Carbon Black Cloud sensor version 3.5.0.1402 is for Windows only. This is a beta release.

Notes:

- The 3.5 MSI file is signed with a SHA256 signature. Support for SHA256 was provided as part of a Windows 7 patch. If Windows 7 machines or Windows Server 2008 R2 machines do not have this patch, you can find it here: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3033929. Machines that are running later operating systems have out-of-the box support.

- Windows 7 requires SHA256 signing as of July 2019. See https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update.

Disable services associated with malware

Malicious services that run at start-up have the potential to execute and impact the endpoint before the sensor starts up. The new feature finds all malicious services associated with Known Malware hashes and puts them in a disabled state. The services remain in disabled state across reboots, and therefore cannot execute at startup. Remediation is manual (via CB LiveResponse). The feature is enabled by default and can be disabled by a request to Support.

The command for the remediation through CB LiveResponse is:

1. Query the service `start type exec: execfg sc.exe qc <servicename>`
2. Change the start type using the command: `execfg sc.exe config <servicename> start=<starttype>`

The possible start types are: `boot | system | auto | demand | disabled | delayed-auto`

The event that is sent during the service disable contains the original start type and displays in the user interface. The user needs this data to return the start type to its original value. If the start type changes to boot, auto or delayed-auto, they must reboot.

Carbon Black, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

Removal of registry keys during deletion

Deletion of files, both manual and through the Malware Removal workflow, previously could not remove registry keys that were created by the malware. The Carbon Black Cloud Windows sensor v3.5 enables the removal of `runOnce` registry keys, together with the configuration that enables the removal of other registry keys. Carbon Black Cloud successfully cleans up HKLM key values, but in multi-user environments, the HKCU key cleanup does not work reliably.

Offline installer

The Windows sensor now supports offline installs to support machines that are configured in an offline environment. The feature is enabled during a command line install by adding the flag “OFFLINE_INSTALL=1”. The sensor connects with the Carbon Black Cloud backend and accesses a policy when network connectivity is restored. Master images maintain this install configuration, so multiple endpoints can be configured based on this image.

Endpoint management improvements

The Windows 3.5 sensor effectively handles non-persistent domain disconnections. Previously, the sensor applied the default policy when the AD attribute was cleared (in instances such as off-network without VPN). Now, the sensor persists the desired AD group and the desired policy. The distinguished name is not cleared unless the machine is not registered as part of the domain.

In the **Endpoints** page, the 3.5 sensor also reports who is logged into an endpoint instead of reporting the user who installed the sensor. In the case of multiple logged in users, the most recently logged in user is associated with the endpoint.

Improved capability to identify command interpreters

CB Defense has improved its methods for identifying a process as command interpreter. By integrating with the yara binary pattern matching utility, the Windows 3.5 sensor better protects against threats where an attacker brings their own copy of standard operating system interpreters. Customers who are already leveraging the **Tries to invoke command interpreter** rule immediately benefit from this update.

As part of this update, Carbon Black’s Threat Analysis Unit (TAU) can dynamically update the definition of what it means to be a command interpreter.

Improved Netconn detection for proxy servers

With the Windows 3.4 sensor, CB ThreatHunter customers who are using a proxy server in their environment saw most (all) outbound network connections being reported with the proxy's address and host name as the destination. The Windows 3.5 sensor improves reporting of network events to report the actual destination IP and hostname, rather than those of the intermediate proxy.

CB ThreatHunter hash blacklisting

The Windows 3.5 GA sensor will enable blacklisting of files by hash for CB ThreatHunter. Once a hash is added to the company blacklist it is prevented from:

- being opened with execute access
- starting a process from a file
- being loaded as a module in a process
- being loaded as a script

Processes that have the blacklisted hash loaded at the time the hash is added to the blacklist are terminated shortly after the sensor receives the updated reputation.

Note: This functionality is enabled in the Windows 3.5 GA sensor, but will not be available for use until a future Carbon Black Cloud console release.

Dynamic tamper protection

The sensor has improved its methods for identifying tamper events. The improvements help prevent access to sensor files and reduce interoperability issues with third-party products.

