SOPHOS

Malware : Intrusion and Containment

Richard Wang

Manager SophosLabs US

Sophos

Topics

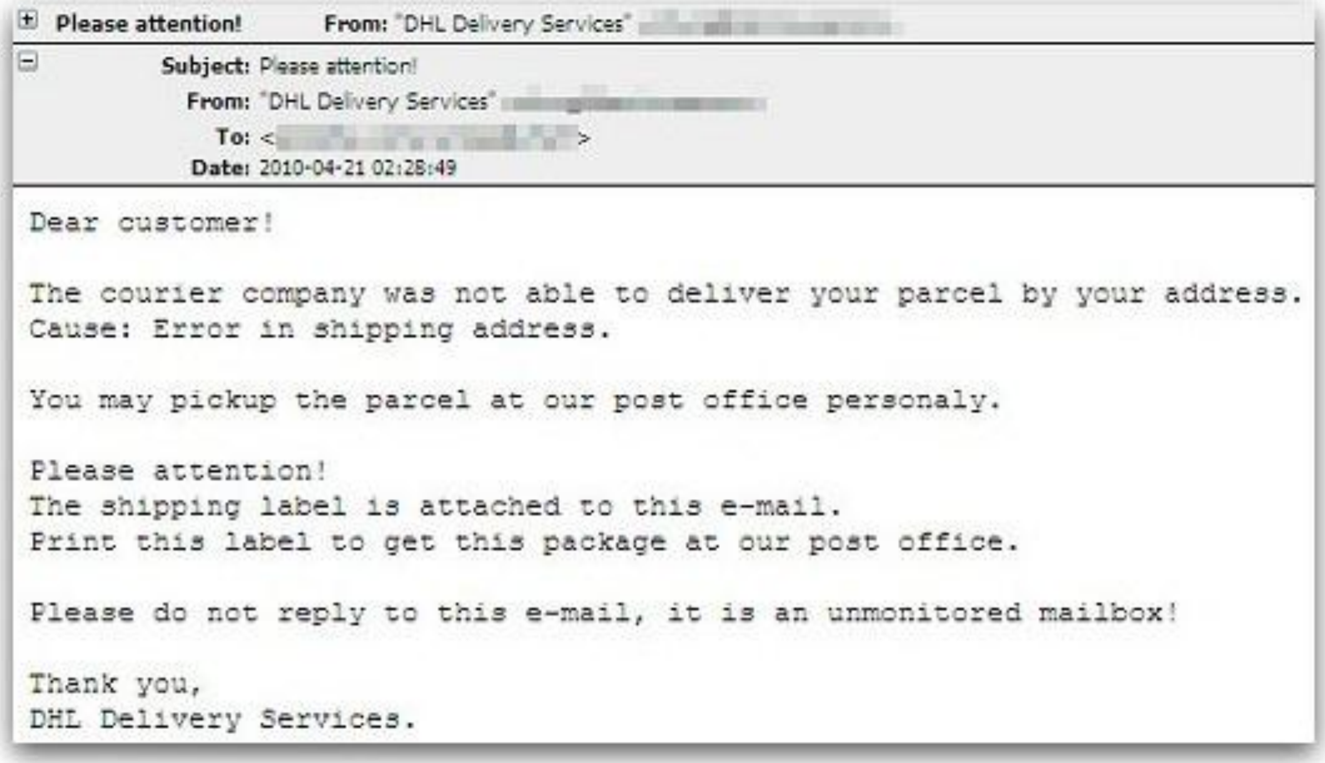
- Reasons for malware intrusion
- Intrusion methods
- Containing malware

Reasons for malware intrusion

- Resource control
  - Botnets
- Data theft
  - Personally Identifying Information (PII)
  - Banking details
  - Intellectual property
- Direct selling
  - Scareware

Email intrusion

- **Spam**
  - **Attachments and Social Engineering**



Please attention! From: "DHL Delivery Services" [redacted]

Subject: Please attention!
From: "DHL Delivery Services" [redacted]
To: <[redacted]>
Date: 2010-04-21 02:28:49

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 personaly.

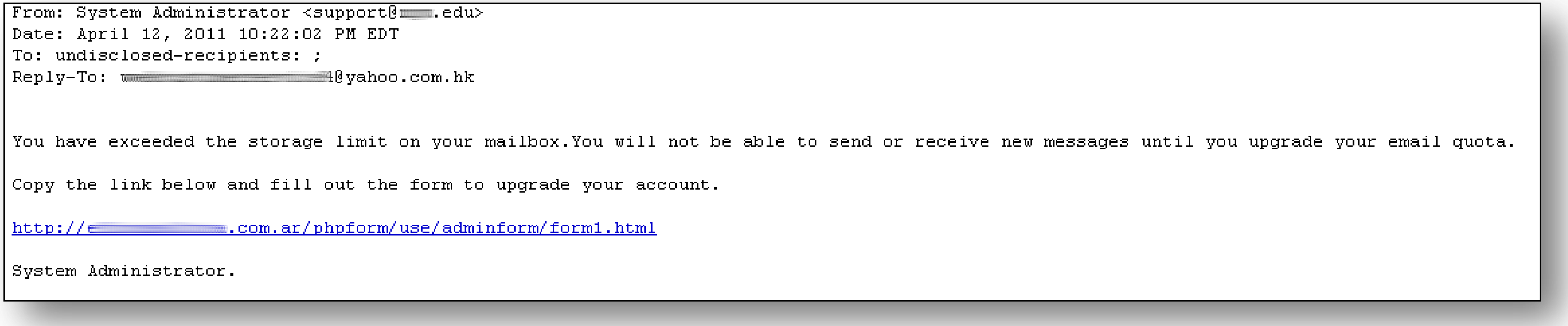
Please attention!
The shipping label is attached to this e-mail.
Print this label to get this package at our post office.

