Nov 2012 - Backdoor.W32.Makadocs Sample

contagiodump.blogspot.com/2012/12/nov-2012-backdoorw32makadocs-sample.html

End of the year presents:
These is a sample of W32.Makadocs
Related News and Analysis:
November 2012
Malware Targeting Windows 8 Uses Google Docs | Symantec
Backdoor.Makadocs | Symantec

Download

Download. (Email me if you need the password scheme - see profile for email) -< fixed link
Download pcap

Files

File: macadocs.exe_
MD5: 546fa31bb7a4164ca25c8667d4352338
Size: 151552

Symantec:

When the Trojan is executed, it creates the following mutex so that only one instance of it runs on the compromised computer:
Next, it connects to Google docs and uses it as a proxy in order to receive commands from command-and-control (C&C) servers

Automatic scans

https://www.virustotal.com/file/60db904b68bc85f4fc62388ee5a00569f46d29ee0c88fae5d6c07624d17efcf1/analysis/

F-Secure Gen:Trojan.Heur.JP.jqW@amwDZ4dG 9.0.17090.0 20121126
Fortinet W32/Agent.IQT!tr 5.0.26.0 20121126
GData Gen:Trojan.Heur.JP.jqW@amwDZ4dG 22 20121126
Ikarus Backdoor.Win32.Makadocs T3.1.1.122.0 20121126
Jiangmin - 13.0.900 20121126
K7AntiVirus Riskware 9.154.7911 20121126
Kaspersky - 9.0.0.837 20121126
Kingsoft - 2012.9.22.155 20121119
McAfee Generic BackDoor.u 5.400.0.1158 20121126
McAfee-GW-Edition Generic BackDoor.u 2012.1 20121126
Microsoft Backdoor:Win32/Godo.A 1.9002 20121126
MicroWorld-eScan Gen:Trojan.Heur.JP.jqW@amwDZ4dG 12.0.250.0 20121126
Norman W32/Obfuscated.D!genr 6.08.06 20121126
nProtect Trojan/W32.Agent.151552.BDE 2012-11-26.02 20121126
Panda Trj/CI.A 10.0.3.5 20121125
Rising Suspicious 24.38.00.01 20121126
Sophos Troj/GoDocs-A 4.83.0 20121126
SUPERAntiSpyware - 5.6.0.1008 20121126
Symantec Backdoor.Makadocs 20121.2.1.2 20121126
TheHacker - None 20121125
TotalDefense - 37.0.10178 20121126
TrendMicro BKDR_MAKADOCS.JG 9.561.0.1028 20121126
TrendMicro-HouseCall BKDR_MAKADOCS.JG 9.700.0.1001 20121126
VBA32 - 3.12.18.3 20121124
VIPRE Trojan.Win32.Generic.pak!cobra 14168 20121126
ViRobot Backdoor.Win32.S.Makadocs.151552 2011.4.7.4223 20121126

VIRUSTOTAL SANDBOX DATA:

PE HEADER INFORMATION
=====================
Target machine : Intel 386 or later processors and compatible processors
Entry point address : 0x00011EE7
Timestamp : 2012-09-20 13:53:00

PE SECTIONS
===========

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	120462	120832	6.54	3ea58442fc447428d5ee9c481ec41a0d
.rdata	126976	22024	22528	5.09	d1a4b555f003f0201966d5237a79b1d4
.data	151552	11644	4608	2.45	c922df55db7e13f8c35fe8405f207863
.rsrc	163840	2400	2560	5.61	a7fa6e5b71905e1ee49e9e968b03b4ca

PE RESOURCES
============

Resource type Number of resources
RT_ICON : 1
RT_GROUP_ICON : 1
Resource language Number of resources
PORTUGUESE BRAZILIAN : 2

