Ofer Shezaf
Xiom.Com, May 2009

Web Automation: Friend Or Foe?

Xiom: the WAF experts

- Focus on real time web application security solutions.
- Free & unbiased expert information about web application firewalls and related technologies.
- Help in making WAFs deliver:
  - Selecting the correct WAF solution for you.
  - Optimizing your WAF implementation.
  - Write rules to ensure effective security.
  - Analyze alerts to understand risk and vulnerabilities of your web application.
  - Implementing ModSecurity based solutions.

www.xiom.com

modsecurity
Open Source Web Application Firewall

Ofer Shezaf

- Background:
  - Design of Web Application Firewalls, at Breach Security.
  - Security research for the Israeli Government.
- Open Source and Community projects:
  - Officer, The Web Application Security Consortium.
  - Leader, OWASP Israeli chapter
  - Project Lead WAFEC, The Web Application Firewall Evaluation Criteria.
  - Project Lead, WHID, The Web Hacking Incident Database.
- Based out of Tel-Aviv, Israel.

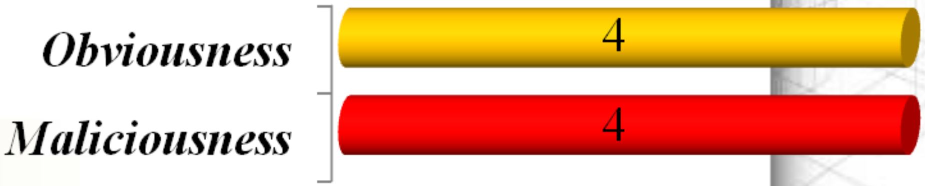
Agenda

- Web Automation:
  - Malicious Attacks
  - Valid Use
  - The In Between
- Solutions:
  - Naïve Solutions
  - Market Economy Solutions
  - Detection

MALICIOUS AUTOMATION ATTACKS

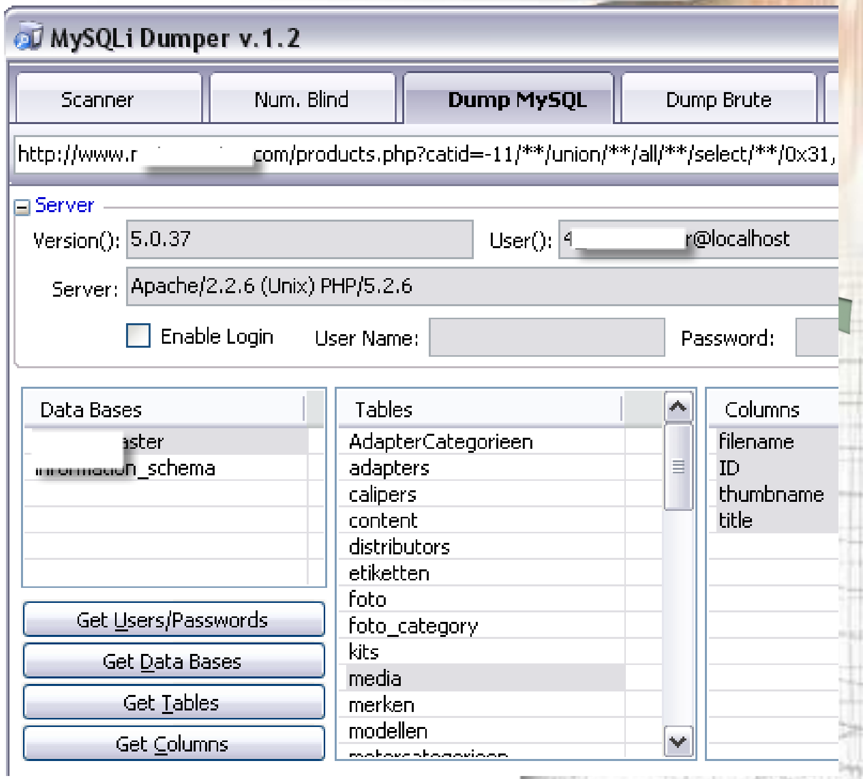
Reconnaissance

- When used maliciously, usually a scan for a single vulnerability across multiples pages.
- Sometimes several vulnerabilities checked together.
- Many times carries out from bot nets.



Blind SQL Injection

Requires a larger number of requests and therefore usually performed by an automated software



MySQLi Dumper v.1.2

http://www.r[redacted]com/products.php?catid=-11/**/union/**/all/**/select/**/0x31,

Server

Version(): 5.0.37

User(): 4[redacted]r@localhost

Server: Apache/2.2.6 (Unix) PHP/5.2.6

□ Enable Login User Name: Password:

Data Bases

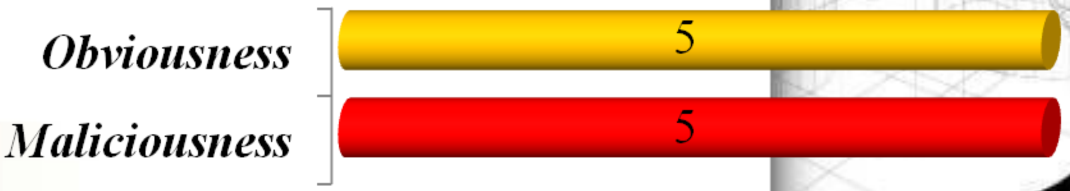
[redacted]ster
[redacted]n_schema

Tables

AdapterCategorieen
adapters
calipers
content
distributors
etiketten
foto
foto_category
kits
media
merken
modellen

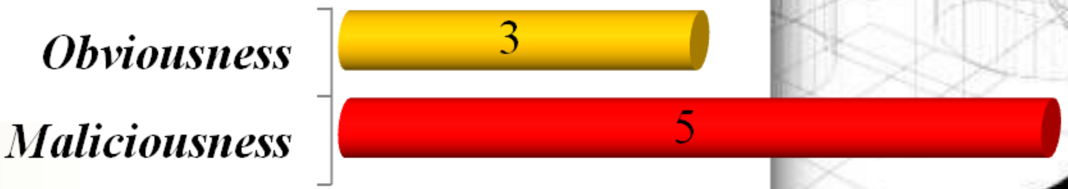
Columns

filename
ID
thumbname
title



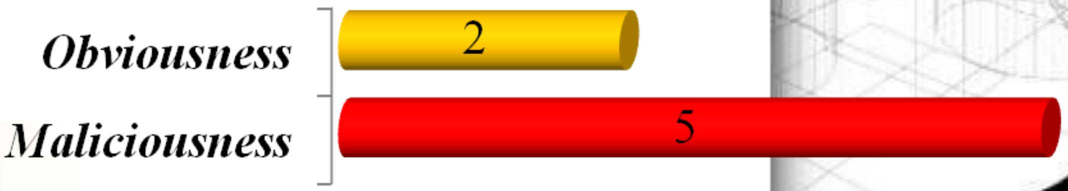
Brute Force

- Determine an unknown value by using an automated process to try a large number of possible values.
- Can be used for:
  - Cracking login credentials
  - Guessing session identifiers
  - Guessing file and directory names (often called “Forceful Browsing”)
  - Credit card information such as CVV and expiration date.
- Process based solutions:
  - Two factor authentication



