Miscellaneous:
tracking on the web
(& start on malware)

CS 161: Computer Security
Prof. Raluca Ada Popa

April 17, 2018

Credit: some slides are adapted from previous offerings of this course or from CS 241 of Prof. Dan Boneh
Miscellaneous topics

- Tracking on the web
- Malware (bots, worms, viruses)
- Bitcoin

All will be covered on exam, you should understand the concepts, but no need to understand the details.
What does a site learn about you when you visit them?

Discuss with your neighbor
The sites you visit learn:

- The **URLs** you’re interested in
  - Google/Bing also learns *what you’re searching for*
- Your **IP address**
  - Thus, your service provider & geo-location
  - Can often link you to other activity including at other sites
- Your browser’s capabilities, which OS you run, which language you prefer
- Which URL you looked at that took you there
  - Via the HTTP “**Referer**” header

They also learn cookies!
They also learn cookies

Why is that harmful?
Let's remove all of our cookies.
Cool, no web site is tracking us …
We do a search on “private browsing”
private browsing

---

**Private Browsing** - Browse the web without saving information about ...  
support.mozilla.org/.../private-browsing-browse-web-without-saving-inf... ▼

When using a shared computer, Private Browsing is great for viewing websites without saving stuff like cookies, temp files and a history of the pages you visit.

---

**Firefox 20 Launches With Improved Private Browsing, New ...**

[link](techcrunch.com/.../firefox-20-launches-with-per-tab-private-bro...)

by Frederic Lardinois - in 18,052 Google+ circles

Apr 2, 2013 – Firefox 20 is now available for download. The emphasis of today’s release is on Firefox's **private browsing** mode, which now allows Firefox ...

---

**Privacy mode - Wikipedia, the free encyclopedia**

[link](en.wikipedia.org/wiki/Privacy_mode)

Internet Explorer 8 in InPrivate mode. Google Chrome in Incognito mode. Privacy mode or "**private browsing**", sometimes informally referred to as "porn mode", ...

---

**Firefox 20 improves private browsing, fixes three critical flaws | ZDNet**

[link](www.zdnet.com/firefox-20-improves-private-browsing-fixes-three-critic...)

Apr 3, 2013 – Mozilla has released the latest version of its Firefox web browser which features new enhancement to **private browsing** and fixes a number of ...

---

**Private Browsing - Web Browsers - About.com**

[link](browsers.about.com/.../Web-Browsers/Web-Browser-Glossary/FAQs)

The methods for activating **private browsing** mode differ across browsers, operating systems, and device types. These step-by-step tutorials teach you how to ...
Google has stored a couple of cookies on our system.
Goodness knows what info they decided to put in the cookie.
But it lasts for months ...
Private browsing

You can turn on a mode called **private browsing** on your browser

What is this? Does it protect you against tracking?
We click on the top result
Note that this mode is privacy from your family, not from web sites!

Private Browsing - Browse the web without saving information about the sites you visit

As you browse the web, Firefox remembers lots of information for you: sites you've visited, files you've downloaded, and more. There may be times, however, when you don't want other users on your computer to see this information, such as when shopping for a birthday present.

Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited. This article explains what information is not saved when in Private Browsing and gives you step-by-step instructions for using it.

Warning: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.
Private browsing

“Private Browsing allows you to browse the Internet without saving any information about which sites and pages you’ve visited.”
- deletes history of URL visits, passwords, cookies too
- Private Browsing maintains cookies for as long as the private browsing window is open. Once you quit the browser, it gets deleted
- So still tracked for a good while!
Ironically, we’ve gained a bunch of cookies in the process.
This one sticks around for two years.

Expires: April 17, 2020
How did *YouTube* enter the picture?

There was YouTube content embedded on the site.
YouTube is remembering the version of Flash I’m running …
We navigate to The New York Times ...
U.S. Announces More Sanctions Against Russia Over Ukraine

By PETER BAKER and MARK LANDLER

The United States ordered travel bans and asset freezes for seven Russian officials, including two said to be in President Vladimir V. Putin’s inner circle, and froze assets for 17 firms.

Egypt Sentences More Than 680 to Death

The Muslim Brotherhood’s spiritual leader and hundreds of others were sentenced on charges of inciting or committing violence. Supporters, above, reacted to the verdict Monday.

Today’s Times Insider

Behind the scenes of The New York Times

- Thinking of Wine as Food With Eric Asimov
- Introducing Times Insider
What a lot of yummy cookies!

