



When Macs Get Hacked

Sarah Edwards

@iamevltwin

oompa@csh.rit.edu

About Me

- ◉ Senior Digital Forensics Analyst
- ◉ Crucial Security (Harris Corporation)
- ◉ Northern Virginia
- ◉ Federal Law Enforcement
- ◉ Intrusion Analysis
- ◉ Counter-Intelligence, Counter-Terrorism, Criminal Cases
- ◉ Mac Nerd at heart.
- ◉ Blog: crucialsecurityblog.harris.com

Current Threats:

Suspicious
Use

Insider
Threat

Data
Exfiltration

Keylogger

Ad-Click
Malware

Information
Stealer

Phishing

Backdoors

Current Threats: Flashback

- Infected 600,000+ systems
- \$10,000/day ad-click revenue for attackers
- Java Vulnerabilities
- Fake Adobe Flash Installer
- Drive-by-Download
 - Compromised Wordpress Blogs

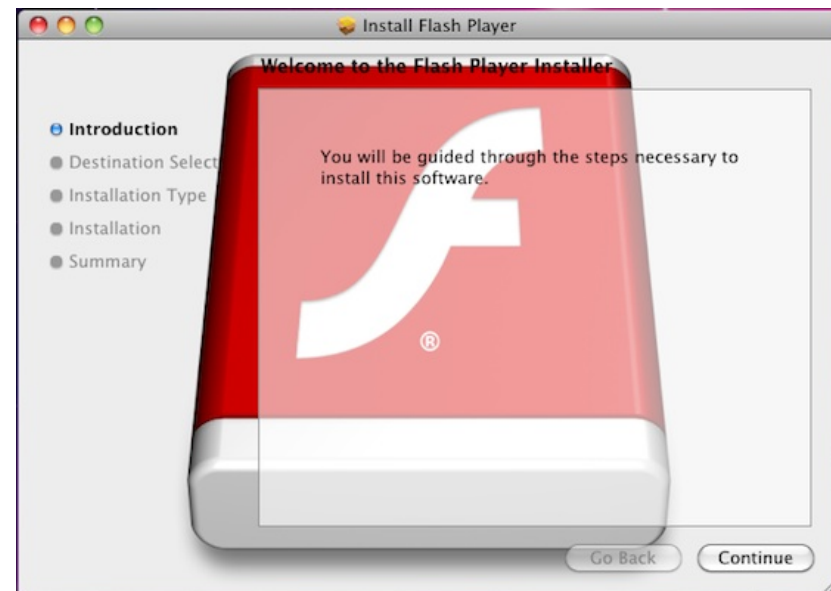


Image Source: <http://www.cultofmac.com/124840/new-flashback-os-x-trojan-is-in-the-wild-and-it-can-kill-os-xs-anti-malware-scams/>

Current Threats: Imuler

- Hidden .app file in Zip Archive
- Installs backdoor
- Information Stealer
 - Files
 - Screenshots

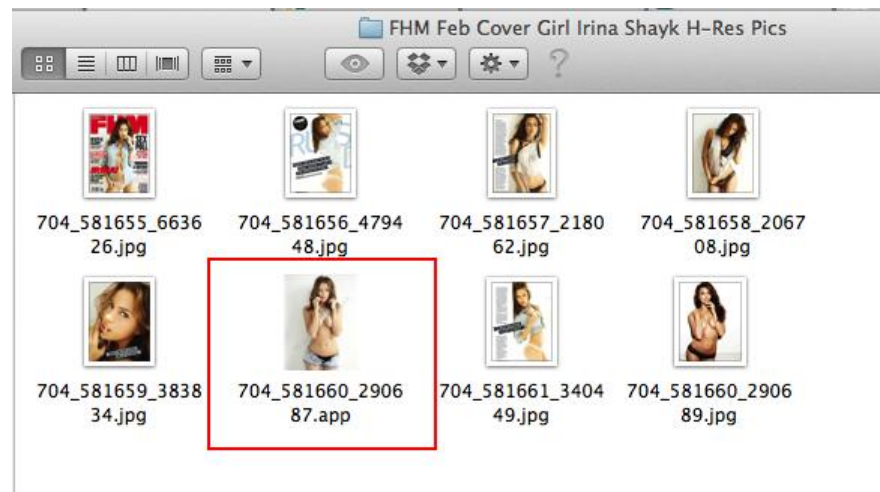


Image Source: <http://blog.eset.com/2012/03/16/osximuler-updated-still-a-threat-on-mac-os-x>

Current Threats: SabPub

- Vulnerabilities
 - Java
 - MS Word
- Malicious/Decoy Word Document
- Targeting Tibetan NGOs
- Backdoor
 - Download/Upload Files
 - Screenshots
 - Shell Execution

༡༤༡ བྱུང་ཡོད་པ་འདྲམ་ནས་པ་ལྟ་ན་ཆས་མཚོག་པ་འདྲིན་ལྟ་པ་ལྟ་བུར་བྱུང་གསལ་ཡིག་ཆ་འདི་མང་ཚོགས་པ་
གསལ་བསྐྱུགས་བྱ་བས་འདྲུག་ཅི་ནས་ཡོང་བསྐྱུགས་མེ་མོ།

[illegible]

ཡན་འདི་ལས་གསལ་བཤམ་ན་ཡང་བཟིན་ཏིང་མི་ལོན་ཏུ་མ་འདི་མེད་པ་དང་།
མ་འོངས་པར་དེ་ལས་མེ་མང་ལ་མོང་ན་ཁྱི་ཚོགས་ཀྱི་ཕྱི་ན་བསྐྱེལ་བཞུགས་ཏེ་རྒྱ་ཡོང་ཆུ་བཟུ་མི་སྒྲོག་
དེས་ན་མང་པོ་ནི་ཁྱི་ལས་པ་བཤམ་དེས་པ་དགོས་འདུག་པས་མ་འོངས་པའི་ཚ་དྲུག་ལས་མང་ནས་གསལ་བ་
ཤེད་ཏེ་རྒྱ་ཁྱི་མོས་ཐག་གཅོད་ཏུ་མ་ཡིན། ༡༩༠༡ ཕྱི་ཟླ ༩ ཚེས ༡༤ ཉིན་ཡུམ་མིའི་ཚོགས་འདུའི་ནང་དོན་
གནད་འདི་ཕྱི་ན་གསལ་བཤམ་ཏུ་ཁྱེད་ཀྱི་མེད་ཆུང་ལ་གནང་པའི་མེད་འདུག་པའི་ཚོགས་འདུ་ནི་ལ་ལུས་ཀྱང་བཀ་
བ་ཁྱོད་ཀྱི་ནང་དུ་མང་པ་དེས་ཀྱིས་ལུས་པ་བཤམ་དོན་མེད་པ་དང་མེད་ཀྱང་།

ཆོག་པ་ཞེས་ཞིག་ནས་མ་གནས་འདུག་ཟེའི་ཆོག་པ་འདྲའི་ར་མའི་ནང་ཁྱིམ་གྱི་མང་ཁྱོད་ཡོད་མཁུ་འགའ་བ་
འཕྱོད་ནི།

མིང་ཤོས་ཀྱིས་ཡུལ་ཡོད་མི་ལྷན་པུ་མ་ཡིན་ནམ་གྱི་ཚོ་ལོགས་ཀྱི་འཕུལ་ལས་དང་མི་མང་པ་རྫོག་མོ་ལ་འཕུལ་ལོན་དྲུག་པ་དང་
འཕུལ་གྲག་མི་མང་གསལ་འཕུལ་དང་འཕུལ་ཀྱི་ཡུལ་ཡོད་པའི་མང་ཁྱུང་གྲག་ལས་འགྲང་ཆེ་པ་མེད་ན།
དེར་འཕུལ་མང་ཚོ་ལོགས་ནས་འཕུལ་ལོན་པ་ལྟར་མི་ཡིན་ཁྱུང་གསལ་འགྲང་གི་ནང་ནས་འཕུལ་དང་ལོན་པ་དེར་ལྷན་འཕུལ་དྲུག་ལས་
དེ་མིན་གྱི་ཚོ་ལོགས་ནང་འཕུལ་ལས་མ་ཕན་གྱི་མི་ལྷན་པུ་མ་ཡིན་ནམ་གྱི་ཚོ་ལོགས་པ་རྫོང་ཀྱུང་དང་ཀྱུང་ལས་
མ་འཕུལ་པ་ལས་མ་དག་པའི་འཕུལ་ལས་ལས། འདི་དེ་ལོགས་མི་མང་གསལ་འཕུལ་དྲུག་ཀྱི་ཚོ་ལོགས་མི་ཕྱིང་ནས་ཡུལ་
ཀུན་ལ་ཕྱིན་གྱི་ལོ་ ༡༩ རྒྱུ་ ༡༩ ལས་འདི་ལས།

www.tibet.net

Image Source: <http://totaldefense.com/blogs/2012/04/18/OSX/SabPub-New-Backdoor-Malware-Threat-for-Mac-OS-X.aspx>

Current Threats: MacControl

- MS Word Vulnerability
- Remote Access Trojan
 - Possible complete control of system
- Targets Tibetan NGOs via phishing emails

Your Excellency
The United Nations Commission for Human Rights
The United Nations Commission for Human Rights Office
Geneva, Switzerland.
Dated: 9th March 2012.

Your Excellency,
The Tibetans throughout the Globe will co-memorate the 53rd Anniversary of the Tibetan National Uprising Day in Lhasa, Tibet in 1959, against the Peoples Republic of China. During these 53 long years of struggle, thousands of innocent Tibetans were tortured, imprisoned and killed by the Chinese government, without a fair trial. Tibet
s rich resources are plundered and the environment destroyed with deforestation, elimination of its rare species of wildlife and diverting and damming of Tibet
s holy rivers which are source of lifeline for many Asian countries.
Since 2008, massive crackdowns and indoctrination of Tibetan monks and nuns were imposed by the Chinese Government. Due to heavy handedness of the Chinese authorities, and the unbearable condition of the Tibetans under their most repressive rule, the Tibetans from all parts of Tibet, especially Ngaba and Karzi regions unitedly protested, demanding the return of Tibet
s spiritual leader H.H. the Dalai Lama and freedom for Tibet. Instead of addressing the problems being faced by the Tibetans under the Chinese repressive rule in Tibet, the Chinese authorities sought to use forceful methods by firing on unarmed Tibetan protestors, beating and injuring them. Since 16th March 2011, over 24 Tibetans have self-immolated, calling for return of Tibet
s spiritual leader H.H. the Dalai Lama and freedom for Tibet. In short, Tibet is cut off from outside world, with ban on the entry of foreign media personnel and tourists.
We therefore, appeal to your Excellency and the representatives of the United Nations member countries to take immediate action on the following demands:-
1) Insist the Peoples Republic of China to immediately call back all Chinese Security personnel from Ngaba and Karzi regions of Tibet.
2) All the monks and nuns must be allowed to return unconditionally to their respective monasteries
3) Insist the Chinese authorities to release all the political prisoners, especially the young Panchen Lama, Gedun Choekyi Nyima and Tulku Tenzin Delek
4) Allow foreign diplomats and independent media unfettered access to all the Tibetan areas for observation
Stop all forms of persecution in Tibet and adhere to Global Human Rights norms.
Your Excellency, we Tibetans inside Tibet and in other parts of the world, appeal and look forward eagerly to genuine political support from the United Nations like any other weaker nations who are facing tremendous aggression from more powerful nations in the world.
As you are aware, we Tibetans, under the leadership of His Holiness the Dalai Lama, the non-violent and compassionate leader who follows non-violent even to last resort, continue to follow His steps to gain Freedom for the Tibetans.
Thanking you,
With due respect and hope,
TENZIN WANGMO
President
RTWA Bylakuppe, Karnataka State
PHURBU LHAMO
President
RTWA Kollegal, Karnataka State

Image Source: <http://labs.alienvault.com/labs/index.php/2012/ms-office-exploit-that-targets-macos-x-seen-in-the-wild-delivers-mac-control-rat/>

Current Threats: Python Backdoor

- Java Vulnerability
- Downloads
install_flash_player.py
 - Sophos: OSX/FlsplySc-A
- Further installs update.py
 - Backdoor
 - Accepts attacker commands
 - Upload code
 - Steals files
 - Run commands
- Also targets Windows systems!

```
command_current = eval(command)

if command_current[0] == 'listDF':
    listDirectoryFile = {}
    listDirectoryFile['c'] = 'listDF'
    listDirectoryFile['arg1'] = command_current[1]
    listDirectoryFile['d'] = [f for f in os.listdir(command_current[1])
                             if os.path.isdir(os.path.join(command_current[1], f))]

    listDirectoryFile['f'] = [(f, os.path.getsize(os.path.join(command_current[1], f)),
                             time.ctime(os.path.getmtime(os.path.join(command_current[1], f))))
                             for f in os.listdir(command_current[1])
                             if os.path.isfile(os.path.join(command_current[1], f))]

    send_back_output(repr(listDirectoryFile))

elif command_current[0] == 'upload':
    listDirectoryFile = {}
    listDirectoryFile['c'] = 'upload'
    listDirectoryFile['arg1'] = command_current[1]
    listDirectoryFile['arg2'] = command_current[2]

    output = open(command_current[2], 'wb')
    output.write(command_current[3])

    send_back_output(repr(listDirectoryFile))

elif command_current[0] == 'download':
    listDirectoryFile = {}
    listDirectoryFile['c'] = 'download'
    listDirectoryFile['arg1'] = command_current[1]
    listDirectoryFile['arg2'] = command_current[2]

    input = open(command_current[1], 'rb')
    listDirectoryFile['data'] = input.read()

    send_back_output(repr(listDirectoryFile))

elif command_current[0] == 'shell':
    listshell = {}
    listshell['c'] = 'shell'
    listshell['arg'] = command_current[1]
    send_back_output(repr(listshell))

elif command_current[0] == 'sleep':
    listSleep = {}
    listSleep['c'] = 'sleep'
```

Image Source: <http://nakedsecurity.sophos.com/2012/04/27/python-malware-mac/>

Windows Investigations

Incident
Response

Autoruns

Prefetch

Internet
History

Email

User
Accounts

Temporary
Directories

Log Analysis

Antivirus
Logs

Time
Stomping

Memory
Analysis

Malware
Reverse
Engineering

Incident Response

What

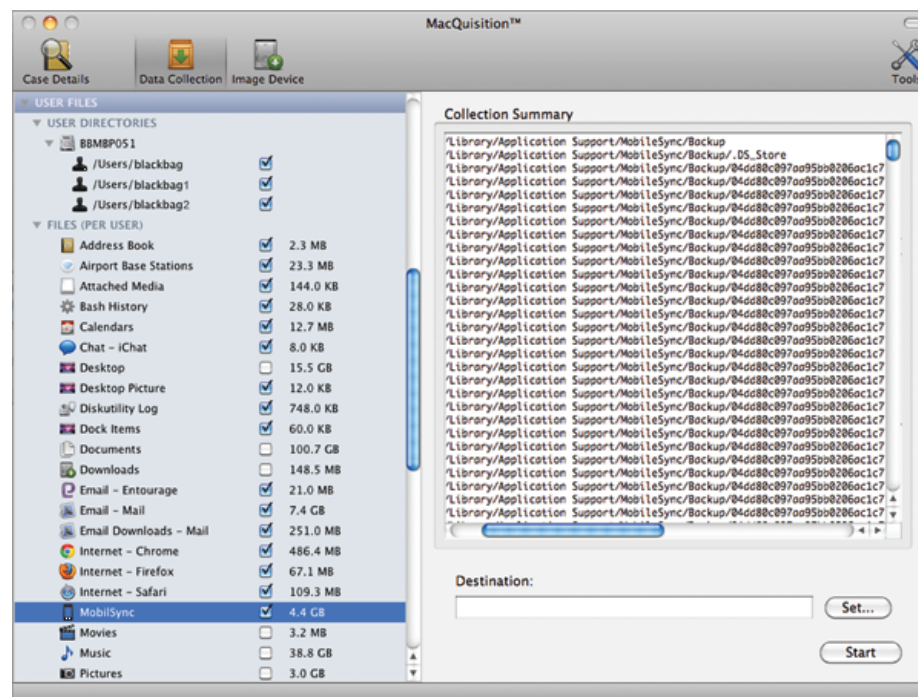
- System Information
- Network Data
- Users Logged On
- Running Processes
- Open Files
- Memory Analysis
- Other Tools

Why

- Collect Volatile Data
- Triage Analysis
- Dead-Box Analysis
- Encryption

Incident Response: MacQuisition by BlackBag

- Volatile Data
 - System Processes
 - Attached Media
 - Bash History
- Memory Acquisition
- HDD Acquisition too!



