# Twarfing: Malicious tweets

Morton Swimmer
Trend Micro

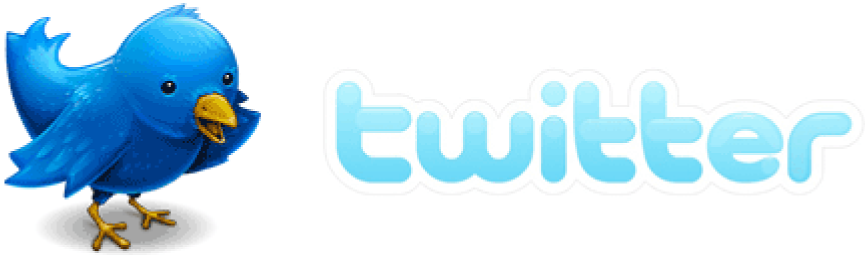
Costin G. Raiu
Kaspersky Lab

Virus Bulletin 2009 – September 24th, Geneva

# Thanks to:

- Special thanks (Costin):
  - Selma Ardelean: GUI+statistics
  - Dan Demeter: daemon, downloader, scanning
  - Alexandru Tudorica: DB design, URL fetching, expansion, scanning
  - Stefan Tanase – suggestions and web 2.0 expertise (you can watch his presentation tomorrow morning in the Corp stream)
- Special thanks (Morton)
  - Rainer Link (architecture)
  - David Sancho (URL expansion)

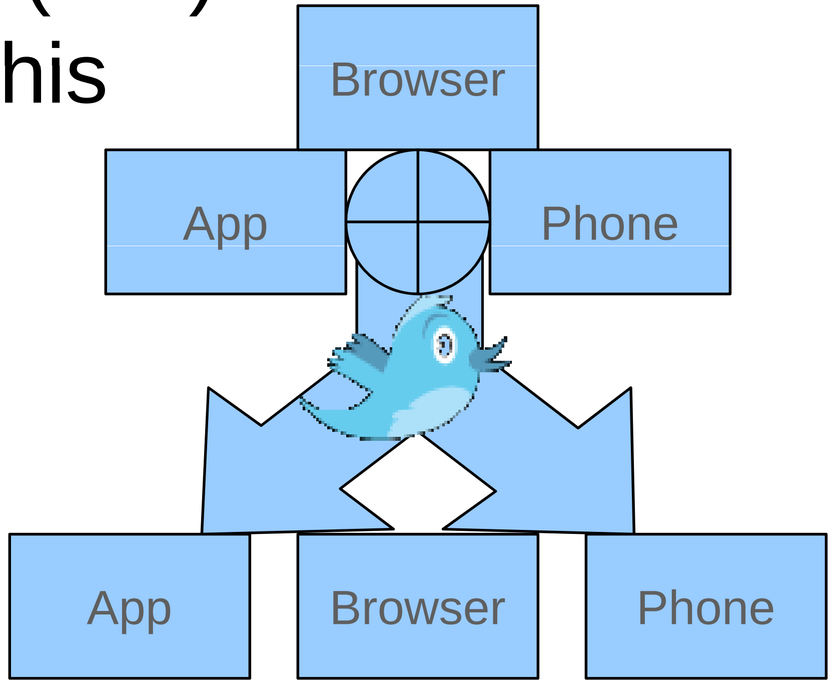
# Overview



- What is Twitter?
- Malware on Twitter
  - Notable incidents
- The link: Twitter and URL shortening services
- Twitter and the Google SB API
- Robots:
  - Kaspersky Architecture and Statistics
  - Trend Architecture and Statistics
- Conclusions

# What is Twitter?

- Publish/Subscribe Communications system
- Founded by Jack Dorsey, Biz Stone and Evan Williams back in 2006
- SMS/Website, WebService (API)
- Subscribers can read from this
- Push
  - SMS: Phone
- Pull
  - Web site: Browser
  - WS API: Application
  - RSS: Application



# Related to:

- Instant Messaging/XMPP
  - Is many to many, but best with small groups or one-to-one
  - Twitter similar, but publish/subscriber model more persistent
  - Twitter also has Direct Messages for IM capability
- Internet Relay Chat (IRC)
  - Handles large groups fairly well
  - Twitter is many to many by default and scales pretty well
  - But Twitter is proprietary
- RSS feeds
  - One-to-many medium: links from one source w/o selection
  - In Twitter you follow who you like and read his selection of links
- Tumblelogs
  - One-to-many medium, but not necessarily links from publisher
  - Link sharing, not messaging

# Twitter internals

- 140 chars max to be SMS compatible
  - SMS has a 160 char restriction
  - But Twitter needed to add the user name
- Message length has been hacked (fixed)
  - might cause BoFs in applications
- Users not necessarily human!
- Devices
  - From buoys to power meters
  - Search for Twitter on instructables.com
- Not surprising that malware would use it, but
  - It's not the best means of C&C communications
  - Easily blocked after detection
  - … and twitter has been trigger happy with blocking

# Twitter internals

- Historically
  - Multiple Ruby on Rails servers
  - Mongrel HTTP servers
  - Central MySQL backed
- Currently: details super-secret, but this is what we think
- Front end
  - Ruby-based front end
  - Mongrel HTTP servers
- Back end
  - Starling for queuing/messaging
  - Scala-based
  - MySQL
    - denormalized data whenever possible
    - Only for backup and persistance
  - Lots of caching (memcached)

# Stats (June 2009)

Probably old already, but here they are:

- 25M users
  - 475K different users posted over a 1 week period (Whitetwarf)
- 300 tweets/sec
- MySQL handles 2400 reqs per second
- API traffic == 10x website traffic!
  - Indicates that far more people are using applications
    - TweetDeck, Twitteriffic, Digsby, Twhirl
    - Many are Adobe Air based (!)
  - One key to Twitter's success!

# But what is ON Twitter?

- San Antonio-based market research firm Pear Analytics analyzed 2,000 tweets (originating from the US and in English) over a 2-week period from 11:00a to 5:00p (CST) and separated them into six categories:
  - News
  - Spam
  - Self-promotion
  - Pointless babble
  - Conversational
  - Pass-along value

- 40.55% of Tweets were determined to be “pointless babble”

* Paper available at http://is.gd/3xmPz

# And what is inside a Tweet?

- RT passes the note along
- L tells friends where I am
- #
  - show associations
  - show group associations
  - just for tagging
- @
  - for public discussion
  - also 'follow friday'
- links
  - URLs automatically identified

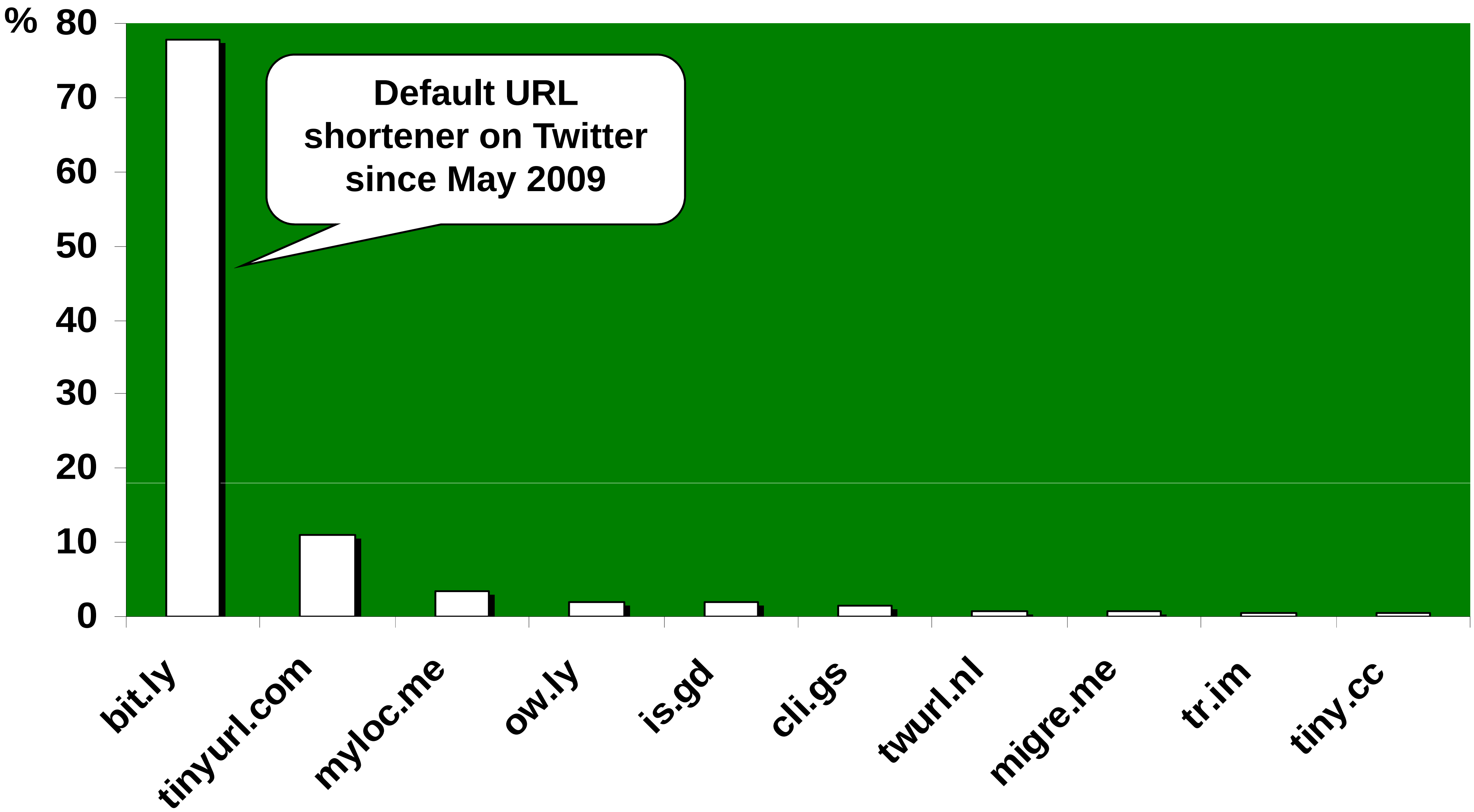
SifuMoraga: presenting together with @craiu at #vb2009 L: Geneva

schouw: RT @SifuMoraga: presenting together with @craiu at #vb2009 L: Geneva

## Long URLs, short URLs

- URLs can be long and ugly
- URL shortening services have grown up around Twitter
  - – longurl.org counts 208 different ones
- Malicious URLs are one potential threat
- URL Shorteners
  - – obscure the true URL
  - – May become malicious
  - – RickRolling, but maliciously
- Benefits:
  - – ‘bit.ly’ blocks malicious URLs

