No Plan Survives Contact

Experience with Cybercrime Measurement

Chris Kanich   Neha Chachra   Damon McCoy
Chris Grier   David Wang   Marti Motoyama
Kirill Levchenko   Stefan Savage   Geoffrey M. Voelker

UC San Diego

UC Berkeley

Security Experiments

- Moc y
  - D
- Pas rld malice
  - P ..
- But gaging with
  - H s?
  - D ls?

page reload after: 8

Captcha bid: $0.5 per thousand

Hint: you can use ENTER key on your keybord instead of using mouse

Engaging the Underground Economy

Started in 2006 with numerous projects since:

- Early infrastructure supporting scams [Security07]
  - Crawl network & host infrastructure from 1M spams
- CAPTCHA-solving ecosystem [Security10]
  - Customer and worker for 8 CAPTCHA-solving services
- Spam value chain [Oakland11]
  - Crawl infrastructure for 1B spams, 100s of purchases
- Order volume, customer demand [Security11]
  - 100s of purchases, inference of revenue & demands
- Freelance marketplace of abuse jobs [Security11]
  - Crawl 7 years of Freelancer.com, hire workers to validate

Requirements

- We have learned the hard way that engagement has two key requirements
- Verisimilitude
  - Attackers defend themselves
  - Need to appear as who they expect
  - Makes engaging at scale more challenging
- Scale
  - Attackers operate at scale
  - Have to engage at scale to observe big picture
  - Need infrastructure to collect, analyze huge data
- Goal: Explain methods and lessons learned to help future security researchers with similar goals

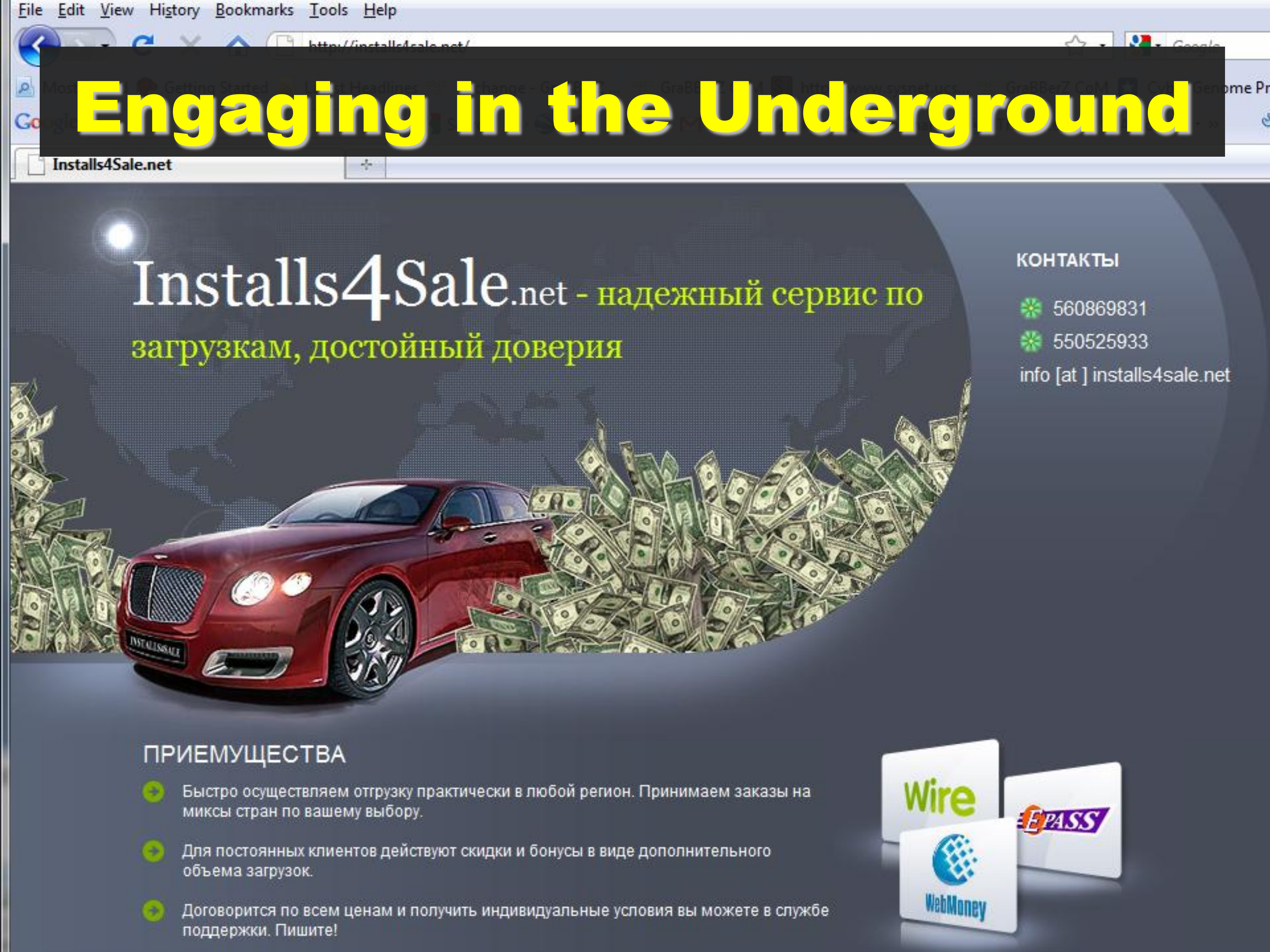
Two Kinds of Engagement

Cover two kinds of engagement in this talk:

- Engagement as an **underground peer**
  - Buy cybercrime software, CAPTCHA solutions, Facebook Likes, …
  - Appear to be a “normal” cybercriminal
  - These guys don’t take VISA! (much less English…)
- Engagement as a **customer**
  - Crawl 100s of millions of URLS, buy 100s of items
  - Appear to be a “normal” customer
  - At scale requires sophisticated identity management

INTERMISSION

Engaging in the Underground


File Edit View History Bookmarks Tools Help
http://installs4sale.net/
Installs4Sale.net
INSTALLS4SALE
Wire
EPASS
WebMoney

Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

КОНТАКТЫ

560869831

550525933

info [at] installs4sale.net

ПРИЕМУЩЕСТВА

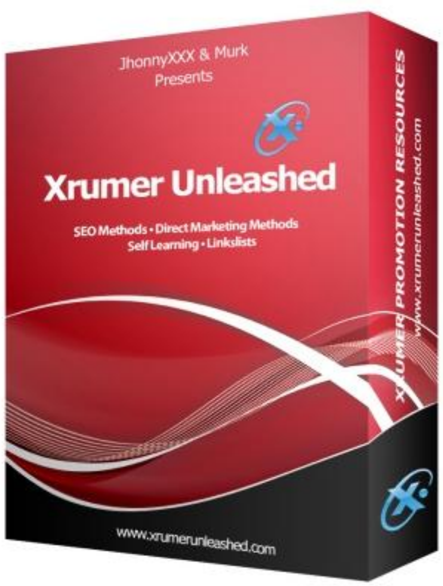
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!

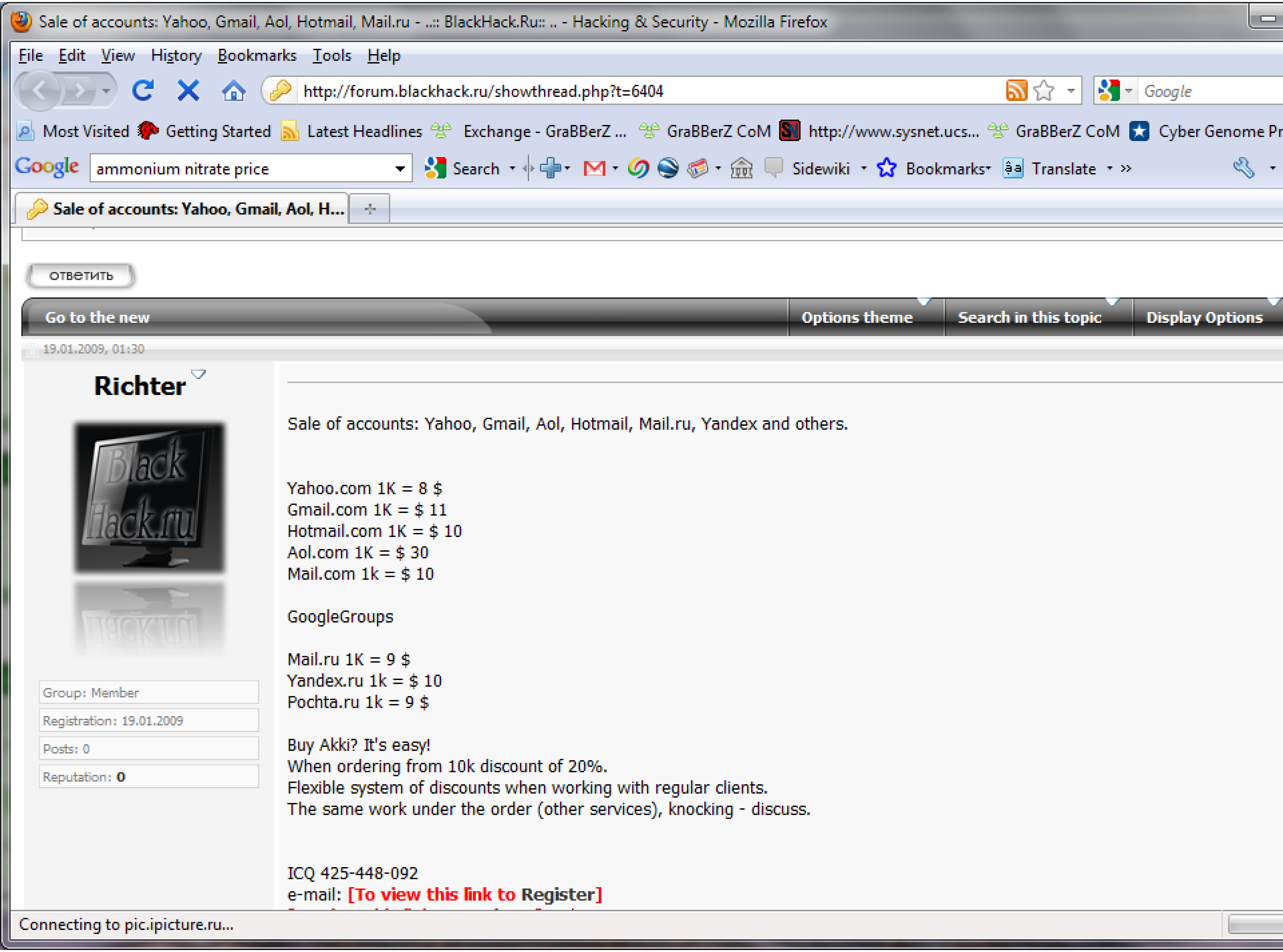
Underground Forums

- Miscreants openly describe their activities and methods on underground forums & IRC
  - Tremendous source of useful information
  - Learned much about affiliate programs
- Forums also serve as a marketplace for buying and selling digital goods
  - Items, quantities, prices, contacts, …

Underground Purchases

- Kinds of purchases we made
  - CAPTCHA services ($3,400)
  - Underground software ($640)
  - Hiring freelance workers ($2,100)
  - Web mail accounts…
- All negotiated online


JhonnyXXX & Murk
Presents
Xrumer Unleashed
SEO Methods • Direct Marketing Methods
Self Learning • Linkslists
XRUMER PROMOTION RESOURCES
www.xrumerunleashed.com
www.xrumerunleashed.com


Sale of accounts: Yahoo, Gmail, Aol, Hotmail, Mail.ru - ..:: BlackHack.Ru:: .. - Hacking & Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://forum.blackhack.ru/showthread.php?t=6404
Google
Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Pr
Google ammonium nitrate price Search Sidewiki Bookmarks Translate
Sale of accounts: Yahoo, Gmail, Aol, H...
ответить
Go to the new
Options theme
Search in this topic
Display Options
19.01.2009, 01:30
Richter
Black Hack.ru
Connecting to pic.ipicture.ru...

Group: Member
Registration: 19.01.2009
Posts: 0
Reputation: **0**

Sale of accounts: Yahoo, Gmail, Aol, Hotmail, Mail.ru, Yandex and others.

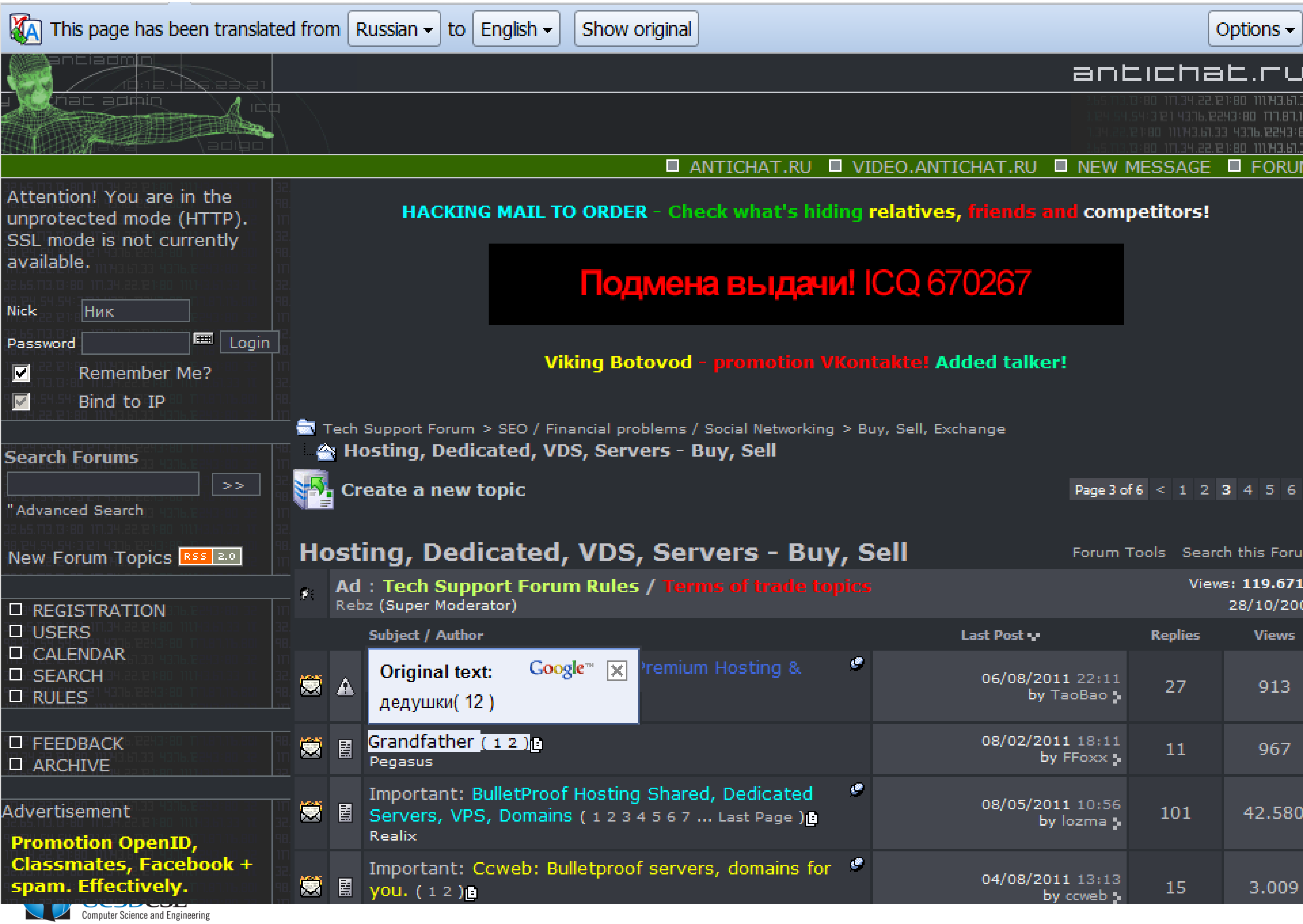
Yahoo.com 1K = 8 $
Gmail.com 1K = $ 11
Hotmail.com 1K = $ 10
Aol.com 1K = $ 30
Mail.com 1k = $ 10