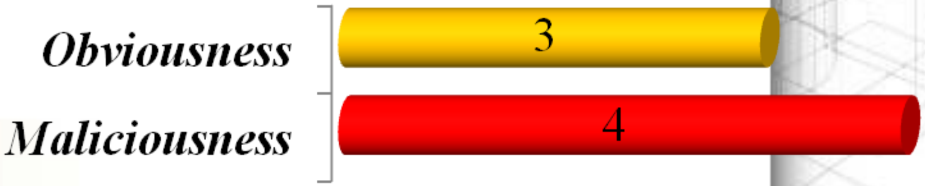
Denial of Service

- In the context of automated web attacks implies:
  - Application layer DoS
  - Caused by large number of requests rather than a resource intensive function.
- Less obvious when distributed.

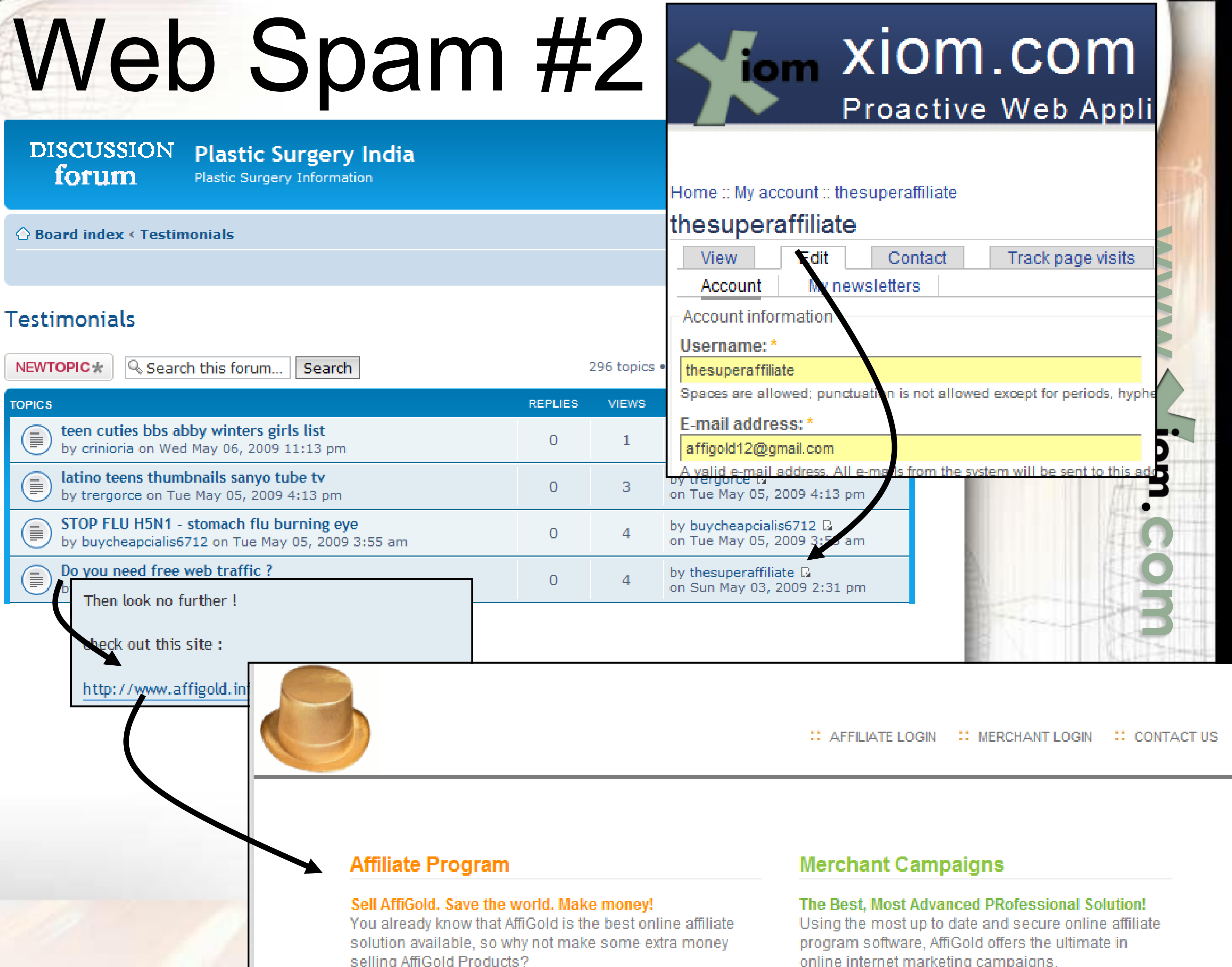


Web Spam

- Abuse public web pages to post links in order to elevate site’s ranking in search results
- Examples are:
  - Blog comment spam
  - Wiki spam.
  - Referrer log spam
- Process based solutions:
  - Moderation,
  - Allow comments only to registered users.



Web Spam #2



DISCUSSION forum

Plastic Surgery India

Plastic Surgery Information

Board index ‹ Testimonials

Testimonials

NEWTOPIC ✱ | Search this forum... | Search | 296 topics •

TOPICS	REPLIES	VIEWS	
teen cuties bbs abby winters girls list by crinioria on Wed May 06, 2009 11:13 pm	0	1	
latino teens thumbnails sanyo tube tv by trergorce on Tue May 05, 2009 4:13 pm	0	3	by trergorce on Tue May 05, 2009 4:13 pm
STOP FLU H5N1 - stomach flu burning eye by buycheapcialis6712 on Tue May 05, 2009 3:55 am	0	4	by buycheapcialis6712 on Tue May 05, 2009 3:55 am
Do you need free web traffic ?	0	4	by thesuperaffiliate on Sun May 03, 2009 2:31 pm

Then look no further !

check out this site :

http://www.affigold.in

xiom.com

Proactive Web Appli

Home :: My account :: thesuperaffiliate

thesuperaffiliate

View | Edit | Contact | Track page visits

Account | My newsletters

Account information

Username: *

thesuperaffiliate

Spaces are allowed; punctuation is not allowed except for periods, hyphe

E-mail address: *

affigold12@gmail.com

A valid e-mail address. All e-mails from the system will be sent to this add

www.xiom.com

:: AFFILIATE LOGIN :: MERCHANT LOGIN :: CONTACT US

Affiliate Program

Sell AffiGold. Save the world. Make money!

You already know that AffiGold is the best online affiliate solution available, so why not make some extra money selling AffiGold Products?