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dotomi.com</td>
<td></td>
</tr>
<tr>
<td>doubleclick.net</td>
<td></td>
</tr>
<tr>
<td>dynamiycyield.com</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td></td>
</tr>
<tr>
<td>imrworldwide.com</td>
<td></td>
</tr>
<tr>
<td>krxd.net</td>
<td></td>
</tr>
<tr>
<td>markets.on.nytimes.com</td>
<td></td>
</tr>
<tr>
<td>mediaplex.com</td>
<td></td>
</tr>
<tr>
<td>nytimes.com</td>
<td></td>
</tr>
<tr>
<td>revsci.net</td>
<td></td>
</tr>
<tr>
<td>scorecardresearch.com</td>
<td></td>
</tr>
<tr>
<td>support.mozilla.org</td>
<td></td>
</tr>
<tr>
<td>wt.o.nytimes.com</td>
<td></td>
</tr>
<tr>
<td>youtube.com</td>
<td></td>
</tr>
</tbody>
</table>

Name: <no cookie selected>  
Content: <no cookie selected>  
Host: <no cookie selected>  
Path: <no cookie selected>  
Send For: <no cookie selected>  
Expires: <no cookie selected>
Here are the ones from the website itself …
The following cookies are stored on your computer:

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>nytimes.com</td>
<td>_dyus_8765260</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>rsi_segs</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag27935.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag27728.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag15486.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag22998.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag21418.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtag22998.day</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_chartbeat2</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>_chartbeat_uuniq</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxtech</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>kxseg</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>krux_segs</td>
</tr>
</tbody>
</table>

- **This one tracks the details of my system & browser**

  Name: kxtech
  Content: device%3DComputer%26manufacturer%3DApple%2520Inc.%26os%3DMac%2520OS%2520X%26browser%3DFirefox%25202
  Host: www.nytimes.com
  Path: /
  Send For: Any type of connection
  Expires: May 28, 2014 at 2:26:53 PM
doubleclick.net - who's that? And how did it get there from visiting www.nytimes.com?

doubleclick.net is a tracker, purposefully embedded by NYTimes for tracking.
Third-Party Cookies

How can a web site enable a third party to plant cookies in your browser & later retrieve them?

- Include on the site’s page (for example):
  - `<img src="http://doubleclick.net/ad.gif" width=1 height=1>`

Why would a site do that?

- Site has a business relationship w/ DoubleClick

Why can this track you?

- Now DoubleClick sees all of your activity that involves their web sites
- Because your browser dutifully sends them their cookies for any web page that has that img
- Identifier in cookie ties together activity as = YOU

* Owned by Google, by the way
Moral: you can be tracked by a site even if you do not visit that site
Remember this 2-year Mozilla cookie?
Google Analytics

- Any web site can (anonymously) register with Google to instrument their site for analytics.
  - Gather information about who visits, what they do when they visit.
- To do so, site adds a small Javascript snippet that loads http://www.google-analytics.com/ga.js.
  - You can see sites that do this because they introduce a "__utma" cookie.
- Code ships off to Google information associated with your visit to the web site.
  - Shipped by fetching a GIF w/ values encoded in URL.
  - Web site can use it to analyze their ad “campaigns”.
  - Not a small amount of info …
Values Reportable via Google Analytics

Affiliation
Billing City
Billing Country
Billing Region
Browser Lang.
Complete URL
Cookie Values
Current Page
Event Tracking
Flash Version
Grand Total

Host Name
Java-enabled
Language Encoding
Order ID
Page Title
Product Code
Product Name
Profile Number
Repeat Campaign Visit
Quantity
Screen Color Depth

Screen Resolution
Shipping Cost
Special Event
Start Campaign Sess.
Tax
Tracking Code Version
Unique GIF ID
Unit Price
User Defined Var
Variations on an Item
Still More Tracking Techniques ...

Any scenario where browsers execute programs that manage persistent state can support tracking by cookies

- Such as .... *Flash* ?
My browser had Flash cookies from 67 sites!

Sure, this is where you’d think to look to analyze what Flash cookies are stored on your machine.

Some Flash cookies “respawn” regular browser cookies that you previously deleted!
A new bug in Internet Explorer allows hackers to commandeer your computer.

NEW YORK (CNNMoney)

If you're using Internet Explorer and click on the wrong link, a hacker could hijack your computer.
What does Facebook learn?

