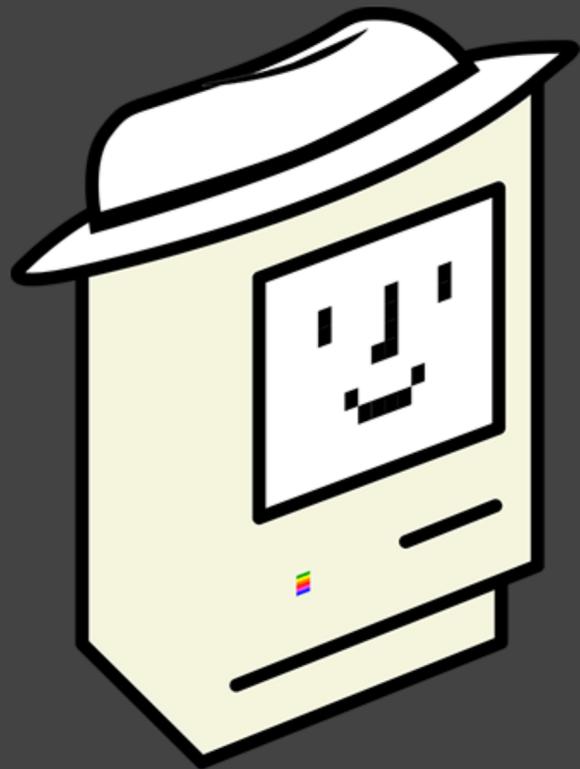


Incident Response on macOS



```
$ whoami
```

```
Thomas Reed
```

```
@thomasareed
```

```
treed@malwarebytes.com
```

What are we talking about?

✓ Incident response!

- Have access to the Mac
- What was done?
- How do you identify the threat elsewhere?
- Assuming you don't have proactive data collection

✗ Forensic collection

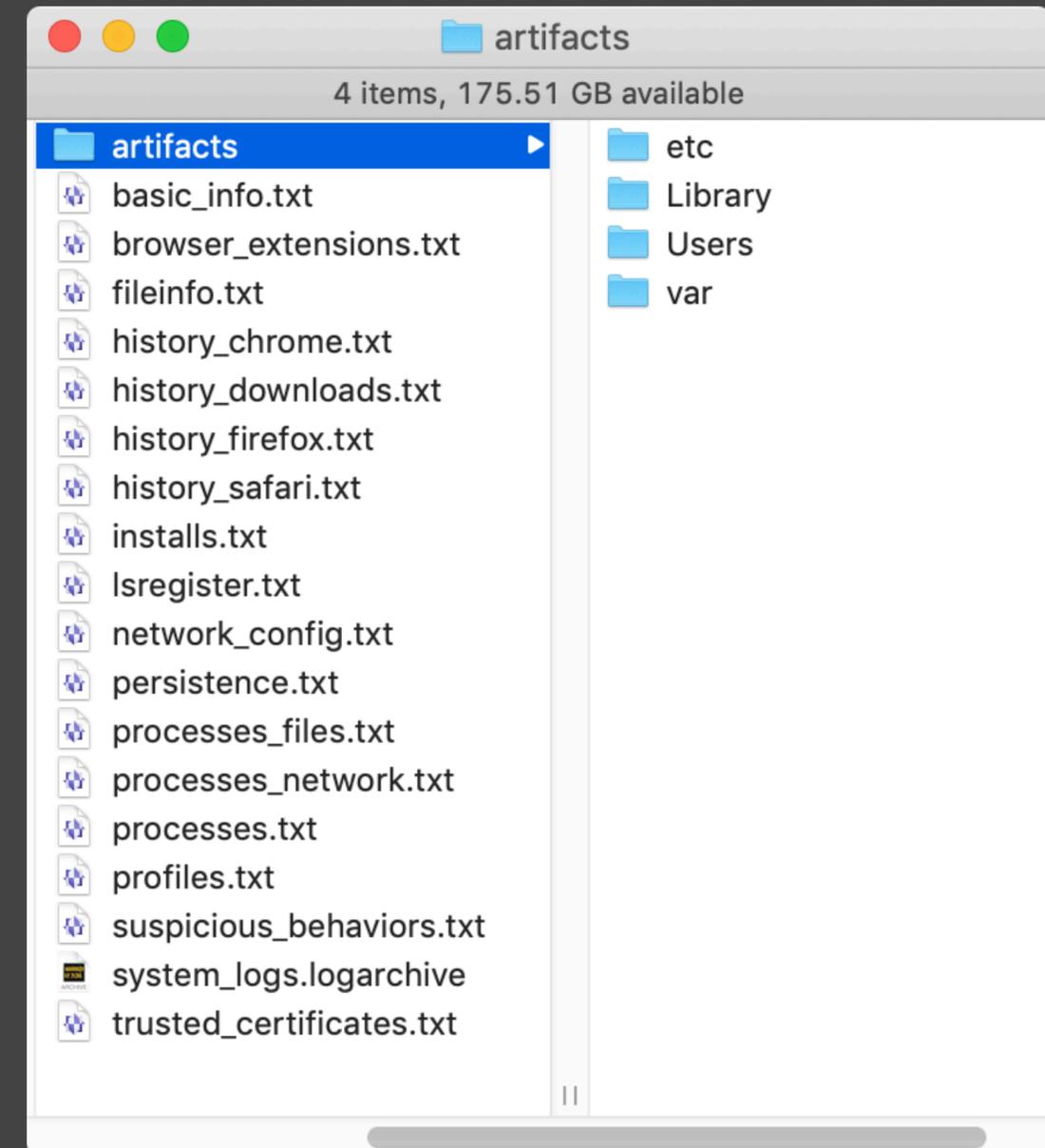
- Need data for legal evidence
- Not needed now, needs to stand up to time
- Out of scope for this talk

How do we collect IR data?

- Post-infection toolkits
 - PICT
 - <https://github.com/thomasareed/pict>
 - OSXCollector
 - <https://yelp.github.io/osxcollector/>
 - AutoMacTC
 - <https://github.com/CrowdStrike/automactc>
- Proactive toolkits
 - Venator
 - <https://github.com/richiercyrus/Venator>
 - osquery
 - <https://osquery.io>

PICT data collection

- Lots of data files to sort through
 - Machine info
 - File listing
 - Browser histories
 - Install history
 - Process listing/info
 - Persistence
 - Suspicious behaviors
 - etc...



basic_info.txt

Collected by user thomas on 2 Jul 2019 @ 21:11:40
UTC (local 2 Jul 2019 @ 17:11:40)

- Collection time
- Uptime
- Basic config info
- System and hardware info
- User list & logins

Uptime: 17:11 up 28 days, 7:54, 2 users, load
averages: 3.02 2.97 2.58

Hostname: test.local

System policy security: assessments enabled

System Integrity Protection status: enabled.