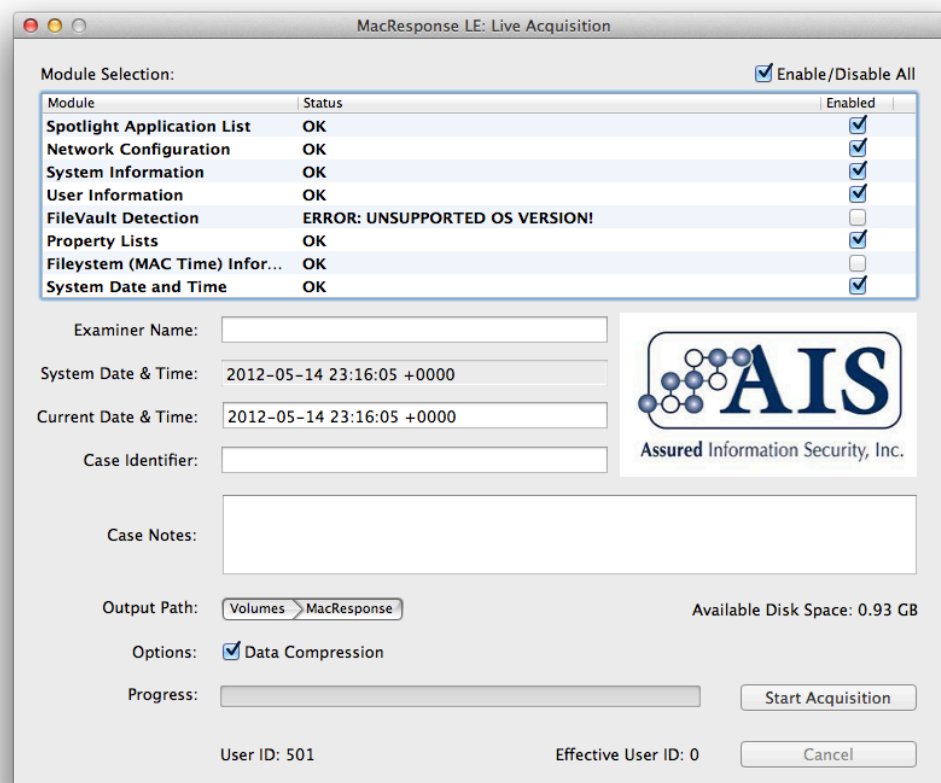
Incident Response: Mac Memory Reader (ATC-NY)

- Supports 10.4 – 10.7 32/64
- dd or Mach-O Formats
- <http://cybermarshal.com/index.php/cybermarshal-utilities/mac-memory-reader>

```
bit:MacMemoryReader oompa$ sudo ./MacMemoryReader -p ../lion_10_7_4.dd
Dumping memory regions:
available 0000000000000000-00000000000008e000 [WRITTEN]
ACPI_NVS 00000000000008f000-000000000000090000 [WRITTEN]
available 000000000000090000-0000000000000a0000 [WRITTEN]
LoaderData 000000000000010000-000000000000010e00 [WRITTEN]
available 000000000000010e00-000000000000020000 [WRITTEN]
LoaderData 000000000000020000-000000000000073200 [WRITTEN]
available 000000000000073200-000000000000080000 [WRITTEN]
LoaderData 000000000000080000-0000000000000257a000 [WRITTEN]
RT_data 0000000000000257a000-00000000000002583000 [WRITTEN]
RT_data 00000000000002583000-00000000000002585000 [WRITTEN]
RT_code 00000000000002585000-00000000000002589000 [WRITTEN]
RT_code 00000000000002589000-00000000000002590000 [WRITTEN]
RT_code 00000000000002590000-00000000000002593000 [WRITTEN]
RT_data 00000000000002593000-00000000000002594000 [WRITTEN]
RT_code 00000000000002594000-00000000000002596000 [WRITTEN]
RT_code 00000000000002596000-0000000000000259b000 [WRITTEN]
RT_data 0000000000000259b000-0000000000000259e000 [WRITTEN]
RT_data 0000000000000259e000-0000000000000259f000 [WRITTEN]
RT_data 0000000000000259f000-000000000000025b9000 [WRITTEN]
RT_code 000000000000025b9000-000000000000025ce000 [WRITTEN]
RT_data 000000000000025ce000-000000000000025cf000 [WRITTEN]
LoaderData 000000000000025cf000-000000000000025fc000 [WRITTEN]
available 000000000000025fc000-0000000000000a7095000 [.....] 41.0%
```


Incident Response: MacResponse by AIS

- App on USB Drive
- Captures:
 - System Information
 - Disk Information
 - User Information
 - Drivers
 - Login Sessions
 - Network Data
 - Processes
 - Screenshot
 - Application Data
 - FileVault Detection
 - Property Lists
 - RAM (10.7 not supported)
- macresponseforensics.com



Incident Response:

Make your own IR Live CD

- Blog: irhowto.wordpress.com
- “Creating a OS X Live IR CD-ROM”
- Step-by-Step Process & Scripts
 - Static Binaries
- Not foolproof
 - May not work on all systems

Incident Response: System Information

- date
- hostname
- uname -a
- sw_vers

```
bit:~ user$ date
Sun May 13 20:34:05 EDT 2012
bit:~ user$ hostname
bit
bit:~ user$ uname -a
Darwin bit 11.4.0 Darwin Kernel Version 11.4.0:
Mon Apr  9 19:32:15 PDT 2012;
root:xnu-1699.26.8~1/RELEASE_X86_64 x86_64
bit:~ user$ sw_vers
ProductName:      Mac OS X
ProductVersion:   10.7.4
BuildVersion:     11E53
```

Incident Response: Network Data

- `netstat -an`
- `lsof -i`

```
bit:~ user$ netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 192.168.1.101.60264     x.x.x.x.80             ESTABLISHED
tcp4    0      0 192.168.1.101.60252     x.x.x.x.443            ESTABLISHED
tcp4    37     0 192.168.1.101.60179     x.x.x.x.443            CLOSE_WAIT
tcp4    0      0 192.168.1.101.60094     x.x.x.x.993            ESTABLISHED
tcp4    37     0 192.168.1.101.59508     x.x.x.x.443            CLOSE_WAIT
tcp4    0      0 192.168.1.101.59437     x.x.x.x.993            ESTABLISHED
...
bit:~ user$ lsof -i
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE/OFF  NODE  NAME
loginwind  65  user   8u  IPv4  0xfffff8012574490  0t0  UDP  *:~
Mail      141  user  37u  IPv4  0xfffff80156e2320  0t0  TCP  bit:59432->mail.some.thing.com:imaps (ESTABLISHED)
Google    144  user   8u  IPv4  0xfffff8015f184e0  0t0  TCP  bit:59421->qc-in-f125.1e100.net:jabber-client (ESTABLISHED)
Google    144  user  59u  IPv4  0xfffff80238ada40  0t0  TCP  bit:60315->iad23s08-in-f0.1e100.net:http (ESTABLISHED)
Google    144  user  75u  IPv4  0xfffff801e1696c0  0t0  TCP  bit:60316->iad23s08-in-f15.1e100.net:http (ESTABLISHED)
iCal      149  user  17u  IPv4  0xfffff80156e1c00  0t0  TCP  bit:49257->17.172.116.48:https (CLOSE_WAIT)
iCal      149  user  20u  IPv4  0xfffff8015f18c00  0t0  TCP  bit:49267->17.164.0.48:https (CLOSE_WAIT)
SystemUIS 153  user   8u  IPv4  0xfffff8012576f28  0t0  UDP  *:~
Finder    155  user  12u  IPv4  0xfffff8012575340  0t0  UDP  *:~
Finder    155  user  26u  IPv4  0xfffff80156e5500  0t0  TCP  localhost:57669->localhost:26164 (ESTABLISHED)
imagent   204  user   7u  IPv4  0xfffff80221f0dd8  0t0  UDP  localhost:53912->localhost:53912
Dropbox   247  user  15u  IPv4  0xfffff8015717500  0t0  TCP  bit:59418->sjc-not18.sjc.dropbox.com:http (ESTABLISHED)
```

Incident Response: Network Data – Routing Table

◉ netstat -rn

```
bit:~ user$ netstat -rn
Routing tables
```

Internet:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	192.168.1.254	UGSc	42	0	en1	
127	127.0.0.1	UCS	0	0	lo0	
127.0.0.1	127.0.0.1	UH	4	6677585	lo0	
169.254	link#5	UCS	1	0	en1	
169.254.204.125	b8:c7:5d:cc:5:80	UHLW	0	7	en1	
172.16.152/24	link#9	UC	2	0	vmnet8	
172.16.152.255	ff:ff:ff:ff:ff:ff	UHLWbI	0	1	vmnet8	
172.16.243/24	link#8	UC	2	0	vmnet1	
172.16.243.255	ff:ff:ff:ff:ff:ff	UHLWbI	0	1	vmnet1	
192.168.1	link#5	UC	5	0	en1	
192.168.1.1	c0:3f:e:8c:59:59	UHLWii	0	186	en1	900
192.168.1.101	127.0.0.1	UHS	0	0	lo0	
192.168.1.133	3c:7:54:3:65:20	UHLWii	1	2886	en1	1109
192.168.1.241	68:9:27:32:15:9c	UHLWii	0	0	en1	1085

Internet6:

Destination	Gateway	Flags	Netif	Expire
::1	link#1	UHL	lo0	
fe80::%lo0/64	fe80::1%lo0	UcI	lo0	
fe80::1%lo0	link#1	UHLI	lo0	
fe80::%en1/64	link#5	UCI	en1	
fe80::9227:e4ff:fef8:e65f%en1	90:27:e4:f8:e6:5f	UHLI	lo0	
fe80::bac7:5dff:fecc:580%en1	b8:c7:5d:cc:5:80	UHLWii	en1	

...

Incident Response: Network Data – ARP Table

- arp -an
- ifconfig

```
bit:~ user$ arp -an
? (169.254.204.125) at b8:c7:5d:cc:5:80 on enl [ethernet]
? (172.16.152.255) at ff:ff:ff:ff:ff:ff on vmnet8 ifscope [ethernet]
? (172.16.243.255) at ff:ff:ff:ff:ff:ff on vmnet1 ifscope [ethernet]
? (192.168.1.1) at c0:3f:e:8c:59:59 on enl ifscope [ethernet]
? (192.168.1.133) at 3c:7:54:3:65:20 on enl ifscope [ethernet]
? (192.168.1.241) at 68:9:27:32:15:9c on enl ifscope [ethernet]
? (192.168.1.254) at e0:69:95:50:4c:6 on enl ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on enl ifscope [ethernet]
...
bit:~ user$ ifconfig
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=2b<RXCSUM,TXCSUM,VLAN_HWTAGGING,TSO4>
    ether c4:2c:03:09:ca:fd
    media: autoselect (none)
    status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 90:27:e4:f8:e6:5f
    inet6 fe80::9227:e4ff:fef8:e65f%en1 prefixlen 64 scopeid 0x5
    inet 192.168.1.101 netmask 0xffffffff broadcast 192.168.1.255
    media: autoselect
    status: active
```

Incident Response: Open Files

• lsof

```
bit:~ user$ lsof
COMMAND  PID  USER  FD      TYPE  DEVICE  SIZE/OFF      NODE NAME
loginwind  65  user   cwd     DIR   14,4      1156         2 /
loginwind  65  user   txt     REG   14,4    1421280    501728 /System/Library/CoreServices/loginwindow.app/Contents/MacOS/
loginwindow
loginwind  65  user   txt     REG   14,4    118384    424796 /System/Library/LoginPlugins/FSDisconnect.loginPlugin/Contents/
MacOS/FSDisconnect
loginwind  65  user   txt     REG   14,4     19328    281526 /private/var/folders/xq/yjffvqj90s313s17vy12w7nr0000gn/C/
com.apple.scriptmanager.le.cache
loginwind  65  user   txt     REG   14,4     17284     27515 /System/Library/PrivateFrameworks/CoreWLANKit.framework/Versions/A/
Resources/AirPort3.pdf
...
Mail      141  user   41u     REG   14,4    1806336    604815 /Users/user/Library/Caches/com.apple.mail/Cache.db
Mail      141  user   42w     REG   14,4     20748    282135 /Users/user/Library/Logs/Sync/syncservices.log
Mail      141  user   43u     REG   14,4     40960    629603 /Users/user/Library/Application Support/AddressBook/MailRecents-
v4.abcdmr
...
Google    144  user   txt     REG   14,4    270336    769873 /Users/user/Library/Caches/Google/Chrome/Default/Media Cache/data_1
Google    144  user   txt     REG   14,4      8192    769874 /Users/user/Library/Caches/Google/Chrome/Default/Media Cache/data_2
Google    144  user   txt     REG   14,4      8192    769875 /Users/user/Library/Caches/Google/Chrome/Default/Media Cache/data_3
```

Incident Response: Users Logged On

- who -a

- w

```
bit:~ user$ who -a
reboot    ~           May 12 11:32 00:14      1
user      console    May 12 11:32 old        65
user      ttys000     May 12 11:33 .          189
user      ttys001     May 13 11:38 09:29     3199
user      ttys002     May 13 20:48 .          8781
user      ttys003     May 13 20:55 00:14     8850
.          run-level 3
bit:~ user$ w
21:10 up 1 day,  9:38, 5 users, load averages: 1.06 1.55 1.81
USER      TTY      FROM          LOGIN@  IDLE WHAT
user      console -              Sat11   33:37 -
user      s000     -              Sat11   - w
user      s001     -              11:38   9:29 more
user      s002     -              20:48   - /usr/bin/less -is
user      s003     -              20:55   14 -bash
```


Incident Response: Running Processes

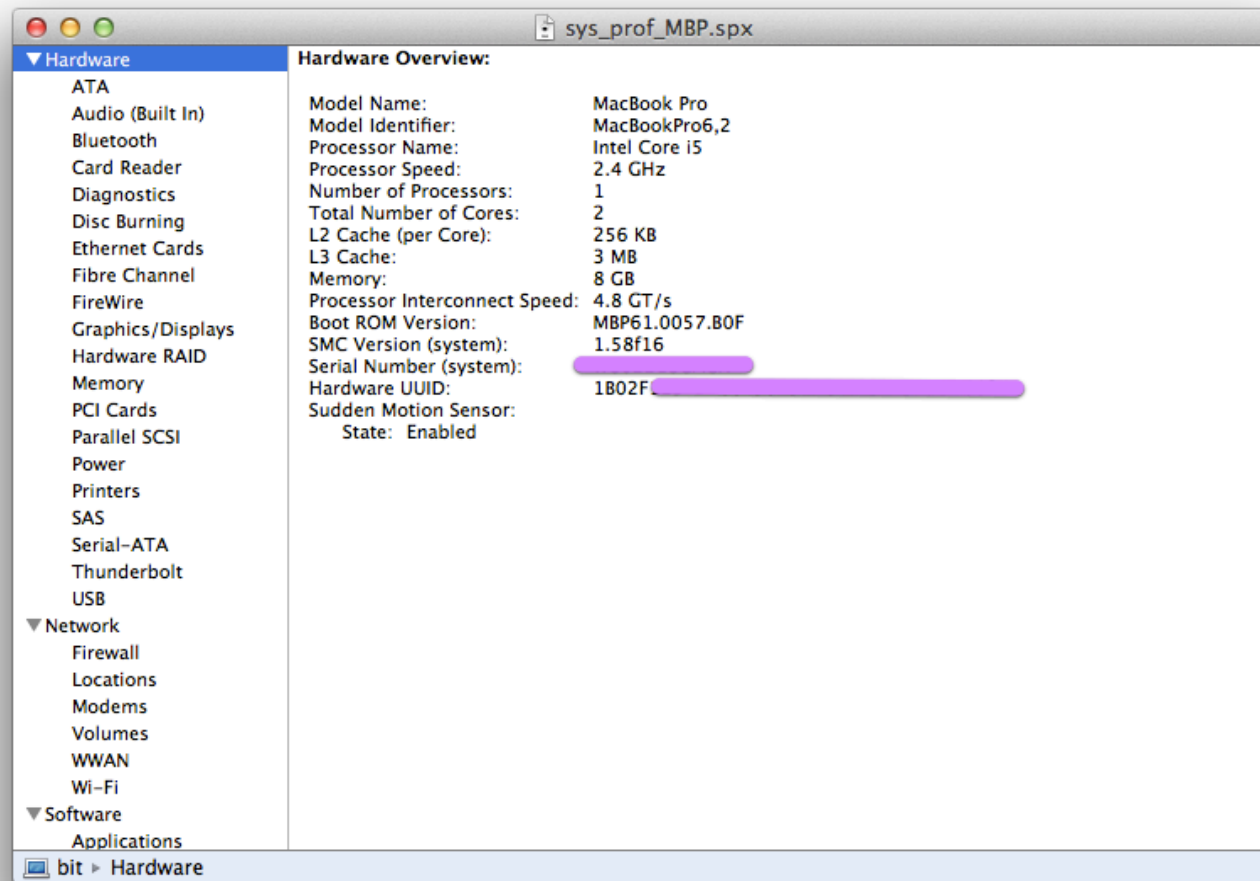
● ps aux

```
bit:~ user$ ps aux
USER   PID   %CPU %MEM    VSZ   RSS  TT  STAT  STARTED      TIME COMMAND
user   143    1.2   0.8 2649292 62964  ??   R    Sat11AM    0:45.27 /Applications/Utilities/
Terminal.app/Contents/MacOS/Terminal -psn_0_36873
user   148    1.0   0.9 4009924 72300  ??   S    Sat11AM    9:43.59 /Applications/iChat.app/
Contents/MacOS/iChat -psn_0_57358
user   6851   0.9   1.2 944492 98236  ??   S      7:06PM    3:56.95 /Applications/Evernote.app/
Contents/MacOS/Evernote -psn_0_12458977
_windowserver 102    0.8   2.3 3456288 194720  ??  Ss    Sat11AM   35:09.10 /System/Library/
Frameworks/user
6700    0.2   user   145    0.1   1.1 1095472 93940  ??   S    Sat11AM
5:25.76 /Applications/Microsoft Office 2011/Microsoft Word.app/Contents/MacOS/Microsoft Word -
psn_0_45067
user   8945    0.0   0.0 2434848    596 s002  S+    9:09PM    0:00.01 man who
user   8851    0.0   0.0 2435492    1124 s003  S+    8:55PM    0:00.01 -bash
root   8850    0.0   0.0 2466544    2076 s003  Ss    8:55PM    0:00.02 login -pf user
user   8800    0.0   0.4 2503560 31720  ??   SN    8:49PM    0:02.62 /System/Library/Frameworks/user
8782    0.0   0.0 2435492    1128 s002  S     8:48PM    0:00.02 -bash
root   8781    0.0   0.0 2458352    2040 s002  Ss    8:48PM    0:00.12 login -pf user
```

Incident Response: System Profiler

- `system_profiler -xml -detaillevel full > /Volume/IR_CASE/sys_prof_MBP.spx`
- Open in "System Information.app"
- Contains:
 - Hardware Information
 - USB Information
 - Network Information
 - Firewall Settings
 - Mounted Volumes
 - System Information
 - Applications
 - Kernel Extensions
 - Log Data

Incident Response: System Profiler



Memory Analysis

What

- Volafix
- Volatility

Why

- Volatile Data
 - Network Connections
 - Open Files
 - Kernel Extensions
 - Running Processes

Memory Analysis: Volafox

- <http://code.google.com/p/volafox>
- Mach-O Image from Mac Memory Reader => Volafox's flattypy.py
- Download from source for latest updates.

```
bit:volafox-read-only oompa$ python flatten.py ../lion_10_7_4.macho ../lion_10_7_4.flat
Copying: available 0000000000000000 0000000000000008e
Copying: ACPI_NVS 0000000000008f00 0000000000000001
Copying: available 0000000000009000 0000000000000010
Copying: LoaderData 0000000000010000 000000000000000e
Copying: available 0000000000010e00 00000000000000f2
Copying: LoaderData 0000000000020000 0000000000000532
```

Memory Analysis: Volafox

- System Information
- Processes
- Open Files
- Kernel Extensions
- Syscall Table
- Network Connections

```
bit:volafox-read-only oompa$ python vol.py -i /Volumes/WDPassport/lion_10_7_3.flat -o ps
[+] Process List
OFFSET(P)      PID  PPID  PRIORITY  NICE    PROCESS_NAME      USERNAME  CREATE_TIME (GMT +0)
0x00BCCB80      0    0      0         0      kernel_task        Fri Apr 06 20:42:50 2012
0x00BCC300      1    0     128       0      launchd           _atsserver Fri Apr 06 20:42:50 2012
0x00BCDA80     10    1     128       0      kextd             root     Fri Apr 06 20:43:11 2012
0x00BCDEC0     11    1     128       0      UserEventAgent    root     Fri Apr 06 20:43:11 2012
0x00BCD640     12    1     255       0      mDNSResponder     _mdnsresponder Fri Apr 06 20:43:11 2012
0x00BCD200     13    1     255       0      opendirectoryd    _mdnsresponder Fri Apr 06 20:43:11 2012
0x00BCEDC0     14    1     128       0      fseventsd         _mdnsresponder Fri Apr 06 20:43:11 2012
0x00BCE980     15    1     128       0      notifyd           _mdnsresponder Fri Apr 06 20:43:11 2012
0x00BCE540     16    1     128       0      syslogd           _mdnsresponder Fri Apr 06 20:43:11 2012
0x00BCFCC0     17    1     128       0      configd           _mdnsresponder Fri Apr 06 20:43:24 2012
```

Memory Analysis: Volaflox

```
bit:volafox-read-only oompa$ python vol.py -i ../lion_10_7_3.flat -o kextstat
[+] Kernel Extention List
```

OFFSET(P)	INFO	KID	KEXT_NAME	VERSION
0x13672C120	1	140	com.atc-ny.devmem	1.0.0d1
0x1D159A9F0	1	137	com.apple.driver.iPodSBCDriver	1.6.0
0x1BE812E20	1	135	com.apple.driver.AppleUSBMergeNub	4.5.3
0x254F7CD60	1	132	com.apple.filesystems.afpfs	9.8
0x25C931600	1	131	com.apple.security.SecureRemotePassword	1.0
0x16A1FA1D0	1	130	com.apple.nke.asp_tcp	6.0.1
0x08079970	1	129	com.apple.filesystems.smbfs	1.7.0
0x14DA56120	1	123	com.apple.driver.AppleProfileTimestampAction	85.2
0x14E123130	1	122	com.apple.driver.AppleProfileThreadInfoAction	85.2

```
bit:volafox-read-only oompa$ python vol.py -i ../lion_10_7_3.flat -o netstat
[+] NETWORK INFORMATION (hashbase)
```

[TCP] Local Address: 0.0.0.0:22, Foreign Address: 0.0.0.0:0, flag: 8000

[TCP] Local Address: 0.0.0.0:88, Foreign Address: 0.0.0.0:0, flag: 8000

[TCP] Local Address: 192.168.1.133:56742, Foreign Address: 207.8.65.20:80, flag: 40008000

[TCP] Local Address: 192.168.1.133:56743, Foreign Address: 207.8.65.20:80, flag: 40008000

[TCP] Local Address: 0.0.0.0:0, Foreign Address: 0.0.0.0:0, flag: 8000

[TCP] Local Address: 192.168.1.133:64945, Foreign Address: 204.245.162.41:80, flag: 40008000

[TCP] Local Address: 192.168.1.133:56704, Foreign Address: 199.47.217.177:443, flag: 40008000

[TCP] Local Address: 127.0.0.1:631, Foreign Address: 0.0.0.0:0, flag: 8000

[TCP] Local Address: 192.168.1.133:56844, Foreign Address: 72.36.210.254:80, flag: 40008000

[TCP] Local Address: 192.168.1.133:56748, Foreign Address: 74.125.228.3:443, flag: 40008000

Memory Analysis: Volatility

- Currently Windows & Linux Systems
- Will have Mac support:
 - Processes
 - Network Information
 - Open Files
 - File System Data

Mac Autoruns

What

- XPC Services
- Launch Daemons & Agents
- LoginItems
- StartupItems
- Login/Logout Scripts

Why

- Persistence
- Persistence
- Persistence

Autoruns: XPC Services

- ◉ Privilege Separation & Stability
- ◉ Sandboxed Environment
- ◉ Runs in user context
- ◉ Services a single application
- ◉ Location:
 - ◉ Application Bundle: /Contents/XPCServices/
 - ◉ /System/Library/XPCServices/

Autoruns: XPC Services Example

Key	Type	Value
BuildMachineOSBuild	String	11D17a
Localization native development region	String	English
Executable file	String	com.apple.qtkitserver
Bundle identifier	String	com.apple.qtkitserver
InfoDictionary version	String	6.0
Bundle name	String	com.apple.qtkitserver
Bundle OS Type code	String	XPC!
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
Bundle version	String	1
DTCompiler	String	
DTPlatformBuild	String	11D17a
DTPlatformVersion	String	GM
DTSDKBuild	String	11D17a
DTSDKName	String	
DTXcode	String	0410
DTXcodeBuild	String	11D17a
Application is agent (UIElement)	Boolean	YES
▼ XPCService	Diction...	(2 items)
▼ EnvironmentVariables	Diction...	(1 item)
MallocCorruptionAbort	String	1
ServiceType	String	Application

Autoruns:

Launch Agents & Daemons

- ◉ Preferred Method
- ◉ Introduced in 10.4 (w/launchd)
- ◉ Property List File
- ◉ Popular with current Mac malware
- ◉ Reference: TN2083

Autoruns: Launch Agents

- Agent – Background User Process
 - Can access user home directory
 - May have GUI (limited, if at all)
- Location:
 - /System/Library/LaunchAgents/
 - /Library/LaunchAgents/
 - ~/Library/LaunchAgents

Autoruns: Launch Agents Examples

```
com.apple.AOSNotificationOSX.plist
com.apple.AddressBook.SourceSync.plist
com.apple.AddressBook.abd.plist
com.apple.AirPortBaseStationAgent.plist
com.apple.AppStoreUpdateAgent.plist
com.apple.AppleGraphicsWarning.plist
com.apple.BezeUI.plist
com.apple.CoreLocationAgent.plist
com.apple.DictionaryPanelHelper.plist
com.apple.DiskArbitrationAgent.plist
com.apple.Dock.plist
com.apple.FTCleanup.plist
com.apple.FileSyncAgent.PHD.plist
com.apple.FileSyncAgent.iDisk.plist
com.apple.Finder.plist
com.apple.FontRegistryUIAgent.plist
com.apple.FontValidator.plist
com.apple.FontValidatorConduit.plist
com.apple.FontWorker.plist
com.apple.KerberosHelper.LKDCHelper.plist
com.apple.LaunchServices.lsboxd.plist
com.apple.NetworkDiagnostics.plist
com.apple.PCIESlotCheck.plist
com.apple.PreferenceSyncAgent.plist
com.apple.PubSub.Agent.plist
com.apple.ReclaimSpaceAgent.plist
com.apple.RemoteDesktop.plist
com.apple.ReportCrash.Self.plist
com.apple.ReportCrash.plist
com.apple.ReportGPURestart.plist
com.apple.ReportPanic.plist
com.apple.ScreenReaderUIServer.plist
com.apple.ServiceManagement.LoginItems.plist
com.apple.SubmitDiagInfo.plist
```

```
com.apple.SystemUIServer.plist
com.apple.TMLaunchAgent.plist
com.apple.TrustEvaluationAgent.plist
com.apple.UserEventAgent-Aqua.plist
com.apple.UserEventAgent-LoginWindow.plist
com.apple.UserNotificationCenterAgent-LoginWindow.plist
com.apple.UserNotificationCenterAgent.plist
com.apple.VoiceOver.plist
com.apple.WebKit.PluginAgent.plist
com.apple.ZoomWindow.plist
com.apple.alf.useragent.plist
com.apple.aos.migrate.plist
com.apple.bluetoothUIServer.plist
com.apple.btsa.plist
com.apple.cfnetwork.AuthBrokerAgent.plist
com.apple.cookiec.plist
com.apple.coredata.externalrecordswriter.plist
com.apple.coreservices.appleid.authentication.plist
com.apple.coreservices.uiagent.plist
com.apple.csuseragent.plist
com.apple.cvmsCompAgent_i386.plist
com.apple.cvmsCompAgent_x86_64.plist
com.apple.distnoted.xpc.agent.plist
com.apple.familycontrols.useragent.plist
com.apple.findmymacmessenger.plist
com.apple.fondd.useragent.plist
com.apple.gssd-agent.plist
com.apple.helpd.plist
com.apple.iCalPush.plist
com.apple.iChat.Theater.plist
com.apple.imagent.plist
com.apple.imklaunchagent.plist
com.apple.imtranscoderagent.plist
com.apple.imtransferagent.plist
```

Autoruns: Launch Agents Examples

Key	Type	Value
▼ ProgramArguments	Array	(1 item)
Item 0	String	/System/Library/PrivateFrameworks/IMCore.framework/imagent.app/Contents/MacOS/imagent
▼ KeepAlive	Diction...	(1 item)
SuccessfulExit	Boolean	NO
Label	String	com.apple.imagent
▼ MachServices	Diction...	(1 item)
▼ com.apple.imagent.desktop.auth	Diction...	(1 item)
ResetAtClose	Boolean	YES
▼ EnvironmentVariables	Diction...	(1 item)
NSRunningFromLaunchd	String	1

Key	Type	Value
Label	String	org.openbsd.ssh-agent
▼ ProgramArguments	Array	(2 items)
Item 0	String	/usr/bin/ssh-agent
Item 1	String	-l
ServiceIPC	Boolean	YES
▼ Sockets	Diction...	(1 item)
▼ Listeners	Diction...	(1 item)
SecureSocketWithKey	String	SSH_AUTH_SOCK
EnableTransactions	Boolean	YES

Key	Type	Value
Label	String	com.apple.bluetoothUIServer
▼ MachServices	Diction...	(1 item)
com.apple.bluetoothUIServer	Boolean	YES
Program	String	/System/Library/CoreServices/BluetoothUIServer.app/Contents/MacOS/BluetoothUIServer
LimitLoadToSessionType	String	Aqua

Autoruns:

Launch Agents – Session Types

Name	Session Type	Notes
GUI launchd agent	Aqua	Access to GUI Services (login item) - App Store Update - Screen Sharing
Non-GUI launchd agent	StandardIO	Runs only in non-GUI login sessions (i.e. SSH)
Per-user launchd agent	Background	Runs in context that is the parent of all contexts for a given user - mdworker (metadata)
Pre-login launchd agent	LoginWindow	Runs in the loginwindow context - Find My Mac

Autoruns: Launch Daemons

- Daemon – Background System Process
- Location:
 - /System/Library/LaunchDaemons
 - /Library/LaunchDaemons

Autoruns: Launch Daemons Example

Fri Apr 13 03:15:00 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:

Filesystem	Size	Used	Avail	Capacity
/dev/disk1	698Gi	431Gi	267Gi	62%
localhost:/YNU-3NIWZFYxg8rbEgggLJ	698Gi	698Gi	0Bi	100%

Network interface status:

Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs
lo0	16384	<Link#1>		38376	0	38376	0
lo0	16384	localhost	fe80::1::1	38376	-	38376	-
lo0	16384	127	localhost	38376	-	38376	-
lo0	16384	ip6-localhost	::1	38376	-	38376	-
gif0*	1280	<Link#2>		0	0	0	0
stf0*	1280	<Link#3>		0	0	0	0
en0	1500	<Link#4>	c4:2c:03:09:ca:fd	0	0	0	0
en1	1500	<Link#5>	90:27:e4:f8:e6:5f	37611065	0	105742931	0
en1	1500	bit.local	fe80::5:9227:e4ff	37611065	-	105742931	-
en1	1500	192.168.1	bit	37611065	-	105742931	-
fw0	4078	<Link#6>	e8:06:88:ff:fe:d5:5d:08	0	0	0	0
p2p0	2304	<Link#7>	02:27:e4:f8:e6:5f	0	0	0	0
vmnet	1500	<Link#8>	00:50:56:c0:00:01	0	0	0	0
vmnet	1500	172.16.73/24	172.16.73.1	0	-	0	-
vmnet	1500	<Link#9>	00:50:56:c0:00:08	0	0	0	0
vmnet	1500	192.168.158	192.168.158.1	0	-	0	-

Local system status:

3:15 up 3 days, 8:06, 4 users, load averages: 0.55 0.57 0.56

-- End of daily output --

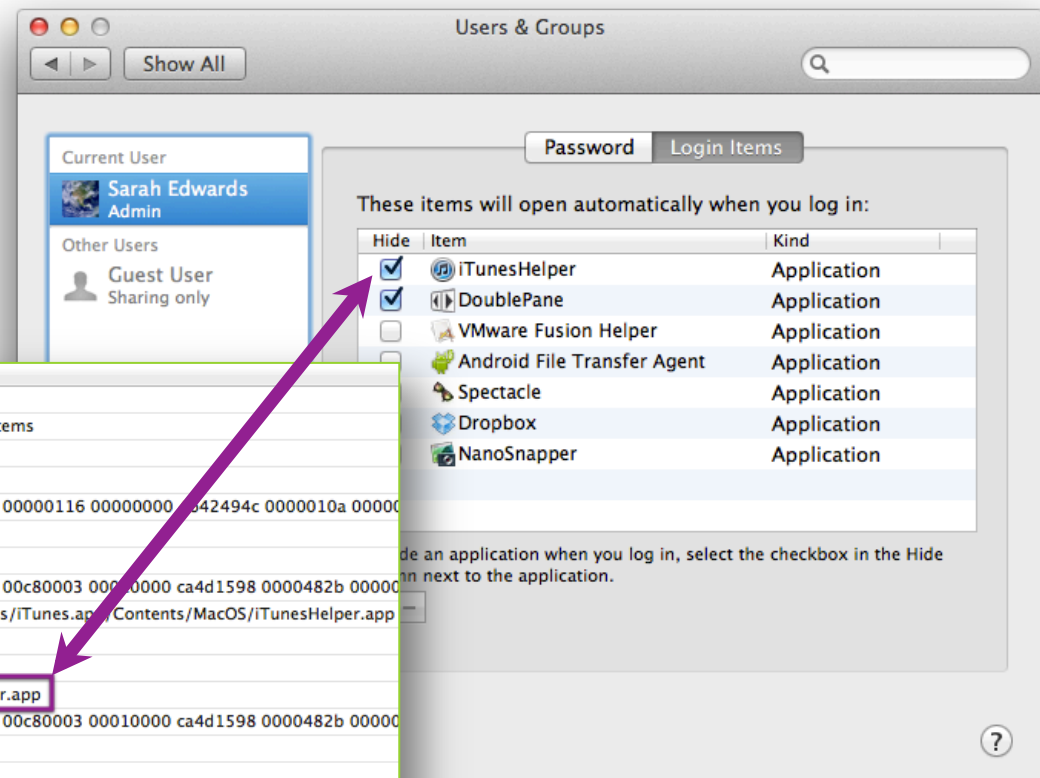
Key	Type	Value
Label	String	com.apple.periodic-daily
▼ ProgramArguments	Array	(2 items)
Item 0	String	/usr/sbin/periodic
Item 1	String	daily
LowPriorityIO	Boolean	YES
Nice	Number	1
▼ StartCalendarInterval	Diction...	(2 items)
Hour	Number	3
Minute	Number	15
AbandonProcessGroup	Boolean	YES

Autoruns: LoginItems

- Launched when user logs into system via GUI
- Location:
 - ~/Library/Preferences/com.apple.loginitems.plist
 - <application>.app/Contents/Library/LoginItems/

Autoruns: LoginItems Example

Key	Type	Value
▼ SessionItems	Diction...	(2 items)
Controller	String	CustomListItems
▼ CustomListItems	Array	(7 items)
▼ Item 0	Diction...	(4 items)
Icon	Data	<496d6752 00000116 00000000 0042494c 0000010a 00000000>
▼ CustomItemProperties	Diction...	(2 items)
▼ com.apple.loginitem.legacyprefs	Diction...	(3 items)
AliasData	Data	<00000000 00c80003 00000000 ca4d1598 0000482b 00000000>
Path	String	/Applications/iTunes.app/Contents/MacOS/iTunesHelper.app
Hide	Boolean	YES
com.apple.loginitem.HideOnLaunch	Boolean	YES
Name	String	iTunesHelper.app
Alias	Data	<00000000 00c80003 00010000 ca4d1598 0000482b 00000000>
▶ Item 1	Diction...	(4 items)
▶ Item 2	Diction...	(4 items)
▶ Item 3	Diction...	(4 items)
▶ Item 4	Diction...	(4 items)
▶ Item 5	Diction...	(4 items)
▶ Item 6	Diction...	(4 items)



Autoruns: Deprecated Methods

/etc/crontab

- Still supported, not recommended

Login/Logout Hooks Deprected as of 10.6

- Run as root
- Com.apple.loginwindow.plist – LoginHook/LogoutHook Keys

Startup Item Deprecated as of 10.4

- /Library/StartupItems
- /System/Library/StartupItems

mach_init Daemon Deprecated as of 10.5

- Property List File in /etc/mach_init.d

mach_init Agent Deprecated as of 10.5

- Property List file in /etc/mach_init_per_user.d/

inetd/xinetd Daemon Deprecated as of 10.4

- Line in /etc/inetd.conf
- Config file in /etc/xinetd.d/

System Login Item Deprecated as of 10.5

- Replaced with pre-login launchd agent.

Autoruns: Malware Examples

Flashback

- ~/Library/LaunchAgents/com.java.update.plist
- References .jupdate in user's home directory.

Imuler

- ~/Library/LaunchAgents/checkvir.plist
- References checkvir file in same directory.

SabPub

- ~/Library/LaunchAgents/com.apple.PubSabAgent.plist
- References ~/Library/Preferences/com.apple.PubSabAgent.pfile

MacControl

- ~/Library/LaunchAgents/com.apple.FolderActionsxl.plist
- References ~/Library/launched
- "MacControl"

Internet History

What

- Browsers
 - Safari
 - Chrome
 - FireFox

Why

- Temporary Internet Files
- Cache Files
- Downloads
- Search History

Internet History: Preferences

Safari

- ~/Library/Preferences/com.apple.Safari.plist
- Default Downloads Directory
- Recent Searches

Chrome

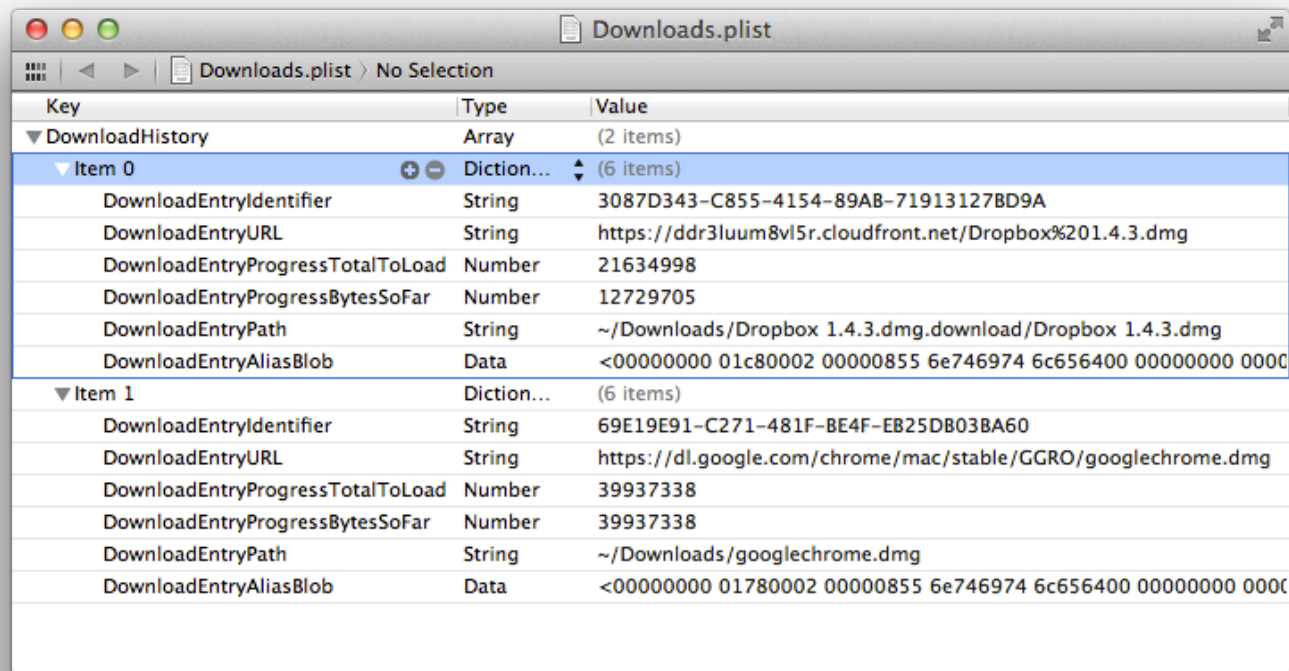
- ~/Library/Application Support/Google/Chrome/Default/Preferences
- JSON Formatted File
- Downloads Directory in "download" section

FireFox

- ~/Library/Application Support/Firefox/Profiles/*****.default/prefs.js
- "browser.download.dir"

Internet History: Safari - Downloads

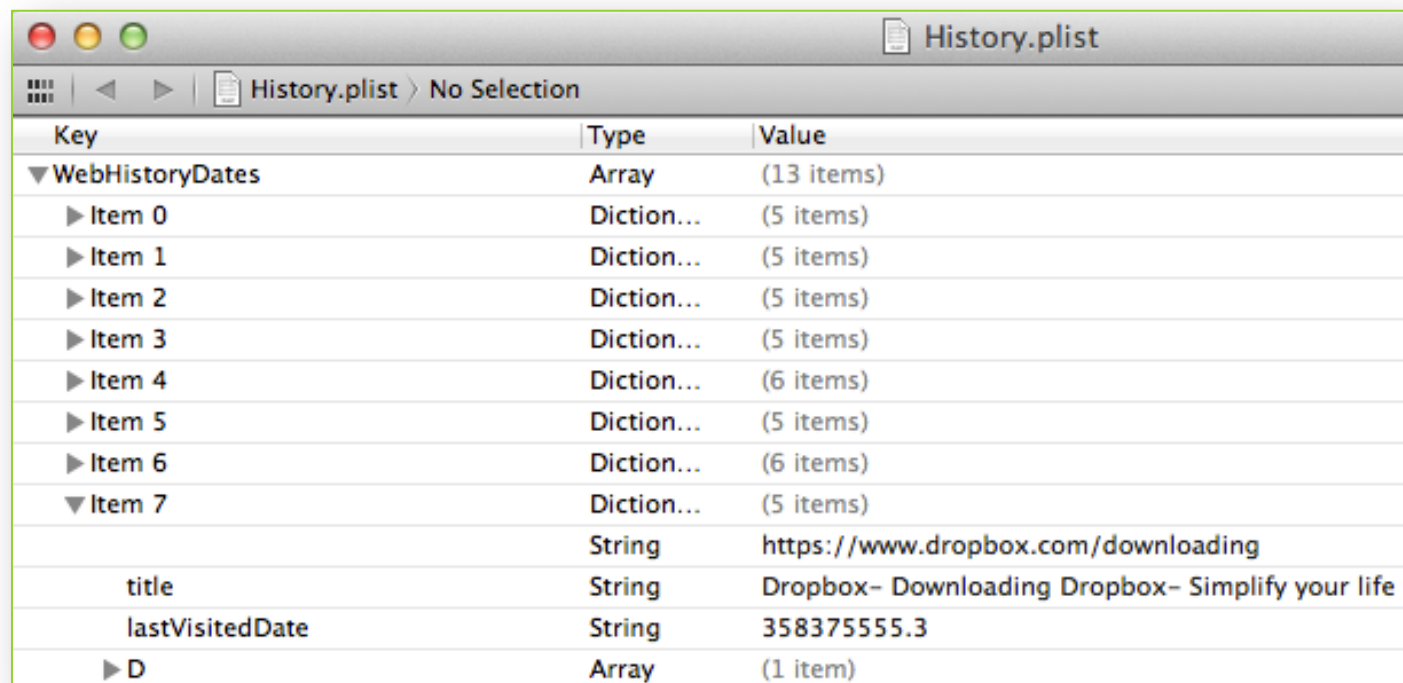
- ~/Library/Safari/Downloads.plist



Key	Type	Value
▼ DownloadHistory	Array	(2 items)
▼ Item 0	Diction...	(6 items)
DownloadEntryIdentifier	String	3087D343-C855-4154-89AB-71913127BD9A
DownloadEntryURL	String	https://ddr3luum8vl5r.cloudfront.net/Dropbox%201.4.3.dmg
DownloadEntryProgressTotalToLoad	Number	21634998
DownloadEntryProgressBytesSoFar	Number	12729705
DownloadEntryPath	String	~/Downloads/Dropbox 1.4.3.dmg.download/Dropbox 1.4.3.dmg
DownloadEntryAliasBlob	Data	<00000000 01c80002 00000855 6e746974 6c656400 00000000 00000000 00000000>
▼ Item 1	Diction...	(6 items)
DownloadEntryIdentifier	String	69E19E91-C271-481F-BE4F-EB25DB03BA60
DownloadEntryURL	String	https://dl.google.com/chrome/mac/stable/GGRO/googlechrome.dmg
DownloadEntryProgressTotalToLoad	Number	39937338
DownloadEntryProgressBytesSoFar	Number	39937338
DownloadEntryPath	String	~/Downloads/googlechrome.dmg
DownloadEntryAliasBlob	Data	<00000000 01780002 00000855 6e746974 6c656400 00000000 00000000 00000000>

Internet History: Safari - History

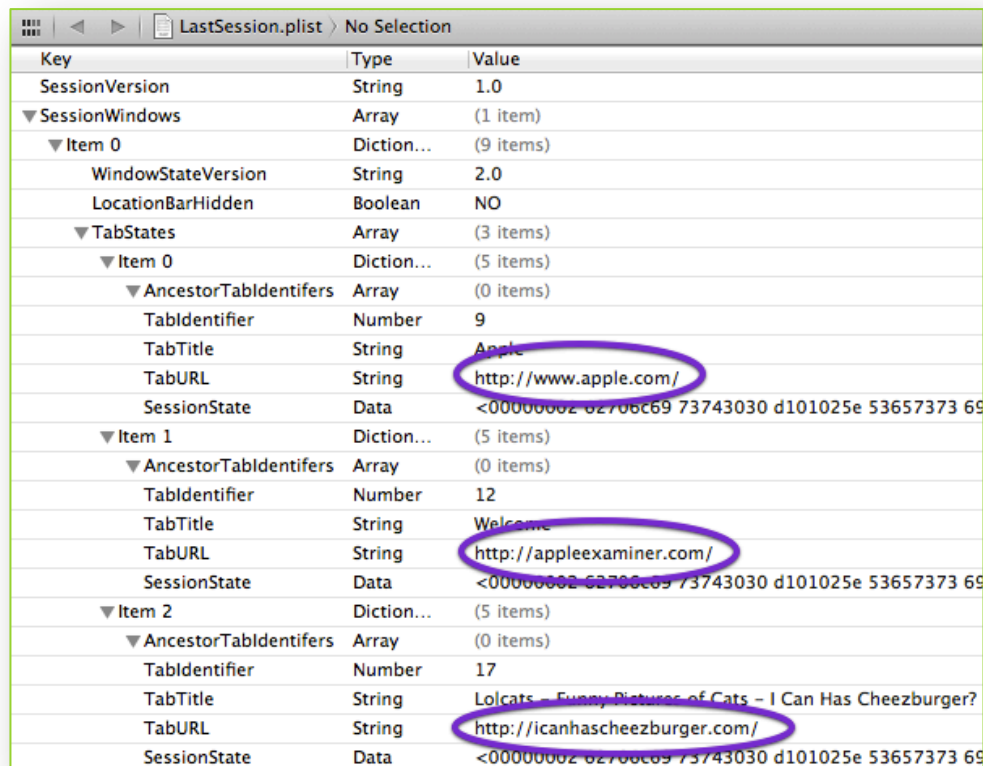
- ~/Library/Safari/History.plist



Key	Type	Value
▼ WebHistoryDates	Array	(13 items)
▶ Item 0	Diction...	(5 items)
▶ Item 1	Diction...	(5 items)
▶ Item 2	Diction...	(5 items)
▶ Item 3	Diction...	(5 items)
▶ Item 4	Diction...	(6 items)
▶ Item 5	Diction...	(5 items)
▶ Item 6	Diction...	(6 items)
▼ Item 7	Diction...	(5 items)
	String	https://www.dropbox.com/downloading
title	String	Dropbox- Downloading Dropbox- Simplify your life
lastVisitedDate	String	358375555.3
▶ D	Array	(1 item)

Internet History: Safari – Last Session

- ~/Library/Safari/LastSession.plist

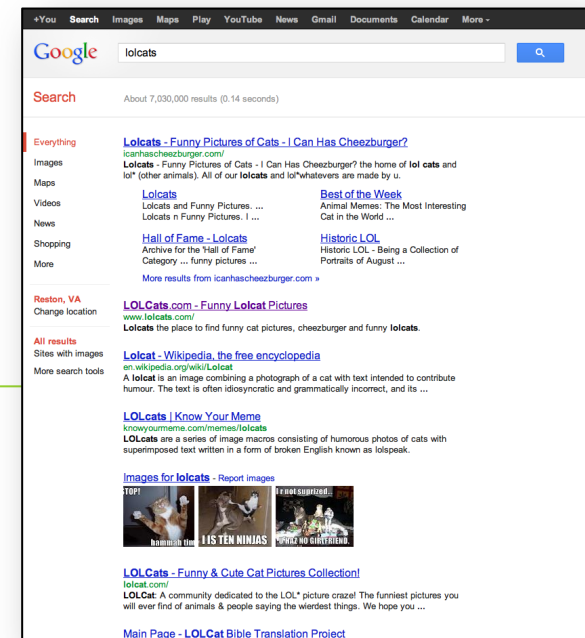


Key	Type	Value
SessionVersion	String	1.0
SessionWindows	Array	(1 item)
▼ Item 0	Diction...	(9 items)
WindowStateVersion	String	2.0
LocationBarHidden	Boolean	NO
▼ TabStates	Array	(3 items)
▼ Item 0	Diction...	(5 items)
▼ AncestorTabIdentifiers	Array	(0 items)
TabIdentifier	Number	9
TabTitle	String	Apple
TabURL	String	http://www.apple.com/
SessionState	Data	<00000002-62706c69-73743030-d101025e-53657373 69>
▼ Item 1	Diction...	(5 items)
▼ AncestorTabIdentifiers	Array	(0 items)
TabIdentifier	Number	12
TabTitle	String	Welcome
TabURL	String	http://appleexaminer.com/
SessionState	Data	<00000002-62706c69-73743030-d101025e-53657373 69>
▼ Item 2	Diction...	(5 items)
▼ AncestorTabIdentifiers	Array	(0 items)
TabIdentifier	Number	17
TabTitle	String	Lolcats - Funny Pictures of Cats - I Can Has Cheezburger?
TabURL	String	http://icanhascheezburger.com/
SessionState	Data	<00000002-62706c69-73743030-d101025e-53657373 69>

Internet History: Safari - Cache

~/Library/Caches/com.apple.Safari/
Webpage Previews/

- Directory containing JPEG & PNG images of webpages.
- May be used to see a webpage taken from a snapshot in time.



~/Library/Caches/com.apple.Safari/Cache.db

- SQLite Database
- Contains download cache files.
- Files with originating location and download date.
- May contain evidence of malicious code, redirects, phishing, etc.

