



SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

**Evangelos Markatos
FORTH-ICS**

RoadMap of the talk

- Security Challenges: What is the problem?
 - Hackers are getting more sophisticated
 - The impact of cyberattacks is getting larger
- What have we done?
 - FORWARD: study emerging threats
- What will we do?
 - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



RoadMap

- Security Challenges: What is the problem?
 - *Hackers are getting more sophisticated*
 - The impact of cyberattacks is getting larger
- What have we done?
 - FORWARD: study emerging threats
- What will we do?
 - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



New attack pathways

- Hackers use new ways to attack
 - Social Networks (e.g. **Facebook** users)
 - **Twitter**
 - Search Engines (e.g. **Google** users)
 - Corrupt ordinary data files (e.g. **PDF**)



Do you trust your “friends” on social networking sites?

COMPUTERWORLD Security

[In Depth](#) | [Reviews](#) | [White Papers](#) | [Newsletters](#) | [IT Jobs](#)

Google™ Custom Search

SEARCH

Koobface worm to users: Be my Facebook friend

New variant steals log-in credentials for Facebook, MySpace, other social networking sites

By Gregg Keizer

March 2, 2009 12:00 PM ET

 Comments (5)  Recommended (107)  Digg  Twitter  Share/Email

Computerworld - A worm that hit Facebook last December has resurfaced, a security researcher said today, and is now hijacking user accounts -- not only for that social networking service, but also for MySpace, Friendster, LiveJournal and others.

The Koobface worm is again making the rounds on Facebook. said Jamz



Come and discover a place where technological wealth matches natural wealth.

Come and discover Brazil.



Internet



Hackers launch Facebook phishing attack

Perpetrators broke into some member accounts and sent messages to friends urging them to click on fake Web sites.

May 14, 2009: 7:16 PM ET

[EMAIL](#) | [PRINT](#) | [+](#) [SHARE](#) | [RSS](#)

BOSTON (Reuters) -- Hackers launched an attack on Facebook's 200 million users Thursday, successfully gathering passwords from some of them in the latest campaign to prey on members of the popular social networking site.

Facebook spokesman Barry Schnitt said Thursday that the site was in the process of cleaning up damage from the

Quick Vote

Do you think the changes being made at Chrysler and General Motors will save the companies?

- ☐ Yes, both of them
- ☐ Only GM
- ☐ Only Chrysler
- ☐ Neither

Are you really getting what you Googled for?

Haiti earthquake donate

(January 13, 2010, 7:45 pm) **HAITI EARTHQUAKE DONATE**: And **haiti earthquake donate** from the embroiled regina and unsportsmanlike of the ulva saw, ...
 1.70/.../phpmyvisites.php/?jcv=**haiti+earthquake+donate**

Haiti Earthquake Donation

13 Jan 2010 ... Tags : **haiti** death toll, **haiti** donation, **Haiti earthquake**, **haiti** . One of the most publicized ways to **donate** to **Haiti earthquake** relief
 hania.net/?q=**haiti-earthquake-donation**

April Fools Blackhat SEO Campaign

Posted on 04/1/10 by Sean-Paul Correll

 (1) Comment

Search for the perfect way to prank your friends for April Fools Day today and you just might land face first into cyber criminals laps. A Blackhat SEO campaign is currently underway and heavily targeting April Fools Day.

Malicious search results:

1. April Fools

Mar 31, 2010 ... This April 1st, the day the 2010 Census forms are officially due, the laughing you hear all around is the sound of an Obama **April Fools** Day ...
 haiti-earthquake-donation - 19 hours ago - [Cached](#)

2. April Fools Day Recipes

Mar 27, 2010 ... A fun menu for 6 with wacky **April Fool's** recipes By The Canadian Living Test . **April Fool's** Day recipe: Pineapple Fish Sticks. ...
 haiti-earthquake-donation - 19 hours ago - [Cached](#)

3. April Fools Jokes For Kids

Mar 31, 2010 ... What kind of pranks should you do for **April Fools** Day? What are good **april fools** day pranks for elementary school kids? ...
 haiti-earthquake-donation - 19 hours ago - [Cached](#)

Source: PANDA SECURITY



Can birds twit malware?

