# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

| | |
|---|---|
| Task ID: | 176 |
| Risk Level: | 5 |
| Date Processed: | 2016-04-28 12:52:02 (UTC) |
| Processing Time: | 61.11 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\fed7d538ffa814cbc2f2a54af94216d3.exe" |

| | |
|---|---|
| Sample ID: | 44 |
| Type: | basic |
| Owner: | admin |
| Label: | fed7d538ffa814cbc2f2a54af94216d3 |
| Date Added: | 2016-04-28 12:44:54 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 444416 bytes |
| MD5: | fed7d538ffa814cbc2f2a54af94216d3 |
| SHA256: | 3143b6299c209ff8ac9144cf2205b0eb247ba7e704da0acfa11887d16fbcee85 |
| Description: | None |

## Pattern Matching Results

| | |
|---|---|
| 5 | Packer: Asprotect |
| 2 | PE: Nonstandard section |
| 5 | PE: Contains compressed section |

## Static Events

| | |
|---|---|
| Anomaly: | PE: Contains a virtual section |
| Anomaly: | PE: Contains one or more non-standard sections |
| Packer: | ASProtect |

## Process/Thread Events

| | |
|---|---|
| Creates process: | C:\windows\temp\fed7d538ffa814cbc2f2a54af94216d3.exe ["C:\windows\temp\fed7d538ffa814cbc2f2a54af94216d3.exe" ] |

## File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\FED7D538FFA814CBC2F2A54AF9421-D5594AA8.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\eftsres.dll |
| Opens: | C:\Windows\SysWOW64\eftsres.dll |
| Opens: | C:\Windows\system\eftsres.dll |
| Opens: | C:\Windows\eftsres.dll |
| Opens: | C:\Windows\SysWOW64\Wbem\eftsres.dll |
| Opens: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\eftsres.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]
```