FileVault status: FileVault is On.

fileinfo.txt

Raw Flags	Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0x8000	hidden	0	0	40755	2019-06-12T 11:18:01	2019-06-12T 11:18:01	2019-06-12T 11:50:53	/Volumes

UTC

Uninterpreted mode, in octal

Group ID

User ID

Interpreted flags (only some flags shown)

Uninterpreted flags

Persistence

- persistence.txt
 - Login items
 - launchd
 - kexts
 - etc
- browser_extensions.txt
 - Safari, Chrome, Firefox
- artifacts
 - launch agent & daemon plists
 - browser extensions
 - common abusable scripts
 - .bash_profile, etc

Browser histories

- Safari, Chrome, Firefox
- "Quarantine events"
- All are fairly similar SQLite databases

history_visits

id	history_item	visit_time
366059	28	580825726.140156

history_items

id	url
28	https://apple.com



Install history

- Only tracked for macOS installer packages
- Logged in a couple different ways



Process info

- ps

- process ID, parent process ID

- path to command + arguments

- lsof

- files being accessed

- network connections open

COMMAND	PID	NODE	NAME
ZoomOpene	19952	TCP	localhost:19421 (LISTEN)

Suspicious behavior

- Processes running from suspicious locations (eg, /tmp)
- Hidden processes
- launchd plists with scripts as the program
- processes pretending to belong to Apple
- suspicious sudoers or hosts changes
- etc

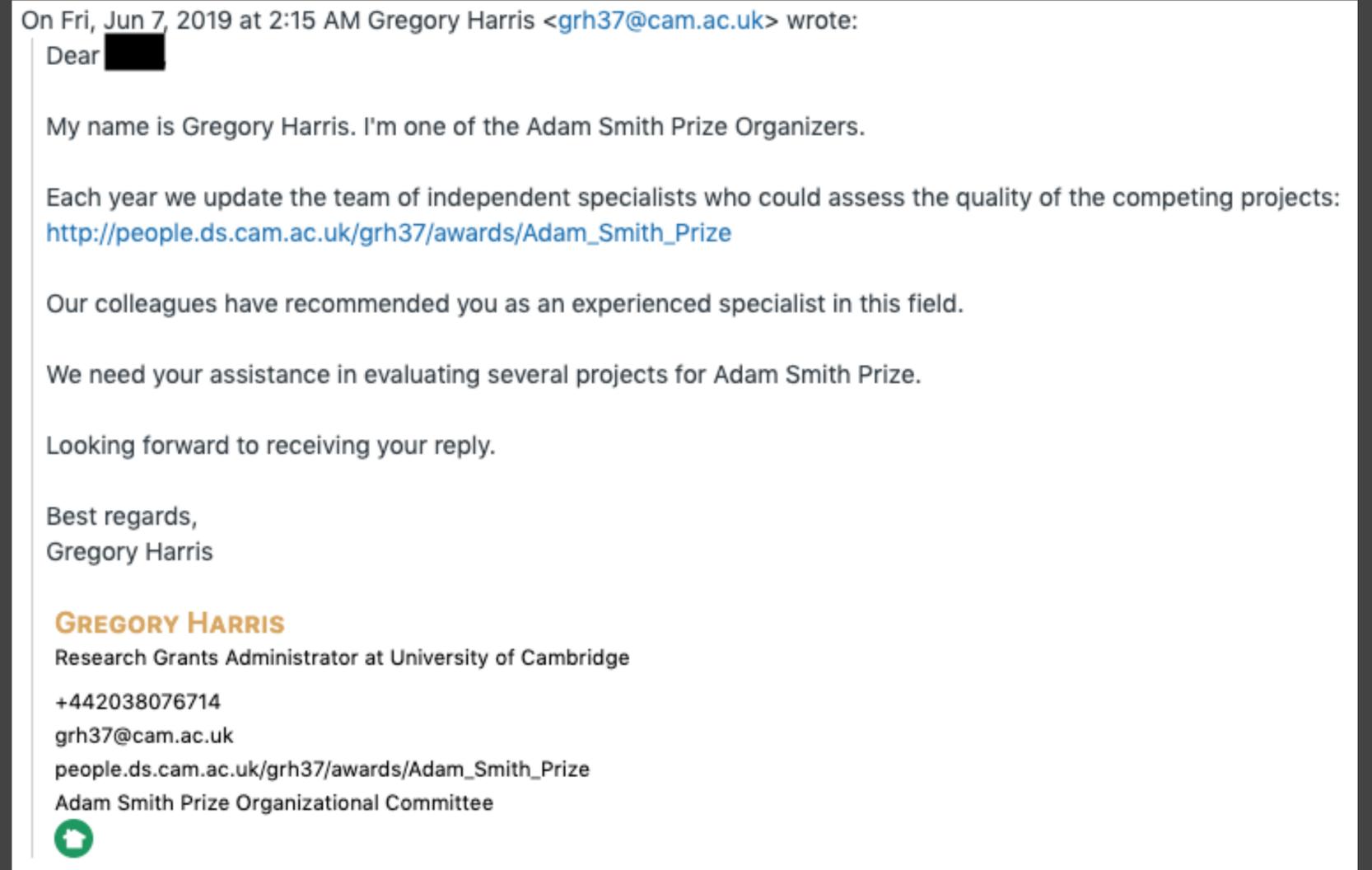
Suspicious processes

```
19952 /Users/thomas/.zoomus/  
ZoomOpener.app/Contents/MacOS/  
ZoomOpener
```

IR examples

Wirednet

- aka NetWire, aka NetWeird
- backdoor
- prior to last year, hadn't been seen since 2014
- dropped as one of two payloads by the Firefox 0-day attack on Coinbase and other cryptocurrency companies



Wirednet walkthrough

- suspicious_behaviors.txt
- Process with PID 529 running from a hidden folder
- Launch agent named com.mac.host.plist
- Are these related? 🤔

Suspicious processes

```
529 /Users/test/.defaults/  
Finder.app/Contents/MacOS/Finder
```

Suspicious agents & daemons

```
/Users/test/Library/LaunchAgents/  
com.mac.host.plist
```

Wirenet walkthrough

- /Users/test/Library/LaunchAgents/com.mac.host.plist
- Responsible for launching the Finder process

```
<dict>
  <key>Label</key>
  <string>com.mac.host</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/
test/.defaults/Finder.app/Contents/
MacOS/Finder</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
  <key>KeepAlive</key>
  <false/>
</dict>
```

