Hacking & digital forensics

Erik Poll

Digital Security

Radboud Universiteit

Overview

- *How* are systems hacked?
- *Why* are systems hacked?
- What can be done to *prevent* hacking?
- What can be done to *detect* hacking?
  - digital forensics & anti-forensics

What is hacking?

Definition (1)

Using a system in a clever, unexpected way to get better performance or better fuctionality

- **Not necessarily something bad,**
  not necessarily a computer system

Definition (2)

***Ab*using a system**

- **to get (unauthorised) access to it , or**
- **to get extra rights on it, aka privilige escalation**

How are systems hacked?

How are computer systems hacked?

Two basic techniques

1. **stealing, eavesdropping, or guessing *credentials*,**
   eg. username/passwords, PIN codes, cookies,...

2. **exploiting a security flaw in the software**
   by feeding malicious input to the victim's software

Often combined with social engineering to trick the human victim into

- **revealing passwords (eg. phishing)**
- **opening a malicious email attachment**

Hacks often involve a combination of both techniques, in several stages.

Attack techniques for stealing credentials

- brute force guessing, eg with a dictionary attack,
  - online on the live system
  - offline on a stolen password file (with hashed passwords)
- fake websites, and phishing email to trick people into going there
- compromising the real website
- installing a physical keylogger or keylogging software
- eavesdropping on network connections
  - eg on public, unprotected wifi connection
- shoulder surfing
- phoning victims and asking them
- ....

After breaking into any system, the attacker will try to obtain more credentials to attack other systems

Security flaws in software

Software is the most complex artifact produced by mankind.

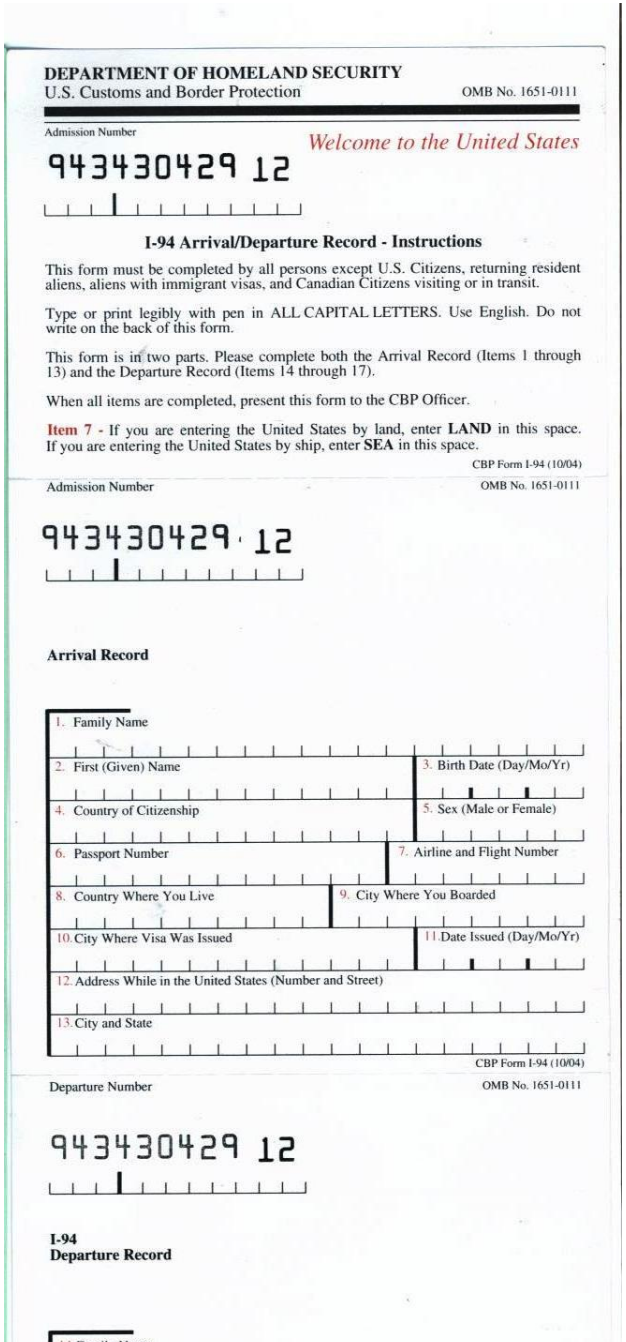
By feeding malicious input to some software an attacker may crash the software or trigger unintended behaviour

Sometimes infecting a computer requires getting the victim

- to open a malicious PDF document, to then exploit a security flaw in Adobe Acrobat Reader
- to visit a website, to then exploit a security flaw
  - in their browser (eg. Internet Explorer)
  - or in some browser plugin (eg Flash video player)

Virus scanners can detect signatures of *known* exploits in downloaded files or in attachments, but not for new zero day attacks.

buffer overflow attack



DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection
OMB No. 1651-0111

Admission Number

943430429 12

Welcome to the United States

I-94 Arrival/Departure Record - Instructions

This form must be completed by all persons except U.S. Citizens, returning resident aliens, aliens with immigrant visas, and Canadian Citizens visiting or in transit.

Type or print legibly with pen in ALL CAPITAL LETTERS. Use English. Do not write on the back of this form.

This form is in two parts. Please complete both the Arrival Record (Items 1 through 13) and the Departure Record (Items 14 through 17).

When all items are completed, present this form to the CBP Officer.

Item 7 - If you are entering the United States by land, enter **LAND** in this space. If you are entering the United States by ship, enter **SEA** in this space.

CBP Form I-94 (10/04)

Admission Number
OMB No. 1651-0111

943430429 12

Arrival Record

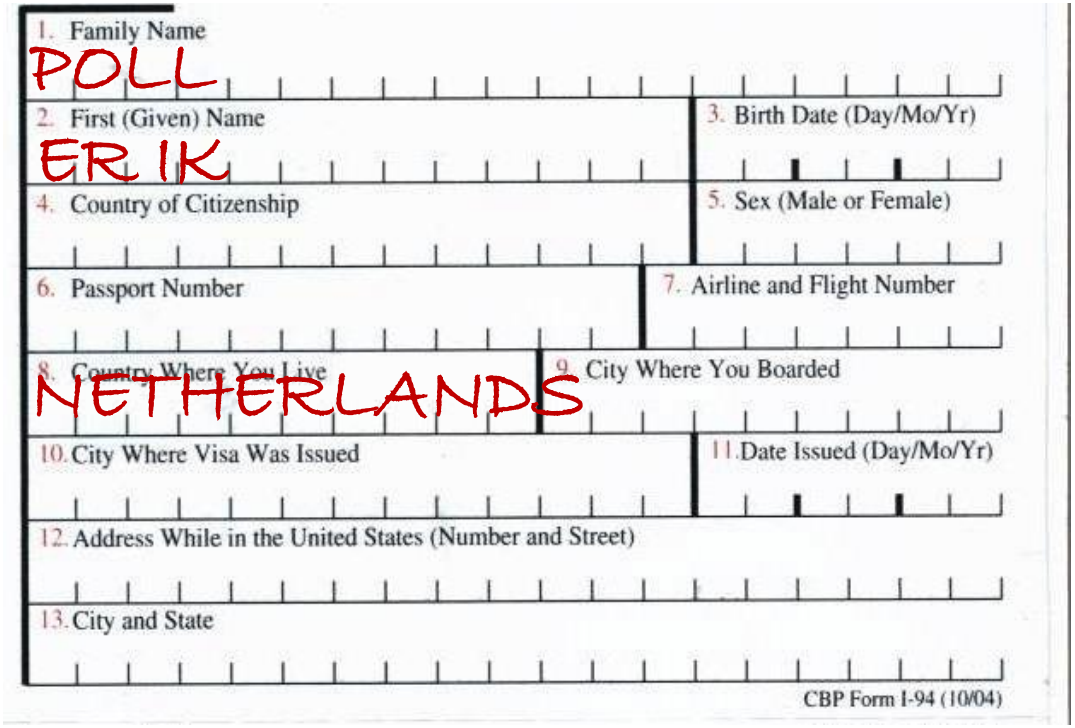
1. Family Name
2. First (Given) Name
3. Birth Date (Day/Mo/Yr)
4. Country of Citizenship
5. Sex (Male or Female)
6. Passport Number
7. Airline and Flight Number
8. Country Where You Live
9. City Where You Boarded
10. City Where Visa Was Issued
11. Date Issued (Day/Mo/Yr)
12. Address While in the United States (Number and Street)
13. City and State

CBP Form I-94 (10/04)

Departure Number
OMB No. 1651-0111

943430429 12

I-94
Departure Record



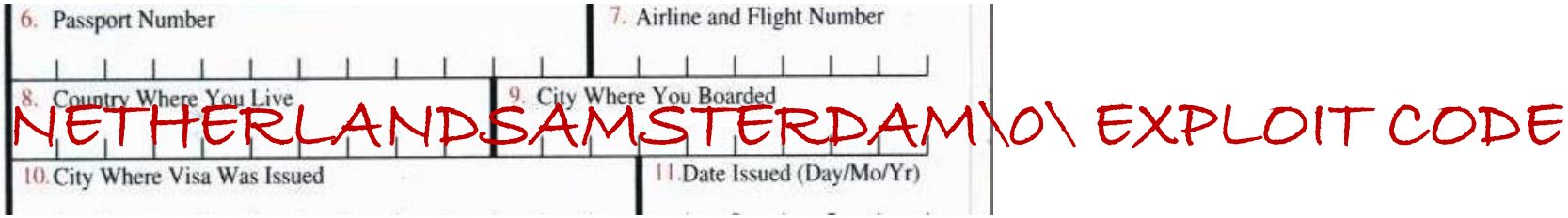
1. Family Name
POLL
2. First (Given) Name
ERIK
3. Birth Date (Day/Mo/Yr)
4. Country of Citizenship
5. Sex (Male or Female)
6. Passport Number
7. Airline and Flight Number
8. Country Where You Live
NETHERLANDS
9. City Where You Boarded
10. City Where Visa Was Issued
11. Date Issued (Day/Mo/Yr)
12. Address While in the United States (Number and Street)
13. City and State

CBP Form I-94 (10/04)

buffer overflow attack

A classic security is the buffer overflow:

some user input to a program too long for the memory reserved to it



The overflow will corrupts some bits in memory, which may trigger all sort of strange behaviour.

