Carbon Black Cloud sensor version 3.5.0.1523 is for Windows only. This release is Generally Available.

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. A 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. If a service binary in question was not malicious or if some other tool is used to clean the malware, then the sensor will not automatically enable the service again. To re-enable the service you must manually do so by using LiveResponse or other standard tools. 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 did not attempt to remove registry keys that were created by the malware. When requested to delete a file, the 3.5 sensor also removes RunOnce registry keys from the HKLM hive that reference the malicious binary that is being deleted. Other auto-start registry keys referencing the malware might remain.

Offline installer

The Windows 3.5 sensor now supports offline installs to support machines that are configured in an offline environment. The feature is enabled during a command line installation 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. The sensor will not provide any visibility or protection until it is connected to the backend.

To use the feature, ensure that there is a host or network level firewall rule in place to prevent the the master image from connecting to the Carbon Black Cloud devices URL. Then, Install the sensor using the OFFLINE_INSTALL parameter and any other parameter that is typically used during a command line install (aside from PROXY). Clone or restore to snapshot. Each snapshot and clone appears as a new device in the backend console and are not treated as a VDI clone unless you explicitly install with VDI=1 or used the repCLI reregister command. Otherwise, console admins are responsible for cleaning up old clones, either manually or via API.

Please note, that if a user changes the company code in the backend, one can no longer make new clones that haven’t registered yet because those clones will continue to try to use the original company code. If you change the company code, you must create new images using the new company code.

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 maintains 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 Windows 3.5 sensor also reports who is logged into an endpoint every 8 hours instead of reporting the user who installed the sensor. If there is no interactive user logged in to the endpoint within the 8 hour window, you may get a non interactive user name such as “Windows Manager\DWM-2”. 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 a command interpreter or as a script host. 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 or tries to hide by running tools with non-standard names. 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 sensor enables 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 sensor, but will not be available for use until a future Carbon Black Cloud console release.

Dynamic tamper protection

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

AMSI Integration

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

In the cloud UI, this integration will manifest in the form of filess_scriptload events, which represents processes that executed commands in fileless execution context. More information will be provided in the backend release notes for the February 17th UI release.

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. Note that actual size of confer.log may increase since, while extraneous data is reduced, valuable log data will remain over a longer course of time due to a seperate change.
DSEN-5626	Previously, the sensor allowed non-execute access to quarantined files. Now, quarantined files are not accessible. This can prevent other security applications from scanning and alerting on the file, but prevents files from spreading to other locations. This issue is 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 resolved.
DSEN-5995, EA-14707,	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

EA-14723, EA-14729	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, which could cause 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 had only applied to CB Defense customers. This issue is 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 could occur 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 multibyte 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-6653	Previously, when the Windows sensor 3.5 was in bypass mode, the sensor uninstall failed. This issue is resolved.
DSEN-6876, EA-15319, EA-15301	Previously, customers may have observed latency associated with Microsoft office apps. This issue is resolved.
DSEN-6871	Previously users could deregister the sensor from Windows Security Center on their own in conflict with the policy setting. This issue is resolved.
DSEN-6826	3.5 beta users may have experienced a performance problem on a Windows 10 19H2 environment with CB Defense and CB ThreatHunter enabled. Previously, a 50% performance spikein repmgr.exe usage was identified when the system is idle. This issue is resolved.
DSEN-6867	The CB LiveResponse API previously defaulted to UTF-16LE encoding rather than UTF-8. Because many customers rely on the latter, the default setting is restored to UTF-8. This issue only impacted 3.5 beta users.
DSEN-6145	Previously, customers who had moved from CB ThreatHunter standalone to CB ThreatHunter with CB Defense can experience false positive blocks. This issue was only reported internally. The issue is resolved.
DSEN-6491	Some users experienced a minor delay in loading common applications This issue is resolved.
DSEN-6569	Previously, while running Carbon Black-signed msi in Windows sensor 3.5, `cmd.exe` is granted full bypass.The `cmd.exe` is only placed in bypass if the sensor msi is executed in `cmd.exe`. This issue is resolved.
DSEN-6625	The Windows sensor did not previously support multi-byte characters in Osquery results in version 3.4.0.1016. This is resolved.
DSEN-6660	One internal user experienced a crash on Windows sensor 3.5.0.1346 running on Windows 8.1 x86. This issue is resolved.

DSEN-6691	In earlier 3.5 builds, if a file had a bypass rule that was removed after the file was deleted, then copies of that file would not be quarantined in place. This issue is resolved.
DSEN-6706	Previously, `Explorer.exe` hung indefinitely on an attempt to run any process in the `confer` install folder as administrator in the Windows sensor 3.5.0.1357. This issue is resolved.
DSEN-5163	The sensor did not prohibit downgrades from existing Windows 3.5 versions to older Windows 3.5 versions. 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-5934, EA-14272, EA-14956	Previously, customers could not open attachments while using applications such as KnowBe4 Second Chance or Digital Guardian's Outlook plug-in. This issue is now fixed.
DSEN-6540	Previously, the sensor user interface might have shown the sensor in bypass when it is active. This issue had only been reproduced internally and is considered a rare event. This issue is now resolved and the sensor UI will show the correct status.
DSEN-6543	Previously, false positive blocks may have occurred due to sharing violations while retrieving signature information. This issue is now resolved.
DSEN-6941	Application launch performance had degraded in the Windows 3.5 sensor as compared to the Windows 3.4 sensor. This issue is now resolved and application launch performance is similar across sensor versions.
DSEN-6899, DSEN-7134	Previously, customers had experienced delays of up to 35 seconds associated with copying files to remote network drives. The sensor no longer reporting signature or reputation information at the time of "last write" (i.e. close of handle that modified an executable file). The sensor will still collect and report that info if the file was executed but will not stall to collect it at time of modification.
DSEN-7005, DSEN-6990	Files with no logical drive mapping (such as some google drive files) may not have been reported to the cloud.This issue impacted beta sensors only and the issue is now resolved.
DSEN-6315	Previously, some sub-processes were left in a suspended state after their parents were terminated. This was only observed internally and is now fixed.
DSEN-7026	One customer had observed a crash on some machines during the 3.5 beta program. This issue will be resolved in the next 3.5 build.

DSEN-7099	There had been observations internally of timeouts which lead to reputation mismatch which could have resulted in false positive blocks. This issue is now resolved.

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, DSEN-4694	A terminate action might be applied to `wmiprvse.exe`, showing an alert in 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-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-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-6622	The Group Policy upgrade from Windows sensor 3.2.1.51 to Windows sensor 3.5.0.1332 failed. The steps to resolve this are documented internally and will be provided in the next update of the user guide.
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 crash.
DSEN-7275	If uninstall or sensor service shutdown occurs during an expedited background scan, then the uninstall or shutdown may not complete in a timely fashion.

DSEN-7254	Creating a folder at a network file has been observed to take up to 15 seconds. Initial folder creates occur within a normal time frame. Mapping the folder drive on initial creation will workaround this issue.
DSEN-7144	When “"disable services of known malware” is enabled, some endpoints have observed a spike in CPU every ~5 minutes.
DSEN-5881	In some cases, metadata associated with blacklisted files is not present in the UI. This has only been reproduced internally.
EA-15703, DSEN-7446	The endpoints page in the cloud UI may not reflect the Active Directory or Organizational Unit information. This issue will be fixed in the next 3.5 maintenance release.