Wirenet walkthrough

- fileinfo.txt
 - both Finder.app and com.mac.host.plist created June 29, 2019 @ 20:26:17

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	40755	2019-06-29T 20:26:17	2019-06-29T 20:26:17	2019-06-29T 20:29:29	/Users/test/.defaults/ Finder.app
0	501	20	100750	2019-06-29T 20:26:17	2019-06-29T 20:26:17	2019-06-29T 20:29:29	/Users/test/Library/ LaunchAgents/ com.mac.host.plist

Wirednet walkthrough

- processes_network.txt
 - Finder process has a network connection open to 89.34.111.113

COMMAND NAME	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE
Finder	529	test	3u	IPv4	0x2888275a1e50e0d5	0t0	TCP
192.168.1.13:49219->89.34.111.113:https (ESTABLISHED)							

Wireshark walkthrough

- system_logs.logarchive

```
log show --start "2019-06-29 20:26:15+0000" --end "2019-06-29  
20:26:20+0000" --timezone "00:00:00" --info --archive  
system_logs.logarchive
```

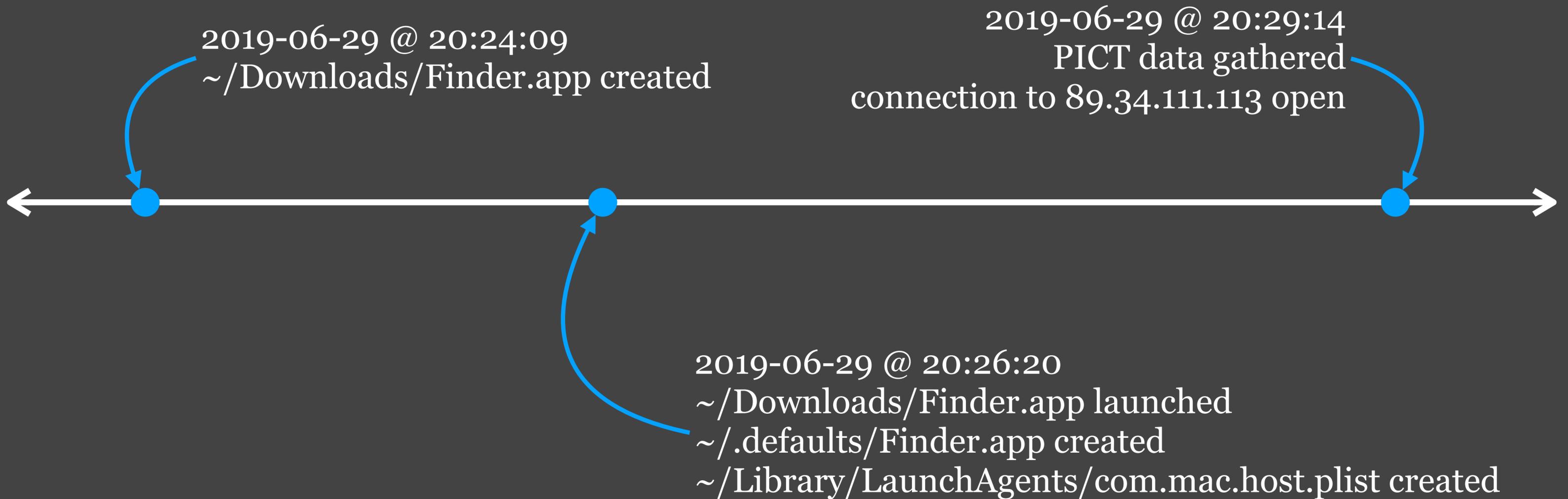
```
2019-06-29 20:26:17.237182+0000 0x1a04 Info 0x51cf 319 0  
Finder: (LaunchServices) [com.apple.launchservices:cas] LaunchApplication:  
appToLaunch={ "ApplicationType"="UIElement", "CFBundleExecutablePath"="/Users/test/  
Downloads/Finder.app/Contents/MacOS/Finder", "CFBundleExecutablePathDeviceID"=16777220,  
"CFBundleExecutablePathINode"=921876, "CFBundleName"="Finder", "CFBundlePackageType"="APPL",  
"LSBundlePath"="/Users/test/Downloads/Finder.app", "LSBundlePathDeviceID"=16777220,  
"LSBundlePathINode"=921873, "LSExecutableFormat"="LSExecutableMach0Format" } modifiers:  
{ "AddPSNArgument"=true, "LSAdditionalEnvironmentVars"={ }, "LSLaunchAsync"=true,  
"LSLaunchStoppedTemporarily"=true } args=[ NULL ]
```