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

Thank you,
DHL Delivery Services.

Email intrusion

- **Phishing**



From: System Administrator <support@[redacted].edu>
Date: April 12, 2011 10:22:02 PM EDT
To: undisclosed-recipients: ;
Reply-To: [redacted]@yahoo.com.hk

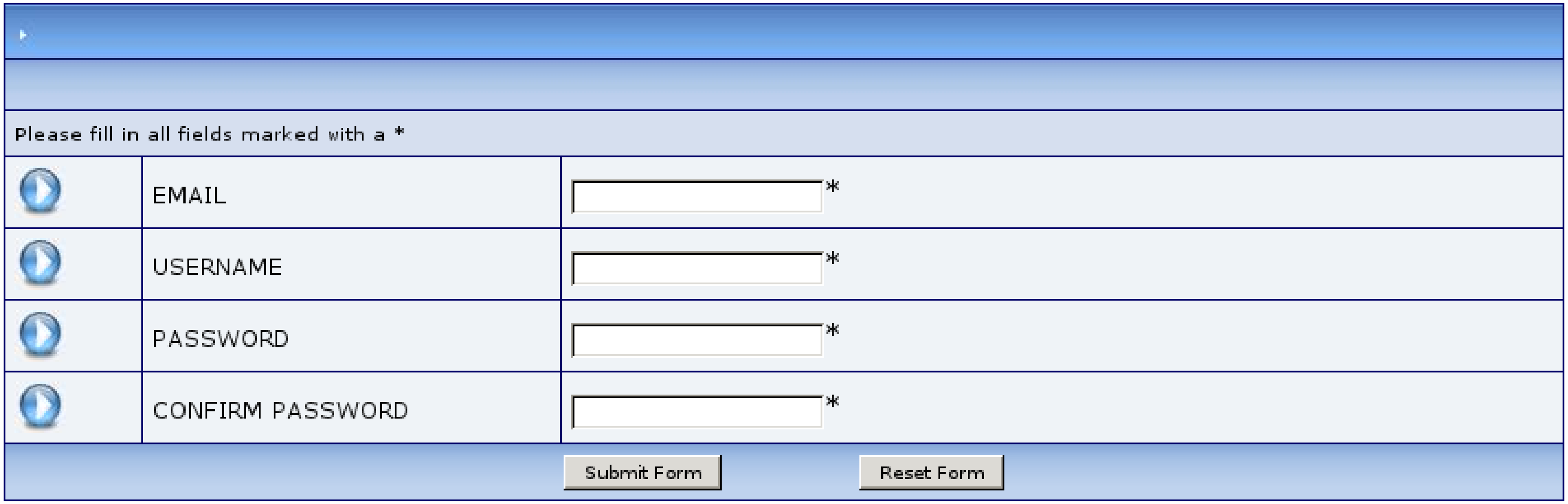
You have exceeded the storage limit on your mailbox.You will not be able to send or receive new messages until you upgrade your email quota.

Copy the link below and fill out the form to upgrade your account.

http://[redacted].com.ar/phpform/use/adminform/form1.html

System Administrator.