- Many pages include a Facebook “Like” button.
- What are the implications, for user tracking?

- Facebook can track you on every site that you visit that embeds such a button, not only when you are actually visit Facebook.
What information does Facebook get when I visit a site with the Like button?

If you’re logged into Facebook and visit a website with the Like button, your browser sends us information about your visit. Since the Like button is a little piece of Facebook embedded on another website, the browser is sending info about the request to load Facebook content on that page.

We record some of this info to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you’re visiting, the date and time and other browser-related info.
Cookies form the core of how Internet advertising works today

- Without them, arguably you’d have to pay for content up front a lot more
  - (and payment would mean you’d lose anonymity anyway)
- A “better ad experience” is not necessarily bad
  - Ads that reflect your interests; not seeing repeated ads

But: ease of gathering so much data so easily \(\Rightarrow\) concern of losing control how it’s used

- Privacy concerns
- Large amounts of private data in one place
Trust in Facebook plummets after Cambridge Analytica scandal, Zuckerberg testimony
When you interview, they Know What You’ve Posted

Gone are the days when all job seekers had to worry about were their résumés and cover letters. Today, those documents remain a staple of the job-search process, but they are joined by a growing phenomenon: social networking.

Forty-five percent of employers reported in a June 2009 CareerBuilder survey that they use social networking sites to screen potential employees, compared to only 22 percent of employers last year. Eleven percent of employers plan to start using social networking sites for the screening process. More than 2,600 hiring managers participated in the survey.
Why employers disregard candidates after screening online

Thirty-five percent of employers reported they have found content on social networking sites that caused them not to hire the candidate, including:

- Candidate posted provocative or inappropriate photographs or information -- 53 percent
- Candidate posted content about them drinking or using drugs -- 44 percent
- Candidate bad-mouthed their previous employer, co-workers or clients -- 35 percent
- Candidate showed poor communication skills -- 29 percent
- Candidate made discriminatory comments -- 26 percent
- Candidate lied about qualifications -- 24 percent
- Candidate shared confidential information from previous employer -- 20 percent
Cookies etc. form the core of how Internet advertising works today
- Without them, arguably you’d have to pay for content up front a lot more
  - (and payment would mean you’d lose anonymity anyway)
- A “better ad experience” is not necessarily bad
  - Ads that reflect your interests; not seeing repeated ads

But: ease of gathering so much data so easily ⇒ concern of losing control how it’s used
- Content shared with friends doesn’t just stay with friends …
- You really don’t have a good sense of just what you’re giving away …
Inadvertent information leaking

Consider posting a picture on Twitter
The world can see it, but what more can an outside figure out about you?
Photos are tagged with location from the camera.
I Can Stalk U
Raising awareness about inadvertent information sharing

Who have we stalked recently?

ICanStalkU was able to stalk RangeLifeEnt at 51 Great Jones St New York NY
1 minute ago • Map Location • View Tweet • View Picture • Reply to RangeLifeEnt

ICanStalkU was able to stalk Inicklassen at http://maps.google.com/?q=57.134444444,12.7141666667
2 minutes ago • Map Location • View Tweet • View Picture • Reply to Inicklassen

ICanStalkU was able to stalk Welerson13 at http://maps.google.com/?q=-15.738055556,-47.898611111
2 minutes ago • Map Location • View Tweet • View Picture • Reply to Welerson13

ICanStalkU was able to stalk BritBangert at 920 Hawley St Taylorville IL
1 minute ago • Map Location • View Tweet • View Picture • Reply to BritBangert

ICanStalkU was able to stalk jiggy_Owla at http://maps.google.com/?q=13.7830055879,100.518500685
4 minutes ago • Map Location • View Tweet • View Picture • Reply to jiggy_Owla

ICanStalkU was able to stalk gcolony at http://maps.google.com/?q=37.7851666667,-122.404166667
4 minutes ago • Map Location • View Tweet • View Picture • Reply to gcolony

Links
- Mayhemic Labs
- PaulDotCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

How did you find me?

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.

Help me fix this!

Disabling Geo-Tagging on your phone is easy. Check your user manual for instructions.
How To Gain Better Privacy?

discuss with your neighbor
How To Gain Better Privacy?

- Force of law
  - Example #1: web site privacy policies
    - US sites that violate them commit false advertising
    - But: policy might be "Yep, we sell everything about you, Ha Ha!"
7. **Collection of Viewing Information.** You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.
How To Gain Better Privacy?

