What the Cyber Criminals are Doing on Your Website (Right Now)

Front Range OWASP Conference

March 22, 2012

Laz

Director of Strategy, Silver Tail Systems

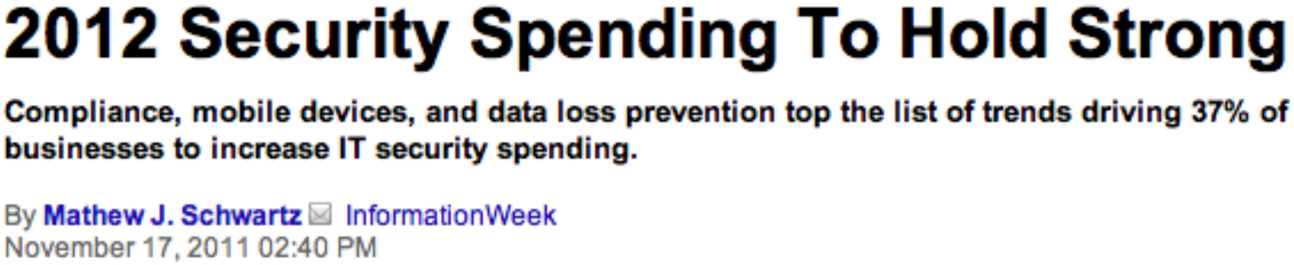
laz@silvertailsystems.com

Twitter: iamlaz

Agenda

- Introductions
- Some IT Security Trends/Statistics
- Use Cases
- Lessons Learned
- Staying Ahead
- Questions

Some IT Security Trends



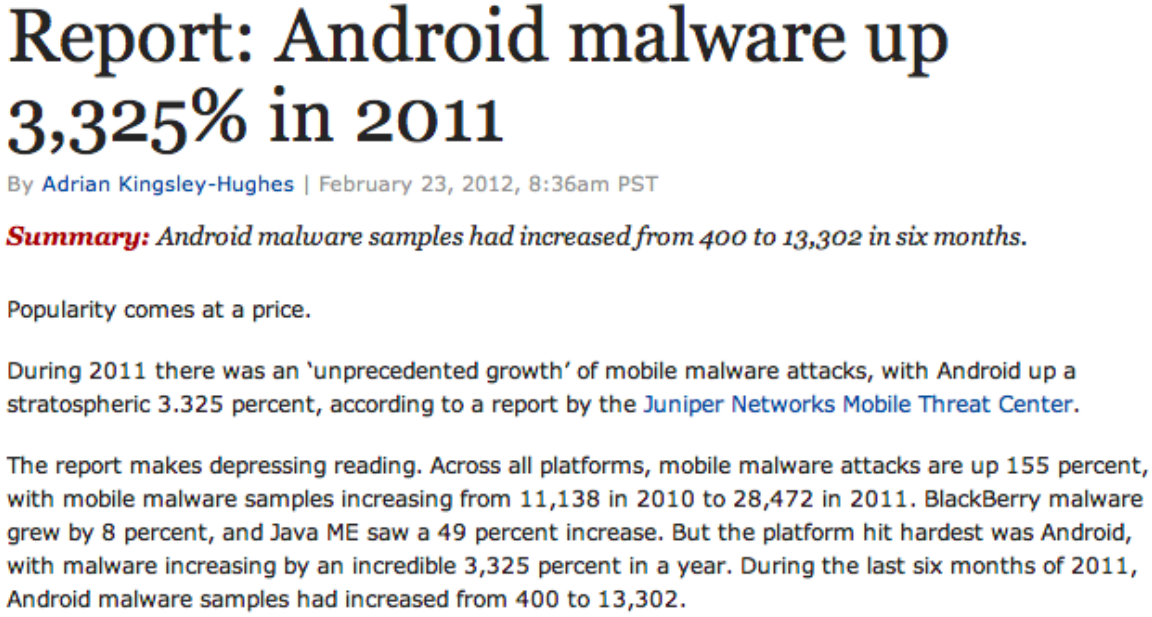
2012 Security Spending To Hold Strong

Compliance, mobile devices, and data loss prevention top the list of trends driving 37% of businesses to increase IT security spending.

By **Mathew J. Schwartz** InformationWeek
November 17, 2011 02:40 PM

For 2012, 37% of information security pr
spending, while only 16% expect their se
are to address compliance, mobile devic

Source: InformationWeek



Report: Android malware up 3,325% in 2011

By Adrian Kingsley-Hughes | February 23, 2012, 8:36am PST

Summary: *Android malware samples had increased from 400 to 13,302 in six months.*

