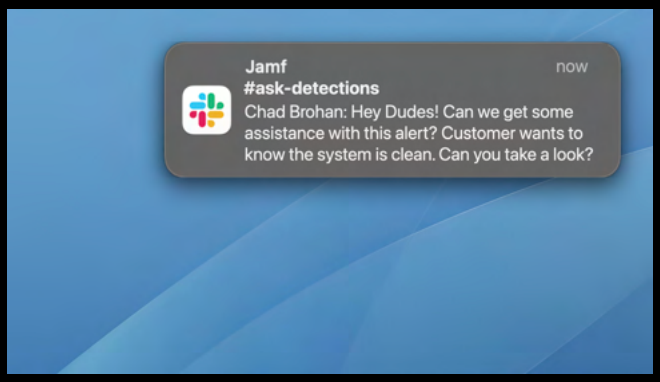
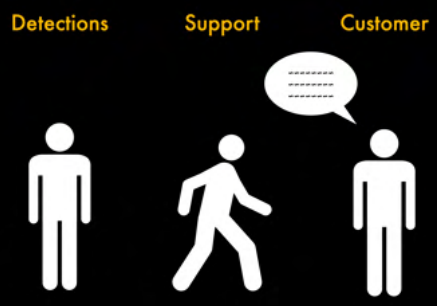
jamf
THREAT LABS

Stuart Ashenbrenner
@stuartjash

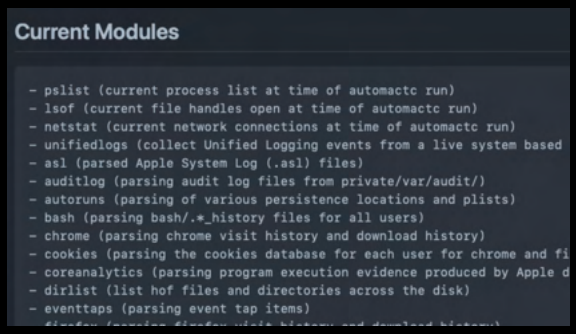
Matt Benyo
@mattbenyo





In our work writing detections for Jamf Protect, we encountered situations where less experienced teams would receive one of our alerts and needed extra help and assurance to confirm whether the system had been compromised and how to assess the impact. These conversations would often get relayed through support, and in many cases, by the time we got involved, too much time had passed to gather fresh and relevant data from the affected endpoint to make definitive assessments.

So we went looking for a collection tool that we could get into the hands of our customers for these situations.



We started looking at existing IR tools. We could one called Automactc from CrowdStrike, however, this was written in python. We definitely drew some inspiration from the modules they were running. There was also Venator, written by Richie Cyrus, but it hadn't been updated in some time.

Ideally, what we were looking for was something light weight that could be installed on endpoints and be on standby for an automatic on-demand execution and collection at the moment our detections were being fired. This would minimize unnecessary collection and accumulation of data, but would also ensure the freshest possible snapshot of the system for incident response and investigation.

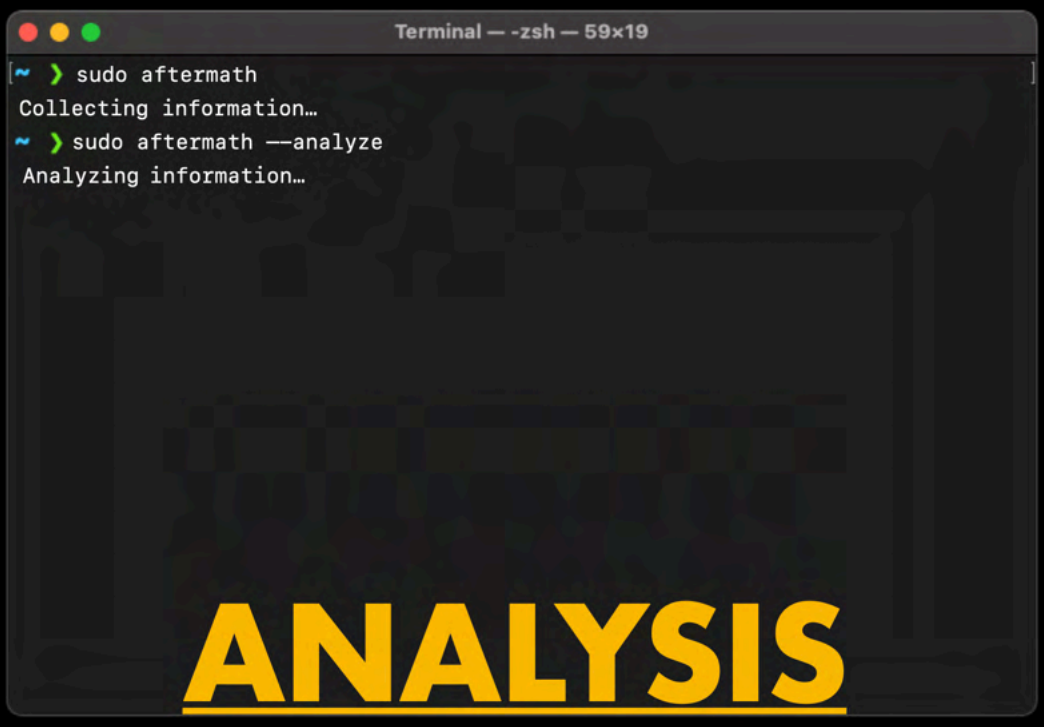
Written in Swift

- It's fast
- It's maintainable
- It's native
- It gives us the most access to built in APIs to allow us to really customize exactly the data we wanted to collect and analyze

So we created Aftermath.

Aftermath is a Swift-based, open sourced, IR framework designed to capture all of the artifacts that are necessary to a proper investigation, then to analyze the relevant data to determine the threat vector used, as well as how we can best remediate the threat.


Terminal — -zsh — 59×19
~ ❯ sudo aftermath
Collecting information…
COLLECTION


Terminal — -zsh — 59×19
~ ❯ sudo aftermath
Collecting information…
~ ❯ sudo aftermath --analyze
Analyzing information…
ANALYSIS

Collection:

- Contains about a dozen modules which are broken into their own classes

These modules include:

- Persistence
- Processes
- Unified Logs
- Browser Data
- System Recon
- Artifacts

kTCCServiceLiverpool	net.shinyfrog.bear	0	2	5	1
kTCCServiceMicrophone	com.apple.garageband10	0	2	2	1
kTCCServiceMicrophone	com.apple.iWork.Keynote	0	0	2	1
kTCCServiceMicrophone	com.figure53.QLab.4	0	2	2	1
kTCCServiceMicrophone	com.google.Chrome	0	2	2	1
kTCCServiceMicrophone	com.tinyspeck.slackmacgap	0	2	2	1
kTCCServiceMicrophone	org.mozilla.firefox	0	2	2	1
kTCCServiceMicrophone	us.zoom.xos	0	2	4	1
kTCCServicePhotos	com.apple.dt.Xcode	0	2	2	1
kTCCServicePhotos	com.apple.iMovieApp	0	2	2	1
kTCCServiceReminders	com.apple.dt.Xcode	0	2	2	1
kTCCServiceReminders	com.culturedcode.ThingsMac	0	2	2	1
kTCCServiceReminders	com.sublimetext.4	0	2	2	1
kTCCServiceSystemPoli...	/Users/stuartashenbrenner/Library/Developer/Xcode...	1	2	2	1
kTCCServiceSystemPoli...	com.apple.dt.Xcode	0	2	2	1
kTCCServiceSystemPoli...	com.druva.inSync	0	2	2	1
kTCCServiceSystemPoli...	com.github.atom	0	2	2	
kTCCServiceSystemPoli...	com.googlecode.iterm2	0	2	2	
kTCCServiceSystemPoli...	com.microsoft.VSCode	0	2	2	1

- We collect the user’s TCC database
- Allows us to see what services requested or have been granted access

2022-09-10T10:32:36	https://www.patreon.com/objective_see
2022-09-10T10:30:13	https://www.google.com/search?q=how+to+thank+objecti
2022-09-10T10:06:38	https://objective-see.com/products.html
2022-09-10T10:05:22	https://www.google.com/search?q=HELP+IM+INFECTED
2022-09-10T09:10:40	https://pondzi.com/downloads.html

We collect relevant browser information like history and downloads. This could allow us to potentially see where an infection originated from.