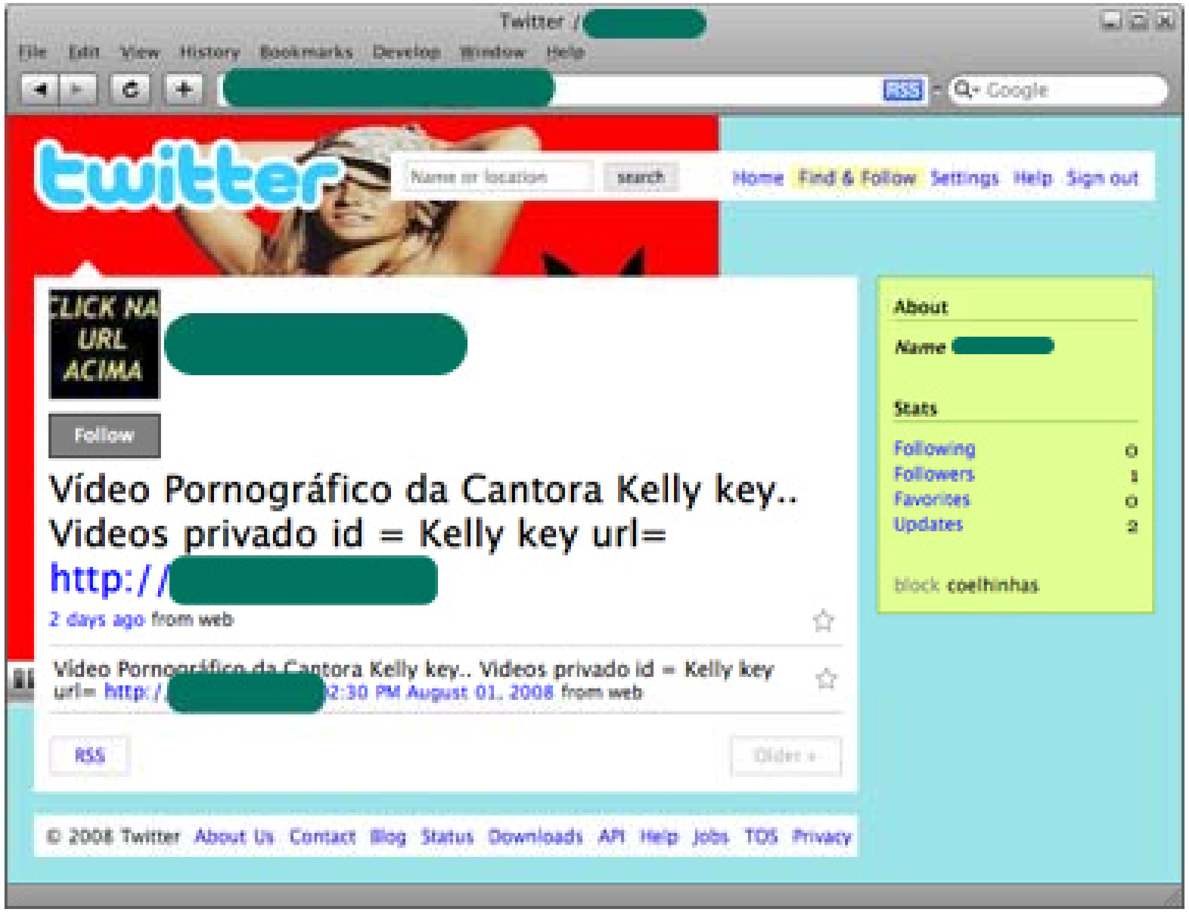
# Most popular URL shortening services



Default URL shortener on Twitter since May 2009

# Malware on Twitter

## August 2008



Twitter / [redacted]
File Edit View History Bookmarks Develop Window Help
[redacted]
RSS
Google
twitter
Name or location
search
Home Find & Follow Settings Help Sign out
CLICK NA URL ACIMA
Follow
RSS
Older »
© 2008 Twitter About Us Contact Blog Status Downloads API Help Jobs TOS Privacy

[redacted]

Vídeo Pornográfico da Cantora Kelly key.. Videos privado id = Kelly key url= http://[redacted]

2 days ago from web

Vídeo Pornográfico da Cantora Kelly key.. Videos privado id = Kelly key url= http://[redacted]2:30 PM August 01, 2008 from web

**About**

*Name* [redacted]

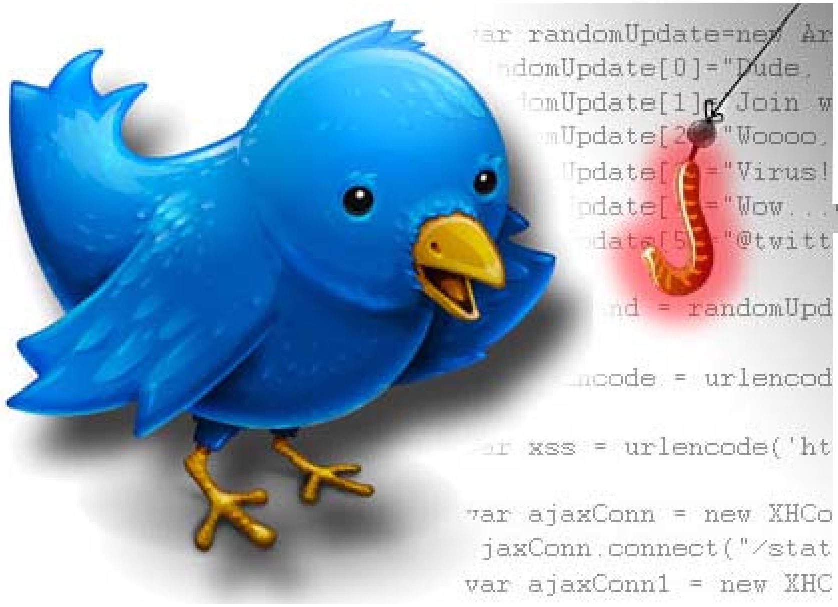
**Stats**

| | |
|---|---|
| Following | 0 |
| Followers | 1 |
| Favorites | 0 |
| Updates | 2 |

block coelhinhas

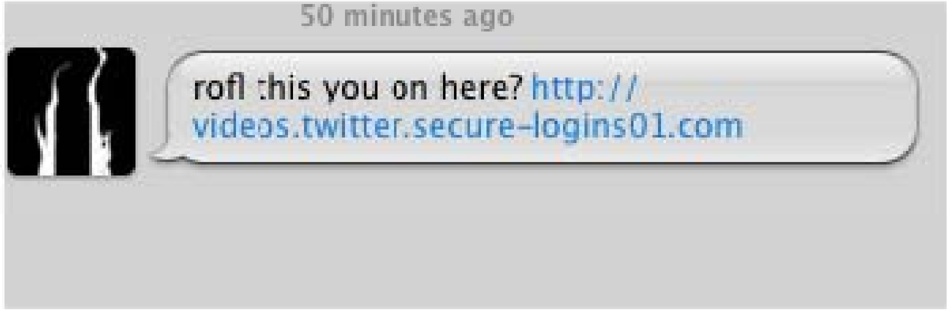
# Notable incidents

- April 2009 – Twitter gets hit by XSS worm
  - Multiple variants of the worm (JS.Twettir.a-h) were identified
  - Thousands of spam messages containing the word "Mikeyy“ filled the timeline
  - Proof of concept – no malicious intent
  - Later, the author (Mikey Mooney) got a job at exqSoft Solutions, a web security company



```
ar randomUpdate=new Ar
ndomUpdate[0]="Dude,
domUpdate[1]="Join w
mUpdate[2]="Woooo,
Update[3]="Virus!
pdate[4]="Wow...www.StalkDaily.com"
date[5]="@twitt
nd = randomUpd
ncode = urlencod
r xss = urlencode('ht
var ajaxConn = new XHCo
jaxConn.connect("/stat
var ajaxConn1 = new XHC
```

