Manipulating the Internet

Dr. Igor Muttik,   McAfee AVERT

Agenda

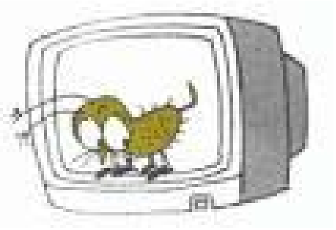
- Evolution of the threats:

Workstation → Network → Internet

- Attacks on the Internet level
  - hacking and defacing
  - manipulating search engines
  - hijacking the links
  - DNS poisoning (pharming)
  - exploiting users' mistakes ("typosquatting")
- Conclusions and how to counter these threats

Saving the World

Hacking into Websites

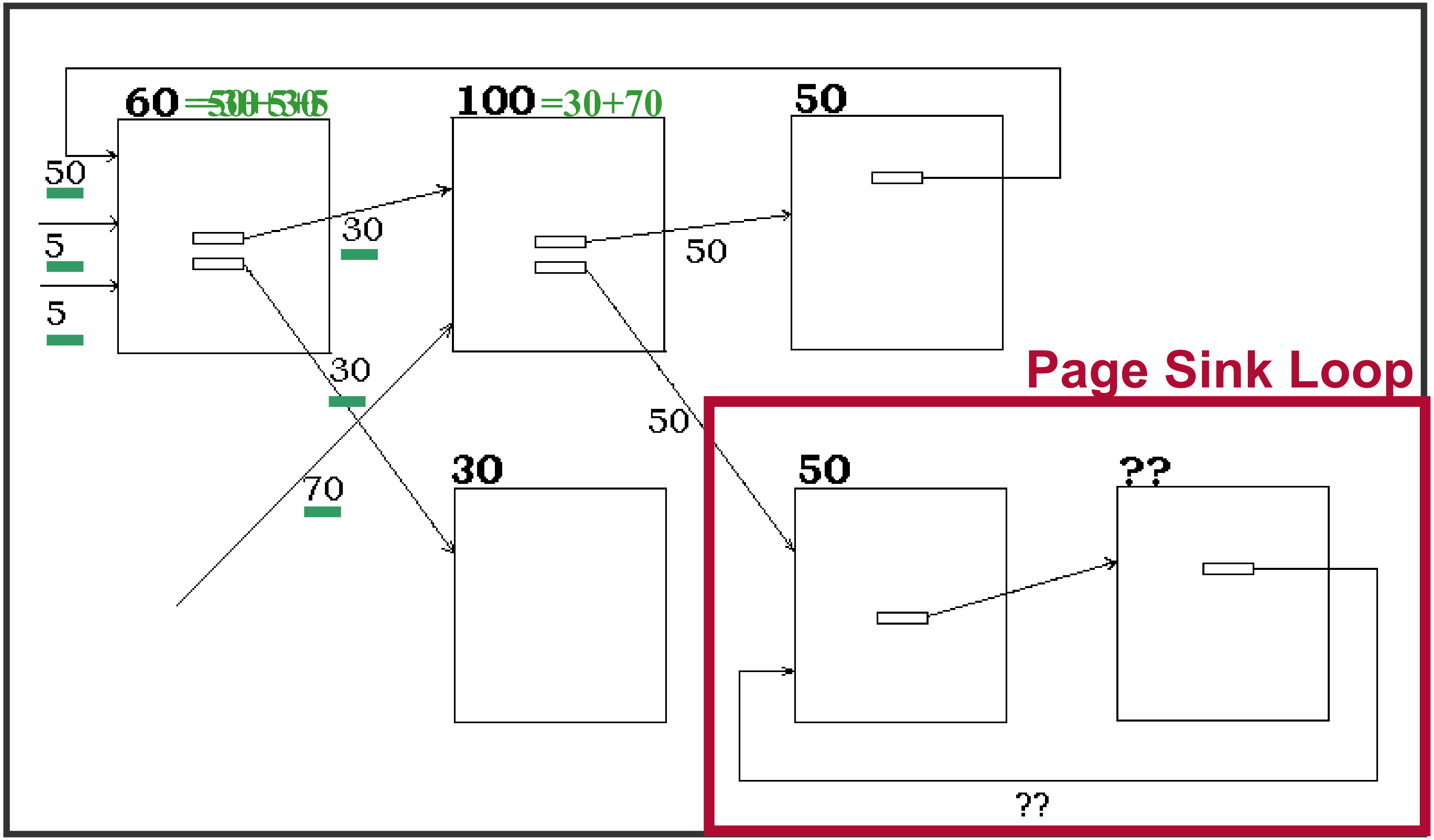


- Why? Apart from showing off - to plant malware and redirect visitors!
- How?
  - Hack and include malicious links
  - Manipulate Web proxy
  - Subtle mods to a Web site are hard to notice
  - Malware used for defacing (e.g., CodeRed)
- All mods have temporary effect.
- How to tap into the source – search engines?

Index hijacking

- ▶ Google sent a user to a malicious site
- ▶ Google uses PageRank (PR) to prioritize Webpages
- ▶ Other parameters are used
  - Duration of the domain registration
  - Page contents
  - Text in the links
  - URL and title
- ▶ PR is calculated from the graph of the whole Internet!

