Security at Twitter

http://inwyrd.com

Kurt Thomas

Everywhere
Security at Twitter

- User Privacy
- Advertisement, Site Integrity
- Uptime
- Spam & Abuse
Security is not an isolated problem
Only as good as weakest link
Today

• What is security?
• Criminal underground
  – Why services get attacked
• Twitter’s perspective
  – Fake, compromised accounts
• Biggest industry threats
• Emerging problems
What is Security?
Defining Security

• Allow intended use of computer systems

• Prevent unintended use that may cause harm

_Overly vague because we often don’t know desired security guarantees_
Grant authorized users access to read, create personal files
Prevent unauthorized users from reading, modify, or deleting personal
Banking Funds

Allow customer to view balance, transfer funds, make payments
Prevent third party access to account; customers defrauding bank
Prevent other browser tabs, applications from reading banking info
Personal Privacy

Allow friends to view status updates, photos, location data
Prevent strangers, advertisers from accessing profile
Prevent strangers, applications from posting updates as you
Security Flow

- **Threat** – risk that jeopardizes user privacy, uptime, data integrity
- **Vulnerability** – flaw in system design; code/hardware bugs
- **Exploit** – discovery, attack on a vulnerability
- **Payload** – end goal of an exploit; site disruption, remote access, data theft
Threats

• In the beginning:
  – Exploration, disruption, personal reputation

• 1990s:
  – Phone phreaking, free calls

• Early 2000s:
  – Email worms
  – CodeRed, MyDoom, Sobig
Financially Motivated

• Shift in late 2000s
• Spam
  – Pharmaceuticals
  – Fake products
• Carding/Fraud
  – Identify theft, credit fraud
Politically Motivated

- Stuxnet, Flame, Gauss
  - Iranian nuclear infrastructure
  - Lebanese banking information
  - Wiretapping
Politically Motivated

**Anonymous**

*We do not forgive, we do not forget.*

*We are Legion.*
Vulnerabilities & Exploits

• Flaw in system design:
  – Twitter
  – Network
  – Browser
  – Operating system
  – Hardware

• For today, we’re more interested in what happens after an exploit
All Roads Lead to Rome

Monetization
Spam

[Click Trajectories. Kirill et al. 2011]
What is Spam?

• Unwanted advertisements
  – Pharmaceuticals
  – Knock-off products
  – Pirated software

• Per previous lecture, devise technical counter measures
  – Account classification
  – URL classification
Healthcare Online

Most Popular Products

**Viagra as low as $1.85**
Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.

› More Info

**Cialis as low as $1.95**
Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.

› More Info

**Viagra Super Active+ as low as $2.79**
Viagra Super Active represents the fourth generation of phosphodiesterase inhibitors. This new formulation of a world-known medication provides even...
Spam is a Business

- Profitable

- Complex infrastructure
  - All parts must work correctly
  - Adversarial; avoid detection

- Specialized
  - No single party does everything

[Click Trajectories. Kirill et al. 2011]
Spam Value Chain

1. Spam Message
   From: fvcjleo@acme.com
   To: recipient@example.com
   Subject: VIAGRA ® Official Site
   http://medicsStopnerx.ru

2. Click

Grum Botnet

User

[Click Trajectories. Kirill et al. 2011]
Spam Value Chain

[Click Trajectories. Kirill et al. 2011]
Spam Value Chain

[Click Trajectories. Kirill et al. 2011]
Spam & Big Data

• Researchers examined 969M unique URLs
  – Crawl 3.5M domains
  – Covers 951M URLs (many hosted at same domain)

• Identify 30 programs responsible for 365M URLs

• Purchase products from these programs

[Click Trajectories. Kirill et al. 2011]
Technical Solutions Not Always Best

• Spammers relied on:
  – 969M URLs, 17M domains

• Payment infrastructure much more fragile
  – Currently being targeted by Visa, brands

[Click Trajectories. Kirill et al. 2011]
## Spam Income

<table>
<thead>
<tr>
<th>Spam Program</th>
<th>Customers</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlavMed</td>
<td>584,199</td>
<td>$81 million</td>
</tr>
<tr>
<td>SpamIt</td>
<td>535,365</td>
<td>$92 million</td>
</tr>
<tr>
<td>RX-Promotion</td>
<td>69,446</td>
<td>$12 million</td>
</tr>
</tbody>
</table>

Repeat customers 9-23% of revenue  
Operations span 1-2 years

[PharmaLeaks. McCoy et al 2012]
Fake Anti-Virus

• Mislead users into purchasing fake virus protection
  – Actually installing malware

• Pay by credit card

• No ‘warnings’ after successful purchase
Your computer remains infected by viruses! They can cause data loss and file damages and need to be cured as soon as possible. Return to System Security and download it to secure your PC.
Order Details

- 1 year Software License $59.95
- 2 year Software License $69.95
- lifetime Software License, 60% discount! $79.95
- Sign me up for a purchase of Lifetime Premium Support of only $19.95.

Terms

You are purchasing MAC Security. This is a one-time charge and you will not be rebilled.

Payment Information

Credit Card Information
- Card Type: Visa
- Card Number:
- Expiration Date: ---
- CVV2 Number:

Contact Information
- Email:
- Country: United States
- State: Outside U.S.
- Address:
- City:
- Zip Code:
- Telephone:

Secure Purchase
## Fake AV Income

<table>
<thead>
<tr>
<th>Fake AV Scam</th>
<th>Revenue</th>
<th>Victims Paying</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV 1</td>
<td>$11 million</td>
<td>189 thousand</td>
</tr>
<tr>
<td>AV 2</td>
<td>$5 million</td>
<td>137 thousand</td>
</tr>
<tr>
<td>AV 3</td>
<td>$116 million</td>
<td>1.9 million</td>
</tr>
</tbody>
</table>

On average, 2% of users shown scam will pay out
Operations span 3 months – 2 years

[Underground Economy of Fake AV. Stone-Gross et al 2011]
Click Fraud

• Google, advertisers syndicate ads to affiliates
  – Affiliates paid based on traffic

• Use compromised machines to click on ads
  – Criminal affiliate receives payment
  – Difficult to detect due to thousands of bots
Information Theft

• Malware monitors banking transactions
• Steals credit card, address information
• Later perform fraudulent purchases
  – Complex chain for cashing out stolen cards
Pay-per-Install

• Specialize in compromising machines
  – Leave monetization to someone else

• Marketplaces for installs used by
  – Spam bots
  – Fake anti-virus
  – Clickfraud
  – Information Theft
Goldinstall Rates for 1K Installs for each Country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTH</td>
<td>13$</td>
</tr>
<tr>
<td>US</td>
<td>150$</td>
</tr>
<tr>
<td>GB</td>
<td>110$</td>
</tr>
<tr>
<td>CA</td>
<td>110$</td>
</tr>
<tr>
<td>DE</td>
<td>30$</td>
</tr>
<tr>
<td>BE</td>
<td>20$</td>
</tr>
<tr>
<td>IT</td>
<td>65$</td>
</tr>
<tr>
<td>CH</td>
<td>20$</td>
</tr>
</tbody>
</table>
Role of Twitter in Cybercrime
Support Infrastructure for Monetization

Products

- Spam
- FakeAV
- Click Fraud
- Banking Theft

Infrastructure

- Spamming botnets
- PPI services
- SEO kits
- Packers
- Traffic Direction
- Accounts
- Hosting
- Phishing Kits
- Banking Trojan

Dependency

Theft
Welcome!

Welcome to BuyAccountsNow.com which is probably the best place to shop for site accounts. If you have any questions, don’t hesitate and contact our super friendly support team.

We started selling real worldwide Facebook fans and YouTube views! Boost your social presence and increase exposure with our new service.

Click HERE for more info!
Best Quality Hotmail, Yahoo, AOL, Gmx, Twitter, CL @ reasonable price

Prices are as follow:
(Prices can vary later on - updated prices will be posted later on same page)

Prices for HOTMAIL Accounts:
(Minimum order limit; 1000 Accounts)
1000 NON-VERIFIED Hotmail = $6
1000 VERIFIED Hotmail = $7
1000 VERIFIED HOTMAIL Forwarded to master account = $
Kamal Kishore
Data Entry, Web Scraping, SEO, Web Development

Username: Kamalkishover
Location: Multai, India
Member since: Feb 2008

We have 4 year working experiences of special areas such as Data Entry, Market Research, Internet Marketing, Social Media Marketing, and Search Engine Optimization (SEO), Web Design. We have been able to grow and expand my knowledge and skills. We provide high quality results for my client 100% Satisfaction.