Internet History:

Chrome – Internet History

~/Library/Application Support/Google/Chrome/Default/History

- SQLite Database

History

- 'urls' Table
- 'visits' Table

Downloads

- 'downloads' Table

Search History

- 'keyword_search_terms' Table

Internet History: Chrome - Cache

- ~/Library/Caches/Google/Chrome/Default/Cache/
- “data_#” index – “Chromium Disk Cache”

```
bit:Cache oompa$ pwd
/Users/oompa/Library/Caches/Google/Chrome/Default/Cache
bit:Cache oompa$ file * | more
data_0:  data
data_1:  data
data_2:  data
data_3:  data
data_4:  data
f_00000b: gzip compressed data, was "hs.base.js", from Unix, last modified: Thu May 10 14:40:25 2012
f_00000c: gzip compressed data, was "dashboard.css", from Unix, last modified: Thu May 10 14:40:16 2012
f_00000d: gzip compressed data, was "hs.dashboard.js", from Unix, last modified: Thu May 10 14:41:14 2012
f_00000e: PNG image data, 119 x 608, 8-bit/color RGBA, non-interlaced
f_00000f: gzip compressed data, was "hs.dependencies.streams.js", from Unix, last modified: Thu May 10
14:42:20 2012
f_000010: HTML document text
f_000011: PNG image data, 214 x 224, 8-bit/color RGBA, non-interlaced
f_000012: gzip compressed data, was "staticlegacy.css", from Unix, last modified: Thu May 10 14:41:05 2012
f_000014: JPEG image data, JFIF standard 1.01
```

Internet History: Chrome - Cache

- ~/Library/Caches/Google/Chrome/Default/Media Cache/
 - “data_#” index – “Chromium Disk Cache”

```
bit:Media Cache oompa$ pwd
/Users/oompa/Library/Caches/Google/Chrome/Default/Media Cache
bit:Media Cache oompa$ file * | more
data_0:  data
data_1:  data
data_2:  data
data_3:  data
f_000001: ISO Media, MPEG v4 system, version 1
f_000002: data
f_000003: data
f_000004: data
f_000005: ISO Media, MPEG v4 system, version 1
f_000006: data
f_000007: data
f_000008: data
f_000009: ISO Media, MPEG v4 system, version 1
```

Internet History:

FireFox - Internet History

History

- ~/Library/Application Support/Firefox/Profiles/*****.default/places.sqlite
- SQLite Database File
- 'moz_places' Table
- 'moz_historyvisits' Table

Downloads

- ~/Library/Application Support/Firefox/Profiles/*****.default/downloads.sqlite
- SQLite Database – Contains one table
- 'moz_downloads' Table

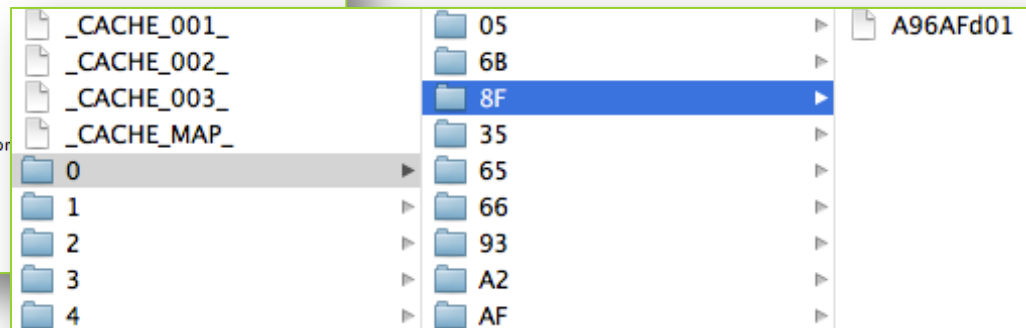
Search History

- ~/Library/Application Support/Firefox/Profiles/*****.default/formhistory.sqlite
- SQLite Database – Contains one table
- 'moz_formhistory' Table
- fieldname = "searchbar-history"

Internet History: FireFox - Cache

- ~/Library/Caches/Firefox/Profiles/
*****.default/Cache
- “CACHE MAP” format

```
bit:Cache oompa$ find . -exec file {} \; | more
.: directory
./0: directory
./0/05: directory
./0/05/B124Bd01: JPEG image data, JFIF standard 1.01
./0/35: directory
./0/35/C4EDDd01: JPEG image data, JFIF standard 1.01
./0/65: directory
./0/65/A921Cd01: gzip compressed data, from Unix
./0/66: directory
./0/66/D444Ad01: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-jpeg v1.0 (using IJ"
./0/6B: directory
./0/6B/CDF64d01: JPEG image data, JFIF standard 1.01
./0/8F: directory
./0/8F/A96AFd01: JPEG image data, JFIF standard 1.02
./0/93: directory
./0/93/5A4B5d01: JPEG image data, JFIF standard 1.01
./0/A2: directory
./0/A2/73A06d01: PNG image data, 558 x 465, 8-bit colormap, non
./0/AF: directory
./0/AF/97F69d01: JPEG image data, JFIF standard 1.01
./0/C6: directory
./0/C6/4F237d01: JPEG image data, JFIF standard 1.01
./0/C8: directory
./0/C8/DB6A1d01: JPEG image data, EXIF standard
```



Email

What

- Apple Mail

Why

- Malicious Attachments
- Phishing
- Data Exfiltration

Email:

Apple Mail

- ~/Library/Mail/V2/MailData/
 - Accounts.plist – Mail Account Information

Key	Type	Value
AccountsVersion	Number	6
▶ DeliveryAccounts	Array	(2 items)
▼ MailAccounts	Array	(4 items)
▶ Item 0	Diction...	(8 items)
▼ Item 1	Diction...	(25 items)
AccountName	String	CSH
AccountPath	String	~/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu
AccountType	String	IMAPAccount

Email:

Apple Mail

- Directories for each email account.
 - Nested messages and attachment directories.
 - File Types: mbox & eml
- Mailboxes
 - ~/Library/Mail/V2/

```
Attachments//435/1.2:
total 32
drwxr-xr-x  3 oompa  staff   102 May 10 16:55 .
drwxr-xr-x  5 oompa  staff   170 May 10 16:55 ..
-rw-r--r--@ 1 oompa  staff 13524 May 10 16:55 image001.jpg

Attachments//435/1.3:
total 32
drwxr-xr-x  3 oompa  staff   102 May 10 16:55 .
drwxr-xr-x  5 oompa  staff   170 May 10 16:55 ..
-rw-r--r--@ 1 oompa  staff 15868 May 10 16:55 image002.png
```

```
bit:Data oompa$ pwd
/Users/oompa/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu/INBOX.mbox/0223CBB8-8F52-487D-9F90-C87F2F6701C4/Data
bit:Data oompa$ ls -la
total 16
drwx----- 11 oompa  staff   374 May 17 21:37 .
drwx-----  4 oompa  staff   136 May 17 21:37 ..
-rw-r--r--@  1 oompa  staff  6148 May 17 21:38 .DS_Store
drwx-----  3 oompa  staff   102 May 10 19:36 0
drwx-----  5 oompa  staff   170 May 22 21:07 1
drwx-----  4 oompa  staff   136 May 10 16:55 2
drwx-----  4 oompa  staff   136 May 10 16:56 3
drwx-----  4 oompa  staff   136 May 10 16:56 4
drwxr-xr-x   3 oompa  staff   102 May 10 17:10 6
drwxr-xr-x  54 oompa  staff  1836 May 17 21:37 Attachments
drwx----- 990 oompa  staff 33660 May 28 14:46 Messages
```

Email:

Apple Mail - Attachments

“QuickLook”

• ~/Library/Mail Downloads/

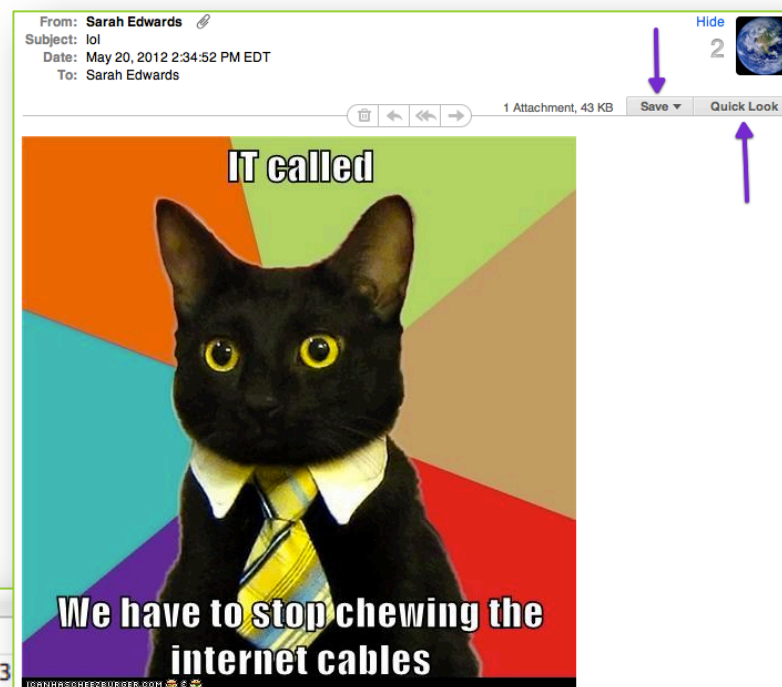
“Saved”

• ~/Downloads

Metadata

• ~/Library/Mail/V2/
MailData/
OpenAttachments.plist

Key	Type	Value
▼ Item 0	Diction...	(5 items)
MessageID	String	<F86B9649-1F9A-4779-A54E-09C84F073
ModDate	Date	May 12, 2012 5:04:13 PM
OpenedDate	Date	May 12, 2012 5:04:13 PM
PartNumber	String	2
Path	String	/Users/oomba/Library/Mail Downloads/photo.JPG



Temporary & Cache Directories

What

- Temporary Directories
- Java Cache

Why

- Remnants of Malicious Files
- Flashback used temp and Java Cache directories

Temp & Cache Directories: Java Temp & Cache

- /tmp & /var/tmp
- /Users/<user>/Library/Caches/Java/tmp
- /Users/<user>/Library/Caches/Java/cache
 - IDX, JAR Files
 - Open Cache in /Applications/Utilities/Java Preferences.app

Show: **Resources**   Cache Size: 13186 KB

Name	URL	Modified	Expired	Version	Size
 vcChair.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcChair.jar.pack.gz	May 27, 2010			34 KB
 vcRecorder.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcRecorder.jar	May 27, 2010			0.2 KB
 vcWhiteboard.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcWhiteboard.jar	Jul 13, 2010			0.3 KB
 vcHand.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcHand.jar	May 27, 2010			0.2 KB
 vcAppShareMacOSXx86...	https://elm.sans.org:443/elmcontrol/lib/10.0/vcAppShareMacOSXx86.jar	Oct 28, 2011			75 KB
 vcPlatformMacOSXx86...	https://elm.sans.org:443/elmcontrol/lib/10.0/vcPlatformMacOSXx8664.jar	May 27, 2010			18 KB
 vcBrowserMacOSXx866...	https://elm.sans.org:443/elmcontrol/lib/10.0/vcBrowserMacOSXx8664.jar	May 27, 2010			30 KB
 vcTelephony.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcTelephony.jar	May 27, 2010			0.2 KB
 vcStartTime.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcStartTime.jar	May 27, 2010			0.2 KB
 vcMultimedia.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcMultimedia.jar.pack.gz	May 27, 2010			181 KB
 vcActivity.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcActivity.jar.pack.gz				
 vcAppShare.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcAppShare.jar.pack.gz				
 guice-2.0-no_aop.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/guice-2.0-no_aop.jar				
 vcCalculator.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcCalculator.jar				
 vcCaption.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcCaption.jar				
 vcDirectMsg.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcDirectMsg.jar.pack.gz				
 vcHand.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcHand.jar.pack.gz				
 vcDirectMsg.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcDirectMsg.jar				
 eLiveFull.jnlp	https://elm.sans.org:443/elmcontrol/lib/10.0/eLiveFull.jnlp				
 vcPresentation.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcPresentation.jar				
 vcInvite.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcInvite.jar.pack.gz				
 vcProfile.jar.pack.gz	https://elm.sans.org:443/elmcontrol/lib/10.0/vcProfile.jar.pack.gz				
 vcParticipant.jar	https://elm.sans.org:443/elmcontrol/lib/10.0/vcParticipant.jar				

Java Preferences

General Security **Network** Advanced

Network settings are used when making Internet connections. By default, Java applets and Web Start applications use the network settings in the system network preferences. Only advanced users should modify these settings.

[Network Settings...](#)

☒ Keep temporary files for fast access:

Select the location where temporary files are kept:

[Change...](#)

Select the compression level for JAR files:

Set the amount of disk space for storing temporary files:

MB

[View Cache Files...](#) [Delete Files...](#) [Restore Defaults](#)

Changes take effect in browsers and Java applications the next time you open them.

Java Temp & Cache: IDX File Contents

```
0000000: 0000 0000 025b 0000 0000 0000 0000 0001 .....[.....
0000010: 28d8 2ea8 4000 0000 0000 0000 0000 0000 (...@.....
0000020: 0000 0000 0000 0000 00ac 0000 0000 0000 .....
0000030: 0000 0000 0000 0000 0136 9959 1234 0000 .....6.Y.4..
0000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000050: 0000 0000 0000 0000 0000 0000 0136 9959 .....6.Y
0000060: 1234 0000 0000 0000 0000 0000 0000 0000 .4.....
0000070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000080: 0000 003a 6874 7470 733a 2f2f 656c 6d2e ...:https://elm.
0000090: 7361 6e73 2e6f 7267 3a34 3433 2f65 6c6d sans.org:443/elm
00000a0: 636f 6e74 726f 6c2f 6c69 622f 3130 2e30 control/lib/10.0
00000b0: 2f76 6343 6170 7469 6f6e 2e6a 6172 0000 /vcCaption.jar..
00000c0: 000b 3636 2e33 352e 3435 2e35 3000 0000 ..66.35.45.50...
00000d0: 0200 063c 6e75 6c6c 3e00 0333 3032 0008 ...<null>..302..
00000e0: 4c6f 6361 7469 6f6e 0042 6874 7470 733a Location.Bhttps:
00000f0: 2f2f 656c 6d2e 7361 6e73 2e6f 7267 3a34 //elm.sans.org:4
000100: 3433 2f65 6c6d 636f 6e74 726f 6c2f 6c69 43/elmcontrol/li
0001010: 622f 3130 2e30 2f76 6343 6170 7469 6f6e b/10.0/vcCaption
0001020: 2e6a 6172 2e70 6163 6b2e 677a .jar.pack.gz
```

Temp & Cache Files: Examples

Flashback

- Mach-O Binary – /tmp/.sysenter
- Java Cache Files
 - rh-3.jar
 - cl-3.jar

Imuler

- /tmp/.mdworker
- /tmp/CurlUpload

MacControl

- /tmp/launch-hs – Bash Script
- /tmp/launch-hse - Malware
- /tmp/file.doc – Decoy Word Doc

Log Analysis

What

- ◉ Apple System Logs
- ◉ Audit Logs
- ◉ Firewall Logs
- ◉ Install Logs

Why

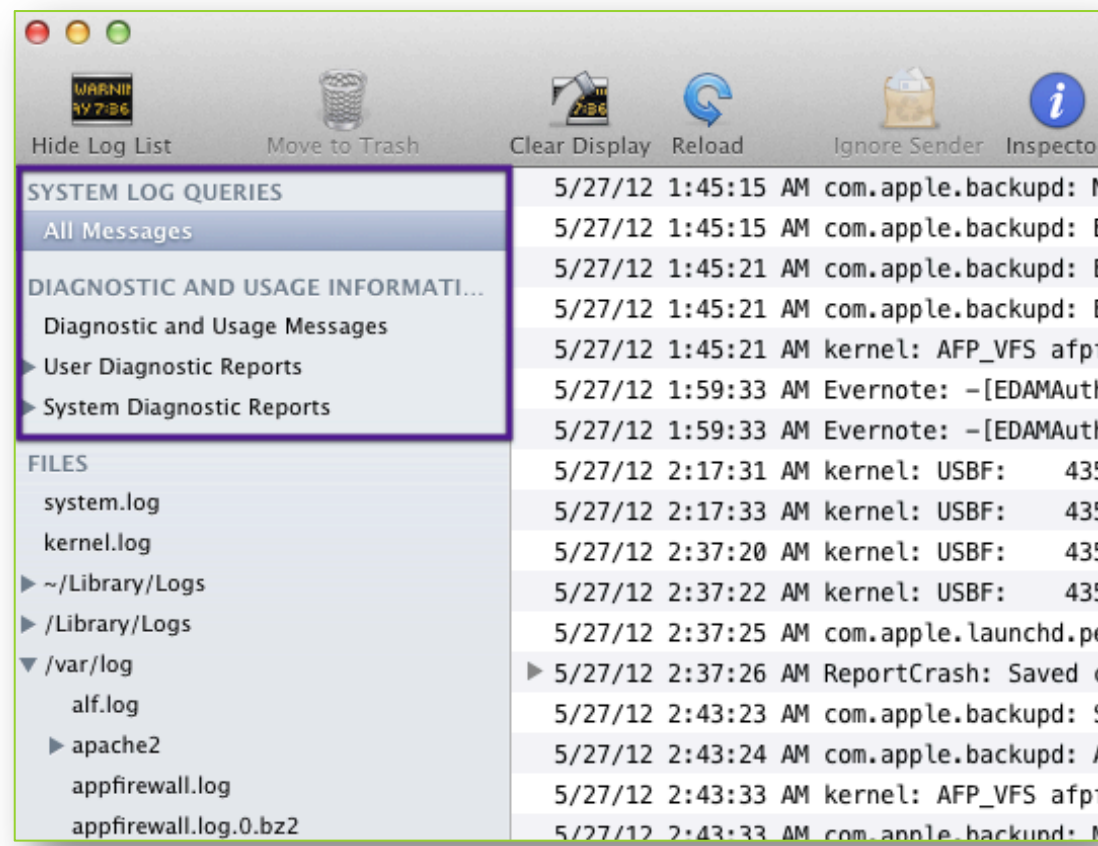
- ◉ Suspicious Use
- ◉ Account Creation
- ◉ Super User Access
- ◉ External Volumes

Log Analysis: Apple System Logs

- Location: /private/var/log/asl/ (>10.5.6)
- syslog “replacement”
- View using Console.app or `syslog` command
- Filename Format: YYYY.MM.DD.[UID].[GID].asl

```
-rw-----+ 1 root  wheel  93522 May 22 23:45 2012.05.22.G80.asl
-rw-----+ 1 root  wheel   8696 May 22 23:45 2012.05.22.U0.G80.asl
-rw-----+ 1 root  wheel  24612 May 22 23:45 2012.05.22.U501.asl
-rw-----+ 1 root  wheel   3720 May 22 22:45 2012.05.22.U89.asl
-rw-----+ 1 root  wheel  87101 May 23 23:45 2012.05.23.G80.asl
-rw-----+ 1 root  wheel   9245 May 23 23:45 2012.05.23.U0.G80.asl
-rw----- 1 root  wheel    864 May 23 21:57 2012.05.23.U0.asl
-rw-----+ 1 root  wheel  18556 May 23 23:35 2012.05.23.U501.asl
-rw-----+ 1 root  wheel   5680 May 23 23:45 2012.05.23.U89.asl
-rw-----+ 1 root  wheel  92582 May 24 23:45 2012.05.24.G80.asl
-rw-----+ 1 root  wheel   9122 May 24 23:45 2012.05.24.U0.G80.asl
-rw-----+ 1 root  wheel  17707 May 24 23:28 2012.05.24.U501.asl
-rw-----+ 1 root  wheel   5680 May 24 23:45 2012.05.24.U89.asl
-rw-----+ 1 root  wheel  92416 May 25 23:45 2012.05.25.G80.asl
```