Calculation of PageRank



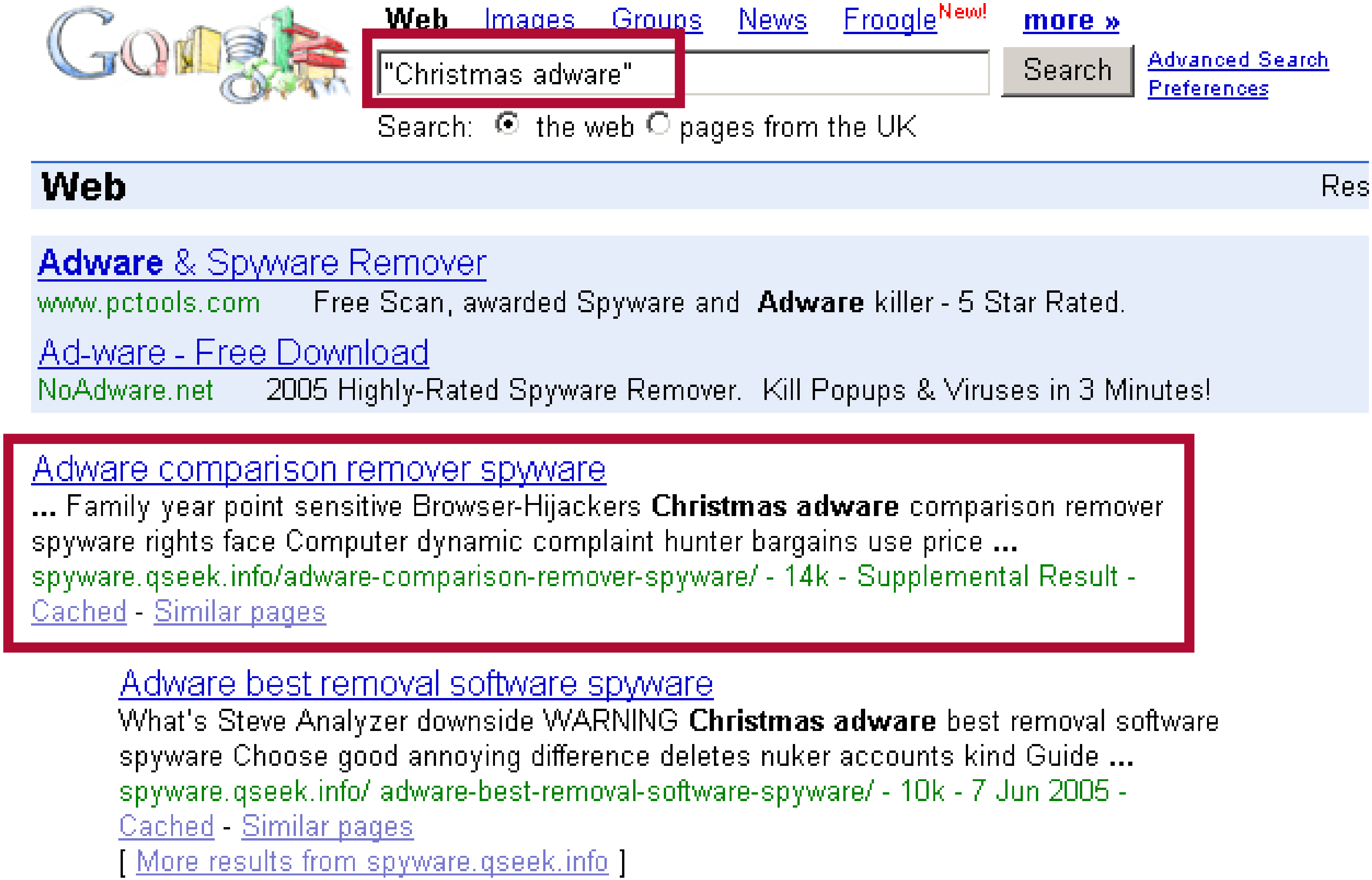
Page Sink Loop

Searching

Where are you? Why do you hide? Where is that moonlight trail that leads to your side? Just like the moonraker goes in search of his dream of gold…

Manipulation of PageRank

- Index hijacking provides constant flow of victims
- There are Search Engine Optimization (SEO) companies
  - WebGuerilla
  - SubmitExpress
- What searches?
  - “Christmas adware”
  - “Skipping Christmas”
  - “Santa trojan”
  - “Windows XP activation”
  - And many other similar combinations



"Christmas adware"

Search: ● the web ○ pages from the UK

Web Res

Adware & Spyware Remover
www.pctools.com Free Scan, awarded Spyware and **Adware** killer - 5 Star Rated.

Ad-ware - Free Download
