Google Santa - Blacklist Apps on macOS

GitHub Site : https://github.com/google/santa

<u>Santa according to Google:</u>

Santa is a project of Google's Macintosh Operations Team.

Santa is a binary whitelisting/blacklisting system for macOS. It consists of a kernel extension that monitors for executions, a userland daemon that makes execution decisions based on the contents of a SQLite database, a GUI agent that notifies the user in case of a block decision and a command-line utility for managing the system and synchronizing the database with a server.

<u>Using Santa to Blacklist Apps on macOS:</u>

- Push Santa as an internal app on mac
  Download dmg file from : https://github.com/google/santa/releases

- Push & Execute the below script with product provisioning on mac to Blacklist the apps

  <u>Product provisioning details:</u>

  - File : blacklistapps.sh
  - Download Location : /ws1/scripts
  - Run command : "sudo chmod +x /ws1/scripts/blacklistapps.sh; sudo /bin/bash/blacklistapps.sh"

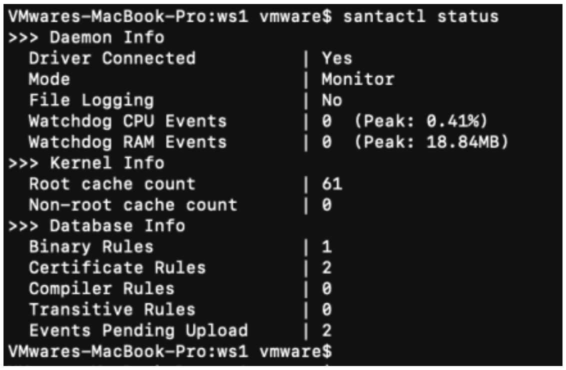
  <u>Script content:</u>

```
#!/bin/bash

# Add the rules to block app
# example : sudo /usr/local/bin/santactl rule --blacklist --path /Applications/<Name_of_app>.app

        sudo /usr/local/bin/santactl rule --blacklist --path /Applications/uTorrent.app
        sudo /usr/local/bin/santactl rule --blacklist --path /Applications/BitTorrent.app

# Reload Service
        sudo /sbin/kextunload -b com.google.santa-driver;
        sudo launchctl unload /Library/LaunchDaemons/com.google.santad.plist;
        sudo launchctl load /Library/LaunchDaemons/com.google.santad.plist;
        sudo /sbin/kextload -b com.google.santa-driver;

#cleanup files
        sudo rm -rf /ws1/scripts/blacklistapps*
```

<u>Command to validate on macOS:</u>

- To check the status of Santa

```
# santactl status
```



```
VMwares-MacBook-Pro:ws1 vmware$ santactl status
>>> Daemon Info
  Driver Connected          | Yes
  Mode                      | Monitor
  File Logging              | No
  Watchdog CPU Events       | 0  (Peak: 0.41%)
  Watchdog RAM Events       | 0  (Peak: 18.84MB)
>>> Kernel Info
  Root cache count          | 61
  Non-root cache count      | 0
>>> Database Info
  Binary Rules              | 1
  Certificate Rules         | 2
  Compiler Rules            | 0
  Transitive Rules          | 0
  Events Pending Upload     | 2
VMwares-MacBook-Pro:ws1 vmware$
```

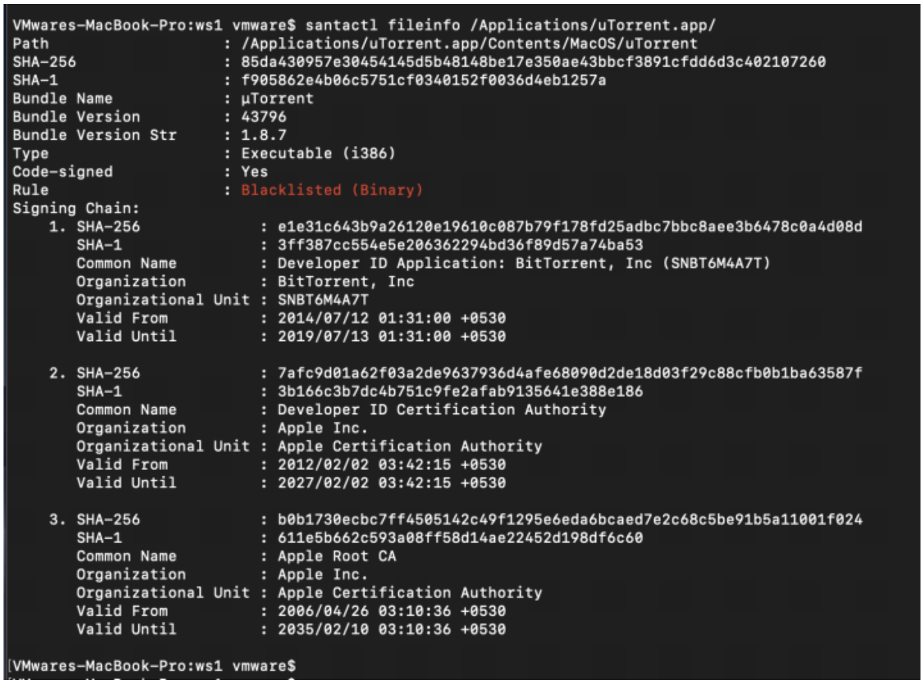
-> Driver Connected should be "Yes"
-> Mode default is "Monitor"

