Sensor Changelog

CB v5.0.0.150416.1350

April 16, 2015

Contents

Future Carbon Black Sensor releases (April 15 2015)

- ** For all future releases of Carbon Black Sensor, please see the Release Notes Document for that version**

Carbon Black Sensor 5.0.0 (January 20 2015)

Changelog

- **WIN-181**
  - CB sensor causing BSOD. Machines are also part of an AV-Container of Kaspersky that have the encryption modules present. ONLY the machines with both the encryption modules AND CB installed ended up with Blue screen.
- **WIN-152**
  - Addressed bug whereby two subsequent network connections via different domain names but the same underlying IP were both reported using the first of the two domain names

Carbon Black Sensor 4.2.5 (March 8 2015)

- **WIN-233 - Toggling Netconn event collection not working correctly**
  - Fix for Sensor Group Netconn event collection not working properly when disabled and re-enabled

- **WIN-229 - Downgrade of sensor from 5.0.0 to 4.2.x resulting in mix of driver versions**
  - fix for downgrade from 5.0.0 to 4.2.x
- **WIN-224 - Upgrade from 4.2.x to 4.2.4 would fail in some cases**
  - fix for timeout on sensor service stop during upgrade on resource limited endpoints
- **WIN-223 - Certain network responses with nested indirect names causes sensor to go into loop**
  - fix for name resolution issue when DNS returns nested label redirection.
- **WIN-209, 153 - Performance enhancement to move discarding of modload events to kernel module**
  - moved dropping of modload events from userspace to kernel
- **WIN-151 - occasionaly reporting corrupted MD5 in mod info message**
  - fixed a helper function that determined reported MD5 in mod info message

Carbon Black Sensor 4.2.4 (January 23 2015)

- **WIN-198 & Win-181 - CB Sensor Causing BSOD**

Employ a fix when certain AV products were installed the endpoint would bluescreen in certain corner cases

- **WIN-162 - update carbonblackk service to point to carbonblackk.sys**

Install fix when sensor was downgraded causing version mismatch of components

- **WIN-159 - On Windows7+ upgrades the carbonblackk.sys file is updated or removed**

Fix for windows 7 upgrade logic to remove unused files

Carbon Black Sensor 4.2.3 (November 20 2014)

Changelog

- **WIN-158 - Enhancement**

Introduce a new sensor setting to prevent file access race condition with 3rd party apps

- **WIN-152 - Bugfix**

Sensor fix to update ip to dns netconn manager map when visiting different hostnames with same IP

- **WIN-150, 157 - 3rd party patch**

Address openssl vulnerability “POODLE” (CVE-2014-3566)

- **SUPPORT-528 - Bugfix**

Address an issue when sensor was leaving file handles open when extracting icons

Carbon Black Sensor 4.2.2 (August 5 2014)

Changelog

- **WIN-104 - Bugfix**

Address Chkdsk not running at boot time

Carbon Black Sensor 4.2.1 (June 27 2014)

Changelog

- **WIN-82 - Address bugcheck in 4.1.5 sensor**

Address improper handling of NULL'ed out UNICODE_STRING

- **WIN-74 - Minimize local disk IO in sensor**

Reduce sensor disk IO by reducing writes to disk

Carbon Black Sensor 4.2.0 (June 9 2014)

Changelog

- **WIN-78 - 3rd party patch**

Address openssl vulnerability (CVE-2014-0024)

- **WIN-75 - Bugfix**

Fix for an issue in unicode string allocations not freeing memory

- **WIN-73 - Bugfix**

Fix for netconn events not having parent process_pid in protobuf

- **WIN-72 - Bugfix**

Fix for Sensor not reading filestore configuration

- **WIN-69 - Bugfix**

Fix for possible dropping of UDP events

Carbon Black Sensor 4.1.6 (May 02 2014)

Changelog

- **WIN-68 - Bugfix**

Fix to limit module info queue growth

- **WIN-67 - Improvement**

Added timing infomation to eventlogger diagnostic log

- **WIN-66 - Bugfix**

Fix to limit event write queue growth related to high memory usage in high modload scenarios

- **WIN-65 - Bugfix**

Fix modload failure

- **WIN-64 - Bugfix**

Reduce cpu usage during high network connection activity

- **WIN-56 - Bugfix**

Harden modinfo path to improve modinfo messages.

- **WIN-55 - Improvement**

Added additional diagnostic information to sensor self-reporting

- **WIN-5 - Bugfix**

Fix for Kernel-mode sensor not reading registry setting on boot

- **ENT-2996 - Bugfix**

Fix for sensor debug output showing incorrect size of internal maps

Carbon Black Sensor 4.1.5 (April 10 2014)

Changelog

- **E-3038 - Bugfix**

Sensor may lock certain critical system dlls against writing, thereby interfering with windows updates

- **E-3021 - 3rd party patch**

Address openssl vulnerability (CVE-2014-0160) in sensor.