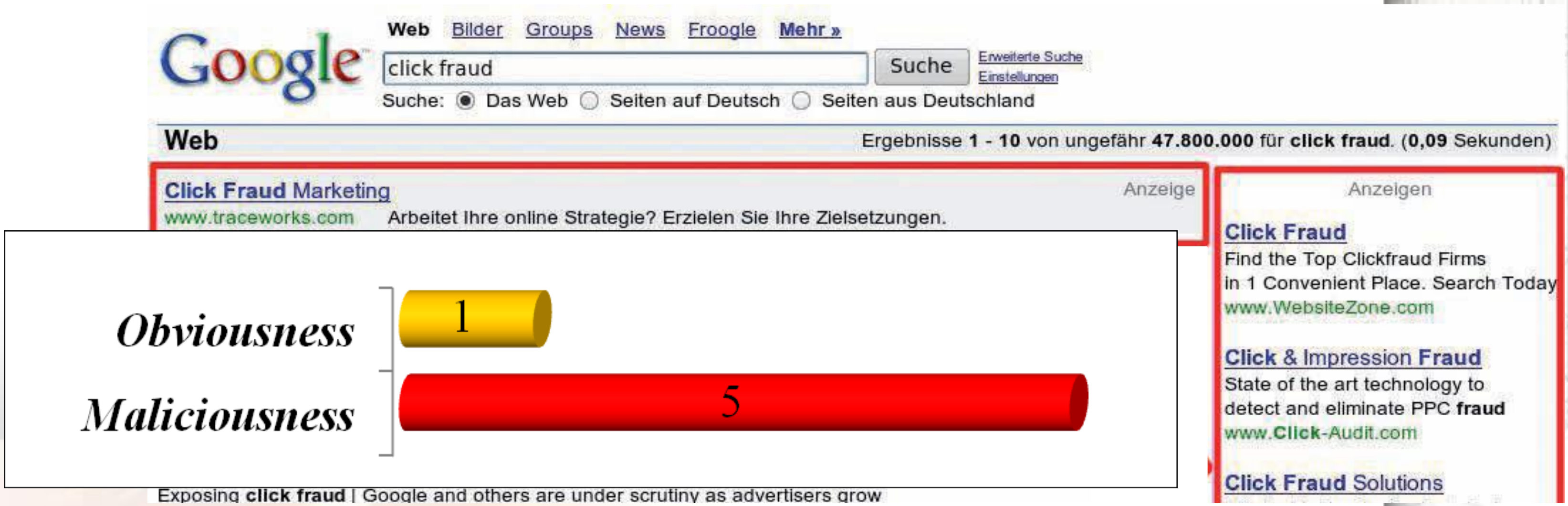
Merchant Campaigns

The Best, Most Advanced PRofessional Solution!

Using the most up to date and secure online affiliate program software, AffiGold offers the ultimate in online internet marketing campaigns.

Click Fraud

- Abuse pay per click advertising by generating automated clicks.
- Performed by owners of web sites displaying ads, competitors and vandals.
- Referrer click fraud/CSRF click fraud.
- Process solutions:
  - Cost Per Action (CPA),
  - Pay Per Impression (PPI)



click fraud

Suche: ● Das Web ○ Seiten auf Deutsch ○ Seiten aus Deutschland

Web Ergebnisse **1** - **10** von ungefähr **47.800.000** für **click fraud**. (**0,09** Sekunden)

Click Fraud Marketing Anzeige
www.traceworks.com Arbeitet Ihre online Strategie? Erzielen Sie Ihre Zielsetzungen.

Exposing **click fraud** | Google and others are under scrutiny as advertisers grow

Anzeigen

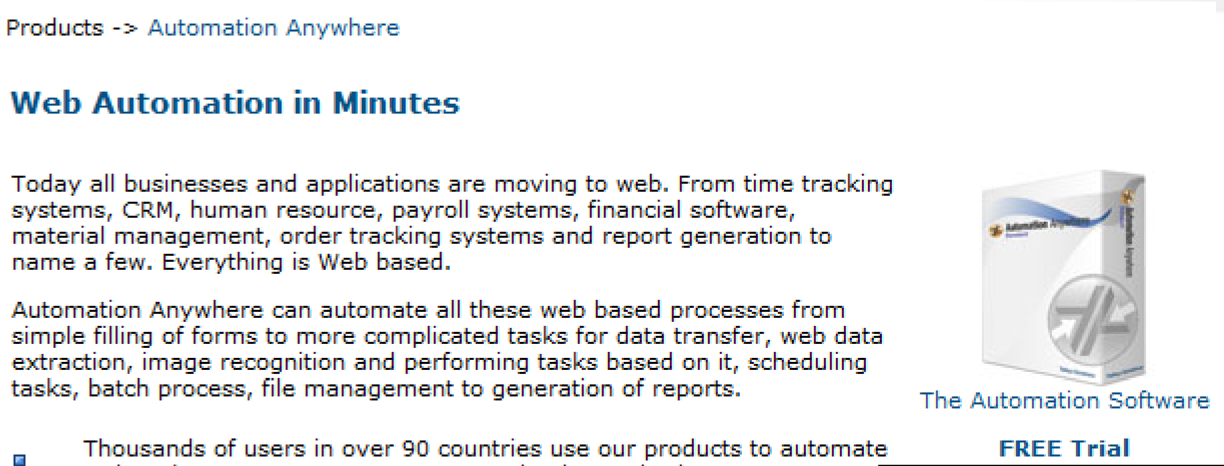
Click Fraud
Find the Top Clickfraud Firms in 1 Convenient Place. Search Today
www.WebsiteZone.com

Click & Impression Fraud
State of the art technology to detect and eliminate PPC **fraud**
www.**Click**-Audit.com

Click Fraud Solutions

Accepted Automation

Automation Usage



Products -> Automation Anywhere

Web Automation in Minutes

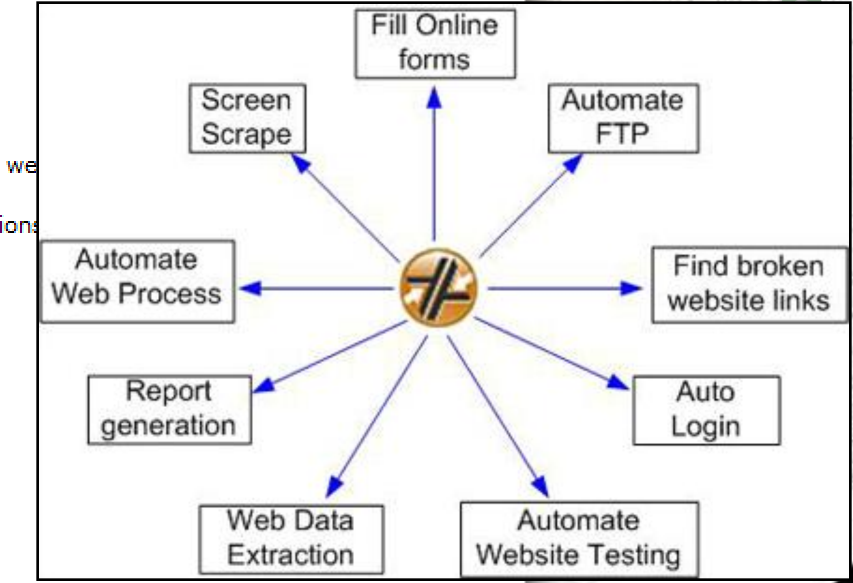
Today all businesses and applications are moving to web. From time tracking systems, CRM, human resource, payroll systems, financial software, material management, order tracking systems and report generation to name a few. Everything is Web based.

