutputDebugStringA
WriteConsoleW
OutputDebugStringW
LCMapStringA
LCMapStringW
GetStringTypeA
OLEAUT32.dll
OleLoadPicture
DispGetIDsOfNames
SafeArrayAllocDescriptor
GetErrorInfo
SetErrorInfo
VariantClear
OleLoadPictureEx
ADVAPI32
RegQueryInfoKeyA
RegSetValueExA
RegOpenKeyExA
RegCreateKeyExA
RegCloseKey
RegDeleteValueA
RegDeleteKeyA
RegEnumKeyExA
SHLWAPI.dll
PathFindExtensionA
WIS_EX
O3b3~3
3;4$6
;9=~=)?
4>5L7
=6>S?s?
9.:q:
414S4

7H7j7
6?:l;

Unicode Strings:

\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D79}
\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
%sU\%08x.@
S-1-5-18
\??\%sU
\??\%s@
\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
shell32.dll
wbem\fastprox.dll
\systemroot
RECYCLER\
$Recycle.Bin\
\$%08x%04x%04x%02x%02x%02x%02x%02x%02x%02x%02x\
c:\windows\system32\z
????????.@
%08x.@
%08x.$
%08x.~
Microsoft Base Cryptographic Provider v1.0

Traffic

| <- data-blogger-escaped--="-"> | | Total |
| Frames Bytes | | Frames Bytes | | Frames Bytes |
172.16.253.130 <-> 81.17.26.187 50 46654 31 3711 81 50365
172.16.253.130 <-> 67.81.86.2 41 38700 30 1696 71 40396
172.16.253.255 <-> 172.16.253.1 57 10592 0 0 57 10592
172.16.253.130 <-> 50.22.196.70 8 1880 10 696 18 2576
194.165.17.3 <-> 172.16.253.130 10 620 0 0 10 620
172.16.253.130 <-> 66.85.130.234 0 0 9 558 9 558
172.16.253.130 <-> 8.8.8.8 4 463 4 296 8 759
224.0.0.22 <-> 172.16.253.130 7 378 0 0 7 378
217.16.132.181 <-> 172.16.253.130 3 174 3 1830 6 2004
172.16.253.130 <-> 24.177.187.254 2 1220 2 116 4 1336
172.16.253.130 <-> 90.230.66.250 2 1220 2 116 4 1336
172.16.253.130 <-> 68.3.172.252 2 1220 2 116 4 1336
172.16.253.130 <-> 68.39.227.12 2 1220 2 116 4 1336

172.16.253.130 <-> 98.192.218.116 2 1220 2 116 4 1336
172.16.253.130 <-> 85.137.174.6 2 1220 2 116 4 1336
201.211.32.247 <-> 172.16.253.130 2 116 2 1220 4 1336
211.7.72.252 <-> 172.16.253.130 1 58 3 1830 4 1888
172.16.253.130 <-> 71.205.240.248 2 1220 2 116 4 1336
222.147.143.23 <-> 172.16.253.130 2 116 2 1220 4 1336
172.16.253.130 <-> 66.31.49.90 2 1220 2 116 4 1336
180.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
184.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
190.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
201.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
212.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
213.253.253.254 <-> 172.16.253.130 4 232 0 0 4 232
172.16.253.130 <-> 71.254.253.254 0 0 4 232 4 232
172.16.253.130 <-> 87.254.253.254 0 0 4 232 4 232
172.16.253.130 <-> 88.254.253.254 0 0 4 232 4 232
172.16.253.130 <-> 115.254.253.254 0 0 4 232 4 232
172.16.253.130 <-> 135.254.253.254 0 0 4 232 4 232
180.254.253.254 <-> 172.16.253.130 4 232 0 0 4 232
190.254.253.254 <-> 172.16.253.130 4 232 0 0 4 232
172.16.253.130 <-> 122.108.42.3 2 1220 1 58 3 1278
172.16.253.130 <-> 77.38.241.250 2 1220 1 58 3 1278
172.16.253.130 <-> 24.192.219.246 0 0 3 174 3 174
187.24.70.8 <-> 172.16.253.130 1 58 2 660 3 718
172.16.253.130 <-> 24.62.58.244 1 610 2 116 3 726
239.255.255.250 <-> 172.16.253.130 3 525 0 0 3 525
173.217.207.244 <-> 172.16.253.130 1 58 1 610 2 668
187.37.221.247 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 77.239.75.251 1 190 1 58 2 248
174.6.201.58 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 96.37.24.59 1 610 1 58 2 668
172.16.253.130 <-> 74.134.198.91 1 610 1 58 2 668
217.122.27.18 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 67.249.162.249 1 610 1 58 2 668
172.16.253.130 <-> 149.169.251.240 1 610 1 58 2 668
172.16.253.130 <-> 79.119.48.248 1 610 1 58 2 668
213.238.99.54 <-> 172.16.253.130 1 58 1 610 2 668
190.18.75.10 <-> 172.16.253.130 1 58 1 610 2 668
174.5.212.39 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 72.185.161.253 1 610 1 58 2 668
172.16.253.130 <-> 76.10.148.252 1 610 1 58 2 668
172.16.253.130 <-> 121.88.136.25 1 610 1 58 2 668