Optimal scenario (for the attacker): remote code execution, where the malicious input gives the attacker complete control of that program

command injection attack

Suppose we program a waiter robot

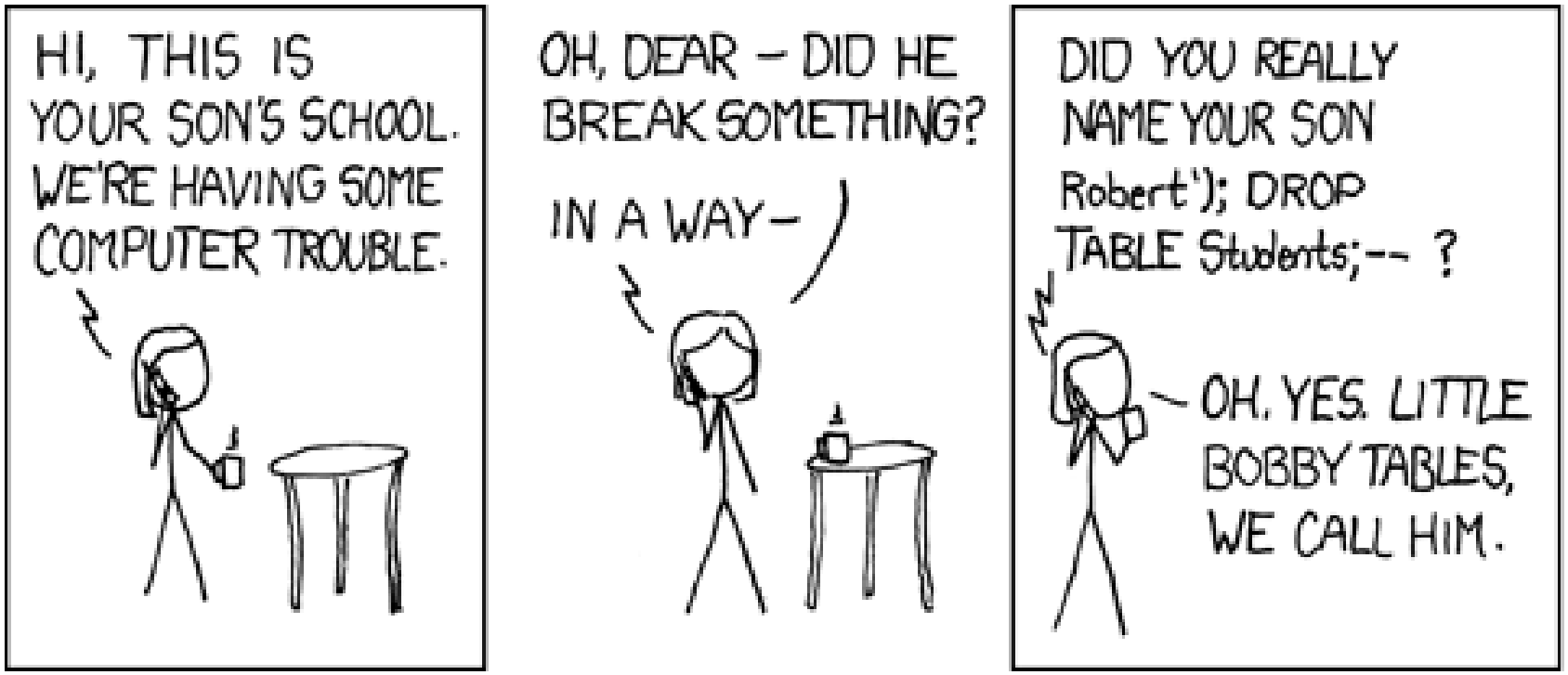
```
1   Wait for customer
2   Ask ("What do you want to drink?")
3   Input($drink)
4   Give($drink)
5   Goto 1
```

An attacker may give malicious input to the waiter robot

```
a coffee and the content of the till
```

Software will happily execute this, without realising anything is wrong

example command injection: SQL injection



Instructions for the database included *in* a malicious user input, eg. username

Security flaws everywhere !

Software – and hence security flaws - are everywhere:

not just in laptops, phones, and servers,

but also in cars, printers, ATMs, routers, firewall equipment,...

To get an impression of the problem, look at weekly security bulletins of US-CERT (http://www.us-cert.gov/ncas/bulletins)

market values of zero-days security vulnerabilities

After a hack

Once attackers have access, they will try to

- look for further applications, user accounts, and systems to attack
  - eg crack password file & try these passwords on other systems
- install a backdoor
  - with malicious software for remote control & remote access
- install additional malware for (ab)using the machine
  - for using the machine, eg for spam of DoS attacks
  - for eavesdropping on other credentials
- erase traces
  - to hide the hack and information about the hack

Why are systems hacked?

Why do hackers hack?

- Amateurs, interested in fun, vandalism, kudos
  - hobbyists, script kiddies, university researchers, ...

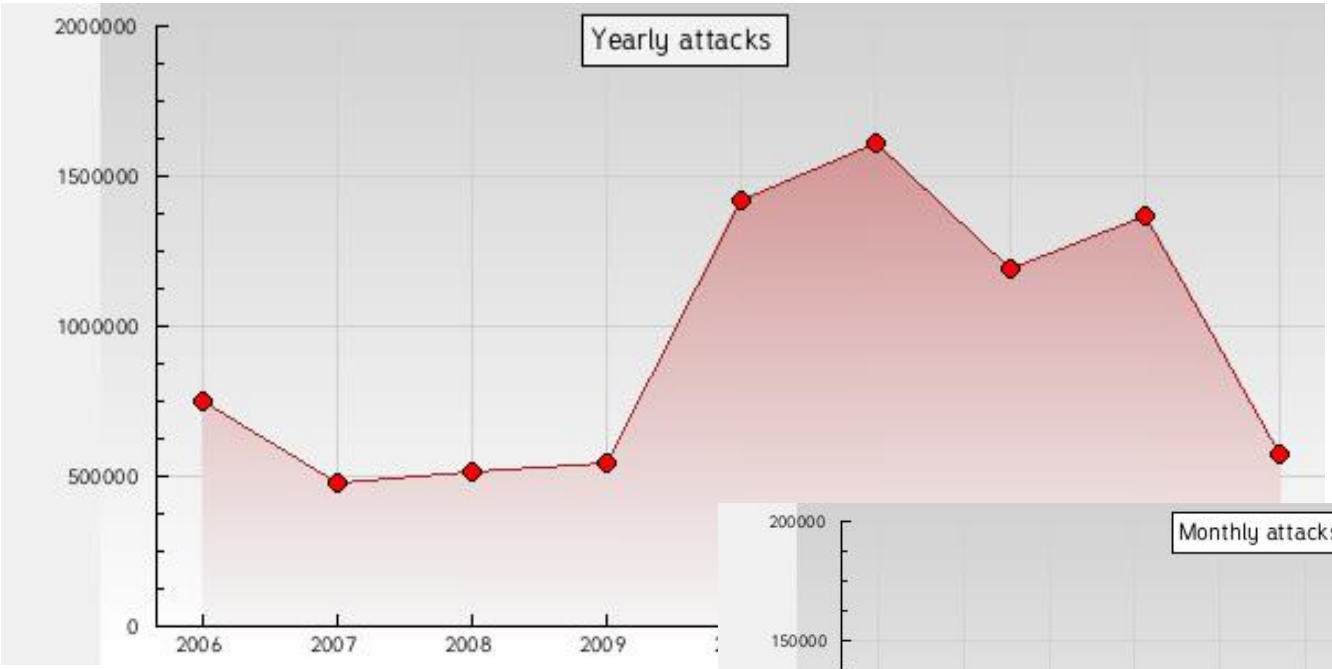
- Professionals
  - Criminals, interested in money
    - by stealing it from victims, or getting paid for services to other criminals
  - Nation states, interested in power, information, ...

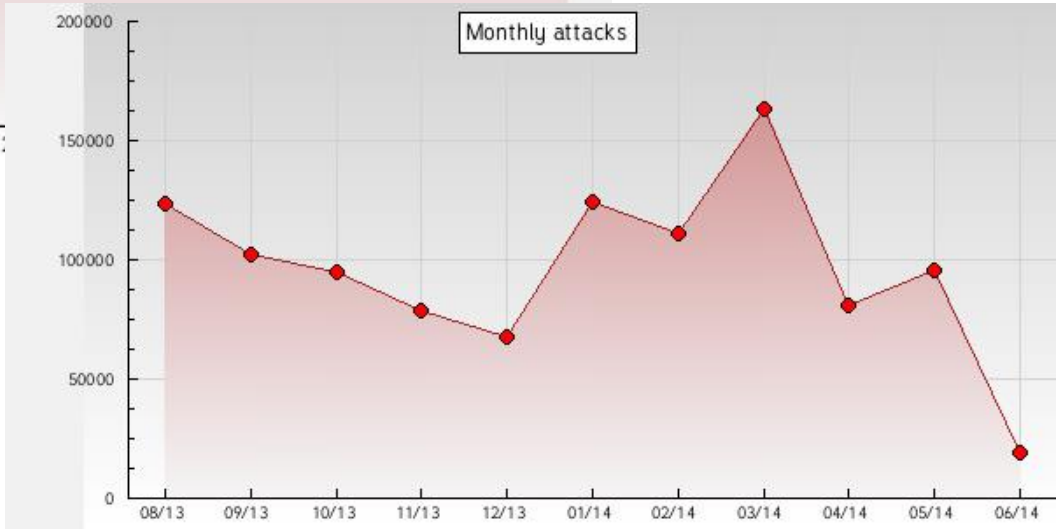
Who do they attack? Attacks can be targetted (eg spear-phishing) or undirected (eg spamming lots of people hoping someone will fall for it)

Online vandalism – web site defacement

www.zone-h.org monitors and archives web site defacements

typically > 100,000 sites per month





Monetisation

The big challenge for the criminal hacker:
how to make some money out of hacked machines?

- **direct financial gain, by stealing credit card info, using paypal accounts, online banking, ...**
- **use the machine as part of a botnet to sell services to other criminals & non-criminals**
  - **spamming**
  - **DDoS attacks (Distributed Denial of Service)**
  - **selling Facebook likes, YouTube views, ...**
- **ransomware**
  - **probably the most successful criminal business model to date**

Internet banking fraud in Netherlands

2008	2.1 M€
2009	1.9 M€
2010	9.8 M€ (7100€ per incident)
2011	35 M€ (4500€ per incident)
2012	34.8 M€
2013	9.6 M€
2014	4.7 M€
2015	3.7 M€

[Source: NVB & Betaalvereniging]

Note: this is serious organized crime, not teenage hackers.

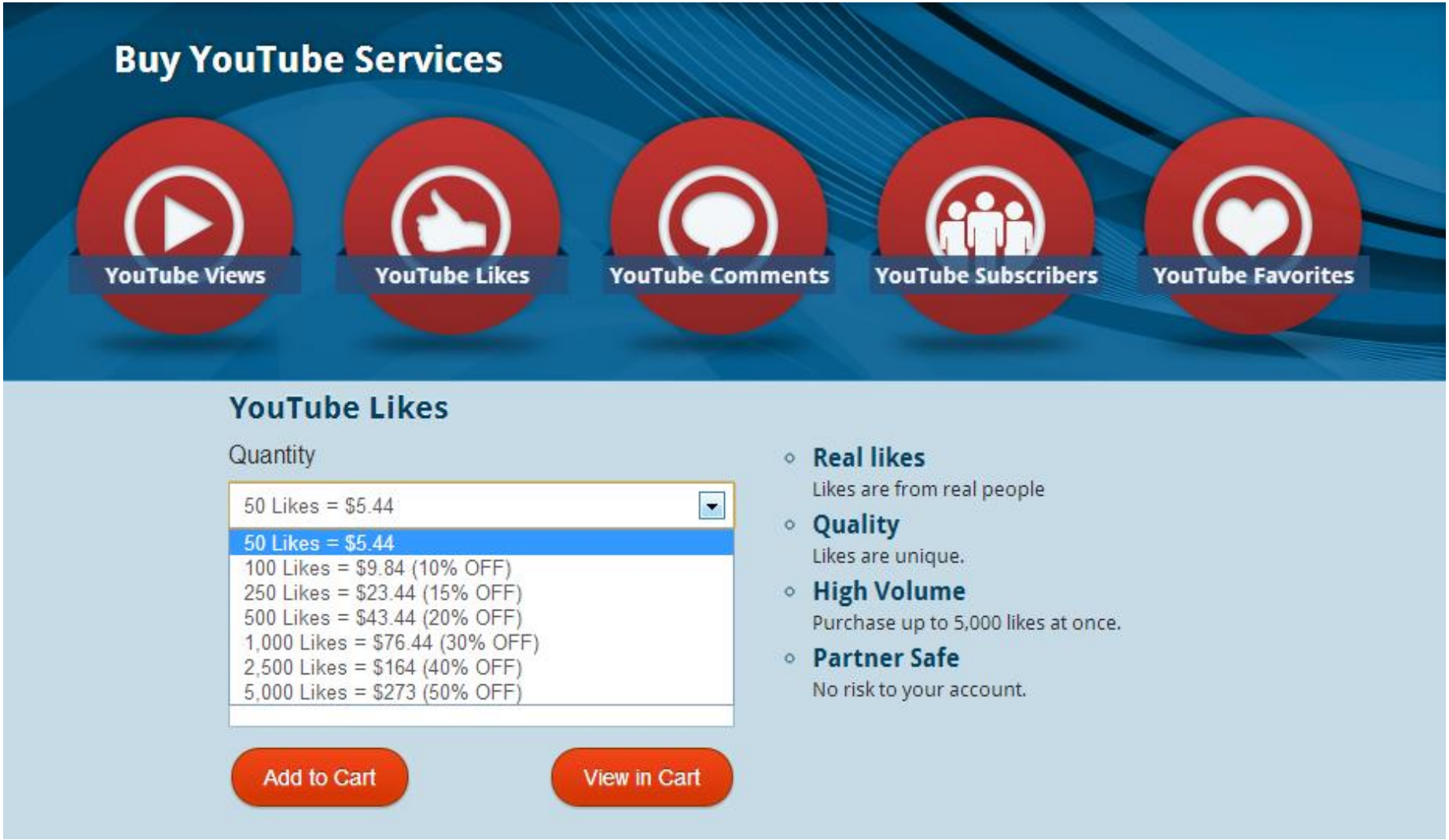
Fraud brought under control by

- better detection of suspicious transactions
- better detection of money mules

Carding sites

for trading dumps of stolen credit cards data & magstripe data

Criminal business models: selling YouTube likes



Criminal business models: selling internet traffic

which other (non?)criminals can use for phishing, advertisements, or spreading their own malware