Automation Anywhere can automate all these web based processes from simple filling of forms to more complicated tasks for data transfer, web data extraction, image recognition and performing tasks based on it, scheduling tasks, batch process, file management to generation of reports.

The Automation Software

FREE Trial

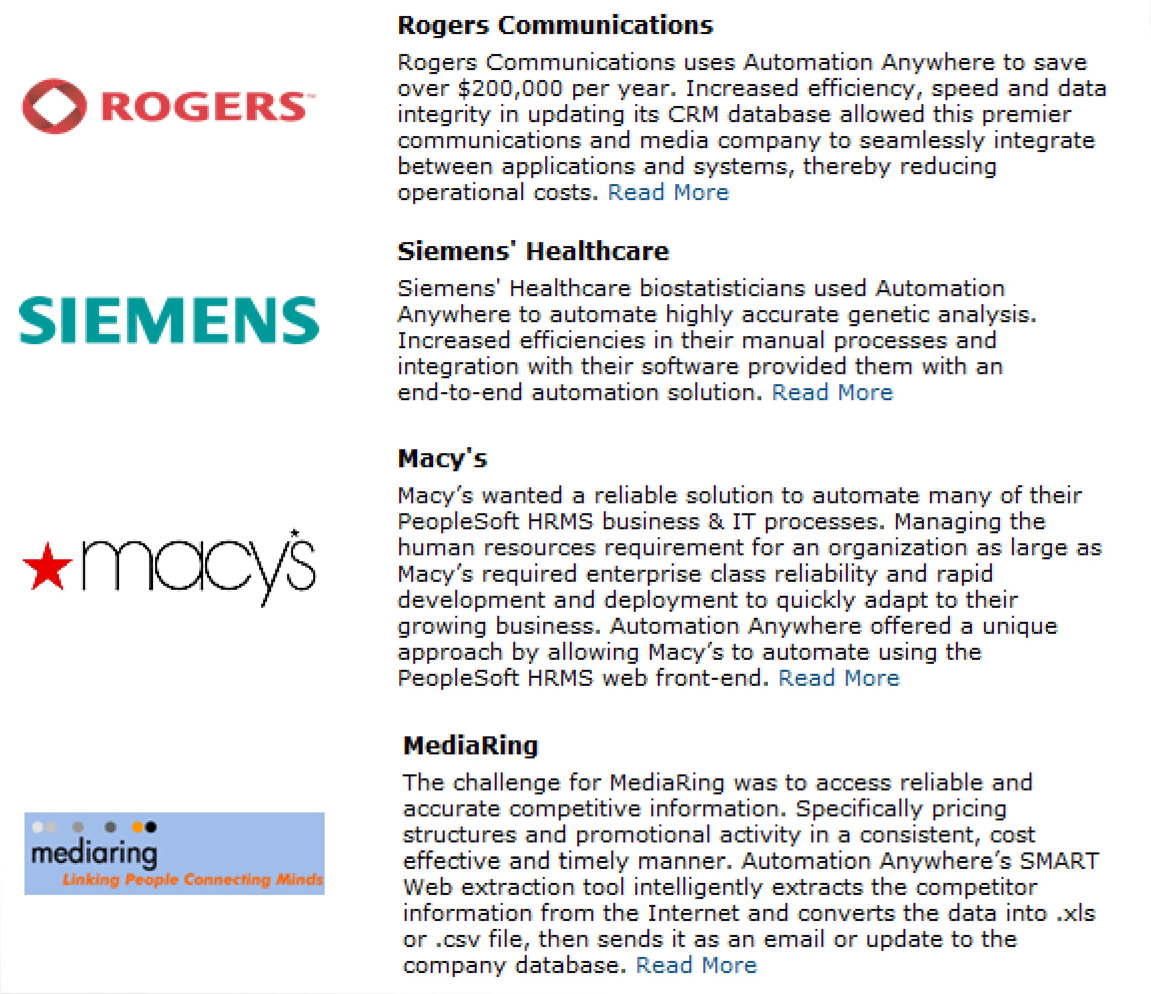
- Thousands of users in over 90 countries use our products to automate web tasks. Easy to use. No programming is required.
- Automation Anywhere works with any website, even complicated websites that use java, javascript, AJAX, Flash and iFrames.
- Agent less Remote Deployment allows the web task to run over various machines on the network.
- Our advanced Web Recorder understands all web controls making we tasks run accurately even if websites change.
- Our SMART Automation Technology offers over 180+ powerful actions for web automation.



Automation is Called:

- EAI (Enterprise Application Integration)
- ETL (extract, load, transform)
- Web Services
- Screen Scraping
- Web 2.0

Automation Case Studies



Rogers Communications

Rogers Communications uses Automation Anywhere to save over $200,000 per year. Increased efficiency, speed and data integrity in updating its CRM database allowed this premier communications and media company to seamlessly integrate between applications and systems, thereby reducing operational costs. Read More

Siemens' Healthcare

Siemens' Healthcare biostatisticians used Automation Anywhere to automate highly accurate genetic analysis. Increased efficiencies in their manual processes and integration with their software provided them with an end-to-end automation solution. Read More

