

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3317, Task ID: 777

Task ID:	777
Risk Level:	5
Date Processed:	2016-05-18 10:37:09 (UTC)
Processing Time:	64.09 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

3	Program causes a crash [Info]
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 event:	\KernelObjects\SystemErrorPortReady
----------------	-------------------------------------

File System Events

Opens:	C:\Windows\Prefetch\57F19466903ED1EF8C74EF4D8C044-2BA20017.pf
Opens:	C:\Windows\System32

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
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]