BigFix and Carbon Black Integration

Tom Sikma
Motorola Solutions

Overview

Phase 1 - Cross Application Visibility

BigFix reporting of Carbon Black Response/Protect installations

Phase 2 - Securing the Endpoint

- BigFix Tamper Protection
  - Insider Threat - The “BESKiller”
- BigFix CB Protect Connector
  - Banned File Cleanup

Phase 1 - Cross Application Visibility

The ability to use BigFix to check CB Protect and Response installations provides valuable information on the endpoint for users with varying management capabilities.

- Report on the agent version and ensure that the service is installed/running
- Verify the CB management server and what policy is applied on the endpoint
- Installation configuration of both CB products
- Validation that machines are able to communicate to respective environments
    - Vlookup with CB server to see installation differences (labs, network changes, etc)

Phase 2 - Securing the Endpoint

The “BESKiller.exe” - BigFix Agent Tamper Protection

Internal Employee trying to avoid corporate mandated deployment

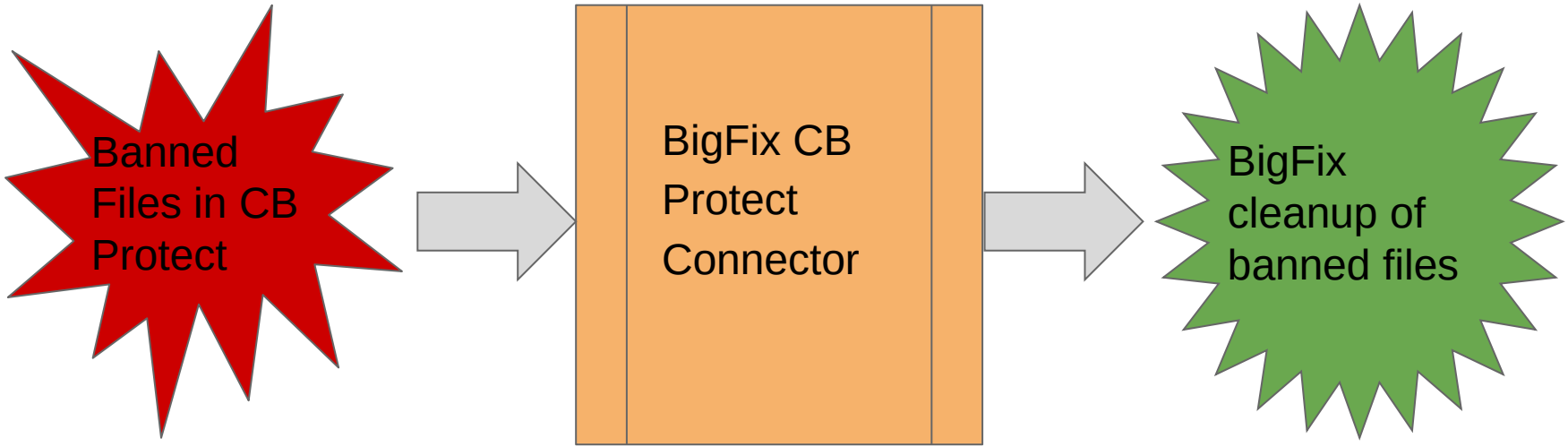
Created an application that stopped the BigFix agent from running

Detected users behavior with internal tools that detected process manipulation (now can be detected with a CB Response Watchlist)

Detected by IT, reported to HR for policy violation and mandate avoidance, no longer with the company

Phase 2 - Securing the Endpoint

The BigFix CB Protect Connector provides integration between the two product to better secure the endpoint



Banned Files in CB Protect

There are different ways that files are banned

CB Protect Event Rules - Files seen as malicious by CB Protect auto banned

Publisher Bans - Software publishers of Adware/Malware/Torrents/etc

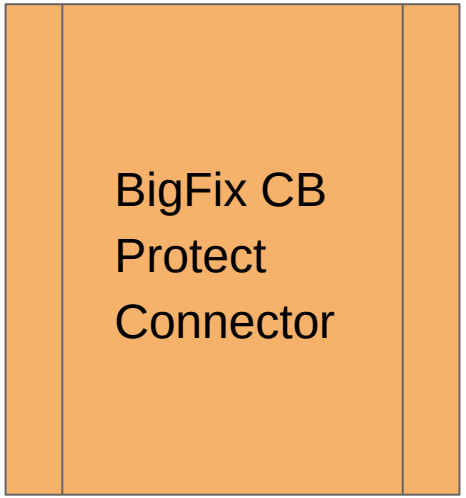
Intelligence Feeds - Proactive ban of file hashes identified through numerous feeds

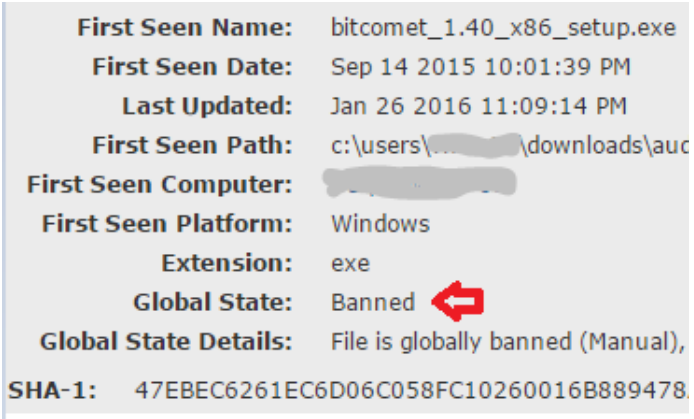
“Other” Sources - CB Response, Licensing Violation, etc

BigFix CB Protect Connector

Service is installed on the CB Protect Server that takes the banned file information and creates a BigFix task for each file hash.

Regular Interval Checks so new banned files are added to BigFix automatically





Automated job creation with proper relevance and action script to remove the banned file

BigFix cleanup of banned files

Name	Site	Applicable Com...
Banned File - sha1=47d03b338dc0a361254b1e9086f709849faa4710	Carbon Black	33 / 24,595
Banned File - sha1=47ebec6261ec6d06c058fc10260016b889478aa5	Carbon Black	1 / 24,595
Banned File - sha1=47f389a36be8d2ce6bc397df88ba79fb2ebfaeb1	Carbon Black	1 / 24,595

As part of the configuration of the connector all banned files appear in their own custom site.

Relevance and Action Script are automatically generated


```
Script Type BigFix Action Script

                if ((exists file "bitcomet_1.40_x86_setup.exe" whose (sha1 of it as lowercase
= "47ebec6261ec6d06c058fc10260016b889478aa5" as lowercase) of folders "c:\users\
\downloads\audiobooks"))
                        delete "c:\users\    \downloads\audiobooks\bitcomet_1.40_x86_setup.exe"
                endif
```