Virus Profile: Skintrim.gen.k!14AB376BEB66

Risk Assessment: Home Low | Corporate Low

Date Discovered: 11/5/2010

Date Added: 11/5/2010

Origin: Unknown

Length: 1921344

Type: Trojan

Subtype: -

DAT Required: 6157

Virus Characteristics

This is a Trojan

File Properties Property Values

McAfee Detection Skintrim.gen.k

Length 1921344 bytes

MD5 14ab376beb661814cb2cdeeea636ebfb

SHA1 926f682057bb9121bdf66ce591b44a9be94d9a6f

Other Common Detection Aliases

Company Names Detection Names

Microsoft TrojanDownloader:Win32/Wintrim.BX

Symantec Trojan.Gen

Other brands and names may be claimed as the property of others.

Activities Risk Levels

No digital signature is present Informational

McAfee Scans Scan Detections

McAfee Beta Skintrim.gen.k

McAfee Supported Skintrim.gen.k

System Changes

Some path values have been replaced with environment variables as the exact location may vary with different configurations.

e.g.

%WINDIR% = \WINDOWS (Windows 9x/ME/XP/Vista/7), \WINNT (Windows NT/2000)

%PROGRAMFILES% = \Program Files

The following files were analyzed:

926F682057BB9121BDF66CE591B44A9BE94D9A6F

The following files have been added to the system:

- %TEMP%\nsz7.tmp\modern-header.bmp

- %TEMP%\nsz7.tmp\modern-wizard.bmp

- %TEMP%\nsz7.tmp\System.dll

- %TEMP%\nsz7.tmp\nsDialogs.dll

- %TEMP%\nsj6.tmp

The following files were temporarily written to disk then later removed:

- %TEMP%\nsz7.tmp

- %TEMP%\nst5.tmp

The following registry elements have been created:

- HKEY\_CURRENT\_USER\SOFTWARE\GAMES-ATTACK\

- HKEY\_LOCAL\_MACHINE\SOFTWARE\GAMES-ATTACK\

The following registry elements have been changed:

- HKEY\_CURRENT\_USER\SOFTWARE\GAMES-ATTACK\DL\_LG = EN

- HKEY\_LOCAL\_MACHINE\SOFTWARE\GAMES-ATTACK\DL\_LG = EN