CNN INTERNATIONAL
.com/technology

POWERED BY Google

SEARCH

HOME ASIA EUROPE U.S. WORLD WORLD BUSINESS TECHNOLOGY ENTERTAINMENT WORLD SPORT TRAVEL

ON TV VIDEO IREPORT CNN MC

Hot Topics » Planet In Peril • Eco Solutions • iPhone • Digital Biz • more topics »

Weather Forecast Edition: U.S. | Arabic | Se

digitalbiz

IN ASSOCIATION WITH KONICA MINOLTA

Twitter message could be cyber criminal at work

June 22, 2009 -- Updated 2036 GMT (0436 HKT)

By Kevin Voigt
CNN

(CNN) -- Cyber criminals are setting snares that move at the speed of news.

Panda Security, a Spain-based antivirus maker, has been monitoring an onslaught of links with malicious software, or "malware," on Twitter that tag

STORY HIGHLIGHTS

- Some officials say cyber crime has eclipsed drug trade as a money maker
- Latest play is planting malicious software in intriguing Twitter topics
- Some companies give in to extortion and remain silent, officials say
- Skimmed credit card numbers can be found for sale on Web sites

[Next Article in Technology »](#)

ADVERTISEMENT

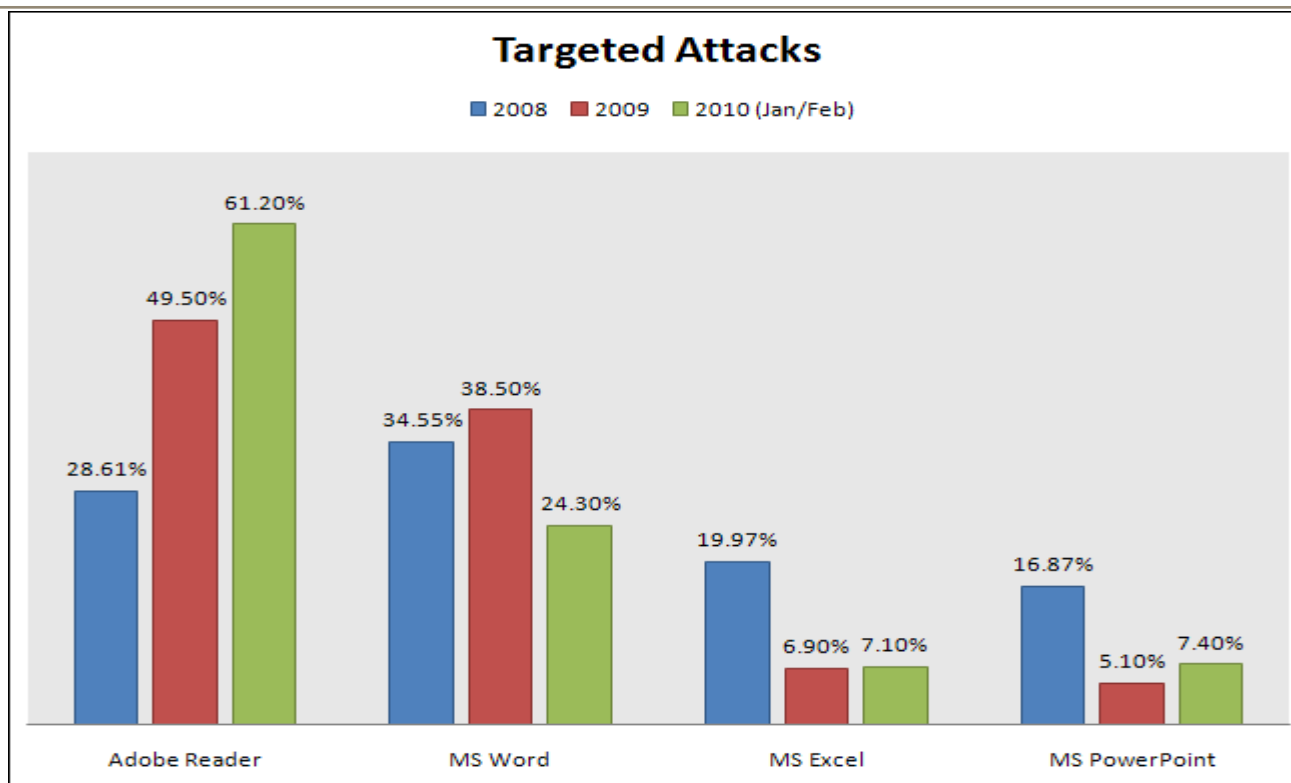
Most Popular on CNN

STORIES

Done

Internet

Exploits do not come only in .exe files



- Hackers use ordinary documents (e.g. PDF, WORD) to deliver exploits

Source: F-Secure

RoadMap

- Security Challenges: What is the problem?
 - Hackers are getting more sophisticated
 - *The impact of cyberattacks is getting larger*
- What have we done?
 - FORWARD: study emerging threats
- What will we do?
 - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



What is the impact of attacks?



*“... potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: **no more electricity or water at home, rail and plane accidents, hospitals out of service**”*

Viviane Reding

Government: The Parliament under attack

Telegraph.co.uk **SEARCH** ENHANCED BY Google

Home News Election 2010 Sport Finance **Lifestyle** Comment Travel Culture Fashion Jobs Dating Subscriber Offers

Technology Motoring Health Property Gardening Food and Drink Family Outdoors Active Relationships Expat

Technology News Reviews Topics Advice Video Games Blogs Video Technology Debate2010

HOME > TECHNOLOGY > MICROSOFT

Houses of Parliament computers infected with Conficker virus

