TOR FORENSICS ON WINDOWS OS

MATTIA EPIFANI

SANS EU DIGITAL FORENSICS SUMMIT

PRAGUE, 5 OCTOBER 2014

REAL CASE

- Management salaries of a big private company were **published on a Blog**
- Through a traditional analysis of the internal network, the company **found a suspect**:
  - He accessed the Excel file containing the salaries by connecting from his desktop to his manager's computer through Terminal Server
  - He saved the file on a pen drive
- Company denounced the employee and Police **seized his personal laptop** at home

PREVIOUS RESEARCH

- Some interesting research by Runa Sandvik is available at

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

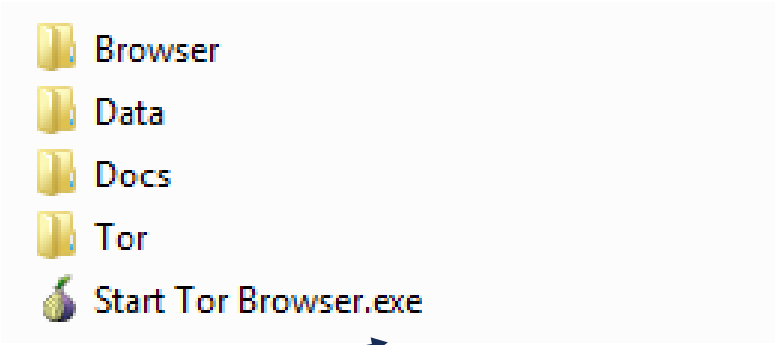
  https://research.torproject.org/techreports/tbb-forensic-analysis-2013-06-28.pdf

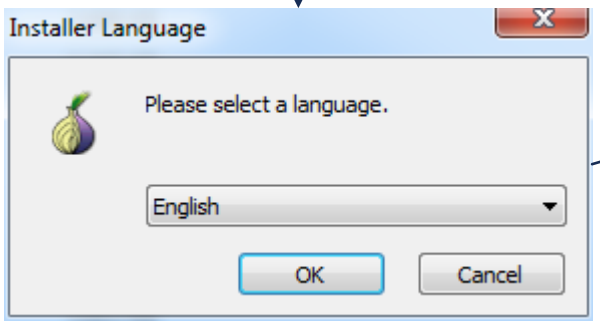
- We started from there to find other interesting artifacts…

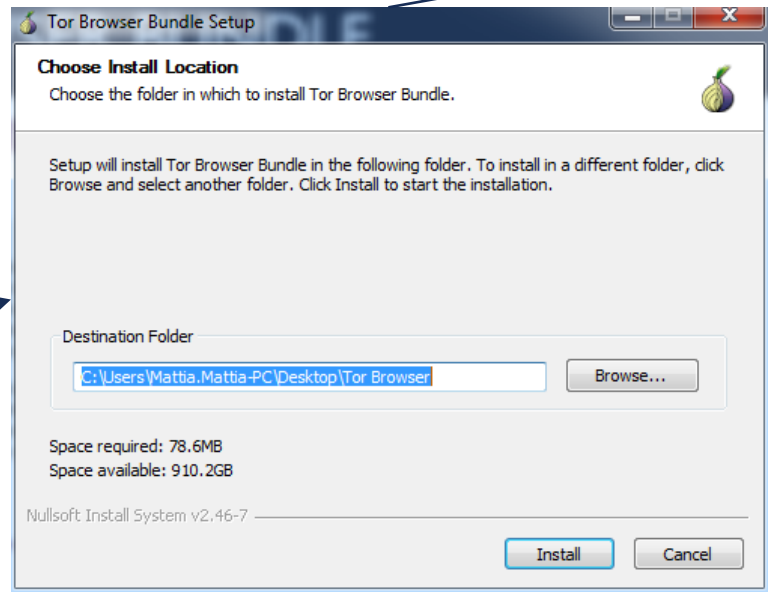
TOR BROWSING TOOLS

- TOR is a system to browse the Internet anonymously
- The tools to surf the Internet through TOR are:
  - **Tor Browser Bundle**
    - Windows/Mac/Linux
    - Can be executed by unzipping it on the hard drive or on an external device (e.g. USB Pen Drive)
  - **Live CD/USB Tails**
  - **Orbot** (Android App)
- Tools available at **https://www.torproject.org**

TOR BROWSER BUNDLE







TOR BROWSER FOLDER

- The most interesting folders are:

\Data\Tor

cached-certs	20	Regular File	15/02/2014 18:...
cached-certs.FileSlack	13	File Slack	
cached-certs.tmp	20	Regular File	15/02/2014 18:...
cached-microdesc-co...	1.084	Regular File	15/02/2014 18:...
cached-microdesc-co...	1.084	Regular File	15/02/2014 18:...
cached-microdescs.new	2.128	Regular File	15/02/2014 18:...
cached-microdescs.ne...	17	File Slack	
control_auth_cookie	1	Regular File	15/02/2014 18:...
control_auth_cookie.Fi...	32	File Slack	
geoip	1.968	Regular File	01/01/2000 01:...
geoip.FileSlack	17	File Slack	
lock	0	Regular File	15/02/2014 18:...
state	1	Regular File	15/02/2014 18:...
state.FileSlack	32	File Slack	
torrc	1	Regular File	15/02/2014 18:...
torrc-defaults	1	Regular File	01/01/2000 01:...
torrc-defaults.FileSlack	32	File Slack	
torrc.FileSlack	32	File Slack	
torrc.orig.1	0	Regular File	01/01/2000 01:...
unverified-microdesc-...	1.084	Regular File	15/02/2014 18:...

\Data\Browser

addons.sqlite-journal	289	Regular File	15/02/2014 19:...
addons.sqlite-journal....	32	File Slack	
blocklist.xml	111	Regular File	15/02/2014 19:...
blocklist.xml.FileSlack	18	File Slack	
bookmarks.html	4	Regular File	01/01/2000 01:...
bookmarks.html.FileSl...	29	File Slack	
cert8.db	64	Regular File	15/02/2014 18:...
compatibility.ini	1	Regular File	15/02/2014 18:...
compatibility.ini.FileSl...	32	File Slack	
cookies.sqlite	512	Regular File	15/02/2014 18:...
cookies.sqlite-journal	1	Regular File	15/02/2014 18:...
cookies.sqlite-journal	33	Regular File	15/02/2014 18:...
cookies.sqlite-journal	33	Regular File	15/02/2014 18:...
cookies.sqlite-journal	33	Regular File	15/02/2014 18:...
downloads.sqlite	96	Regular File	15/02/2014 19:...
downloads.sqlite-jour...	1	Regular File	15/02/2014 19:...
downloads.sqlite-jour...	33	Regular File	15/02/2014 19:...
downloads.sqlite-jour...	33	Regular File	15/02/2014 19:...
downloads.sqlite-jour...	32	File Slack	
extensions.ini	1	Regular File	15/02/2014 18:...
extensions.ini.FileSlack	32	File Slack	

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

- It is the traditional Firefox folder containing the user profile, but **without usage traces**
- The most interesting files are **Compatibility.ini** and **Extension.ini** and contain the **browser execution path**

```
[ExtensionDirs]
Extension0=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
```

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 **START TOR BROWSER.EXE-<PATH-HASH>.pf**
  - NTUSER.DAT registry hive → **User Assist** key

PREFETCH FILES

- We can recover:
  - **Install date**
  - **First execution date**
  - **Last execution date**
  - **Number of executions**

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 execution**
  - **Execution path**
- By analyzing various NTUSER.DAT from VSS we can **identify the number and time of execution in a period of interest**