190.188.23.234 <-> 172.16.253.130 1 58 1 610 2 668
181.46.99.30 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 24.251.155.31 1 610 1 58 2 668
216.212.30.6 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 68.227.164.2 1 610 1 58 2 668
221.31.86.14 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 50.89.229.3 1 610 1 58 2 668
172.16.253.130 <-> 24.8.220.1 1 610 1 58 2 668
172.16.253.130 <-> 76.85.130.1 1 610 1 58 2 668
201.242.155.52 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 68.97.69.21 1 610 1 58 2 668
172.16.253.130 <-> 78.210.148.146 1 610 1 58 2 668
172.16.253.130 <-> 132.239.127.98 1 610 1 58 2 668
172.16.253.130 <-> 74.197.22.12 1 610 1 58 2 668
172.16.253.130 <-> 71.86.90.31 1 610 1 58 2 668
172.16.253.130 <-> 82.130.176.36 1 610 1 58 2 668
172.16.253.130 <-> 71.75.94.251 1 610 1 58 2 668
184.63.10.2 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 68.198.104.16 1 610 1 58 2 668
172.16.253.130 <-> 68.63.59.19 1 610 1 58 2 668
172.16.253.130 <-> 72.208.52.19 1 610 1 58 2 668
172.16.253.130 <-> 74.88.223.17 1 610 1 58 2 668
172.16.253.130 <-> 74.78.96.3 1 610 1 58 2 668
172.16.253.130 <-> 62.83.76.8 1 610 1 58 2 668
172.16.253.130 <-> 24.189.56.15 1 610 1 58 2 668
172.16.253.130 <-> 72.9.76.230 1 610 1 58 2 668
172.16.253.130 <-> 37.61.145.4 1 610 1 58 2 668
172.16.253.130 <-> 114.42.77.245 1 610 1 58 2 668
186.95.53.23 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 98.244.14.31 1 610 1 58 2 668
172.16.253.130 <-> 50.138.151.250 1 610 1 58 2 668
172.16.253.130 <-> 83.166.29.245 1 610 1 58 2 668
172.16.253.130 <-> 97.82.141.252 1 610 1 58 2 668
172.16.253.130 <-> 74.210.227.231 1 610 1 58 2 668
190.183.66.239 <-> 172.16.253.130 2 116 0 0 2 116
172.16.253.130 <-> 83.155.101.250 1 610 1 58 2 668
172.16.253.130 <-> 67.171.167.239 1 610 1 58 2 668
172.16.253.130 <-> 98.226.151.245 1 610 1 58 2 668
172.16.253.130 <-> 78.136.84.249 1 610 1 58 2 668
187.11.74.251 <-> 172.16.253.130 1 58 1 330 2 388
172.16.253.130 <-> 98.15.165.19 1 610 1 58 2 668
172.16.253.130 <-> 83.250.104.244 1 610 1 58 2 668