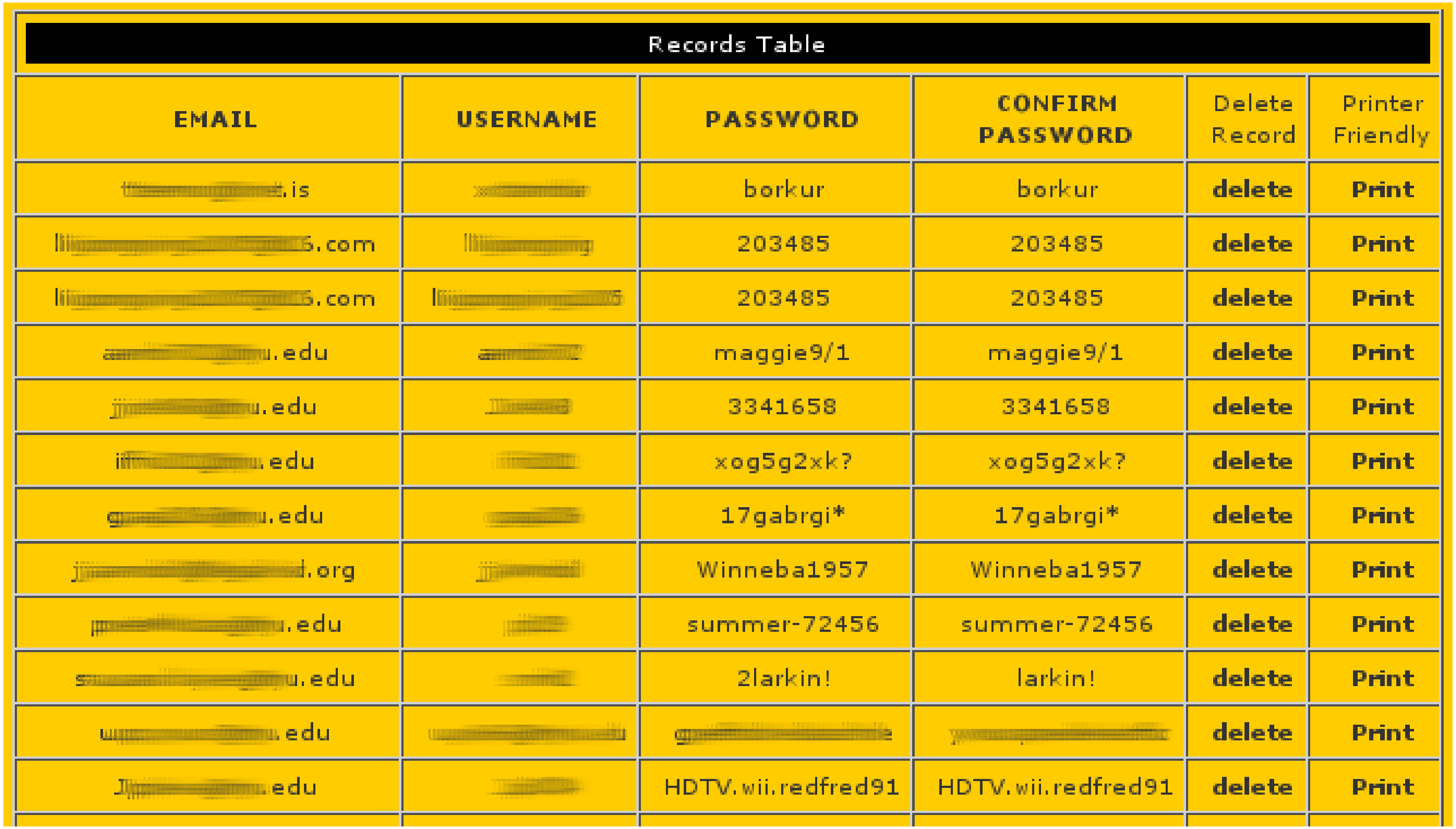
Email intrusion



Please fill in all fields marked with a *

	EMAIL	*
	USERNAME	*
	PASSWORD	*
	CONFIRM PASSWORD	*

Email intrusion



Records Table

EMAIL	USERNAME	PASSWORD	CONFIRM PASSWORD	Delete Record	Printer Friendly
[redacted].is	[redacted]	borkur	borkur	delete	Print
[redacted].com	[redacted]	203485	203485	delete	Print
[redacted].com	[redacted]	203485	203485	delete	Print
[redacted].edu	[redacted]	maggie9/1	maggie9/1	delete	Print
[redacted].edu	[redacted]	3341658	3341658	delete	Print
[redacted].edu	[redacted]	xog5g2xk?	xog5g2xk?	delete	Print
[redacted].edu	[redacted]	17gabrgi*	17gabrgi*	delete	Print
[redacted].org	[redacted]	Winneba1957	Winneba1957	delete	Print
[redacted].edu	[redacted]	summer-72456	summer-72456	delete	Print
[redacted].edu	[redacted]	2larkin!	larkin!	delete	Print
[redacted].edu	[redacted]	[redacted]	[redacted]	delete	Print
[redacted].edu	[redacted]	HDTV.wii.redfred91	HDTV.wii.redfred91	delete	Print

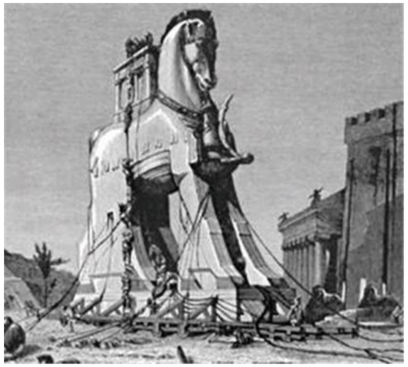
Web intrusion

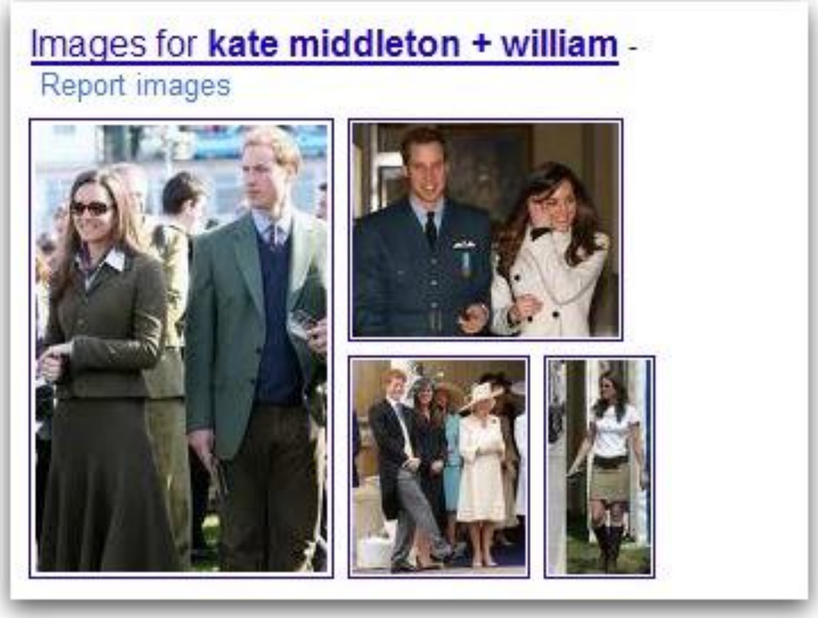
- Social engineering
- Software vulnerabilities
  - Browser
  - Applications
- SQL injection
- Social networks

Social engineering

Social engineering is the primary method of attack

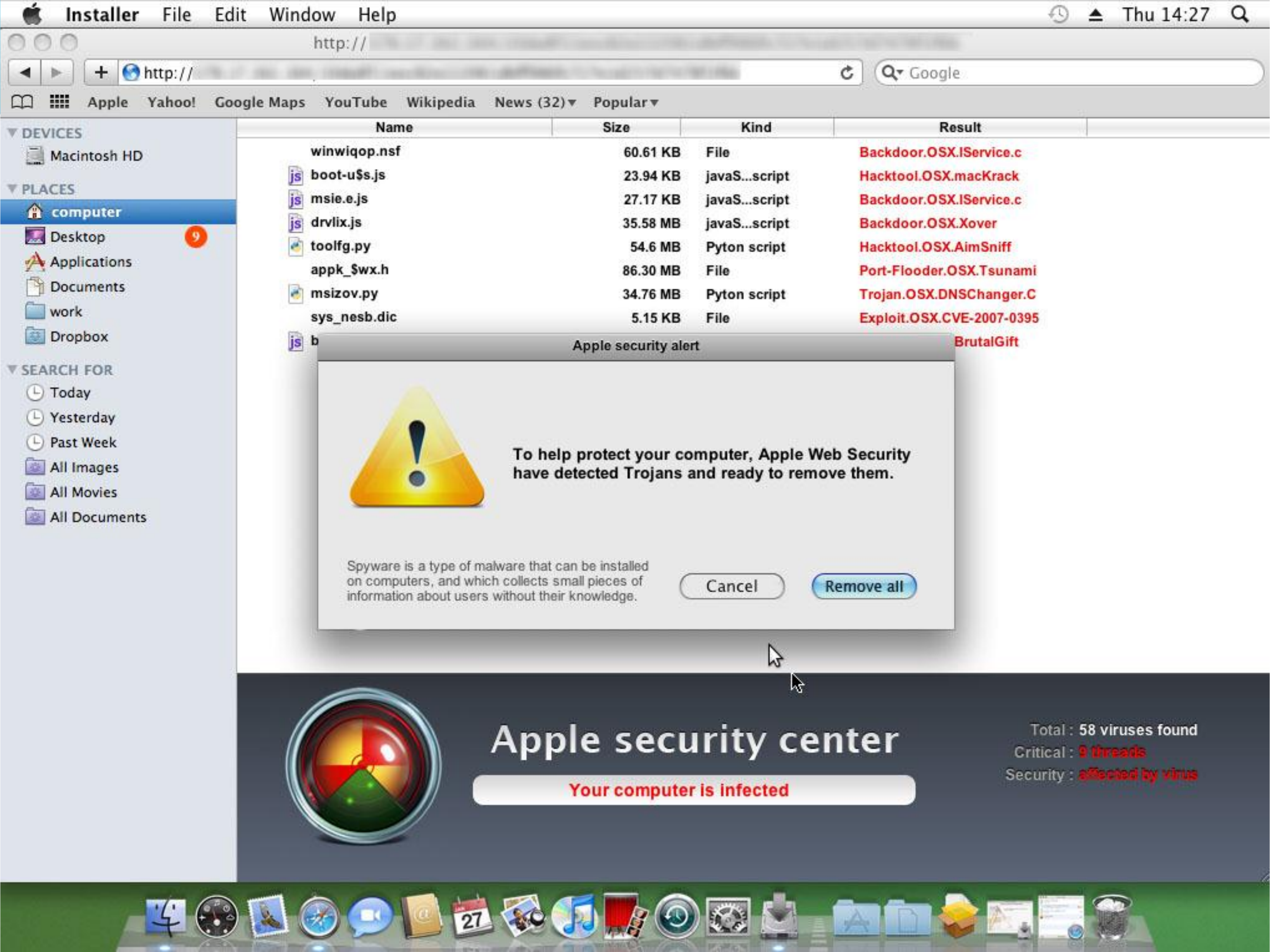
- Scammers have used social engineering tricks for thousands of years, and won’t be stopping anytime soon
- Often spread via poisoned search engine results





Images for **kate middleton + william** -

Report images



Name	Size	Kind	Result
winwiqop.nsf	60.61 KB	File	Backdoor.OSX.IService.c
boot-u$s.js	23.94 KB	javaS...script	Hacktool.OSX.macKrack
msie.e.js	27.17 KB	javaS...script	Backdoor.OSX.IService.c
drvlix.js	35.58 MB	javaS...script	Backdoor.OSX.Xover
toolfg.py	54.6 MB	Pyton script	Hacktool.OSX.AimSniff
appk_$wx.h	86.30 MB	File	Port-Flooder.OSX.Tsunami
msizov.py	34.76 MB	Pyton script	Trojan.OSX.DNSChanger.C
sys_nesb.dic	5.15 KB	File	Exploit.OSX.CVE-2007-0395
b			BrutalGift

Apple security alert

To help protect your computer, Apple Web Security have detected Trojans and ready to remove them.

Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.

Apple security center

Your computer is infected

Total : 58 viruses found

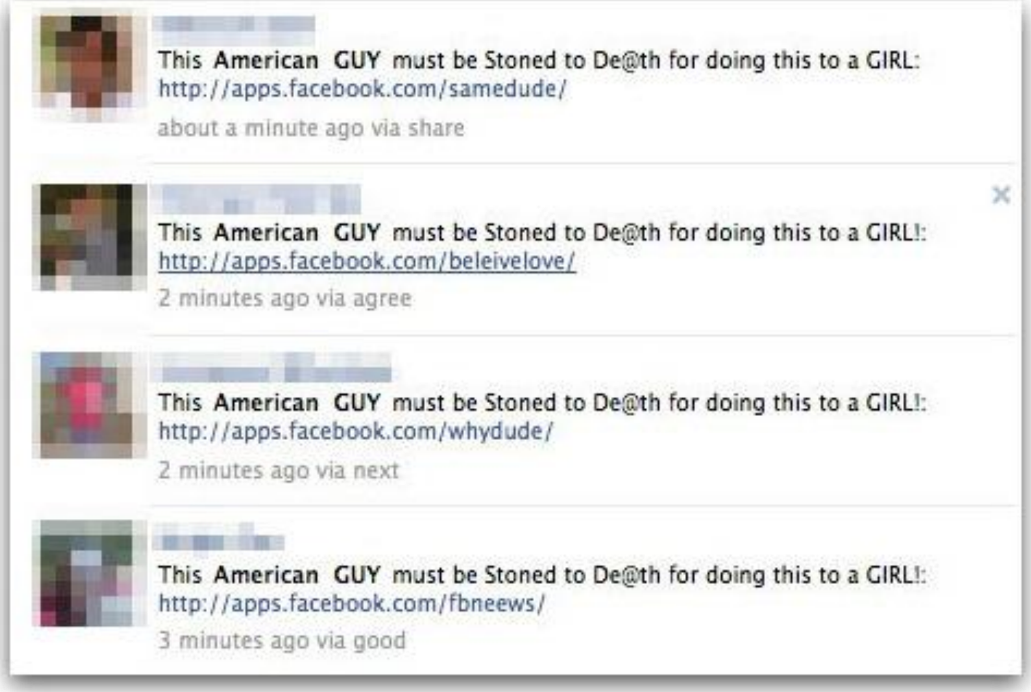
Critical : 9 threads

Security : affected by virus

Software vulnerabilities

- Browser
- Applications
  - Flash
  - Adobe Reader

Social Networking intrusion



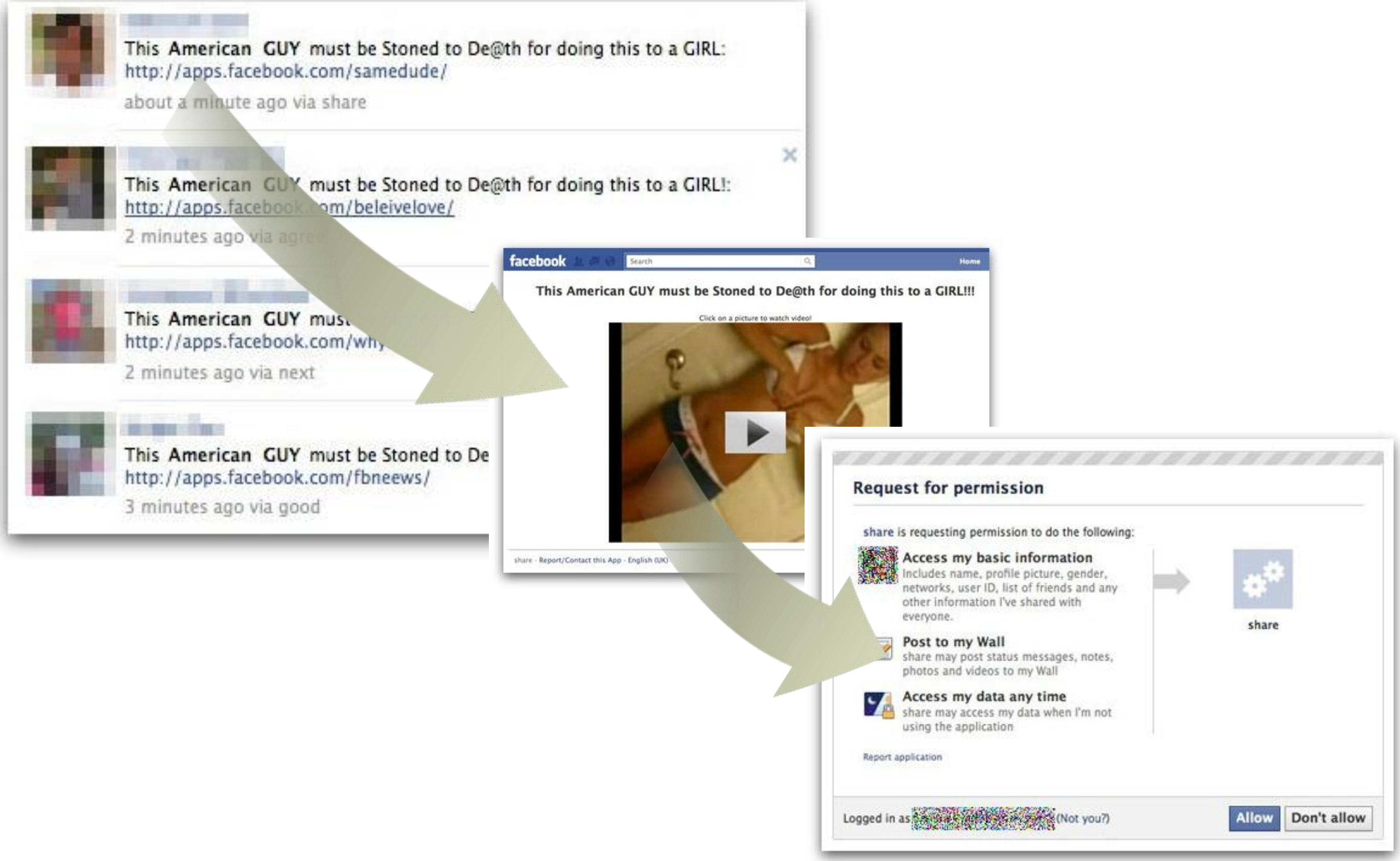
This American GUY must be Stoned to De@th for doing this to a GIRL:
http://apps.facebook.com/samedude/
about a minute ago via share

This American GUY must be Stoned to De@th for doing this to a GIRL!:
http://apps.facebook.com/beleivelove/
2 minutes ago via agree

This American GUY must be Stoned to De@th for doing this to a GIRL!:
http://apps.facebook.com/whydude/
2 minutes ago via next

This American GUY must be Stoned to De@th for doing this to a GIRL!:
http://apps.facebook.com/fbneews/
3 minutes ago via good

Social Networking intrusion



[redacted]
This American GUY must be Stoned to De@th for doing this to a GIRL:
http://apps.facebook.com/samedude/
about a minute ago via share

[redacted]
This American GUY must be Stoned to De@th for doing this to a GIRL!:
http://apps.facebook.com/beleivelove/
2 minutes ago via agre

[redacted]
This American GUY mus
http://apps.facebook.com/why
2 minutes ago via next

[redacted]
This American GUY must be Stoned to De
http://apps.facebook.com/fbneews/
3 minutes ago via good

This American GUY must be Stoned to De@th for doing this to a GIRL!!!

Click on a picture to watch video!

share · Report/Contact this App · English (UK)

Request for permission

share is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.

