SHA256: e2b5555c60b17be43545bb02a1a88b9da3a14d6c5d1b9bc0d6d9b107159e3008

File name: Automatically_Open_up_IE_create_SynoSurvStation_login.exe

Detection ratio: 12 / 56

Analysis date: 2016-04-03 02:42:20 UTC (1 minute ago)

Condensed report! The following is a condensed report of the behaviour of the file when executed in a controlled environment. The actions and events described were either performed by the file itself or by any other process launched by the executed file or subjected to code injection by the executed file.

Opened files

C:\e2b5555c60b17be43545bb02a1a88b9da3a14d6c5d1b9bc0d6d9b107159e3008 (successful)
C:\WINDOWS\Registration\R000000000007.clb (successful)
\\.\PIPE\lsarpc (successful)
C:\WINDOWS\system32\stdole2.tlb (successful)
C:\WINDOWS\system32\xpsp3res.dll (successful)
c:\autoexec.bat (successful)
C:\WINDOWS\WindowsShell.manifest (successful)
C:\WINDOWS\system32\shell32.dll (successful)
C:\WINDOWS\system32\url.dll (successful)
C:\WINDOWS\system32\mshtml.dll (successful)
C:\Program Files\Internet Explorer\iexplore.exe (successful)
C:\WINDOWS\system32\inetcpl.cpl (successful)
C:\WINDOWS\system32\mshtml.tlb (successful)

Contract

Read files

C:\WINDOWS\Registration\R000000000007.clb (successful)
C:\WINDOWS\system32\stdole2.tlb (successful)
c:\autoexec.bat (successful)
C:\WINDOWS\system32\shell32.dll (successful)
C:\WINDOWS\system32\url.dll (successful)
C:\Program Files\Internet Explorer\iexplore.exe (successful)
C:\WINDOWS\system32\mshtml.tlb (successful)

Code injections in the following processes

IEXPLORE.EXE (successful)

Created mutexes

RasPbFile (failed)
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)

Opened mutexes

RasPbFile (successful)

Searched windows

CLASS: Shell_TrayWnd
NAME: (null)

CLASS: MS_AutodialMonitor
NAME: (null)

CLASS: MS_WebcheckMonitor
NAME: (null)

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

kernel32.dll (successful)

comctl32.dll (successful)

clbcatq.dll (successful)

rpcrt4.dll (successful)

ole32 (successful)

ole32.dll (successful)

c:\windows\system32\rpcrt4.dll (successful)

oleaut32.dll (successful)

urlmon.dll (successful)

wininet.dll (successful)

c:\windows\system32\shdoclc.dll (successful)

mlang.dll (successful)

wsock32 (successful)

ws2_32 (successful)

c:\windows\system32\mswsock.dll (successful)

hnetcfg.dll (successful)

c:\windows\system32\wshtcpip.dll (successful)

ws2_32.dll (successful)

rasapi32.dll (successful)

rtutils.dll (successful)

sensapi.dll (successful)

ntdll.dll (successful)

shell32.dll (successful)

userenv.dll (successful)

netapi32.dll (successful)

c:\windows\system32\xpsp3res.dll (successful)

c:\windows\system32\imm32.dll (successful)

imm32.dll (successful)

oleaut32 (successful)

user32.dll (successful)

uxtheme.dll (successful)

Contract

Additional details

The file uses the IsDebuggerPresent (http://msdn.microsoft.com/en-us/library/windows/desktop/ms680345(v=vs.85).aspx) Windows API function in order to see whether it is being debugged.

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 (http://msdn.microsoft.com/en-us/library/windows/desktop/ms644990(v=vs.85).aspx) Windows API function.

UDP communications

<MACHINE_DNS_SERVER>:53