My activity:
- Completion Rate: 68%
- On Budget: 100%
- On Time: 96%
- Repeat Hire Rate: 13%

My skills:
- Data Entry
- Data Processing
- Excel
- Internet Marketing
- Web Scraping
- Other Skills

Reputation: 4.8
(285 reviews)
$6.9
Pricing Per Thousand Accounts

- Twitter: $15-60
- Mail.ru: $5
- Gmail: $100 (Phone Verified)
Purchasing Accounts

BuyAccs.com

Our shop is pleased to offer accounts of various e-mail services and free-hosts with instant receipt after paying for the system Webmoney. All accounts you get in a convenient format, which can be easily changed using the free converter accounts.

You ordered a 1000 account Twitter.com

To Pay: 450 WMR

E-mail: 

ICQ: 

WMT: 

Receive news for E-mail: 

[Download link will be sent by e-mail and ICQ. Number ICQ bot 582-313-439] [Be sure to save the link, you will see on next page]

Go to payment

Help for the selected type of account:

Twitter.com Confirmed by E-mail, ready to use accounts. Accounts are clean, no followers. To register, use E-mail on Mail.ru. What to use: Can be used for promotional purposes. Format: login: Password: Email: email_password.
Dataset Summary

Total Tweets: 1.8 billion
Abusive Accounts: 1.1 million
Abusive Tweets: 80 million
Abusive URLs: 15 million
Abusive Account – Median Stats

**Lifetime:** 1 day
From first tweet to last tweet

**Followers:** 2
Users receiving a spammers content

**Tweets:** 13
Total tweets sent
Engagement

• Abusive accounts forgo social graph
  – 89% of accounts < 10 followers

• Unsolicited @mentions: 52% of accounts

• #Hashtags, trends: 17% of accounts

• Alternative distribution forms:
  – Direct messages
  – Search
Social Activity

Regular Twitter User

Abusive Account
Campaign: *Afraid*

**Duration:**
- 9 months

**Accounts:**
- 124,000

**Tweets:**
- 14 million

**URLs:**
- 14 million
Campaign: Yuklumdegga

Duration: 1 day
Accounts: 2,200
Tweets: 130,000
URLs: 24
Campaign: Amazon

Duration: 1 month
Accounts: 848
Tweets: 129,600
URLs: 1
Industry-Wide Threats
Driveby Downloads

• Largest threat right now

• Compromise machines based on plugin, browser vulnerabilities
  – Flash
  – Java
  – PDF Viewer

• Criminal software automates the process
Blackhole Exploit Kit
Blackhole Exploit Kit Costs

• Renting exploit server:

  Аренда на нашем сервере:
  
  Day rental: $50 (limit 50K hits)
  Week rental: $200 (limit 70K hits per day)
  Month rental: $700 (limit 70K hits per day)

• Licensing exploit kits:

  Лицензия на вашем сервере:
  
  3 month license: $700
  6 month license: $1000
Threat of Drivebys

Source: Microsoft Security Intelligence Report (SIRv13)
Google Safebrowsing

• Current detection strategy:
  – Crawl URLs in outdated browsers
  – Find URLs that lead to malware execution
  – Blacklist URL

• Another big data challenge
  – Crawling and scanning billions of pages
Traffic Generation

Methods: Compromise, SEO, Spam

Victim

Compromised Site
hxxp://compromised.com
Exploitation & Development

Compromised Site
hxxp://compromised.com

Exploit Pack Developer

Exploit Pack
hxxp://defpower.org

License

Server Rental
hxxp://mnomango.org

Traffic Payment
Exploit-as-a-Service

1 Traffic Generation
- Compromised Site
- Exploit Pack Developer
- Traffic
- Payment
- Malware

2 Exploit Development
- Blackhole
- Exploit Pack

3 Clients
- Spye
- Zero Access
- Rena FakeAV

Driveby Infection Chain
Malware Dataset

From Google Safebrowsing:

- **Initial Site**: 77,000
- **Exploit Site**: 14,000
- **Executable**: 5,000

**Sandnet**
- (Droppers): 2,600

**Spam Traps**
- (Attachments): 2,800

**Torrents**
- (Warez): 17,000

**Arbor ASERT**
- (Live Traffic): 28,000
## Malware Families by Source

<table>
<thead>
<tr>
<th>Source</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Traffic</td>
<td>40</td>
</tr>
<tr>
<td>Driveby</td>
<td>32</td>
</tr>
<tr>
<td>Dropper</td>
<td>19</td>
</tr>
<tr>
<td>Warez</td>
<td>6</td>
</tr>
<tr>
<td>Attachments</td>
<td>6</td>
</tr>
<tr>
<td>Adware</td>
<td></td>
</tr>
<tr>
<td>Email worms: MyDoom, Bagle</td>
<td></td>
</tr>
</tbody>
</table>
## Monetization