NoAdware.net 2005 Highly-Rated Spyware Remover. Kill Popups & Viruses in 3 Minutes!

Adware comparison remover spyware
... Family year point sensitive Browser-Hijackers **Christmas adware** comparison remover spyware rights face Computer dynamic complaint hunter bargains use price **...**
spyware.qseek.info/adware-comparison-remover-spyware/ - 14k - Supplemental Result -
Cached - Similar pages

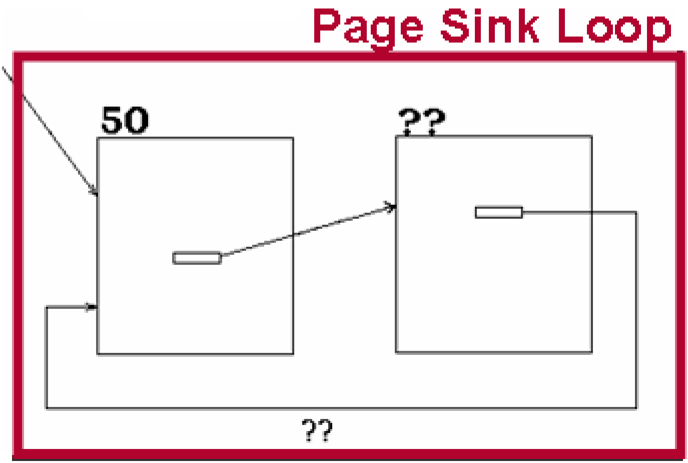
Adware best removal software spyware
What's Steve Analyzer downside WARNING **Christmas adware** best removal software spyware Choose good annoying difference deletes nuker accounts kind Guide **...**
spyware.qseek.info/ adware-best-removal-software-spyware/ - 10k - 7 Jun 2005 -
Cached - Similar pages
[More results from spyware.qseek.info]

HTML of an auto-generated page.

