

Tor Forensics on Windows OS

Ву

Mattia Epifani, Marco Scarito and Francesco Picasso

Presented At

The Digital Forensic Research Conference

DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

TOR BROWSER FORENSICS ON WINDOWS OS

MATTIA EPIFANI, FRANCESCO PICASSO, MARCO SCARITO, CLAUDIA MEDA

DFRWS 2015

DUBLIN, 24 MARCH 2015

REAL CASE

- Management salaries of a private company were published on a Blog
- Through an analysis of the internal network, we found a possible suspect because he accessed the Excel file containing the salaries the day before the publication
- Company asked us to analyze the employee laptop
- We found evidences that confirm that the Excel file was opened [LNK, Jumplist, ShellBags]
- But no traces were found in browsing history about the publishing activity on the blog...

PREVIOUS RESEARCH

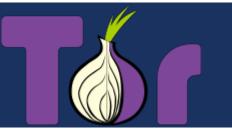
An interesting research by Runa Sandvik is available at

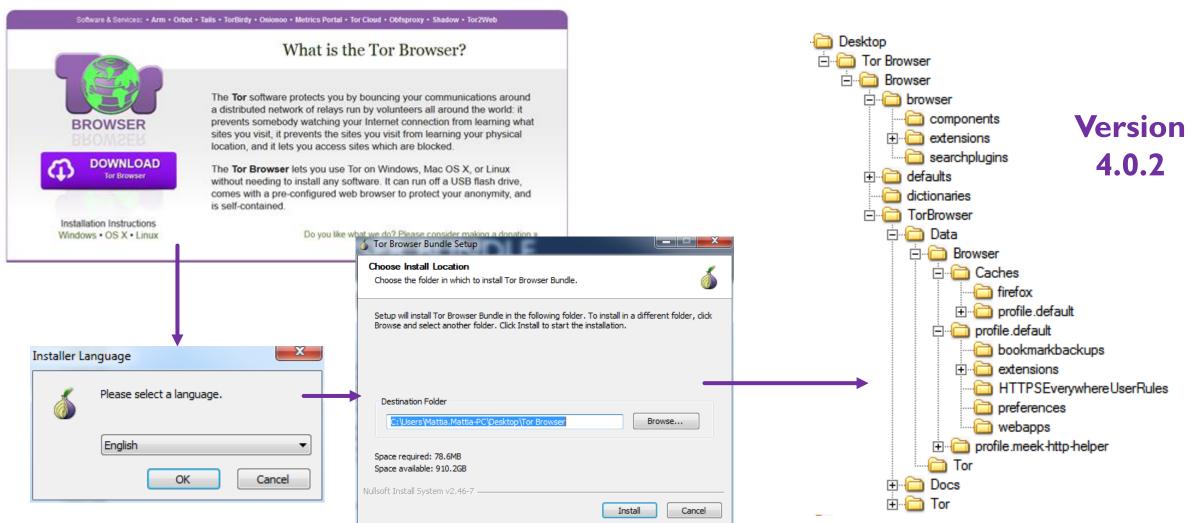
Forensic Analysis of the Tor Browser Bundle on OS X, Linux, and Windows

https://research.torproject.org/techreports/tbb-forensic-analysis-2013-06-28.pdf

We started from her work to find other interesting artifacts



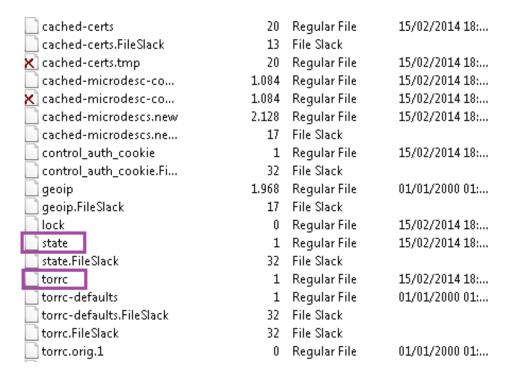




TOR BROWSER FOLDER

■ The most interesting folders are located in \Tor Browser\Browser\Tor Browser:

\Data\Tor



\Data\Browser\profile.default

뷆 bookmarkbackups	1
extensions	1
HTTPSEverywhereUser	1
ll preferences	1
ll webapps	1
SI30	8
g blocklist.xml	146
blocklist.xml.FileSlack	3
o bookmarks.html	4
compatibility.ini	1
cookies.sqlite	512
extensions.ini	1
extensions.ini.FileSlack	4
extensions.json	10
extensions.json.FileSlack	3
extensions.sqlite	0

1	Directory	12/12/2014 14:
1	Directory	30/01/2015 15:
1	Directory	12/12/2014 14:
1	Directory	12/12/2014 14:
1	Directory	30/01/2015 14:
8	NTFS Index All	30/01/2015 15:
146	Regular File	01/01/2000
3	File Slack	
4	Regular File	01/01/2000
1	Regular File	30/01/2015 14:
512	Regular File	12/12/2014 15:
1	Regular File	30/01/2015 14:
4	File Slack	
10	Regular File	30/01/2015 14:
3	File Slack	
0	Regular File	12/12/2014 14:

FOLDER DATA\TOR

State: it contains the last execution date

```
# Tor state file last generated on 2014-02-15 18:59:26 local time
# Other times below are in UTC
# You *do not* need to edit this file.

TorVersion Tor 0.2.4.20 (git-d90102bcf0c25d96)
LastWritten 2014-02-15 17:59:26
```

Torrc: it contains the path from where the Tor Browser was launched with the drive letter

```
# This file was generated by Tor; if you edit it, comments will not be preserved # The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it
```

```
DataDirectory E:\Tor Browser\Data\Tor
DirReqStatistics 0
GeoIPFile E:\Tor Browser\Data\Tor\geoip
```

FOLDER \DATA\BROWSER\PROFILE.DEFAULT

- The traditional Firefox folder containing the user profile without usage traces
- The most interesting files:
 - Compatibility.ini
 - Extension.ini

```
[ExtensionDirs]
ExtensionO=E:\Tor Browser\Data\Browser\profile.default\extensions\tor-launcher@torproject.o
Extension1=E:\Tor Browser\Data\Browser\profile.default\extensions\torbutton@torproject.org.
Extension2=E:\Tor Browser\Data\Browser\profile.default\extensions\{73a6fe31-595d-460b-a920-Extension3=E:\Tor Browser\Data\Browser\profile.default\extensions\https-everywhere@eff.org
```

```
[Compatibility]
LastVersion=24.3.0_20000101000000/20000101000000
LastOSABI=WINNT_x86-gcc3
LastPlatformDir=E:\Tor Browser\Browser
```

LastAppDir=E:\Tor Browser\Browser\browserInvalidateCaches=1

- Browser execution path
- Date Created → First execution
- Date Modified → Last execution

OS ARTIFACTS ANALYSIS

- Evidence of TOR usage can be found (mainly) in:
 - ☐ Prefetch file TORBROWSERINSTALL-<VERSION>-<PATH-HASH>.pf
 - ☐ Prefetch file TOR.EXE-<PATH-HASH>.pf
 - □ Prefetch file FIREFOX.EXE-<PATH-HASH>.pf
 - ☐ Prefetch file **START TOR BROWSER.EXE-<PATH-HASH>.pf** (old version < 4.0.2)
 - □ NTUSER.DAT registry hive → User Assist key
 - Windows Search Database
 - ☐ Thumbnail cache

PREFETCH FILES

- We can recover:
 - First execution date
 - Last execution date
 - In Windows 8/8.1 → Last 8 executions
 - Number of executions
 - Execution Path
 - Install date (from Tor Browser Install prefetch file)
 - Tor Browser version (from Tor Browser Install prefetch file)

File Name	Created Date	Modified Dat	Date Last Run	Num Times Run	Physical Path
TORBROWSER-INSTALL-3.6.6_EN-U-6C8C8FDE.pf	giovedì 2 otto	giovedì 2 ott	giovedì 2 ottobre 2014 (gio) 20:44:01	1	\DEVICE\HARDDISKVOLUME2\USERS\MATTIA.MATTIA-PC\DOWNLOADS\TORBROWSER-INSTALL-3.6.6_EN-US.EXE
START TOR BROWSER.EXE-E2BF03B1.pf	giovedì 2 otto	giovedì 2 ott	giovedì 2 ottobre 2014 (gio) 21:36:34	5	\DEVICE\HARDDISKVOLUME2\USERS\MATTIA.MATTIA-PC\DESKTOP\TOR BROWSER\START TOR BROWSER.EXE
TOR.EXE-60C44E64.pf	giovedì 2 otto	giovedì 2 ott	giovedì 2 ottobre 2014 (gio) 21:36:35	5	\DEVICE\HARDDISKVOLUME2\USERS\MATTIA.MATTIA-PC\DESKTOP\TOR BROWSER\TOR\TOR.EXE

USER ASSIST

- We can recover:
 - Last execution date
 - Number of executions
 - Execution path
- By analyzing various NTUSER.DAT from VSS we can identify the number and time of execution in a period of interest

```
userassist2 v.20120528
(NTUSER.DAT) Displays contents of UserAssist subkeys
```

UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Wed Jul 24 16:27:27 2013 (UTC)

```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Mon Feb 17 08:30:05 2014 Z
Microsoft.InternetExplorer.Default (2)
Sat Feb 15 17:59:09 2014 Z
E:\Tor Browser\Start Tor Browser.exe (1)
```

OTHER ARTIFACTS ON THE HARD DRIVE

- Other files noted:
 - Thumbnail Cache
 - It contains the TOR Browser icon
 - Windows Search Database
 - Tor Browser files and folders path

BROWSING ACTIVITIES

- Evidence of browsing activities can be found in:
 - Bookmarks (places.sqlite database)
 - Pagefile.sys
 - Memory Dump / Hiberfil.sys

BOOKMARKS

User saved bookmarks:

Recent Tags	<null></null>	<null></null>	1414688034288000	1414688034288000	Qj3Kx5y2EcFe
REALITY NET - System Solutions - Digital Forensics	≺null≻	<null></null>	1414839318764000	1414839319124000	bvDNaxlUnvmU