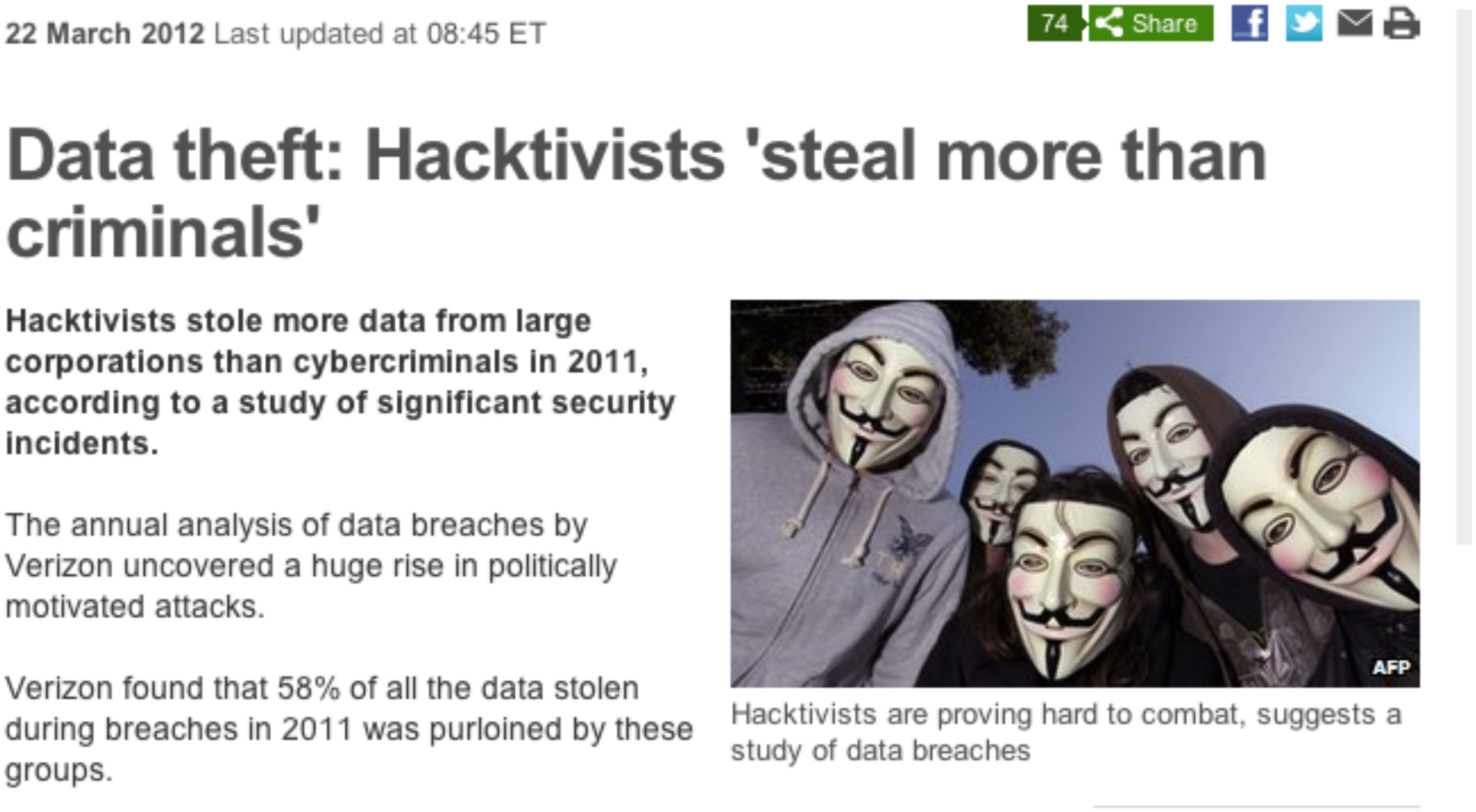
Popularity comes at a price.

During 2011 there was an 'unprecedented growth' of mobile malware attacks, with Android up a stratospheric 3.325 percent, according to a report by the Juniper Networks Mobile Threat Center.

The report makes depressing reading. Across all platforms, mobile malware attacks are up 155 percent, with mobile malware samples increasing from 11,138 in 2010 to 28,472 in 2011. BlackBerry malware grew by 8 percent, and Java ME saw a 49 percent increase. But the platform hit hardest was Android, with malware increasing by an incredible 3,325 percent in a year. During the last six months of 2011, Android malware samples had increased from 400 to 13,302.

Source: Juniper Networks Mobile Threat Center

More….



22 March 2012 Last updated at 08:45 ET

Data theft: Hacktivists 'steal more than criminals'

Hacktivists stole more data from large corporations than cybercriminals in 2011, according to a study of significant security incidents.