Macy's

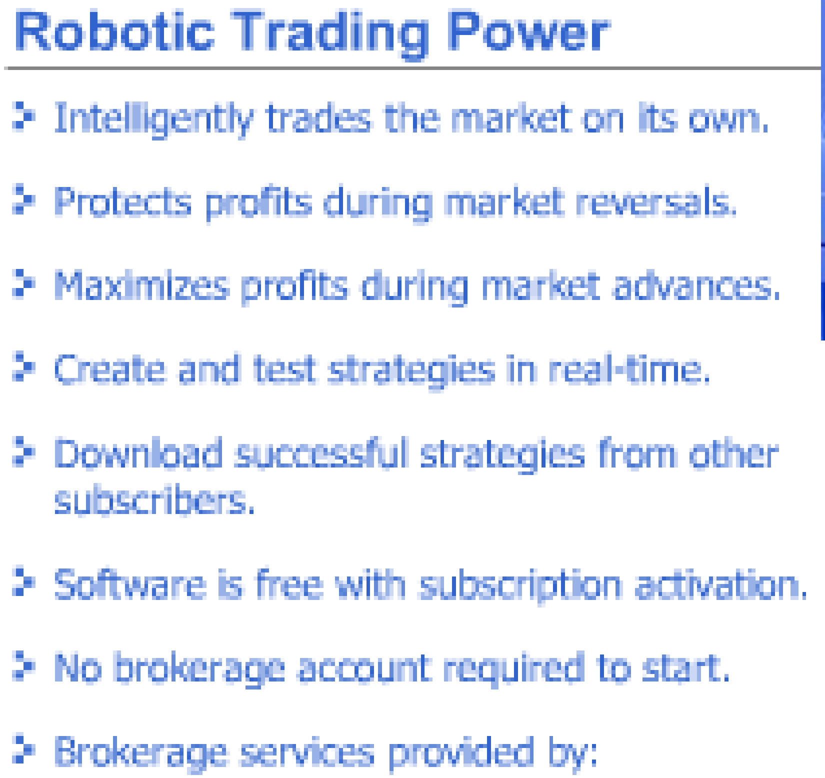
Macy's wanted a reliable solution to automate many of their PeopleSoft HRMS business & IT processes. Managing the human resources requirement for an organization as large as Macy's required enterprise class reliability and rapid development and deployment to quickly adapt to their growing business. Automation Anywhere offered a unique approach by allowing Macy's to automate using the PeopleSoft HRMS web front-end. Read More

MediaRing

The challenge for MediaRing was to access reliable and accurate competitive information. Specifically pricing structures and promotional activity in a consistent, cost effective and timely manner. Automation Anywhere's SMART Web extraction tool intelligently extracts the competitor information from the Internet and converts the data into .xls or .csv file, then sends it as an email or update to the company database. Read More

????

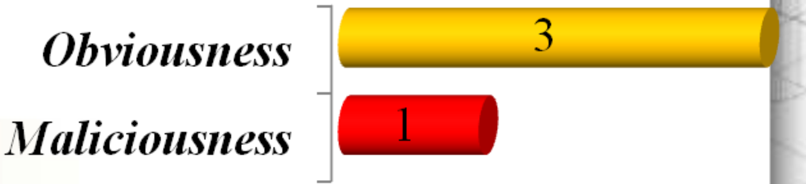
Automated Stock Trading



Robotic Trading Power

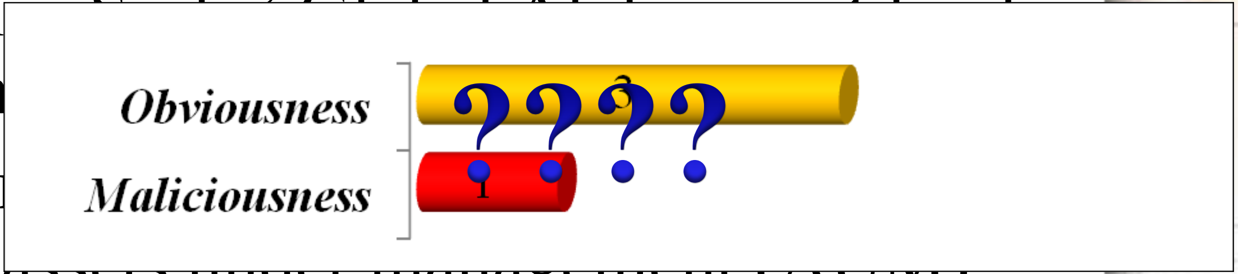
- Intelligently trades the market on its own.
- Protects profits during market reversals.
- Maximizes profits during market advances.
- Create and test strategies in real-time.
- Download successful strategies from other subscribers.
- Software is free with subscription activation.
- No brokerage account required to start.
- Brokerage services provided by:

Take Your Trading to the Next Level
CoolTrade Automated Trading
Shares
Trades
Total Profit
200
136
$16,362.00



Automated Stock Trading #2

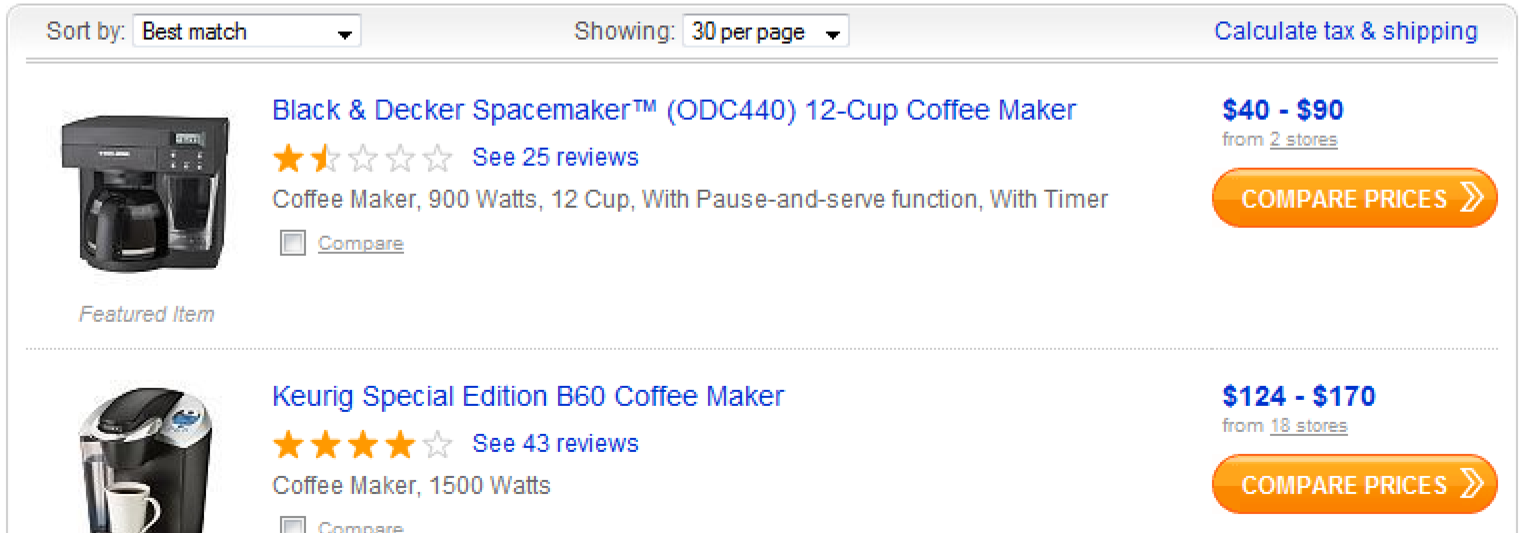
- A quant fund is a hedge fund that relies on complex and sophisticated mathematical algorithms. In other words, a bot.
- Goldm
  made a
- Aite Gr
  global assets under management (AUM) was driven by quant at the end of 2007, representing $6.65 trillion.
- Quant funds are often blamed for the current financial crisis.



http://www.washingtonpost.com/wp-dyn/content/article/2007/08/20/AR2007082001846.html?wpisrc=newsletter

Comparative Shopping

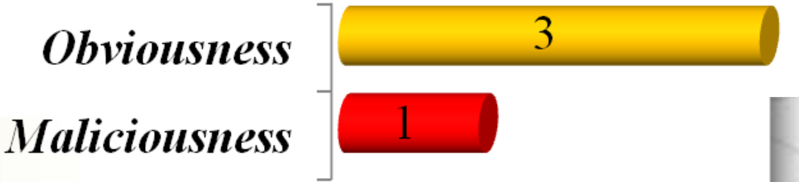
Historically hostile, but today part of the e-commerce marketing chain.