Wirenet walkthrough

- fileinfo.txt
 - ~/Downloads/Finder.app created June 29, 2019 @ 20:24:09

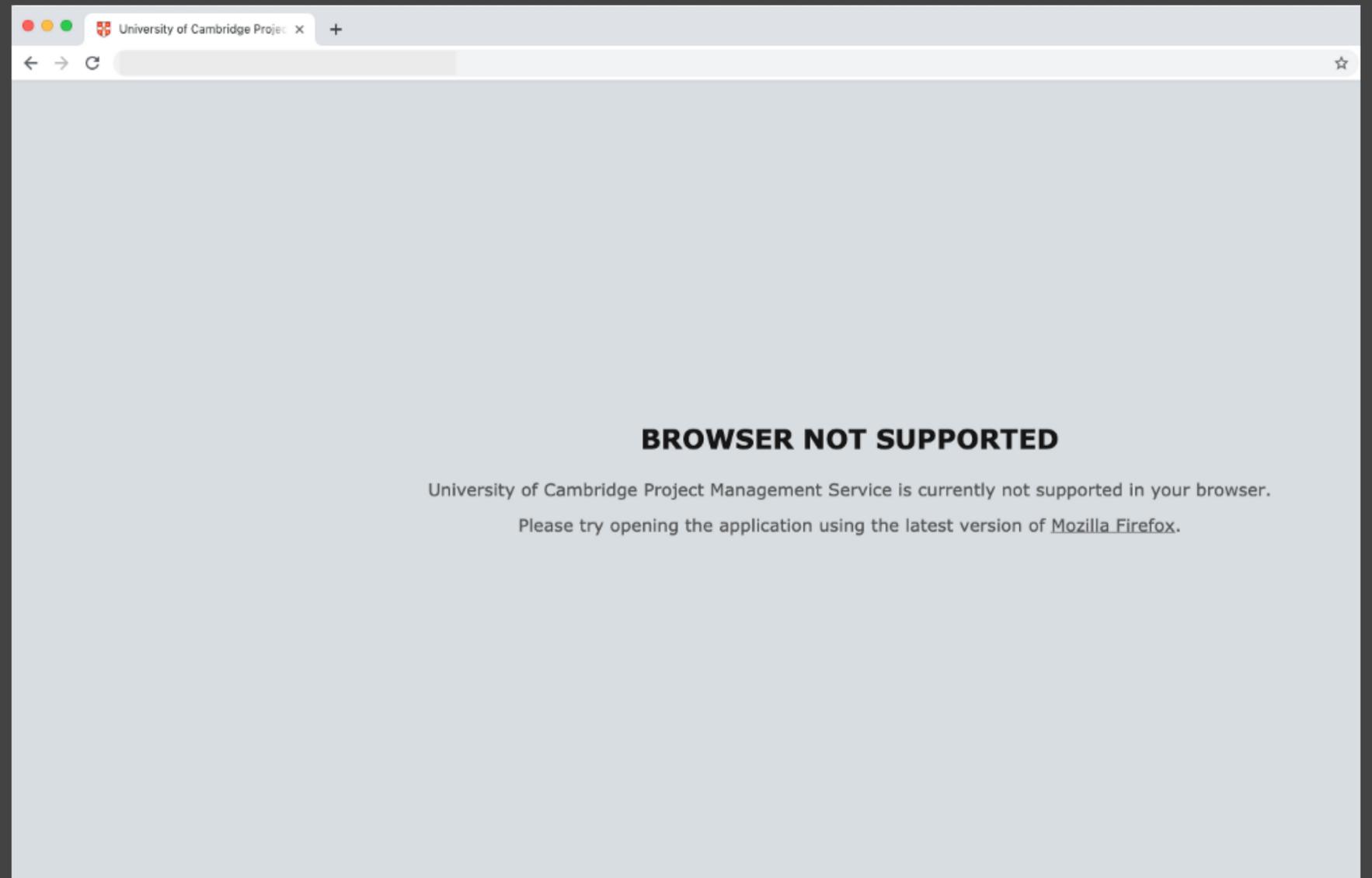
Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	40755	2019-06-29T 20:24:09	2019-06-29T 20:24:09	2019-06-29T 20:29:31	/Users/test/Downloads/ Finder.app

Wirenet timeline



Mokes

- backdoor
- prior to the end of June, hadn't been seen since 2016
- dropped as second of two payloads by the Firefox 0-day attack on Coinbase and other cryptocurrency companies



Mokes walkthrough

- persistence.txt
 - What is ~/Library/LaunchAgents/storeaccountd.plist? 🤔

User launch agents

```
-----  
/Users/test/Library/LaunchAgents  
total 24  
-rw-r--r--@ 1 test  staff  -      808 Jun 20 08:42 com.google.keystone.agent.plist  
-rw-r--r--@ 1 test  staff  -      914 Jun 20 08:42 com.google.keystone.xpcservice.plist  
-rw-r--r--  1 test  staff  -      400 Jun 29 17:34 storeaccountd.plist
```

Mokes walkthrough

- /Users/test/Library/LaunchAgents/storeaccountd.plist
- launches ~/Library/App Store/storeaccountd

```
<dict>
  <key>Label</key>
  <string>storeaccountd</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/test/Library/App
Store/storeaccountd</string>
  </array>
  <key>RunAtLoad</key><true/>
  <key>KeepAlive</key><true/>
</dict>
```

Mokes walkthrough

- processes.txt
 - storeaccountd has PID 495
 - parent PID = 1 = launchd
 - launched at 5:34 PM (local time, not UTC)

USER	PID	PPID	STARTED	TIME	COMMAND
test	495	1	5:34PM	0:00.09	/Users/test/Library/App Store/storeaccountd

Mokes walkthrough

- basic_info.txt
 - process launched at 5:34 PM local time
 - 2019-06-29 17:35:01 local time == 2019-06-29 21:35:01 UTC
 - process launched at 21:34:?? UTC

Collected by user test on 29 Jun 2019 @ 21:35:01 UTC (local 29 Jun 2019 @ 17:35:01)

Uptime: 17:35 up 45 mins, 2 users, load averages: 1.08 1.31 1.25

...

Mokes walkthrough

- fileinfo.txt
 - storeaccountd, storeaccountd.plist created 2019-06-29 @ 21:34:01

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100555	2019-06-29T 21:34:01	2019-06-29T 21:34:01	2019-06-29T 21:34:01	/Users/test/Library/App Store/storeaccountd
0	501	20	100644	2019-06-29T 21:34:31	2019-06-29T 21:34:31	2019-06-29T 21:35:41	/Users/test/Library/LaunchAgents/storeaccountd.plist

Mokes walkthrough

- processes_network.txt
 - storeaccountd has attempted to connect with 185.49.69.210, but has not received a response

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
storeacco	495	test	25u	IPv4	0x9ddae8da804e137b	0t0	TCP	
192.168.1.13:49224->185.49.69.210:http (SYN_SENT)								
storeacco	495	test	28u	IPv4	0x9ddae8da7ac74ab3	0t0	UDP	*:*

Mokes walkthrough

- processes_files.txt
 - storeaccountd has a zero-byte file open for read/write
 - (This is a marker file, used by the malware to identify which variant is installed)

```
COMMAND    PID  USER  FD      TYPE  DEVICE  SIZE/OFF  NODE NAME
storeacco  495  test  11u     REG   1,4      0 928151 /Users/test/
Library/Application Support/72769f032fd8c672bcb1a3e21a55726a
```

Mokes walkthrough

- fileinfo.txt
 - 72769f032fd8c672bcb1a3e21a55726a created 2019-06-29 @ 21:34:21

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100644	2019-06-29T 21:34:21	2019-06-29T 21:34:21	2019-06-29T 21:34:21	/Users/test/Library/ Application Support/ 72769f032fd8c672bcb1a3e 21a55726a

Mokes walkthrough

- system_logs.logarchive

```
log show --start "2019-06-29 21:33:55+0000" --end "2019-06-29  
21:34:05+0000" --timezone "00:00:00" --info --archive  
system_logs.logarchive
```