- **Force of law**
  - **Example #1**: web site privacy policies
    - US sites that violate them commit false advertising
    - But: policy might be “Yep, we sell everything about you, Ha Ha!”
  - **Example #2**: SB 1386 (bill in CA legislature)
    - Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)
    - Quite effective at getting sites to pay attention to securing personal information
  - **Example #3**: GDPR law
May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waqqener, UCB's chief technology officer, said in a press conference Friday afternoon.
General Data Protection Regulation (GDPR)

New European law (2018) designed to allow individuals to better control their personal data

- Requires consent or strong reason to process and store personal information
- Gives a user the right to know what information is held about them
- Allows a user to request that their information is deleted and that they are ‘forgotten’
- Requires that personal information is properly protected.
- ... and more

Applies to US companies with European customers too
How To Gain Better Privacy?

Technology

- Various browser additions
- Special browser extensions
- Tor and anonymizers to hide IP addresses
Browser: “Tracking protection”

Private browsing includes tracking protection.

You can choose a blocking list in your Firefox browser for example:

- **Basic (default):** Blocks third-party trackers based on Disconnect.me. **Blocks commonly known analytics trackers, social sharing trackers, and advertising trackers,** but allows some known content trackers to reduce website breakage.

- **strict:** **blocks all known trackers, including analytics, trackers, social sharing trackers, and advertising trackers as well as content trackers.** The strict list will break some videos, photo slideshows, and some social networks.
Browsers: Do not track flag

You can turn on this flag in your browser

What does it do?
- Tells web servers you want to opt-out of tracking
- It does this by transmitting a Do Not Track HTTP header every time your data is requested from a web server

It does not enforce that there is no tracking, it is up to the web servers whether they decide to track or not
Some ad companies do provide more generic ads as a result of this flag
Browser extension: Ghostery

User installs browser extension:

1. Recognizes third-party tracking scripts on a web page based on an actively curated database of such scripts

2. Blocks HTTP requests to these sites
   • as a result, Facebook buttons don’t even show

3. Users can create “Whitelists” of allowed sites
   • e.g., allow FB button but note that you allow tracking by FB too
Users can opt-in to sending anonymously data back to Evidon, the parent company, to improve its tracking database.

Evidon sells this data to ad companies.

Attempted excuse: strategy is transparent, users opt into this.
Conclusions

- Third-party apps can track us even if we don't visit their website.
- Tracking is very common on the web and can collect a lot of data about you.
- Some solutions exist, but have caveats.
Miscellaneous: malware

Credit for some slides: Damon McCoy and Vitaly Shmatikov
Malware

- Malicious code often masquerades as good software or attaches itself to good software.
- Some malicious programs need host programs:
  - Trojan horses (malicious code hidden in a useful program), logic bombs (a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects), backdoors.
- Others can exist and propagate independently:
  - Worms, automated viruses.
- Many infection vectors and propagation methods.
- Modern malware often combines trojan, rootkit, and worm functionality.
Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections
[Updated]
Superfish may make it trivial for attackers to spoof any HTTPS website.

by Dan Goodin - Feb 19, 2015 8:36am PST
Viruses vs. Worms

**VIRUS**
- Propagates by infecting other programs
- Usually inserted into host code (not a standalone program)

**WORM**
- Propagates automatically by copying itself to target systems
- A standalone program
“Reflections on Trusting Trust”

Ken Thompson’s 1983 Turing Award lecture

1. Added a backdoor-opening Trojan to login program
2. Anyone looking at source code would see this, so changed the compiler to add backdoor at compile-time
3. Anyone looking at compiler source code would see this, so changed the compiler to recognize when it’s compiling a new compiler and to insert Trojan into it

“The moral is obvious. You can’t trust code you did not totally create yourself.”
Viruses

- **Virus** propagates by **infecting other programs**
  - Automatically creates copies of itself, but to propagate, a human has to run an infected program
  - Self-propagating viruses are often called **worms**
- Many propagation methods
  - Insert a copy into every executable (.COM, .EXE)
  - Insert a copy into boot sectors of disks
  - Infect common OS routines, stay in memory
First Virus: Creeper

