

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 186, Task ID: 744

| | |
|----------------------|--|
| Task ID: | 744 |
| Risk Level: | 4 |
| Date Processed: | 2016-04-28 13:08:00 (UTC) |
| Processing Time: | 2.57 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe" |
| Sample ID: | 186 |
| Type: | basic |
| Owner: | admin |
| Label: | 253635f7a1de05ca2b150731c2473fbc |
| Date Added: | 2016-04-28 12:45:09 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 929280 bytes |
| MD5: | 253635f7a1de05ca2b150731c2473fbc |
| SHA256: | 7f6d85e11a306b88b0f8ef0d1c83df643defd9bd03402bd9e057a594e0912347 |
| Description: | None |

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

| | |
|---|--|
| Creates process: | C:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe |
| ["C:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe"] | |
| Terminates process: | C:\Windows\Temp\253635f7a1de05ca2b150731c2473fbc.exe |

Named Object Events

| | |
|----------------|---|
| Creates mutex: | \Sessions\1\BaseNamedObjects\DBWinMutex |
|----------------|---|

File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\253635F7A1DE05CA2B150731C2473-76DCDF68.pf |
| Opens: | C:\Windows\System32 |
| Opens: | C:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe.Local\ |
| Opens: | C:\Windows\winsxs\x86_microsoft.windows.common- |
| controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2 | |
| Opens: | C:\Windows\winsxs\x86_microsoft.windows.common- |
| controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll | |
| Opens: | C:\windows\temp\WINMM.dll |
| Opens: | C:\Windows\System32\winmm.dll |
| Opens: | C:\windows\temp\VERSION.dll |
| Opens: | C:\Windows\System32\version.dll |
| Opens: | C:\Windows\System32\sechost.dll |
| Opens: | C:\Windows\System32\imm32.dll |
| Opens: | C:\Windows\WindowsShell.Manifest |
| Opens: | C:\Windows\System32\rpcss.dll |
| Opens: | C:\windows\temp\CRYPTBASE.dll |
| Opens: | C:\Windows\System32\cryptbase.dll |
| Opens: | C:\Windows\System32\uxtheme.dll |

Windows Registry Events

| | |
|------------|--|
| Opens key: | HKLM\system\currentcontrolset\control\session manager |
| 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
 Opens key: HKCU\
 Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
 Opens key: HKLM\software\policies\microsoft\mui\settings
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop\languageconfiguration
 Opens key: HKCU\control panel\desktop
 Opens key: HKCU\control panel\desktop\muicached
 Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
 Opens key:
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key: HKLM\system\currentcontrolset\control\error message instrument\
 Opens key: HKLM\system\currentcontrolset\control\error message instrument
 Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
 Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
 Opens key: HKLM\
 Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
 Opens key: HKLM\software\microsoft\ole
 Opens key: HKLM\software\microsoft\ole\tracing
 Opens key: HKLM\software\microsoft\oleaut
 Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[cwdillegalindllsearch]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKCU\control panel\desktop[preferreduilanguages]
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
 HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[253635f7a1de05ca2b150731c2473fbc]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]