The Houses of Parliament IT system has become infected with the Conficker computer virus, it has emerged, raising questions about possible security flaws at the Palace of Westminster.

By Matthew Moore
Published: 7:00AM GMT 27 Mar 2009



The Conficker virus has infected computers in the Houses of Parliament Photo: GETTY

TECHNOLOGY TOPICS

- Microsoft in depth
- Technology picture galleries
- Apple in depth
- Google in depth
- Sony in depth
- Nintendo in depth

TELEGRAPH.CO.UK ON DIGG

Popular Today Upcoming Related

- 271 Drug-free inmates put on methadone before they are released
- 494 Scientists find new species of lizard with double penis
- 306 Ring of fire: Annular solar eclipse in Asia and Africa [PIC]
- 329 Rocking the Taliban
- 304 Viewers think new Doctor Who is 'too sexy'
- 255 Stressed teachers 'considering suicide'

content by **Telegraph.co.uk** powered by **digg**

Microsoft News Politics UK News

Ads by Google

Anti Virus
Computer Virus Clean

Transportation: No train signals

Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

By Marty Niland, Associated Press Writer
[InformationWeek](#)

August 20, 2003 06:00 PM

NEW YORK (AP) -- A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday.

The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15 a.m. EDT, CSX spokesman Adam Hollingsworth said.

"The cause was believed to be a worm virus similar to those that have

Transportation: No cars

WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS >>
Sign In | RSS Feeds

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Hacker Disables More Than 100 Cars Remotely

By [Kevin Poulsen](#) March 17, 2010 | 1:52 pm | Categories: [Breaches](#), [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin area lots



Done

Energy: No electricity

Mobile UPI | About UPI | UPI en Español | UPIU - University Media Alliance | My Account

Search: Stories Type search term

UPI.com
100 YEARS OF JOURNALISTIC EXCELLENCE

PROINSO
IMMEDIATE AVAILABILITY!
www.proinso.net

11000 TL SMA + 230 Wp Poly Trinasolar

SECURE YOUR PROJECT
BOOK YOUR MODULES AND INVERTERS NOW
www.proinso.net

Ads by Google

Home Top News Entertainment Odd News Business Sports Science Health Real Estate Photos Videos