Products (Total Items: 14)

Price: Low to High

More results: [1] 2 Next Page View All

WW Adult Traffic
Adult traffic from around the world.
Add to Cart

US Adult Traffic
US-Targeted Adult traffic.
Add to Cart

GEO Adult Traffic
GEO-Targeted Adult traffic.
Add to Cart

Mobile Traffic
Traffic from mobile devices.
Add to Cart

Expired Domain Traffic
To be added.
Add to Cart

US Alexa Traffic
Alexa traffic from the US target of your choice.
Add to Cart

WW Alexa Traffic
Alexa traffic from around the world.
Add to Cart

GEO Alexa Traffic
Alexa traffic from the GEO target of your choice.
Add to Cart

WW Popunder Traffic
Popunder traffic from around the world.
Add to Cart

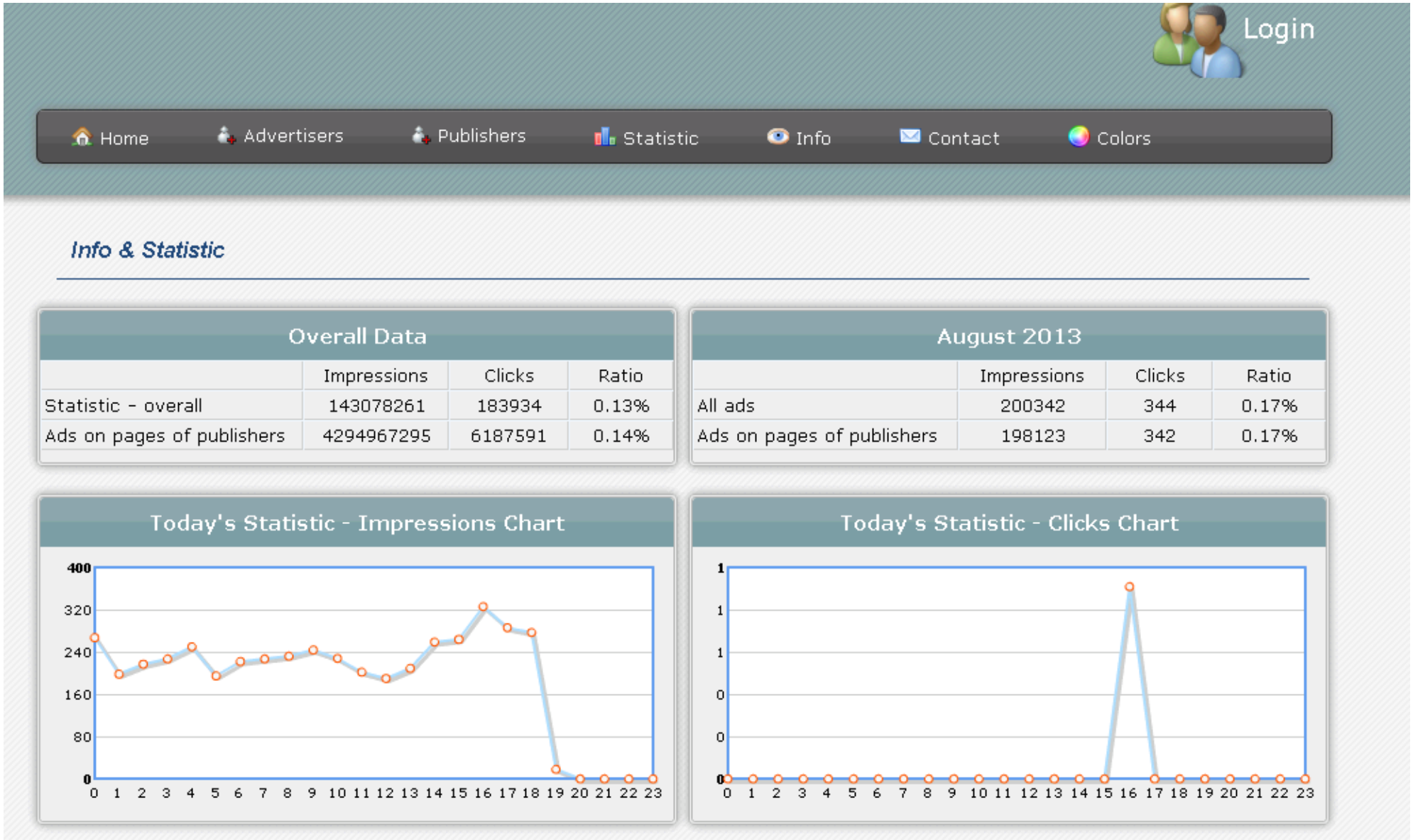
US Popunder Traffic
Popunder traffic from the US target of your choice.
Add to Cart

GEO Popunder Traffic
Popunder traffic from the GEO target of your choice.
Add to Cart

Worldwide Traffic
Traffic from around the world.
Add to Cart

More results: [1] 2 Next Page View All

Criminal business models: selling traffic for ads



scaring or forcing victim into paying

Ransomware: CryptoWall

Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

167h 56m 11s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Your file is successfully decoded. You can download it

Download decrypted file

Inside the CryptoWall code

```
gForbiddenCountryCodeCRCs dd 9121D628h

                          dd 87CECAE8h
                          dd 0D2558852h
                          dd 0D9EA3CDBh
                          dd 0A0D65196h
```

Exempted countries: Russia, Bellorussia, Kazachstan, Ukraine.

Later also Armenia and Iran

Goal: remain a low-priority problem for your local law enforcement.

Ransomware franchising

BS Registered Member

Registered Users

Join Date: Sep 2014

Location: blackstuff

Posts: 21

TorLocker Ransomware (Daily BTC inflow)

TorLocker Ransomware
What is this?
An affiliate program.
I provide a password for the control panel of TorLocker, a binary made in assembly for Windows, a builder, and a tor.exe standalone executable.
What is TorLocker?
TorLocker is a ransomware that works using TOR, BitCoin, RSA-2048, AES-256.
Is it similar to CryptoLocker?
Yes and No.
TorLocker encrypts files and demands user for a ransom. So CryptoLocker does.
TorLocker don't need internet connectivity to start encrypting files, CryptoLocker does.
TorLocker has 128 public keys inside the .exe body. Each affiliate receives new different encryption keys already inside the .exe.
After 10 different payments, i generate a new .exe for you, so no repeated keys are going to be used.
TorLocker command and control is hosted behind TOR hidden services. Can't be shutdown easily.
TorLocker accepts BitCoin only (Moneypak,Ukash Already Available for First Set Buyers)
TorLocker process payments and encryption key delivery, automatically. No human intervention is necessary.
How it works?
It will encrypt all files (extensions below) from the computer you send it, connect to TOR, retrieves the amount the user needs to pay (currently 0.380 BTC), the deposit address (a new address for every new client), how many days the user has to pay (currently 9 days counting down to 0 when decryption will not be possible).
After 6 confirmations from the BitCoin network, 70% of the ransom is sent to you. 30% goes to me, and the RSA-2048 decryption key is automatically delivered to the client, who get access to his files again. Each file is encrypted with a random AES-256 key, which is encrypted with the RSA-2048 key and then appended to the encrypted file.
How larger encrypted files become?
512 bytes
Is unicode supported?
Yes
What if I find a bug?
Report and I will correct it.
*Which extensions are currently being used?
".accdb",0,".ai",0,".arw",0,".bay",0,".blend", 0,". cdr",0,".cer",0,".cr2",0,".crt",0,".crw",0,".dbf" ,
0,".dcr",0,".der",0,".dng",0,".doc",0,".docm",0, ". docx",0,".dwg",0,".dxf",0,".dxg",0,".eps",0,".erf"
,0,".indd",0,".jpe",0,".jpg",0,".jpeg",0,".kdc",0 , ".mdb",0,".mdf",0,".mef",0,".mrw",0,".nef",0," .nrw
",0,".odb",0,".odm",0,".odp",0,".ods",0,".odt" ,0," .orf",0,".p12",0,".p7b",0,".p7c",0,".pdd",0,".pdf"
,0,".pef",0,".pem",0,".pfx",0,".ppt",0,".pptm",0, " .pptx",0,".psd",0,".pst",0,".ptx",0,".r3d",0,".raf
",0,".raw",0,".rtf",0,".rw2",0,".rwl",0,".srf" ,0," .srw",0,".wb2",0,".wpd",0,".wps",0,".xlk",0,".xls" ,0,".xlsb",0,".xlsm",0,".xlsx",0,0**
What I need to do to start cashing?
An offline BitCoin wallet. bitcoin-qt is fine. Synchronize the bitcoin wallet with the network (it will take some time).
Download tor browser bundle. Configure TOR as the SOCKS proxy in the bitcoin client (this is a very important step to your safety).
Generate a new address. Get your password for the TorLocker panel from me (buying this listing). Register you BitCoin address in the panel (you will be asked only once, in the first time you login). Spread the .exe, receive the money.
In how many time will you setup my account?
Maximum 4 days.

70% of the ransom is sent to you. 30% goes to me,

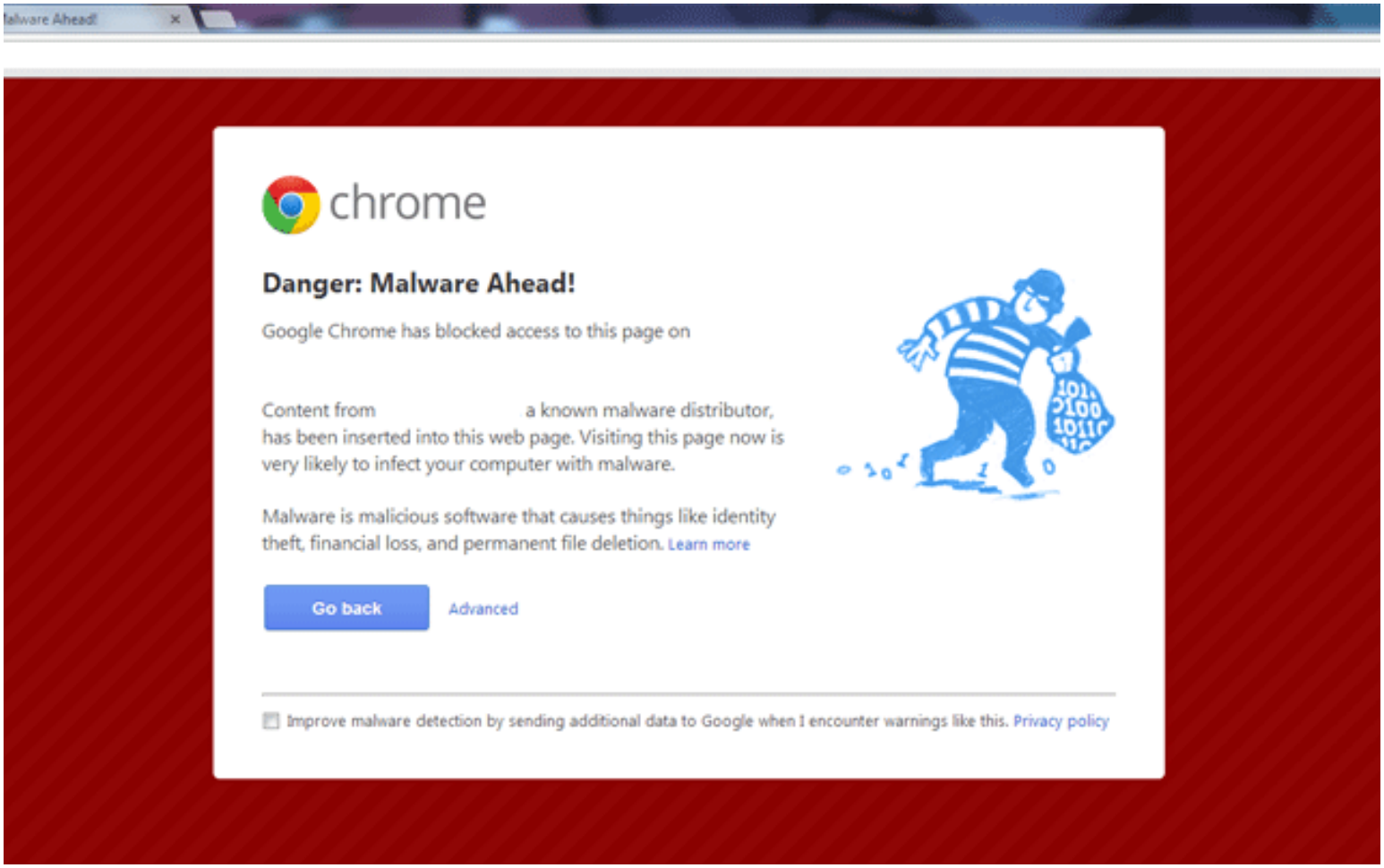
Prevention & Detection

Preventing attacks

- Be on your guard for social engineering
- Updating software to patch *known & fixed* security flaws
- Virus scanners, which look for
  1. signatures of *known* attacks in email attachments, downloads, ..
  2. malicious files on your file system, incl. suspicious executables
  3. look for malicious or suspicious processes on a machine
- Firewalls and Intrusion Detection Systems (IDS)
  which look for / block suspicious patterns in network behaviour
- Browsers & search engines warnings
  which warn about *known* malicous web sites

NB most of this only protects against *known* attacks ☹

Example browser warning



Example search engine warning

But… warnings can be faked

For social engineering attacks using scareware

No need for the attacker to hack anything!

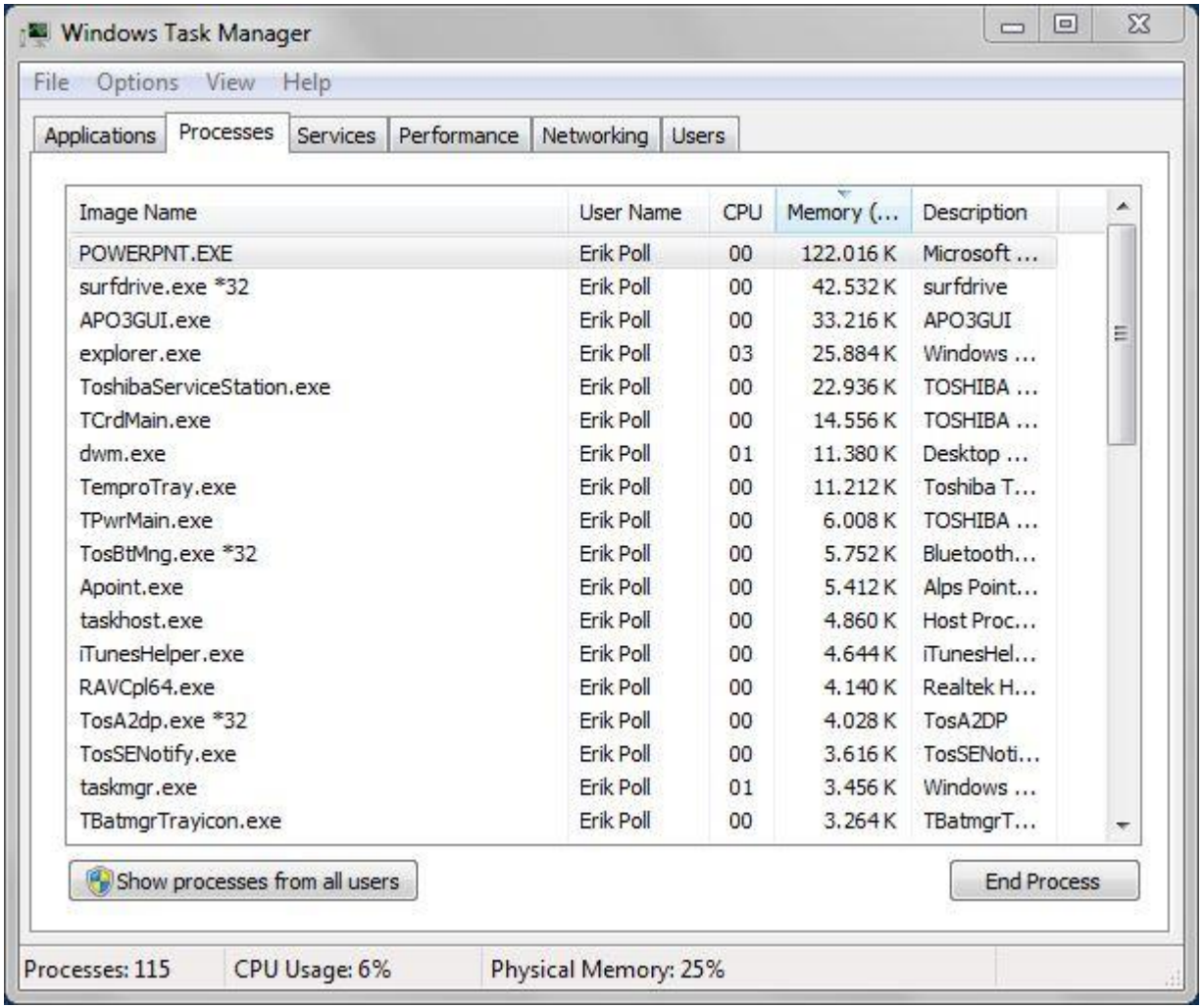
- as victim willingly installs malware (as part of the “free scan”)

Detection
& digital forensics

Detecting attacks

- 'live', as the computer is running
  - suspicious processes
    - eg on Windows computer, look in the `Processes` and `Services` in the `Task Manager`
  - suspicious network traffic
    - incl. suspicious destinations, traffic volumes, times

Detecting attacks: `Windows Task Manager`



Detecting attacks

- 'live', as the computer is running
  - suspicious processes
    - eg on Windows computer, look in the `Processes` and `Services` in the `Task Manager`
  - suspicious network traffic
    - incl. suspicious destinations, traffic volumes, times

- after the fact: digital forensics

Digital forensics

Actions & connections leave traces, eg.

- if an application is started or a file is opened, this leaves traces: on the file system, in the operating system, and in that application
- if two computers communicate over the network, information from each will appear in processes & log files of the other
- if removable media (eg. USB stick) is connected to a computer, information about it will remain on that computer

Such information can be volatile or persistent,

- volatile storage, ie. RAM, disappears when computer is switched off
- persistent storage, on hard disk or USB sticks, remains when computer is switched

Example digital traces: USB

For example, log files on a Windows machine reveal list of all USB storage devices that has ever been plugged into a computer

- incl. vendor, product number, version number, serial number, first time used, last time used

Digital forensics – where to find digital traces

- on a computer or phone, esp. in log files

  Also embedded computers, eg. in cars, houses,..
- on the network
  - in log files logs of servers, for internet or mobile phone
- in de cloud
  - data & log files at online services
    gmail, facebook, google-docs, flickr, picasa, twitter,..

    NB also Office 365
  - online backup & synchronisation:
    Google Drive, iCloud, Firefox Sync, ...

Digital evidence on a computer

At different levels

- hardware level
  esp. hard disk and other persistent data storage (USB sticks)
- operating system level
  incl. log files, the file system and file system explorer
- applications
  eg. web browser, Office, mp3 players, video players, ...

Forensically interesting locations on a Windows PC

Windows OS

- Temp folder
- Recycle Bin
- Event logs & Register entries
- thumbnail images in Thumbs.
- Installed USB devices
- Printer spool folder

Windows Explorer

- Recently opened files & folders
- Recent searches
- Network Shortcuts
- Recently run from the "Run" bar
- User Assist

Web browser

- Cache & downloads
- Cookies
- History
- Typed URLs
- Forms AutoComplete
- Passwords (not) remembered

Other applications

- Recently Opened Office Docs
- Files recently accessed by Windows Media Player
- Offline Outlook Mailbox
- Temp folder for Outlook attachments

Log files kept by the OS

The operating system keeps time-stamped logs of all sorts of events

- **on Windows, so-called artifacts in Event Logs & the Windows Registery**

incl.

successful/failed logon, type of logon (interactive, network, batch, service, remote desktop)

screen saver invoked/dismissed, remote desktop session dis/connected,

user account created/deleted, password change, security permission change

request to authenticate to a wireless/wired network,

networks connected to,

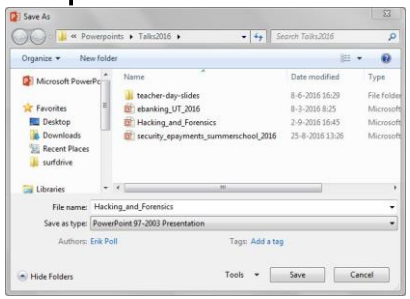
external devices connected,

installation/updating of software,

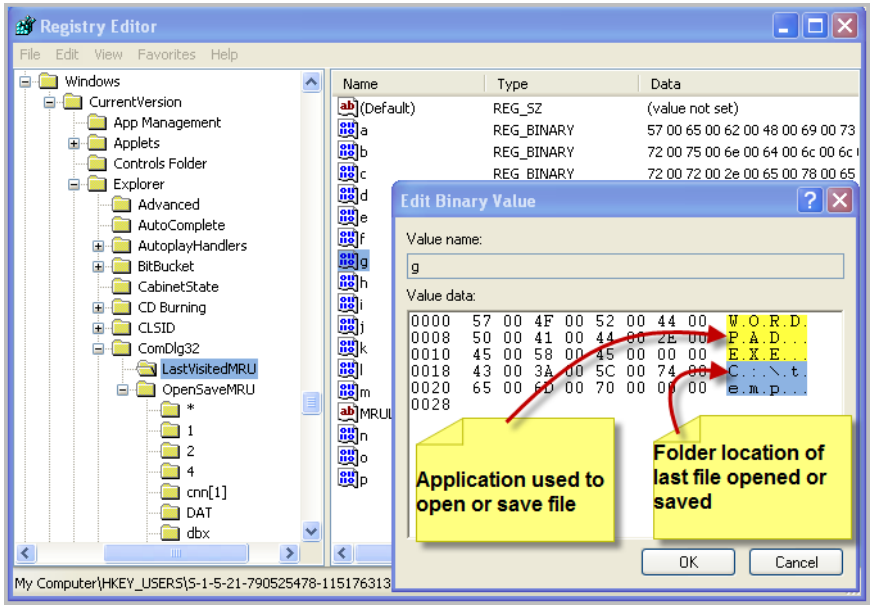
....