GoogleGroups

Mail.ru 1K = 9 $
Yandex.ru 1k = $ 10
Pochta.ru 1k = 9 $

Buy Akki? It's easy!
When ordering from 10k discount of 20%.
Flexible system of discounts when working with regular clients.
The same work under the order (other services), knocking - discuss.

ICQ 425-448-092
e-mail: **[To view this link to Register]**



This page has been translated from Russian ▾ to English ▾ Show original Options ▾

antichat.ru

□ ANTICHAT.RU □ VIDEO.ANTICHAT.RU □ NEW MESSAGE □ FORU

Attention! You are in the unprotected mode (HTTP). SSL mode is not currently available.

Nick Ник

Password Login

☑ Remember Me?

☑ Bind to IP

Search Forums

>>

" Advanced Search

New Forum Topics RSS 2.0

□ REGISTRATION
□ USERS
□ CALENDAR
□ SEARCH
□ RULES

□ FEEDBACK
□ ARCHIVE

Advertisement

Promotion OpenID, Classmates, Facebook + spam. Effectively.

HACKING MAIL TO ORDER - Check what's hiding relatives, friends and competitors!

Подмена выдачи! ICQ 670267

Viking Botovod - promotion VKontakte! Added talker!

Tech Support Forum > SEO / Financial problems / Social Networking > Buy, Sell, Exchange

Hosting, Dedicated, VDS, Servers - Buy, Sell

Create a new topic

Page 3 of 6 < 1 2 3 4 5 6

Hosting, Dedicated, VDS, Servers - Buy, Sell

Forum Tools Search this Foru

Ad : Tech Support Forum Rules / Terms of trade topics
Rebz (Super Moderator)

Views: 119.671
28/10/200

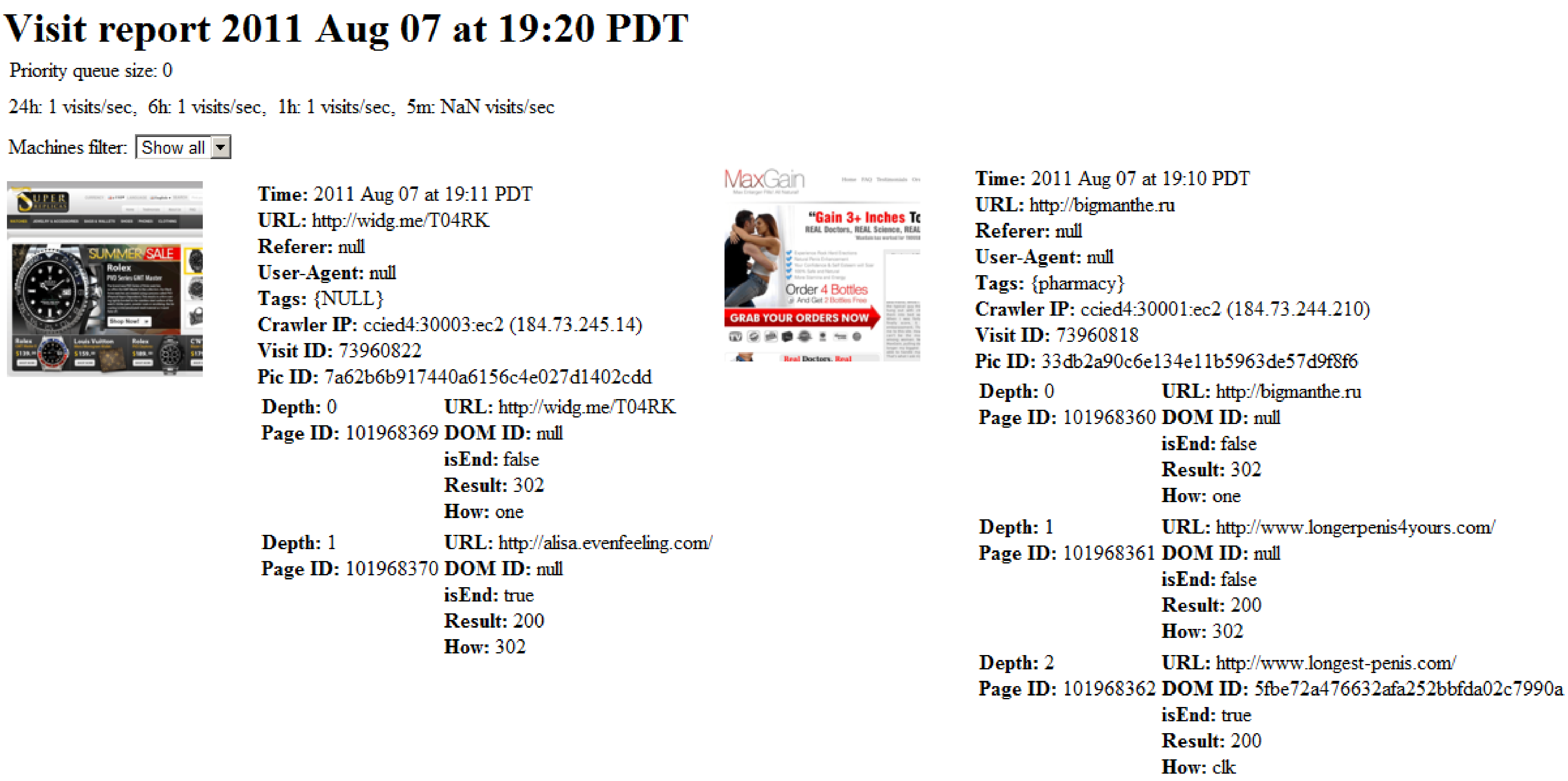
Subject / Author	Last Post	Replies	Views
Original text: Google™ ☒ дедушки(12) remium Hosting &	06/08/2011 22:11 by TaoBao	27	913
Grandfather (1 2) Pegasus	08/02/2011 18:11 by FFoxx	11	967
Important: BulletProof Hosting Shared, Dedicated Servers, VPS, Domains (1 2 3 4 5 6 7 ... Last Page) Realix	08/05/2011 10:56 by lozma	101	42.580
Important: Ccweb: Bulletproof servers, domains for you. (1 2)	04/08/2011 13:13 by ccweb	15	3.009

Engaging as a Customer

Visiting Their Sites

When visiting 1B URLs over three months…

- Full-featured browsers necessary for verisimilitude
  - Redirection: Flash/javascript, clicking on popups, …
  - More danger, more complexity, beefier machines
- IP diversity is necessary at scale
  - Deterrence: You will get blacklisted, plan for it
  - Cloud providers and IP-hiding services easy to use



Visit report 2011 Aug 07 at 19:20 PDT

Priority queue size: 0

24h: 1 visits/sec, 6h: 1 visits/sec, 1h: 1 visits/sec, 5m: NaN visits/sec

Machines filter: Show all ▾

Time: 2011 Aug 07 at 19:11 PDT
URL: http://widg.me/T04RK
Referer: null
User-Agent: null
Tags: {NULL}
Crawler IP: ccied4:30003:ec2 (184.73.245.14)
Visit ID: 73960822
Pic ID: 7a62b6b917440a6156c4e027d1402cdd

Depth: 0 **URL:** http://widg.me/T04RK
Page ID: 101968369 **DOM ID:** null
isEnd: false
Result: 302
How: one

Depth: 1 **URL:** http://alisa.evenfeeling.com/
Page ID: 101968370 **DOM ID:** null
isEnd: true
Result: 200
How: 302

Time: 2011 Aug 07 at 19:10 PDT
URL: http://bigmanthe.ru
Referer: null
User-Agent: null
Tags: {pharmacy}
Crawler IP: ccied4:30001:ec2 (184.73.244.210)
Visit ID: 73960818
Pic ID: 33db2a90c6e134e11b5963de57d9f8f6

Depth: 0 **URL:** http://bigmanthe.ru
Page ID: 101968360 **DOM ID:** null
isEnd: false
Result: 302
How: one

Depth: 1 **URL:** http://www.longerpenis4yours.com/
Page ID: 101968361 **DOM ID:** null
isEnd: false
Result: 200
How: 302

Depth: 2 **URL:** http://www.longest-penis.com/
Page ID: 101968362 **DOM ID:** 5fbe72a476632afa252bbfda02c7990a
isEnd: true
Result: 200
How: clk

Crawling Challenges

- Blacklisting by bad guys
  - Hierarchical IP space usage
- Scale
  - Dozens of machines, 100s of browsers/machine
  - Central dispatcher, distributed client
- Poisoning by bad guys
  - A spammer started inserting well-formed junk URLs
  - Added an importance-based crawl scheduler

Blacklisting

```
#!/bin/bash

iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -F INPUT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p udp --dport 53 -j DROP

if [ "$1" = "zeus"  ]
then
        sh google_block.sh
        sh zeustracker_block.sh
fi
…
iptables -A INPUT -s 149.20.54.132              -j DROP          #pt1b.phishtank.com
iptables -A INPUT -s 149.20.54.134              -j DROP          #pt2b.phishtank.com

iptables -A INPUT -s 133.5.16.238              -p tcp -m multiport --dports
80,443,8080 -j DROP     #HidemaruMail SpamFilter Agent Kyushu University
iptables -A INPUT -s 198.134.135.0/24   -j DROP
             #University of California at San Diego FAKE UA,REF
iptables -A INPUT -s 216.163.176.0/20   -j DROP          #Commtouch Inc.
iptables -A INPUT -s 95.211.120.0/24    -j DROP          #leaseweb.com BAD BLOCK
…
```

Purchasing as a Customer

- How to do this at scale?
  - 100s of purchases, $17K spent on items + shipping
- When buying from an online pharmacy you need:
  - Name, shipping address, email, phone number
  - IP address from which to make the purchase
  - Method for receiving and cataloging the goods
- And you want to collect:
  - Virtual properties (site ID, communication style)
  - Financial properties (VISA BIN, Bank name)
  - Physical properties (where from, active ingredient)

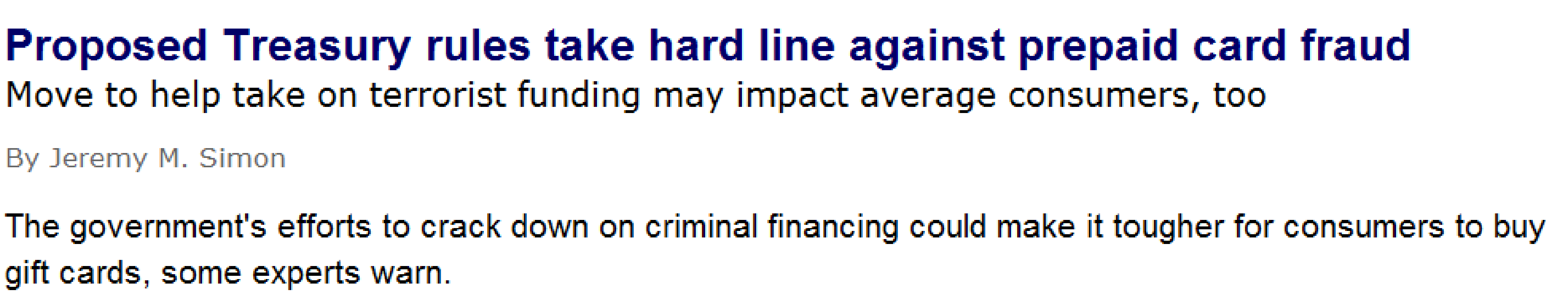
Identity Management (Corporeal)