AMSI logging

The Windows 3.5 sensor enables the collection of deobfuscated command line data through AMSI for CB ThreatHunter customers. The feature requires the Windows 3.5 sensor when it becomes available on the backend. For more information on AMSI, see https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
DSEN-3992	Previously, subkeys could be created under the `CBDefense` key in the Windows registry.
DSEN-4054, DSEN-4033	The LiveResponse memdump command was previously observed to cause crashes. It was disabled by default on Windows sensors 3.3 and 3.4 . It is now enabled by default and no longer causes crashes.
DSEN-4375	The sensor previously wrote large amounts of extra data to the `confer.log` file. Numbers vary across environments, but the issue is resolved so that the extraneous data written to `confer.log` is reduced, and the sensor disk size is reduced.
DSEN-5626	Previously, the sensor allowed non-execute access to quarantined files. Now, quarantined files are not accessed. This can prevent other security applications from scanning and alerting on the file, but prevents files from spreading to other locations. This issue is now resolved.
DSEN-6322, EA-14880	There were reports of intermittent delays when opening various Office files and navigating file systems on Windows 10. This issue is now resolved.
DSEN-5995, EA-14707, EA-14723, EA-14729	Previously, customers who were using Windows sensor versions from 3.4.0.1047 to 3.4.0.1077 had Office applications such as Word and Excel hang when updating a file on Google File Stream and similar products (Box, Citrix Cloud, etc.). This issue is fixed in 3.5 and 3.4.0.1086 versions of the sensor.
EA-14455, DSEN-5699	Sensor install failed on Windows Server 2019 machines where there is a missing directory value for registry key `HKLM\SYSTEM\CurrentControlSet\Control\EarlyLaunch value "BackupPath"`. The value is typically `C:\Windows\ELAMBKUP`.
DSEN-5493, DSEN-5491	During updates to Windows 1H19, the system either blocked the update or potentially crashed during the update. This issue was only reproduced and identified internally, and the issue did not reproduce if the sensor was in Bypass mode.

DSEN-4050	Previously, if a user executed an unattended install with the flag and argument "`INSTALLFOLDER=<path>`", the sensor installed but was non-functional. Carbon Black now forces an install failure if a user tries to use a non-standard install folder.
DSEN-4043	Under high load, `repmgr.exe's` handle counts grew very large, causing minor performance issues.
DSEN-6372	Previously, if the sensor's background scan changed from **disabled** (either via install arguments or cloud policy) to **expedited**, a race condition could put the background scan into disabled state. This issue was not observed externally.
DSEN-6077	Windbg had been observed to crash. This issue is now resolved.
DSEN-3061	Previously, the sensor did not whitelist files by certificate if the certificate is signed with multi-byte characters. A backend fix was implemented for this issue.
EA-15148, DSEN-6552	A crash occurs on file renames on network drives, although it was unlikely to happen consistently..
DSEN-6535, DSEN-6591	Sensor upgrades failed with error 1603 when attempting to perform the upgrade at the same time as a Windows upgrade to Redstone 5.
DSEN-4756, DSER-14090, EA-13906	Customers running CB ThreatHunter standalone might have seen Windows Security Center Real Time protection feature disabled. This issue was resolved by navigating to the **Policies** page, clicking the **Sensor** tab, and unchecking **Use Windows Security Center**.
DSEN-6057	Previously, release notes stated that blacklisted scripts execute if the policy is refreshed on the backend after blacklisting. Only scripts executing when sensor was coming out of bypass were not blocked. Blacklisted scripts executed after bypass is disabled are blocked. This issue is functioning as designed.
DSEN-6487	In Sensor environments 3.4.0.1070 and 3.4.0.1077 (and 3.4.0.1016), sensor crashed upon running any process from a path with Japanese characters (c:\見る) when UBS for CB ThreatHunter customers was enabled.
DSEN-6490	HTML file load and open and close performance has degraded in 3.5 as compared to 3.4. This fix was implemented in 3.5.0.1402.
DSEN-6491	Previously, end users can experience a minor delay in loading common applications. This issue was fixed in sensor version 3.5.0.1339.

Known issues

Issue ID	Description
DSEN-1987	False positive alert when the [application name] attempts to access raw disk on the file. See https://community.carbonblack.com/docs/DOC-10730.
DSEN-1180, DSEN-3065	When using CB Live Response, users can terminate the sensor if they terminate `RepMgr.exe`. Terminating this process means that the sensor cannot connect to the backend and the CB LiveResponse session ends. The sensor does not recover until after a reboot. Users can also delete certain files within the `confer` directory. Users are advised to use caution during CB LiveResponse sessions.
DSEN-2378	During an attended install, the Windows installer shows a blank error dialogue when attempting to install on an unsupported operating system.
DSEN-1387	Background Scan remains disabled on devices where VDI=1 was used. See https://community.carbonblack.com/docs/DOC-12001.
DSEN-4216	The Windows 3.4 sensor accumulates deleted files within the sensor cache and does not remove them when the files are removed from disk. This can lead to the sensor reporting that malware is still on disk when it has been removed.
DSEN-4143	Users might experience blocks of Microsoft OS upgrades if an upgrade is attempted shortly after release, before the Carbon Black Cloud product has established a reputation for the operating system. An admin can work around this issue by either placing the sensor in Bypass or adding the following paths to bypass: 1. `**\windows\servicing\**` 2. `**\$windows.~b\**` Make sure that the policy configuration: **When an unknown application tries to run - deny/terminate** is disabled when you upgrade.
DSEN-4591, EA-13682	Arcmap files are corrupted or missing in certain environments.
DSEN-4581,	A terminate action might be applied to `wmiprvse.exe`, showing an alert in