- September 2009 - Yet another attack
- Phishing for the login details

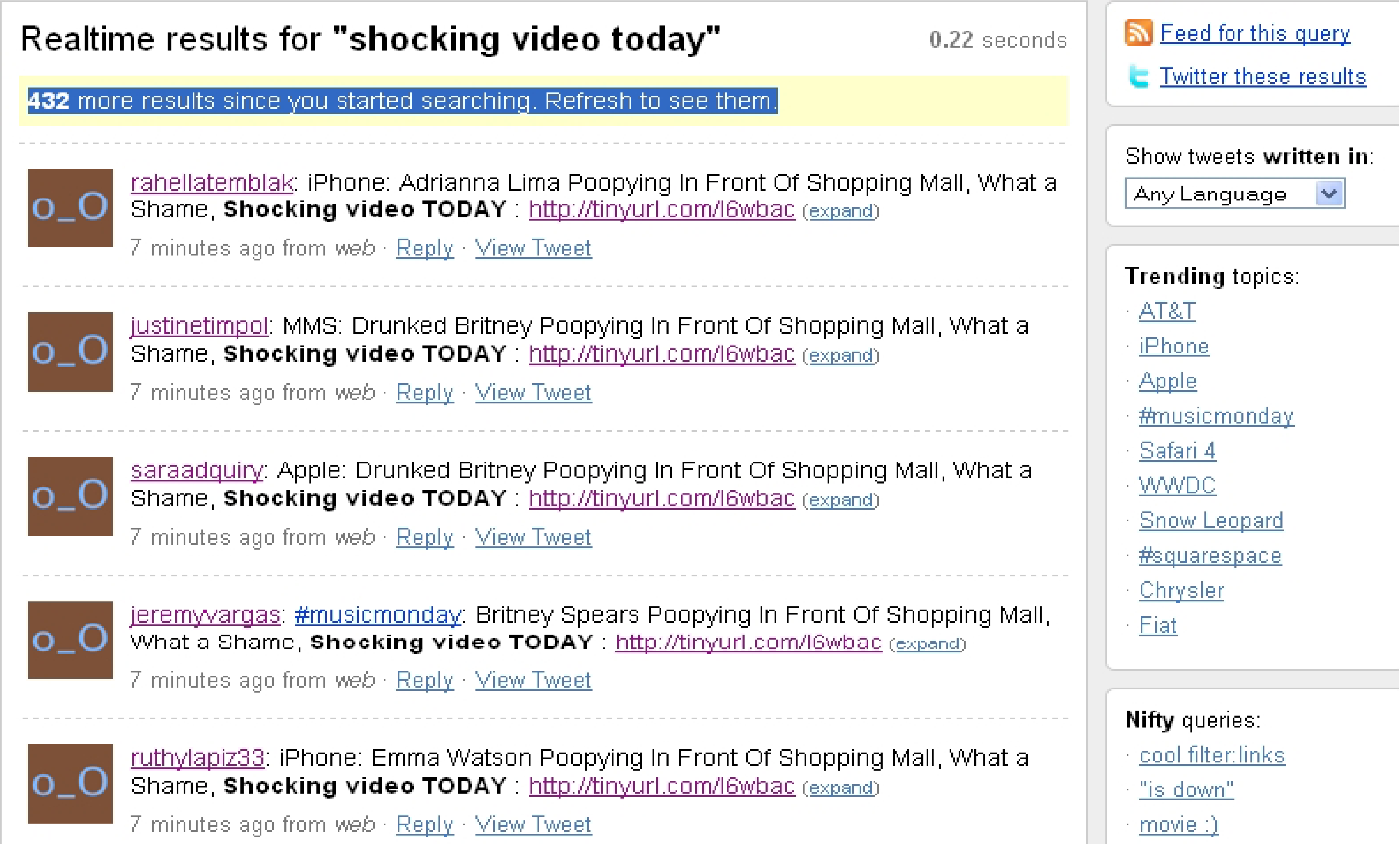


50 minutes ago

rofl this you on here? http://videos.twitter.secure-logins01.com

# Notable incidents

- June 2009 – Trending topics start being exploited



Realtime results for "shocking video today" 0.22 seconds

432 more results since you started searching. Refresh to see them.

rahellatemblak: iPhone: Adrianna Lima Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)
7 minutes ago from *web* · Reply · View Tweet

justinetimpol: MMS: Drunked Britney Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)
7 minutes ago from *web* · Reply · View Tweet

saraadquiry: Apple: Drunked Britney Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)
7 minutes ago from *web* · Reply · View Tweet

jeremyvargas: #musicmonday: Britney Spears Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)
7 minutes ago from *web* · Reply · View Tweet

ruthylapiz33: iPhone: Emma Watson Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)
7 minutes ago from *web* · Reply · View Tweet

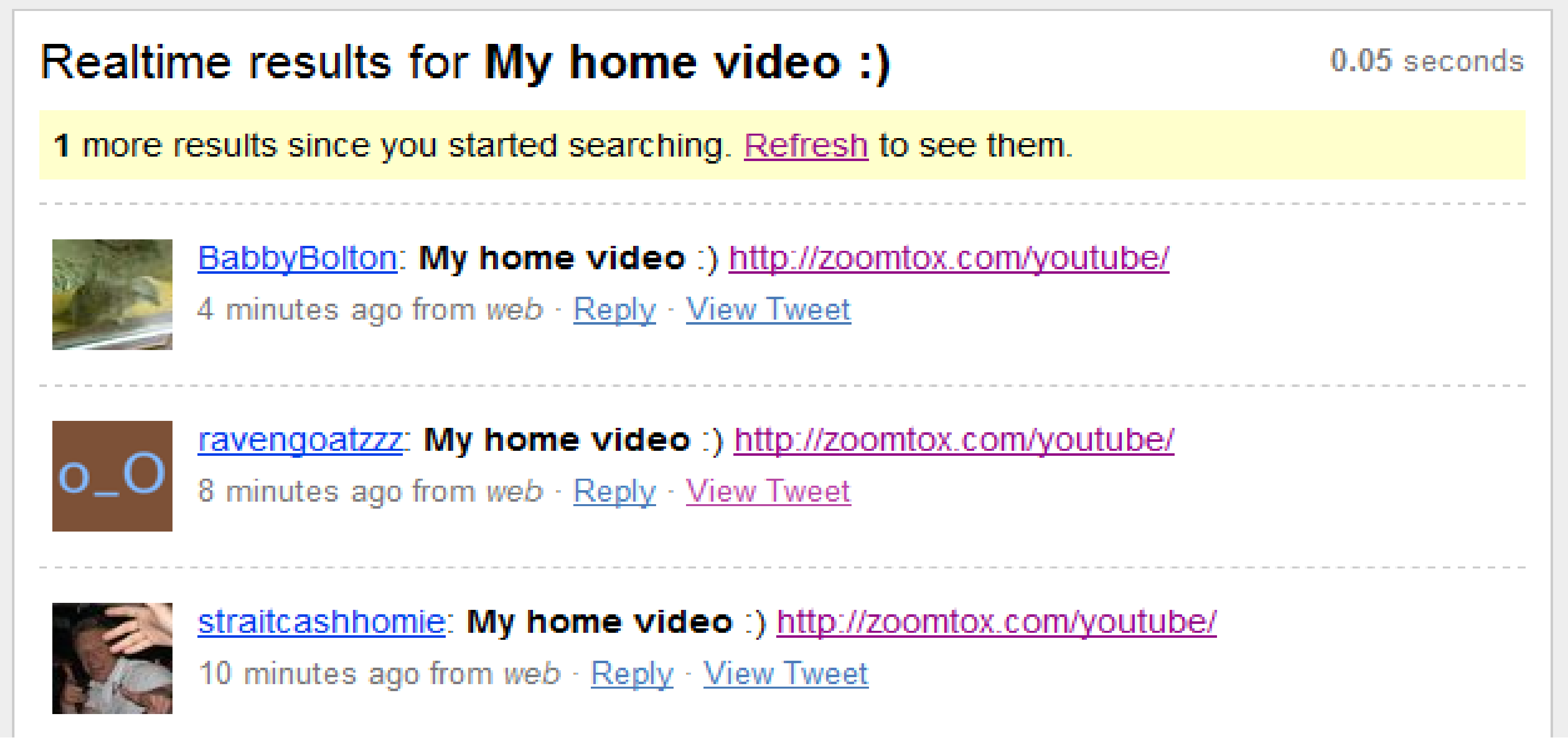
Show tweets written in: Any Language

**Trending** topics:
- AT&T
- iPhone
- Apple
- #musicmonday
- Safari 4
- WWDC
- Snow Leopard
- #squarespace
- Chrysler
- Fiat

**Nifty** queries:
- cool filter:links
- "is down"
- movie :)

# Notable incidents

- June 2009 – Koobface spreading through Twitter
- Originally, Koobface was only targeting Facebook and MySpace users
- Constantly “improved”, now spreading through more social networks: Facebook, MySpace, Hi5, Bebo, Tagged, Netlog and most recently… Twitter



Realtime results for **My home video :)** 0.05 seconds

**1** more results since you started searching. Refresh to see them.

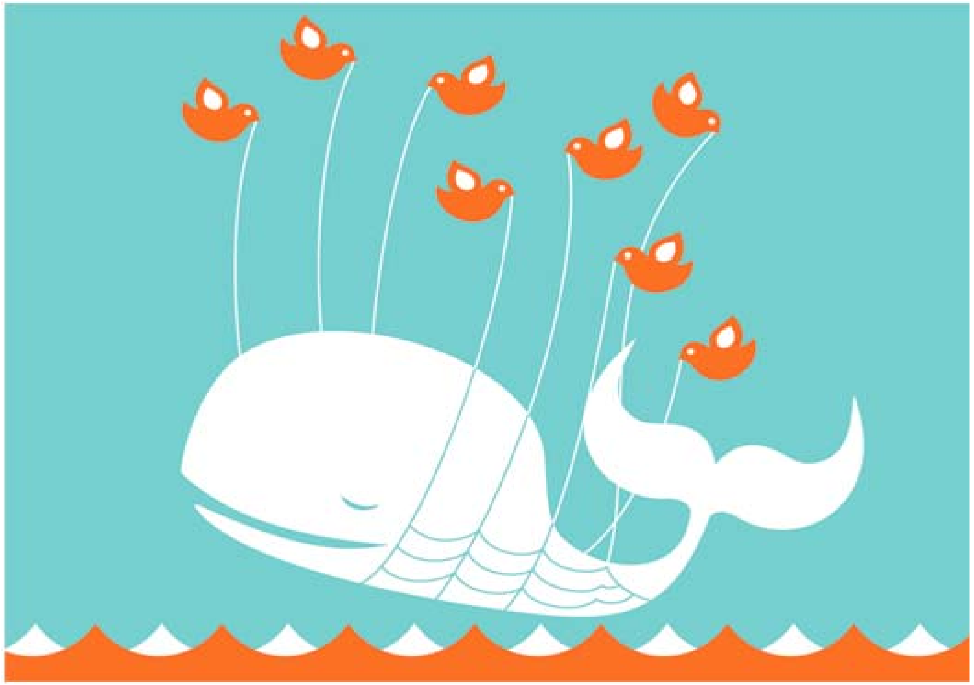
BabbyBolton: **My home video** :) http://zoomtox.com/youtube/
4 minutes ago from *web* · Reply · View Tweet

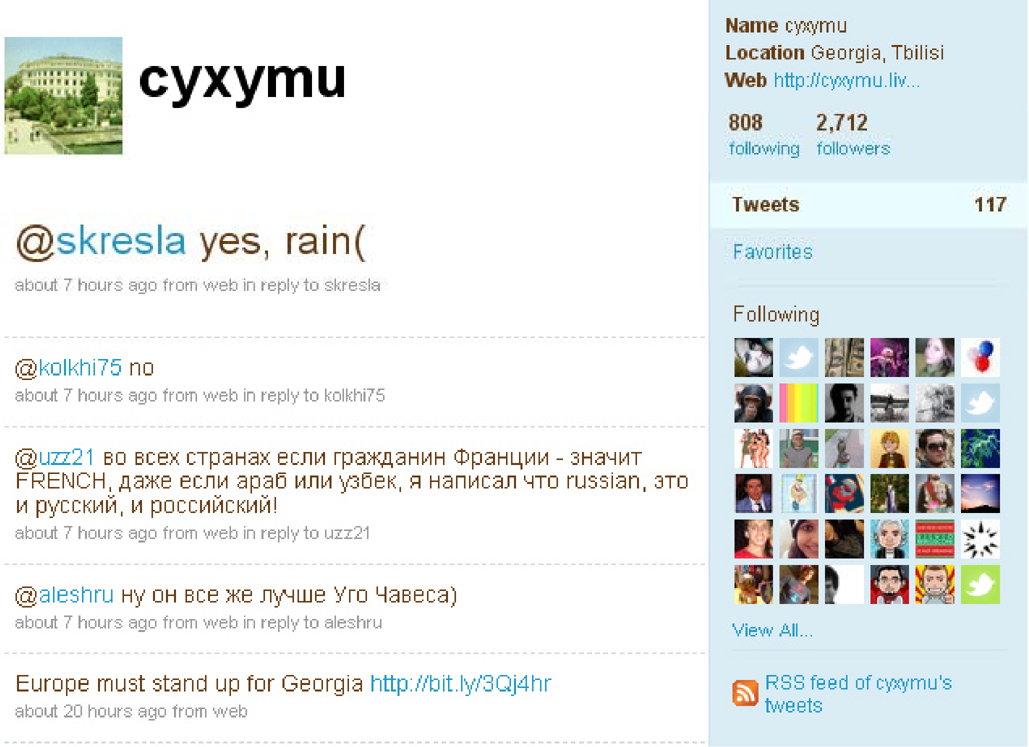
ravengoatzzz: **My home video** :) http://zoomtox.com/youtube/
8 minutes ago from *web* · Reply · View Tweet

straitcashhomie: **My home video** :) http://zoomtox.com/youtube/
10 minutes ago from *web* · Reply · View Tweet