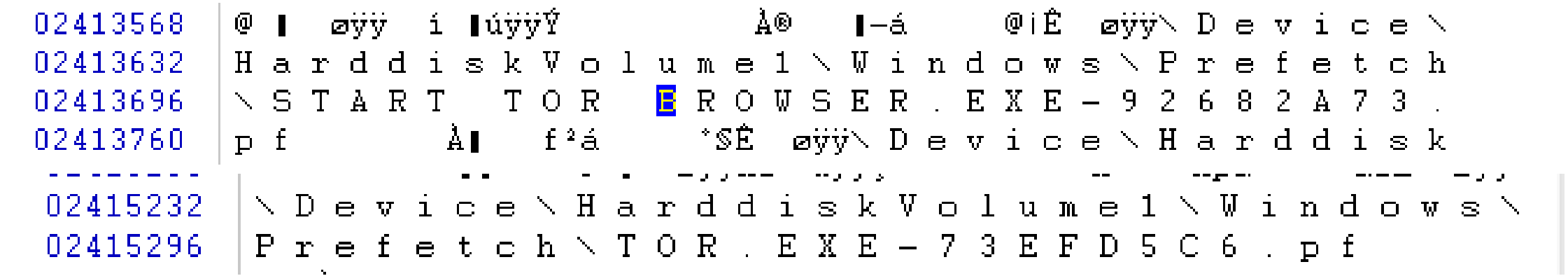
```
userassist2 v.20120528
(NTUSER.DAT) Displays contents of UserAssist subkeys

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 (PAPER)

- In Runa Sandvik paper other files are noted:
  - **Thumbnail Cache** (it contains the TOR Browser icon)
  - **USRCLASS.DAT registry file**
  - **Windows Search Database**

BOOKCKCL.ETL

- We can recover information about Prefetch file created by the OS
- It is useful because you can identify that the Tor Browser was used **also if the Prefetch files were deleted**
- Strings are saved in UNICODE



PAGEFILE.SYS

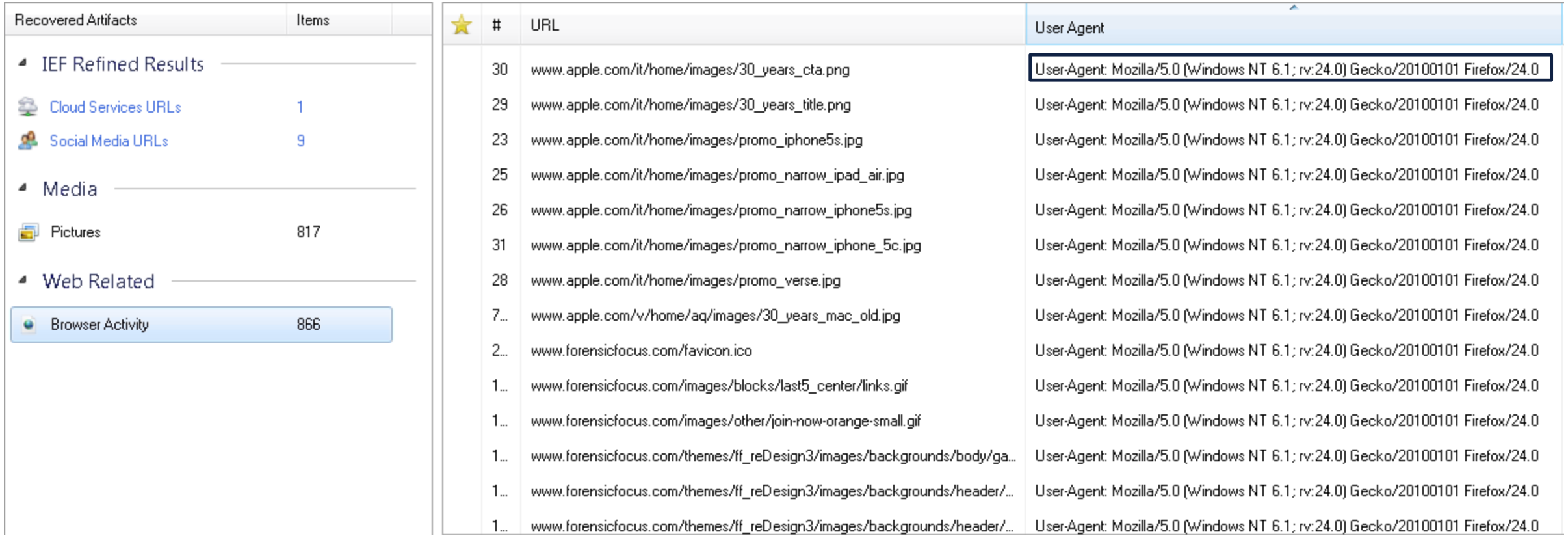
- Here you can find **information about visited websites**!
- Search for the keyword **HTTP-memory-only-PB**

```
..óy...˜....ý...HTTP-memory-only-PB:domain=genoacfc.it&uri=http:
//genoacfc.it/wp-content/plugins/footballclub/js/yoxview/images/
popup_ajax_loader.gif.....................................
```

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**
- 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 WITH INTERNET EVIDENCE FINDER



ANALYSIS METHODOLOGY

Prefetch files

- Install date
- First execution date
- Last execution date
- Number of executions

NTUSER\UserAssist key

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

Other possilbe artifacts

- BookCKCL.etl
- Thumbnail Cache
- USRCLASS.DAT registry
- Windows Search Database

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

- By analyzing the laptop we **found evidence of Excel file opening from the same pen drive** on personal laptop
- But **no traces** were found **in browsing history** about the publishing activity on the blog…
- We indexed the entire hard drive and searched for the blog URL
- We found some **interesting URLs in the pagefile**, indicating the access to the **Blog Admin page**

REAL CASE

- The URLs were always **preceded by the string HTTP-MEMORY-ONLY-PB**
- 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…10 minutes before the publish date and time on the blog!**

Q&A?

Mattia Epifani

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

Mail	**mattia.epifani@realitynet.it**
Twitter	**@mattiaep**
Linkedin	**http://www.linkedin.com/in/mattiaepifani**
Blog	**http://blog.digital-forensics.it**
	http://mattiaep.blogspot.it