Here we can see an order of events, and even where a user noticed they were infected.

We could then visit the malicious site and see it's a common PUP (Potentially Unwanted Program) called Pondzi.

SYSTEM RECON

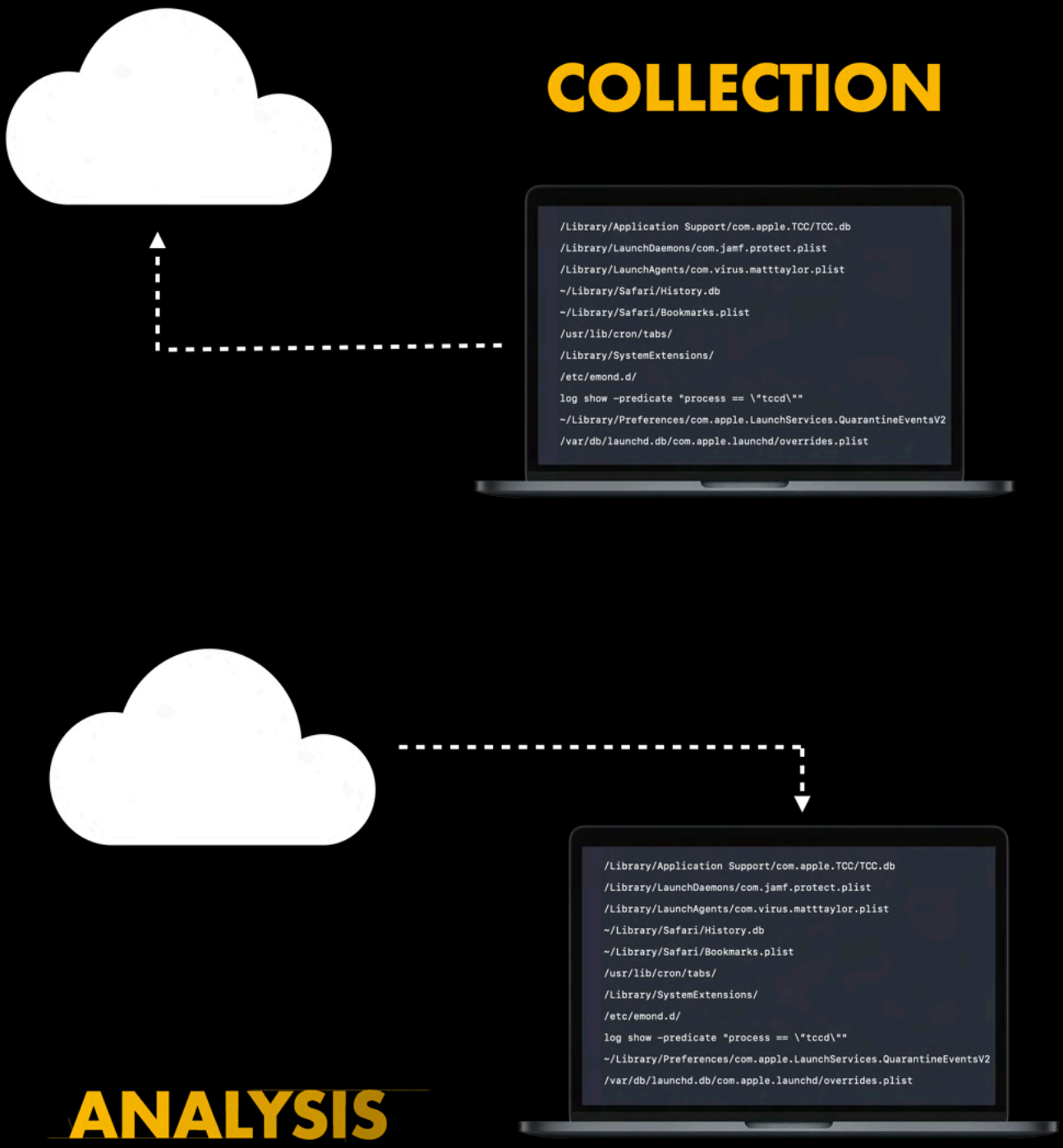
```
HostName: hexleys-mac-mini.local
UserName: root
FullName: System Administrator
System Version: Version 12.4 (Build 21F79)
XProtect Version: 2162
XProtect Remediator Version: 74
MRT Version: 1.93
```

This produces a text file which tells administrators and security professionals information like:

- XProtect Version
- MRT Version
- XProtect Remediator Version
- Firewall Status
- Screen Sharing Status
- Installed apps
- Install history
- Environment variables