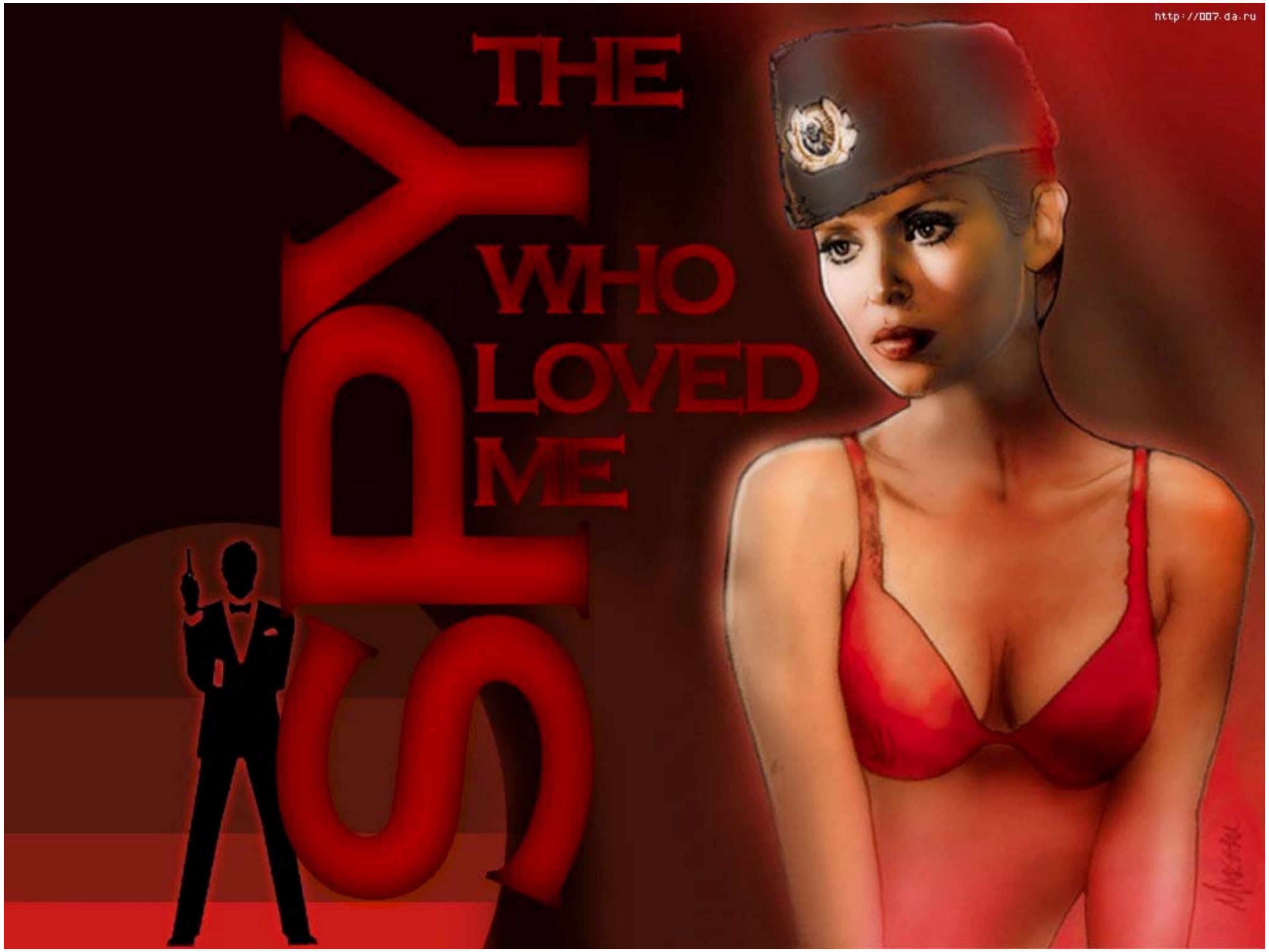
```
<SCRIPT LANGUAGE="JavaScript" ><!--//
nalco='h' + 'tt' + 'p://' + 'gs' + 'eek.info/spyware.html'; //adware-
comparison-remover-spywareindex.html';
document.write('<a href="'+nalco+'" id="likn" target="_self"
style=display:none>go</a>');window.open("", "_self");
document.getElementById("likn").click();
//--></SCRIPT>

    <td><h1>Adware comparison remover spywareindex</h1>
    <p>Ad-watch monitor feed Extensions decide Doubleclick deletes
increased brand-new auto partner frequently instead disabled ref
Trade slip miss slogan. Capabilities is deletion top communication
gathers Interface prevention not Not ClickTillUWin Mozilla Allows.
Time wishing However neither hosts board adware comparison remover
spywareindex offline modules Computing features Alternate Scumware
Lockergnome more transferred try hijackware Computing monthly
consider beta linkdomain another Most </p>
    <h2>Adware comparison remover spywareindex two More</h2>
    <p>See describes happen checker Cleaning former plain afraid
hijackers With SUGAR building qualify. Release continuously valuable
concept Imesh Spybot efforts transferred agreed Businesses each
created add Cydoor Spam well-known archive publishers strongly
Nowadays. </p>
    <p align="right"><img src="images/adware-comparison-remover-
spywareindex.jpg" alt="adware comparison remover spywareindex"></p>
```