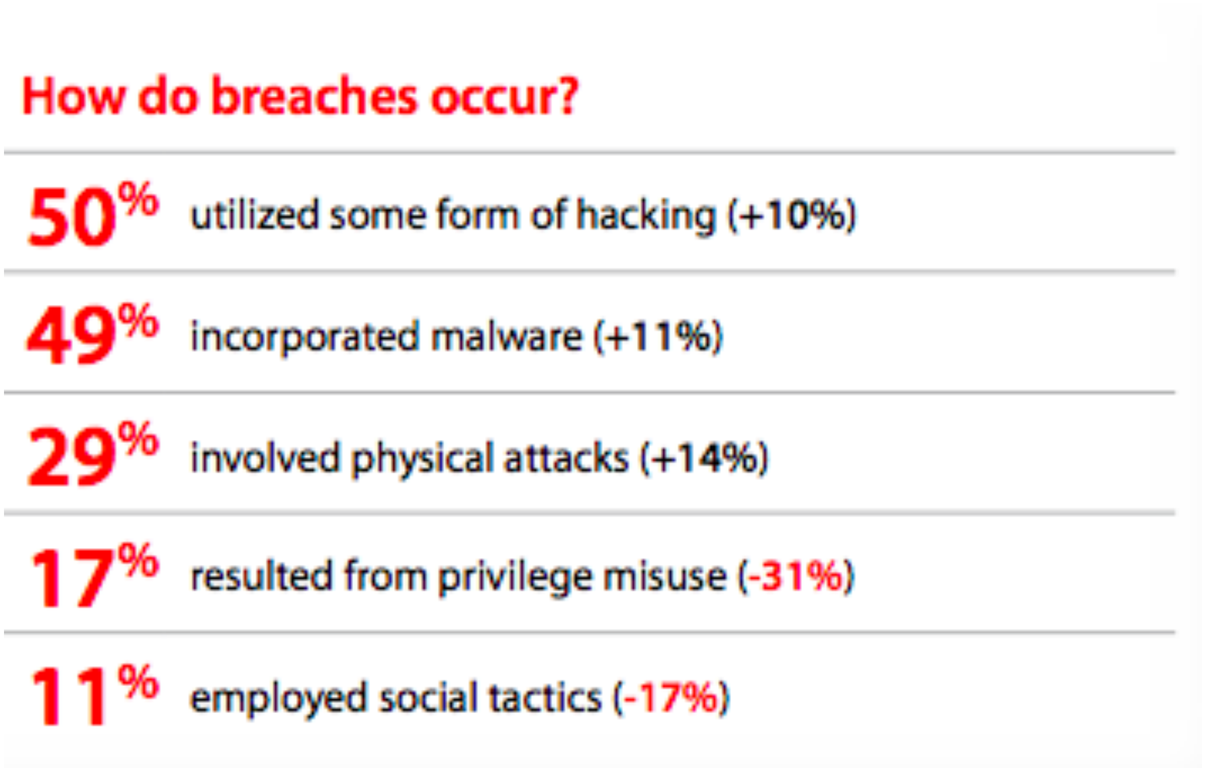
The annual analysis of data breaches by Verizon uncovered a huge rise in politically motivated attacks.

Verizon found that 58% of all the data stolen during breaches in 2011 was purloined by these groups.

Hacktivists are proving hard to combat, suggests a study of data breaches

Source: Verizon 2011 Data Breach Investigations Report and BBC

Some Statistics

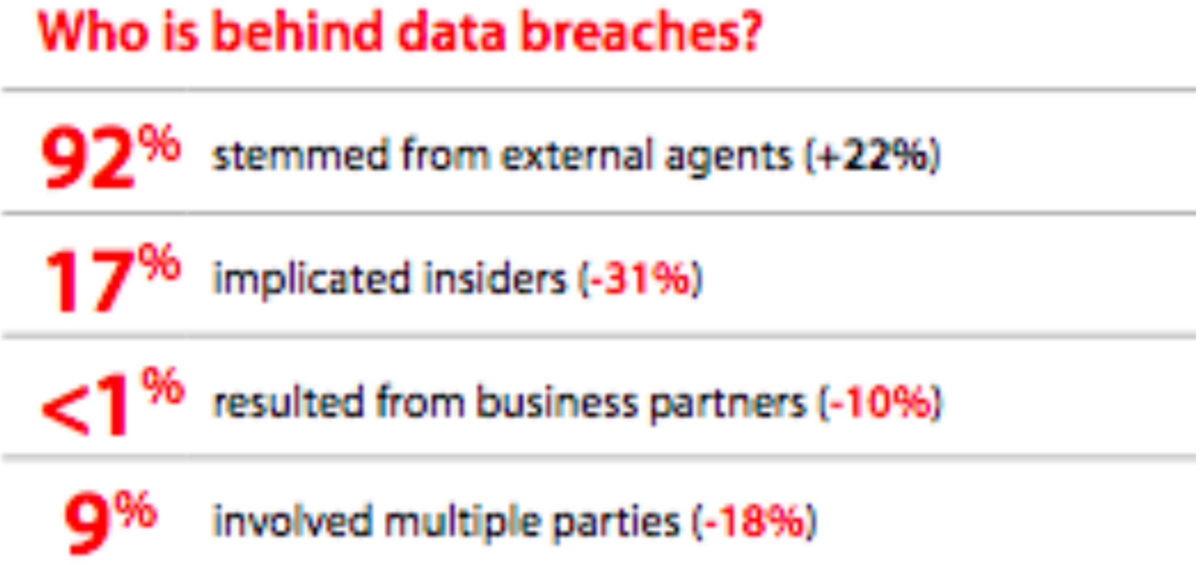


How do breaches occur?

50%	utilized some form of hacking (+10%)
49%	incorporated malware (+11%)
29%	involved physical attacks (+14%)
17%	resulted from privilege misuse (-31%)
11%	employed social tactics (-17%)

Source: Verizon 2011 Data Breach Investigations Report

Some Statistics



Who is behind data breaches?

92%	stemmed from external agents (+22%)
17%	implicated insiders (-31%)
<1%	resulted from business partners (-10%)
9%	involved multiple parties (-18%)

Source: Verizon 2011 Data Breach Investigations Report

Identifying Known Issues

- Identifying the issues through:
  - Pen testing
  - Application/Network/OS Scans
  - Internal testing
  - Monitoring/SIEM

What About Unknown Issues?

- Some indicators that things were going bad
  - Always started with a phone call
  - Site performance degrading over time, which resulted in a decline of sales due to bad performance
  - Increase in Customer Service phone calls
- Research is time consuming!
  - How can you justify pulling revenue generating resources off of projects to investigate something?

How will this type of behavior hurt the company brand?