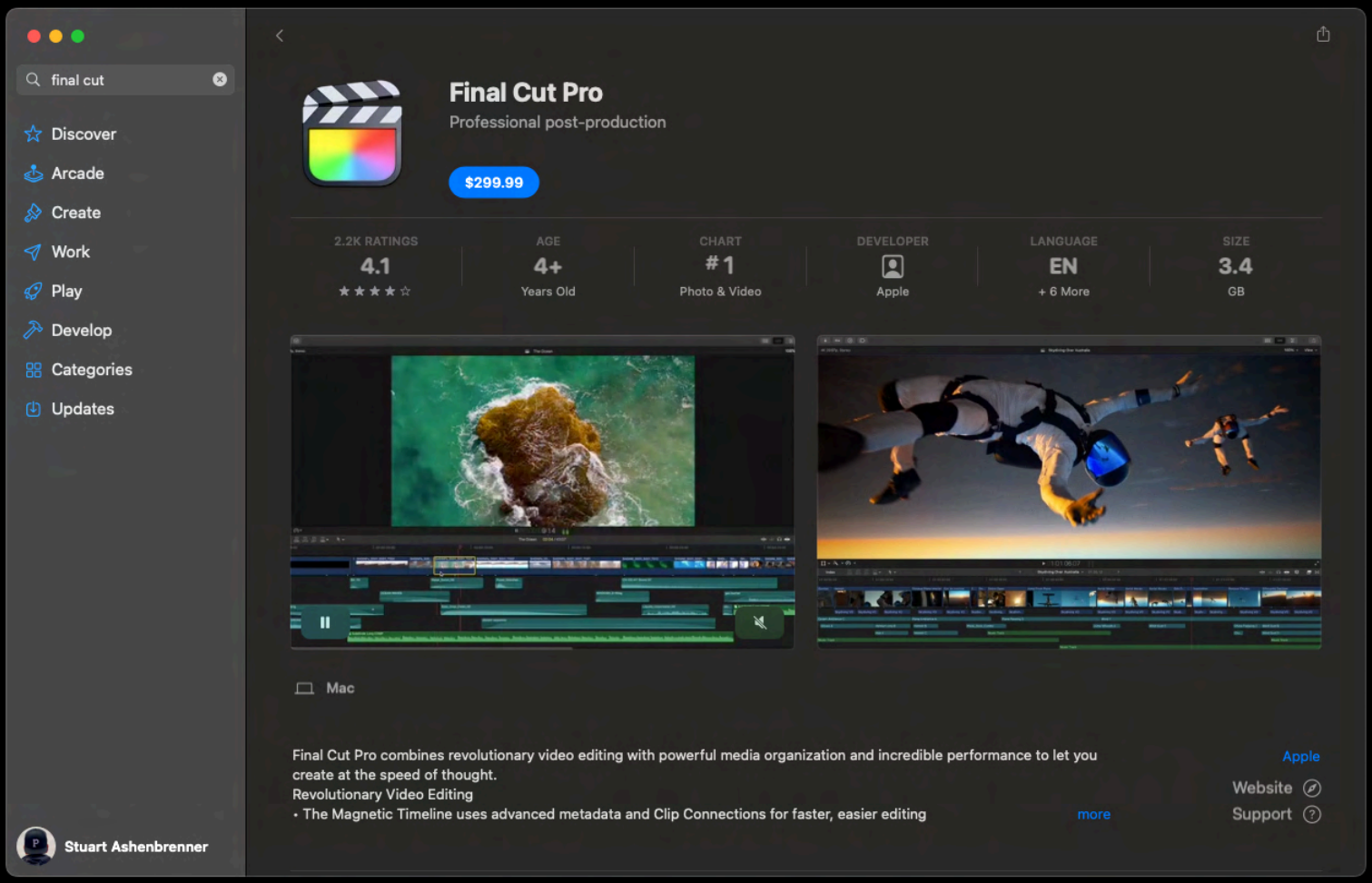
COLLECTION

ANALYSIS

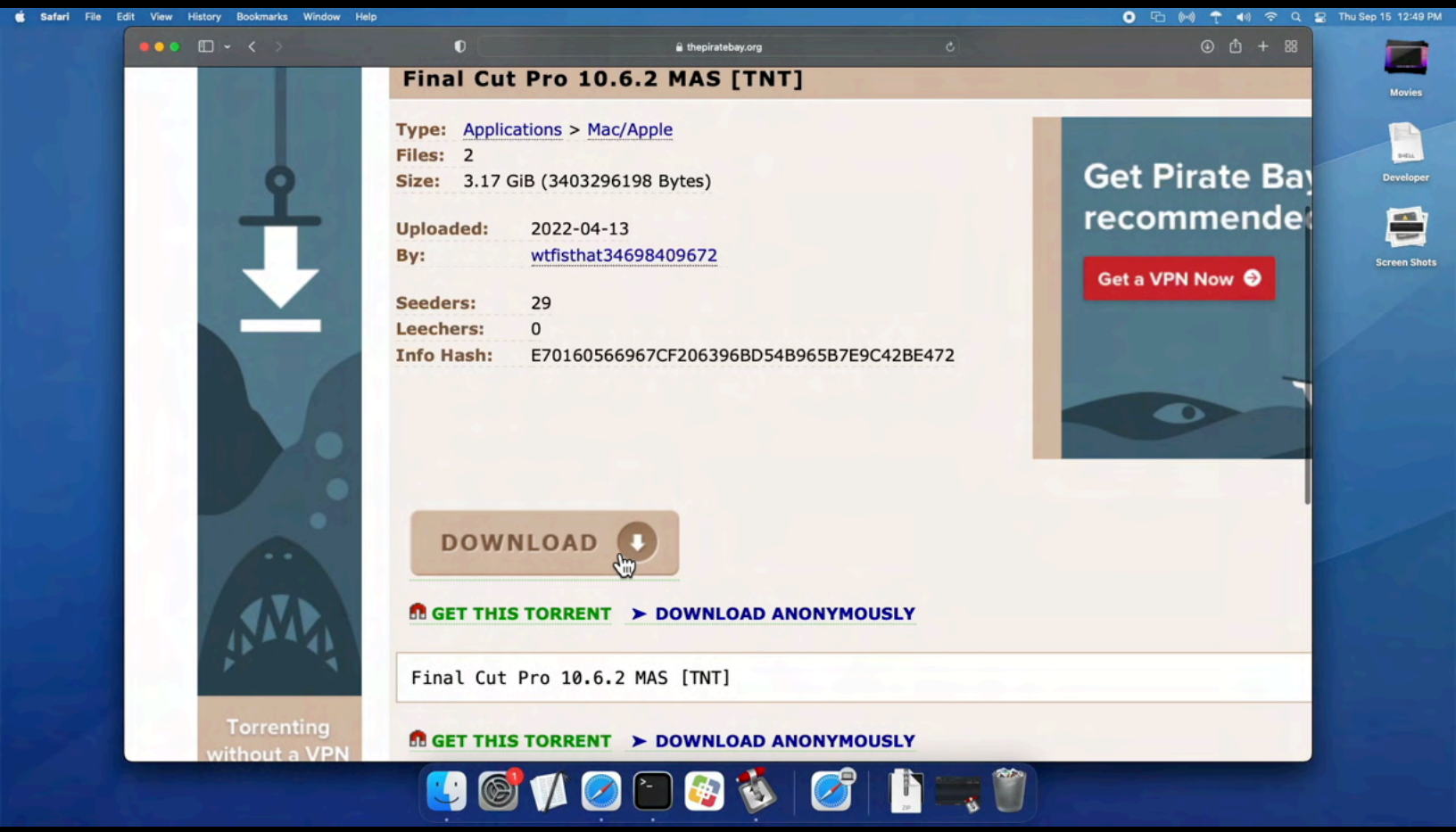


So once we have all of this data, both in raw and lightly parsed form, we pivot to analysis, which is typically performed on a different machine than the victims.

In the end, we get a storyline that tells us the entire story of the malware. So what is that story?



If we were a user, and say, we wanted to download FinalCut Pro to make some overproduced TikTok vids. But at the same time, we don't want to drop the $300 it costs to buy a license, so instead we elect to pirate it. Not an uncommon thing to do, and also not uncommon to get a bad case of malware while you're at it .

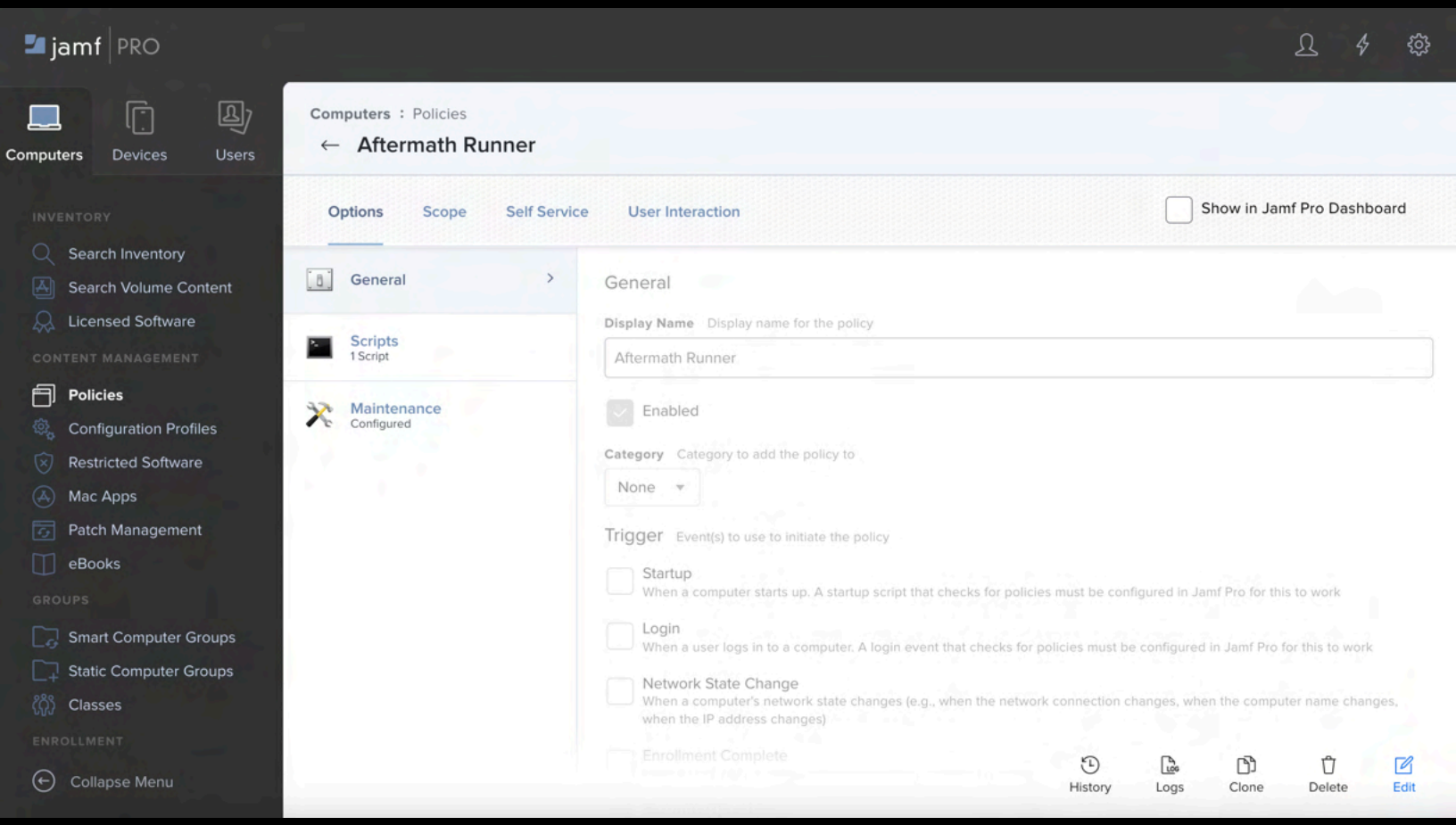


So we navigate over to PirateBay like it's 2010 and find a slick, cracked version of it. We download it, mount the disk image it resides in, then install the application.

