On-line advertising

- Banner, popup
- Targetted ads
- Malware
- Adblockers

- Classified advertising
- Personal informations
- Third party services
- Risks
Ad Serving Architecture

- User visits a website (1)
- Publisher sends content (2)
- User is directed to an ad server (3)
- Ad server sends a script (4)
- User's browser executes the script and requests ads (5)
- Ad server serves ads (6)
Figure 1.1 The ad serving architecture. Advertisers subscribe to an Ad Network whose role is to automatically embed ads into related Web pages. Publishers and ad networks have a contractual agreement (dashed arrow) that lets ad servers add advertisement to publishers’ Web pages. Ads are stored at Ad Servers, which belong to the ad network. When a User visits a website of a publisher that hosts ads (step 1), the user’s browser starts downloading the content of the Web page (step 2), and is then directed to one of the ad servers belonging to the ad network (step 3). During the first communication with the ad server, a script is served to the user (step 4) that executes on the user’s machine and requests ads from the ad server (step 5). The ad server chooses and serves ads that match users’ interest (step 6) in order to maximize the potential ad revenue.
Targeted Advertising

- can be targeted to individual user’s interests

- ad targeting techniques
  - Contextual
  - Behavioral
  - Location-based
Revenue Models

- per impression model
  - cost-per-mille (CPM) - used for brand advertising
- per click - pay-per-click (PPC) model
  - cost-per-click (CPC) – instant feedback
  - clickthrough rate (CTR) – clicked/delivered
- per action model – targeted
  - cost-per-action (CPA) – eg.: subscribing a newsletter – used for collecting contacts
Exploits of Online Advertising Systems

- Rely on HTTP protocol
- Selfish adversary
  - Click fraud
- Malicious adversary
  - Malwertising
  - DoS attack
  - Botnets
Click Fraud

- ROI – Return Of Investment
- Publisher click inflation attack
  - PPC revenue model
- Advertiser competitor clicking attack
  - Exhaust the daily budget of other advertisers
  - Impression based: fake pages containing ads that users never see
  - PPC: clicks are not generated by legitimate users
  - Action based: simulate the action of legitimate user
Attacks

- **Badvertising** - fraudulent clicks are generated on ads hosted by the attacker corrupting the JavaScript required to properly include ads into Web pages
- **Clickjacking** - multiple transparent layers of Web pages
Figure 1.2 Clickjacking attack. In a clickjacking attack, a victim browses a Web page (in this example myphotos.com in the bottom frame) that loads an invisible top frame (in this case a Google search result page) and tricks the victim into clicking on the bottom frame while actually affecting the site in the top frame. We have made the top frame partially transparent for the purpose of illustration, whereas in the actual attack the top page is invisible to users. When the victim clicks on the button "Next" to proceed to the following photo on the myphotos.com page, the click is hijacked and turned into a click on a CPC ad on the invisible Google search result page.

Figure 1.3 Schema of a click fraud attack. A fraudster buys legitimate traffic from a pornographic website in order to generate traffic at its own website (step 1) and produce legitimate-looking click traffic on ads. The fraudster’s website creates a number of invisible iframes (step 2) that load parked domain websites (step 3) owned by the fraudster and hosting CPC ads (step 4). In collaboration with clicking websites, the parked domain websites produce fraudulent clicks on their CPC ads (step 5). Fraudulent clicks result in lodging of legitimate big-name-brand publishers with their own CPM ads (step 6). Reputable advertisers that pay for their ads to appear on quality publishers’ websites have their ads appear within pornographic websites, which enables AdSafe to detect the fraud.
Malvertising: Spreading Malware via Ads

• Ads that attempt to infect an ad viewer’s computer
• users do not even have to click on ads to trigger malware
• hidden iFrame communicate with a malware server in the background
• adding its ad to a legitimate ad network
Inflight Modification of Ad Traffic

- display to end users altered ads, as well as altered search results
- Bahama botnet
  - corrupting the DNS translation
  - Google.com was translated to IP owned by the attacker
  - The returned query was modified
- Botnets of compromised wireless routers
- HTTPS
Adware: Unsolicited Software Ads

- Published for users who do not wish to pay for certain software
- Spyware - that collects information about users in order to display advertisements in the Web browser
- Read the terms of use
Summary

- Ad-serving architecture
- Targeted Advertising
- Revenue Models
- Exploits
  - Click fraud
  - Malvertising
  - Adware
Classified advertising

- Seller
  - Serving personal informations
  - Verification (email, phone)
  - Buying features, services
  - Contact
  - Delivering the product

- Buyer
  - Contact
  - Serving personal informations
  - Verification (email, phone)
  - Receive the product
Personal informations

- **Seller**
  - Name
  - Email address
  - Phone number
  - Address (pick up, invoice)
  - Bank account number

- **Buyer**
  - Email address
  - Bank account number
  - Delivery address
  - Phone number
Security

- Personal information management
  - Third party services
  - Permission
  - According to terms

- Risks
  - Identity theft, data theft, phising
  - The loss of product
  - The loss of money
Protection against ...

- Identity -, data theft, phishing
  - Visibility management – personal informations
  - Using images instead of text
- Scammers, fraudsters
  - Ad review, moderation,
  - Pre-screening messages (harassment)
  - Monitoring the activity
  - Find patterns
Summary

- Classified advertising
- Personal informations
- Security
- Protection
Thank you for your attention
Sources