Log Analysis: Console.app



Log Analysis: Console.app

```
4/6/12 4:45:20 PM login: USER_PROCESS: 304 ttys004
4/6/12 4:45:21 PM login: USER_PROCESS: 308 ttys005
4/28/12 3:31:05 PM login: DEAD_PROCESS: 278 ttys000
4/28/12 3:31:05 PM login: DEAD_PROCESS: 300 ttys003
4/28/12 3:31:05 PM login: DEAD_PROCESS: 292 ttys001
4/28/12 3:31:05 PM login: DEAD_PROCESS: 296 ttys002
4/28/12 3:31:06 PM login: DEAD_PROCESS: 304 ttys004
4/28/12 3:31:06 PM login: DEAD_PROCESS: 308 ttys005
4/28/12 5:36:50 PM login: USER_PROCESS: 96459 ttys000
4/28/12 5:36:50 PM login: USER_PROCESS: 96460 ttys001
4/28/12 5:36:51 PM login: USER_PROCESS: 96467 ttys002
4/28/12 5:36:51 PM login: USER_PROCESS: 96471 ttys003
4/28/12 5:36:51 PM login: USER_PROCESS: 96472 ttys004
4/28/12 5:36:51 PM login: USER_PROCESS: 96479 ttys005
5/15/12 10:44:23 AM login: DEAD_PROCESS: 96459 ttys000
5/15/12 10:44:23 AM login: DEAD_PROCESS: 96460 ttys001
5/15/12 10:44:24 AM login: DEAD_PROCESS: 96467 ttys002
5/15/12 10:44:25 AM login: DEAD_PROCESS: 96471 ttys003
5/15/12 10:44:27 AM login: DEAD_PROCESS: 96479 ttys005
5/15/12 10:44:59 AM login: USER_PROCESS: 35204 ttys000
5/15/12 7:44:24 PM sshd: USER_PROCESS: 39491 ttys001
5/15/12 8:08:56 PM sshd: DEAD_PROCESS: 39491 ttys001
5/20/12 12:43:58 PM sshd: USER_PROCESS: 49332 ttys001
5/20/12 12:48:19 PM sshd: DEAD_PROCESS: 49332 ttys001
```

Message Inspector	
Key	Value
ASLExpireTime	1368747864
ASLMessageID	3546564
Facility	com.apple.system.lastlog
GID	0
Host	byte
Level	5
PID	39488
ReadGID	80
Sender	sshd
Time	1337125464
TimeNanoSec	436116000
UID	0
ut_host	bit
ut_id	s001
ut_line	ttys001
ut_pid	39491
ut_tv.tv_sec	1337125464
ut_tv.tv_usec	420174
ut_type	7
ut_user	oompa
Message	USER_PROCESS: 39491 ttys001

Log Analysis: syslog Command

```
sh-3.2# syslog -d asl/ | more
Mar 12 17:15:01 byte login[63585] <Notice>: USER_PROCESS: 63585 ttys003
Mar 15 01:41:32 byte login[48848] <Notice>: USER_PROCESS: 48848 ttys004
Mar 15 01:44:22 byte login[48905] <Notice>: USER_PROCESS: 48905 ttys005
Mar 15 01:52:19 byte login[48848] <Notice>: DEAD_PROCESS: 48848 ttys004
Mar 15 01:52:19 byte login[48905] <Notice>: DEAD_PROCESS: 48905 ttys005
Mar 15 01:52:21 byte login[48960] <Notice>: USER_PROCESS: 48960 ttys004
Mar 15 01:53:16 byte login[48960] <Notice>: DEAD_PROCESS: 48960 ttys004
Mar 15 01:53:18 byte login[50861] <Notice>: USER_PROCESS: 50861 ttys004
Mar 15 01:53:52 byte login[50861] <Notice>: DEAD_PROCESS: 50861 ttys004
Mar 15 01:53:53 byte login[52753] <Notice>: USER_PROCESS: 52753 ttys004
Mar 15 01:54:19 byte login[53625] <Notice>: USER_PROCESS: 53625 ttys005
```

Log Analysis:

`syslog -T utc -F raw -d /asl`

- [ASLMessageID 3555356]
- [Time 2012.05.28 19:39:32 UTC]
- [TimeNanoSec 887175000]
- [Level 5]
- [PID 908]
- [UID 0]
- [GID 20]
- [ReadGID 80]
- [Host byte]
- [Sender login]
- [Facility com.apple.system.utmpr]
- [Message DEAD_PROCESS: 908 ttys002]
- [ut_user oompa]
- [ut_id s002]
- [ut_line ttys002]
- [ut_pid 908]
- [ut_type 8]
- [ut_tv.tv_sec 1338233972]
- [ut_tv.tv_usec 886961]
- [ASLExpireTime 1369856372]

Log Analysis: Audit Logs

- Location: /private/var/audit/
- BSM Audit Logs
- StartTime.EndTime
- YYYYMMDDHHMMSS.YYYYMMDDHHMMSS

```
drwx-----  8 root  wheel    272 May 28 15:22 .
drwxr-xr-x  29 root  wheel    986 May  9 21:39 ..
-r--r-----  1 root  wheel  48987 May 10 00:46 20120509232853.20120510044637
-r--r-----  1 root  wheel  57158 May 12 11:31 20120510204054.20120512153135
-r--r-----  1 root  wheel  92166 May 27 20:02 20120512153220.20120528000216
-r--r-----  1 root  wheel  20805 May 28 15:20 20120528000250.20120528192006
-r--r-----  1 root  wheel   4619 May 28 21:07 20120528192235.not_terminated
lrwxr-xr-x   1 root  wheel    40 May 28 15:22 current -> /var/audit/20120528192235.not_terminated
```

Log Analysis:

`praudit -xn /var/audit/*`

- su Example:

```
<record version="11" event="user authentication" modifier="0" time="Mon May 28
21:12:51 2012" msec=" + 41 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20" pid="552"
sid="100004" tid="552 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos; node &apos;/Local/
Default&apos;;</text>
<return errval="success" retval="0" />
</record>
```

```
<record version="11" event="user authentication" modifier="0" time="Mon May 28
21:12:55 2012" msec=" + 449 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20" pid="554"
sid="100004" tid="554 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos; node &apos;/Local/
Default&apos;;</text>
<return errval="failure: Unknown error: 255" retval="5000" />
</record>
```

Log Analysis: User Logins / Logouts

Local Terminal

- May 28 14:48:04 byte login[693]: USER_PROCESS: 693 ttys000
- May 28 14:48:07 byte login[698]: USER_PROCESS: 698 ttys001
- May 28 15:07:29 byte login[812]: USER_PROCESS: 812 ttys002
- May 28 15:07:51 byte login[812]: DEAD_PROCESS: 812 ttys002

Login Window

- May 28 12:42:23 byte loginwindow[66]: DEAD_PROCESS: 74 console
- May 28 14:28:04 byte loginwindow[66]: USER_PROCESS: 60 console

SSH

- May 28 15:15:38 byte sshd[831]: USER_PROCESS: 842 ttys002
- May 28 15:15:52 byte sshd[831]: DEAD_PROCESS: 842 ttys002

Screen Sharing

- 5/28/12 3:31:33.675 PM screensharingd: Authentication: SUCCEEDED ::
User Name: Sarah Edwards :: Viewer Address: 192.168.1.101 :: Type:
DH

Log Analysis monthly.out

- Account Audit
- Monthly
- Uses `ac -p` command to calculate account time on system.
- “Accumulated connected time in decimal hours”

```
-- End of monthly output --  
  
Wed Apr  4 09:15:54 EDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
    total      3678.85  
    sledwards  3678.76  
    root        0.09  
  
-- End of monthly output --  
  
Tue May  1 05:30:00 PDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
    total      4301.95  
    sledwards  4301.77  
    root        0.18  
  
-- End of monthly output --  
  
Fri Jun  1 06:46:13 PDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
    total      5047.22  
    sledwards  5047.04  
    root        0.18  
  
-- End of monthly output --
```

Log Analysis: Privilege Escalation

SU

- 5/27/12 8:54:21.646 PM su: BAD SU oompa to root on /dev/ttys001
- 5/28/12 8:57:44.032 PM su: oompa to root on /dev/ttys000

sudo

- 5/27/12 8:48:15.790 PM sudo: oompa :
TTY=ttys000 ; PWD=/Users/oompa/Documents ;
USER=root ; COMMAND=/usr/bin/iosnoop

Log Analysis: Account Creation

Audit Logs

- ```
<record version="11" event="create user" modifier="0"
time="Mon May 28 21:25:49 2012" msec=" + 677 msec" >
<subject audit-uid="501" uid="501" gid="20" ruid="501"
rgid="20" pid="585" sid="100004" tid="585 0.0.0.0" />
<text>Create record type Users
'supersecretuser'; node ';/Local/
Default';</text>
<return errval="success" retval="0" />
</record>
```

## secure.log

- ```
May 28 21:25:22 bit com.apple.SecurityServer[24]: UID
501 authenticated as user oompa (UID 501) for right
'system.preferences.accounts'
```

Log Analysis: Firewall Logs

- Location: /private/var/log/appfirewall.log

```
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:31365
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:3702
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:48189
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:27899
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:1804
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:59846
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:31335
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:20817
from 192.168.1.100:57188
May 28 21:58:22 bit Firewall[81]: Stealth Mode connection attempt to UDP 192.168.1.101:16974
```

Log Analysis: install.log

```
May 27 11:59:03 MBP Installer[470]: logKext  Installation Log
May 27 11:59:03 MBP Installer[470]: Opened from: /Users/oomba/Downloads/
logKext-2.3.pkg
May 27 11:59:03 MBP Installer[470]: Product archive /Users/oomba/Downloads/
logKext-2.3.pkg trustLevel=100
May 27 11:59:17 MBP Installer[470]: InstallerStatusNotifications plugin loaded
May 27 11:59:26 MBP runner[477]: Administrator authorization granted.
May 27 11:59:26 MBP Installer[470]:
=====
May 27 11:59:26 MBP Installer[470]: User picked Standard Install
May 27 11:59:26 MBP Installer[470]: Choices selected for installation:
...
May 27 12:01:34 MBP installd[481]: Installed "logKext" ()
May 27 12:01:35 MBP installd[481]: PackageKit: ----- End install -----
```


Log Analysis: Log Recovery

- Logs get “removed” or “turned over”
- GREP or keyword search for specific date/
log formats.
 - “May 18 23:17:15”
 - “Thu May 31 19:35:35 EDT 2012”
 - “ASL DB”
 - “launchctl::Audit startup”
 - “BZh91AY&SY”

Volume Analysis

What

- Log Files
- MRU Files
- Property List Files

Why

- Insider Threat
- Data Exfiltration
- Distribute Malware

Volume Analysis: system.log & daily.log

```
May 19 08:58:23 bit fsevents[20]: log dir: /Volumes/Time Machine Backups/.fsevents getting new uuid: 5420A642-DE8C-4B90-B2B4-B948288F5E3F
May 19 16:52:30 bit fsevents[20]: log dir: /Volumes/NO NAME/.fsevents getting new uuid: DD64986D-F58C-407B-901B-5BD27104F062
May 23 20:10:35 bit fsevents[20]: log dir: /Volumes/NO NAME/.fsevents getting new uuid: 0D8CB03B-0691-4381-ACEF-8F7F421D12DF
May 26 14:01:03 bit fsevents[20]: log dir: /Volumes/WDPassport/.fsevents getting new uuid: CDCE4339-A254-4925-A909-97B4553BDAC1
May 26 15:40:38 bit fsevents[20]: log dir: /Volumes/WDPassport/.fsevents getting new uuid: D4FFFB2-16A8-4CB3-88DE-327CDE1551EC
```

Fri May 11 17:12:29 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/disk0s2	698Gi	22Gi	675Gi	4%	/
localhost:/35wJAmjuh-MSBDh6mJulon	698Gi	698Gi	0Bi	100%	/Volumes/MobileBackups
/dev/disk6s2	107Mi	107Mi	0Bi	100%	/Volumes/Google Chrome

Volume Analysis: kernel.log

- Search for “USBMSC”
- Serial Number, Vendor ID, Product ID, Version

```
Apr 25 12:27:11 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:32:31 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:47:29 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:49:43 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:52:46 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 25 12:53:37 Pro kernel[0]: USBMSC Identifier (non-unique): ABCDEF0123456789 0xe90 0x5 0x0
Apr 25 13:04:21 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 13:04:29 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 26 12:36:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 27 09:02:59 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 30 09:07:14 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
May 3 05:43:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
May 3 06:24:05 Pro kernel[0]: USBMSC Identifier (non-unique): SWOC22905731 0x1199 0xffff 0x323
May 24 11:22:43 Pro kernel[0]: USBMSC Identifier (non-unique): 000000009833 0x5ac 0x8403 0x9833
May 24 11:53:25 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 25 12:48:38 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 30 06:50:01 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 31 13:10:09 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
Jun 1 07:16:03 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
```

Volume Analysis: kernel.log

Jun 3 11:11:53 bit kernel[0]: USBMSC Identifier
(non-unique): FBF1011220504638 0x90c 0x1000 0x1100

Flash Disk:

Capacity: 8.02 GB (8,019,509,248 bytes)
Removable Media: Yes
Detachable Drive: Yes
BSD Name: disk2
Product ID: 0x1000
Vendor ID: 0x090c (Silicon Motion, Inc. - Taiwan)
Version: 11.00
Serial Number: FBF1011220504638
Speed: Up to 480 Mb/sec
Manufacturer: USB
Location ID: 0xfd130000 / 5
Current Available (mA): 500
Current Required (mA): 500
Partition Map Type: MBR (Master Boot Record)
S.M.A.R.T. status: Not Supported
Volumes:

BLACKBAG:

Capacity: 8.02 GB (8,019,476,992 bytes)
Available: 7.87 GB (7,868,444,672 bytes)
Writable: Yes
File System: MS-DOS FAT32
BSD Name: disk2s1
Mount Point: /Volumes/BLACKBAG
Content: DOS_FAT_32

Volume Analysis: com.apple.finder.plist

- FXDesktopVolumePositions
- FXRecentFolders (10 most recent)

▼ FXRecentFolders	Array	(10 items)
▼ Item 0	Diction...	(2 items)
file-bookmark	Data	<626f6f6b ac030000
name	String	STUFF
▼ Item 1	Diction...	(2 items)
file-bookmark	Data	<626f6f6b 3c030000
name	String	TechnoSecurity2012
▼ Item 2	Diction...	(2 items)
file-bookmark	Data	<626f6f6b 8c020000
name	String	oompa
▼ Item 3	Diction...	(2 items)
file-bookmark	Data	<626f6f6b c0020000
name	String	Dropbox

Key
▼ FXDesktopVolumePositions
▶ STUFF_-0x1.d27e44p+29
▶ VMware Fusion_0x1.3f5f0e2p+28
▶ WDPassport_-0x1.d27e44p+29
▶ DATA_0x1.3db4fc2p+28
▶ OmniOutliner_0x1.25dcb04p+27
▶ Sample Docs_0x1.eefdap+26
▶ NO NAME_-0x1.3c0752p+29
▶ OmniOutliner Pro_0x1.25dcad2p+27
▶ Time Machine Backups_0x1.438f33dp

Antivirus

What

- ◉ Extended Attributes
- ◉ File Quarantine
- ◉ Xprotect
- ◉ GateKeeper
- ◉ Third-party Vendors

Why

- ◉ File Metadata
- ◉ Logs
- ◉ Quarantine Directories
- ◉ Weaknesses & Limitations

Antivirus: File Quarantine

- ◉ Introduced in 10.5
- ◉ Quarantines downloaded files
- ◉ Applications (Browsers, Email, etc)
- ◉ Weaknesses
 - ◉ Files on USB drives
 - ◉ Applications that do not implement File Quarantine

Antivirus: File Quarantine

- Application's Info.plist
 - LSFileQuarantineEnabled Key set to True

```
<key>KSProductID</key>
<string>com.google.Chrome</string>
<key>KSUpdateURL</key>
<string>https://tools.google.com/service/update2</string>
<key>KSVersion</key>
<string>19.0.1084.46</string>
<key>LSFileQuarantineEnabled</key>
<true/>
<key>LSHasLocalizedDisplayName</key>
<string>1</string>
<key>LSMinimumSystemVersion</key>
<string>10.5.0</string>
<key>NSAppleScriptEnabled</key>
<true/>
```

KSProductID	String	com.google.Chrome
KSUpdateURL	String	https://tools.google.com/service/update2
KSVersion	String	19.0.1084.46
File quarantine enabled	Boolean	YES
Application has localized display name	String	YES
Minimum system version	String	10.5.0
Scriptable	Boolean	YES

Antivirus:

File Quarantine Events

Lion
10.7

- ~/Library/Preferences/
com.apple.LaunchServices.QuarantineEvents.V2

Snow
Leopard
10.6

- ~/Library/Preferences/
com.apple.LaunchServices.QuarantineEvents

Antivirus: File Quarantine

- Quarantine Events – LSQuarantineEvent Table

Key	Example Data
LSQuarantineEventIdentifier	68F08939-EF7F-4326-BDA3-810542E43579
LSQuarantineTimeStamp	358820762.0
LSQuarantineAgentBundleIdentifier	com.google.Chrome
LSQuarantineAgentName	Google Chrome
LSQuarantineDataURLString	http://ash.barebones.com/TextWrangler_4.0.dmg
LSQuarantineSenderName	NULL
LSQuarantineSenderAddress	NULL
LSQuarantineTypeNumber	0
LSQuarantineOriginTitle	NULL
LSQuarantineOriginURLString	http://www.barebones.com/products/textwrangler/
LSQuarantineOriginAlias	NULL

Antivirus: Extended Attributes

- Command: `xattr`
- Quarantine**
- Metadata:
 - kMDItemWhereFroms**
 - `com.apple.backup_excludelim`
- Disk Images
- FinderInfo
- TextEncoding
- Preview UI State
- Resource Fork
- DropBox
- Etc.

```
bit:Downloads oompa$ xattr -xl TextWrangler_4.0.dmg
com.apple.diskimages.fsck:
00000000  A1 52 D4 F1 FC 10 76 E8 A6 EB E3 EB 73 3F 8F A1  |.R....v.....s?..|
00000010  46 83 68 3C                                     |F.h<|
00000014
com.apple.diskimages.recentcksum:
00000000  69 3A 31 34 39 33 37 34 39 20 6F 6E 20 33 39 38  |i:1493749 on 398|
00000010  31 45 32 45 36 2D 30 43 41 43 2D 33 41 33 45 2D  |1E2E6-0CAC-3A3E-|
00000020  42 45 31 44 2D 39 30 44 35 38 33 46 38 39 41 35  |BE1D-90D583F89A5|
00000030  44 20 40 20 31 33 33 37 31 32 37 39 36 34 20 2D  |D @ 1337127964 -|
00000040  20 43 52 43 33 32 3A 24 45 36 41 31 34 31 31 34  | CRC32:$E6A14114|
00000050
com.apple.metadata:kMDItemWhereFroms:
00000000  62 70 6C 69 73 74 30 30 A2 01 02 5F 10 2D 68 74  |bplist00..._.-ht|
00000010  74 70 3A 2F 2F 61 73 68 2E 62 61 72 65 62 6F 6E  |tp://ash.barebon|
00000020  65 73 2E 63 6F 6D 2F 54 65 78 74 57 72 61 6E 67  |es.com/TextWrang|
00000030  6C 65 72 5F 34 2E 30 2E 64 6D 67 5F 10 2F 68 74  |ler_4.0.dmg_./ht|
00000040  74 70 3A 2F 2F 77 77 77 2E 62 61 72 65 62 6F 6E  |tp://www.barebon|
00000050  65 73 2E 63 6F 6D 2F 70 72 6F 64 75 63 74 73 2F  |es.com/products/|
00000060  74 65 78 74 77 72 61 6E 67 6C 65 72 2F 08 08 3B  |textwrangler/..;|
00000070  00 00 00 00 00 00 01 01 00 00 00 00 00 00 00 03  |.....|
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D  |.....m|
00000090
com.apple.quarantine:
00000000  30 30 30 31 3B 34 66 62 32 66 34 31 64 3B 47 6F  |0001;4fb2f41d;Go|
00000010  65 67 6C 65 20 43 68 72 65 6D 65 38 36 38 46 30  |ogle Chrome;68F0|
00000020  89 39 EF 7F 43 26 B1 00 00 00 00 00 00 00 00 00 00  |8939-EF7F-4326-B|
00000030  DA 3-810542E43579 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |DA3-810542E43579|
00000040  |com.google.Chro|
00000050  |me|
00000052
```

```
-rw-r--r--@ 1 oompa staff 18041097 May 11 20:01 Rdio.dmg
-rw-r--r--@ 1 oompa staff 5416932 May 15 20:26 TextWrangler_4.0.dmg
-rw-r--r--@ 1 oompa staff 188900306 May 11 19:22 VMware-Fusion-4.1.2-683185-light.dmg
-rw-r--r--@ 1 oompa staff 39937338 Apr 30 15:30 googlechrome.dmg
```

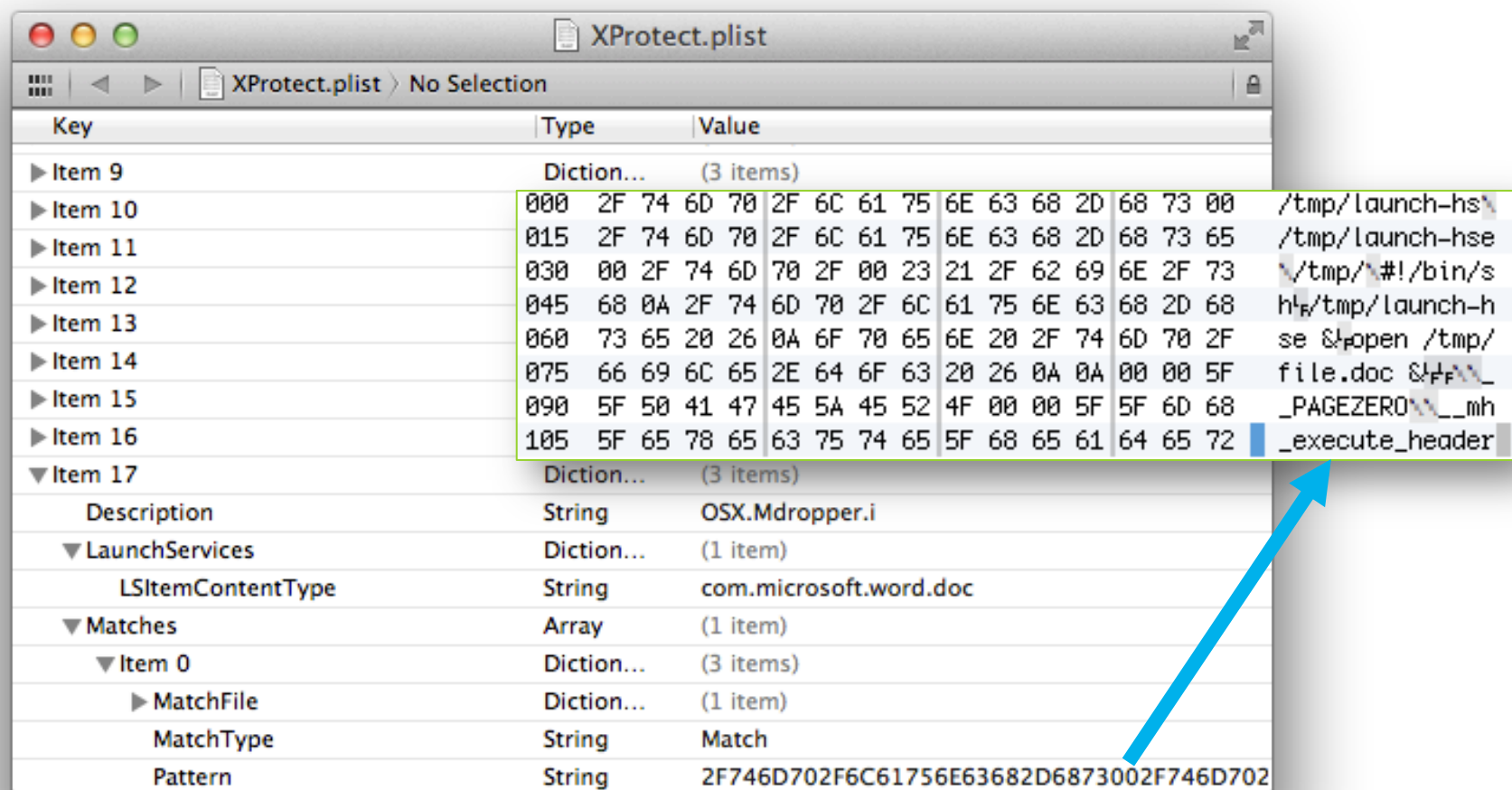
Antivirus: Extended Attributes

com.apple.quarantine	Related Key in QuarantineEvents Database
4fb2f41d	LSQuarantineTimeStamp
Google Chrome	LSQuarantineAgentName
68F08939-EF7F-4326-BDA3-810542E43579	LSQuarantineEventIdentifier
com.google.Chrome	LSQuarantineAgentBundleIdentifier
com.apple.metadata:kMDItemWhereFroms	
http://ash.barebones.com/TextWrangler_4.0.dmg	LSQuarantineDataURLString
http://www.barebones.com/products/textwrangler/	LSQuarantineOriginURLString

Antivirus: XProtect

- /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources
 - XProtect.meta.plist
 - Last Update Date & Version
 - XProtect.plist
 - AV Signatures
- Weaknesses
 - Apple updates it, sometimes.
 - Very few signatures on blacklist
 - No Heuristics
 - Only checks “quarantined” files

Antivirus: XProtect



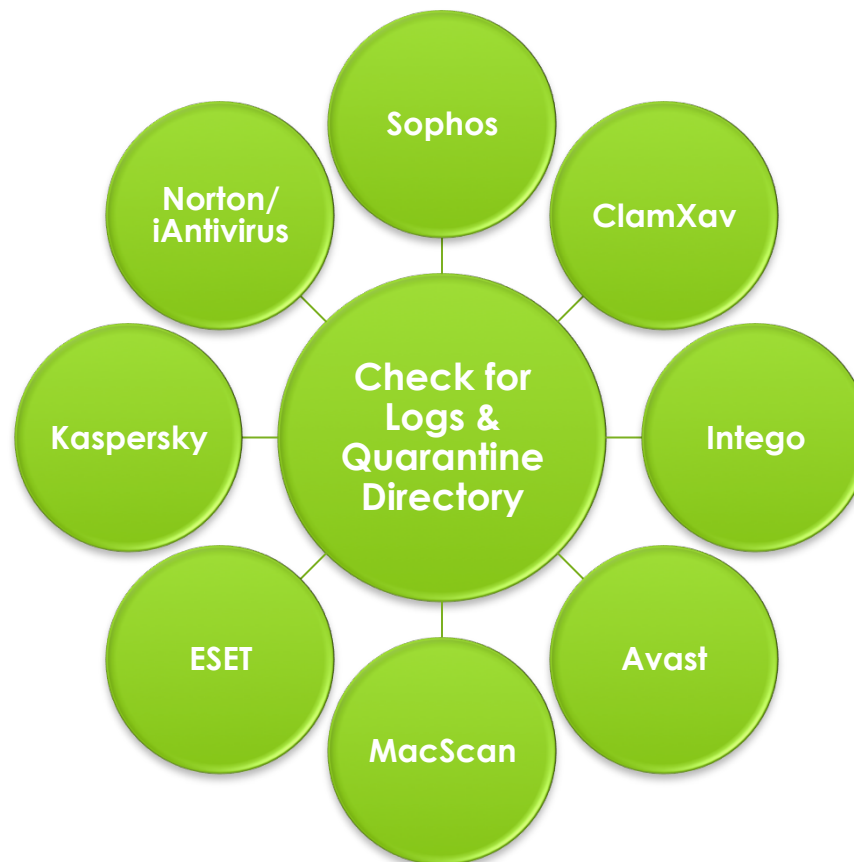
The screenshot shows a macOS plist editor window titled 'XProtect.plist'. The main table lists various keys and their values. A blue arrow points to the '_execute_header' value in Item 16.

Key	Type	Value
▶ Item 9	Diction...	(3 items)
▶ Item 10		000 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 73 00 /tmp/launch-hs\
▶ Item 11		015 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 73 65 /tmp/launch-hse
▶ Item 12		030 00 2F 74 6D 70 2F 00 23 21 2F 62 69 6E 2F 73 \tmp/\#!/bin/s
▶ Item 13		045 68 0A 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 h\mp/launch-h
▶ Item 14		060 73 65 20 26 0A 6F 70 65 6E 20 2F 74 6D 70 2F se &\open /tmp/
▶ Item 15		075 66 69 6C 65 2E 64 6F 63 20 26 0A 0A 00 00 5F file.doc &\f\
▶ Item 16		090 5F 50 41 47 45 5A 45 52 4F 00 00 5F 5F 6D 68 _PAGEZERO__mh
▶ Item 16		105 5F 65 78 65 63 75 74 65 5F 68 65 61 64 65 72 _execute_header
▼ Item 17	Diction...	(3 items)
Description	String	OSX.Mdropper.i
▼ LaunchServices	Diction...	(1 item)
LSItemContentType	String	com.microsoft.word.doc
▼ Matches	Array	(1 item)
▼ Item 0	Diction...	(3 items)
▶ MatchFile	Diction...	(1 item)
MatchType	String	Match
Pattern	String	2F746D702F6C61756E63682D6873002F746D702

Antivirus: GateKeeper

- ◉ 10.8 - Mountain Lion
- ◉ Similar Functionality to File Quarantine/XProtect
- ◉ Security Settings
 - ◉ Mac App Store
 - ◉ Users can only run apps from the store.
 - ◉ Mac App Store & Identified Developers
 - ◉ Default Setting
 - ◉ Users can only run software signed using Apple Developer ID
 - ◉ Anywhere
 - ◉ Users can run anything from anywhere

Antivirus: Third-Party Software



Anti-Forensics

What

- Encryption
- Optimization Software
- Secure Erase

Why

- Suspicious Use
- Data Removal

Anti-forensics: FileVault Encryption

FileVault (Legacy)

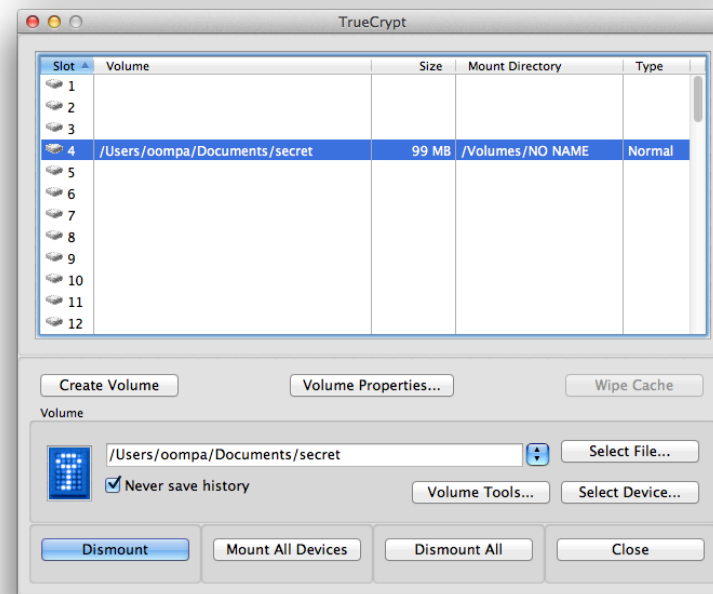
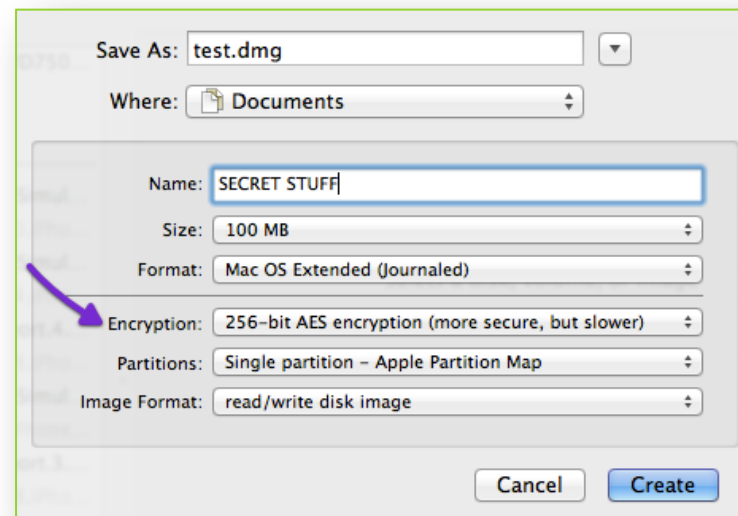
- Home Directory
- Introduced in 10.3
- Password
- Sparse Disk Image <10.4
- Sparse Bundle >10.5

FileVault 2

- Full Disk Encryption
- Introduced in 10.7
- Password or Recovery Key

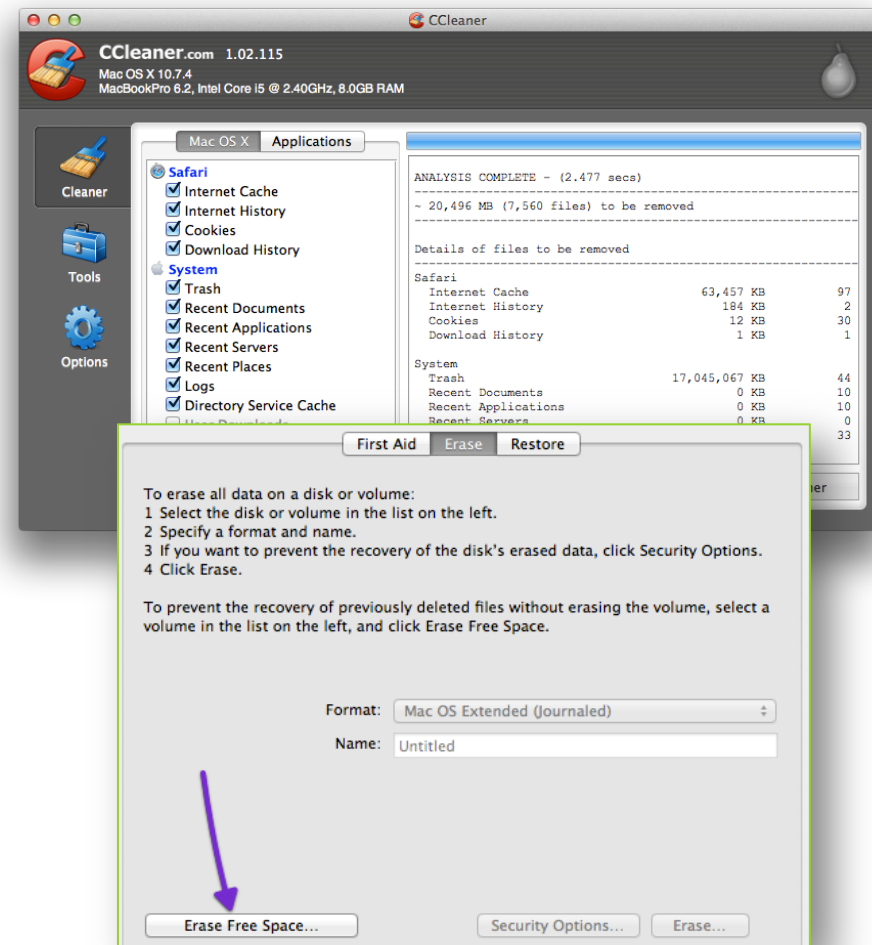
Anti-forensics: Other Encryption

- Apple Encrypted Disk Images
- TrueCrypt
- Check Point FDE
- McAfee Endpoint Encryption