172.16.253.130 <-> 66.25.254.251 1 610 1 58 2 668
172.16.253.130 <-> 75.108.175.6 1 610 1 58 2 668
200.83.116.254 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 67.86.22.250 1 610 1 58 2 668
172.16.253.130 <-> 85.219.65.249 1 610 1 58 2 668
172.16.253.130 <-> 93.129.51.17 1 610 1 58 2 668
172.16.253.130 <-> 50.82.72.7 1 610 1 58 2 668
172.16.253.130 <-> 84.22.46.10 1 610 1 58 2 668
172.16.253.130 <-> 68.3.136.248 1 610 1 58 2 668
172.16.253.130 <-> 42.2.8.26 1 610 1 58 2 668
172.16.253.130 <-> 74.50.161.16 1 610 1 58 2 668
172.16.253.130 <-> 92.36.232.253 1 610 1 58 2 668
172.16.253.130 <-> 67.242.141.7 1 610 1 58 2 668
172.16.253.130 <-> 68.97.192.245 1 610 1 58 2 668
172.16.253.130 <-> 76.179.132.243 1 610 1 58 2 668
172.16.253.130 <-> 109.91.69.10 1 610 1 58 2 668
172.16.253.130 <-> 72.228.143.4 1 610 1 58 2 668
172.16.253.130 <-> 24.122.95.248 1 610 1 58 2 668
172.16.253.130 <-> 71.230.164.254 1 610 1 58 2 668
172.16.253.130 <-> 88.156.158.252 1 610 1 58 2 668
184.155.119.6 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 92.245.80.12 1 610 1 58 2 668
172.16.253.130 <-> 75.74.147.252 1 610 1 58 2 668
172.16.253.130 <-> 75.178.72.213 1 610 1 58 2 668
172.16.253.130 <-> 24.50.88.235 1 610 1 58 2 668
172.16.253.130 <-> 68.200.221.136 1 610 1 58 2 668
201.82.178.48 <-> 172.16.253.130 1 58 1 610 2 668
201.213.33.102 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 68.230.14.194 1 610 1 58 2 668
172.16.253.130 <-> 66.75.24.66 1 610 1 58 2 668
172.16.253.130 <-> 50.149.21.3 1 610 1 58 2 668
172.16.253.130 <-> 69.244.161.47 1 610 1 58 2 668
172.16.253.130 <-> 68.50.37.55 1 610 1 58 2 668
172.16.253.130 <-> 75.109.4.31 1 610 1 58 2 668
217.29.105.122 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 71.142.137.30 1 610 1 58 2 668
189.47.43.134 <-> 172.16.253.130 1 58 1 610 2 668
172.16.253.130 <-> 96.54.179.14 1 610 1 58 2 668
172.16.253.130 <-> 65.55.21.20 1 90 1 90 2 180
172.16.253.254 <-> 172.16.253.130 0 0 2 684 2 684
255.255.255.255 <-> 0.0.0.0 2 697 0 0 2 697
209.33.87.124 <-> 172.16.253.130 1 58 0 0 1 58

172.16.253.130 <-> 66.67.35.253 0 0 1 58 1 58
172.16.253.130 <-> 66.103.121.14 0 0 1 58 1 58
172.16.253.130 <-> 76.209.55.86 0 0 1 58 1 58
181.164.33.60 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 75.72.214.254 0 0 1 58 1 58
172.16.253.130 <-> 95.234.193.232 0 0 1 58 1 58
209.188.69.239 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 114.42.103.2 0 0 1 58 1 58
172.16.253.130 <-> 69.113.243.26 0 0 1 58 1 58
172.16.253.130 <-> 46.42.233.237 0 0 1 58 1 58
172.16.253.130 <-> 170.51.113.2 0 0 1 58 1 58
172.16.253.130 <-> 65.181.33.2 0 0 1 58 1 58
172.16.253.130 <-> 31.147.118.11 0 0 1 58 1 58
189.100.56.246 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 80.198.94.247 0 0 1 58 1 58
172.16.253.130 <-> 41.200.172.238 0 0 1 58 1 58
172.16.253.130 <-> 42.72.147.237 0 0 1 58 1 58
184.41.210.243 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 108.35.221.6 0 0 1 58 1 58
172.16.253.130 <-> 96.20.100.20 0 0 1 58 1 58
172.16.253.130 <-> 93.114.195.25 0 0 1 58 1 58
189.68.39.1 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 92.86.70.249 0 0 1 58 1 58
190.108.27.11 <-> 172.16.253.130 1 58 0 0 1 58
184.6.88.20 <-> 172.16.253.130 1 58 0 0 1 58
205.204.22.110 <-> 172.16.253.130 1 58 0 0 1 58
172.16.253.130 <-> 24.247.237.237 0 0 1 58 1 58
172.16.253.130 <-> 76.20.50.19 0 0 1 58 1 58
172.16.253.130 <-> 91.242.217.247 0 0 1 62 1 62
172.16.253.130 <-> 4.2.2.2 0 0 1 76 1 76
==========

