securityweek.com


# Dubious Report Highlights Known Risks of Cloud-Based Multiscanners

*Ionut Arghire is an international correspondent for SecurityWeek.*

7-9 minutes

---

**Over the past week, a debate has spurred over a report from security services firm DirectDefense, claiming that Carbon Black's endpoint detection and response (EDR) solution, Cb Response, is a prolific data leaker and exposes client data.**

DirectDefense claims that the issues is related to the product's ability to automatically upload binaries to a cloud-based multiscanner (namely, Google-owned VirusTotal) to better assess whether they are malicious or not. Specifically, the company says that it was able to pinpoint files uploaded to the multiscanner using the API key associated with Cb Response.

DirectDefense claimed that this setup creates, "the world's largest pay-for-play data exfiltration botnet," because clients of the multiscanner can access any of the uploaded files, regardless of where they came from. Further, because Cb Response associates its API key to the uploaded files, one would be able to learn information on Carbon Black enterprise customers based on these files alone.

"When a new file appears on a protected endpoint, a cryptographic hash is calculated. This hash is then used to look the file up in

Carbon Black's cloud. If Carbon Black has a score for this file, it gives the existing score, but if no entry exists, it requests an upload of the file. Since Carbon Black doesn't know if this previously unseen file is good or bad, it then sends the file to a secondary cloud-based multiscanner for scoring. This means that all new files are uploaded to Carbon Black at least once," DirectDefense explains.

The explanation is accurate, but only up to a specific point: it doesn't mention that customers have control over the option to upload binaries to VirusTotal, and that the feature is turned off by default. The report also fails to point out that Carbon Black actually warns customers of the risks involved in enabling the option to share files with VirusTotal, which is an external source.

"By electing to enable the 'Scan unknown binaries with VirusTotal' feature, your server will send unknown binaries to Carbon Black with your consent. By electing to enable the 'Share binary hashes with VirusTotal' feature, your server will send binary hashes and other metadata to Carbon Black with your consent. Each binary and/or hash and file metadata, as the case may be, will be submitted to VirusTotal and governed solely by the Terms of Service and Privacy Policy of VirusTotal. Carbon Black shall not be responsible for this submission or for any act or omission by VirusTotal," the warning reads.

Carbon Black, which has already issued a response to the report, points out that the so-called "data leak" vulnerability – which DirectDefense says "is nearly impossible to stop […] with the architecture [Carbon Black] devised – is in fact a feature that only Cb Response customers benefit from. The company also notes that, not only is the option off by default, but it also includes "many

options to ensure privacy, and a detailed warning before enabling."

DirectDefense also claims to have downloaded some of the files supposedly uploaded by Cb Response, and that their analysis led to identifying data pertaining to specific companies, including a streaming company (AWS IAM credentials, Slack API keys, Google Play keys, Apple Store ID), a social media company (hardcoded AWS and Azure keys, along with internal proprietary information, such as usernames and passwords), and a financial services company (shared AWS keys that granted access to customer financial data, trade secrets).

While the report alleges that Carbon Black's product is the data leaker, the actual issue resides with VirusTotal, which provides access to the analyzed files to those willing to pay. There are numerous other security products that upload files to VirusTotal, and DirectDefense also notes that this might be the case, and even points out that the cloud-based multiscanner is spreading these files further.

"Cloud-based multiscanners operate as for-profit businesses. They survive by charging for access to advanced tools sold to malware analysts, governments, corporate security teams, security companies, and basically whomever is willing to pay. Access to these tools includes access to the files submitted to the multiscanner corpus," DirectDefense notes.

Some experts following the story have taken a similar route, denouncing the report for inaccurately presenting Carbon Black's product as being at fault. Some even called the report down right biased, based on DirectDefense's association with Cylance, a competitor of Carbon Black. Recently named Solutions Partner of

the Year by Cylance and using hyperbole-based comments in their report, DirectDefense can be easily accused of intentional smearing.

Security expert Adrian Sanabria, co-founder of Savage Security, calls the report "bullshit" and DirectDefense "opens itself up to criticism and closer scrutiny" by picking on Carbon Black. The reason, he says, is that "dozens of other security vendors either have an option to automatically submit binaries (yes, whole binaries, not just the hash) to VirusTotal or do it without the customers' knowledge altogether."

Martin Zinaich, information security officer for the City of Tampa, also points out that the report is biased and that DirectDefense had a hidden agenda when writing it: "DirectDefense poorly executed their discovery disclosure and no doubt did so purposefully. Thereby continuing the role of valued solutions partner."

However, he also notes that many security professionals would turn to sharing information with VirusTotal without a second thought: "Neither the use of VirusTotal nor the [Carbon Black] disclaimer would make even the most hypersensitive InfoSec professional contemplate data leaking to other users of said service. Moreover, it would hardly cross the mind of a typical endpoint administrator."

"How many other vendors are leveraging a multiscanner with API access? DirectDefense's clumsy disclosure should not take away from what they did in fact discover," Zinaich points out.

In a post denouncing the manner in which some news outlets were quick to report on DirectDefense's story without waiting for Carbon Black's response, investigative journalist Brian Krebs too points out that the real issue is the use of VirusTotal within corporate networks

without fully understanding what it involves.

“If DirectDefense’s report helped some security people better grasp the risks of oversharing with multiscanners like VirusTotal, that’s a plus,” Krebs notes. However, he also says that “overblown research reports” such as this one should not be taken for granted, especially if the company that discovered the so-called issue didn’t even bother to contact the affected vendor before going public.

So, is the automatic (or manual) upload of files to VirusTotal bad practice? Yes and no. It is both a feature and a risk, depending on how it is used and on how well security teams and admins understand what it involves. On the one hand, sending a file to a multiscanner clearly brings a great deal of benefits by increasing the chances of discovering malicious intent. On the other hand, however, if used irresponsibly, this option could result in data leaks, potentially doing more harm than good. Thus, fully understanding the risks associated with the practice should help companies improve their security stance.

**Related**: VirusTotal Policy Change Rocks Anti-Malware Industry

**Related**: Inside The Competitive Testing Battlefield of Endpoint Security

Previous Columns by Ionut Arghire: