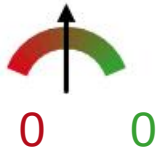
SHA256: e2b5555c60b17be43545bb02a1a88b9da3a14d6c5d1b9bc0d6d9b107159e3008

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)



The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2015-12-10 23:12:54
Entry Point	0x00027F4A
Number of sections	5

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	580910	581120	6.68	c2c2260508750422d20cd5cbb116b146
.rdata	585728	188686	188928	5.76	4513b58651e3d8d87c81a396e5b2f1d1
.data	778240	36724	20992	1.20	c2de4a3d214eae7e87c7bfc06bd79775
.rsrc	815104	54112	54272	7.50	2ad7877da568e47c8fcd0a755f12c7d0
.reloc	872448	28976	29184	6.78	1254908a9a03d2bcf12045d49cd572b9

PE imports

[+] ADVAPI32.dll ()
[+] COMCTL32.dll ()
[+] COMDLG32.dll ()
[+] GDI32.dll ()
[+] IPHLPAPI.DLL ()
[+] KERNEL32.dll ()
[+] MPR.dll ()
[+] OLEAUT32.dll ()
[+] PSAPI.DLL ()
[+] SHELL32.dll ()
[+] USER32.dll ()
[+] USERENV.dll ()
[+] UxTheme.dll ()
[+] VERSION.dll ()
[+] WININET.dll ()
[+] WINMM.dll ()
[+] WSOCK32.dll ()
[+] ole32.dll ()

Number of PE resources by type

RT_STRING	7
RT_ICON	4
RT_GROUP_ICON	4
RT_MANIFEST	1
RT_MENU	1
RT_RCDATA	1
RT_VERSION	1

Number of PE resources by language

ENGLISH UK	18
NEUTRAL	1

Debug information

Type	Timestamp	Offset	Size
IMAGE_DEBUG_TYPE_RESERVED10 (10) ()	Fri Sep 18 14:02:32 2015	738872	4 Bytes

ExifTool file metadata

UninitializedDataSize	0
InitializedDataSize	293376
ImageVersion	0.0
FileVersionNumber	0.0.0.0
LanguageCode	English (British)
FileFlagsMask	0x0000
CharacterSet	Unicode
LinkerVersion	12.0
EntryPoint	0x27f4a
MIMEType	application/octet-stream
TimeStamp	2015:12:11 00:12:54+01:00
FileType	Win32 EXE
PEType	PE32
SubsystemVersion	5.1
OSVersion	5.1
FileOS	Win32
Subsystem	Windows GUI
MachineType	Intel 386 or later, and compatibles
CodeSize	581120
FileSubtype	0
ProductVersionNumber	0.0.0.0
FileTypeExtension	exe
ObjectFileType	Executable application