ꓤEVERSINGLABS   Carbon Black.

Detect Advanced Threats with Intelligence on Files from Every Endpoint

EDR data enriched with file intelligence exposes malware in unknown files

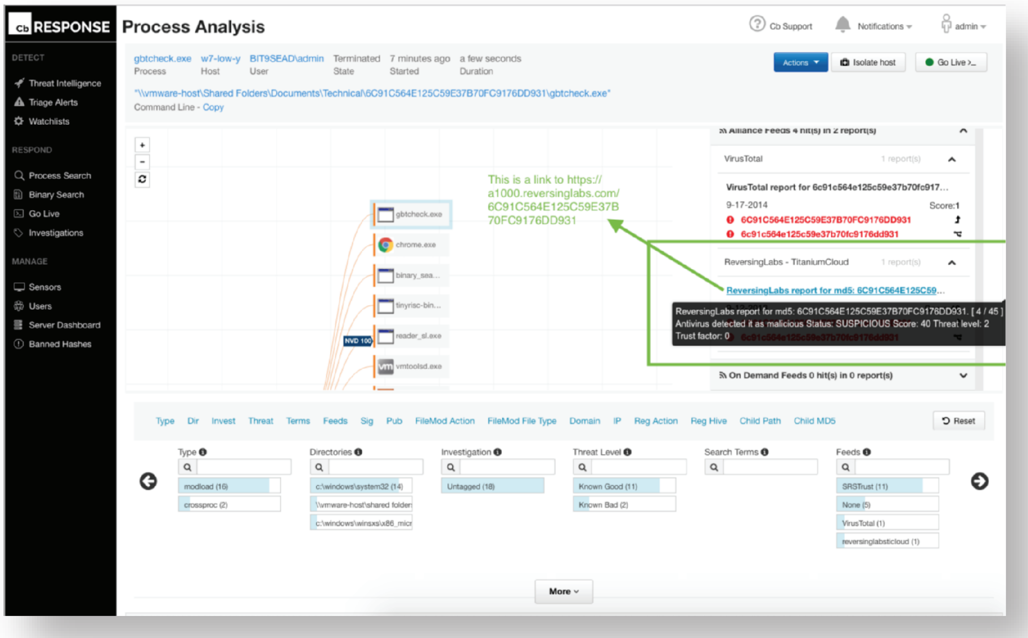
With the volume of files that SOC teams have to analyze for threats, they struggle to quickly identify and expose malware due to lack of visibility into files. ReversingLabs and Carbon Black have created an integrated solution that enriches EDR data with authoritative file intelligence across all file types, so that security teams can quickly visualize and respond to attacks.

The solution instantly displays threat classification and rich context results from RL's authoritative file reputation database of over eight billion goodware and malware files on hashes sent from Carbon Black agents that may contain malware. The solution also enables analysts to quickly pivot to the ReversingLabs Malware Analysis and Hunting platform from the Carbon Black UI for instant malware analysis results on hashes they want to further inspect. This removes time consuming steps to identify and respond to malware as well as identifying functionally similar files and malware families.

The A1000 also supports development, testing and deployment of YARA rules so Carbon Black agents can identify malware the next time it shows up. This frees security teams to focus on the highest severity threats RL has displayed in the UI so they don't have to spend time investigating something that's now known goodware or known malware.

Solution Highlights

- **Enriches Carbon Black EDR data with critical threat data to quickly classify and identify malware at enterprise scale.**
- **Submit unknown files directly from the Carbon Black UI to the ReversingLabs A1000 Malware Analysis and Hunting platform to identify malware and develop actionable intelligence.**
- **Access detailed intelligence and reputation data on all files with 1-click access to the ReversingLabs A1000 Malware Analysis and Hunting platform.**



Process Analysis

gbtcheck.exe Process | w7-low-y Host | BIT9SEAD\admin User | Terminated State | 7 minutes ago Started | a few seconds Duration

"\\vmware-host\Shared Folders\Documents\Technical\6C91C564E125C59E37B70FC9176DD931\gbtcheck.exe"
Command Line - Copy

This is a link to https://a1000.reversinglabs.com/6C91C564E125C59E37B70FC9176DD931

Alliance Feeds 4 hit(s) in 2 report(s)

VirusTotal 1 report(s)

VirusTotal report for 6c91c564e125c59e37b70fc917...
9-17-2014 Score:1
6C91C564E125C59E37B70FC9176DD931
6c91c564e125c59e37b70fc9176dd931