- **E-2952 - Bugfix**

Sensor fix for hang at login while both Carbonblack and Symantec EP are installed on x86 systems.

Carbon Black Sensor 4.1.4

No Sensor release

Carbon Black Sensor 4.1.3

Changelog

- E-2861 - Bugfix - Add additional code signing checks to sensor upgrade

Sensor upgrade code signing checks updated to Publisher and ability to validate new cert

- E-2823 - Bugfix - Zero byte log file handling

Sensor can now handle a zero byte log file if this happens

- E-2749 - Improvement - Sensor License text

Updated Sensor license text with new date and names

- E-2745 - Improvement - Sensor Install UI Rebranding

Updated UI branding

Carbon Black Sensor 4.1.0

Backwards Compatibility Note

The 4.1.0 sensor does not work with a pre-4.1 Enterprise Server. Deployment of 4.1 sensors must be done after deployment of the 4.1.0+ Enterprise Server.

Highlights

- Process user context

The sensor can now report the user context that a process is running under. This infomation is reported as the SID and the human readable format.

- Web request netconn improvement

The sensor now reports the actual destination of an HTTP/HTTPS connection by inspecting the request packet. If the web traffic is being proxied, this will determine the correct remote endpoint for the initial request.

- File write type and MD5 hash reporting

The sensor can now report the file type and MD5 hash for certain types of files when they are written to disk. These types include Archives (ZIP, TAR, RAR), Microsoft Office Documents, PDF, and Portable Executable binares (EXE, DLL, SYS).

- Sensor installer enhancements

The installer now contains various enhancements to streamline and improve the sensor install/upgrade/uninstall workflow.

Changelog

- E-380 - Bugfix - File write reporting

The 4.0.x and prior sensors failed to report a file write event when the file was written using memory-mapped IO. The sensor now captures and reports these file writes.

- E-506 - New Feature - Netconn web proxy support

The sensor now reports the actual destination endpoint for proxied web requests.

- E-597 - Bugfix - Registry key deletions

The sensor now correctly reports registry key deletions.

- E-1143 - Bugfix - Registry key renames

The sensor now captures and reports the old and new key name on a registry key rename operation.

- E-1329 - New Feature - File write md5/type

The sensor can now report the md5 hash and file type for certain classes of file when they are written to disk. This collection can be enabled or disabled via policy on the server.

- E-1704 - New Feature - Process user context

The sensor can now report the user context associated with a process. This collection can be enabled or disabled via policy on the server.

- E-2150 - Improvement - Sensor installer

The upgrade process now ensures that the correct version of the sensor is reflected in the Windows installed programs database. The install/uprade process now ensures that only one installation entry is reflected in the Windows installed programs database. The uninstall process now ensures that Carbon Black sensor artifacts are removed from the filesystem and registry.

- E-2183 - Improvement - Sensor/server time delta

The sensor now communicates with the server to determine any delta that may exist between the sensor clock and the server clock. This allows event times to be reported correctly.

- E-2202 - Improvement - Sensor event log transfer

The sensor now compresses the collected event logs prior to transmitting the logs to the server.

- E-2318 - Bugfix - Sensor service

Under certain rare conditions, a malformed debugging string was causing an exception in the usermode sensor service. This is corrected in the new sensor.

- E-1978 - Improvement - Sensor/server communications

The sensor now communicates to the server endpoints by appending the sensor id to the request url. This improves troubleshooting and analysis.

- E-1361 - Bugfix - Sensor id collisions

The 4.0.x and prior sensors could have sensor id collisions when machines are cloned, leading to multiple sensors reporting information to the server with the same sensor id, thereby appearing to be the same sensor. The new sensor received a registration token from the server and this token is used by the server to determine duplicate sensor id instances. If collisions are found, the sensor is asked to re-register and gets a new sensor id.

- E-1658 - Imrovement - Sensor service directory permissions

The entire sensor directory on the filesystem is now secured with an admin-only ACL.

- E-1681, E-1683, E-1685 - Improvement - Core Driver

The 4.1.0 sensor core driver (carbonblackk.sys) includes a series of small, targeted improvements that can, in certain edge cases, provide performance improvements.

Carbon Black Sensor 4.0.2

Changelog

- E-2308 - Bugfix - Sensor service

The Carbon Black sensor service (carbonblack service, normally running as cb.exe) had a memory leak. In particular, long-running processes that repeatedly loaded and unloaded certain classes of dynamic link libraries (DLLs) caused the sensor service to use excessive amounts of memory. This memory was only reclaimed when the long-running process(es) terminated. If the long-running process(es) did not terminate, memory usage grew unbounded.