Sort by: Best match | Showing: 30 per page | Calculate tax & shipping

Black & Decker Spacemaker™ (ODC440) 12-Cup Coffee Maker
★★☆☆☆ See 25 reviews
Coffee Maker, 900 Watts, 12 Cup, With Pause-and-serve function, With Timer
□ Compare
Featured Item
$40 - $90
from 2 stores
COMPARE PRICES »

Keurig Special Edition B60 Coffee Maker
★★★★☆ See 43 reviews
Coffee Maker, 1500 Watts
□ Compare
Featured Item
$124 - $170
from 18 stores
COMPARE PRICES »



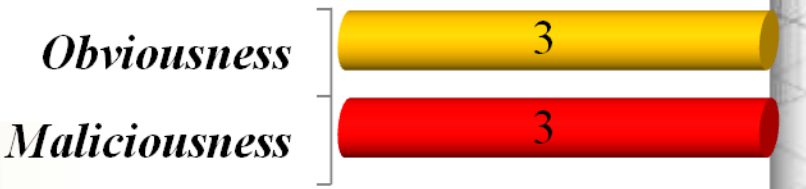
And all the Rest

- Search engines
  - Alerting tools
- Testing:
  - Link checking
  - Monitoring
  - Security assessment
- IP infringement bots
- Intermidiators:
  - Translation,
  - aggregation

Borderline Automation Usage

Queue Jumping

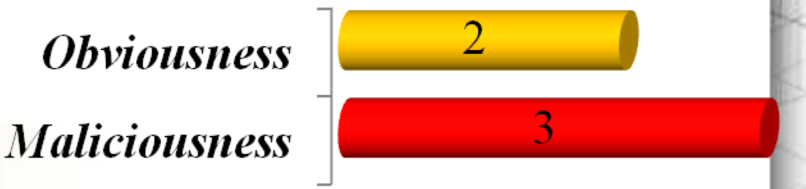
- Ticketmaster confessed to “fighting like the dickens“ queue jumping.
- Travel agents known to automate air line ticketing systems.
- Scalping is legal in some territories and illegal in others.
- Timing sales of perishable goods is an issues regardless of automation.
- Process based solution:
  - Credit card maximums.



Auctions Sniping

Watching a timed online auction and placing a winning bid at the last possible moment giving the other bidders no time to outbid the sniper.

“Bid Sniper” is bot that performs auction sniping.

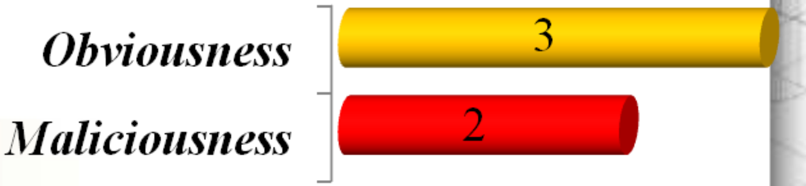


Auction Sniping #2

- In most auction sites sniping is legal. Some do not allow it.
- Usually viewed by sellers and other buyers as negative.
- Process based solutions:
  - Random termination time
  - Automatic extension after last bid

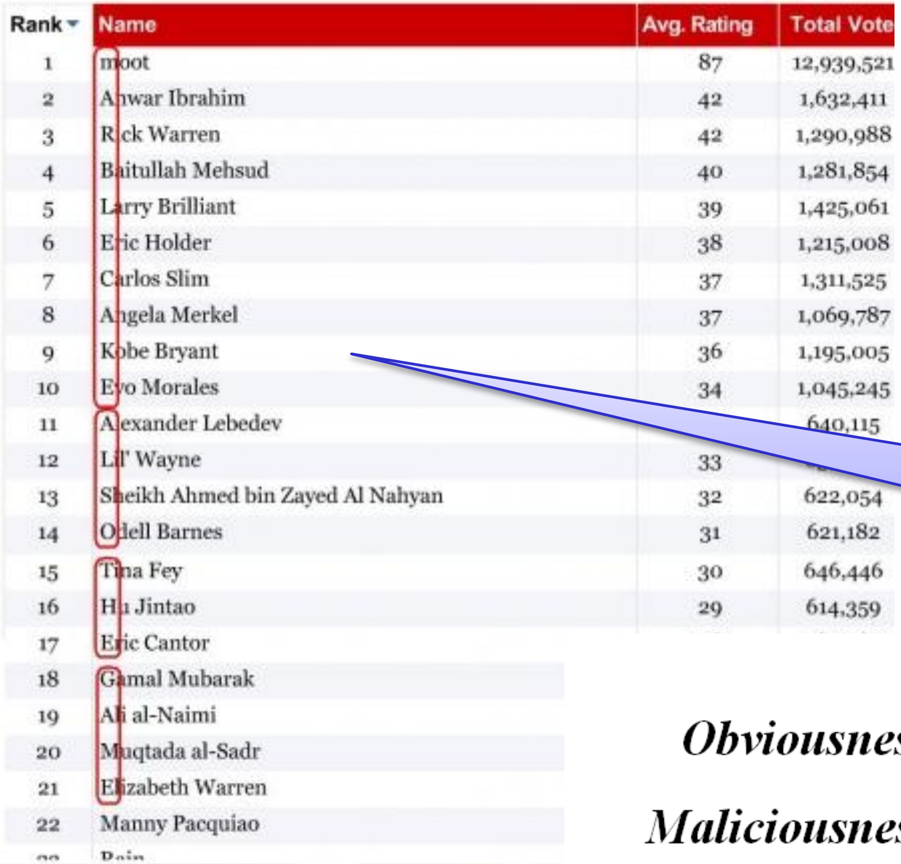
Gaming Bots

- MUD, Virtual Worlds & Second Life bots:
  - Gain Wealth, and turn it into money in Second Life.
- Poker Bots:
  - Share information between several bots at one table.
  - Monitor tables to choose the weak once.
  - Play well.

