Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 152, Task ID: 608

Task ID:	608
Risk Level:	1
Date Processed:	2016-04-28 13:03:37 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe"
Sample ID:	152
Type:	basic
Owner:	admin
Label:	e8fcc1e157e865519dd42edea53b1a53
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	52544 bytes
MD5:	e8fcc1e157e865519dd42edea53b1a53
SHA256:	1f094c241fbefd8ac33e0ef5508cf51a94d05cbc5154a94a74fef0435de09c02
Description:	None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe ["C:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe"]

File System Events

Opens: C:\Windows\Prefetch\E8FCC1E157E865519DD42EDEA53B1-3BDC4F98.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\rtl120.bpl
Opens: C:\Windows\system32\rtl120.bpl
Opens: C:\Windows\system\rtl120.bpl
Opens: C:\Windows\rtl120.bpl
Opens: C:\Windows\System32\Wbem\rtl120.bpl
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\rtl120.bpl

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]