These are Still Well Known Issues

- Man in the Middle
- Man in the Browser
- Man in the Mobile

Criminal behavior looks much different than normal behavior

Some Unknown Issues

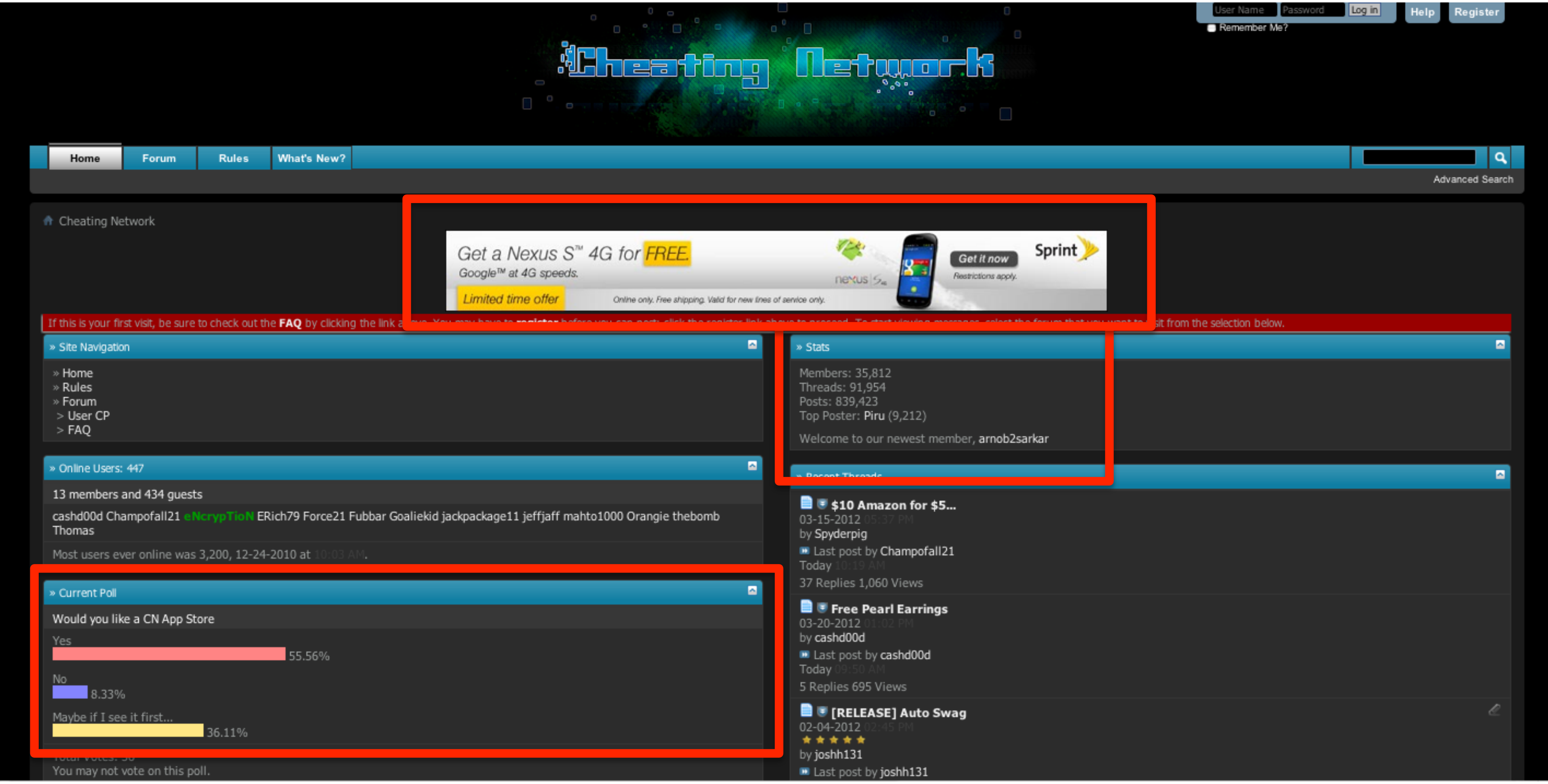
- People gaming the system to abuse marketing, sweepstakes, loyalty, and incentive programs
- Increase to fraudulent activities due to lack of visibility into the Web session – cyber criminals are getting more creative with their approach!
- Manipulating the session with Mobile devices
- Site scraping for content, pricing, or inventory/architecture probing
- DDoS (recon and actual attack) attacks

IDS/IPS/WAF and transaction-based solutions are being by-passed by cyber criminals

People Gaming the System

- Business Drivers
  - Online marketing campaigns, sweepstakes, or incentives to acquire new customers
- Challenges Identified
  - Unique registration patterns over time
  - Registrants signing up from all over the world
  - Random name generator from multiple IP addresses
- Research
  - Cheating Network
  - The Botting Network (TBN)

Cheating Network



Cheating Network

If this is your first visit, be sure to check out the **FAQ** by clicking the link above. You may have to **register** before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

» Site Navigation

- » Home
- » Rules
- » Forum
  - > User CP
  - > FAQ

» Online Users: 447

13 members and 434 guests

cashd00d Champofall21 eNcrypTioN ERich79 Force21 Fubbar Goaliekid jackpackage11 jeffjaff mahto1000 Orangie thebomb Thomas

Most users ever online was 3,200, 12-24-2010 at 10:03 AM.

» Current Poll

Would you like a CN App Store

Yes 55.56%

No 8.33%

Maybe if I see it first... 36.11%

Total Votes: 36

You may not vote on this poll.