ReversingLabs - TitaniumCloud 1 report(s)

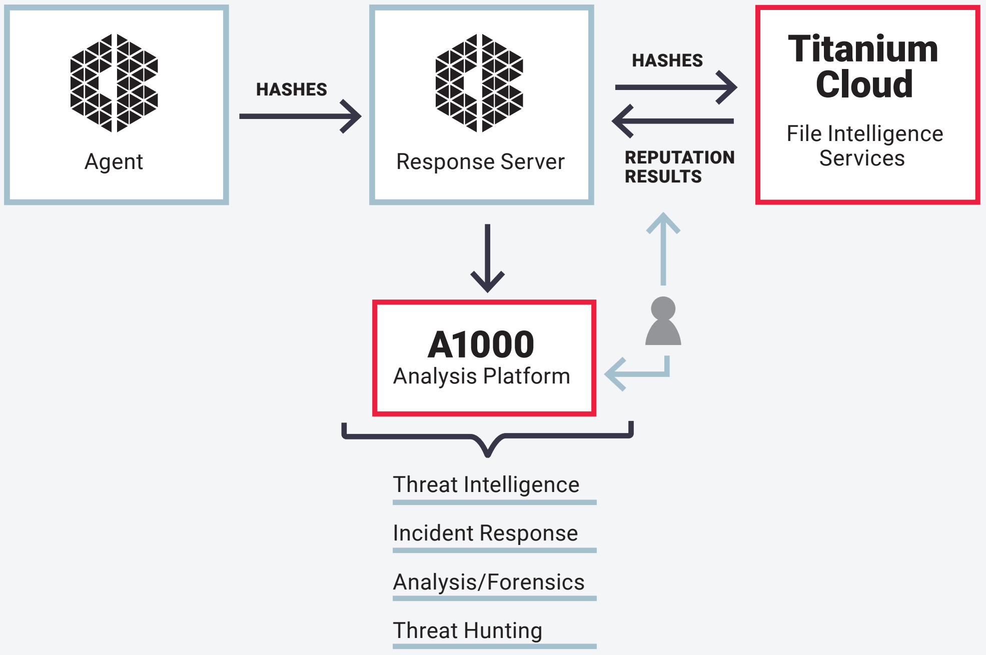
ReversingLabs report for md5: 6C91C564E125C59...

ReversingLabs report for md5: 6C91C564E125C59E37B70FC9176DD931. [4 / 45] Antivirus detected it as malicious Status: SUSPICIOUS Score: 40 Threat level: 2 Trust factor: 0

On Demand Feeds 0 hit(s) in 0 report(s)

Type: modload (16), crossproc (2)
Directories: c:\windows\system32 (14), \\vmware-host\shared folder, c:\windows\winsxs\x86_micr
Investigation: Untagged (18)
Threat Level: Known Good (11), Known Bad (2)
Search Terms
Feeds: SRSTrust (11), None (5), VirusTotal (1), reversinglabsticloud (1)

ReversingLabs Carbon Black Architectural Workflow



How It Works

The joint integration gives security analysts the ability to pass hashes from Carbon Black to ReversingLabs for analysis to lookup critical threat data which is then sent to SIEM and analytics platforms for correlation and analysis to improve threat intelligence and accelerate event detection and response.

- Carbon Black endpoint agents send hashes of all suspicious files related to a potential attack to the Carbon Black Response Server.
- Hashes are passed from the Carbon Black Response Server to TitaniumCloud for reputation intelligence results within milliseconds. The results are returned to the Carbon Black Response Server, which provides the file intelligence to analysts right in the UI.
- Detailed analysis information on all files are available with 1-click to the A1000 UI. If the hash comes back as high risk or known but not detected by AV for example, then security analysts may upload them from the UI into an onsite ReversingLabs A1000 with 1-click for automated deeper analysis to quickly expose malware and display file characteristics and threat indicators.
- The A1000 extracts and classifies thousands of indicators on each file and supports YARA rules development, testing and deployment so that custom rules can be created for newly discovered malware and pushed out across security tools to quickly identify malware the next time it shows up.

Solution Components

The solution is comprised of the following products:

- ReversingLabs TitaniumCloud File Reputation TCA-0101
- ReversingLabs A1000 Malware Analysis Platform
- Carbon Black:
    - CB Response (EDR)
    - CB Defense (NGAV + EDR)
    - CB Protection (App Control)
    - CB Predictive Security Cloud (PSC)