- Written in 1971 at BBN
- Infected DEC PDP-10 machines running TENEX OS
- Jumped from machine to machine over ARPANET
  - Copied its state over, tried to delete old copy
- Payload: displayed a message
  “I’m the creeper, catch me if you can!”
- Later, Reaper was written to hunt down Creeper

http://history-computer.com/Internet/Maturing/Thomas.html
Polymorphic Viruses

- **Encrypted viruses**: constant decryptor content followed by the encrypted virus body
- **Polymorphic viruses**: each copy creates a new random encryption of the same virus body
  - Decryptor code constant and can be detected
  - Historical note: “Crypto” virus decrypted its body by brute-force key search to avoid explicit decryptor code
Virus Detection

1. Simple anti-virus scanners
   - Look for signatures (fragments of known virus code)
   - Heuristics for recognizing code associated with viruses
     - Example: polymorphic viruses often use decryption loops
   - Integrity checking to detect file modifications
     - Keep track of file sizes, checksums, keyed HMACs of contents

2. Generic decryption and emulation
   - Emulate CPU execution for a few hundred instructions, recognize known virus body after it has been decrypted
   - Does not work very well against viruses with mutating bodies and viruses not located near beginning of infected executable
Virus Detection by Emulation

Say you want to detect if F is a virus, but it is polymorphic so you are not sure:
- Run it in a sandbox
- The virus will start decrypting its payload and executing it
- Look at the set of instructions that are executed and see if those match a signature of a known virus

Insight here: check signature at runtime instead of signature of file content (which could be different)
Metamorphic Viruses

- Obvious next step: *mutate the virus body*, too
- Apparition: an early Win32 metamorphic virus
  - Carries its source code (contains useless junk)
  - Looks for compiler on infected machine
  - Changes junk in its source and recompiles itself
  - New binary copy looks different! [So new instruction sequences]
- Mutation is common in macro and script viruses
  - A macro is an executable program embedded in a word processing document (MS Word) or spreadsheet (Excel)
  - Macros and scripts are usually interpreted, not compiled
Obfuscation and Anti-Debugging

- Common in all kinds of malware
- Goal: prevent code analysis and signature-based detection, foil reverse-engineering
- Code obfuscation and mutation
  - Packed binaries, hard-to-analyze code structures
  - Different code in each copy of the virus
    - Effect of code execution is the same, but this is difficult to detect by passive/static analysis (undecidable problem)
- Detect debuggers and virtual machines, terminate execution
Mutation Techniques

- Large arsenal of obfuscation techniques
  - Instructions reordered, branch conditions reversed, different register names, different subroutine order
  - Jumps and NOPs inserted in random places
  - Garbage opcodes inserted in unreachable code areas
  - Instruction sequences replaced with other instructions that have the same effect, but different opcodes
    - Mutate `SUB EAX, EAX` into `XOR EAX, EAX` or `MOV EBP, ESP` into `PUSH ESP; POP EBP`
Propagation via Websites

- Websites with popular content
  - Games: 60% of websites contain executable content, one-third contain at least one malicious executable
  - Celebrities, adult content, everything except news

[Moschuk et al.]
Drive-By Downloads

- Websites “push” malicious executables to user’s browser with inline JavaScript or pop-up windows
  - Naïve user may click “Yes” in the dialog box
- Can install malicious software *automatically* by exploiting bugs in the user’s browser
  - 1.5% of URLs - Moshchuk et al. study
  - 5.3% of URLs - “Ghost Turns Zombie”
  - 1.3% of Google queries - “All Your IFRAMEs Point to Us”
- Many infectious sites exist only for a short time, behave non-deterministically, change often
Obfuscated JavaScript

[Provos et al.]

document.write(unescape("%3CHEAD%3E%0D%0A%3C/HEAD%3E%0D%0A
%3C/SCRIPT%3E%0D%0A/*%criptografado%20pelo%20Fal%20-%20Deboa%E7%E3o%20gr%E1tis%20para%20seu%20site%20renda%20extra%0D
...%3C/SCRIPT%3E%0D%0A%3C/HEAD%3E%0D%0A%3CBODY%3E%0D%0A%3C/HTML%3E%0D%0A"));
//-->
</SCRIPT>
“Ghost in the Browser”

- Large study of malicious URLs by Provos et al. (Google security team)
- In-depth analysis of 4.5 million URLs
  - About 10% malicious
- Several ways to introduce exploits
  - Compromised Web servers
  - User-contributed content
  - Advertising
  - Third-party widgets
Trust in Web Advertising

