Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 97, Task ID: 389

Task ID:	389
Risk Level:	7
Date Processed:	2016-04-28 12:57:43 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"
Sample ID:	97
Type:	basic
Owner:	admin
Label:	e55165a67c552497d9d653069eae0a8c
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	110080 bytes
MD5:	e55165a67c552497d9d653069eae0a8c
SHA256:	e30c0a5cd916b4f9242e6d77470cff238914cd16806422a8c4f422b37976aa6b
Description:	None

Pattern Matching Results

7 YARA score 7

Static Events

YARA rule hit: KeyLoggerStrings

Process/Thread Events

Creates process: C:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe
["C:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"]

File System Events

Opens: C:\Windows\Prefetch\E55165A67C552497D9D653069EAE0-329CDBF9.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\windows\temp\TaskBrws.dll
Opens: C:\Windows\SysWOW64\TaskBrws.dll
Opens: C:\Windows\system\TaskBrws.dll
Opens: C:\Windows\TaskBrws.dll
Opens: C:\Windows\SysWOW64\Wbem\TaskBrws.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\TaskBrws.dll

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]