What we didn't realize when we downloaded this version of Final Cut is that when we launch final cut, we are also running a crypto miner in the background. And it's a sneaky one. When we check out Activity Monitor, the miner stops.

So eventually we get suspicious or maybe we even triggered an alert in our detections. So it's time to use aftermath to get to the bottom of what's going on on our system.

So eventually we get suspicious or maybe we even triggered an alert in our detections. So it's time to use aftermath to get to the bottom of what's going on on our system.

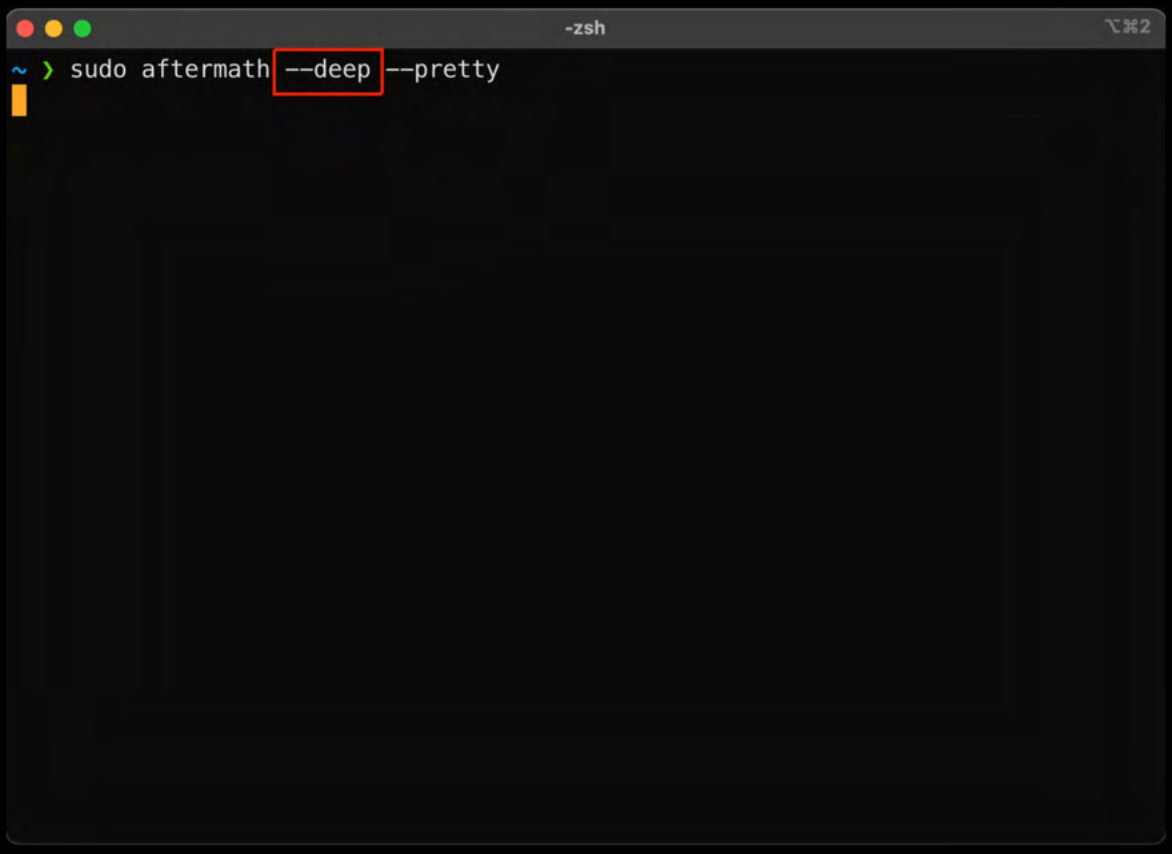


We can either do this straight from the command line, or via a policy from your MDM

If you run it from a terminal, need FDA

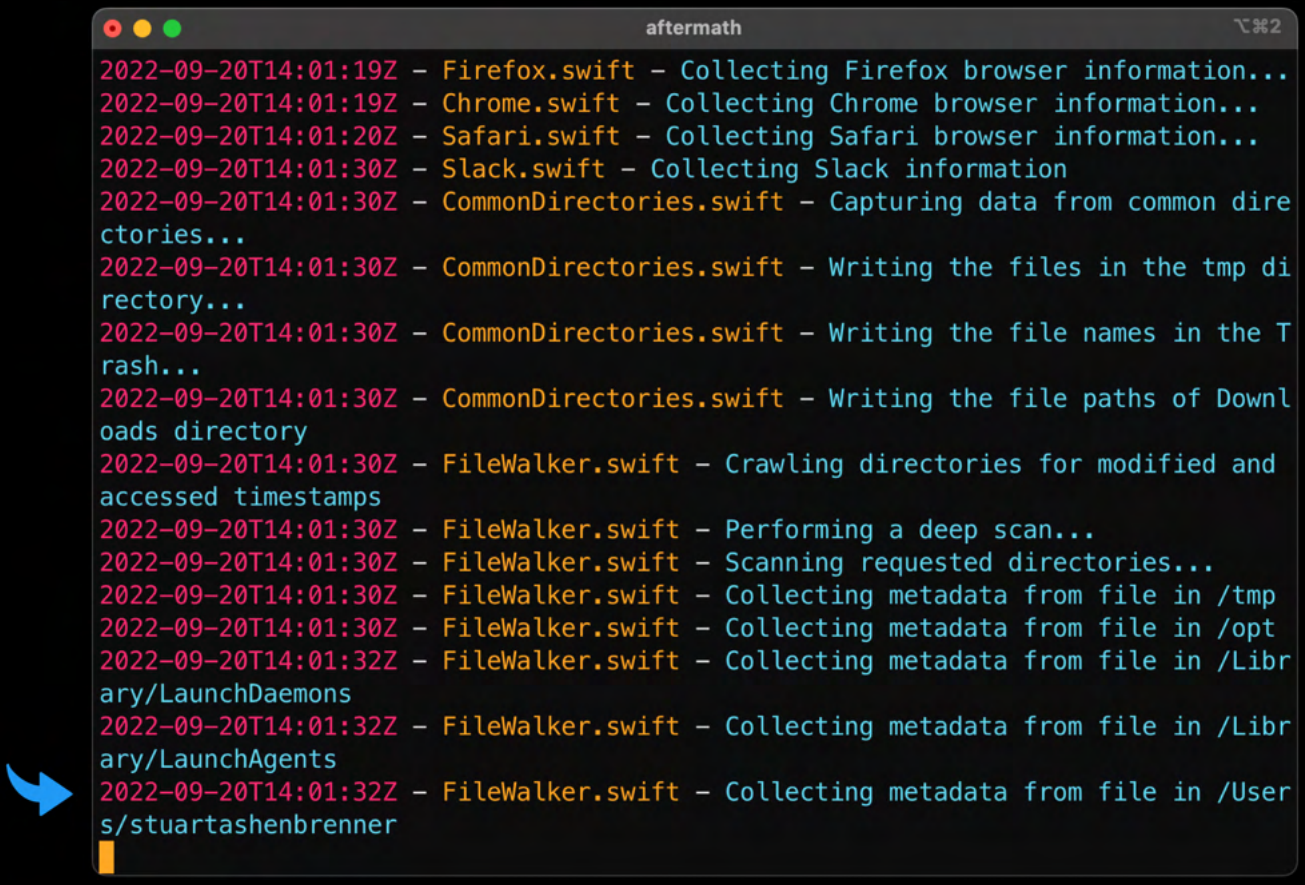
The advantage of triggering via MDM is
Runs with MDM priv

Brief aside demo, to show how these pieces fit together. Can work with different stacks



In our case, we ran it from the command line, you can scan the user's entire home directory collecting the timestamp metadata on each file as opposed to just directories that are more commonly associated with malware. Fortunately, I have it on good authority that this miner does a lot of its nefariousness in the users's Application Support directory, whose timestamps we actually collect by default, so for the sake of this example, we can ignore the deep argument.