Example info in Windows Registry

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU **records file names selected in Save As or Open dialog box by *any* application**

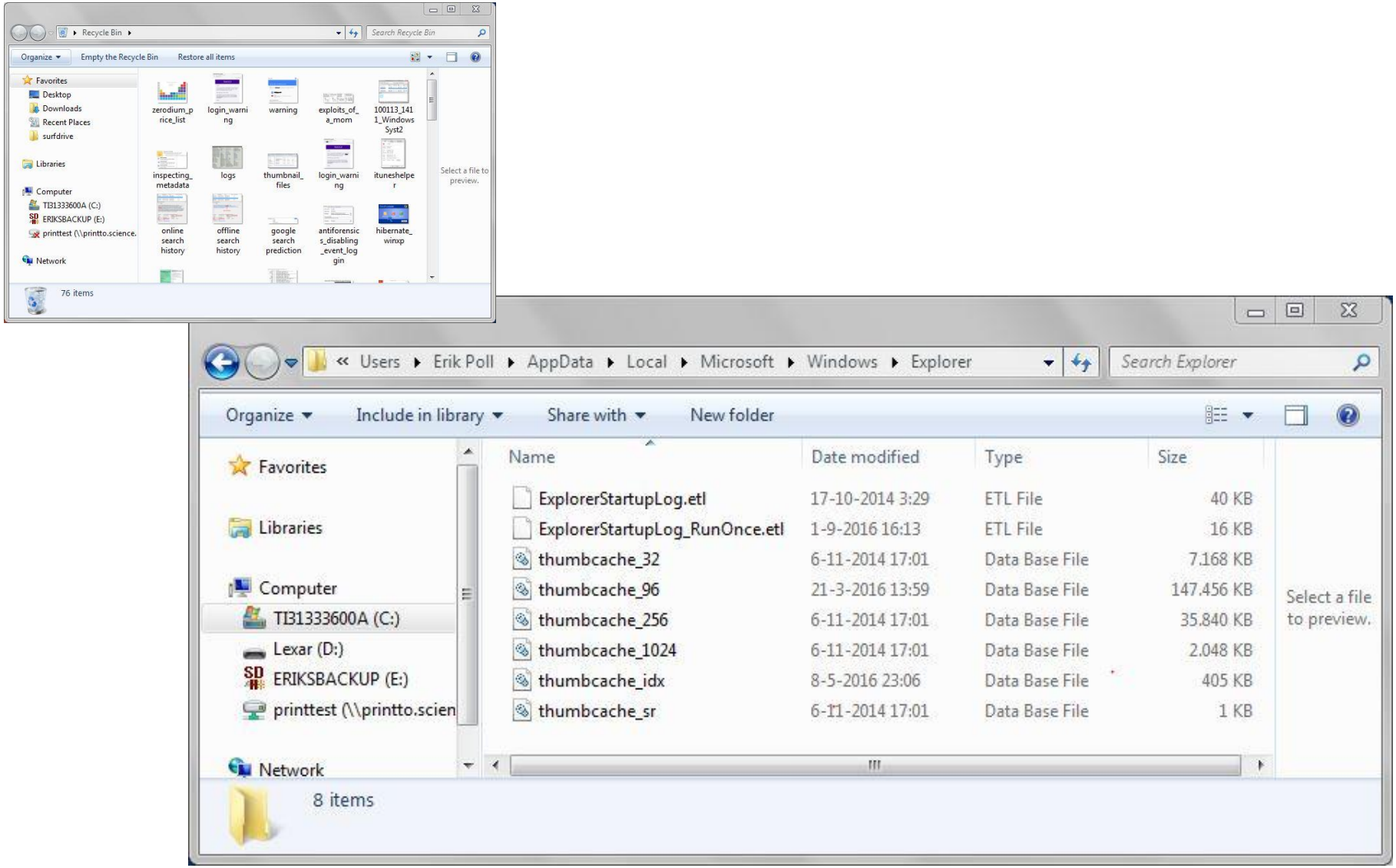


- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU **records application used to open file & folder last used by that application**

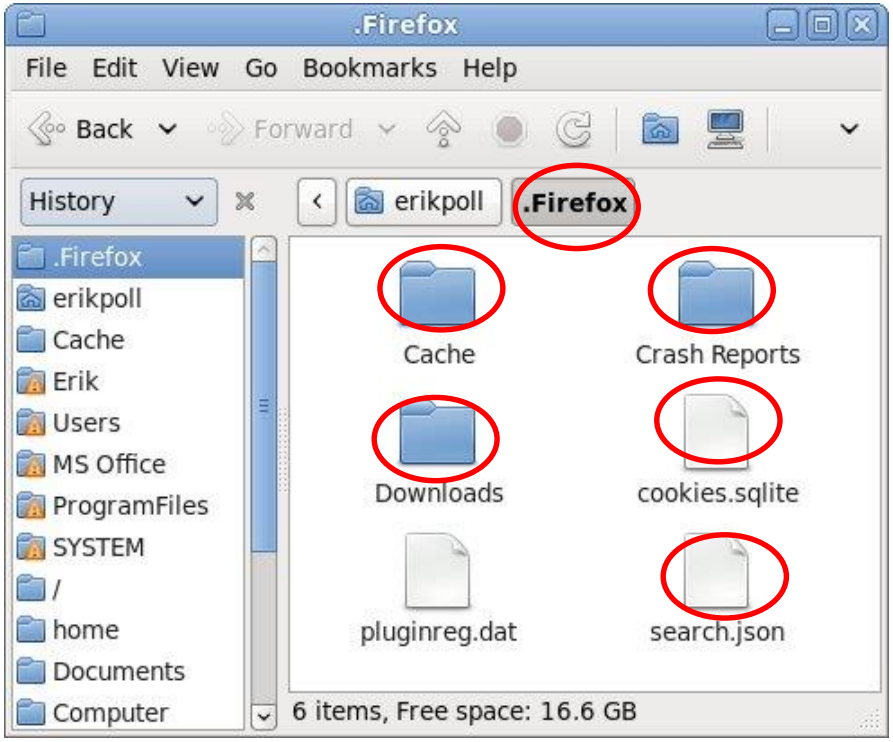


(Cached) thumbnail images of file system explorer

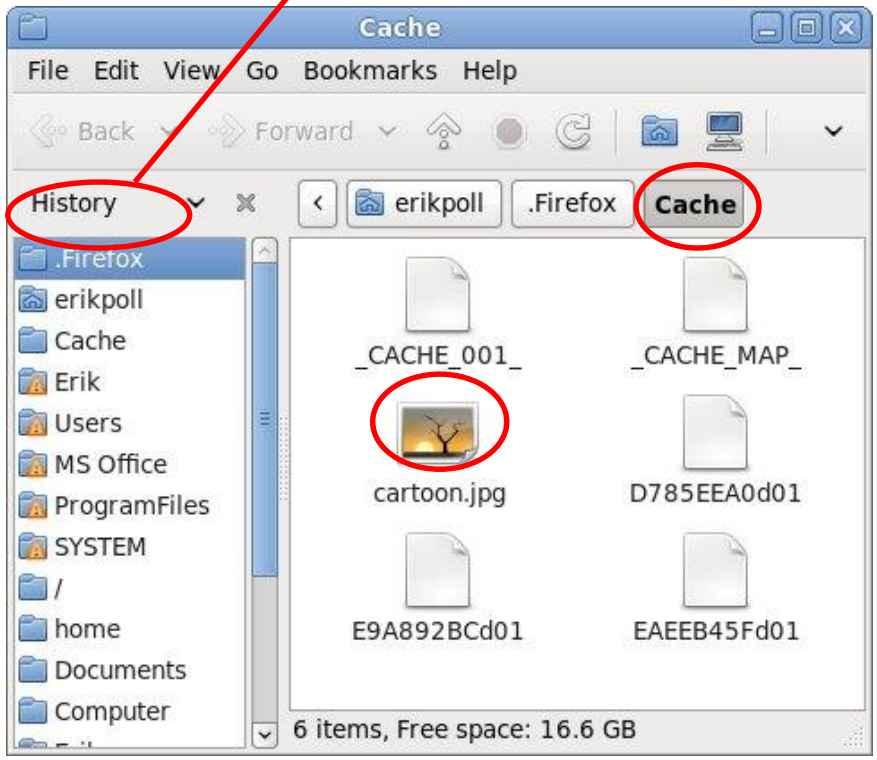
Thumbnails images used by Windows Explorer are cached by default