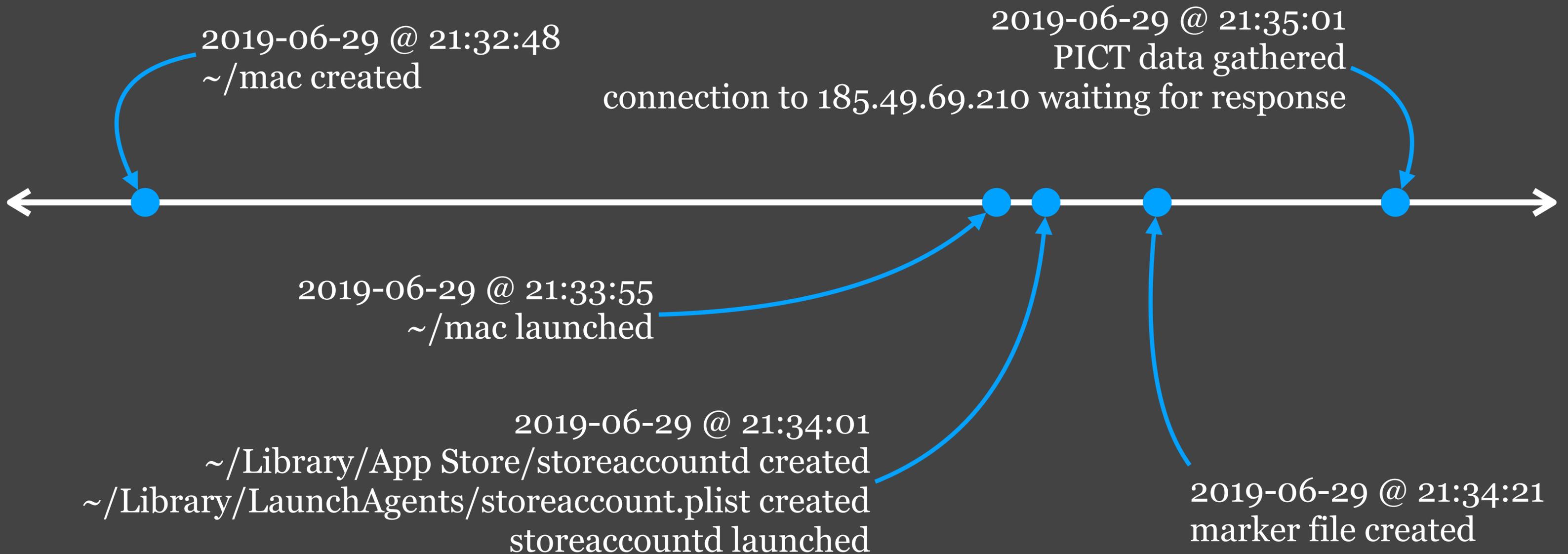
```
2019-06-29 21:33:55.600942+0000 0x249e Info 0x0  
492 0 mac: (LaunchServices) [com.apple.launchservices:cas]  
{ "ApplicationType"="BackgroundOnly", "CFBundleExecutablePath"="/  
Users/test/mac", "CFBundlePackageType"="????",  
"CFBundleSignature"="????", "Flavor"=2, "LSArchitecture"="x86_64",  
"LSCheckInTime*"="now-ish 2019/06/29 17:33:55", "LSDisplayName"="mac",  
"LSExecutableFileName"="mac" }
```

Mokes walkthrough

- fileinfo.txt
 - ~/mac created 2019-06-29 @ 21:32:48

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100755	2019-06-29T 21:32:48	2019-06-29T 21:32:53	2019-06-29T 21:34:10	/Users/test/mac

Mokes timeline



BirdMiner

- cryptocurrency miner
- Distributed through pirated audio software
- Uses an interesting code obfuscation technique

```
QEMU - (Press ctrl + alt + g to release Mouse)
Booting Core 9.0
Running Linux Kernel 4.14.10-tinycore64.
Checking boot options... Done.
Starting udev daemon for hotplug support... Done.
Waiting as requested... 5
Scanning hard disk partitions to create /etc/fstab
Setting Language to C Done.
Possible swap partition(s) enabled.
Loading extensions...^[[C Done.
Setting keymap to us Done.
Restoring backup files from /mnt/sda1/tce/mydata.tgz -
Done.
Setting hostname to box Done.

login[37811]: root login on 'tty1'

box login:
```

BirdMiner walkthrough

- persistence.txt
 - Three weird-looking launch daemons

Launch daemons

```
-----  
total 32  
-rw-r--r--  1 root  wheel  -   406 Jun 29 07:36 com.Heteroneura.plist  
-rw-r--r--  1 root  wheel  -   403 Jun 29 07:36 com.Mukden.plist  
-rw-r--r--  1 root  wheel  -   384 Jun 29 07:36 com.Tang.plist
```

BirdMiner walkthrough

- /Users/test/Library/LaunchDaemons/
com.Heteroneura.plist
 - launches /Library/Application Support/Per/
Aht
- /Users/test/Library/LaunchDaemons/
 - launches /Library/Application Support/Q/
Fulgora
- /Users/test/Library/LaunchDaemons/
 - launches /usr/local/bin/Augean

```
<dict>
  <key>Label</key>
  <string>com.Tang.plist</string>

  <key>ProgramArguments</key>
  <array>
    <string>/usr/local/bin/Augean</
string>
  </array>

  <key>RunAtLoad</key>
  <true/>

  <key>KeepAlive</key>
  <true/>
</dict>
```

BirdMiner walkthrough

- processes.txt
 - Aht PID = 848, Fulgora PID = 850, Augean PID = 1332, run by bash
 - Aht, Fulgora launched 7:36 am local time (11:36 UTC)
 - Augean launched 7:39 am local time (11:39 UTC)

USER	PID	PPID	STARTED	TIME	COMMAND
root	848	1	7:36AM	0:00.00	/bin/bash /Library/Application Support/Per/Aht
root	850	1	7:36AM	0:00.00	/bin/bash /Library/Application Support/Q/Fulgora
root	1332	1	7:39AM	0:00.00	/bin/bash /usr/local/bin/Augean

BirdMiner walkthrough

- processes.txt
 - Aht is parent process of Per, PID 861
 - Fulgora is parent process of Q, PID 870
 - Augean is parent process of s leep, PID 1342

```
USER      PID    PPID  STARTED      TIME  COMMAND
root      861    848   7:36AM      5:18.18 /usr/local/bin/Per -M accel=hvf --cpu host /Library/
Application Support/Per/Stercorarius -display none
root      870    850   7:36AM      5:17.66 /usr/local/bin/Q -M accel=hvf --cpu host /Library/
Application Support/Q/Canchi -display none
root     1342   1332   7:39AM      0:00.00 sleep 600
```