https://www.virustotal.com/file/984fb2e07de82bc4a228c715dd0790e45dc1d104f6a9b082da9a4cecc0e151b7/analysis/

SHA256: 984fb2e07de82bc4a228c715dd0790e45dc1d104f6a9b082da9a4cecc0e151b7
SHA1: 5842f0d4fe3f177f2bb06a2e5878da55f7d814c7
MD5: 251a2c7eff890c58a9d9eda5b1391082
File size: 160.5 KB (164352 bytes)
File name: vti-rescan
File type: Win32 EXE
Tags: peexe
Detection ratio: 14 / 46
Analysis date: 2012-12-26 05:35:35 UTC (1 hour, 12 minutes ago)

AntiVir TR/Kazy.131060 20121225
Avast Win32:ZAccess-NF [Trj] 20121226
BitDefender Trojan.Generic.KDZ.2714 20121226
DrWeb Trojan.DownLoader7.45342 20121226
ESET-NOD32 a variant of Win32/Kryptik.AREI 20121225
F-Secure Trojan.Generic.KDZ.2714 20121225
Fortinet W32/Kryptik.ARCN!tr 20121226
GData Trojan.Generic.KDZ.2714 20121226
Kaspersky Backdoor.Win32.ZAccess.apvo 20121226
Kingsoft Win32.Hack.ZAccess.ap.(kcloud) 20121225
Malwarebytes Rootkit.0Access 20121226
Microsoft Trojan:Win32/Sirefef.P 20121226
TrendMicro-HouseCall TROJ_GEN.R47H1LP 20121225
ViRobot Backdoor.Win32.A.ZAccess.164352.E 20121226

https://www.virustotal.com/file/d9dfcc507d773bf76075eed8abbb61e54f03f5f920b5c348fd7a0bf5f7bab3dd/analysis/
SHA256: d9dfcc507d773bf76075eed8abbb61e54f03f5f920b5c348fd7a0bf5f7bab3dd
SHA1: 56104a626101126eed10e65171a26e25b6e50712
MD5: 1a12137bd701bd9ed607671ce1b7806a
File size: 160.5 KB (164352 bytes)
File name: amateur_dog_sex_01.avi.exe
File type: Win32 EXE
Tags: peexe
Detection ratio: 6 / 46
Analysis date: 2012-12-25 10:50:38 UTC (19 hours, 59 minutes ago)
BitDefender Gen:Variant.Kazy.131060 20121225
F-Secure Gen:Variant.Kazy.131060 20121225
Kaspersky Backdoor.Win32.ZAccess.apvo 20121225
Malwarebytes Rootkit.0Access 20121225
TrendMicro-HouseCall TROJ_GEN.F47V1225 20121225

https://www.virustotal.com/file/13586ffeca632e34c5813dcce4729b20852db0c9fb3ae0b6319699c739f5be29/analysis/

SHA256: 13586ffeca632e34c5813dcce4729b20852db0c9fb3ae0b6319699c739f5be29
SHA1: 865cf7a7ff3dde0828e7764751d76c8df6291506
MD5: 59b247f0266b107451104243261a7ecf
File size: 159.5 KB (163328 bytes)
File name: animal-xxx-movie.avi.exe
File type: Win32 EXE
Tags: peexe
Detection ratio: 13 / 46
Analysis date: 2012-12-25 19:00:57 UTC (11 hours, 50 minutes ago)
AhnLab-V3 Backdoor/Win32.ZAccess 20121225