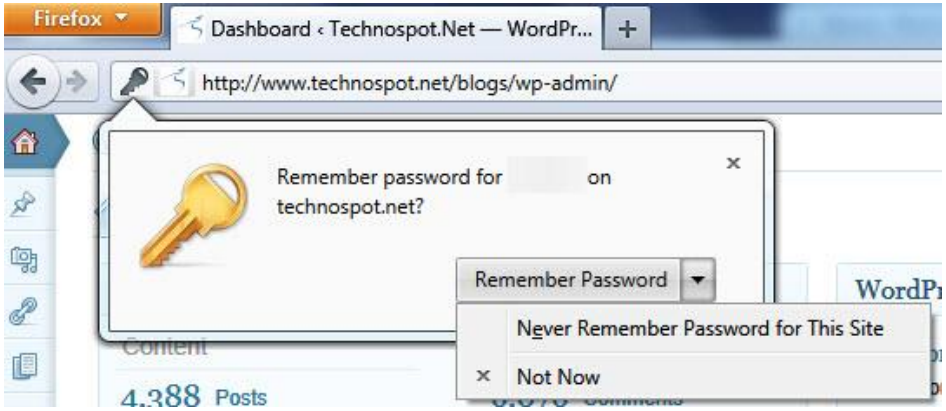


‘Old’ data kept by web browser

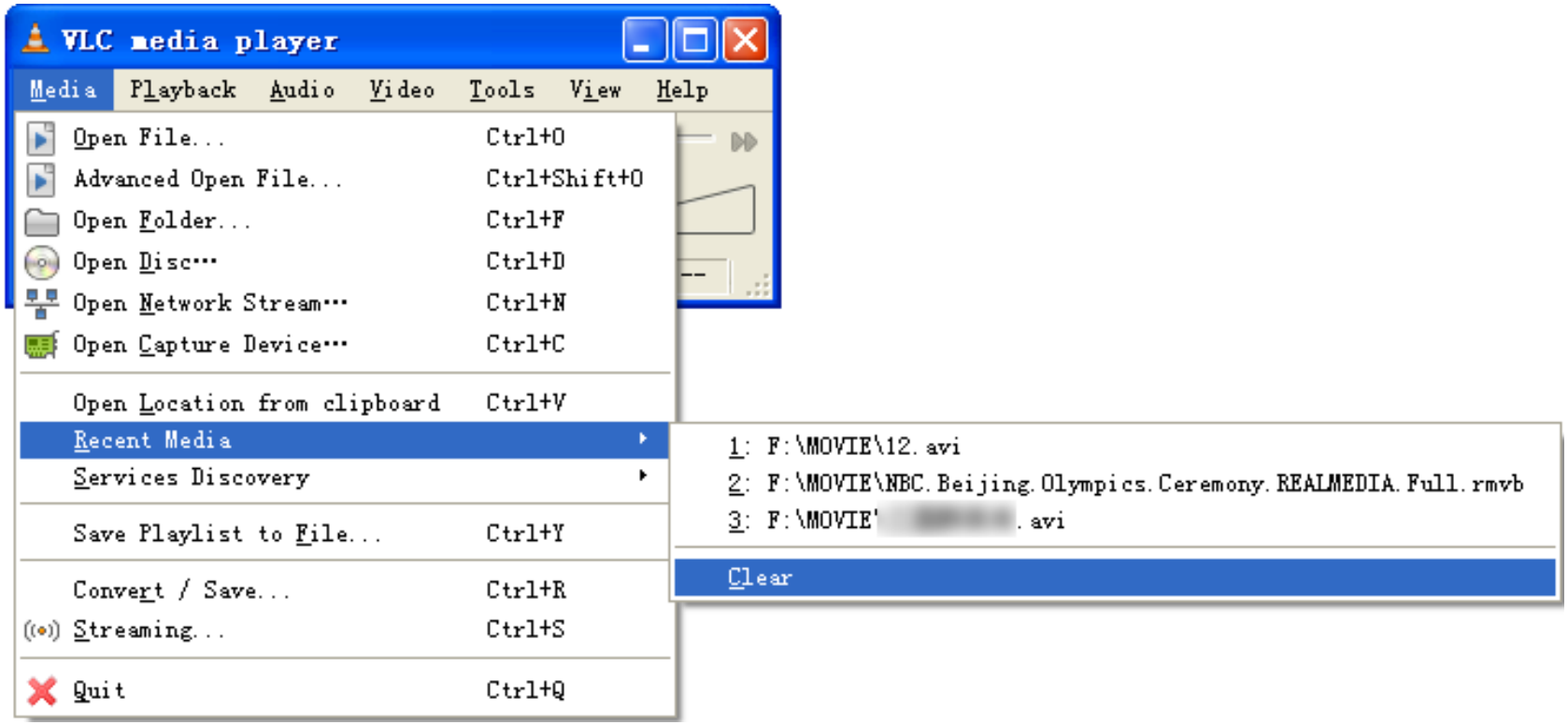


not of the *web* browser
but of the *file* browser

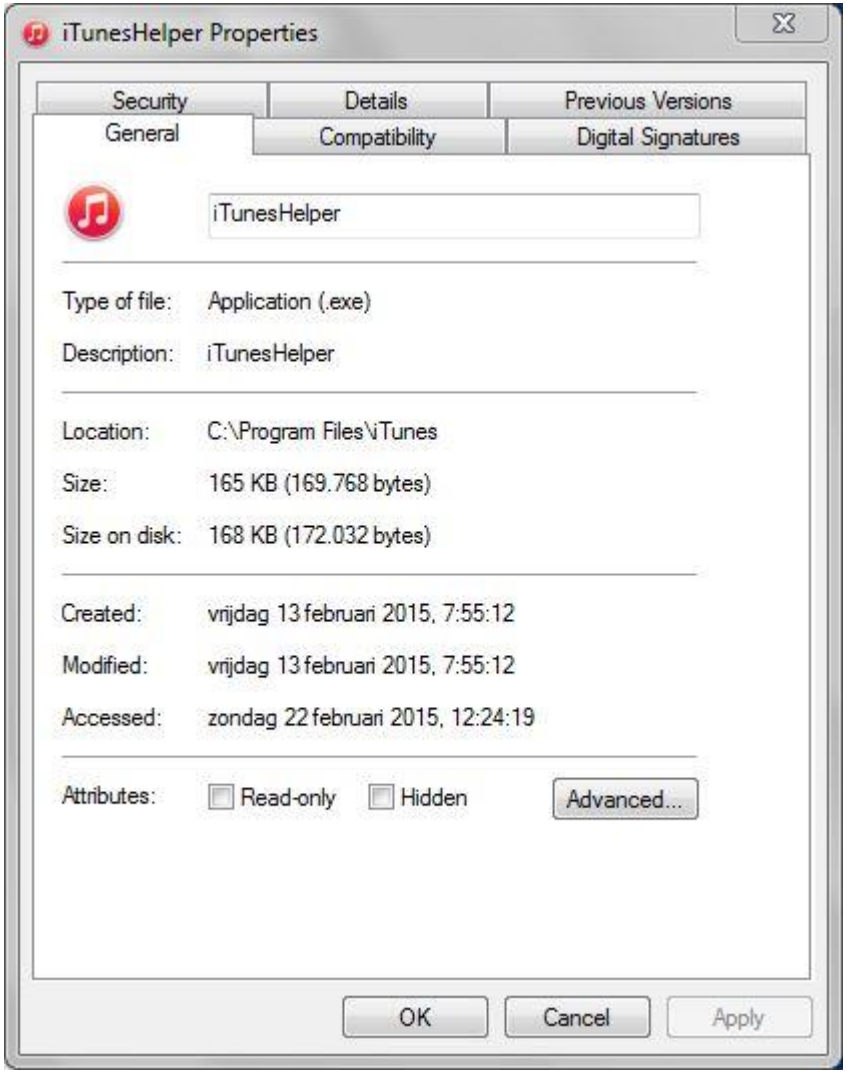




Historical data kept by applications



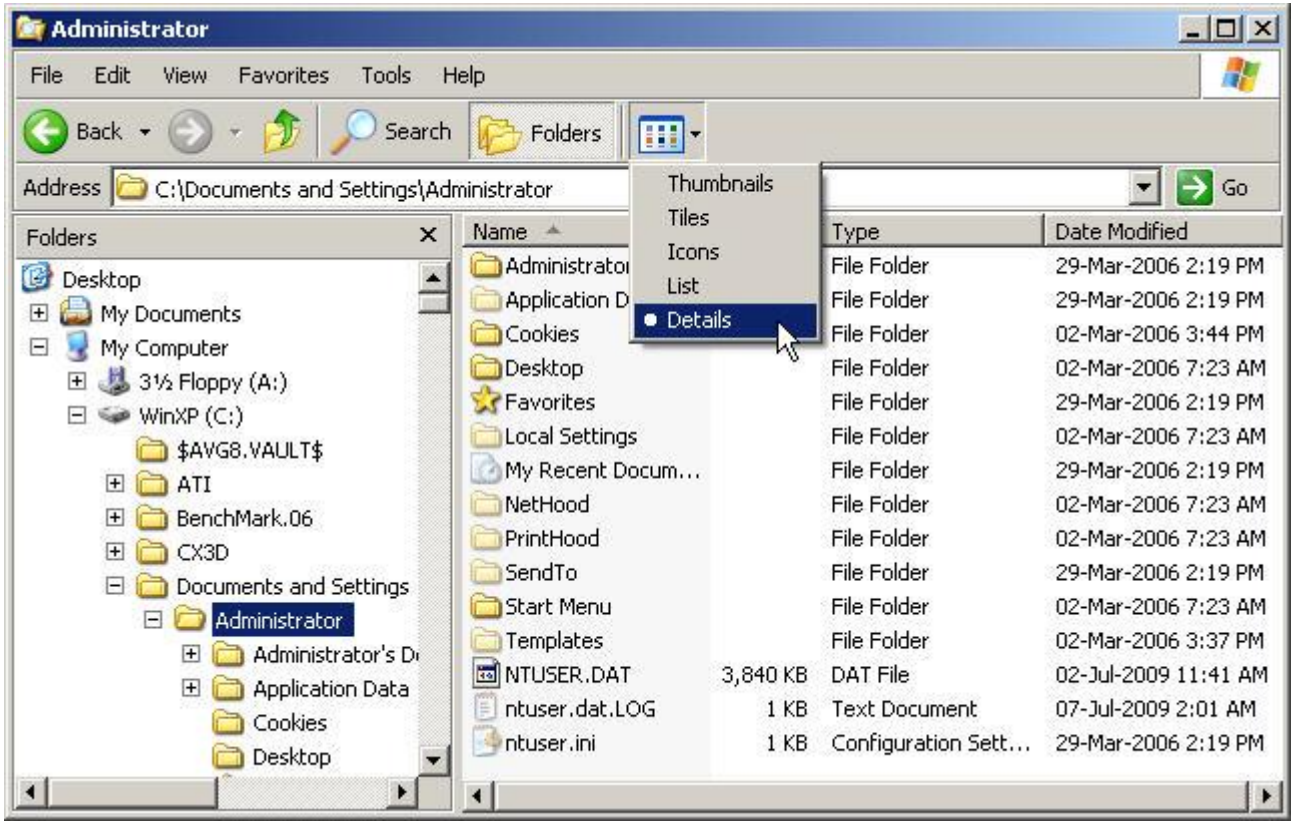
Information about installed software



Meta-data in the file system

Time a file is created, last accessed, last modified, MTF record last modified

Some, but not all, of this info is visible in eg. Windows Explorer. Forensic tools will show it.



Meta-data *inside* files

A file will contain meta-data, about

- file name

  Possibly including location on file system

- file type

  Eg *Windows 2007 Office .doc*

- authors

  Eg *username*

- history

  Eg *revision history, track-changes*

How meta-data can ruin your day...

The UK intelligence report on Iraq's weapons of mass destruction, distributed as .doc file, contained

```
Rev. #1: "cic22" edited file
"C:\DOCUME~1\phamill\Temp\AutoRecovery save of Iraq -
security.asd" ...

Rev. #6: "ablackshaw" edited file
"C:\ABlackshaw\Iraq -  security.doc" ...

Rev. #10: "MKhan" edited file
"C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc" ...
```

revealing some of the people who edited this file, incl.

- Paul Hamill - Foreign Office official
- Alison Blackshaw - personal assistant of Tony Blair's press secretary
- Murtaza Khan - Junior press officer for Tony Blair

Old data on disk: ‘delete’ is not delete

Desktop	
Forensics.ppt	address
tentamen.pdf	

```
MS Powerpoint 2007 ...
MS Comic Sans ...
Title: Digital Forensics
Footer: Erik ...
110101001010101010101010010
101010101010101010101010010
102101010101010101010111010
101000101111010100110101010
001011101010101110100011 1
```

Old data on disk: ‘delete’ is not delete

Desktop	
XXrensics.ppt	XXXX
tentamen.pdf	

After deleting `Forensics.ppt` and emptying the `Recycle Bin`

```
XX Powerpoint 2007 ...
MS Comic Sans ...
Title: Digital Forensics
Footer: Erik ...
110101001010101010101010010
101010101010101010101010010
102101010101010101010111010
101000101111010100110101010
001011101010101110100011 1
```

‘delete’ only removes reference to the file & changes first bytes.

To really delete the info, this part of the hard disk has to be overwritten with new information. On a big hard disk, this may take time.

- Also, ‘save’ may well leave a ‘deleted’ copy of the old file.

Hibernation

When computer hibernates,

a snapshot of the volatile memory (RAM)

is written to persistent disk

Forensic analysis of disk later can reveals the exact state of all applications that were running at that time.

- Crashes of software can also leave persistent traces, eg in crash reports

Digital forensic tools

There is a *vast* amount of log entries and meta-data, of operating system, file system, and all applications.

Digital forensic tools collect and present this data to facilitate analysis

- **for instance to construct a timeline**

Example: processing using `log2timelime`

```
root@SIFT-Workstation:/cases/timeline-output-folder# log2timeline -f list
-----------------------------------------------------------------------------
                Name    Ver.    Description
-----------------------------------------------------------------------------
             altiris     0.1    Parse the content of an XeXAMInventory or AeXProcessList log file
        analog_cache     0.1    Parse the content of an Analog cache file
      apache2_access     0.3    Parse the content of a Apache2 access log file
       apache2_error     0.2    Parse the content of a Apache2 error log file
              chrome     0.3    Parse the content of a Chrome history file
   encase_dirlisting     0.2    Parse the content of a CSV file that is exported from FTK Imager (dirlisting)
                 evt     0.2    Parse the content of a Windows 2k/XP/2k3 Event Log
                evtx     0.5    Parse the content of a Windows Event Log File (EVTX)
                exif     0.4    Extract metadata information from files using ExifTool
         ff_bookmark     0.3    Parse the content of a Firefox bookmark file
            ff_cache     0.2    Parse the content of a Firefox _CACHE_00[123]_ file
            firefox2     0.3    Parse the content of a Firefox 2 browser history
            firefox3     0.8    Parse the content of a Firefox 3 history file
      ftk_dirlisting     0.3    Parse the content of a CSV file that is exported from FTK Imager (dirlisting)
       generic_linux     0.3    Parse content of Generic Linux logs that start with MMM DD HH:MM:SS
           iehistory     0.8    Parse the content of an index.dat file containg IE history
                 iis     0.5    Parse the content of a IIS W3C log file
              isatxt     0.4    Parse the content of a ISA text export log file
      jp_ntfs_change     0.1    Parse the content of a CSV output file from JP (NTFS Change log)
             l2t_csv     0.1    Parse the content of a body file in the l2t CSV format
            mactime     0.6    Parse the content of a body file in the mactime format
             mcafee     0.3    Parse the content of log files from McAfee AV engine
        mcafeefireup     0.1    Parse the content of an XeXAMInventory or AeXProcessList log file
           mcafeehel     0.1    Parse the content of a McAfee HIPS event.log file
            mcafeehs     0.1    Parse the content of a McAfee HIPShield log file
                 mft     0.1    Parse the content of a NTFS MFT file
        mssql_errlog     0.2    Parse the content of an ERRORLOG file produced by MS SQL server
              ntuser     1.0    Parses the NTUSER.DAT registry file
             openvpn     0.1    Parse the content of an openVPN log file
               opera     0.2    Parse the content of an Opera's global history file
                oxml     0.4    Parse the content of an OpenXML document (Office 2007 documents)
                pcap     0.5    Parse the content of a PCAP file
                 pdf     0.3    Parse some of the available PDF document metadata
            prefetch     0.7    Parse the content of the Prefetch directory
     proftpd_xferlog     0.1    Parse the content of a ProFTPd xferlog log file
            recycler     0.6    Parse the content of the recycle bin directory
             restore     0.9    Parse the content of the restore point directory
              safari     0.3    Parse the contents of a Safari History.plist file
                 sam     0.1    Parses the SAM registry file
            security     0.1    Parses the SECURITY registry file
            setupapi     0.5    Parse the content of the SetupAPI log file in Windows XP
           skype_sql     0.1    Parse the content of a Skype database
            software     0.1    Parses the SOFTWARE registry file
                 sol     0.5    Parse the content of a .sol (LSO) or a Flash cookie file
               squid     0.5    Parse the content of a Squid access log (http_emulate off)
            symantec     0.1    Parse the content of a Symantec log file
              syslog     0.2    Parse the content of a Linux Syslog log file
              system     0.1    Parses the SYSTEM registry file
                 tln     0.5    Parse the content of a body file in the TLN format
           volatility     0.2    Parse the content of a Volatility output files (psscan2, sockscan2, ...)
            win_link     0.7    Parse the content of a Windows shortcut file (or a link file)
             wmiprov     0.2    Parse the content of the wmiprov log file
           xpfirewall     0.4    Parse the content of a XP Firewall log
```