Anti-forensics: Optimization Software & Secure Erase

- Piriform CCleaner
- Intego Washing Machine 2
- Disk Utility
 - Disk Wipe
 - Erase Free Space



Other Files

What

- Kernel Extensions
- Bash History
- User Accounts
- Applications
- Shared Directory

Why

- Suspicious Use
- Hidden Files
- Unknown Accounts
- Suspicious Software
- Application Misuse

Other Files: Kernel Extensions

- Dynamically loaded executable code in kernel space
 - Low Level Device Drivers
 - Network Filters
 - File Systems
 - ...keyloggers?

```
MBP:Extensions oompa$ pwd
/System/Library/Extensions
MBP:Extensions oompa$ ls -la | grep "logKext"
drwxr-xr-x  3 root  wheel  102 Nov 19  2009 logKext.kext
```

76	0	0xffffffff7f81340000	0xa000	0xa000	com.apple.driver.AppleMCCSControl (1.0.24) <55 9 7 5 4 3 1>
77	0	0xffffffff7f81214000	0x5000	0x5000	com.apple.driver.AppleUpstreamUserClient (3.5.9) <55 9 8 7 5 4 3 1>
78	1	0xffffffff7f813e5000	0xa4000	0xa4000	com.apple.driver.DspFuncLib (2.1.1f12) <67 66 5 4 3 1>
79	0	0xffffffff7f81489000	0xaf000	0xaf000	com.apple.driver.AppleHDA (2.1.1f12) <78 67 65 64 57 55 6 5 4 3 1>
81	1	0xffffffff7f80f67000	0x5000	0x5000	com.apple.kext.triggers (1.0) <7 6 5 4 3 1>
82	0	0xffffffff7f80f6c000	0x9000	0x9000	com.apple.filesystems.autofs (3.0) <81 7 6 5 4 3 1>
83	0	0xffffffff7f81631000	0x5000	0x5000	com.vmware.kext.vmmemctl (0068.29.96) <7 5 4 3 1>
85	0	0xffffffff7f81637000	0xa000	0xa000	com.vmware.kext.vmhgfs (0068.29.96) <5 4 3 1>
88	0	0xffffffff7f80802000	0x4000	0x4000	com.fsb.kext.logKext (2.3) <25 4 3>

Other Files: Bash History

- ~/.bash_history
- File not written until logout
- 500 Entries by default
- Incident Response Tip:
 - Run the 'history' command for the logged in user.



Other Files:

User Accounts

- /private/var/db/dslocal/nodes/Default/users/
- Password Shadow – ShadowHashData Key (Lion)
- Password Shadow - /private/var/db/shadow/<User GUID>

```
sh-3.2# ls -lat
total 224
drwx----- 77 root wheel 2618 May 15 03:05 .
-rw----- 1 root wheel 1525 May 15 03:05 root.plist <- Not enabled by default!
-rw----- 1 root wheel 103449 May 12 19:21 user.plist
drw----- 12 root wheel 408 May 10 16:41 ..
-rw----- 1 root wheel 250 May 10 00:36 _taskgated.plist
-rw----- 1 root wheel 666 May 9 19:29 _krbtgt.plist
-rw----- 1 root wheel 260 May 9 19:20 _amavisd.plist
-rw----- 1 root wheel 261 May 9 19:20 _appowner.plist
-rw----- 1 root wheel 276 May 9 19:20 _appserver.plist
-rw----- 1 root wheel 248 May 9 19:20 _ard.plist
-rw----- 1 root wheel 254 May 9 19:20 _atsserver.plist
-rw----- 1 root wheel 266 May 9 19:20 _avbdeviced.plist
-rw----- 1 root wheel 250 May 9 19:20 _calendar.plist
```

Other Files:

Application Hooking

Flashback Example: DYLD_INSERT_LIBRARIES

Credentials Given

- Inserts the key "LSEnvironment" in subkey DYLD_INSERT_LIBRARIES in /Applications/Safari.app/Contents/Info.plist
- References *.xsl and/or *.png files in:
 - /Applications/Safari.app/Contents/Resources/

No Credentials Given

- Inserts DYLD_INSERT_LIBRARIES into ~/.MacOSX/environment.plist
- References: /Users/Shared/.libgmalloc.dylib file
 - References: Hidden .tmp file in /Users/<user>/Application Support/

Other Files: Shared Directory

/Users/Shared/

- Writable to all users

Flashback –
Mach-O
binaries

- Hidden *.so files
- .libgmalloc.dylib (Previous Slide)
- .tdem

Python
Backdoor

- update.py - backdoor
- update.sh – script to execute update.py

Basic Reverse Engineering

What

- Basic Reverse Engineering tools & techniques

Why

- Deeper look at the malware internals.

Basic Reverse Engineering:

Static: file & xxd

```
MBP:~ oompa$ file /Users/oompa/Downloads/logKext-2.3.pkg
/Users/oompa/Downloads/logKext-2.3.pkg: xar archive - version 1
MBP:~ oompa$ xxd /Users/oompa/Downloads/logKext-2.3.pkg | more
00000000: 7861 7221 001c 0001 0000 0000 0000 0b91  xar!.....
00000010: 0000 0000 0000 63e7 0000 0001 78da ec97  ....C....x...
00000020: 4b8f db36 1080 eff9 1582 ef8e f87e 045c  K..6.....~.\
00000030: 056d 81a0 bd15 e8f6 d21b 450e 6dc1 b264  .m.....E.m..d
00000040: 48da ad9d 5f5f 4a96 1fbb 6b79 dd2e d2a4  H..._J...ky....
00000050: 454e 1a0e 4743 8a33 1f67 643e 6ed7 65f2  EN..GC.3.gd>n.e.
00000060: 084d 5bd4 d5dd 0cbf 47b3 042a 57fb a25a  .M[.....G...*W..Z
```

Basic Reverse Engineering: Static: lipo

- Architecture Information

```
MBP:logKext oompa$ file logKextDaemon
logKextDaemon: Mach-O universal binary with 3 architectures
logKextDaemon (for architecture x86_64):      Mach-O 64-bit executable x86_64
logKextDaemon (for architecture i386):      Mach-O executable i386
logKextDaemon (for architecture ppc7400):      Mach-O executable ppc
MBP:logKext oompa$ lipo -detailed_info logKextDaemon
Fat header in: logKextDaemon
fat_magic 0xcafebabe
nfat_arch 3
architecture x86_64
    cputype CPU_TYPE_X86_64
    cpusubtype CPU_SUBTYPE_X86_64_ALL
    offset 4096
    size 24352
    align 2^12 (4096)
architecture i386
    cputype CPU_TYPE_I386
    cpusubtype CPU_SUBTYPE_I386_ALL
    offset 28672
    size 23896
    align 2^12 (4096)
architecture ppc7400
    cputype CPU_TYPE_POWERPC
    cpusubtype CPU_SUBTYPE_POWERPC_7400
    offset 53248
    size 21300
    align 2^12 (4096)
```

Basic Reverse Engineering:

Static: nm

- Display symbols
- Capabilities of program
- Xcode Required

```
bit:VMSHARE oompa$ nm -arch x86_64 logKextDaemon | more
0000000010000229e s stub helpers
                  U _BF_ecb_encrypt
                  U _BF_set_key
                  U _CFArrayAppendValue
                  U _CFArrayCreateMutable
                  U _CFBooleanGetValue
                  U _CFDataAppendBytes
                  U _CFDataCreate
                  U _CFDataCreateMutable
                  U _CFDataDeleteBytes
                  U _CFDataGetBytePtr
                  U _CFDataGetBytes
                  U _CFDataGetLength
                  U _CFDictionaryGetValue
                  U _CFLocaleCopyCurrent
                  U _CFNumberCreate
                  U _CFNumberFormatterCreate
                  U _CFNumberFormatterCreateStringWithValue
                  U _CFPreferencesAppSynchronize
                  U _CFPreferencesCopyAppValue
                  U _CFPreferencesGetAppBooleanValue
                  U _CFPreferencesGetAppIntegerValue
                  U _CFPreferencesSetAppValue
                  U _CFPropertyListCreateFromStream
                  U _CFReadStreamClose
                  U _CFReadStreamCreateWithFile
                  U _CFReadStreamOpen
                  U _CFRelease
```

Basic Reverse Engineering:

Static: otool

- Shared Libraries
- Xcode Required

```
bit:VMSHARE oompa$ otool -L logKextDaemon | more
logKextDaemon:
    /System/Library/Frameworks/IOKit.framework/Versions/A/IOKit (compatibility version 1.0.0, current version 275.0.0)
    /usr/lib/libcrypto.0.9.7.dylib (compatibility version 0.9.7, current version 0.9.7)
    /System/Library/Frameworks/Security.framework/Versions/A/Security (compatibility version 1.0.0, current version 36371.0.0)
    /System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation (compatibility version 150.0.0, current version 476.18.0)
    /System/Library/Frameworks/SystemConfiguration.framework/Versions/A/SystemConfiguration (compatibility version 1.0.0, current version 212.2.0)
    /usr/lib/libstdc++.6.dylib (compatibility version 7.0.0, current version 7.4.0)
    /usr/lib/libgcc_s.1.dylib (compatibility version 1.0.0, current version 1.0.0)
    /usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 111.1.4)
```


Basic Reverse Engineering: Dynamic: vmmap

- Display virtual memory regions for a process.

```
MBP:~ oompa$ sudo vmmap 296 | more
Virtual Memory Map of process 296 (logKextDaemon)
Output report format: 2.2 -- 64-bit process

==== Non-writable regions for process 296
__TEXT                0000000010000000-00000000100003000 [ 12K] r-x/rwx SM=COW /Library/Application Support/logKext/logKextDaemon
__LINKEDIT            00000000100005000-00000000100007000 [  8K] r--/rwx SM=COW /Library/Application Support/logKext/logKextDaemon
__TEXT                00000000100007000-000000001000eb000 [ 912K] r-x/rwx SM=COW /usr/lib/libcrypto.0.9.7.dylib
__LINKEDIT            0000000010010a000-00000000100140000 [ 216K] r--/rwx SM=COW /usr/lib/libcrypto.0.9.7.dylib
MALLOC metadata       00000000100140000-00000000100141000 [  4K] r--/rwx SM=COW
```

Basic Reverse Engineering: Dynamic: lsof

- com.fsb.logKext <- Keylog file!

```
MBP:~ oompa$ sudo lsof -p 53
COMMAND  PID USER  FD   TYPE    DEVICE  SIZE/OFF  NODE NAME
logKextDa 53 root  cwd    DIR      14,2    1156      2 /
logKextDa 53 root  txt    REG      14,2   74548  426352 /Library/Application Support/logKext/logKextDaemon
logKextDa 53 root  txt    REG      14,2  2251584   5803 /usr/lib/libcrypto.0.9.7.dylib
logKextDa 53 root  txt    REG      14,2   51288  427680 /private/var/db/mds/system/mdsDirectory.db
logKextDa 53 root  txt    REG      14,2   35640  426371 /Library/Keychains/System.keychain
logKextDa 53 root  txt    REG      14,2 16285968  34732 /usr/share/icu/icudt46l.dat
logKextDa 53 root  txt    REG      14,2   599232   8982 /usr/lib/dyld
logKextDa 53 root  txt    REG      14,2 288935936 282671 /private/var/db/dyld/dyld_shared_cache_x86_64
logKextDa 53 root  0r     CHR       3,2       0t0     302 /dev/null
logKextDa 53 root    1     PIPE 0xffffffff80066784d0 16384 -->0xffffffff8006678580
logKextDa 53 root    2     PIPE 0xffffffff80066784d0 16384 -->0xffffffff8006678580
logKextDa 53 root   3w     REG      14,2    3912  426390 /Library/Preferences/com.fsb.logKext
logKextDa 53 root   4u  KQUEUE                   count=1, state=0x2
```

Basic Reverse Engineering: Dynamic: iosnoop

- Track IO events

```
MBP:~ oompa$ cat lk_install.txt | grep -i logkext
0 397 W 16955040 36864 installld ???/Boms/com.fsb.logkext.logkextReadme.pkg.bom
0 397 W 16955144 8192 installld ???/Root/LogKext Readme.html
0 397 W 16956112 36864 installld ???/Boms/com.fsb.logkext.logkextuninstall.pkg.bom
0 397 W 16956184 4096 installld ???/Root/LogKextUninstall.command
0 397 W 16956192 36864 installld ???/Boms/com.fsb.logkext.logkext.pkg.bom
0 397 W 16956264 4096 installld ???/LaunchDaemons/logKext.plist
0 397 W 16956272 36864 installld ???/Boms/com.fsb.logkext.logkextkeymap.pkg.bom
0 397 W 16956344 8192 installld ???/logKext/logKextKeymap.plist
0 397 W 16956448 36864 installld ???/Boms/com.fsb.logkext.logkextExt.pkg.bom
0 397 W 16956520 4096 installld ???/com.fsb.logkext.logkextExt.pkg.Gjplwp/postflight
0 397 W 16956528 4096 installld ???/com.fsb.logkext.logkextExt.pkg.Gjplwp/postinstall
0 397 W 17100768 12288 installld ???/MacOS/logKext
0 397 W 17100800 36864 installld ???/Boms/com.fsb.logkext.logkextdaemon.pkg.bom
0 397 W 17100872 73728 installld ???/logKext/.BC.jZ0cU5
0 397 W 17101016 4096 installld ???/logKext/logKextDaemon
0 397 W 17101024 36864 installld ???/Boms/com.fsb.logkext.logkextclient.pkg.bom
0 397 W 17102792 4096 installld ???/bin/logKextClient
0 397 W 17247288 36864 installld ???/Boms/com.fsb.logkext.logkextkeygen.pkg.bom
0 397 W 18349472 40960 installld ???/logKext/.BC.tB0fse
0 397 W 18349552 4096 installld ???/logKext/logKextKeyGen
89 343 R 16955144 4096 mdworker ???/Macintosh HD/LogKext Readme.html
89 343 R 16955144 8192 mdworker ???/Macintosh HD/LogKext Readme.html
89 343 R 16956184 4096 mdworker ???/Macintosh HD/LogKextUninstall.command
0 10 R 17068304 4096 kextd ???/MacOS/logKext
0 10 R 17068312 28672 kextd ???/MacOS/logKext
0 10 R 17068368 20480 kextd ???/MacOS/logKext
0 414 R 16956528 4096 installld ???/com.fsb.logkext.logkextExt.pkg.Gjplwp/postinstall
0 426 R 18349472 4096 sh ???/logKext/logKextKeyGen
```

Reverse Engineering: Dynamic: execsnoop

- Track process execution events.

```
MBP:~ oompa$ cat lk_install.txt
UID    PID    PPID  ARGS
0      394     1    diskmanagementd
0      395     1    sandboxd
501    396     391    runner
92     397     1    SecurityAgent
0      398     1    authorizationhos
0      399     1    kcm
0      400     1    installd
0      401     1    authorizationhos
0      402     1    authorizationhos
0      403     1    authorizationhos
0      404     400    update_dyld_shar
501    405     55    SFLSharedPrefsTo
501    406     55    SFLSharedPrefsTo
501    407     140   PubSubAgent
0      408     400    xpchelper
0      409     400    shove
0      410     400    kextcache
0      411     1    launchdadd
0      412     400    kextcache
0      412     400    kextcache
0      10      1    kextd
0      10      1    kextd
0      416     400    sh
0      417     416    find
0      418     417    chmod
0      419     417    chmod
0      420     417    chmod
0      421     417    chmod
0      422     417    chmod
0      423     417    chmod
0      424     417    chmod
0      425     417    chmod
0      426     416    kextunload
0      427     416    kextload
0      429     1    taskgated
0      428     416    logKextKeyGen
0      430     416    launchctl
0      431     1    logKextDaemon
0      432     416    open
0      433     55    SFLTconTool
501    346     140   Safari
0      435     1    launchdadd
0      436     400    efw_cache_update
0      437     55    SFLSharedPrefsTo
```

Basic Reverse Engineering: Other Tools

- ◉ opensnoop – File Opens
- ◉ rwsnoop – File Read/Writes
- ◉ IDA – Disassembler (hex-rays.com)
- ◉ GDB – GNU Debugger
- ◉ Instruments (Xcode Developer Tools)



When Macs Get Hacked

Sarah Edwards

@iamevltwin

oompa@csh.rit.edu