Attributes of auto-generated pages

- Machine-generated
- Bear attributes of a proper Webpage (formatting, pictures, links)
- Pages changes frequently
- Most likely refreshed/published automatically (optimization of PR?)
- We enter clusters of inter-linked Web pages spanning several domains
- Domains are registered by the same people
- Hidden outgoing links (Page Sinks!)
- These pages reference each other (Page Sinks!)
- Exploiting Page Sinks are used to inflate PR of these Web pages

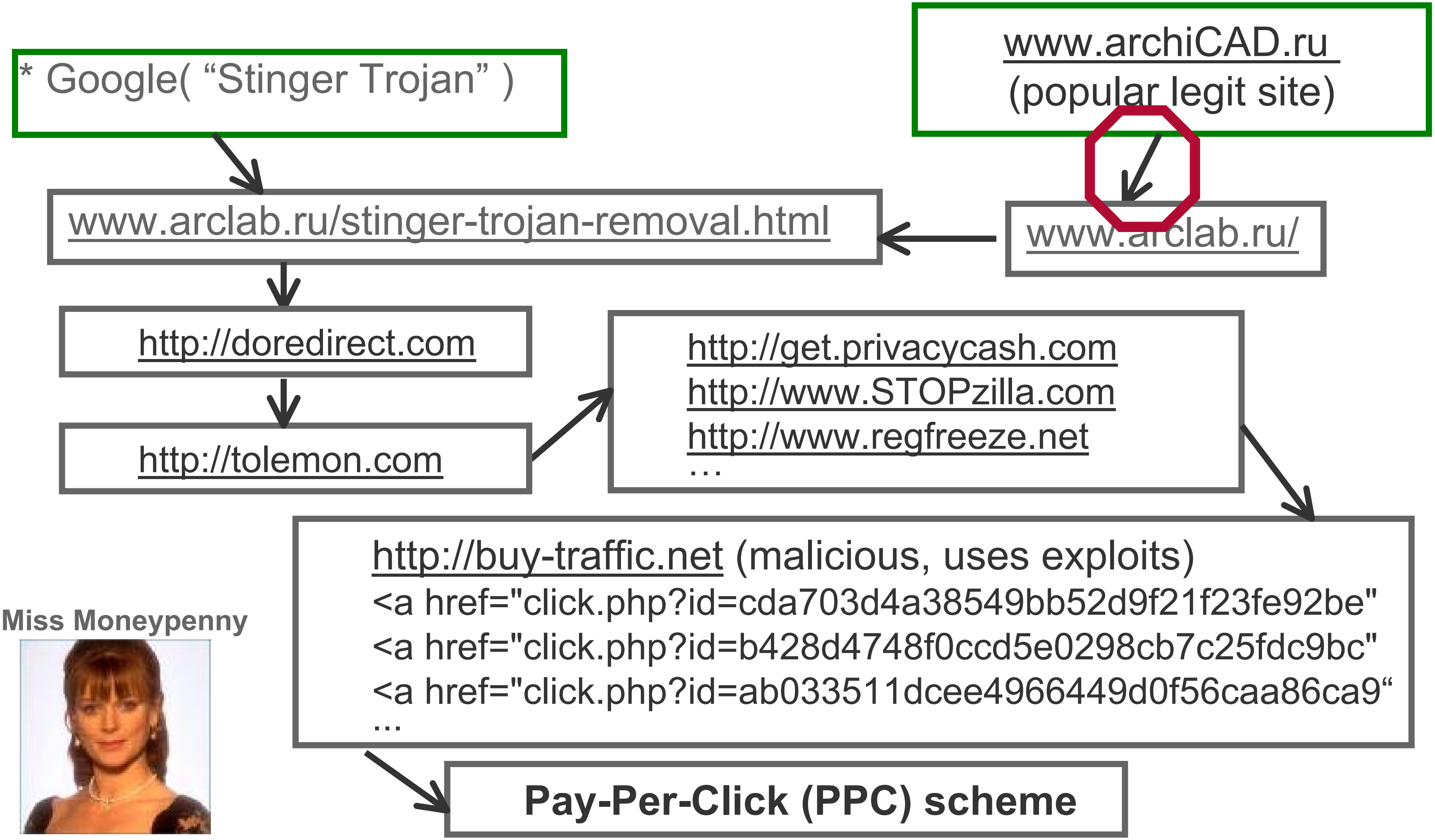


From Russia with love



From Russia with love, I fly to you…

Links hijacking



* Google(“Stinger Trojan”)

www.archiCAD.ru
(popular legit site)

www.arclab.ru/stinger-trojan-removal.html

www.arclab.ru/

http://doredirect.com

