Carbon Black.

Cb Defense Sensor 3.0.2 for Mac

Release Notes

February 28th, 2018

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

General Notes

These Cb Defense Sensor version 3.0 release notes are for the Mac operating system only.

New Features

This is a maintenance release to improve stability and performance of the sensor. It includes no new features

Issues Resolved in 3.0.2

ID	Description
DSEN-1859 / EA-11294	This release mitigates an interoperability issue between enterprise version of Dropbox (that uses a kernel extension) and CbD, which, in rare cases, could lead to kernel panics.
DSEN-1610	End users were experiencing delays in some cases when leveraging IT tools feature for development tools. IT Tools feature was not handling well timing conditions such when IT Tool launches and immediately drops code (within 1 sec after the tool launch), and, next, the new code runs immediately. This release improves the feature efficacy that will eliminate delay associated with reputation lookups for files dropped by IT Tool and executed, within these timing scenarios. The improvements should enable admins to more effectively leverage IT Tools feature to handle the developer use-case and whitelist common development tools in the environment (code editors, build tools, and other sanctioned code droppers). Documentation on IT Tools Whitelisting can be found here: https://community.carbonblack.com/docs/DOC-5821
DSEN-1753	This fix improves the whitelisting of both scripts that trigger ransomware false positives and scripts that were executed with the interpreter on the command-line.
DSEN-1558	Efficacy fix to reduce Ransomware false positives associated with IDEs and developer tools.

DSEN-1954	Previously, policies were not applied to shell scripts sourced into shell interpreter or shell script. This fix ensures policies will be applied to those shell scripts (security efficacy improvement).
DSEN-1716	Efficacy fix to reduce false positives associated with process termination due to code injection prevention policy rule.
DSEN-1749, DSEN-1832	Performance improvements when handling High Sierra minor operating system updates.
DSEN-1695	Performance improvements on High Sierra devices which spawn large number of new processes frequently, such as build or developer devices.
DSEN-1565	Previously, the attended uninstaller UI would incorrectly indicate an uninstall had failed. This fix resolves the UI bug and the UI will accurately communicate the status of the uninstall.

Known Issues and Caveats

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

Description
We are dropping official support for macOS versions 10.6 - 10.9. The last sensor version for 10.6-10.9 is 1.2.4 (eol, but available for download). The range of macOS versions covered is as follows: **3.X sensor: macOS 10.10 - 10.13 (official support)** **1.X sensor (eol): 10.6 - 10.12** The following behavior is expected when pushing 3.0 sensor upgrade (cloud, attended, and unattended) to 1.X sensors that are running on an unsupported OS: - Devices running 10.6-10.7 will not upgrade. Devices running 10.8-10.9 will upgrade to 3.0 but will be running an unsupported sensor version for that OS.
There is currently a typo with the email that is triggered through the Sensor Management -> Sensor Options -> Add User. The email that is triggered to the user through these steps suggests that the link does not currently include a downloader that supports the 10.13 OSX Installer. It does support 10.13, this is only a typo

Sensor installations on macOS 10.13, High Sierra, require initial KEXT approval of the product kernel extension by administrative policy or end-user. This new requirement enforced by Apple applies to all third party products that have a driver component.

Cb Defense recommends that you preconfigure High Sierra devices with Cb Defense pre-approved drivers by using: MDM policy, netboot, or pre-configured images. This approach simplifies sensor deployment, especially in unattended mode.

If Cb Defense drivers are not pre-approved before sensor installation, the behavior is as follows:

- Unattended installation: installation finalizes and returns success, but logs a warning to installation logs. Because CB Defense drivers cannot load, sensor enters Bypass state and reports this state to the cloud. After KEXT is approved (either by an end-user or an administrator with MDM policy), the sensor recovers within one hour and enters the full protection state.

- Attended installation is handled similarly to unattended, with two differences: (1) sensor installation displays a dialog message that requests the end user to approve the KEXT using system preferences; (2) installer stalls for up 10 minutes, giving a user a chance to approve the KEXT.

To identify devices with sensors not supporting currently loaded OS, go to Enrollment page, change Status filter to ***All***, and type the following search query:

sensorStates:UNSUPPORTED_OS

Use the following search query to help identify devices with sensors that do support the new OS but with sensor KEXT not approved:

sensorStates:DRIVER_INIT_ERROR

See *Apple Technical Note TN2459* for more details and recommendations for enterprise.

MacOS Sensor 3.0.2 will be the last planned release signed with the legacy code-signing certificate (presented as "Scargo, Inc" common name). The next 3.1 release will be signed with the new Carbon Black, Inc. certificate.

This new code signature will require KEXT re-approval on 10.13 since the certificate has changed. MacOS Sensor 3.0.2 will be the last chance to absorb the fixes mentioned above without undergoing the process for KEXT approval.

Certificate Whitelisting feature introduced in 3.0 does not fully support PKG installers. Although the rule does apply to trusted, signed and verified PKG files, it currently does not extend to files that are embedded in the trusted signed PKG installers.

New installer code format: To fresh-install 3.0 sensors, use the 3.0-supported company installation and individual device installation codes. This might require a configuration update to software deployment tools.
Changed command-line interface for sensor unattended uninstallation to require a confirmation switch. The change might require an update of remote management tools. The new unattended procedure can be invoked via: */Applications/Confer.app/uninstall -y*
If you are using script *cbdefense_install_unattended.sh* for **unattended sensor installation or upgrade**, update your software deployment environment to use the script for 3.0 sensor DMG (extracted from */Volumes/CbDefense-3.0.X.X/docs/cbdefense_install_unattended.sh*). The script for 1.X installers is not compatible with 3.0 installer PKG.
Due to enhanced installer protections and new reputation engine, a downgrade from 3.0 to 1.2 is not supported out-of-the-box. Contact Support if this downgrade is required. Uninstall and install is an alternative to a downgrade path; however, this process results in a new device ID and loss of linkage to the original device data.
Live Response feature on macOS does not currently include the memory dump command.
Policy: ***Use Windows Security Center***: setting has no affect on Mac. Policy: ***Delay Execute for Cloud Scan***: setting has no effect on Mac devices. Mac sensor implicitly enables delay execute for cloud scan, based on the configured policy rules. The delay is disabled when no prevention rules are present or when the only policy rules are for "Application" targets: - "At path" - "Company Blacklist" Otherwise, the delay is implicitly enabled to facilitate rules that rely on the cloud reputations and make policy enforcement decisions at pre-execution time.