Convert epoch to human readable date and vice versa

414839318764000 Timestamp to Human date e [batch convert timestamps to human dates]

Assuming that this timestamp is in microseconds (1/1,000,000 second):

GMT: Sat, 01 Nov 2014 10:55:18 GMT

Your time zone: sabato 1 novembre 2014 11:55:18 GMT+1:00

PAGEFILE.SYS

- Information about visited websites
- Search for the keywordHTTP-memory-only-PB

HTTP-MEMORY-ONLY-PB

- A function used by Mozilla Firefox for Private Browsing (not saving cache data on the hard drive)
- Tor Browser uses the Private Browsing feature of Mozilla Firefox
- But Tor Browser typically uses an old Firefox version, based on Firefox
 ESR
- To distinguish if the browsing activity was made with Mozilla Firefox or with Tor Browser:
 - Check if Firefox is installed
 - If it is installed, verify the actual version

PAGEFILE.SYS - EXAMPLE

```
00 A / P# @ Ae. b / @#
68 65 M
               «àa
                             GET /The
      mes/default/images/theme/frame r
72 6F epeat.png HTTP/1.1 Host: silkro
  6F ad5v7dvwlc.onion User-Agent: Mo
  34 zilla/5.0 (Windows NT 6.1; rv:24
30 0D .0) Gecko/20100101 Firefox/24.0
2E 38 Accept: image/png,image/*;g=0.8
     ,*/*;q=0.5 Accept-Language: en-
      us,en;q=0.5 Accept-Encoding: gz
     ip, deflate Referer: http://sil
  75 kroad5v7dywlc.onion/Themes/defau
3A 20 lt/css/index.css?fin20 Cookie:
62 71 PHPSESSID=ulgi0a8rdhslnhpu5012bg
OD OA u5p6 Connection: keep-alive
```

```
79 2D 6F 6E 6C 79
72 69 3D 68 74 74
2F 69 6D 61 67 65
00 00 00 00 00 00
```

```
67 65 73
           eep-alive
                        GET /it/home/images
A 48 6F 73 /30 years copy.png HTTP/1.1 Hos
A 20 4D 6F
           t: www.apple.com User-Agent: Mo
6 3A 32 39 zilla/5.0 (Windows NT 6.1; rv:24
4 2E 30 0D .0) Gecko/20100101 Firefox/24.0
D 30 2E 38
           Accept: image/png,image/*;q=0.8
           ,*/*;q=0.5 Accept-Language: en-
A 20 67 7A
           us, en; q 0.5 Accept-Encoding: qz
           ip, deflate Referer: https://ww
           w.applk.com/it/ Connection: kee
           p-alive
5 73 2F 70 |
                      GET /it/home/images/p
```

```
:úçak" % HTTP-memory-only
-PB:domain=www.apple.com&uri=htt
ps://www.apple.com/it/home/image
s/30 years copy.png
```

ANALYSIS METHODOLOGY

Prefetch files

- Install date
- First execution date
- Last execution date(s)
- Number of executions
- Tor Browser version

NTUSER\UserAssist key

- Execution path
- Last execution date
- Total number of executions
- Verify the history of execution through the Volume Shadow Copies

Other possible artifacts

- Thumbnail Cache
- Windows Search Database

Tor Browser Files

- State
- Torrc
- Compatibility.ini
- Extension.ini
- Places.sqlite [Bookmarks]

Pagefile.sys (keywords search)

- •HTTP-memory-only-PB
- Torproject
- •Tor
- •Torrc
- Geoip
- Torbutton
- •Tor-launcher

Hiberfil.sys

- · Convert to a memory dump
- · Analyze through
- Volatility
- Keywords search

REAL CASE

- We indexed the hard drive and searched for the blog URL
- We found some interesting URLs in the pagefile, indicating the access to the Blog Admin page (http://www. blognameblabla.com/wp-admin/)

REAL CASE

- All the URLs were preceded by the string HTTP-MEMORY-ONLY-PB and Firefox is not installed on the laptop
- We found that the TOR Browser was downloaded with Google
 Chrome the night in which the file was published on the blog
- By analyzing the OS artifacts we found that it was installed and only executed once, 3 minutes before the publish date and time on the blog

ACTIVE RESEARCHES

- Memory Dump with Volatility and Rekall
- Can we find any temporal reference for browsing activities?
- Can we correlate Tor Browser cache entries to carved files from pagefile/hiberfil/memory dump?
- Tor Browser on Mac OS X
- Tor Browser on Linux
- Orbot on Android

Q&A?

Mattia Epifani

- Digital Forensics Analyst
- CEO @ REALITY NET System Solutions
- GCFA, GMOB, GNFA, GREM
- CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

Mail mattia.epifani@realitynet.it

Twitter @mattiaep

Linkedin http://www.linkedin.com/in/mattiaepifani

Web http://www.realitynet.it

Blog http://blog.digital-forensics.it

http://mattiaep.blogspot.it



KEEP CALM AND THANK YOU FOR YOUR ATTENTION