Avast Win32:ZAccess-NF [Trj] 20121226
BitDefender Trojan.Generic.KD.817138 20121225
DrWeb Trojan.DownLoader7.45437 20121226
ESET-NOD32 a variant of Win32/Kryptik.AREI 20121225
F-Secure Trojan.Generic.KD.817138 20121225
Fortinet W32/Kryptik.ARCN!tr 20121225
GData Trojan.Generic.KD.817138 20121225
Kaspersky Backdoor.Win32.ZAccess.apzt 20121225
Malwarebytes Rootkit.0Access 20121225
McAfee-GW-Edition - 20121225
Microsoft Trojan:Win32/Meredrop 20121226
MicroWorld-eScan Trojan.Generic.KD.817138 20121225
TrendMicro-HouseCall TROJ_GEN.F47V1225 20121225

SHA256: ac263c2267892fc9995ad841fc649e2071f8626dcc0d2d27cbce4ab6cb54f4ca

SHA1: 33395e02036526ef7c3ab05afb137c7af2bcd6df

MD5: 98a993d62d367682048ec70df109e7d8

File size: 161.0 KB (164864 bytes)

File name: vti-rescan

File type: Win32 EXE

Tags: peexe

Detection ratio: 20 / 46

Analysis date: 2012-12-26 05:39:43 UTC (1 hour, 12 minutes ago)

AhnLab-V3 Backdoor/Win32.ZAccess 20121225

AntiVir TR/Rogue.kdz.2666.1 20121225

Avast Win32:ZAccess-NE [Trj] 20121226

AVG BackDoor.Generic16.ZLB 20121225

BitDefender Trojan.Generic.KDZ.2666 20121226

Comodo UnclassifiedMalware 20121226

DrWeb Trojan.DownLoader7.45110 20121226

ESET-NOD32 a variant of Win32/Kryptik.AREI 20121225

F-Secure Trojan.Generic.KDZ.2666 20121225

Fortinet W32/ZAccess.APQP!tr.bdr 20121226

GData Trojan.Generic.KDZ.2666 20121226

Kaspersky Backdoor.Win32.ZAccess.apqp 20121226

Kingsoft Win32.Malware.Generic.a.(kcloud) 20121225

Malwarebytes Rootkit.0Access 20121226

McAfee-GW-Edition - 20121226

Microsoft Trojan:Win32/Sirefef.P 20121226

nProtect Trojan.Generic.KDZ.2666 20121225

Panda Suspicious file 20121225

TrendMicro-HouseCall TROJ_GEN.R47H1LP 20121225

VIPRE Trojan.Win32.Generic!BT 20121226

ViRobot Backdoor.Win32.A.ZAccess.164864.L 20121226

SHA256: 71b38f041b4a4ae169c44e3aff412e527e1156f92c27f1340a8abe70a45bee10

SHA1: 6d21fc25b9da49d746b2b7609a5efaed4d332e6a

MD5: a2611095f689fadffd3068e0d4e3e7ed

File size: 160.0 KB (163840 bytes)

File name: amateur_dog_sex_01.avi.exe

File type: Win32 EXE

Tags: peexe

Detection ratio: 14 / 45

Analysis date: 2012-12-26 00:19:54 UTC (6 hours, 35 minutes ago)

Avast Win32:ZAccess-NF [Trj] 20121226

BitDefender Trojan.Generic.KD.817217 20121226

Comodo TrojWare.Win32.Trojan.Agent.Gen 20121226

DrWeb Trojan.DownLoader7.45527 20121226

Emsisoft Backdoor.Win32.ZAccess (A) 20121226

Fortinet W32/Kryptik.ARCN!tr 20121226

GData Trojan.Generic.KD.817217 20121226

Ikarus Backdoor.Win32.ZAccess 20121226

Kaspersky Backdoor.Win32.ZAccess.aqep 20121226

Kingsoft Win32.Malware.Generic.a.(kcloud) 20121225

Malwarebytes Rootkit.0Access 20121226

McAfee-GW-Edition - 20121226

MicroWorld-eScan Trojan.Generic.KD.817217 20121226

SUPERAntiSpyware - 20121224

Symantec WS.Reputation.1 20121226

TrendMicro-HouseCall TROJ_GEN.RFFH1LQ 20121226