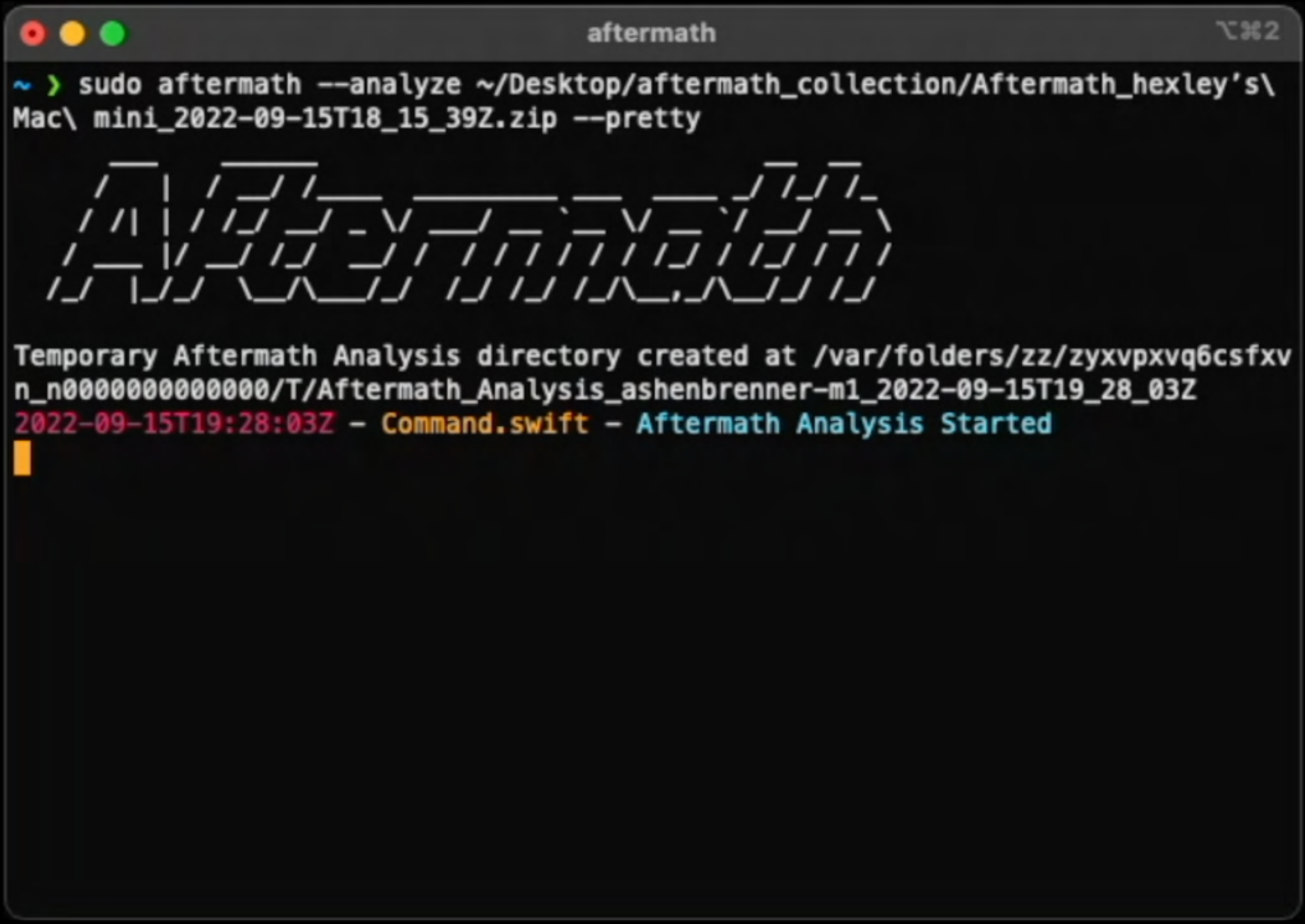
you can scan the user's entire home directory collecting the timestamp metadata on each file as opposed to just directories that are more commonly associated with malware. Fortunately, I have it on good authority that this miner does a lot of its nefariousness in the users's Application Support directory, whose timestamps we actually collect by default, so for the sake of this example, we can ignore the deep argument.



You can run `--collect-dirs` and actually dump the raw contents of whichever directories you pass it. So if we wanted to actually grab all of the files from tmp and Downloads, we could. Of course, use at your discretion, because heaven forbid the user just downloaded the latest Xcode beta and has a nice 8GB file in there. Or maybe they haven't cleaned out their Downloads since 1976.

In the case that we run it directly from the Terminal, we can get a nice output of what Aftermath is doing. We can fast forward through some of this, so we can get to what I think is the cool part. Now that the collection details are on disk, let's take a look at what we collected. If we open the folder in Finder, then we can unzip that archive and dive into the data.

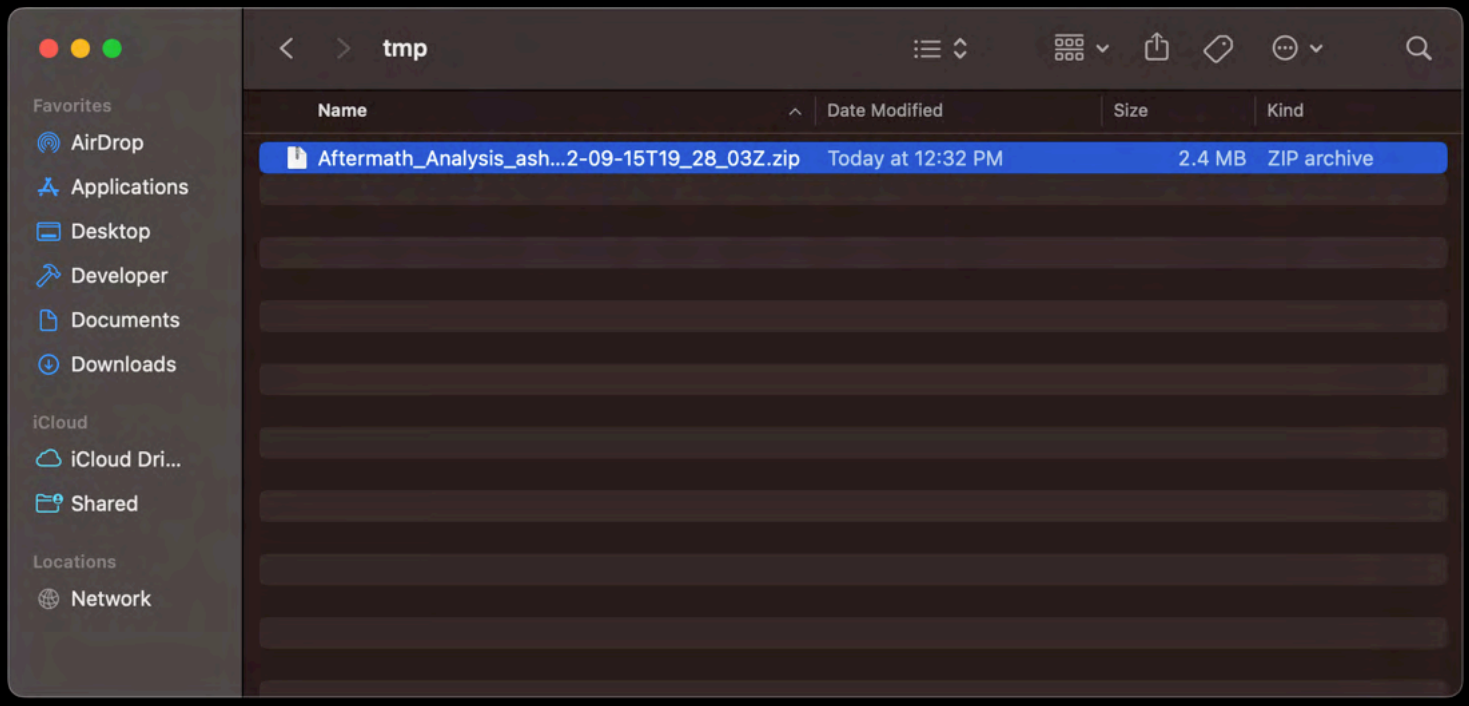

ANALYSIS

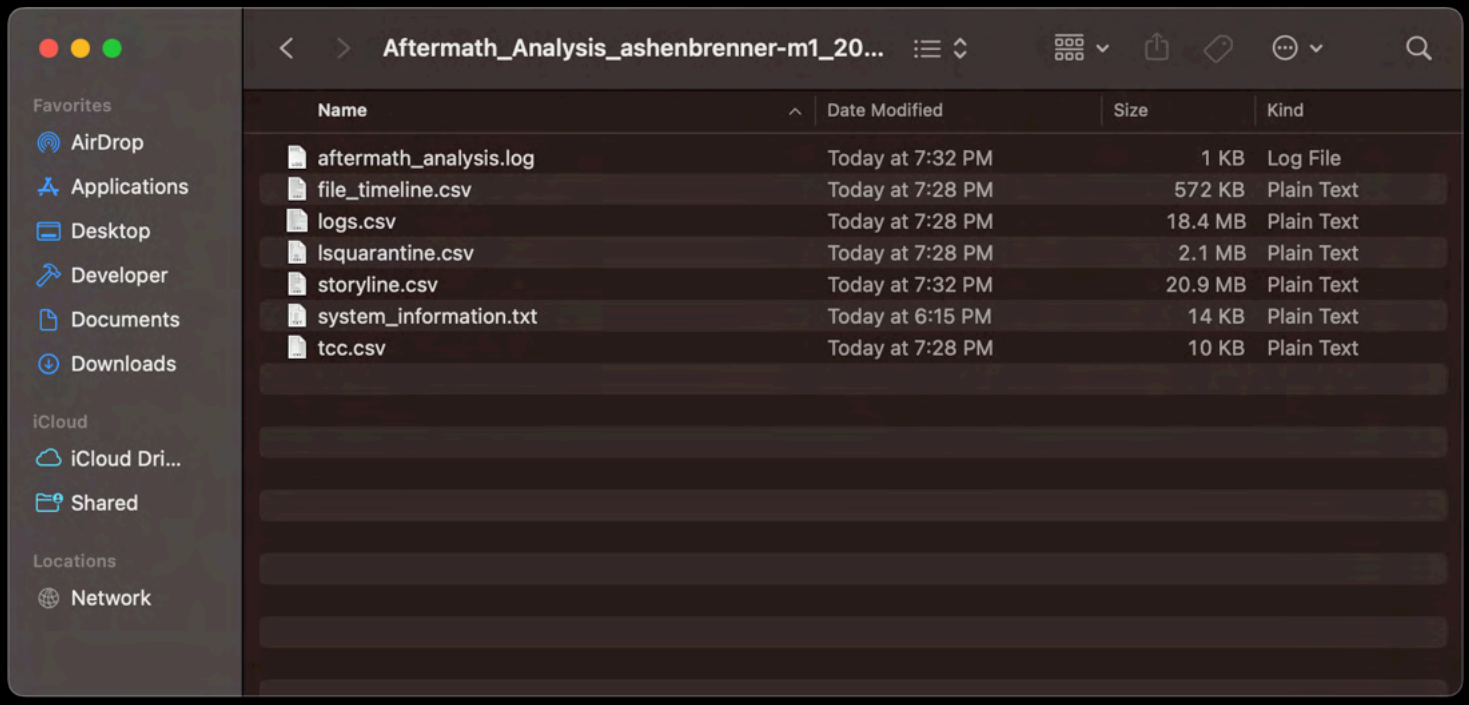

aftermath
~ ❯ sudo aftermath --analyze ~/Desktop/aftermath_collection/Aftermath_hexley's\ Mac\ mini_2022-09-15T18_15_39Z.zip --pretty
Temporary Aftermath Analysis directory created at /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/Aftermath_Analysis_ashenbrenner-m1_2022-09-15T19_28_03Z
2022-09-15T19:28:03Z - Command.swift - Aftermath Analysis Started

Standardizing Timestamps

Chrome history	2022-06-07 13:51:30
Install history	2022-06-07 13:51:30 UTC
Install log	2022-06-07T13:51:30-07
XProtectRemediator log	2022-06-07T13:51:30.381439-0700
System log	Jun 07 13:51:30
File metadata (epoch)	1654609890.475343
LSQuarantine (Mac absolute time)	676302690.475343

Where some databases and apps use Mac Absolute Time, others use epoch, and some use local time, so in this process, we standardize all of these timestamps and dump it into a few different files. We'll talk about the more in a moment.





Since we didn’t specify an output location, it lands here in tmp.

Here, we can see some different csv files - we’ll start with one of two databases - TCC. If we pop this open, we can actually see the parsed content.

TCC

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

client

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

service

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

auth value

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

auth reason

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

last modified

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	camera	denied	userConsent	2022-08-19T22:34:24Z
com.figure53.QLab.4	microphone	allowed	userConsent	2022-08-19T22:34:22Z
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

tcc

/Library/Objective-See/RansomWhere/RansomWhere	fda	allowed	servicePolicy	2021-01-16T23:50:13Z
com.objective-see.blockblock	fda	allowed	systemSet	2021-01-16T23:44:15Z
com.apple.iWork.Keynote	addressBook	allowed	userConsent	2022-09-15T21:22:05Z
org.mozilla.firefox	microphone	allowed	userConsent	2022-09-13T23:02:16Z
org.mozilla.firefox	camera	allowed	userConsent	2022-09-13T23:02:15Z
com.mothersruin.SuspiciousPackageApp	desktopFolder	denied	userConsent	2022-09-08T20:50:29Z
com.apple.PlaygroundsMac	icloud	allowed	servicePolicy	2022-08-31T17:35:03Z
com.figure53.QLab.4	**camera**	**denied**	**userConsent**	**2022-08-19T22:34:24Z**
com.figure53.QLab.4	**microphone**	**allowed**	**userConsent**	**2022-08-19T22:34:22Z**
com.github.atom	desktopFolder	allowed	userConsent	2022-08-16T18:01:36Z

So if we look at Qlab - which is used for making audio cues, we can see that the camera and mic requested access, right around the same time, and the user, me, denied the former and allowed the latter

2022-09-15T17:56:21	modified	/Users/hexley/Library/Application Support/Transmission/Transfers.plist
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/AddressBook-v22.abcddb-
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:56:08	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/.info
2022-09-15T17:56:06	modified	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:55:57	accessed	/Users/hexley/Library/Application Support/AddressBook/Metadata/3EB52CD2-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/28FEF9DE-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/
2022-09-15T17:54:59	PROCESS	68184 1 68184 0 /System/Library/PrivateFrameworks/PhotoAnalysis.framework/
2022-09-15T17:49:56	birth	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/Final Cut Pro 10.6.2 MAS
2022-09-15T17:49:56	modified	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/README.TXT
2022-09-15T17:49:40	modified	/Users/hexley/Library/Application Support/Transmission/Torrents/
2022-09-15T17:49:25	accessed	/Users/hexley/Downloads/.DS_Store
2022-09-15T17:49:22	PROCESS	68013 1 67181 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68010 1 67181 0 /System/Library/Frameworks/QuickLookUI.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68009 1 67181 0 /System/Library/Frameworks/AppKit.framework/Versions/C/
2022-09-15T17:48:58	safari_history	https://www.opera.com/gx?utm_content=2923_c25be22e-ac35-4bba-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/fp.engine?id=7bc53178-2459-465f-89da-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/Redirect.eng?
2022-09-15T17:48:55	PROCESS	67985 1 60028 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:48:52	safari_history	about:blank
2022-09-15T17:48:42	safari_history	https://thepiratebay.org/description.php?id=58223349

If we take the trojanized Final Cut example and analyze the Aftermath output in the Storyline format, the story of what happened starts to emerge.

2022-09-15T17:56:21	modified	/Users/hexley/Library/Application Support/Transmission/Transfers.plist
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/AddressBook-v22.abcddb-
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:56:08	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/.info
2022-09-15T17:56:06	modified	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:55:57	accessed	/Users/hexley/Library/Application Support/AddressBook/Metadata/3EB52CD2-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/28FEF9DE-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/
2022-09-15T17:54:59	PROCESS	68184 1 68184 0 /System/Library/PrivateFrameworks/PhotoAnalysis.framework/
2022-09-15T17:49:56	birth	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/Final Cut Pro 10.6.2 MAS
2022-09-15T17:49:56	modified	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/README.TXT
2022-09-15T17:49:40	modified	/Users/hexley/Library/Application Support/Transmission/Torrents/
2022-09-15T17:49:25	accessed	/Users/hexley/Downloads/.DS_Store
2022-09-15T17:49:22	PROCESS	68013 1 67181 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68010 1 67181 0 /System/Library/Frameworks/QuickLookUI.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68009 1 67181 0 /System/Library/Frameworks/AppKit.framework/Versions/C/
2022-09-15T17:48:58	safari_history	https://www.opera.com/gx?utm_content=2923_c25be22e-ac35-4bba-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/fp.engine?id=7bc53178-2459-465f-89da-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/Redirect.eng?
2022-09-15T17:48:55	PROCESS	67985 1 60028 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:48:52	safari_history	about:blank
2022-09-15T17:48:42	safari_history	https://thepiratebay.org/description.php?id=58223349

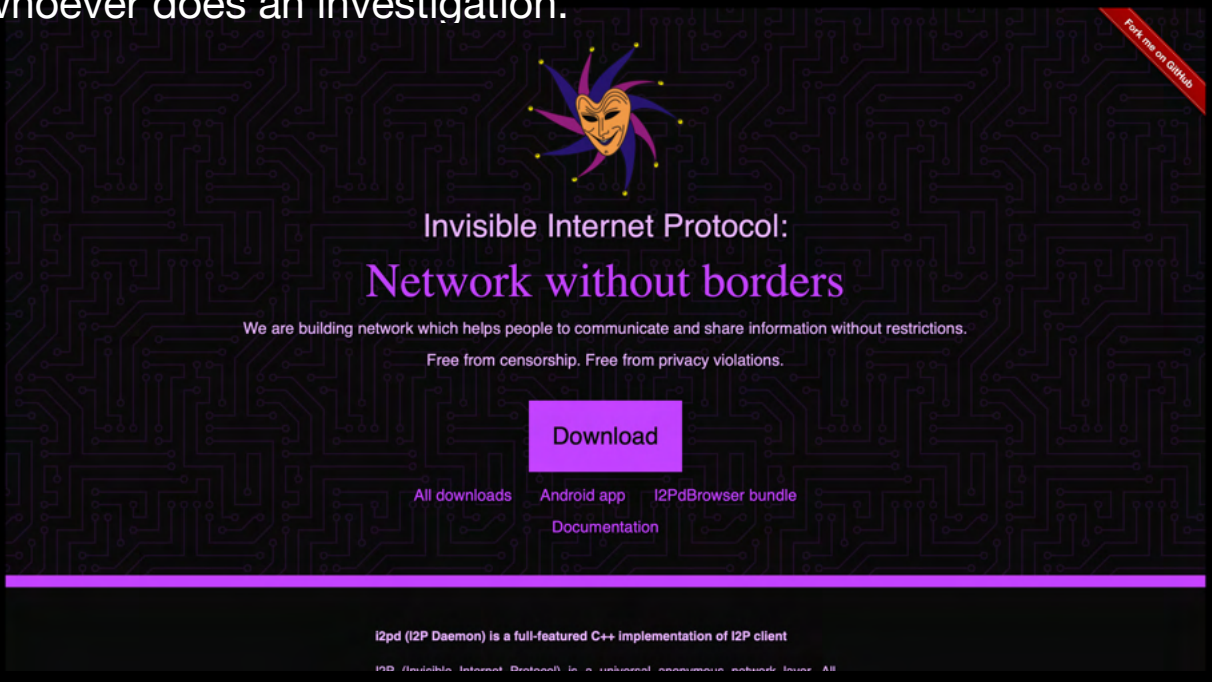
Moving from bottom to top, we can see the visit to the pirate bay as well as the torrent file download and the beginning of the transfer via Transmission app.

2022-09-15T17:56:21	modified	/Users/hexley/Library/Application Support/Transmission/Transfers.plist
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/AddressBook-v22.abcddb-
2022-09-15T17:56:08	accessed	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:56:08	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/.info
2022-09-15T17:56:06	modified	/Users/hexley/Library/Application Support/AddressBook/Sources/
2022-09-15T17:55:57	accessed	/Users/hexley/Library/Application Support/AddressBook/Metadata/3EB52CD2-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/28FEF9DE-
2022-09-15T17:55:57	modified	/Users/hexley/Library/Application Support/AddressBook/Metadata/
2022-09-15T17:54:59	PROCESS	68184 1 68184 0 /System/Library/PrivateFrameworks/PhotoAnalysis.framework/
2022-09-15T17:49:56	birth	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/Final Cut Pro 10.6.2 MAS
2022-09-15T17:49:56	modified	/Users/hexley/Downloads/Final Cut Pro 10.6.2 MAS [TNT]/README.TXT
2022-09-15T17:49:40	modified	/Users/hexley/Library/Application Support/Transmission/Torrents/
2022-09-15T17:49:25	accessed	/Users/hexley/Downloads/.DS_Store
2022-09-15T17:49:22	PROCESS	68013 1 67181 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68010 1 67181 0 /System/Library/Frameworks/QuickLookUI.framework/Versions/A/
2022-09-15T17:49:21	PROCESS	68009 1 67181 0 /System/Library/Frameworks/AppKit.framework/Versions/C/
2022-09-15T17:48:58	safari_history	https://www.opera.com/gx?utm_content=2923_c25be22e-ac35-4bba-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/fp.engine?id=7bc53178-2459-465f-89da-
2022-09-15T17:48:56	safari_history	https://engine.spotscenered.info/Redirect.eng?
2022-09-15T17:48:55	PROCESS	67985 1 60028 0 /System/Library/Frameworks/Metal.framework/Versions/A/
2022-09-15T17:48:52	safari_history	about:blank
2022-09-15T17:48:42	safari_history	https://thepiratebay.org/description.php?id=58223349