BirdMiner walkthrough

- Per, Q both have used a significant amount of processor time
 - Processes started @ 7:36 am local time
 - basic_info.txt -> capture happened @ 7:43 am local time (7 minutes later)
 - Malware has already used more than 5 minutes of processor time! 🤔

```
USER      PID    PPID  STARTED    TIME  COMMAND
root      861    848   7:36AM    5:18.18 /usr/local/bin/Per -M accel=hvf --cpu host /Library/
Application Support/Per/Stercorarius -display none
root      870    850   7:36AM    5:17.66 /usr/local/bin/Q -M accel=hvf --cpu host /Library/
Application Support/Q/Canchi -display none
root     1342   1332   7:39AM    0:00.00 sleep 600
```

BirdMiner walkthrough

- If we don't have samples of the files, this is useful information:
 - Per `-M accel=hvf --cpu host .../Stercorarius`
- Google "accel=hvf"
 - First five hits relate to Qemu
 - Qemu = Linux emulator that runs on macOS
 - Stercorarius, Canchi probably Qemu VMs



Now that qemu has accel=hvf, any good macOS front-ends? : qemu_kvm

...

https://www.reddit.com/r/qemu.../now_that_qemu_has_accelhvf_any_good_macos/ ▼

Apr 25, 2018 - 1 post - 1 author

Qemu 2.12 has added support for macOS's Hypervisor.framework (essentially KVM for Macs). Are there any good front-ends for macOS?

QEMU + HVF : qemu_kvm

Mar 5, 2019

Fuchsia's Ermine user shell in Android Emulator : Fuchsia

May 2, 2019

[More results from www.reddit.com](#)

Qemu on MacOSX with Hypervisor Framework | Breakintheweb

breakintheweb.com/2017/10/14/Qemu-on-MacOSX-with-Hypervisor-Framework/ ▼

Oct 14, 2017 - Launch Qemu. The two switches are required to use the hypervisor.framework. 1.

`/usr/local/bin/qemu-system-x86_64 -M accel=hvf --cpu host ...`

[Qemu-discuss] qemu with -accel hvf - The Mail Archive

<https://www.mail-archive.com/qemu-discuss@nongnu.org/msg04313.html> ▼

Sep 26, 2018 - Hi, let me introduce myself, I am new on this list, currently playing around with qemu on macOS, trying to run virtual machines (linux guests, e.g. ...

Bug #1815263 "hvf accelerator crashes on quest boot" : Bugs : QEMU

<https://bugs.launchpad.net/bugs/1815263> ▼

Feb 9, 2019 - `sudo qemu-system-x86_64 -M accel=hvf -boot d -cdrom ~/Downloads/install64.iso.`

Password: qemu-system-x86_64: warning: host doesn't ...

Add support for hvf accelerator to QEMU builder · Issue #6189 ...

<https://github.com/hashicorp/packer/issues/6189> ▼

Apr 25, 2018 - QEMU 2.12 has added "Experimental support for two new virtualization accelerators:

Apple's Hypervisor.framework ("-accel hvf") and ...

BirdMiner walkthrough

- Evidence suggests this is a cryptominer
- ...but we can't be sure!
- If we had the files and could analyze, we would find XMRig code in the Qemu VM

```
#!/bin/sh
# put other system startup commands here
/mnt/sda1/tools/bin/idgenerator 2>&1 > /dev/null
/mnt/sda1/tools/bin/xmrig_update 2>&1 > /dev/null
/mnt/sda1/tools/bin/ccommand_update 2>&1 > /dev/null
/mnt/sda1/tools/bin/ccommand 2>&1 > /dev/null
/mnt/sda1/tools/bin/xmrig
```

BirdMiner walkthrough

- processes_network.txt
 - Per and Q both have connections open to subdomain of njalla.net, a hosting service
 - IP address = 185.193.126.159

```
COMMAND      PID      USER     FD      TYPE          DEVICE          SIZE/OFF      NODE NAME
Per          861      root     16u     IPv4          0xc9bce5804a5a9af7      0t0          TCP
192.168.1.13:49230->host-185-193-126-159.njalla.net:http-alt (ESTABLISHED)
Q            870      root     16u     IPv4          0xc9bce5804a5a8837      0t0          TCP
192.168.1.13:49231->host-185-193-126-159.njalla.net:http-alt (ESTABLISHED)
```

BirdMiner walkthrough

- fileinfo.txt
 - Aht, Fulgora modified 2019-06-29 @ 11:36:14
 - No data for /usr/local/bin/Augean, because /usr has restricted flag, and was skipped

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	0	80	100700	2019-06-29T 11:36:14	2019-06-29T 11:36:57	2019-06-29T 11:37:08	/Library/Application Support/Per/Aht
0	0	80	100700	2019-06-29T 11:36:14	2019-06-29T 11:36:57	2019-06-29T 11:36:57	/Library/Application Support/Q/Fulgora

BirdMiner walkthrough

- fileinfo.txt
 - Stercorarius, Canchi accessed 2019-06-29 @ 11:38:35

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	0	80	100700	2019-06-29T 11:39:06	2019-06-29T 11:39:06	2019-06-29T 11:38:35	/Library/Application Support/Per/Stercorarius
0	0	80	100700	2019-06-29T 11:39:06	2019-06-29T 11:39:06	2019-06-29T 11:38:36	/Library/Application Support/Q/Canchi

BirdMiner walkthrough

- installs.txt
 - Something called ValhallaVintageVerb was installed on 2019-06-29 @ 11:36:15

```
2019-06-29 11:36:15 +0000 Library/Application Support/Digidesign/Plug-Ins installer
valhallavintageverb-1.pkg com.ValhallaDSP.valhallavintageverb171.ValhallaVintageVerb-2.pkg
1.7.1
2019-06-29 11:36:15 +0000 Library/Application Support/Valhalla DSP, LLC/ValhallaVintageVerb/
Presets/ installer presets.pkg com.ValhallaDSP.valhallavintageverb171.Presets.pkg 1.7.1
2019-06-29 11:36:15 +0000 Library/Audio/Plug-Ins/Components installer
valhallavintageverb.pkg com.ValhallaDSP.valhallavintageverb171.ValhallaVintageVerb-3.pkg 1.7.1
...
```

BirdMiner walkthrough

- history_safari.txt
 - Site vstcrack[dot]com visited on 2019-06-29 @ 11:31:42

2019-06-20 16:40:47 https://www.google.com/search?

client=safari&rls=en&q=firefox&ie=UTF-8&oe=UTF-8

2019-06-20 16:40:50 https://www.mozilla.org/en-US/firefox/new/

2019-06-20 16:40:52 https://www.mozilla.org/en-US/firefox/download/thanks/

2019-06-29 11:31:42 http://www.vstcrack.com/elementor-240/

2019-06-29 11:31:42 http://www.vstcrack.com/elementor-240/

2019-06-29 11:31:43 http://www.vstcrack.com/elementor-240/

BirdMiner walkthrough

- history_downloads.txt
 - Last entry for Firefox, no sign of what was downloaded from vstcrack
 - This is unreliable for Safari!