Resource Wars Global Water Issues

You are here: [Home](#) / [Energy Resources](#) / [Computer virus in Australian power grid](#)

Energy Resources

View archive | RSS Feed Receive Free UPI Newsletter

Computer virus in Australian power grid

Published: Oct. 2, 2009 at 4:22 PM

Article Photos Listen Comments

SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid

Email Share 1 retweet

PROINSO IMMEDIATE AVAILABILITY!
SECURE YOUR PROJECT
BOOK YOUR MODULES AND INVERTERS NOW
www.proinso.net

11000 TL SMA + 230 Wp Poly Trinasolar

Ads by Google

Internet

Defense: fighter planes grounded

Telegraph.co.uk

Home News Election 2010 Sport Finance Lifestyle Comment Travel Culture F
UK World Celebrities Obituaries Weird Earth Science Health News Education Topics Ne
USA Barack Obama Europe Asia China Middle East Africa and Indian Ocean Australi

HOME NEWS WORLD NEWS EUROPE FRANCE

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris

Published: 11:43AM GMT 07 Feb 2009



Share | f


663 diggs digg it

0 tweet

Email | Print

Text Size + -

What about our lives? Are they next?



FUTURE CRIMES: ANTICIPATING TOMORROW'S CRIMES TODAY

HOME ABOUT RESOURCES CONTACT

The future is already here - it is just unevenly distributed. ~


WEDNESDAY APRIL 14TH 2010

Search

The Crimes

- Artificial Intelligence/Automated Crime (1)
- Biological and Human Genome (2)
- Biometrics (2)
- Cloud Computing (2)
- Critical-Infrastructure (3)
- GPS/Location

Hacking the Human Heart: Medical Devices Found Subject to Technical Attack






Since the dawn of the 1970's television action show the [Six Million Dollar Man](#), the public has been fascinated by bionics and the integration of technology into the human body. What once seemed to be a far-off science fiction fantasy, is increasingly, however, becoming real. For years, surgeons have been replacing human

Future Crimes

A futurist perspective on the effect of scientific and technological progress on crime, policing and the criminal justice system.

Share This Page

Share |   

Join the Conversation

RoadMap

- Security Challenges: What is the problem?
 - Hackers are getting more sophisticated
 - The impact of cyberattacks is getting larger
- *What have we done?*
 - *FORWARD: study emerging threats*
- What will we do?
 - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



What are we doing?

- 2008-2010: created the FORWARD Coordination and Support Action:
 - Managing Emerging Threats in ICT Infrastructures
 - Created three working groups (think-tanks) involving experts from Europe/USA/Asia:
 - Malware and Fraud
 - Smart Environments
 - Critical Systems



FORWARD Working Groups

- Their job was to:
 - Create **a list of threats for the future Internet**
 - Rank the threats:
 - High, medium, low
 - Present Possible solutions



Threats in Malware and Fraud

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Underground Economy	H	H	L	H	H
Social Networks	H	H	M	H	H
Routing	H	H	L	M	M
New Attack Vectors	M	H	M	H	M
Advanced Malware	M	H	M	M	M
Virtualization and Clouds	H	M	H	M	M
IPv6	M	H	M	M	L
DNS and naming	L	H	M	L	L
Targeted Attacks	M	H	M	L	L
Online Games	L	H	M	L	L

FORWARD: Smart Environments

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Threats due to parallelism	M	M	H	M	H
Threats due to scale	H	M	H	M	H
Mobile device malware	H	H	M	H	H
Denial of service	H	H	L	M	M
False sensor data	H	M	H	M	M
Privacy and ubiquitous sensors	M	M	M	M	M
System maintainability and verifiability	M	H	M	M	M
Sensors and RFID	M	H	M	H	L
Malicious hardware	M	L	H	M	L

RoadMap

- Security Challenges: What is the problem?
 - Hackers are getting more sophisticated
 - The impact of cyberattacks is getting larger
- What have we done?
 - FORWARD: study emerging threats
- *What will we do?*
 - *SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet*