# Notable incidents

- August 6, 2009 – massive DDoS attack against Twitter (and others)
- Twitter knocked offline for several hours, API problems lasted for days
- Reason: to silence a relatively unimportant blogger in Georgia (really?)





cyxymu

@skresla yes, rain(

about 7 hours ago from web in reply to skresla

@kolkhi75 no

about 7 hours ago from web in reply to kolkhi75

@uzz21 во всех странах если гражданин Франции - значит FRENCH, даже если араб или узбек, я написал что russian, это и русский, и российский!

about 7 hours ago from web in reply to uzz21

@aleshru ну он все же лучше Уго Чавеса)

about 7 hours ago from web in reply to aleshru

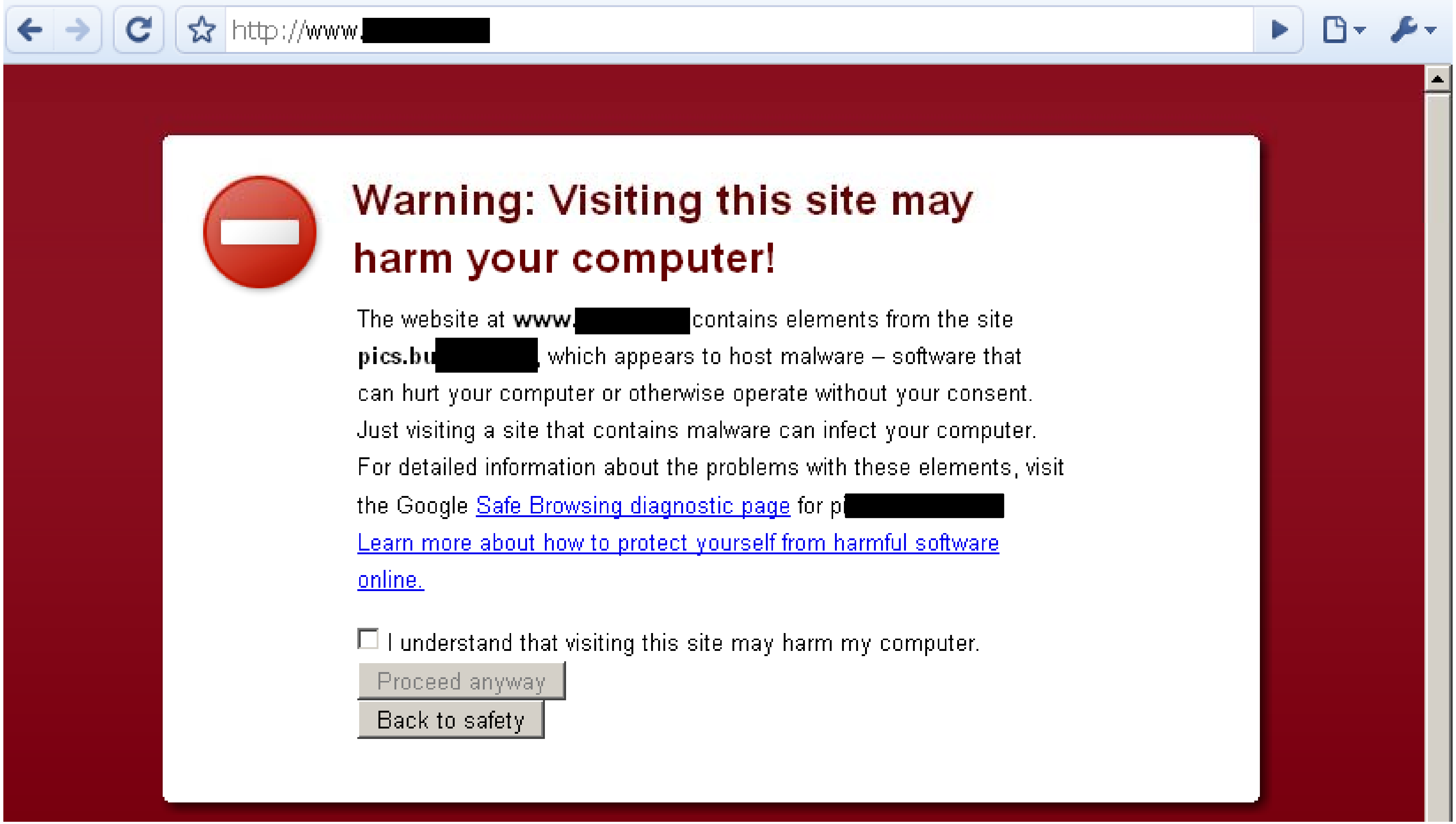
Europe must stand up for Georgia http://bit.ly/3Qj4hr

about 20 hours ago from web

**Name** cyxymu
**Location** Georgia, Tbilisi
**Web** http://cyxymu.liv...

808 following 2,712 followers

# Twitter and Google SB API



http://www.[redacted]

## Warning: Visiting this site may harm your computer!

The website at **www.**[redacted] contains elements from the site **pics.bu**[redacted], which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

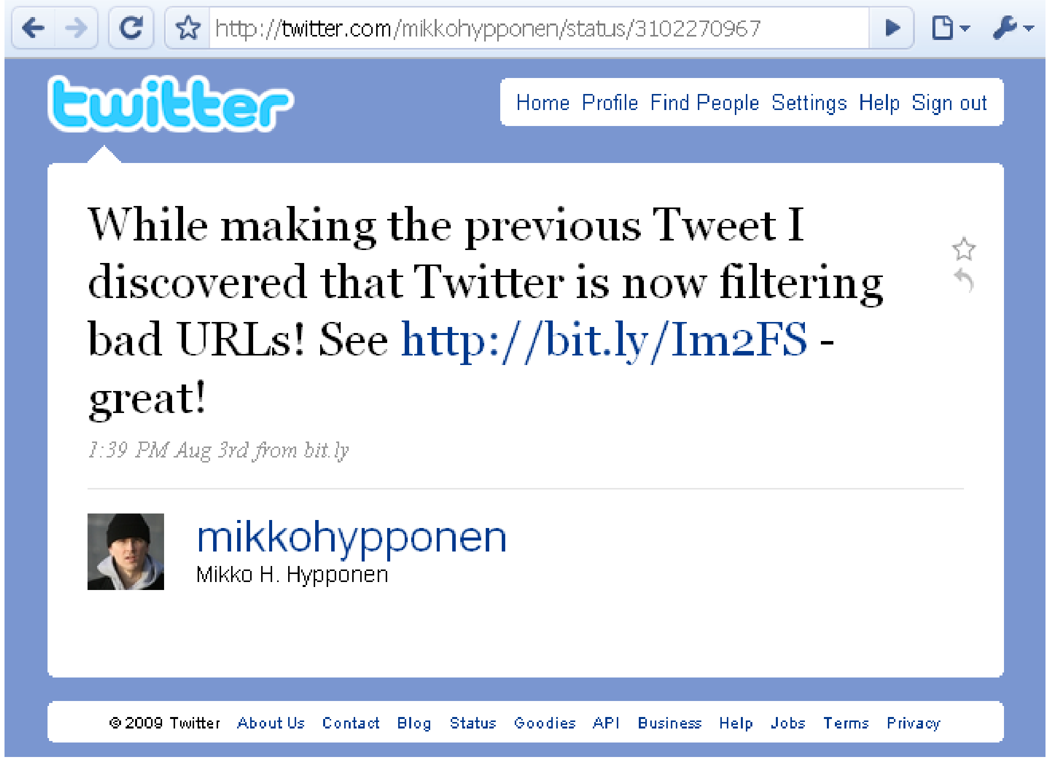
For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for p[redacted]

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

# Google SB API

- In August 2009, Twitter began filtering malicious URLs
  - – Mikko Hypponen:
- Initial testing seemed to indicate Google SB API!
- But after a bit more testing, we discovered it is SB API but with some additional filtering


http://twitter.com/mikkohypponen/status/3102270967
twitter
Home Profile Find People Settings Help Sign out

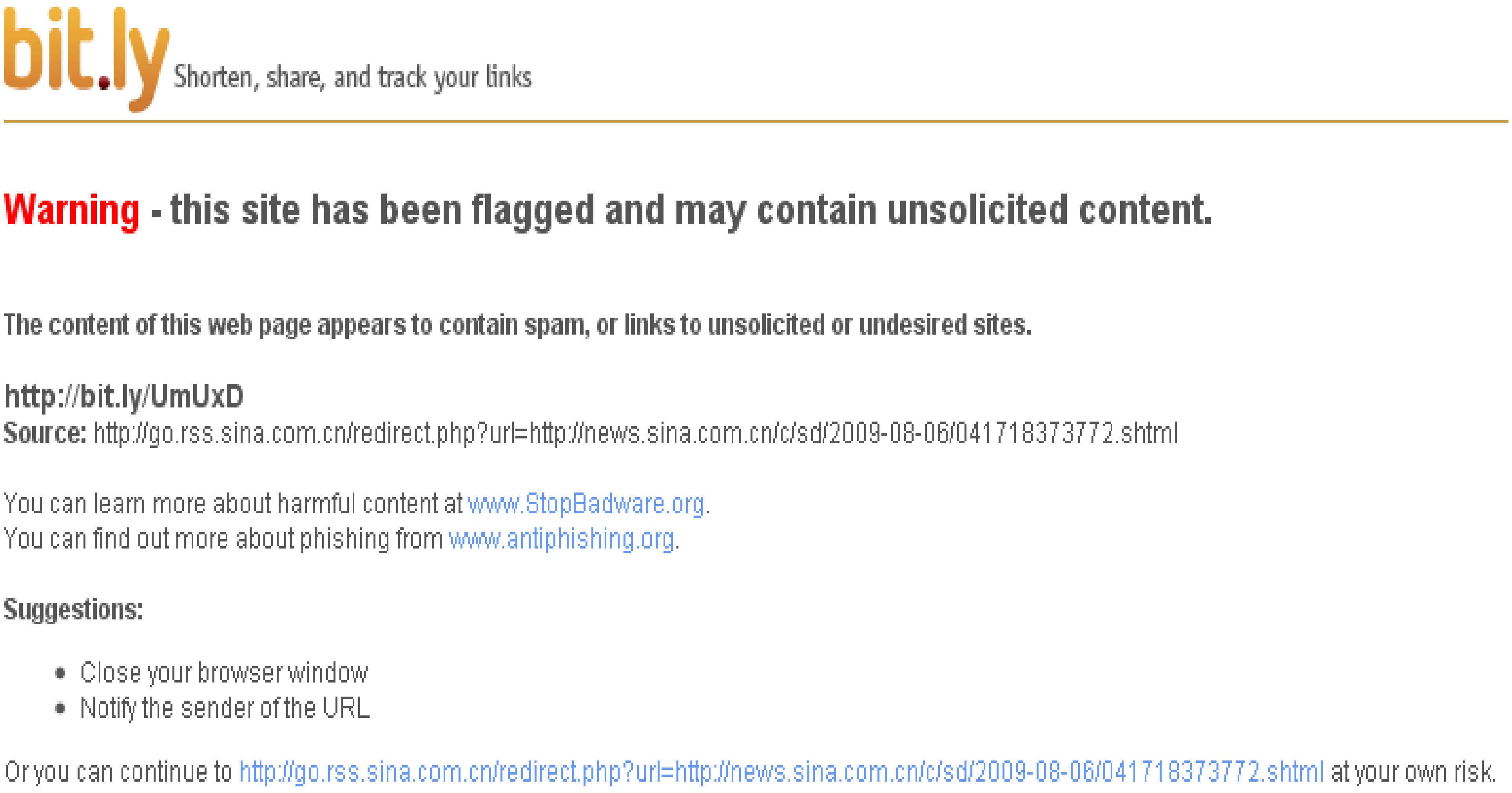
While making the previous Tweet I discovered that Twitter is now filtering bad URLs! See http://bit.ly/Im2FS - great!

1:39 PM Aug 3rd from bit.ly

mikkohypponen
Mikko H. Hypponen

© 2009 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy

# A bit about ‘bit.ly’ / ‘j.mp’



bit.ly Shorten, share, and track your links

**Warning - this site has been flagged and may contain unsolicited content.**

**The content of this web page appears to contain spam, or links to unsolicited or undesired sites.**

**http://bit.ly/UmUxD**
**Source:** http://go.rss.sina.com.cn/redirect.php?url=http://news.sina.com.cn/c/sd/2009-08-06/041718373772.shtml

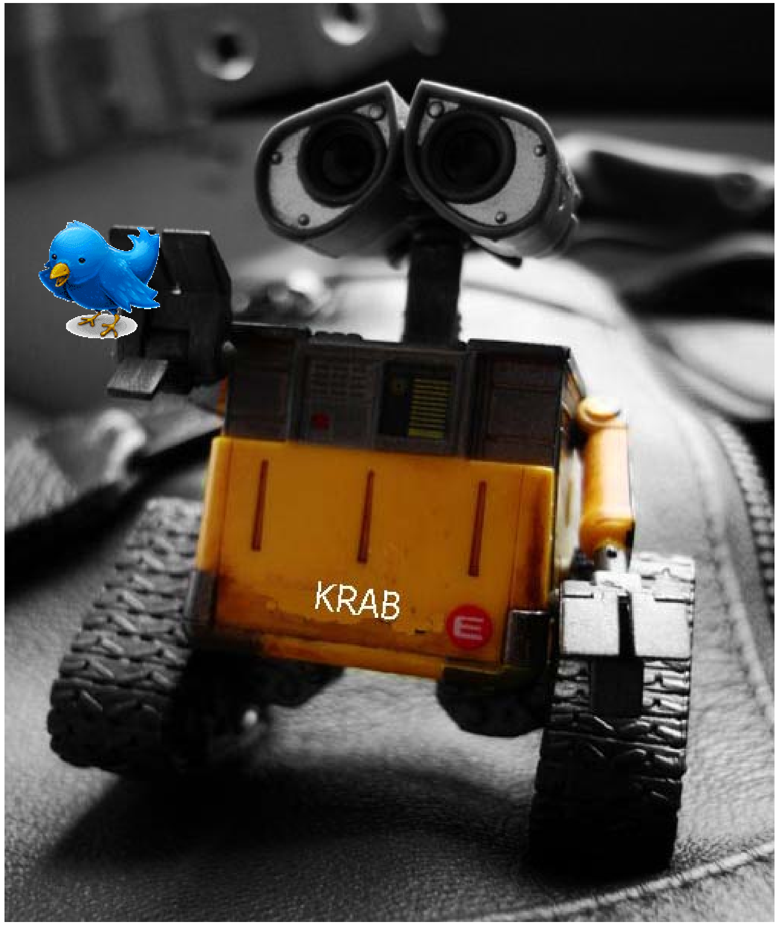
You can learn more about harmful content at www.StopBadware.org.
You can find out more about phishing from www.antiphishing.org.

**Suggestions:**

- Close your browser window
- Notify the sender of the URL

Or you can continue to http://go.rss.sina.com.cn/redirect.php?url=http://news.sina.com.cn/c/sd/2009-08-06/041718373772.shtml at your own risk.