- Originally: Pseudonyms + “P.O. Box”
  - Specialty issuer: no pseudonyms
  - High volume spooked the P.O. Box guys
- State of the art: real names + home addresses
  - Ordering legal, end user goods
  - Odd orders, but our money is green
- Prepaid cell phones + add’l Google Voice #s
  - Difficult to know which order/customer call is for
  - Required on-the-spot creativity at times

Identity Management (Virtual)

- Email through Google Apps free account
  - Can create nonce address for each purchase
  - gmail/hotmail/ymail increases fraud score
- Purchase from SD residential IP addresses
  - IP Geo-location important for fraud score
  - VPN tunnel to home machine, 3G,
    stay home and buy drugs

Financial Transactions History



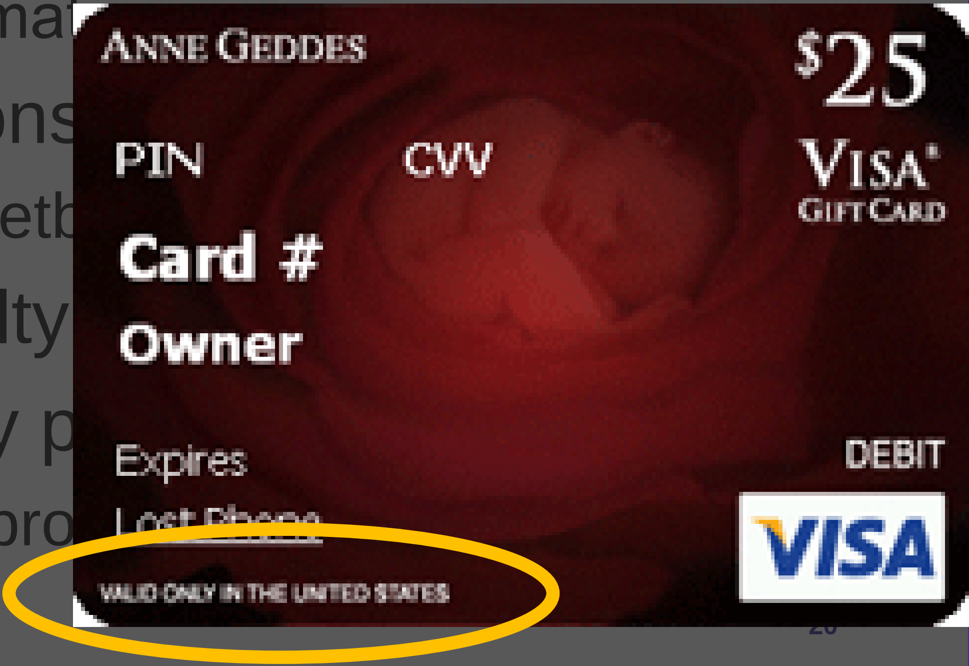
Proposed Treasury rules take hard line against prepaid card fraud

Move to help take on terrorist funding may impact average consumers, too

By Jeremy M. Simon

The government's efforts to crack down on criminal financing could make it tougher for consumers to buy gift cards, some experts warn.

- Collecting data by phone very error prone
- Couldn't get BIN informati
- Tried several other cons
  - C a major setb
- Call l specialty
- Spe ier finally p
  - Manual, batch-based pro



Internal red tape

- As involved as solving the technical problems

- Extensive oversight
  - Legal oversight
  - Research oversight

- Build trust slowly, incrementally

  Our capabilities are the result of years of trust-building

Final Takeaways

- Full-fidelity crawling architecture necessary for verisimilitude
    - But increases challenges for achieving scale…
- Underground forums provide “finger on the pulse”
- Acquiring payment data was priceless
- Engagement can lead to serendipitous opportunities

Thank You!

UCSDCSE
Computer Science and Engineering

THE UNIVERSITY OF CALIFORNIA BERKELEY
1868