DSEN-4694	the Carbon Black Cloud console during machine start-up. At the time, `wmiprvse` has an unknown reputation and is scraping `lsass.exe`. This commonly happens during Windows updates. `Wmiprvse.exe` should execute after the reputation resolves, and the update should succeed.
DSEN-4924 EA-13414	Some customers have reported interoperability issues with Skype, Lync, and Windbg on Windows 7. Other operating systems are unaffected.
DSEN-5934, EA-14272, EA-14956	Customers cannot open attachments while using applications such as KnowBe4 Second Chance or Digital Guardian's Outlook plug-in.
DSEN-5163	The sensor does not prohibit downgrades from existing Windows 3.5 versions to older Windows 3.5 versions. Carbon Black does not recommend a downgrade between 3.5 builds because it leaves the sensor uninstalled. This issue is resolved in all released 3.5 builds except for 3.5.0.1278. Carbon Black does not recommend or support downgrades, but the downgrade to 3.5.0.1278 is not prevented.
DSEN-3408	The `CLI_USERS=<Sid>` command line option works correctly when you install non-interactively using a `COMPANY_CODE`, but it doesn't work if you use the direct end user installer using the activation code.
DSEN-6540	This sensor user interface might show the sensor in bypass when it is active. This issue has only been reproduced internally and is considered a rare event.
DSEN-6534	False positive blocks can occur due to sharing violations while retrieving signature information.
DSEN-6491	Application launch performance has degraded in the Windows 3.5 sensor as compared to the Windows 3.4 sensor.
DSEN-6706	`Explorer.exe` hangs indefinitely on attempt to run any process in the `confer` install folder as administrator in the Windows sensor 3.5.0.1357.
DSEN-6691	If a file has a bypass rule that is removed after the file is deleted, then copies of that file will not be quarantined in place.
DSEN-6660	One internal user experienced a crash on Windows sensor 3.5.0.1346 running on Windows 8.1 x86.
DSEN-6654	A Windows freeze was reported during the first login with a domain account during a Group Policy upgrade from Windows sensor 3.4.0.1077 to Windows sensor 3.5.0.1339.

DSEN-6625	The Windows sensor does not support Japanese characters in Osquery results in version 3.4.0.1016.
DSEN-6622	The Group Policy upgrade from Windows sensor 3.2.1.51 to Windows sensor 3.5.0.1332 failed. This was reported internally in a test environment.
DSEN-6569	When running Carbon Black-signed msi in Windows sensor 3.5.0.1317, `cmd.exe` is granted full bypass.The `cmd.exe` is only placed in bypass if the sensor msi is executed in `cmd.exe`.
DSEN-6145	When the sensor is in CB ThreatHunter standalone mode, **Ready** queue items are inserted into the database. Customers who move from CB ThreatHunter standalone to CB ThreatHunter with CB Defense can experience false positive blocks.
DSEN-6136	Non-executable file reads, writes, and deletes are 40+% slower on Windows sensor 3.5.0.1160 than Windows sensor 3.4.0.1078.
DSEN-4924	One customer observed windbg and Lync crashed.
DSEN-6867	In the Windows 8 VM, Windows sensor 3.5.0.1339, the CB LiveResponse API creates an output file with UTF-16LE encoding.
DSEN-6315	Some sub-processes were left in a suspended state. This was only observed internally.
DSEN-6826	In Windows 10 19H2 environment with CB Defense and CB ThreatHunter enabled, a 50% performance spike is identified in Repmgr usage when the system is idle.
DSEN-6871	When running rep manager as an admin in Windows sensor 3.5.0.1445 and Windows sensor 3.5.0.1446 environments, the sensor becomes deregistered from the Windows Security Center.
DSEN-6876	When installing Windows sensor 3.4.0.1086, latency is observed with certain Windows applications.
DSEN-6653	When the Windows sensor 3.5 is in bypass mode, the sensor uninstall fails.We recommend keeping the sensor active during uninstall.