

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3317, Task ID: 775

Task ID:	775
Risk Level:	5
Date Processed:	2016-05-18 10:36:56 (UTC)
Processing Time:	62.64 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe"
Sample ID:	3317
Type:	basic
Owner:	admin
Label:	57f19466903ed1ef8c74ef4d8c044ddf
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	123930 bytes
MD5:	57f19466903ed1ef8c74ef4d8c044ddf
SHA256:	4dff3c207a81610c4c3a9294dae7bb15471ab1694aff5104bf0d9ded5e6e3264
Description:	None

Pattern Matching Results

5	PE: Contains compressed section
2	PE: Nonstandard section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
["C:\windows\temp\57f19466903ed1ef8c74ef4d8c044ddf.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

File System Events

Opens:	C:\Windows\Prefetch\57F19466903ED1EF8C74EF4D8C044-2BA20017.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\57f19466903ed1ef8c74ef4d8c044ddf.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb

Windows Registry Events

Opens key:	HKLM\software\microsoft\wow64
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\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
 Opens key: HKLM\system\currentcontrolset\control\nls\language
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
 Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
 Opens key: HKLM\software\policies\microsoft\mui\settings
 Opens key: HKCU\
 Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
 Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
 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\wow6432node\microsoft\windows\currentversion\sidebyside
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
 execution options
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions
 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: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
 HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
 us[alternatecodepage]
 Queries value: HKCU\control panel\desktop[preferreduilanguages]
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKCU\software\microsoft\windows
 nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions[usefilter]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions[57f19466903ed1ef8c74ef4d8c044ddf.exe]