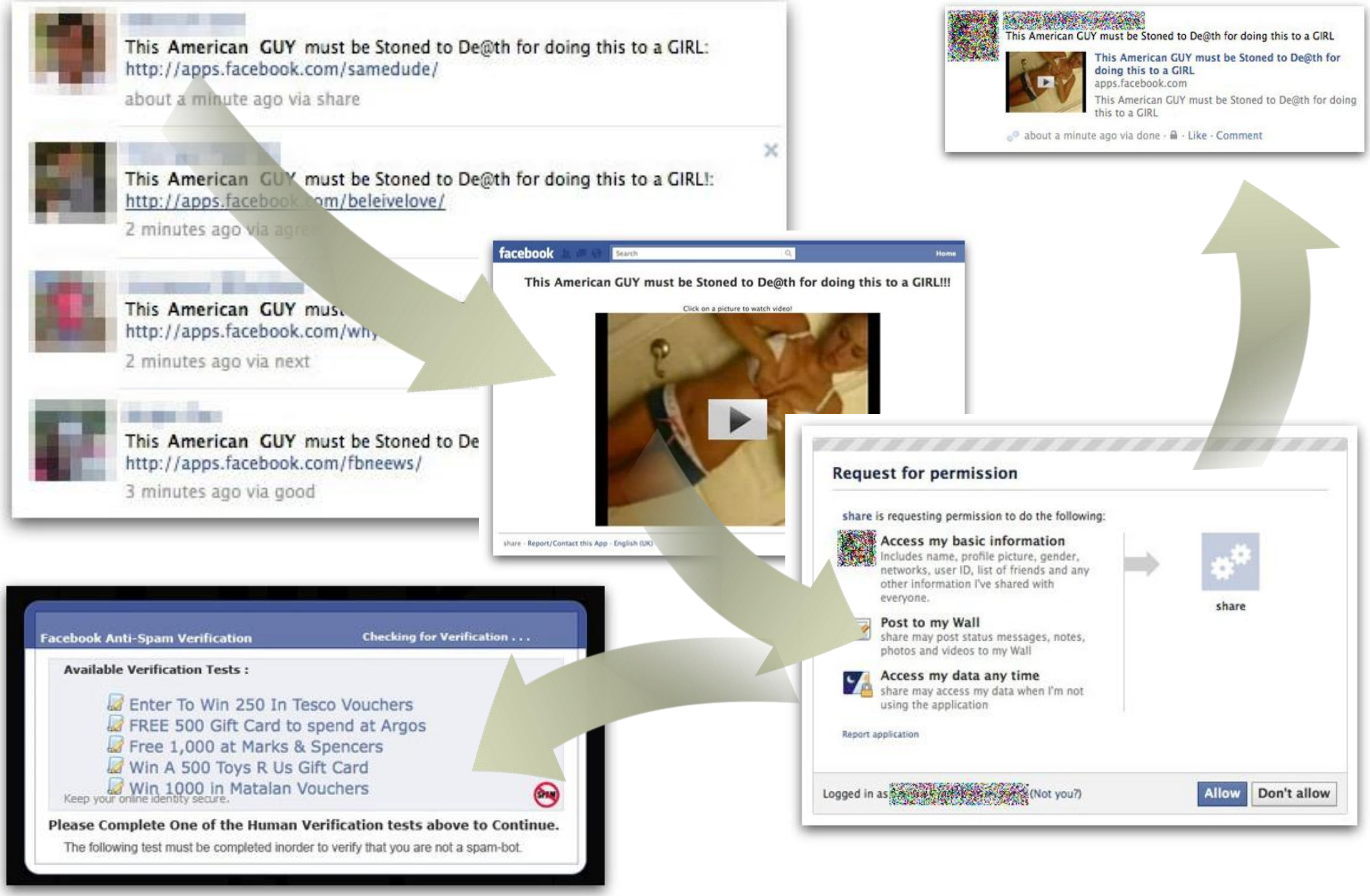
Post to my Wall
share may post status messages, notes, photos and videos to my Wall

Access my data any time
share may access my data when I'm not using the application

Report application

Logged in as [redacted] (Not you?)

Social Networking intrusion



[redacted]

This American GUY must be Stoned to De@th for doing this to a GIRL:
http://apps.facebook.com/samedude/
about a minute ago via share

[redacted]

This American GUY must be Stoned to De@th for doing this to a GIRL!:
http://apps.facebook.com/beleivelove/
2 minutes ago via agre

[redacted]

This American GUY mus
http://apps.facebook.com/wh
2 minutes ago via next

[redacted]

This American GUY must be Stoned to De
http://apps.facebook.com/fbneews/
3 minutes ago via good

[redacted]

This American GUY must be Stoned to De@th for doing this to a GIRL

This American GUY must be Stoned to De@th for doing this to a GIRL
apps.facebook.com
This American GUY must be Stoned to De@th for doing this to a GIRL

about a minute ago via done · Like · Comment

This American GUY must be Stoned to De@th for doing this to a GIRL!!!

Click on a picture to watch video!

share · Report/Contact this App · English (UK)

Request for permission

share is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.

Post to my Wall
share may post status messages, notes, photos and videos to my Wall

Access my data any time
share may access my data when I'm not using the application

Report application

Logged in as [redacted] (Not you?)

Facebook Anti-Spam Verification Checking for Verification . . .

Available Verification Tests :

- Enter To Win 250 In Tesco Vouchers
- FREE 500 Gift Card to spend at Argos
- Free 1,000 at Marks & Spencers
- Win A 500 Toys R Us Gift Card
- Win 1000 in Matalan Vouchers

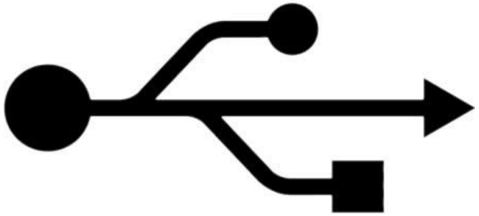
Keep your online identity secure.

Please Complete One of the Human Verification tests above to Continue.

