Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	228
Risk Level:	1
Date Processed:	2016-04-28 12:53:42 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\600497742f11729df78f50577e2e6dfc.exe"`
Sample ID:	57
Type:	basic
Owner:	admin
Label:	600497742f11729df78f50577e2e6dfc
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	372736 bytes
MD5:	600497742f11729df78f50577e2e6dfc
SHA256:	7c867fae813d162fa6dc3d43c8ee89f62ba7cf949b7b17887e1c2ae83a028061
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\600497742f11729df78f50577e2e6dfc.exe
["C:\windows\temp\600497742f11729df78f50577e2e6dfc.exe"]

File System Events

Opens:	`C:\Windows\Prefetch\600497742F11729DF78F50577E2E6-6AEE154F.pf`
Opens:	`C:\Windows\System32`
Opens:	`C:\windows\temp\600497742f11729df78f50577e2e6dfc.exe.Local\`
Opens:	`C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2`
Opens:	`C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll`
Opens:	`C:\Windows\System32\sechost.dll`
Opens:	`C:\windows\temp\MMFS2.dll`
Opens:	`C:\Windows\system32\MMFS2.dll`
Opens:	`C:\Windows\system\MMFS2.dll`
Opens:	`C:\Windows\MMFS2.dll`
Opens:	`C:\Windows\System32\Wbem\MMFS2.dll`
Opens:	`C:\Windows\System32\WindowsPowerShell\v1.0\MMFS2.dll`

Windows Registry Events

Opens key:	`HKLM\system\currentcontrolset\control\session manager`
Opens key:	`HKLM\system\currentcontrolset\control\terminal server`
Opens key:	`HKLM\system\currentcontrolset\control\safeboot\option`
Opens key:	`HKLM\system\currentcontrolset\control\srp\gp\dll`
Opens key:	`HKLM\software\policies\microsoft\windows\safer\codeidentifiers`
Opens key:	`HKCU\software\policies\microsoft\windows\safer\codeidentifiers`
Opens key:	`HKCU\`
Opens key:	`HKCU\control panel\desktop\muicached\machinelanguageconfiguration`
Opens key:	`HKLM\softare\policies\microsoft\mui\settings`
Opens key:	`HKCU\software\policies\microsoft\control panel\desktop`
Opens key:	`HKCU\control panel\desktop\languageconfiguration`
Opens key:	`HKCU\control panel\desktop`
Opens key:	`HKCU\control panel\desktop\muicached`
Opens key:	`HKLM\software\microsoft\windows\currentversion\sidebyside`

Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
    Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
    Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
    Queries value: HKCU\control panel\desktop[preferreduilanguages]
    Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
    Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]