- Advertising, by definition, is ceding control of Web content to another party.
- Webmasters must trust advertisers not to show malicious content.
- Sub-syndication allows advertisers to rent out their advertising space to other advertisers.
  - Companies like Doubleclick have massive ad trading desks, also real-time auctions, exchanges, etc.
- Trust is not transitive!
  - Webmaster may trust his advertisers, but this does not mean he should trust those trusted by his advertisers.
Example of an Advertising Exploit

- Video sharing site includes a banner from a large US advertising company as a single line of JavaScript...
- ... which generates JavaScript to be fetched from another large US company
- ... which generates more JavaScript pointing to a smaller US company that uses geo-targeting for its ads
- ... the ad is a single line of HTML containing an iframe to be fetched from a Russian advertising company
- ... when retrieving iframe, “Location:” header redirects browser to a certain IP address
- ... which serves encrypted JavaScript, attempting multiple exploits against the browser

[Provos et al.]
Not a Theoretical Threat

- Hundreds of thousands of malicious ads online
  - 384,000 in 2013 vs. 70,000 in 2011 (source: RiskIQ)
  - Google disabled ads from more than 400,000 malware sites in 2013

- Dec 27, 2013 – Jan 4, 2014: Yahoo! serves a malicious ad to European customers
  - The ad attempts to exploit security holes in Java on Windows, install multiple viruses including Zeus (used to steal online banking credentials)
Social Engineering

- **Goal:** trick the user into “voluntarily” installing a malicious binary
- **Fake video players and video codecs**
  - Example: website with thumbnails of adult videos, clicking on a thumbnail brings up a page that looks like Windows Media Player and a prompt:
    - “Windows Media Player cannot play video file. Click here to download missing Video ActiveX object.”
  - The “codec” is actually a malware binary
- **Fake antivirus (“scareware”)**
  - January 2009: 148,000 infected URLs, 450 domains

[Provos et al.]
Fake Antivirus
### Сумма, USD

<table>
<thead>
<tr>
<th>Loader</th>
<th>Сетапы</th>
<th>Покупки</th>
<th>Покупки</th>
<th>Возвраты</th>
<th>Рефералы</th>
<th>Прибыль</th>
</tr>
</thead>
<tbody>
<tr>
<td>37943</td>
<td>19989</td>
<td>667</td>
<td>29853.86</td>
<td>-436.72</td>
<td>0.00</td>
<td>29417.14</td>
</tr>
<tr>
<td>39895</td>
<td>19722</td>
<td>74</td>
<td>5420.64</td>
<td>0.00</td>
<td>0.00</td>
<td>5420.64</td>
</tr>
<tr>
<td>41687</td>
<td>18619</td>
<td>384</td>
<td>28148.96</td>
<td>-36.71</td>
<td>0.00</td>
<td>28112.25</td>
</tr>
<tr>
<td>38059</td>
<td>16038</td>
<td>249</td>
<td>13908.24</td>
<td>-118.54</td>
<td>0.00</td>
<td>13789.70</td>
</tr>
<tr>
<td>39160</td>
<td>15335</td>
<td>176</td>
<td>9726.17</td>
<td>0.00</td>
<td>0.00</td>
<td>9726.17</td>
</tr>
<tr>
<td>29968</td>
<td>12076</td>
<td>207</td>
<td>11672.71</td>
<td>0.00</td>
<td>0.00</td>
<td>11672.71</td>
</tr>
<tr>
<td>13293</td>
<td>6866</td>
<td>129</td>
<td>6920.81</td>
<td>0.00</td>
<td>0.00</td>
<td>6920.81</td>
</tr>
<tr>
<td>18055</td>
<td>8915</td>
<td>157</td>
<td>7557.25</td>
<td>0.00</td>
<td>0.00</td>
<td>7557.25</td>
</tr>
<tr>
<td>29642</td>
<td>14802</td>
<td>265</td>
<td>12852.29</td>
<td>0.00</td>
<td>0.00</td>
<td>12852.29</td>
</tr>
<tr>
<td>50457</td>
<td>22463</td>
<td>464</td>
<td>21055.29</td>
<td>0.00</td>
<td>0.00</td>
<td>21055.29</td>
</tr>
<tr>
<td>338159</td>
<td>154825</td>
<td>2772</td>
<td>147116.22</td>
<td>-591.97</td>
<td>0.00</td>
<td>146524.25</td>
</tr>
</tbody>
</table>

### Loads Installs Purchases Total Refunds Net Profit

---

Source: Joe Stewart, Secureworks