If driver connected is "No" then use the below command to reload service

```
        sudo /sbin/kextunload -b com.google.santa-driver;
        sudo launchctl unload /Library/LaunchDaemons/com.google.santad.plist;
        sudo launchctl load /Library/LaunchDaemons/com.google.santad.plist;
        sudo /sbin/kextload -b com.google.santa-driver;
```

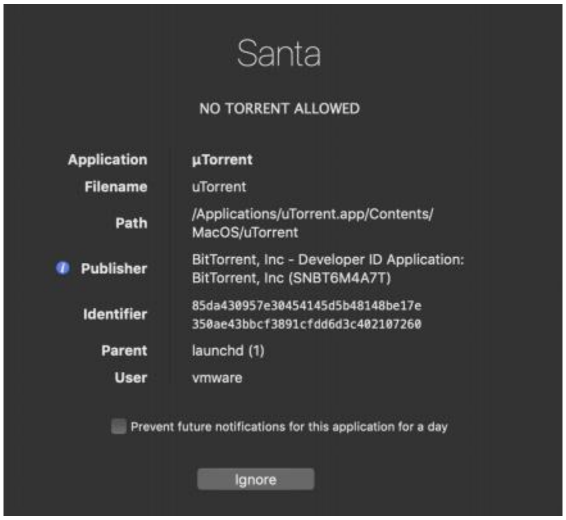
- To check is application is Blacklisted

```
# santactl fileinfo /Applications/<Name_of_APP>.app/
```



```
VMwares-MacBook-Pro:ws1 vmware$ santactl fileinfo /Applications/uTorrent.app/
Path                     : /Applications/uTorrent.app/Contents/MacOS/uTorrent
SHA-256                  : 85da430957e30454145d5b48148be17e350ae43bbcf3891cfdd6d3c402107260
SHA-1                    : f905862e4b06c5751cf0340152f0036d4eb1257a
Bundle Name              : µTorrent
Bundle Version           : 43796
Bundle Version Str       : 1.8.7
Type                     : Executable (i386)
Code-signed              : Yes
Rule                     : Blacklisted (Binary)
Signing Chain:
    1. SHA-256             : e1e31c643b9a26120e19610c087b79f178fd25adbc7bbc8aee3b6478c0a4d08d
       SHA-1               : 3ff387cc554e5e206362294bd36f89d57a74ba53
       Common Name         : Developer ID Application: BitTorrent, Inc (SNBT6M4A7T)
       Organization        : BitTorrent, Inc
       Organizational Unit : SNBT6M4A7T
       Valid From          : 2014/07/12 01:31:00 +0530
       Valid Until         : 2019/07/13 01:31:00 +0530

    2. SHA-256             : 7afc9d01a62f03a2de9637936d4afe68090d2de18d03f29c88cfb0b1ba63587f
       SHA-1               : 3b166c3b7dc4b751c9fe2afab9135641e388e186
       Common Name         : Developer ID Certification Authority
       Organization        : Apple Inc.
       Organizational Unit : Apple Certification Authority
       Valid From          : 2012/02/02 03:42:15 +0530
       Valid Until         : 2027/02/02 03:42:15 +0530

    3. SHA-256             : b0b1730ecbc7ff4505142c49f1295e6eda6bcaed7e2c68c5be91b5a11001f024
       SHA-1               : 611e5b662c593a08ff58d14ae22452d198df6c60
       Common Name         : Apple Root CA
       Organization        : Apple Inc.
       Organizational Unit : Apple Certification Authority
       Valid From          : 2006/04/26 03:10:36 +0530
       Valid Until         : 2035/02/10 03:10:36 +0530

[VMwares-MacBook-Pro:ws1 vmware$
```

Behavior when launching the applications:

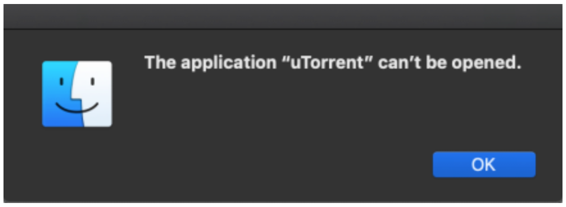


Santa

NO TORRENT ALLOWED

Application	**µTorrent**
Filename	uTorrent
Path	/Applications/uTorrent.app/Contents/MacOS/uTorrent
Publisher	BitTorrent, Inc - Developer ID Application: BitTorrent, Inc (SNBT6M4A7T)
Identifier	85da430957e30454145d5b48148be17e350ae43bbcf3891cfdd6d3c402107260
Parent	launchd (1)
User	vmware

☐ Prevent future notifications for this application for a day



The application “uTorrent” can’t be opened.