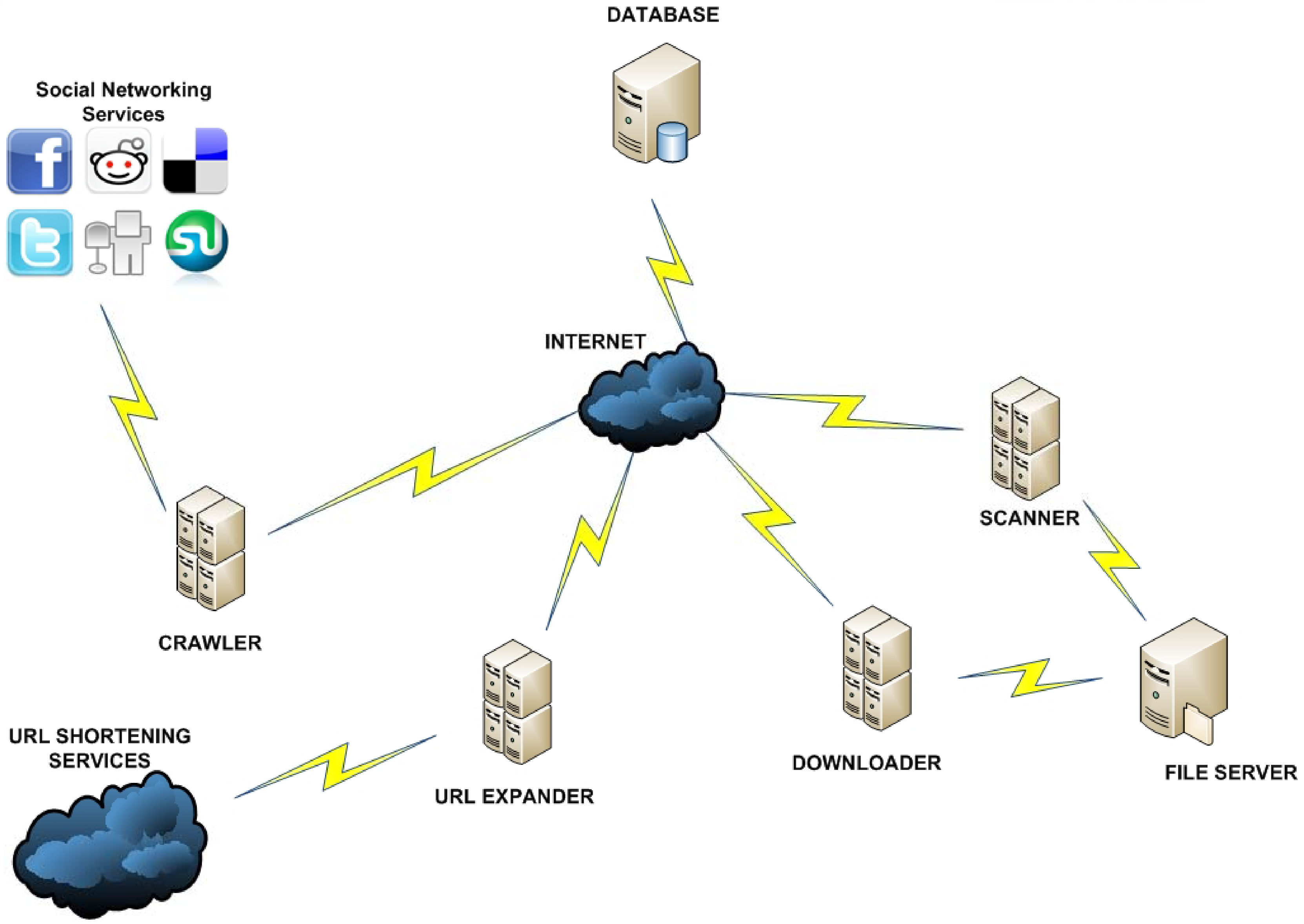
# Our Robot(s) – Krab Krawler



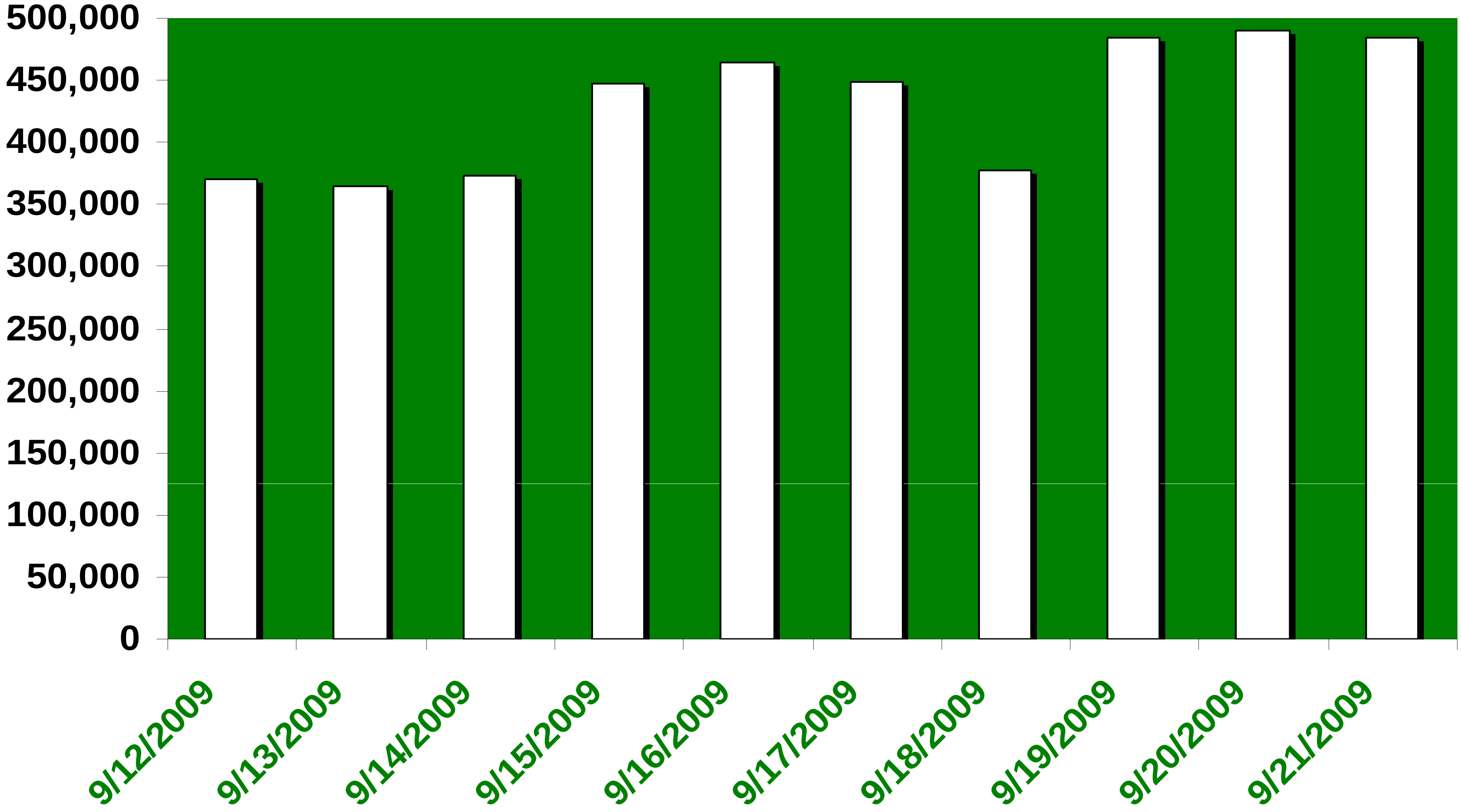
# Kaspersky Robot

- Codenamed: Krab Krawler
- Specs: Linux + PHP + MySQL
- Operation: It continuously fetches the Twitter public timeline on multiple threads, extracts URLs and injects them into a DB
- Target: URLs are analysed and expanded if necessary
- Execution: Modules check the URLs for malware
- Design: Costin G. Raiu, Stefan Tanase
- Assembly: Selma Ardelean, Dan Demeter, Alexandru Tudorica