2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/rW/routerInfo-wlvLTRxzfESRuYASTb7BW		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/rW/routerInfo-wOWthzXjmK-tKCmuqMY~		
2022-09-15T18:06:49	birth	/Users/hexley/Library/Application Support/i2pd/netDb/rP/routerInfo-pZlOFnjQmCOWAlTZuYot4[		
2022-09-15T18:06:49	birth	/Users/hexley/Library/Application Support/i2pd/netDb/rP/routerInfo-pPMsFrWtc1q11JeayBxUS.		
2022-09-15T18:06:49	accessed	/Users/hexley/Library/Application Support/i2pd/netDb/rY/routerInfo-Yr0lQWv11AFqI8aVZmv5u6		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/rY/routerInfo-yw4r9bLBXKHqMcoM8RBZ		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/rY/routerInfo-yzLdw2NzV0Z-YgKJO6cNS		
2022-09-15T18:06:49	accessed	/Users/hexley/Library/Application Support/i2pd/netDb/r2/routerInfo-24DCe76q3URjfvgfkzZJXDe		
2022-09-15T18:06:49	accessed	/Users/hexley/Library/Application Support/i2pd/netDb/r2/routerInfo-28peP5T4-HVoymOBcEZ0E		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/r2/routerInfo-2I4lG1FlhDUle9aTs32OBn4Y		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/r2/routerInfo-274TSmg2KH2DRg2AMdgtl		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/r~/routerInfo-~KhbQ2bvyrBUDYRDlDaj8U		
2022-09-15T18:06:49	birth	/Users/hexley/Library/Application Support/i2pd/netDb/r~/routerInfo-~Xovx4wq1sFxtcAHkUqs0lt		
2022-09-15T18:06:49	accessed	/Users/hexley/Library/Application Support/i2pd/netDb/r~/routerInfo-~K3A1N1Hq1GRRxoTAmnm		
2022-09-15T18:06:49	accessed	/Users/hexley/Library/Application Support/i2pd/netDb/r~/routerInfo-~O9kY8c33ySCuGznLhx66/		
2022-09-15T18:06:49	modified	/Users/hexley/Library/Application Support/i2pd/netDb/r~/routerInfo-~TeFi-UwNBOLy4m2fNPQx(		
2022-09-15T18:06:06	tcc	allowed	photos	photos
2022-09-15T18:06:06	accessed	/Users/hexley/Library/Application Support/com.apple.TCC/TCC.db		
2022-09-15T18:05:40	modified	/Users/hexley/Library/Application Support/i2pd/transparent		
2022-09-15T18:05:39	PROCESS	69031 1 69031 0 unknown		
2022-09-15T18:05:39	modified	/Users/hexley/Library/Application Support/i2pd/i2pd.pid		
2022-09-15T18:05:39	modified	/Users/hexley/Library/Application Support/i2pd/router.keys		

As we move up further, we see a lot of suspicious file activity in the Application Support directory prefixed with i2pd. After doing some digging, we discovered that i2p is a tor like invisible internet protocol that the malware was using to send traffic out.

Even if a less experienced team is not equipped to make these connections, the important part is that with Aftermath they will be able to capture this valuable information in the moment while it matters and pass it to whoever does an investigation.



VERSION 2

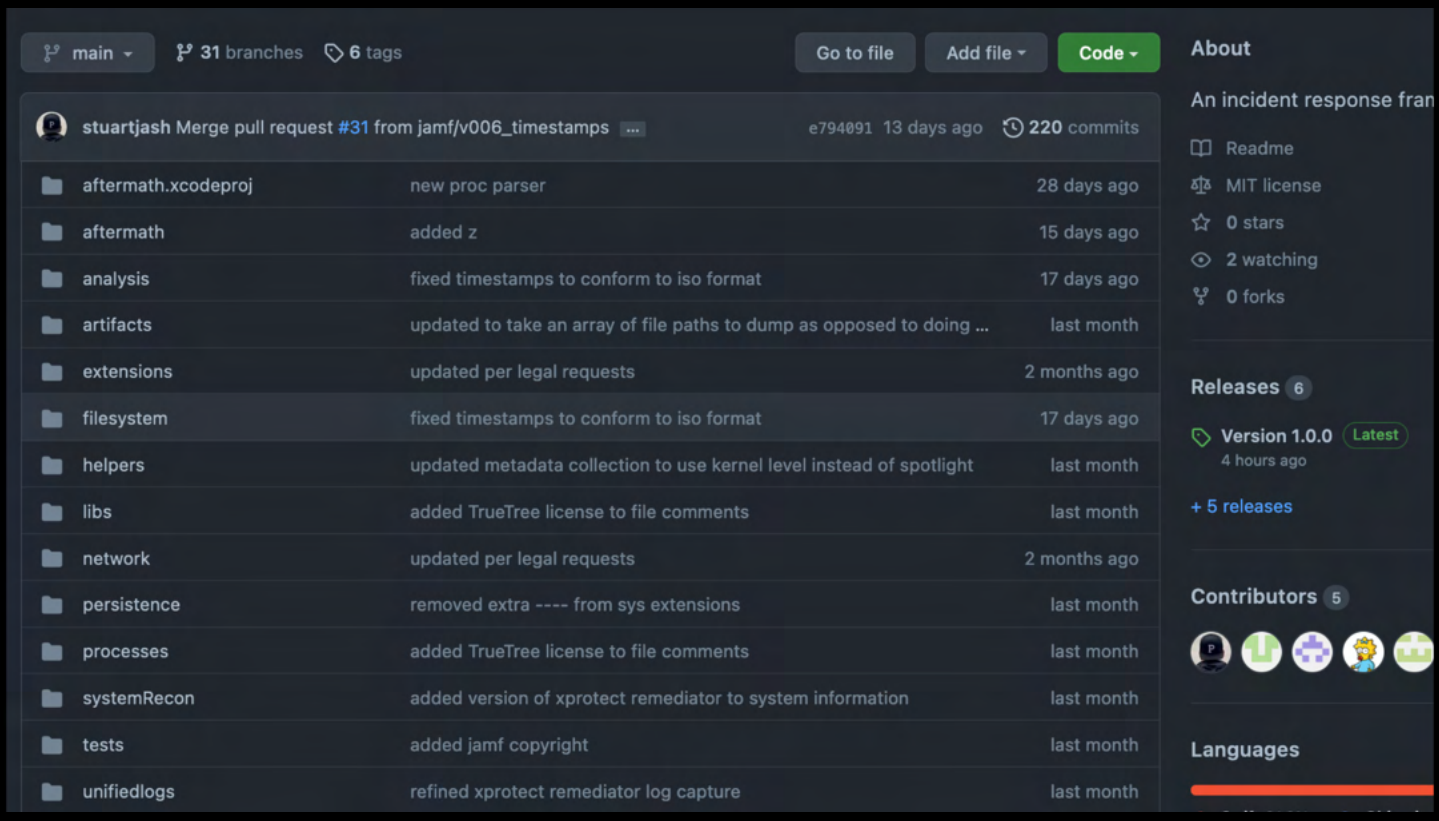
xattr

Looking forward to version 2, we're looking to add support to uploading to AWS via S3

We also want to collect and parse extended attributes

Lastly, having the ability to collect a plist file, which we currently do, but then pivot off of the plist and collect the binary it is pointing at.

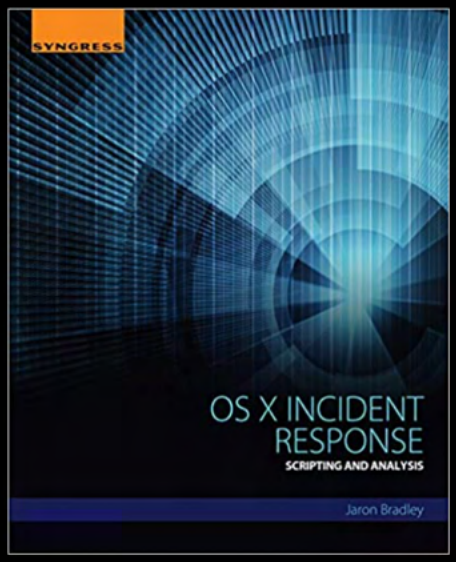
```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>MachServices</key>
    <dict>
        <key>com.objective-see.blockblock</key>
        <true/>
    </dict>
    <key>Label</key>
    <string>com.objective-see.blockblock</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Library/Objective-See/BlockBlock/BlockBlock.app/Contents/MacOS/BlockBlock</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>EnableTransactions</key>
    <false/>
    <key>LSUIElement</key>
    <true/>
</dict>
</plist>
```



https://github.com/jamf/aftermath

Contributors

- Stuart Ashenbrenner
- Jaron Bradley
- Maggie Zirnhelt
- Matt Benyo
- Ferdous Saljooki



https://github.com/jamf/aftermath

Discord: @stuartjash

Third Requirement:

This is not specifically mentioned in the policy, but follows the spirit of what Jamf is trying to accomplish with an Open Source Policy. This is a public repository representing Jamf. As such, a well crafted README is required before publishing. I cannot imagine an alien holding a decapitated human head is appropriate to represent Jamf.