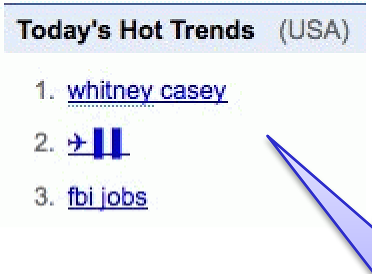


Poll Skewing

Picture is worth a thousand words



Rank	Name	Avg. Rating	Total Vote
1	moot	87	12,939,521
2	Anwar Ibrahim	42	1,632,411
3	Rick Warren	42	1,290,988
4	Baitullah Mehsud	40	1,281,854
5	Larry Brilliant	39	1,425,061
6	Eric Holder	38	1,215,008
7	Carlos Slim	37	1,311,525
8	Angela Merkel	37	1,069,787
9	Kobe Bryant	36	1,195,005
10	Evo Morales	34	1,045,245
11	Alexander Lebedev	[illegible]	640,115
12	Lil' Wayne	33	[illegible]
13	Sheikh Ahmed bin Zayed Al Nahyan	32	622,054
14	Odell Barnes	31	621,182
15	Tina Fey	30	646,446
16	Hu Jintao	29	614,359
17	Eric Cantor		
18	Gamal Mubarak		
19	Ali al-Naimi		
20	Muqtada al-Sadr		
21	Elizabeth Warren		
22	Manny Pacquiao		
23	Rain		

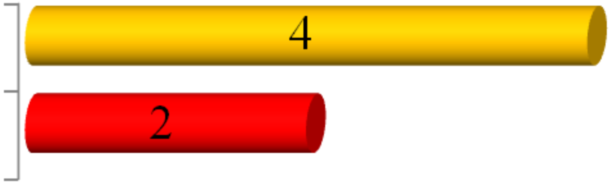


Today's Hot Trends (USA)

1. whitney casey
2. →▌▌
3. fbi jobs

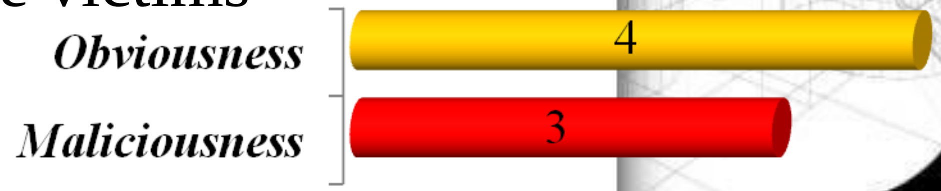
Google Trends

Time Most Influential People Poll



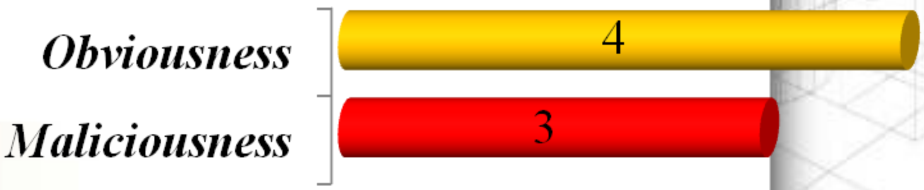
Information Harvesting and Mirroring

- Harvests:
  - E-mail and personal information
  - Competitive information
  - Record oriented information such as CVs
  - Entire Web sites for creating a mirror
- Executed from:
  - Local computer
  - Distributed, potentially using bot net
  - Trojans, exploiting the victims credentials at the site.



Information Harvesting and Mirroring #2

- Legal status varies
  - E-mail harvesting illegal in many territories due to spam legislation.
- Process based solutions:
  - Randomizing the information while keeping the visible output clear



Automation Summary

- Automation can be valid, malicious or somewhere in between.
- Malicious automation abuse either volume or timing.
- In many cases changing the process can solve the issue, albeit reduce usability.

SOLUTIONS

Naïve Solutions

Negative Security

- Generic attack signatures:
  - Blind SQL injection,
  - Comment Spam
- Black listing:
  - IP Addresses (IP Reputation)
  - Keywords
  - User Agents
  - Missing host header
- Naïve, but eliminates the masses

Confuse the Bot

- Return the wrong meta data including status code & mime type.
- Obfuscate the information
- Detect a browser by including code that a browser would execute such as references resources.
- Still naïve, but still eliminates the masses

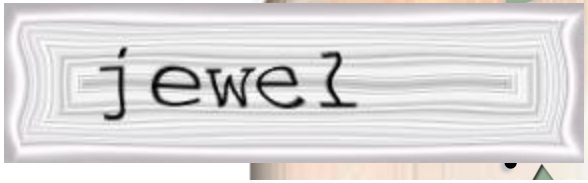
Market Economy Solutions

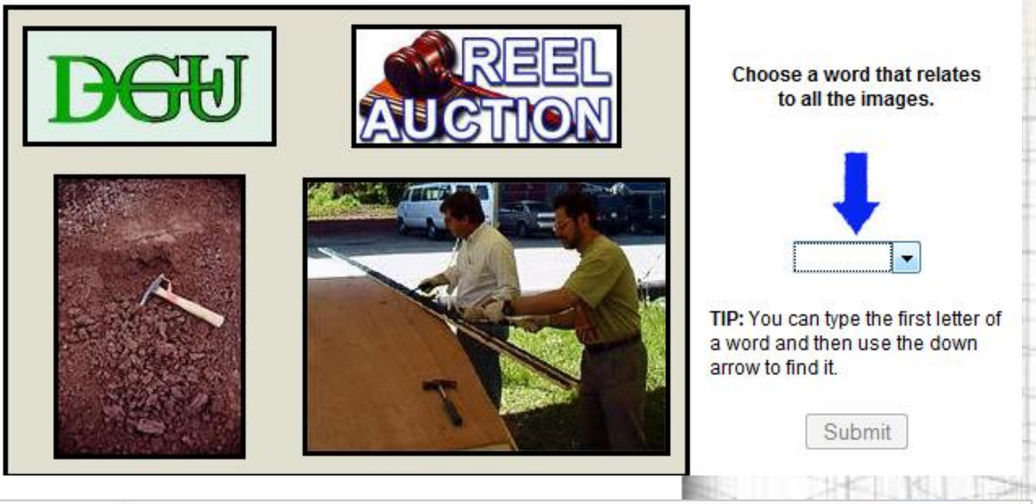
Require Site Flow

- Follow:
  - HTTP referer header
  - Nonce:
    - A one time token for each request.
    - Similar to referer but does not rely on HTTP behavior.
- Flow can be configured, learned or built into a framework.
- Only raises the price of automation

Challenge/Response

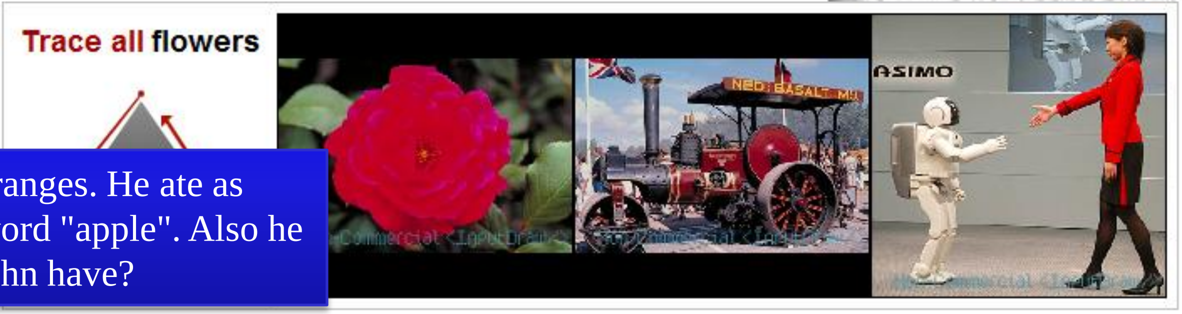
- Provide a Turing test that only a human can solve.
- Usually called CAPTCHA
- Not necessarily an OCR challenge





Choose a word that relates to all the images.