The 4.0.2 sensor addresses this issue by properly handling these classes of DLL loads and avoiding the memory leak.

Carbon Black Sensor 4.0.0

Highlights

- Windows 8.1 ‘Blue’ Support

The sensor now supports Windows 8.1 ‘Blue’, including Windows Server 2012.

- Power state reporting

The sensor now reports power state transitions, including the power state at last check-in is reflected in the ‘Computers’ page in the web UI. This can assist in determining why a sensor is marked as “Offline”.

Changelog

- E-2057 - Bugfix - TDI Network Monitoring Driver

The Carbon Black sensor ships with two network monitor (NetMon) drivers: a Transport Device Interface (TDI) driver for Windows XP and 2003, and a Windows Filtering Platform (WFP) driver for Vista and higher. The Carbon Black 3.x TDI NetMon driver had a memory leak. On high-load XP and 2003 systems, in particular IIS systems, this could exhibit itself as a failure in Windows in accepting new network connections. The 4.0.0 sensor addresses this issue by removing the memory leak.

- E-1838 - Bugfix - Uninstallation

The 3.2.x and prior sensors sometimes failed to uninstall, or failed to properly uninstall, when the uninstallation was initiated from the Carbon Black web UI. The 4.0.0 sensor addresses this issue by making sensor uninstallation via the web UI reliable. The uninstallation issues in 3.x could be mitigated by using various other uninstallation options; contact Carbon Black support for more information. The 3.2.x and prior sensors sometimes failed to calculate the computer SID when the sensor was installed on domain controllers.

- E-1975 - Bugfix - Sensor Registration

The 3.2.x and prior sensors sometimes failed to calculate the computer SID when the sensor was installed on domain controllers. The 4.0.0 sensor addresses this issue by properly tracking the SID. The 4.0.0 sensor addresses this issue by properly tracking the SID.

- E-1918 - New Feature

The 4.0.0 sensor supports Windows Blue, includes Windows 8.1 and Windows Server 2012 R2.|

- E-1849 - New Feature - Checkin Logic

The 4.0.0 sensor now attempts to check-in with the Enterprise Server when the host computer is going to sleep or powering off. This data is then presented on the “Computers” page in the Carbon Black web UI.

- E-1688, E-1677, E-1674 - Improvement - Core Driver

The 4.0.0 sensor core driver (carbonblackk.sys) includes a series of small, targeted improvements that can, in certain edge cases, provide performance improvements.

Carbon Black Sensor 3.2.1

Highlights

The 3.2.1 sensor fixes a bug in the checkin interval timing. The server sends the next required checkin in seconds, but Windows requires the time in 100 nanosecond blocks. If the next checkin was greater than 214 seconds, the conversion to nanoseconds overflowed a 32-bit value before being assigned to the 64-bit destination variable. This caused sensors to checkin nearly immediately, increasing load on the server unnecessarily.

Carbon Black Sensor 3.2.0

Highlights

The 3.2.0 sensor collects child process events. Two different type of child process events are collected: child process creation and child process termination. Combined with changes in the Enterprise Server v3.2.0, these changes allow for tagging a process to an investigation. Furthermore, they allow for new queries, including querying by child process name, MD5, and count of child processes.

Changelog

- E-1155 - New Feature - Sensor Service

Add support for child process events

- E-1215 - Improvement - Sensor Service

Improve support for capturing binary metadata, such as file version and, digital signature information, during software installation/uninstall scenarios including Windows update.

- E-1520, E-1773 - Improvement - Sensor Service

Additional debug logging when sensor service is unable to calculate computer SID.

- E-1628 - Bugfix - Sensor Core Driver

Avoid bugcheck (BSOD) with Windows Server 2012, Terminal Services, Fair Share and 3rd party software.

- E-1694 - Improvement - Sensor Service

Avoid reporting any IP->name mapping from the `%WINDIR%\system32\drivers\hosts` file. Only over-the-wire name responses are used for IP->name mapping. This can improve reporting with certain host-based network security products, which can block certain known-bad domains by "sinkholing" name resolution to 127.0.0.1 or similar.

- E-1783 - Improvement - Sensor Service

Sensor now reports S_FALSE (0x00000001), a success code, rather than E_FAIL (0x8000FFFF) for the initial core driver status. The E_FAIL was a default error that was reported when the core driver had not yet been started.

- E-1767 - Improvement - Sensor Core Driver

Sensor core driver has improved performance during file operations, particularly on file opens on network shares.

- E-1645 - Bugfix - Sensor Core Driver

Avoid system hang when running with certain older versions of TrendMicro AntiVirus software.

Carbon Black Sensor 3.1.0

Highlights

Sensors now use SSL client certificates to further improve security. Each sensor group is dynamically assigned a unique client certificate. Client certificates can be revoked in response to a potential compromise of the certificates.