PE IMPORTS
==========

urlmon.dll
URLDownloadToFileA
SHELL32.dll
SHGetPathFromIDListA
SHGetSpecialFolderLocation
SHGetFolderPathA
KERNEL32.dll
GetStdHandle
GetConsoleOutputCP
WaitForSingleObject
HeapDestroy
FreeEnvironmentStringsA
CreatePipe
GetCurrentProcess
GetConsoleMode
GetLocaleInfoA
FreeEnvironmentStringsW
SetStdHandle
FindResourceExA
GetCPInfo
GetStringTypeA
WriteFile
GetSystemTimeAsFileTime
HeapReAlloc
GetStringTypeW

InitializeCriticalSection
LoadResource
InterlockedDecrement
SetLastError
PeekNamedPipe
IsDebuggerPresent
ExitProcess
GetVersionExA
GetModuleFileNameA
SetProcessWorkingSetSize
UnhandledExceptionFilter
TlsGetValue
MultiByteToWideChar
CreateMutexA
DeleteCriticalSection
SetUnhandledExceptionFilter
SetEnvironmentVariableA
TerminateProcess
WriteConsoleA
GetCurrentThreadId
LeaveCriticalSection
WriteConsoleW
InitializeCriticalSectionAndSpinCount
HeapFree
EnterCriticalSection
SetHandleCount
GetOEMCP
QueryPerformanceCounter
GetTickCount
TlsAlloc
FlushFileBuffers
LoadLibraryA
RtlUnwind
GetStartupInfoA
GetProcAddress
GetProcessHeap
CompareStringW
CompareStringA
GetComputerNameA
DuplicateHandle
GetFileType
TlsSetValue

CreateFileA
HeapAlloc
InterlockedIncrement
GetLastError
LCMapStringW
GetConsoleCP
LCMapStringA
GetEnvironmentStringsW
SizeofResource
GetCurrentProcessId
LockResource
WideCharToMultiByte
HeapSize
GetCommandLineA
RaiseException
TlsFree
SetFilePointer
ReadFile
CloseHandle
GetACP
GetModuleHandleW
GetEnvironmentStrings
CreateProcessA
IsValidCodePage
HeapCreate
VirtualFree
Sleep
FindResourceA
VirtualAlloc
OLEAUT32.dll
Ord(4)
Ord(6)
Ord(7)
Ord(9)
ADVAPI32.dll
RegCloseKey
RegSetValueExA
RegQueryValueExA
GetUserNameA
RegOpenKeyExA
RegCreateKeyA
ole32.dll

CoUninitialize
CoCreateInstance
CoInitialize

EXIF METADATA
=============
MIMEType : application/octet-stream
Subsystem : Windows GUI
MachineType : Intel 386 or later, and compatibles
TimeStamp : 2012:09:20 14:53:00+01:00
FileType : Win32 EXE
PEType : PE32
CodeSize : 120832
LinkerVersion : 9.0
EntryPoint : 0x11ee7
InitializedDataSize : 36864
SubsystemVersion : 5.0
ImageVersion : 0.0
OSVersion : 5.0
UninitializedDataSize : 0

File system activity

Opened files...

C:\WINDOWS\system32\net.exe (successful)
C:\WINDOWS\Registration\R000000000007.clb (successful)
\\.\PIPE\lsarpc (successful)
C:\WINDOWS\system32\shdocvw.dll (successful)
C:\WINDOWS\system32\stdole2.tlb (successful)
C:\WINDOWS\system32\mshtml.tlb (successful)
c:\autoexec.bat (successful)
C:\WINDOWS\system32\rsaenh.dll (successful)
C:\WINDOWS\system32\dssenh.dll (successful)
C:\WINDOWS\WindowsShell.manifest (successful)

Read files...

C:\WINDOWS\Registration\R000000000007.clb (successful)
C:\WINDOWS\system32\shdocvw.dll (successful)
C:\WINDOWS\system32\stdole2.tlb (successful)
C:\WINDOWS\system32\mshtml.tlb (successful)
c:\autoexec.bat (successful)
C:\WINDOWS\system32\rsaenh.dll (successful)
C:\WINDOWS\system32\dssenh.dll (successful)
C:\WINDOWS\system32\shell32.dll (successful)

C:\WINDOWS\system32\url.dll (successful)
C:\WINDOWS\system32\mshtml.dll (successful)

Registry activity

Set keys...