» Stats

Members: 35,812
Threads: 91,954
Posts: 839,423
Top Poster: Piru (9,212)

Welcome to our newest member, arnob2sarkar

» Recent Threads

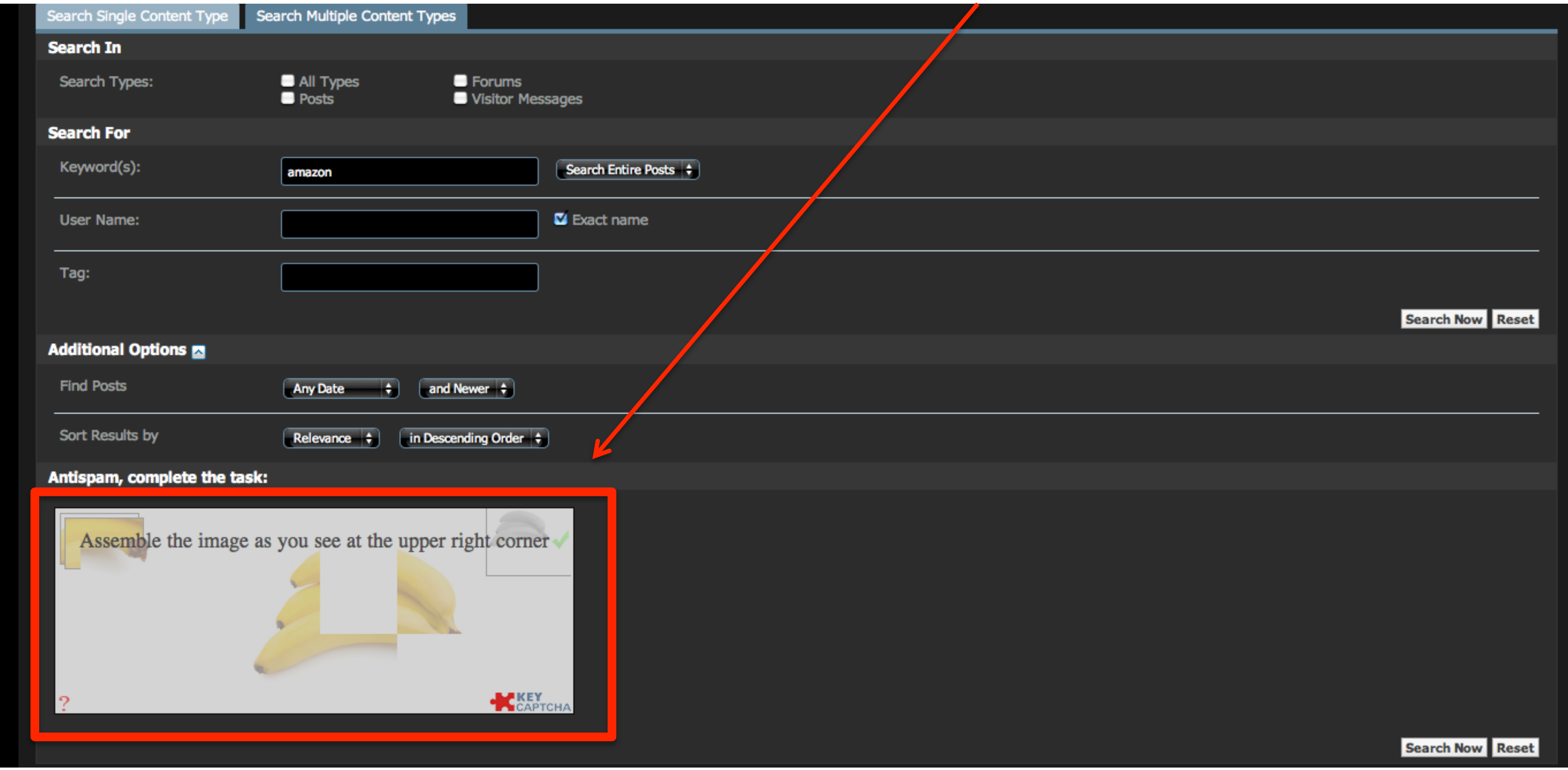
$10 Amazon for $5...
03-15-2012 05:37 PM
by Spyderpig
Last post by Champofall21
Today 10:19 AM
37 Replies 1,060 Views

Free Pearl Earrings
03-20-2012 01:02 PM
by cashd00d
Last post by cashd00d
Today 09:50 AM
5 Replies 695 Views

[RELEASE] Auto Swag
02-04-2012 02:45 PM
★★★★★
by joshh131
Last post by joshh131

Cheating Network

Captcha Built In!



Search In

Search Types: □ All Types □ Posts □ Forums □ Visitor Messages

Search For

Keyword(s): amazon — Search Entire Posts

User Name: ☑ Exact name

Tag:

Additional Options

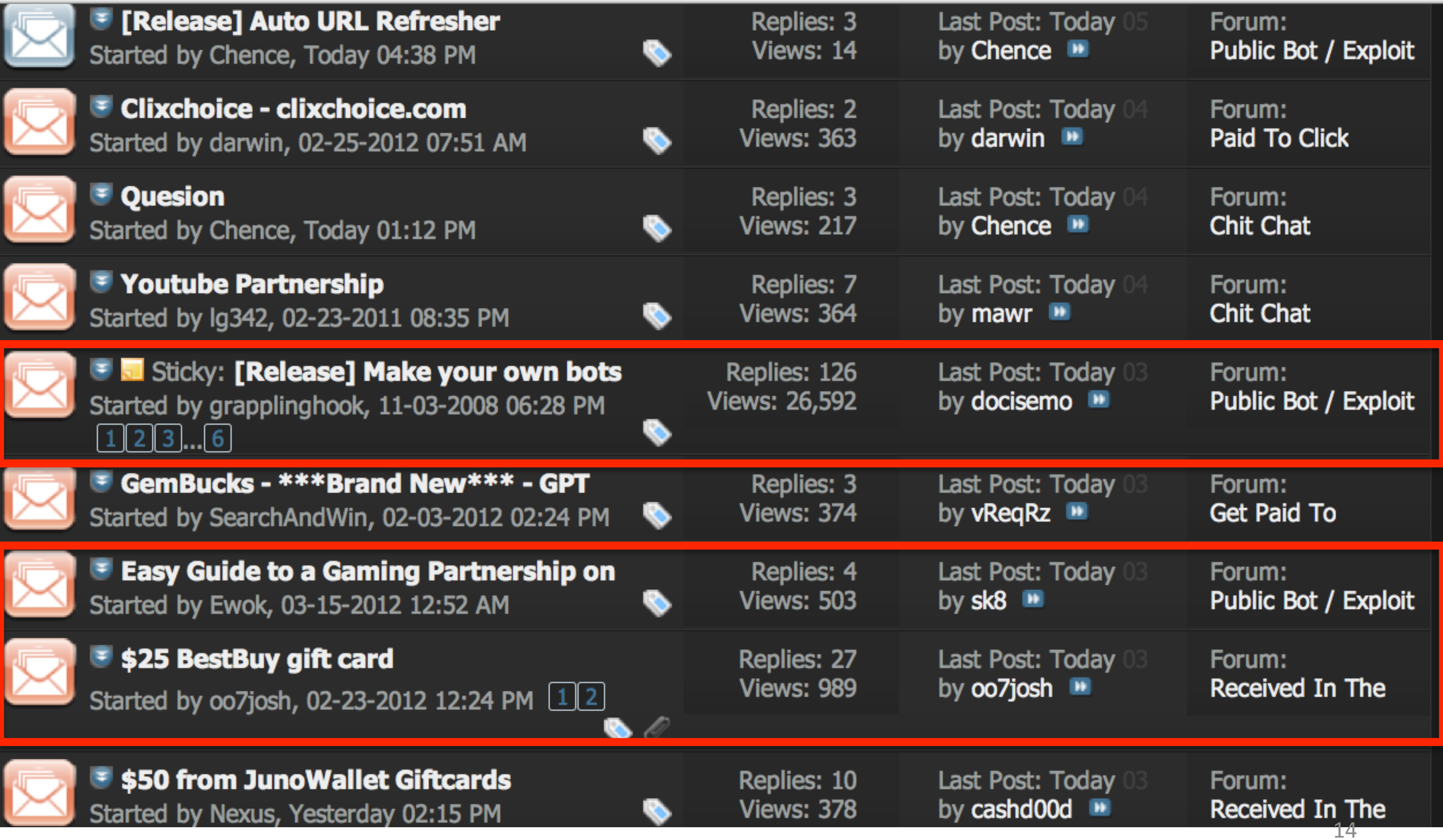
Find Posts: Any Date — and Newer

Sort Results by: Relevance — in Descending Order

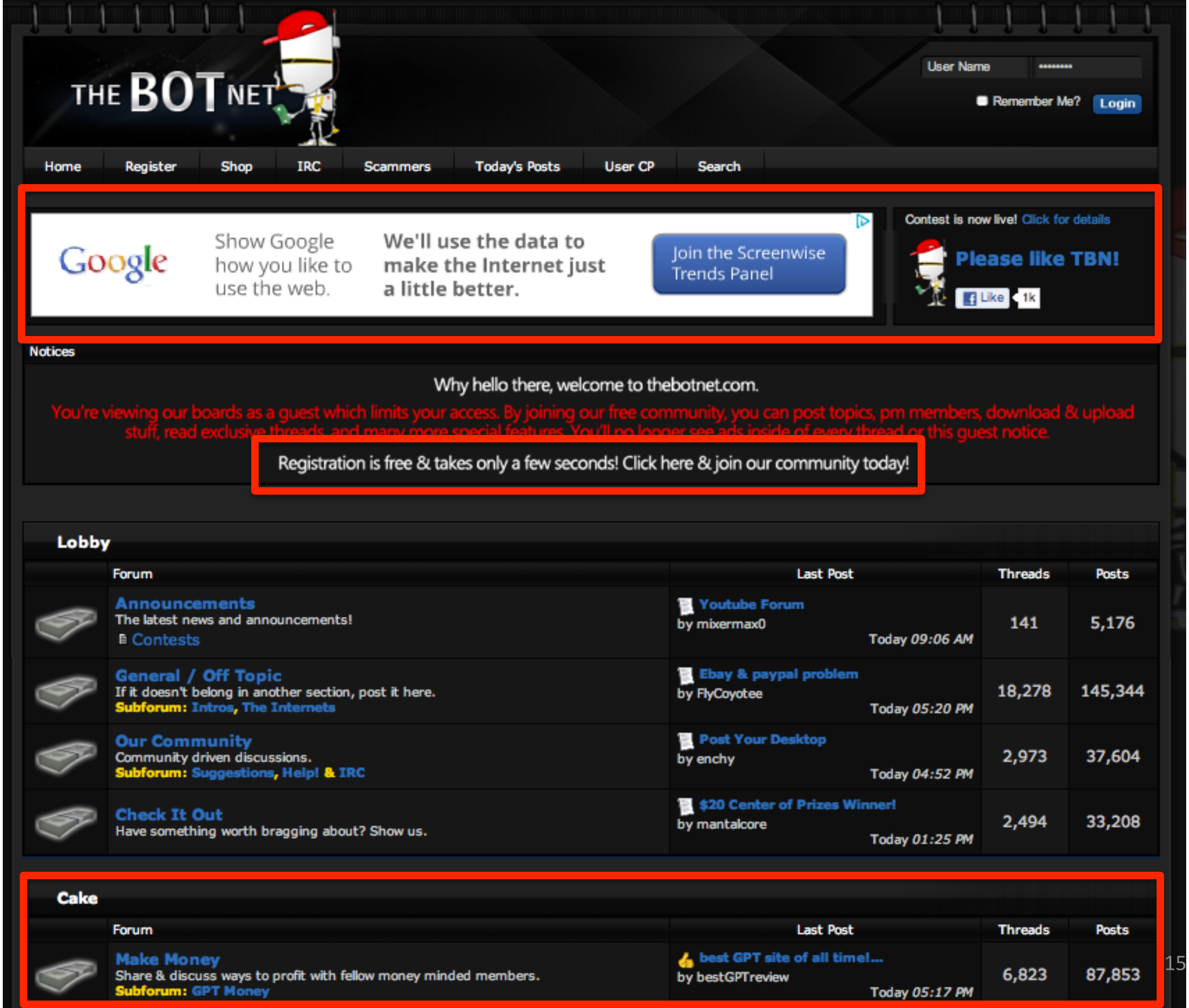
Antispam, complete the task:

Assemble the image as you see at the upper right corner ✓

Cheating Network



[Release] Auto URL Refresher Started by Chence, Today 04:38 PM	Replies: 3 Views: 14	Last Post: Today 05 by Chence	Forum: Public Bot / Exploit
Clixchoice - clixchoice.com Started by darwin, 02-25-2012 07:51 AM	Replies: 2 Views: 363	Last Post: Today 04 by darwin	Forum: Paid To Click
Quesion Started by Chence, Today 01:12 PM	Replies: 3 Views: 217	Last Post: Today 04 by Chence	Forum: Chit Chat
Youtube Partnership Started by lg342, 02-23-2011 08:35 PM	Replies: 7 Views: 364	Last Post: Today 04 by mawr	Forum: Chit Chat
Sticky: **[Release] Make your own bots** Started by grapplinghook, 11-03-2008 06:28 PM 1 2 3 ... 6	Replies: 126 Views: 26,592	Last Post: Today 03 by docisemo	Forum: Public Bot / Exploit
GemBucks - ***Brand New* - GPT** Started by SearchAndWin, 02-03-2012 02:24 PM	Replies: 3 Views: 374	Last Post: Today 03 by vReqRz	Forum: Get Paid To
Easy Guide to a Gaming Partnership on Started by Ewok, 03-15-2012 12:52 AM	Replies: 4 Views: 503	Last Post: Today 03 by sk8	Forum: Public Bot / Exploit
$25 BestBuy gift card Started by oo7josh, 02-23-2012 12:24 PM 1 2	Replies: 27 Views: 989	Last Post: Today 03 by oo7josh	Forum: Received In The
$50 from JunoWallet Giftcards Started by Nexus, Yesterday 02:15 PM	Replies: 10 Views: 378	Last Post: Today 03 by cashd00d	Forum: Received In The



Contest is now live! Click for details

Please like TBN!

Notices

Why hello there, welcome to thebotnet.com.

You're viewing our boards as a guest which limits your access. By joining our free community, you can post topics, pm members, download & upload stuff, read exclusive threads, and many more special features. You'll no longer see ads inside of every thread or this guest notice.

Registration is free & takes only a few seconds! Click here & join our community today!