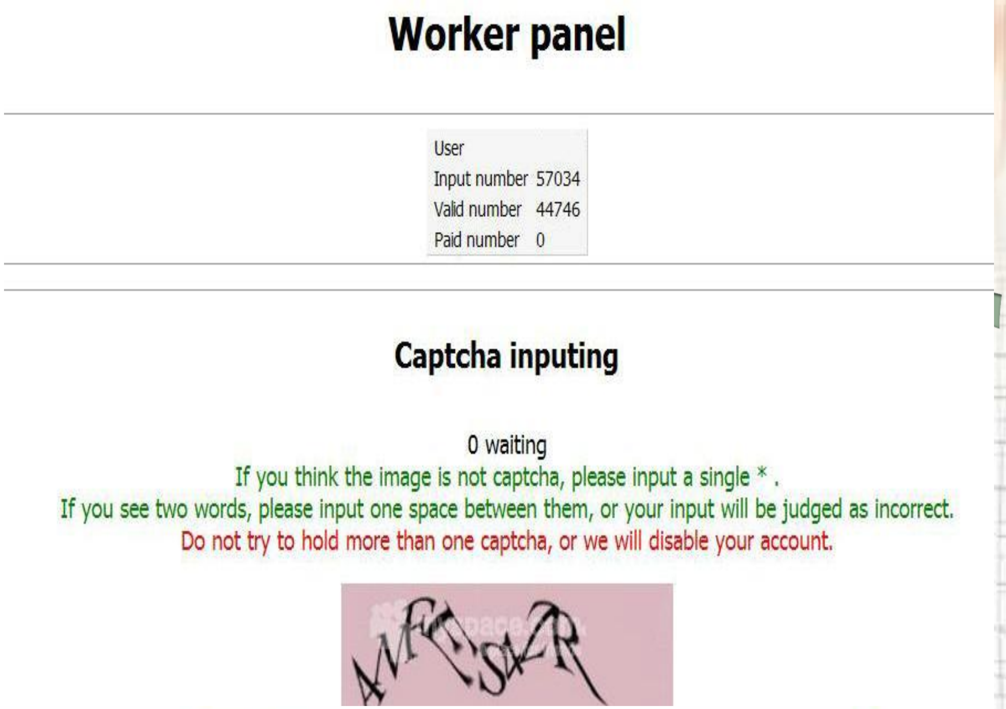
TIP: You can type the first letter of a word and then use the down arrow to find it.



John had one thousand apples and five oranges. He ate as many of his apples as there is letters in word "apple". Also he ate two bananas :-). How many apples John have?

Slow Down the Bot

- Server side throttling
- Client side computational challenge:
  - Reverse hashing
  - CAPTCHA – nearly universally breakable at a cost, automatically or manually.



Worker panel

User	
Input number	57034
Valid number	44746
Paid number	0

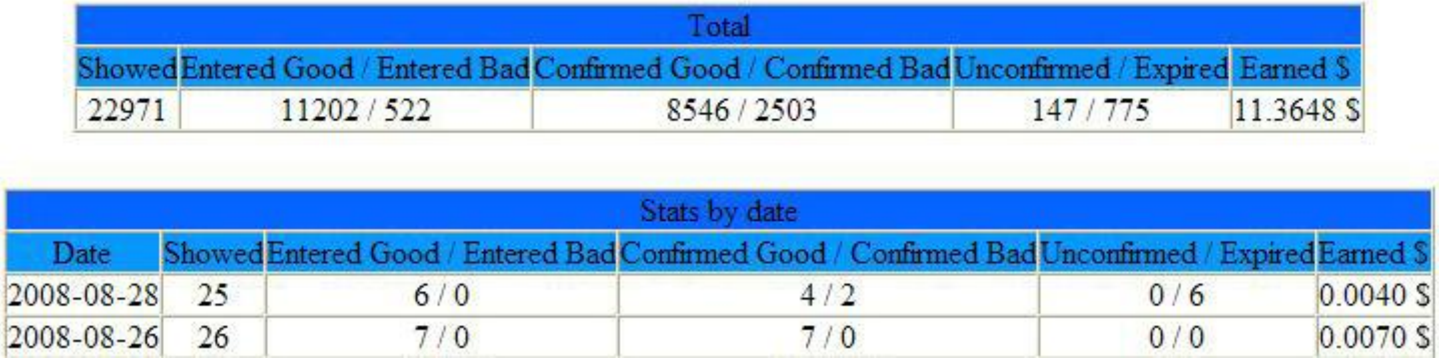
Captcha inputing

0 waiting

If you think the image is not captcha, please input a single * .

If you see two words, please input one space between them, or your input will be judged as incorrect.

Do not try to hold more than one captcha, or we will disable your account.



Total					
Showed	Entered Good / Entered Bad	Confirmed Good / Confirmed Bad	Unconfirmed / Expired	Earned $
22971	11202 / 522	8546 / 2503	147 / 775	11.3648 $

Stats by date						
Date	Showed	Entered Good / Entered Bad	Confirmed Good / Confirmed Bad	Unconfirmed / Expired	Earned $
2008-08-28	25	6 / 0	4 / 2	0 / 6	0.0040 $
2008-08-26	26	7 / 0	7 / 0	0 / 0	0.0070 $

AUTOMATION DETECTION

Rate Based Detection

- Count accesses from the same source and block excessive access
- Hard to define:
  - Source: IP, Session, User?
  - Excessive access

Rate Detection: Source

- Non authenticated requests need to be counted by source IP which presents challenges:
  - Proxies
  - Distributed attacks
- Authenticated requests can be counted per user:
  - Must protect the registration function

Rate Detection: Threshold

- Need to compensate or white list proxy sources.
- Need to take into account variation in traffic due to events or seasonality.
- Hard to configure manually and requires learning.

Duplicate and Anomaly Detection

- Assume automated request are similar and look for repeating patterns:
  - Timing
  - Source
  - Content
- Assume automated requests are different than the normal use, learn base line and detect anomalies

Response

- Blocking
- Global or directed throttling
- Challenge/response
- Alerting only

Ofer Shezaf, shezaf@xiom.com