Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1, Task ID: 3

Task ID:	3
Risk Level:	1
Date Processed:	2016-04-28 12:46:38 (UTC)
Processing Time:	66.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\21354e5538706ad6b28941f656b70119.exe"
Sample ID:	1
Type:	basic
Owner:	admin
Label:	21354e5538706ad6b28941f656b70119
Date Added:	2016-04-28 12:44:49 (UTC)
File Type:	PE32:win32:gui
File Size:	65536 bytes
MD5:	21354e5538706ad6b28941f656b70119
SHA256:	38cfeb218e204b232bddc8a071f201d0932bfce0fae32fa344e750cbd2278c9f
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\21354e5538706ad6b28941f656b70119.exe ["C:\windows\temp\21354e5538706ad6b28941f656b70119.exe"]

File System Events

Opens: C:\Windows\Prefetch\21354E5538706AD6B28941F656B70-A7EC65CA.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\USBHID.dll
Opens: C:\Windows\system32\USBHID.dll
Opens: C:\Windows\system\USBHID.dll
Opens: C:\Windows\USBHID.dll
Opens: C:\Windows\System32\Wbem\USBHID.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\USBHID.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
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]