CARBON BLACK

ARM YOUR ENDPOINTS

Carbon Black Defense Sensor for Windows 2.0.1.8

Release Notes

December 5, 2016

General Notes

Cb Defense Sensor version 2.0.1.8 is a GA (General Availability) release for the Windows operating system only.

New Features

This section lists features introduced in this version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Enhanced Protection Engine

Cb Defense Sensor 2.0 contains many improvements in its engine that detects, blocks and reports malware. Specific improvements include:
- Improved offline protection through the introduction of a signature-based scanner
- Improved behavioral protection for attacks using PDFs, JARs, and macros

Note that the introduction of the signature-based scanner has introduced an additional log file (scanner\scanhost.log) and backend-dashboard options, including options that can be used to optimize performance.

Sensor Settings

☐ Allow Executable Uploads for Scans

☑ Show Sensor UI

☑ Allow User to Disable Protection

☑ Private Logging Level ❓

☐ Run background scan

☐ Scan files on network drives

☑ Scan execute on network drives

☐ Delay Execute for Cloud Scan

☑ Hash MD5

See the User's Guide for details about configuration of these new features.

### *New Cb Defense Sensor User Interface (UI)*

Cb Defense Sensor 2.0 contains a new client UI that can be enabled to notify end users when Cb Defense blocks the execution of suspicious software. The UI can also optionally be configured to allow the end user to enable and disable the Cb Defense Sensor's protection.

Enhanced Whitelist Capabilities

Cb Defense Sensor 2.0 contains enhanced whitelisting capabilities to make it easier for IT administrators to deploy enterprise software. Administrators can leverage a new "IT_TOOLS" whitelist option, and admins can specify that files signed with particular certificates are whitelisted.

Controlling Invocation of Untrusted Applications

Cb Defense Sensor 2.0 contains enhanced ability to control the invocation of untrusted applications.
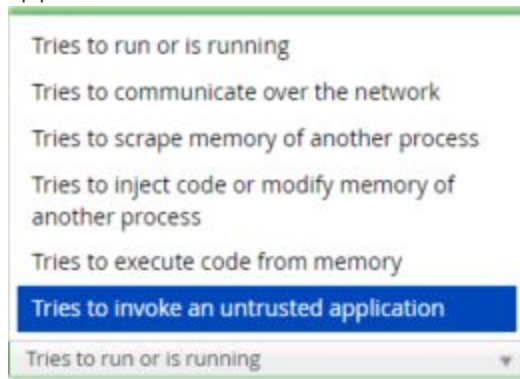
Known Issues and Caveats

The following section lists known issues in this version of Cb Defense Sensor.

ID	Description
n/a	Support for Windows XP, Windows Server 2003, and Windows Vista has been dropped in Cb Defense Sensor 2.0. See the User's Guide for details. Note: Users who need support for these legacy operating systems can continue to use the 1.x Cb Defense Sensor. Contact your Carbon Black account manager for details.
CIT-10032	The "DELAY_SIG_DOWNLOAD=0" installer command-line option (which immediately updates AV signature definitions) cannot be used when upgrading the Cb Defense Sensor (the CLI option works for fresh installs only).
CIT-10273 CIT-10234	The Sensor User Interface's log file (RepUx.log) is in the *user's* temp directory (%TEMP%) rather than the *system* temp directory. Similarly, user-interface "mini-dump" files would be written to this same %TEMP% directory.

Issues Resolved

The following section lists corrective content changes made.

ID	Description
CIT-10009	Internet Explorer 11 crash on Windows 10
CIT-9884	Fatal system error when processing IPv6 information
CIT-6545	Improved processing of app exclusions
CIT-6779	Improved detection of scripts invoked before Sensor start
CIT-10203 CIT-10204	Improved reputation processing and logging in a variety of corner-case situations, including when file certificate verification fails.
CIT-10119	Avoid instance of a false-positive script termination