Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	809
Risk Level:	4
Date Processed:	2016-04-28 13:09:53 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9af75510bac6aa983165d40392917512.exe"
Sample ID:	202
Type:	basic
Owner:	admin
Label:	9af75510bac6aa983165d40392917512
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	443416 bytes
MD5:	9af75510bac6aa983165d40392917512
SHA256:	776b9b4fac717c342ab35fb19f65ac6b4c311ca206fdc844cec2ef84826cc274
Description:	None

Pattern Matching Results

`4` Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\9af75510bac6aa983165d40392917512.exe
["C:\windows\temp\9af75510bac6aa983165d40392917512.exe"]

File System Events

Opens:	C:\Windows\Prefetch\9AF75510BAC6AA983165D40392917-0F7D552F.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\QtGui4.dll
Opens:	C:\Windows\SysWOW64\QtGui4.dll
Opens:	C:\Windows\system\QtGui4.dll
Opens:	C:\Windows\QtGui4.dll
Opens:	C:\Windows\SysWOW64\Wbem\QtGui4.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\QtGui4.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]