Example timeline constructed from log

Spear Phish Email Received w/Java Applet attack w/PDF and link (Email was about IRS w-2 tax forms) The victim clicked on the link http://bit.ly/GEUMQQ

4/2/2012 20:32:52	MACB	Firefox 3 history	http://bit.ly/GEUMQQ () [count: 2] Host: bit.ly (URL not typed directly) type: LINK
4/2/2012 20:32:52	MACB	Firefox 3 history	http://207.58.245.179/ (Internal Revenue Service) [count: 2] visited from: http://bit.ly/GEUMQQ (URL not typed directly) type: REDIRECT_PERMANENT
4/2/2012 20:32:57	M.CB	NTFS $MFT	C:/WINDOWS/Sun/Java/Deployment
4/2/2012 20:32:57	M.CB	NTFS $MFT	C:/WINDOWS/Sun
4/2/2012 20:32:57	M.CB	NTFS $MFT	C:/WINDOWS/Sun/Java
4/2/2012 20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft
4/2/2012 20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment
4/2/2012 20:32:58	MACB	NTUSER key	Key name: HKEY_USER/Software/JavaSoft/JavaRuntimeEnvironment/1.6.0_31
4/2/2012 20:32:58	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/deployment.properties
4/2/2012 20:33:06	...B	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/68b75a3e-77699f39.idx
4/2/2012 20:33:07	...B	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/lastAccessed
4/2/2012 20:33:15	M.CB	NTFS $MFT	C:/Documents and Settings/tdungan/Local Settings/Temp/pkxezy1tji98.exe
4/2/2012 20:33:15	...B	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/4/6f13884-712bc739.idx
4/2/2012 20:33:16	M.C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012 20:33:16	..C.	NTFS $MFT	C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/
4/2/2012 20:33:17	MACB	XP Prefetch	PKXEZY1TJI98.EXE-0BCBF29B.pf - [PKXEZY1TJI98.EXE] was executed - run cou
4/2/2012 20:33:17	MACB	Firefox 3 history	http://www.irs.gov/ (Internal Revenue Service) [count: 1] Host: www.irs.gov visited from: http://207.58.245.179/ (URL not typed directly) type: LINK
4/2/2012 20:33:27	M.CB	NTFS $MFT	C:/WINDOWS/Prefetch/PKXEZY1TJI98.EXE-0BCBF29B.pf
4/2/2012 20:34:26	...B	NTFS $MFT	C:/WINDOWS/system32/dllhost
4/2/2012 20:35:10	M.CB	NTFS $MFT	C:/WINDOWS/system32/dllhost/svchost.exe
4/2/2012 20:35:10	M.CB	NTFS $MFT	C:/WINDOWS/system32/dllhost/winclient.reg
4/2/2012 20:35:49	M.C.	NTFS $MFT	C:/WINDOWS/system32/dllhost
4/2/2012 20:36:03	...B	NTFS $MFT	C:/WINDOWS/Prefetch/REG.EXE-0D2A95F7.pf
4/2/2012 20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet002/Services/Netman/domain
4/2/2012 20:37:14	MACB	SYSTEM key	Key name: HKLM/System/ControlSet001/Services/Netman/domain
4/2/2012 20:39:24	MACB	SOFTWARE key	Key name: HKLM/Software/Microsoft/Windows/CurrentVersion/Run

Java Applet attack hits – Download of malware into /temp folder

Malware run from /temp folder

Files Dropped – svchost.exe is beacon malware

Beacon Interval Set and Persistence Achieved via "RUN" Key

Trend: more (meta) data in the cloud

Office 365 | Outlook | Calendar | People | Newsfeed

EDIT LINKS

Documents › Most Popular Items

Result type

Excel

PDF

PowerPoint

Word

Content Type

application/vnd.openxmlf...

Document

application/vnd.openxmlf...

application/pdf Document

application/vnd.openxmlf...

SHOW MORE

Author

Corey Roth

Vesa Juvonen

Template

Most Views

	Recent ↓	Ever
Introduction to SP15 dotnetmafiapreview.sharepoint.com/.../Ig15_SP_IT_M01V1_introduction... Popularity Trends	0	3
SP15 System Requirements dotnetmafiapreview.sharepoint.com/.../Ig15_SP_IT_M02V1_requirements... Popularity Trends	0	7
Request Management SharePoint o15 Ignite training material dotnetmafiapreview.sharepoint.com/.../Ig15_SP_IT_M03V1_requestmgmt.... Popularity Trends	0	4
Analytics in SharePoint 15 SharePoint o15 Ignite training material dotnetmafiapreview.sharepoint.com/.../Ig15_SP_IT_M03V2_analytics.pp... Popularity Trends	0	10
Distributed Cache Service SharePoint o15 Ignite training material dotnetmafiapreview.sharepoint.com/.../Ig15_SP_IT_M04V1_cacheservice... Popularity Trends	0	3

Meta-data of Windows Office 365

Usage [Protected View] - Excel

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW POWERPIVOT

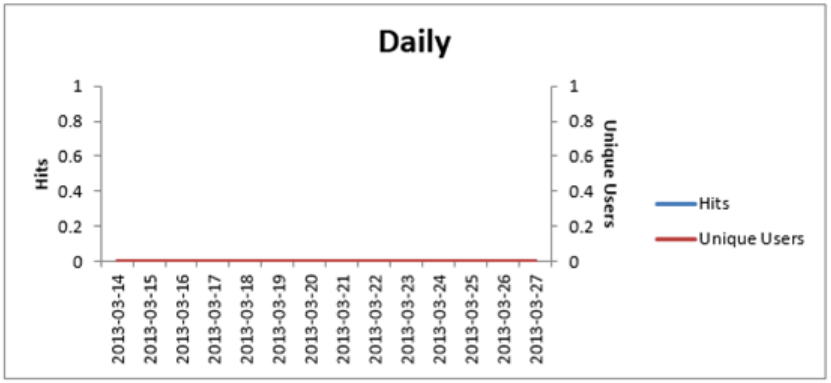
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

A1 Usage Details: Views

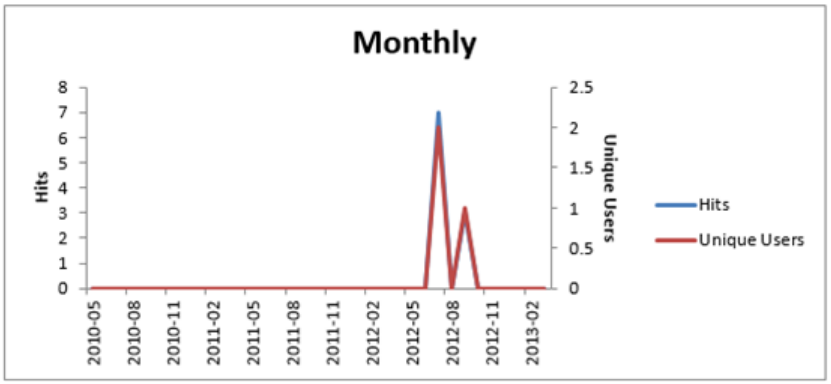
Usage Details: Views

Item: lg15_SP_IT_M03V2_analytics

Day	Hits	Unique Users
2013-03-14	0	0
2013-03-15	0	0
2013-03-16	0	0
2013-03-17	0	0
2013-03-18	0	0
2013-03-19	0	0
2013-03-20	0	0
2013-03-21	0	0
2013-03-22	0	0
2013-03-23	0	0
2013-03-24	0	0
2013-03-25	0	0
2013-03-26	0	0
2013-03-27	0	0



Month	Hits	Unique Users
2010-05	0	0
2010-06	0	0
2010-07	0	0
2010-08	0	0
2010-09	0	0
2010-10	0	0
2010-11	0	0
2010-12	0	0
2011-01	0	0
2011-02	0	0
2011-03	0	0
2011-04	0	0
2011-05	0	0
2011-06	0	0



Trend: from prevention to detection & reaction

Instead of trying to *prevent* problems, trying to *detect* and *respond* to problems often more (cost) effective way to improve security.

- Example: breaking into a Dutch house, which huge glass windows on the ground floor, is trivial. Only the risk of *detection* and the *reaction* then (ie. getting caught) is deterring criminals.
- Example: banks have combatted skimming fraud & online banking fraud with better detection.

Note: this is often related to making the criminal business model less attractive.

This means that cloud service providers are collecting more info to detect abuse.

meta-data in the cloud

Unexpected sign-in attempt Friday, July 22, 2016 11:59 AM

From: "Yahoo" <noreply@yahoo-inc.com>

To: [redacted]@yahoo.com

Full Headers Printable View

YAHOO!

Hi Erik,

On Fri, Jul 22, 2016 3:29 PM GMT+5:30, we noticed a successful sign in to your Yahoo account [redacted] from an unrecognized device in India.

If this was you, you're all set!

If this wasn't you and you believe someone may have tried to access your account, please change your password and update your account recovery information.

Yahoo

so Yahoo mail tracks user locations and devices

meta-data in the cloud

Google

Nieuwe login via Firefox op Linux

Hallo,
Uw Google-account [redacted] is zojuist gebruikt om in te loggen vanuit Firefox op Linux.