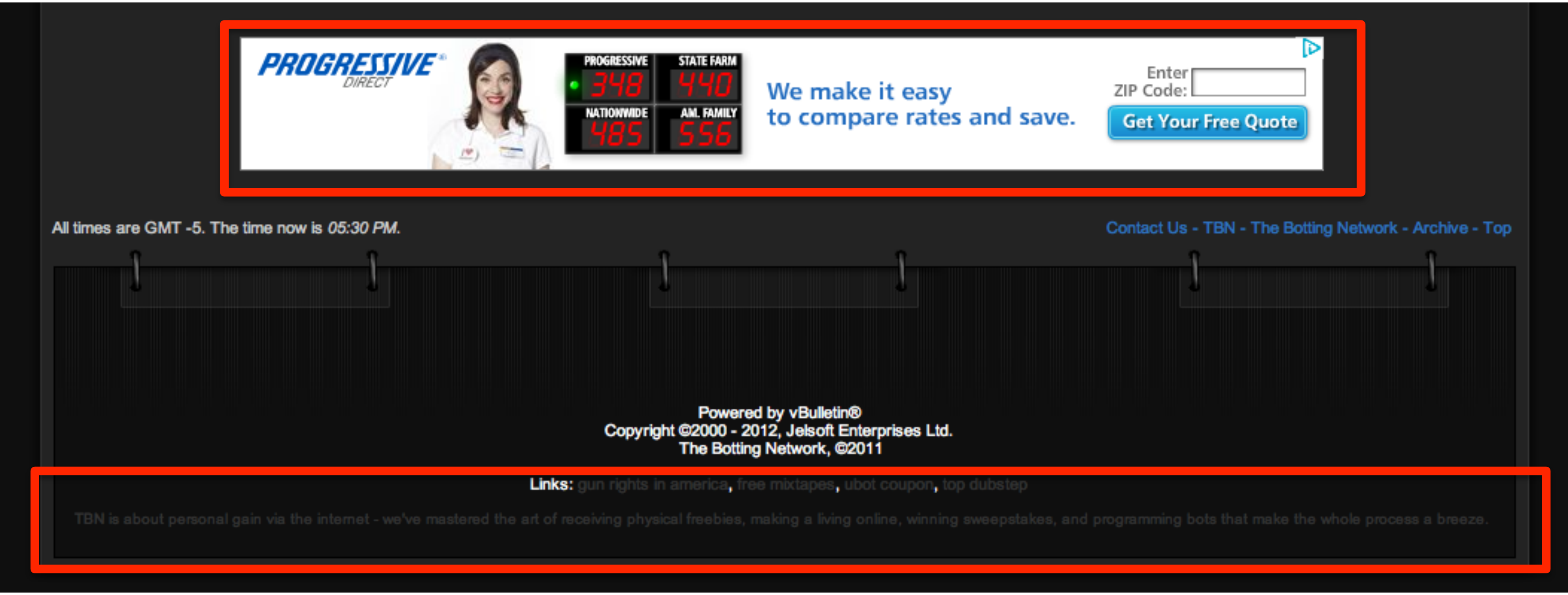
Lobby

Forum	Last Post	Threads	Posts
Announcements The latest news and announcements! Contests	Youtube Forum by mixermax0 Today 09:06 AM	141	5,176
General / Off Topic If it doesn't belong in another section, post it here. Subforum: Intros, The Internets	Ebay & paypal problem by FlyCoyotee Today 05:20 PM	18,278	145,344
Our Community Community driven discussions. Subforum: Suggestions, Help! & IRC	Post Your Desktop by enchy Today 04:52 PM	2,973	37,604
Check It Out Have something worth bragging about? Show us.	$20 Center of Prizes Winner! by mantalcore Today 01:25 PM	2,494	33,208

Cake

Forum	Last Post	Threads	Posts
Make Money Share & discuss ways to profit with fellow money minded members. Subforum: GPT Money	best GPT site of all time!... by bestGPTreview Today 05:17 PM	6,823	87,853

TBN – The Botting Network



All times are GMT -5. The time now is *05:30 PM*.

Contact Us - TBN - The Botting Network - Archive - Top

Powered by vBulletin®
Copyright ©2000 - 2012, Jelsoft Enterprises Ltd.
The Botting Network, ©2011

Links: gun rights in america, free mixtapes, ubot coupon, top dubstep

TBN is about personal gain via the internet - we've mastered the art of receiving physical freebies, making a living online, winning sweepstakes, and programming bots that make the whole process a breeze.

Increase in Fraud/Malicious Behavior

- Who’s paying for fraud?
- Is this type of behavior violating the Terms of Use of your website agreement?
- Traditional fraudulent behavior is changing – not just hard dollars anymore
- Moving to other parts of the site to compromise the system and/or business logic

Engage Fraud and Legal to Discuss the Emerging Threats

Mobile Issues

- Business Drivers
  - We want to have a multi channel solution to acquire and retain customers through the use of email updates, instant coupons, rebates, and other promotions to our customers
  - We want to communicate with all of our customers in near-realtime
- Challenges Identified
  - User login using IE 7 running Windows OS
  - User continues the session, but the session switches to Firefox on Linux
- Research
  - Compromised phones are accessing the Web site
  - Mobile emulation programs are probing the Web site

Slow Site Scraping for Content, Pricing, Inventory, or just Probing

- Different velocity scans hitting the Web site to find out:
  - How many items are in inventory
  - How much items cost
  - What type of systems/services are running to support the site
  - Moving through the site to understand if there were any translation to other languages
- Research
  - Items were being held in shopping carts and never purchased
  - What is the relationship between Women's shoes and Women's clothing searches and page views?

DDoS

- Repeated behavior indicated something was going to happen
- Trending data allowed the team to be prepared
- Preparation included:
  - Simulated DDoS testing
  - Enhancements to the SOPs
  - Understanding where revenue was being generated – which countries and locations were high revenue areas

There is no silver bullet for a DDoS attack

Lessons Learned

- It’s about the data
- Quantify your research
- There are tools out there to solve this complex issue – evaluate the solutions now
- Disk is cheap/creative with storage solutions to trend data over longer periods of time
- Research events and tie the patterns/trends together
- Collaborate, collaborate, collaborate

Staying Ahead – Where to Go

- OWASP Meetings
- ISSA Meetings
- US Secret Service Briefings
- FBI InfraGard
- E-crime Congress
- Financial Services - Information Sharing and Analysis Center (FS-ISAC) (Finance / Financial Services)
- Merchant Risk Council (MRC) (Online / Retail)

Build Your Network of Subject Matter Experts!

Resources

- ww.cheatingnetwork.net
- www.cybercrime.gov
- www.datalossdb.org
- www.darkreading.com
- www.e-crimecongress.org
- www.fsisac.com
- www.merchantriskcouncil.org
- www.owasp.org
- www.thebotnet.com

Questions?

Thank You!

Laz

Director of Strategy, Silver Tail Systems

laz@silvertailsystems.com

Twitter: iamlaz