Changelog

- E-1096 - Bugfix - Sensor

The 3.0.0 sensor improperly reported the number of binary files pending upload to the server as zero, regardless of how many files were actually pending upload. The 3.1.0 sensor addresses this issue by properly reporting the number of binaries awaiting upload. See the "Sensor Data Queued - Historical View" in the host detail page to see the history of number and size of binary files to be uploaded.

- E-1067 - Improvement - Sensor Installer

The 3.0.0 sensor installer attempted to apply settings provided via the sensor download package. If the settings were missing, most often because the settings were not extracted from the zipped download package, installation continued but the resultant install could not communicate with the server, as no settings were applied. The 3.1.0 sensor installer addresses this issue by aborting the installation if no settings file exists.

- E-1153 - Improvement - Sensor

The 3.0.0 sensor queried the registry frequently for updated settings. The 3.1.0 sensor addresses this issue by only querying the registry when the settings have been updated, thereby reducing load on the host computer.

- E-1154 - Improvement - Sensor

The 3.1.0 sensor improves the ‘sensorcomms.log’ diagnostic log by making the field width for server URL wider. This keeps the tabular data aligned when using long server URLs.

- E-1127 - Bugfix - Sensor

The 3.0.0 sensor ‘throttled’ repeated network connections by identifying ‘duplicate’ network connections. Duplicates were defined as having the same five characteristics: remote IP, remote port, protocol, connection direction, and process ID. In the case of inbound network connections, this was an erroneous comparison and the result was potentially significantly increased event volume. No data was lost; instead, repeated connections with the same characteristics were reported repeatedly. 3.1.0 addresses this issue by comparing the local port, rather than the remote port, for inbound connections. The result is significantly reduced event volumes and data storage requirements for servers with numerou inbound network connections from the same remote hosts.

- E-1169 - Bugfix - Sensor

The 3.0.0 sensor reported all local IPs bound to all local interfaces. It also included an ‘empty’ set of IPs for those interfaces for which no IP was bound. This resulted in an empty output line in the host detail page in the web UI. 3.1.0 addresses this issue by reporting only valid IP addresses for the host computer.

- E-1141 - Bugfix - Sensor

The 3.0.0 sensor inconsistently reported registry value names as part of registry modification events. The key name was consistently and correctly reported, but the value name was sometimes missing. The 3.1.0 sensor addresses this issue by consistently and correctly reported the value name.

- E-1136 - Improvement - Sensor

The 3.0.0 sensor locked down the event log subdirectory to allow only administrators access. The 3.1.0 sensor improves upon this by locking down the debug log, diagnostic log, and binary file directories to allow only administrators access.

- E-1076 - Improvement - Sensor

The 3.1.0 sensor improves support for valid SSL certificates. It is now possible to configured a valid, root-signed SSL server certificate and use it to secure server-sensor communications.

- E-1125 - Improvement - Sensor

The sensor installer now provides settings in an INI file format. This contrasts with the .bin file format of 3.0.0. The INI format has the advantage of being human-readable and human-editable. Note that the INI file format must be used with 3.1.0 and greater sensors.

- E-1282 - Improvement - Sensor

The 3.1.0 sensor adds a new on-host diagnostic mechanism. Using “sc control carbonblack 202” from an elevated administrative command prompt, many in-memory debugging statistics are cleared. This, in combination with the existing 201 diagnostic code to dump debugging information to the `%WINDIR%\CarbonBlack\Diagnostics` directory, provides for more granular control over debugging statistics.

- E-1243 - Bugfix - Sensor

The 3.0.0 sensor can, in certain cases, hang indefinitely on a network operation to the Enterprise Server. 3.1.0 addresses this issue by adding a reasonable timeout and aborting network operations that last too long. This issue is related to E-1293.

- E-1293 - Bugfix - Sensor

The 3.0.0 sensor can, in certain cases, fail to respond to a stop command, for example with “sc stop carbonblack”. 3.1.0 addresses this issue by aborting any outstanding network operations to expediently handle a stop request.

- E-1284 - Bugfix - Sensor

The 3.0.0 sensor can, in certain edge cases, report improper version information for a binary file such as an EXE or DLL. 3.1.0 addresses this issue by providing additional protections to ensure accurate reporting. If accurate reporting is not possible, then the subset of accurate data is provided.

- E-1270 - Bugfix - Sensor

The 3.0.0 sensor can improperly report the status of the NetMon driver as successful if the NetMon driver start type is disabled. The sensor never puts the NetMon driver in the Disabled start type state, so this issue only presents itself if someone manually sets the state. The 3.1.0 sensor addresses this issue by properly reporting the NetMon driver state even when the NetMon driver start type is disabled.