



FORTH

Institute of Computer Science



The Cost of Cyber-Insecurity

Sotiris Ioannidis

Institute of Computer Science

Foundation for Research and Technology - Hellas

Threat Landscape

- Security challenges
 - Miscreants becoming smarter and more effective
 - Impact of cyberattacks becoming greater and more important
- Some numbers (Symantec)
 - **431** mil. adult victims in 2010
 - **\$388** bil. lost globally
 - **\$288** bil. world market for cannabis, cocaine and heroin



New attack pathways

- Hackers always find a way:
 - Social networks (e.g. Facebook, Twitter users)
 - 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



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

6

Can birds twit malware?



POWERED BY 

[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](#)



IN ASSOCIATION WITH



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 ploy 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 »](#)

TEXT SIZE

ADVERTISEMENT

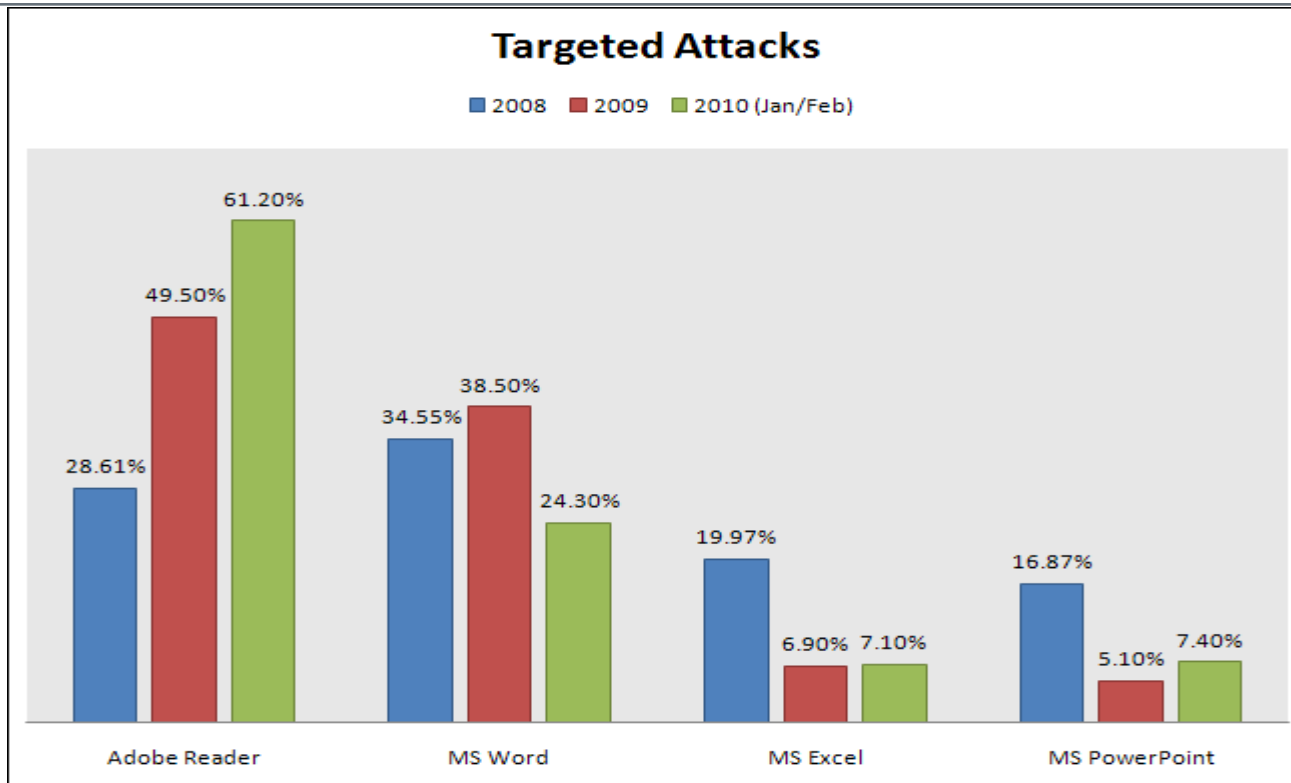
Most Popular on CNN

— STORIES

Done

Internet

Exploits do not only come in .exe files



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

Source: F-Secure

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

Share

Facebook

Twitter

StumbleUpon

Digg submit

0 tweet

Email

Print

Text Size

+

-

Microsoft

News

Politics

UK News

Ads by Google

Anti Virus

Computer Virus Clean

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™

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 Go











[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



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 | |

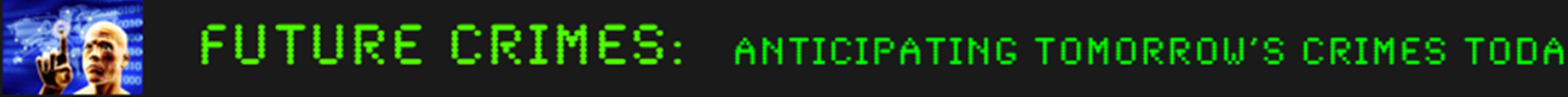
663 diggs digg it

0 tweet

Email | Print

Text Size + -

What about our lives? Are they next?



[HOME](#)
[ABOUT](#)
[RESOURCES](#)
[CONTACT](#)


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

WEDNESDAY APRIL 14TH 2010

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

AV industry in 1998



AV industry in 2008



Image Copyright: IKARUS Security Software GmbH

European Cybersecurity Month



*“in tomorrow’s world **if the internet isn’t secured, nothing will be ...**”*

Neelie Kroes
VP of the European Commission

What is the impact of attacks?

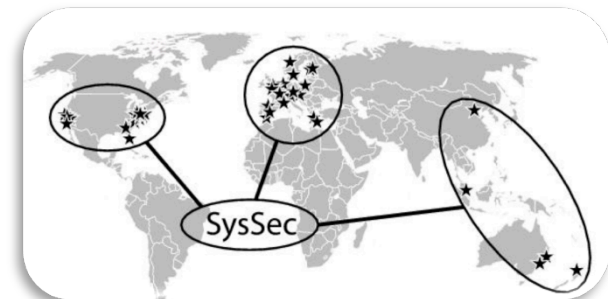


*“... potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: **no more electricity or water at home, rail and plane accidents, hospitals out of service**”*

Viviane Reding
VP of the European Commission

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.



Conclusions

- Hackers are getting more **sophisticated**
- The **impact** of cyberattacks is getting higher
- We must collaborate to manage emerging threats on the Future Internet
- Grand Challenges
 - No device should be compromisable
 - Give users control over their data
 - Provide private moments in public places
 - Develop compromise-tolerant systems
- <http://red-book.eu>