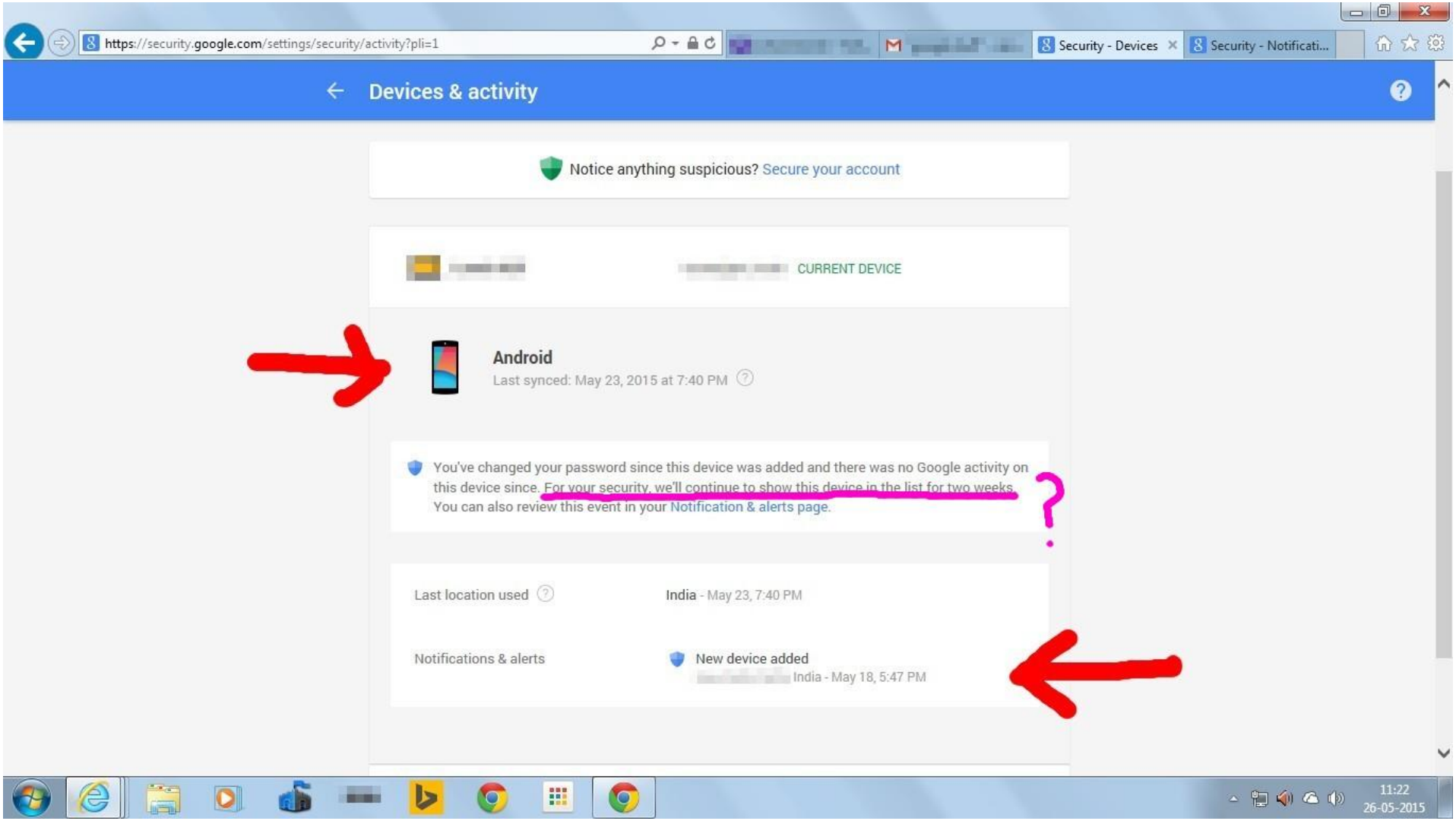
[redacted]

Linux
vrijdag 2 september 2016 13:58 (Midden-Europese zomertijd)
Nijmegen, Nederland*
Firefox

Herkent u deze activiteit niet?
Controleer nu uw onlangs gebruikte apparaten.

so Google checks which browser and operating system I use

meta-data in the cloud



so Google Drive tracks user devices & synchronisation

Anti-forensics

Anti-forensics

All these digital traces can be erased or altered!

to hide evidence that a hack occurred,
and to prevent analysis of what happened

There is anti-forensics software to do this. But:

- **big changes or deletion of log files will be easy to detect;**

  subtle changes will not not be, but are more work.

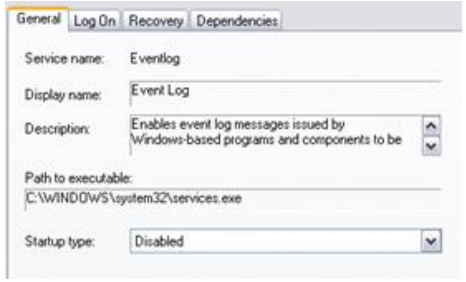
- **anomalies (eg in time stamps on files) may stand out.**

Practical problems for the attacker

- **the attacker usually wants to keep a backdoor open**
  - **which requires some persistent malware on the sytem**
- **the attacker cannot clear evidence in external logs in the cloud**

Anti-forensics (on criminal's computer)

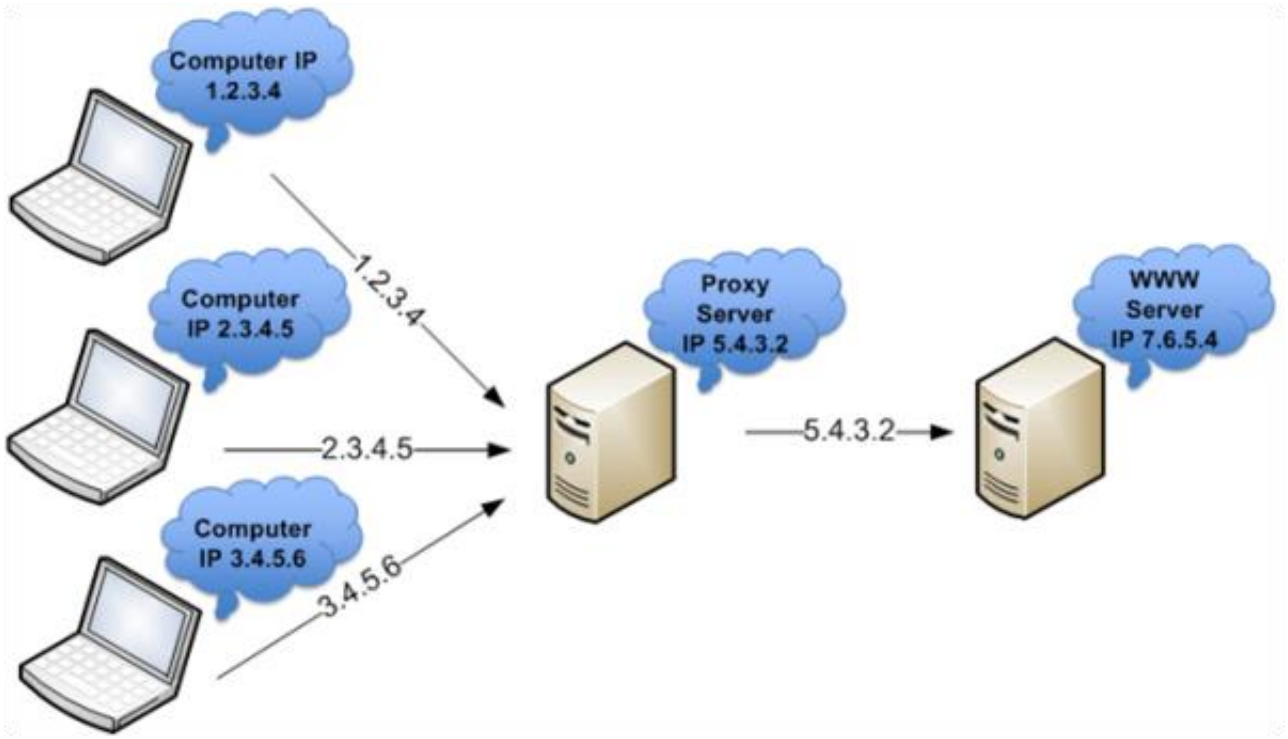
To hamper analysis of his own computer, in case it is seized



- turn off logging, turn of use of thumbnails,...
- encrypt hard drives and backups
- overwrite disks to make sure deleted data is wiped
- quantity
  have lots of data, on many computers, hard disks, USB drives,...
- never let your computer hibernate
- regularly reset the system time
  - to complicate analysis of meta-data and any remaining logs
- use anonimising Tor browser or a proxy
  - to hide your real IP address on the web

Anonymity on the internet: proxy

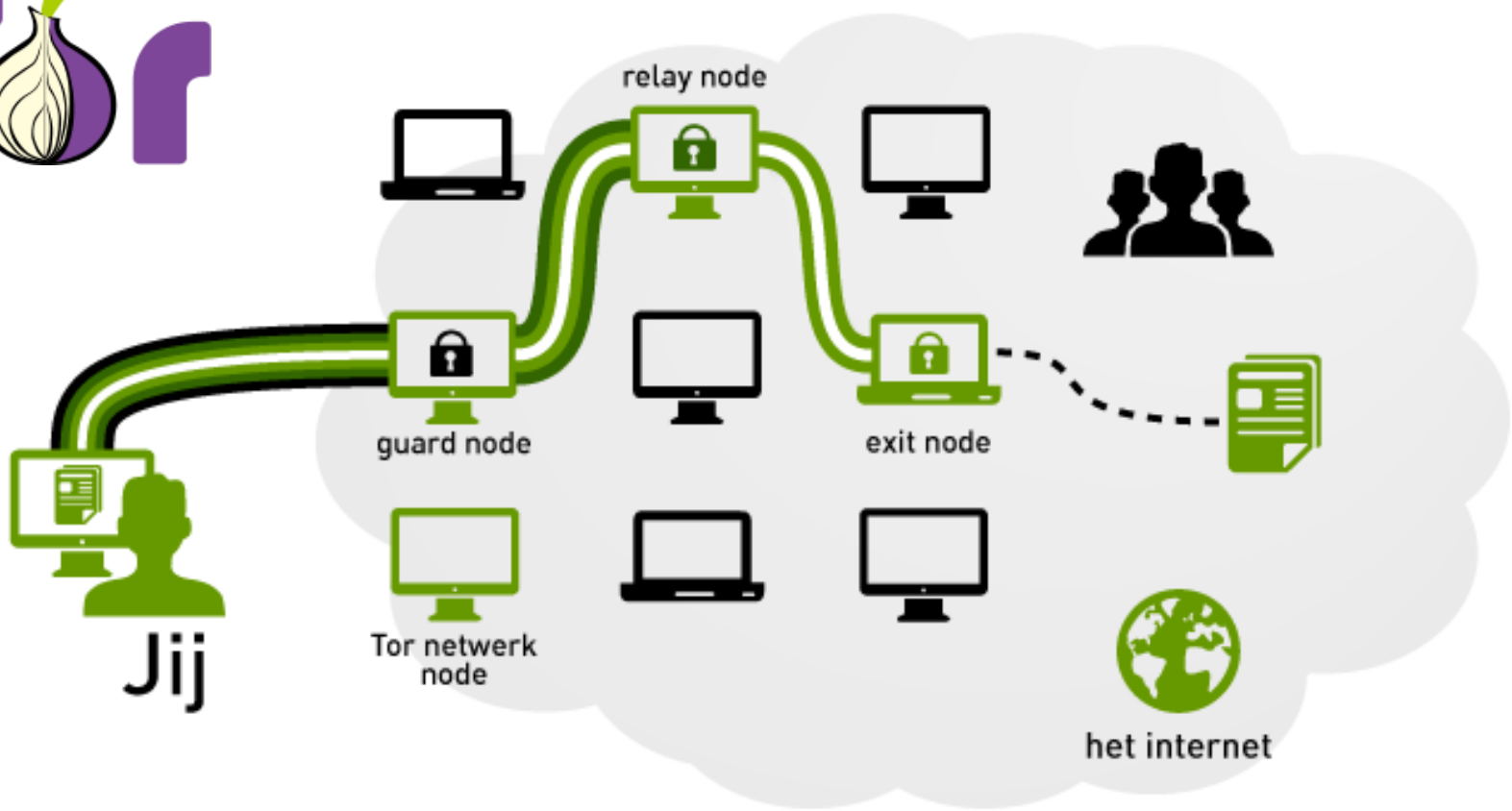
Countermeasure to revealing IP address (and location):
ues proxy as intermediary for internet traffic



Downside: the proxy server can see everything:
who is connecting to whom & all traffic

Anonymity on the internet: Tor

Layered encryption and traffic relayed via multiple nodes



Thanks for your attention!

Questions?