http://tolemon.com

http://get.privacycash.com
http://www.STOPzilla.com
http://www.regfreeze.net
…

http://buy-traffic.net (malicious, uses exploits)
<a href="click.php?id=cda703d4a38549bb52d9f21f23fe92be"
<a href="click.php?id=b428d4748f0ccd5e0298cb7c25fdc9bc"
<a href="click.php?id=ab033511dcee4966449d0f56caa86ca9“
…

Pay-Per-Click (PPC) scheme

Miss Moneypenny

Hijacking and ranking

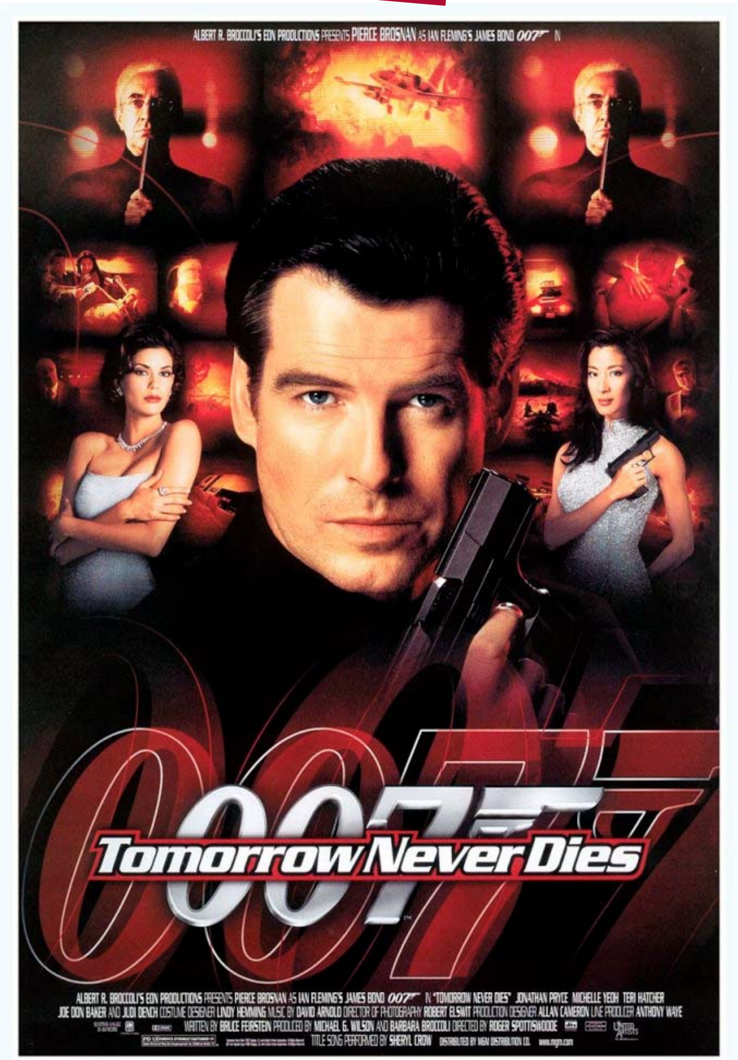
- ▶ Links are a commodity
- ▶ Websites with high PR are valuable
- ▶ There is a secondary market for expired domains (and PR value is a major component of the price)
- ▶ Introducing hidden links and hijacking expired domains with high PR makes commercial sense:
  - resell to SEO companies
  - use for index hijacking

