

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 66, Task ID: 264

| | |
|----------------------|--|
| Task ID: | 264 |
| Risk Level: | 6 |
| Date Processed: | 2016-04-28 12:54:09 (UTC) |
| Processing Time: | 61.29 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\1e1ec93bb4f5555fb4d45b0472a6171b.exe" |
| Sample ID: | 66 |
| Type: | basic |
| Owner: | admin |
| Label: | 1e1ec93bb4f5555fb4d45b0472a6171b |
| Date Added: | 2016-04-28 12:44:56 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 206336 bytes |
| MD5: | 1e1ec93bb4f5555fb4d45b0472a6171b |
| SHA256: | d7f4fef158bf433b7bf7e8ea796be29e555b7991e7a6659af6fcec53fc444280 |
| Description: | None |

Pattern Matching Results

| | |
|---|----------------------------|
| 6 | PE: File has TLS callbacks |
| 2 | PE: Nonstandard section |

Static Events

| | |
|----------|--|
| Anomaly: | PE: Contains a virtual section |
| Anomaly: | PE: Contains one or more non-standard sections |
| Anomaly: | PE: File contain TLS callbacks |

Process/Thread Events

| | |
|---|--|
| Creates process: | C:\windows\temp\1e1ec93bb4f5555fb4d45b0472a6171b.exe |
| ["C:\windows\temp\1e1ec93bb4f5555fb4d45b0472a6171b.exe"] | |

File System Events

| | |
|--------|---|
| Opens: | C:\Windows\Prefetch\1E1EC93BB4F5555FB4D45B0472A61-84A5F567.pf |
| Opens: | C:\Windows\System32 |
| Opens: | C:\windows\temp\libkdeccore.dll |
| Opens: | C:\Windows\system32\libkdeccore.dll |
| Opens: | C:\Windows\system\libkdeccore.dll |
| Opens: | C:\Windows\libkdeccore.dll |
| Opens: | C:\Windows\System32\Wbem\libkdeccore.dll |
| Opens: | C:\Windows\System32\WindowsPowerShell\v1.0\libkdeccore.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] |