KEY: HKEY_USERS\S-1-5-21-1275210071-920026266-1060284298-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\MigrateProxy
TYPE: REG_DWORD
VALUE: 1 (successful)

KEY: HKEY_USERS\S-1-5-21-1275210071-920026266-1060284298-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable
TYPE: REG_DWORD
VALUE: 0 (successful)

KEY: HKEY_CURRENT_CONFIG\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable
TYPE: REG_DWORD
VALUE: 0 (successful)

KEY: HKEY_USERS\S-1-5-21-1275210071-920026266-1060284298-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
TYPE: REG_BINARY
VALUE: (successful)

KEY: HKEY_LOCAL_MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication\Name
TYPE: REG_SZ
VALUE: iexplore.exe (successful)

KEY: HKEY_LOCAL_MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication\ID
TYPE: REG_DWORD
VALUE: 37 (successful)

KEY: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProxyBypass
TYPE: REG_DWORD
VALUE: 1 (successful)

KEY: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName
TYPE: REG_DWORD
VALUE: 1 (successful)

KEY: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\UNCAsIntranet
TYPE: REG_DWORD
VALUE: 1 (successful)

KEY: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012012102920121105\CachePath
TYPE: REG_EXPAND_SZ
VALUE: %USERPROFILE%\Local Settings\History\History.IE5\MSHist012012102920121105\ (successful)

Deleted keys...

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012012110420121105 (successful)

Process activity

Created processes...

net.exe localgroup Administrators (successful)
net.exe localgroup Administradores (successful)
net.exe group Domain Admins" /domain" (successful)
net.exe group Admins. do Dom\xednio" /domain" (successful)
Code injections in the following processes...

IEXPLORE.EXE (successful)

Mutex activity

Created mutexes...

G46A33F21110 (successful)
CTF.LBES.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 (successful)
CTF.Compart.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 (successful)
CTF.Asm.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 (successful)
CTF.Layouts.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 (successful)
CTF.TMD.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 (successful)
DDrawWindowListMutex (successful)
DDrawDriverObjectListMutex (successful)
__DDrawExclMode__ (successful)
__DDrawCheckExclMode__ (successful)
Opened mutexes...

ShimCacheMutex (successful)
!SHMSFTHISTORY! (failed)

Application windows activity

Searched windows...

CLASS: MS_AutodialMonitor
NAME: (null)

CLASS: MS_WebcheckMonitor
NAME: (null)

Windows service activity

Opened service managers...

MACHINE: localhost
DATABASE: SERVICES_ACTIVE_DATABASE (successful)
Opened services...

RASMAN (successful)

Hooking activity

TYPE: WH_MOUSE
METHOD: SetWindowsHook (successful)

TYPE: WH_KEYBOARD
METHOD: SetWindowsHook (successful)

Runtime DLLs

oleaut32.dll (successful)
secur32.dll (successful)
version.dll (successful)
advapi32.dll (successful)
clbcatq.dll (successful)
rpcrt4.dll (successful)
ole32 (successful)
ole32.dll (successful)
c:\windows\system32\rpcrt4.dll (successful)
sxs.dll (successful)

Additional details

- The file sends control codes directly to certain device drivers making use of the DeviceIoControl Windows API function.
- The file installs an application-defined hook procedure into a hook chain. You would install a hook procedure to monitor the system for certain types of events. These events are associated either with a specific thread or with all threads in the same desktop as the calling thread. This is done making use of the SetWindowsHook Windows API function.

Network activity

DNS requests...

docs.google.com (173.194.41.67)
www.gstatic.com (173.194.41.79)
www.google.com (74.125.132.99)

TCP connections...

173.194.41.73:443
173.194.41.79:443
74.125.132.99:443

UDP communications...

<MACHINE_DNS_SERVER>:53