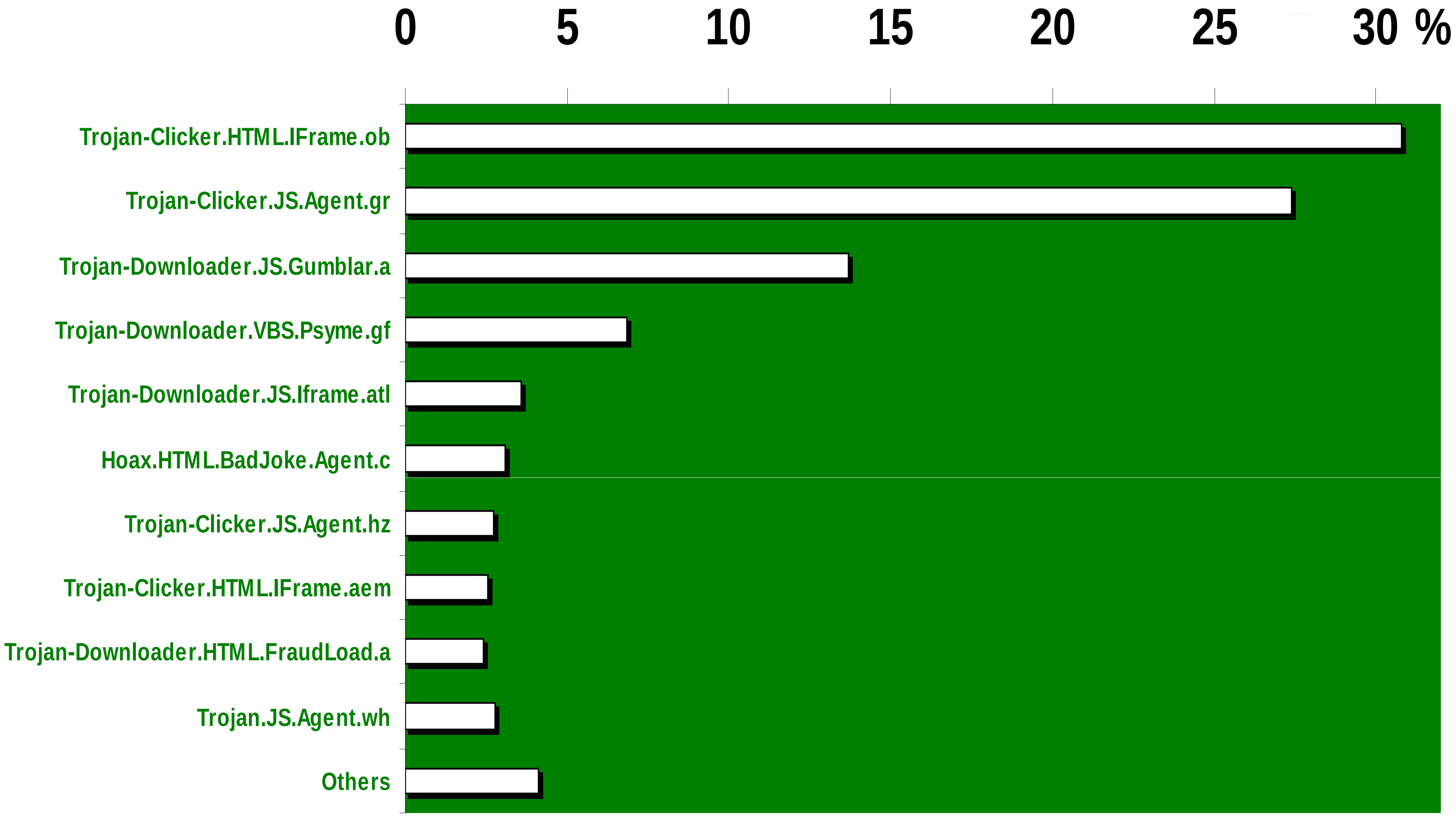
# Krab Krawler: Architecture



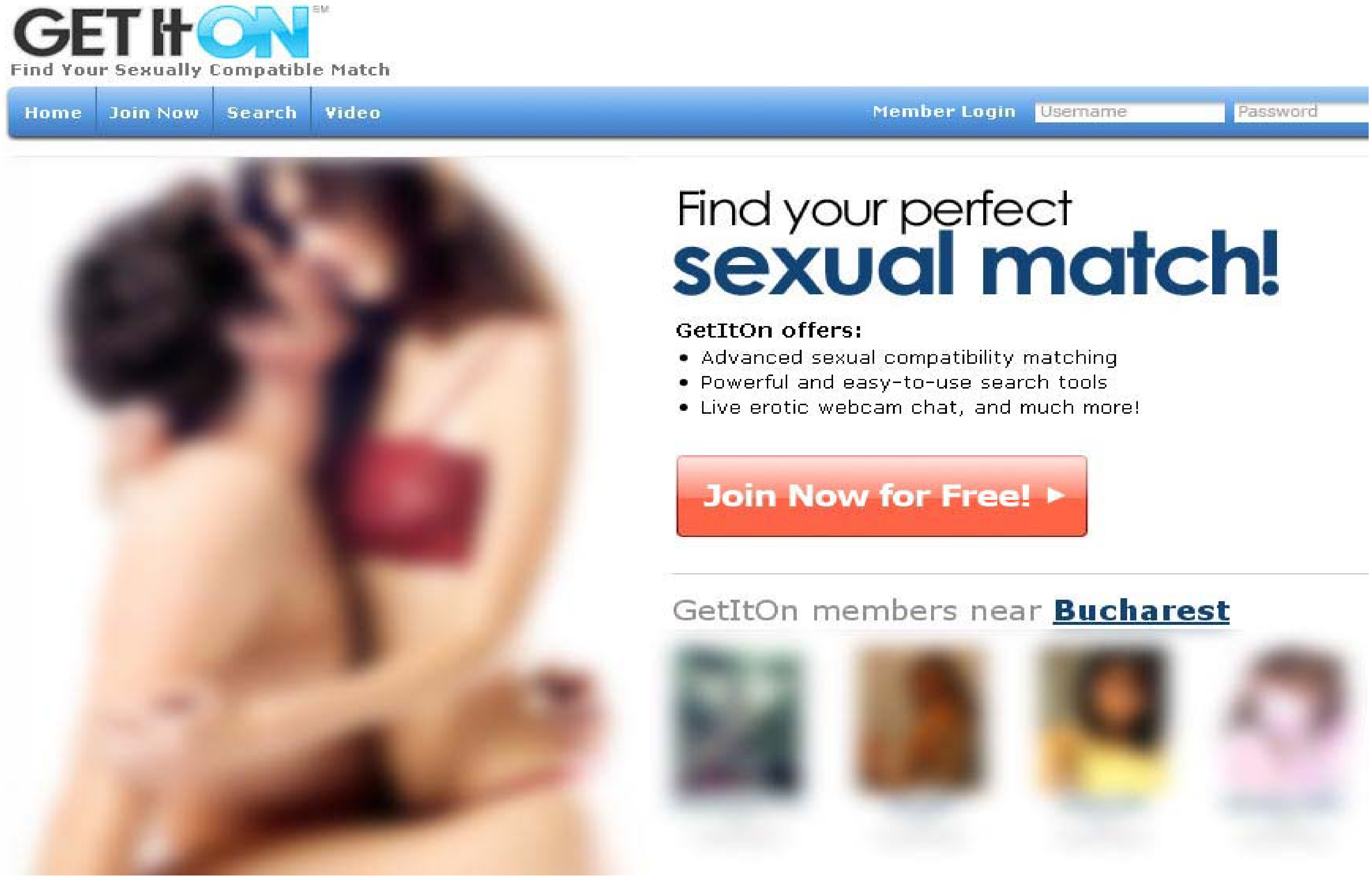
# New unique URLs per day



# Malware we found so far



# General stats



Find Your Sexually Compatible Match

Find your perfect **sexual match!**

**GetItOn offers:**

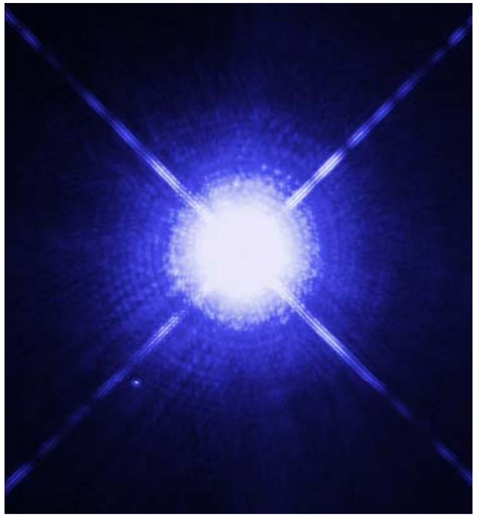
- Advanced sexual compatibility matching
- Powerful and easy-to-use search tools
- Live erotic webcam chat, and much more!

GetItOn members near **Bucharest**

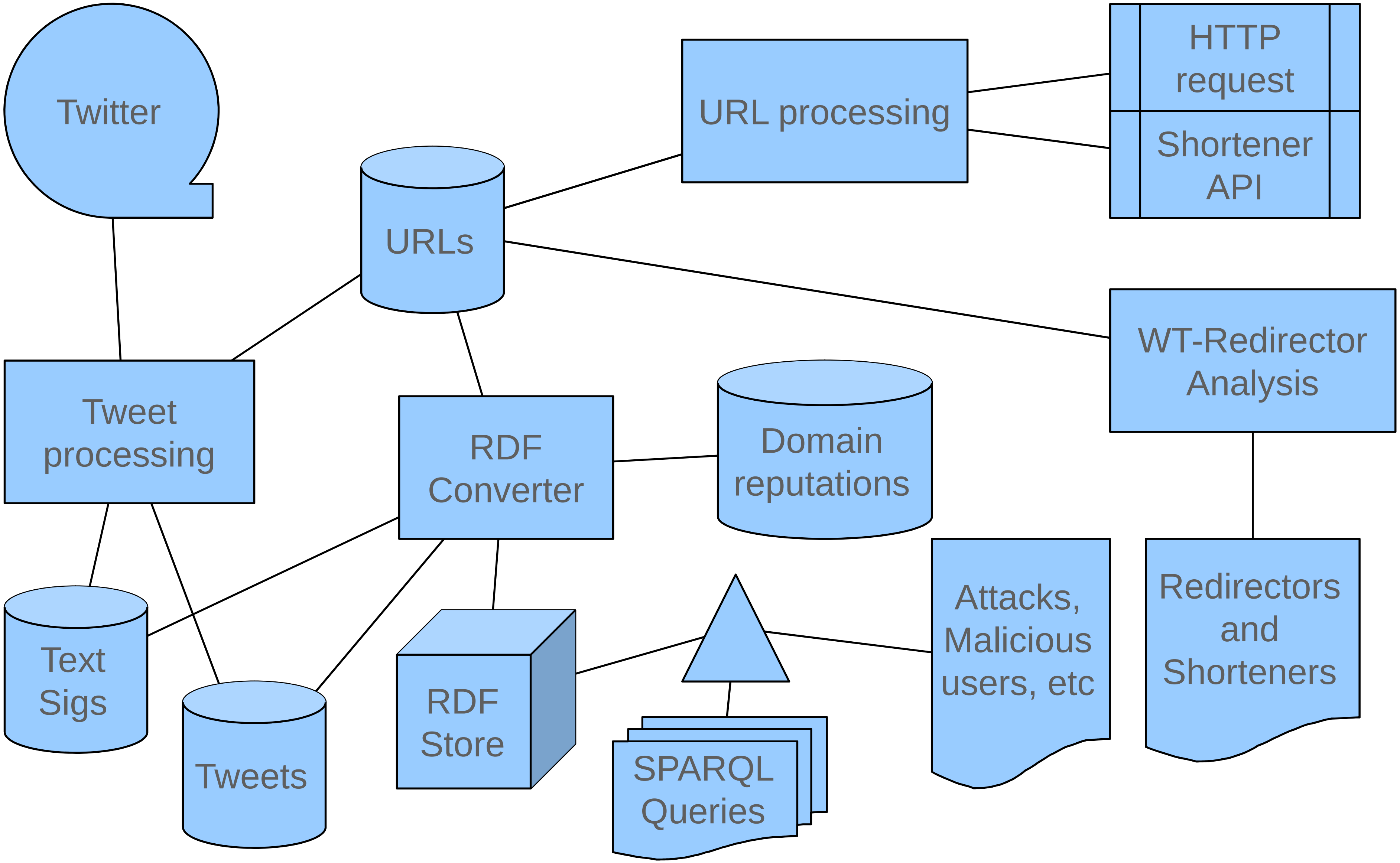
# Our Robot(s) – Red Twarf

# Whitetwarf

- An early prototype system
- Receives a subset of the tweets via twitter search
- Stores external metadata from twitter
- Processes text part for internal metadata
  - User references, hashtags, Informal tags
- Creates canonical text representations
- Export to an RDF store for analysis
- Hard coded detection of attacks



# WhiteTwarf – the exploratorium



# WhiteTwarf in detail

- Tweet Processing phase
  - loop forever
    - Fetch a limited number of tweets
      - These come back as JSON code
    - Extract metadata
    - Enter this into the database
    - then we wait adaptively before doing this again
  - from the tweets, we extract
    - Tags, URLS, user references
    - Text signatures
      - Meant to remove small differences in text
      - Normalization and whitespace removal
      - UTF-8 tricks expansion/removal
      - Keyword extraction (future)
    - other metadata

# URL redirector processing

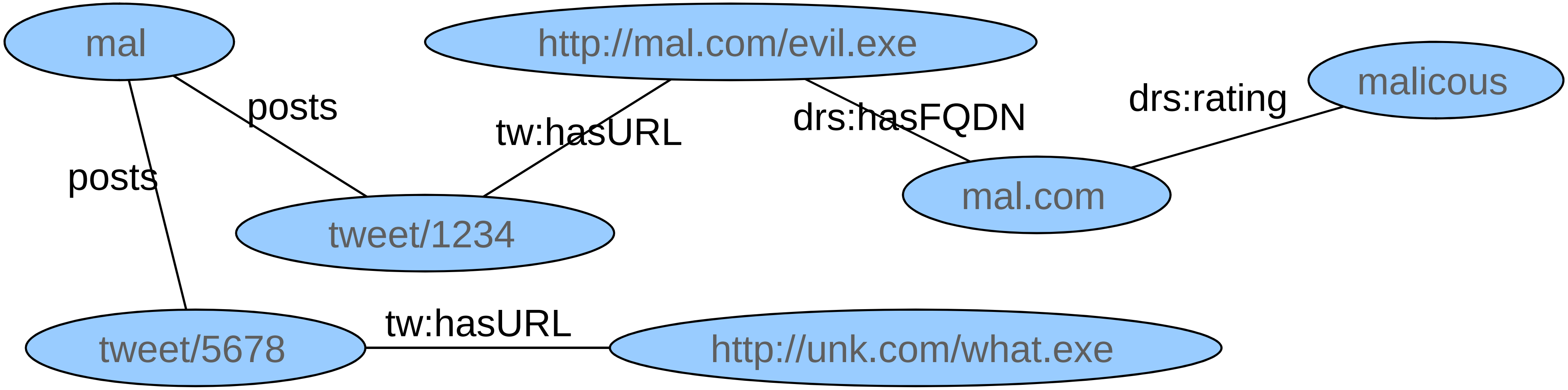
- For every URL entered into the DB we follow the link
- With a HEAD request
- In most cases we get a 30x response
- These get entered into the DB for further processing
- Testing showed that it is usually faster to use shortener APIs
- So we are testing code that will ID shorteners and use API instead of HEAD
- We also capture other HTTP metadata
- Basically we are looking for possible file downloads

# The next stage: RedTwarf

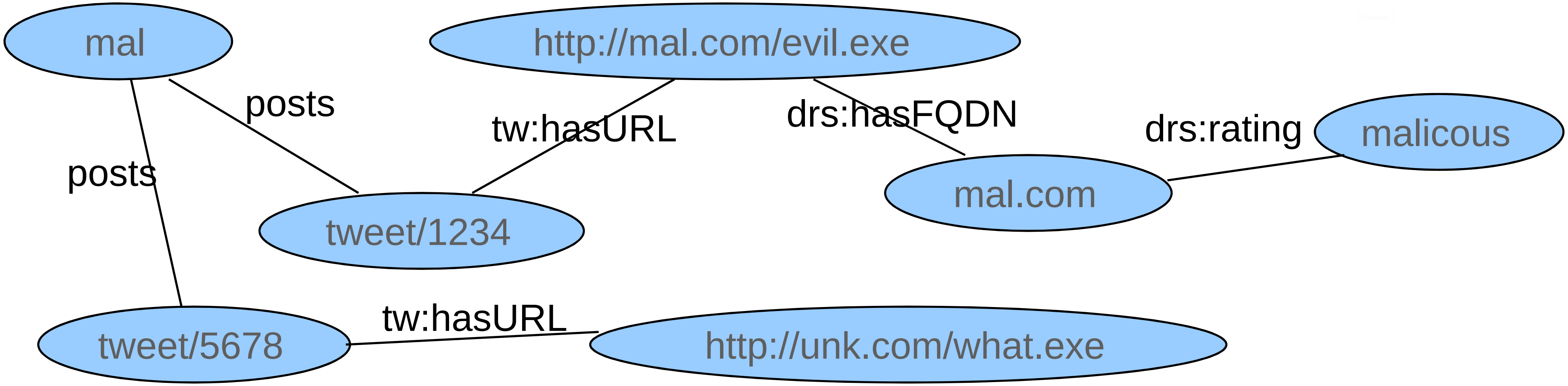
- Will capture the entire Twitter feed
- Goal: looking for new attack patterns
- Based on same data as in WhiteTwarf
- Using Text-mining techniques to detect rules