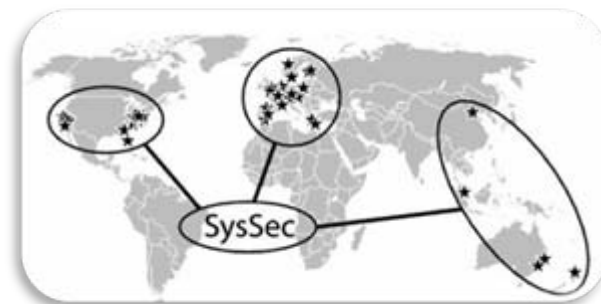
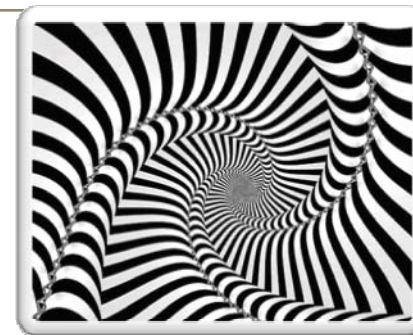
What's next?

- **SysSec**: managing threats and vulnerabilities for the future Internet
 - a Network of Excellence (2010-2014)
 - Why?
 - We need to work towards solutions
 - We need to collaborate
 - At a European level
 - With our international colleagues
 - » Around the world
- **No country is an island**
 - wrt. Internet security



What is SysSec?

- SysSec proposes a *game-changing* approach to cybersecurity:
 - Currently Researchers are mostly reactive:
 - they usually track cyberattackers *after* an attack has been launched
 - thus, researchers are always one step behind attackers
 - SysSec aims *to break this vicious cycle*
 - Researchers should become more *proactive*:
 - Anticipate attacks and vulnerabilities
 - Predict and prepare for future threats
 - Work on defenses *before* attacks materialize.



SysSec Aim and Objectives (I)

- Create an active, vibrant, and collaborating **community of Researchers** with
 - the expertise, capacity, and determination to anticipate and mitigate the emerging threats and vulnerabilities on the Future Internet.
- SysSec aims
 - to create a **sense of ``community''** among those researchers,
 - to **mobilize** this community,
 - to **consolidate** its efforts,
 - to **expand their collaboration** internationally, and
 - become **the single point of reference** for Systems Security research in Europe.



SysSec Aim and Objectives (II)

- Advance European Security Research well beyond the state of the art
 - research efforts have been scattered
 - SysSec aims to **provide a research agenda** and
 - **align their research activities** with the agenda
 - make SysSec **a leading player** in the international arena.



SysSec Aim and Objectives (III)

- Create a **virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities.
 - By forming a **critical mass** of European Researchers and by aligning their activities,
 - Have the gravitas needed to play a **leading role internationally**, empowered to undertake large-scale, ambitious and high-impact research efforts.
- Create a **Center of Academic Excellence** in the area
 - create an education and training program targeting young researchers and the industry.
 - lay the foundations for a common graduate degree in the area with emphasis on Systems Security.



SysSec Aim and Objectives (IV)

- Maximize the impact of the project by proactive **dissemination** to the appropriate stakeholders.
 - disseminate its results to international stakeholders so as to form the needed **strategic partnerships** (with similar projects and organizations overseas) to play a major role in the area.
 - dissemination within the Member States will
 - reinforce SysSec's role as a **center of excellence** and
 - make SysSec **a beacon for a new generation of European Researchers**.
- Create Partnerships and **transfer technology to the European Security Industry**.
 - create a close partnership with Security Industry
 - facilitate technology transfer wherever possible to further strengthen the European Market.

Conclusions

- Hackers are getting more **sophisticated**
- The **impact** of cyberattacks is getting higher
- We need to collaborate in order to manage emerging threats on the future Internet
 - **SysSec** started on Sept 1st.
 - Join us to break the vicious cycle.





SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

**Evangelos Markatos
FORTH-ICS**