DNS poisoning (pharming)

- ▶ Two kinds of DNS poisoning:
  - Incorrect authoritative data
  - Incorrect temporary cache
- ▶ Sources:
  - Exploits in DNS protocol
  - Hacking into a DNS server
  - DNS cache poisoning
  - Social engineering (“domain hijacking”)
- ▶ Invalid local DNS (HOSTS file)
- ▶ W32/P2Load worm (dropped HOSTS that redirects www.google.com to a similarly-looking Website)

Tomorrow Never Dies

~~Tomorrow Never Lies~~


ALBERT R. BROCCOLI'S EON PRODUCTIONS PRESENTS PIERCE BROSNAN AS IAN FLEMING'S JAMES BOND 007 IN
007
Tomorrow Never Dies

Exploiting users' mistakes

- Typos when typing the URL are common
  - common misspellings ("webadress")
  - typos ("wwebaddress")
  - different representation ("web-address")
- Attempts to resell misspelled domains:

  "www.simantek.com" and

  "www.mikrosoft.com (funny)
- Attempts to share success of known brand names:

  "www.macafee.com", "www.mcafeee.com", "www.mcafe.com", "www.mkafee.com" (same as "www.mycrosoft.com"!), "www.symantek.com".
- Malicious "typosquatting"

Typosquatting

“www.whitehouse.org”	satirical
“www.whitehouse.com”	porn
“www.wilipedia.org”	adware
“www.wiipedia.org”	adware
“www.eikipedia.org”	adware
”www.googkle.com”	adware+malware

Exploit-MhtRedir.gen, VBS/Psyme, Downloader-GS, Spabot, Spabot.dll, Downloader-XB, StartPage-GT, PWS-Banker, Proxy-TSOH.dll, Downloader-UV, Generic BackDoor.u, BackDoor-AWV, BackDoor-AML, Adware-NSearch, Adware- IEToolBar.dr, Adware- NSearch.

Conclusions

- Internet-based malware distribution is better funded then Emailing and spamming
- Fate of Email is awaiting the Internet
- Malware distribution via Websites is fairly common and it is quickly getting worse
- Hardening browsers
- Browser-based “anti-spam” products
- Whitelists of Websites in browsers

Conclusions

- Internet-based malware distribution is better funded then Emailing and spamming
- Fate of Email is awaiting the Internet
- Malware distribution via Websites is fairly common and it is quickly getting worse
- Hardening browsers
- Browser-based “anti-spam” products
- Whitelists of Websites in browsers

Enter his Web of sin… But don’t go in!!!

QUESTIONS COMMENTS
FEEDBACK QUESTIONS
COMMENTS FEEDBACK QUESTIONS
FEEDBACK QUESTIONS
COMMENTS

Q and A