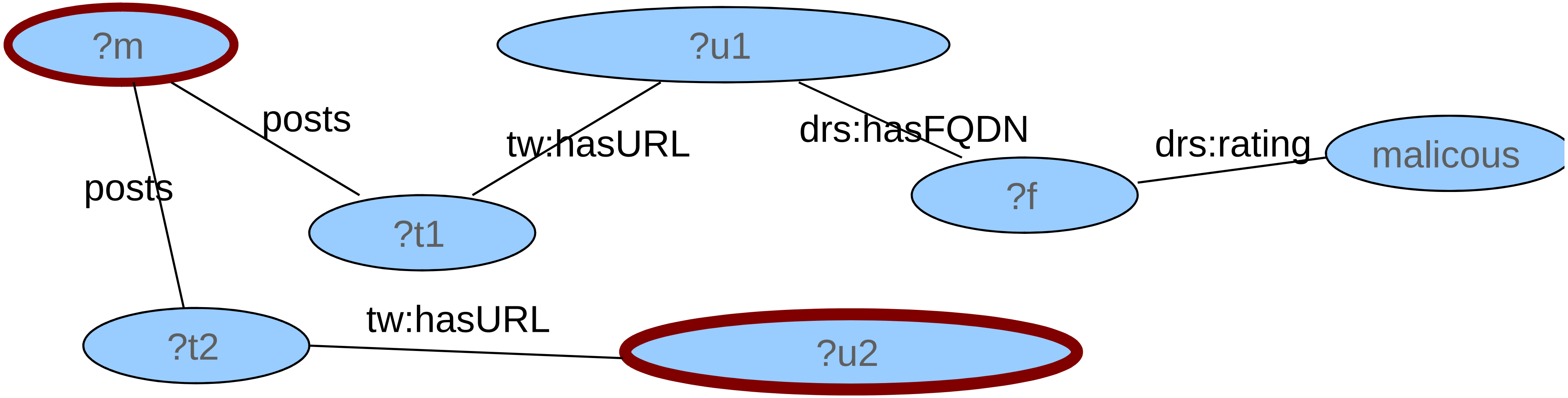
# Detection malicious activity

- Data exported to an RDF Store
  - This is a graph database
  - Allows for complex queries
  - Does have some performance issues and is not real time
- Simple Attack scenario
  - User is observed to post to a malicious domain
  - We want to see what else he has posted



# Matching graphs



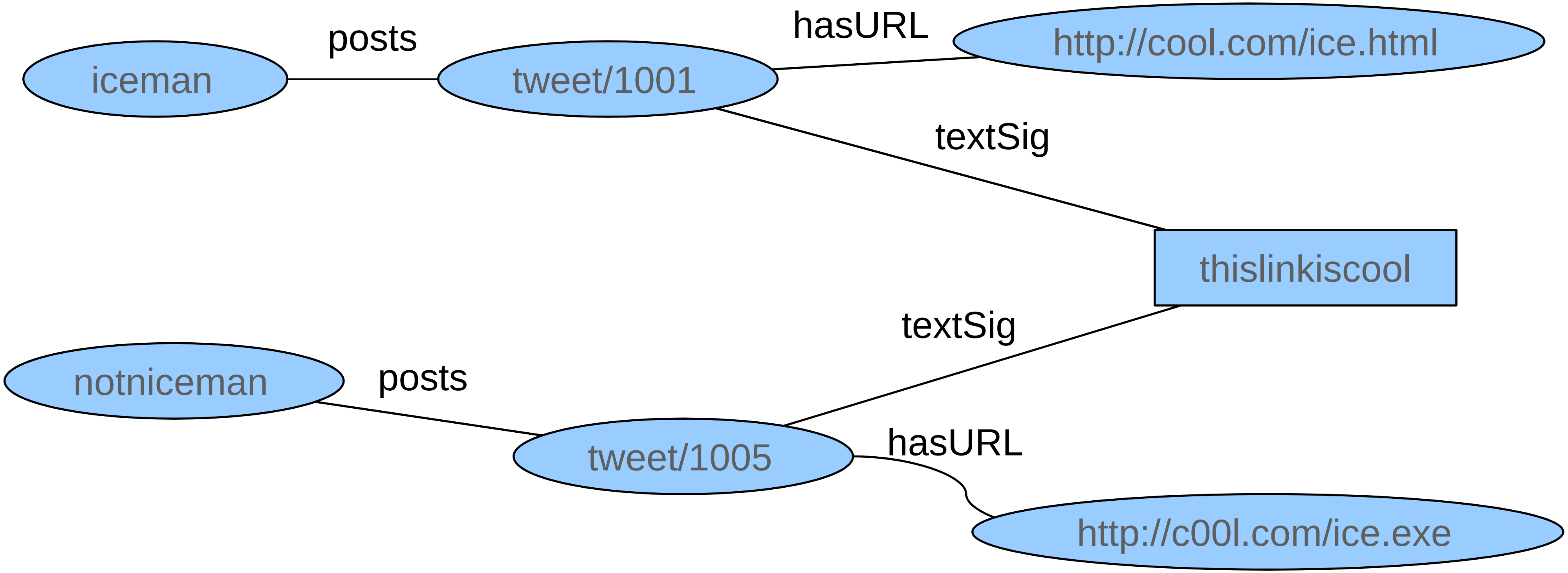


# More complex attack

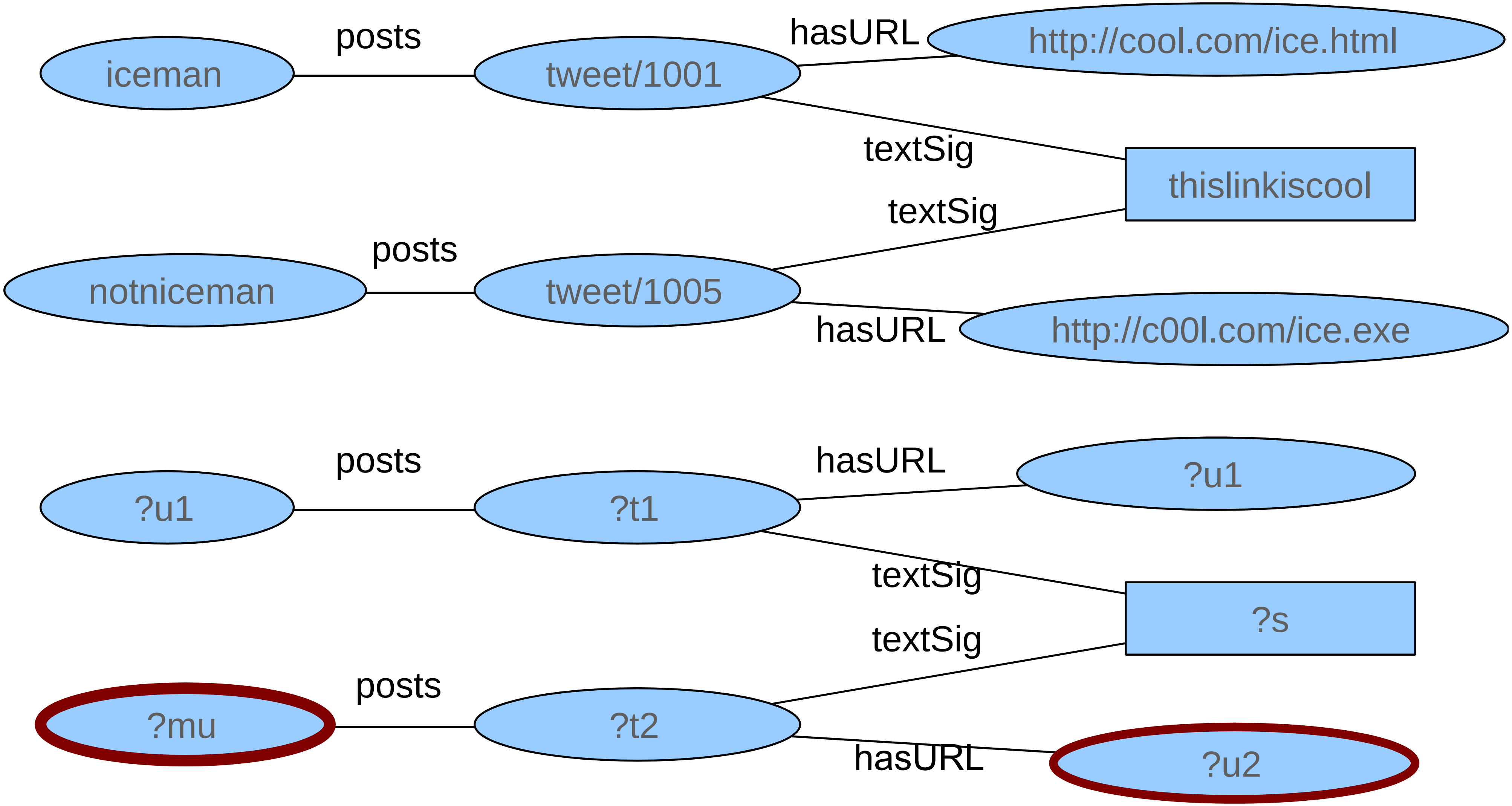
Observed: User modified URL on retweet to be malicious

```
@iceman: This link is cool
http://cool.com/ice.html
```

```
@notniceman: RT: @iceman: This link
is cool http://c00l.com/ice.exe
```



# Matching Graphs



# Conclusions

- Twitter is becoming a popular attack vector
- Two approaches to detecting threats broadcast via Twitter
- There are serious security dependencies due to the URL Shorteners
- Common goal: protecting you, our customers
- Identifying the future development directions of Twitter threats

We would like to thank VB and the charming audience for your support with 140 characters and guess what, we just did it! #vb2009

# Thank you!

morton@swimmer.org
twitter.com/sifumoraga

craiu@kaspersky.ro
twitter.com/craiu