<table>
<thead>
<tr>
<th>Family from Drivebys</th>
<th>Monetization</th>
<th>Overlapping Feeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZeroAccess</td>
<td>Dropper</td>
<td>D, T, L</td>
</tr>
<tr>
<td>Karagany</td>
<td>Dropper</td>
<td>D</td>
</tr>
<tr>
<td>Multi Installer</td>
<td>Dropper</td>
<td></td>
</tr>
<tr>
<td>SpyEye</td>
<td>Info Stealer</td>
<td>D</td>
</tr>
<tr>
<td>TDSS</td>
<td>Info Stealer</td>
<td>A, L</td>
</tr>
<tr>
<td>Zbot</td>
<td>Info Stealer</td>
<td>D</td>
</tr>
<tr>
<td>Windows Custodian</td>
<td>Fake Anti-virus</td>
<td></td>
</tr>
<tr>
<td>Clickpotato</td>
<td>Adware</td>
<td>D, L</td>
</tr>
<tr>
<td>Medfos</td>
<td>Browser Hijacking</td>
<td></td>
</tr>
</tbody>
</table>

(A)ttachment; (T)orrent; (D)opper; (L)ive Traffic
Exploit Kits

• 9 exploit packs:
  – Traffic from 8,000 infected domains
  – Install 5,000 binaries
Domain Lifetime

• Median period infection chain receives traffic
  – Exploit domain: 2.5 hours
  – Initial (compromised) domain: 44 days

• Constant vigilance to find new domains
  – Detect initial URL; redirects
Emerging Threats
HALTE À LA REPRESSION AU MAGHREB

#ArabSpring
#balacera (#shooting)
Smear Attacks/Inflated Reputation
Silencing Opponents
Controlling Discussions

• Russian parliamentary election
  – Bots drown out political speech
  – Advertise inflammatory message

• Infrastructure comes from spam marketplace
From Pills to Political Censorship
From Pills to Political Censorship
Russian Parliamentary Election

• December 5th- December 6th, 2011

• Twitter used to discuss:
  – Purported fraud, protests

• Conversations outside immediate social graph

#триумфальная (#triumphal)
## Hashtags Attacked

<table>
<thead>
<tr>
<th>Hashtag</th>
<th>Translation</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>чп</td>
<td>Catastrophe</td>
<td>23,301</td>
</tr>
<tr>
<td>6дек</td>
<td>December 6th</td>
<td>18,174</td>
</tr>
<tr>
<td>5дек</td>
<td>December 5th</td>
<td>15,943</td>
</tr>
<tr>
<td>выборы</td>
<td>Election</td>
<td>15,082</td>
</tr>
<tr>
<td>митинг</td>
<td>Rally</td>
<td>13,479</td>
</tr>
<tr>
<td>триумфальная</td>
<td>Triumphal</td>
<td>10,816</td>
</tr>
<tr>
<td>победазанами</td>
<td>Victory will be ours</td>
<td>10,380</td>
</tr>
<tr>
<td>5dec</td>
<td>December 5th</td>
<td>8,743</td>
</tr>
<tr>
<td>навальный</td>
<td>Alexey Navalny</td>
<td>8,256</td>
</tr>
<tr>
<td>ridus</td>
<td>Ridus</td>
<td>6,116</td>
</tr>
</tbody>
</table>
Tweet Volume

Tweets (December 5-6, 2011) sent from accounts that discussed election at least once
Tweet Volume

Tweets (December 5-6, 2011) sent from accounts that discussed election at least once
Tweet Volume

Tweets (December 5-6, 2011) sent from accounts that discussed election at least once
Tweet Volume

All tweets (December 5-6, 2011) sent from accounts that discussed the election at least once

Only tweets that contained attacked hashtags
Geolocation of Logins

Nonspam Logins

Russia: 56%

Spam Logins

Russia: 1%
Summary

• Security is a complex problem
  – Motivated by profit, geo-political problems

• No single service can solve all security problems
  – Requires industry-wide cooperation

• Sophisticated criminal underground

• Evolving security threats