Downloaded: 2019-06-20 16:41:38 by agent: com.apple.Safari

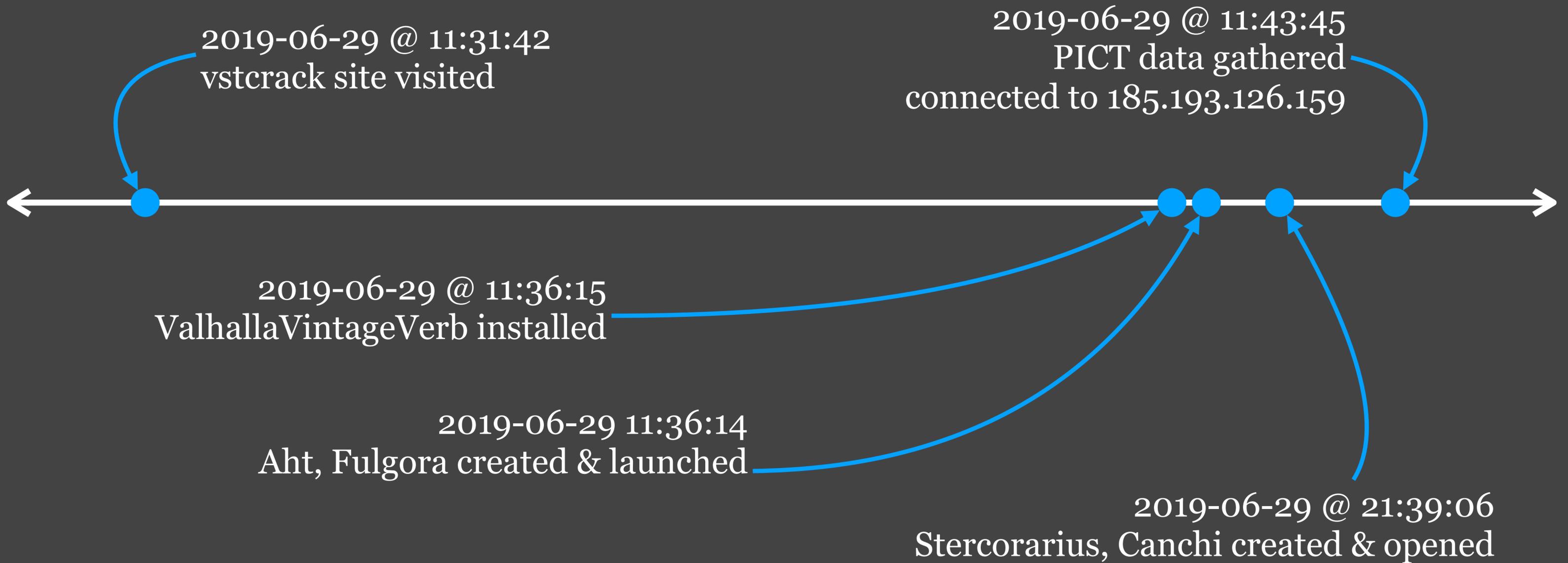
File:

<https://download-installer.cdn.mozilla.net/pub/firefox/releases/67.0.3/mac/en-US/Firefox%2067.0.3.dmg>

Origin:

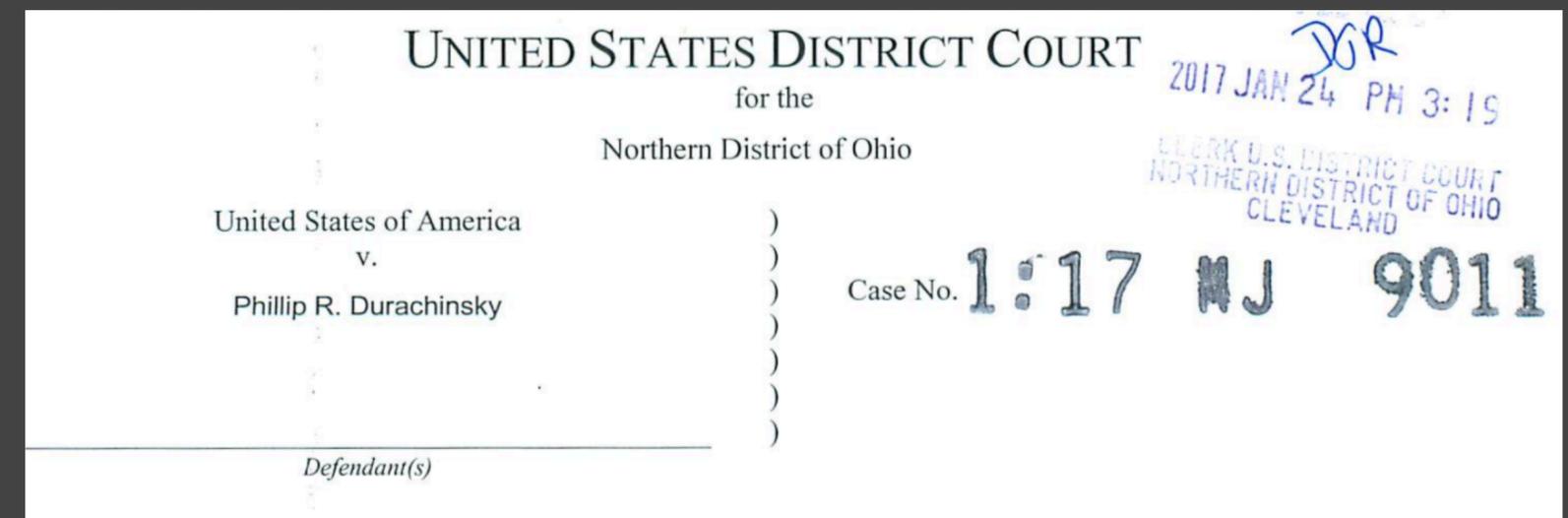
<https://www.mozilla.org/en-US/firefox/download/thanks/>

BirdMiner timeline



FruitFly

- backdoor
- Used to infect Macs for a decade
- Creepy! Likes to access the webcam, microphone, etc
- Alleged culprit, Phillip Durachinsky, is in prison awaiting trial



FruitFly walkthrough

- suspicious_behaviors.txt
 - user launch agent: com.client.client.plist

Suspicious agents & daemons

/Users/test/Library/LaunchAgents/com.client.client.plist

FruitFly walkthrough

- /Users/test/Library/LaunchAgents/com.client.client.plist
- launches ~/.client
- NSUIElement indicates no icon should be shown in the Dock

```
<dict>
  <key>KeepAlive</key>
  <true/>
  <key>Label</key>
  <string>com.client.client</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/test/.client</
string>
  </array>
  <key>RunAtLoad</key>
  <true/>
  <key>NSUIElement</key>
  <string>1</string>
</dict>
```

FruitFly walkthrough

- processes.txt
 - Shows no matches for "client"
- persistence.txt
 - .client launched with PID 536

```
345  0  com.apple.UserEventAgent-Aqua
470  0  com.apple.followupd
-  0  com.apple.ReportPanic
536  0  com.client.client
403  0  com.apple.identityservicesd
407  0
com.apple.telephonyutilities.callserv
icesd
-  0  com.apple.DwellControl
```

FruitFly walkthrough

- processes.txt
 - Java was launched with PID 536
 - Is .client a shell script that runs Java? 🤔

USER	PID	PPID	STARTED	TIME	COMMAND
test	536	1	3:41PM	0:00.07	java

FruitFly walkthrough

- processes_files.txt
 - Process 536 listed as perl... .client must be a perl script!

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
perl5.18	536	test	txt	REG	1,4	52864	819599	/usr/bin/perl5.18
...								
perl5.18	536	test	3r	REG	1,4	82947	916530	/Users/test/.client

FruitFly walkthrough

- fileinfo.txt
 - ~/.client created 2019-06-29 @ 19:38:47

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100711	2019-06-29T 19:38:47	2019-06-29T 19:38:47	2019-06-29T 19:41:30	/Users/test/.client

FruitFly walkthrough

- history_*.txt, installs.txt, /Library/Receipts/InstallHistory.plist
 - A whole lot of nuthin'!
 - It doesn't look like this was downloaded/installed by the user

FruitFly walkthrough

- /Users/test/.bash_history
 - Evidence of manual installation!
 - Did the attacker have physical or remote access?
 - logout at the end suggests remote, but how can we be sure?

```
ls -al
ls -al
chmod +x .client
launchctl load Library/LaunchAgents/com.client.client.plist
ls -al Library/LaunchAgents
launchctl load Library/LaunchAgents/com.client.client.plist
ls -al Library/LaunchAgents
ls -al
chmod +x .client
launchctl load Library/LaunchAgents/com.client.client.plist
ls -al
launchctl list
launchctl list | grep -v com.apple
launchctl load Library/LaunchAgents/com.client.client.plist
launchctl load -w Library/LaunchAgents/
com.client.client.plist
launchctl list | grep -v com.apple
logout
```

FruitFly walkthrough

- system_logs.logarchive

- log show --start "2019-06-29 19:38:40+0000" --end "2019-06-29 19:39:00+0000" --timezone "00:00:00" --info --archive system_logs.logarchive

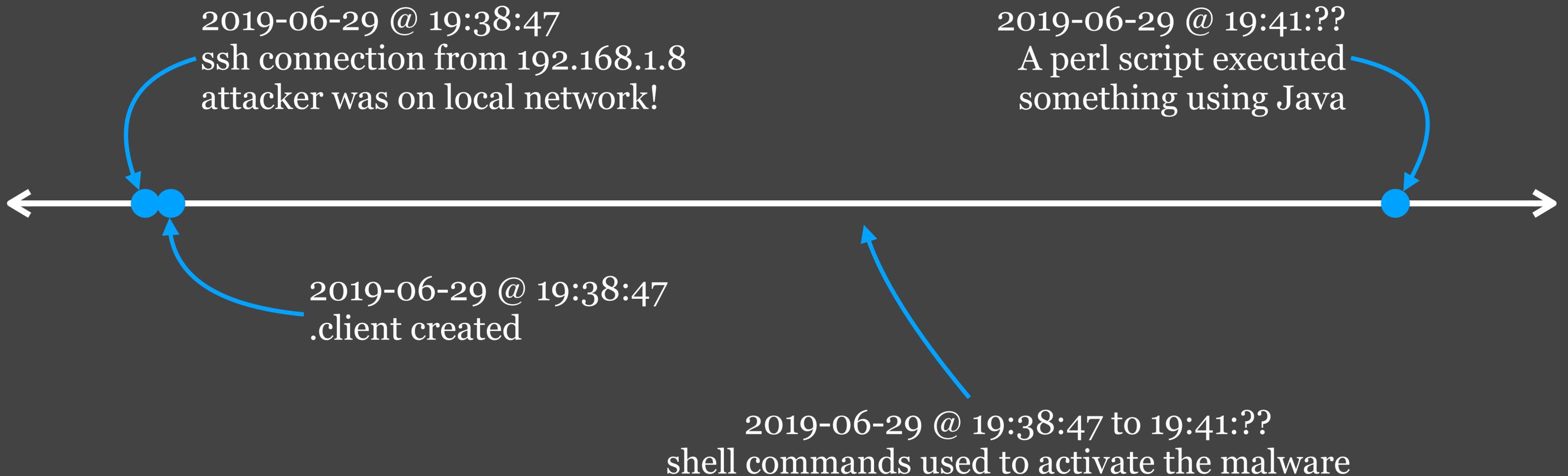
```
2019-06-29 19:38:47.211236+0000 0x19ba      Info      0x0      517      0
sshd: Postponed keyboard-interactive/pam for test from 192.168.1.8 port 58996 ssh2
[preauth]
...
2019-06-29 19:38:47.216254+0000 0x19ba      Info      0x0      517      0
sshd: Accepted keyboard-interactive/pam for test from 192.168.1.8 port 58996 ssh2
2019-06-29 19:38:47.217026+0000 0x19bd      Info      0x0      72       0
opendirectoryd: [com.apple.opendirectoryd:session] PID: 518, Client: 'sshd', exited with 0
session(s), 0 node(s) and 0 active request(s)
```

FruitFly walkthrough

Technical Details

The attack vector included the scanning and identification of externally facing Mac services to include the Apple Filing Protocol (AFP, port 548), RDP, VNC, SSH (port 22), and Back to My Mac (BTMM), which would be targeted with weak passwords or passwords derived from 3rd party data breaches.

FruitFly timeline



Questions?

Slides:

<https://github.com/thomasareed/presentations>