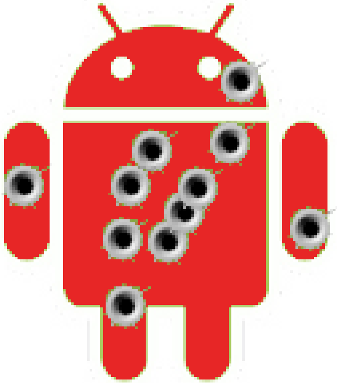
The following test must be completed inorder to verify that you are not a spam-bot.

Mobile device intrusion

- Portable storage
  - USB drives
  - MP3 players



- Mobile devices
  - Smartphones



Malware Containment

Containing malware – known malware

- Malware warnings from around the network
- Malware that ‘keeps coming back’

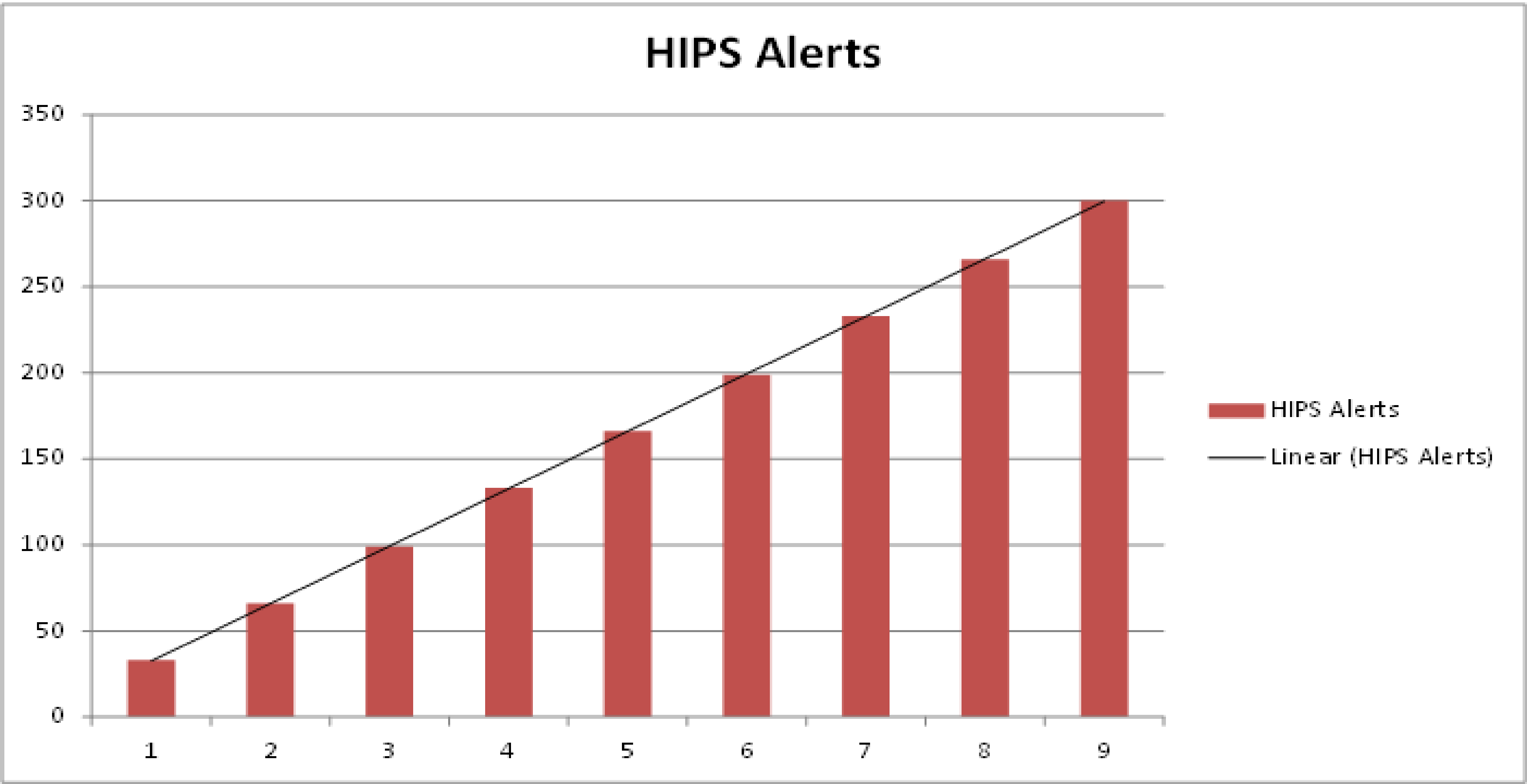
- Locate the source of infection

Containing malware – unknown malware

- **Why does unknown malware exist?**

Containing malware – unknown malware

- **Example of machines HIPS alerting during an attack.**



Containing malware – unknown malware

- Hospitality company
- Targeted attack aimed at payment processing software
- 1500+ HIPS warnings over 9 months!
- ‘Something’ is registering a new service on payment processing servers.

Staying ahead of the curve

Search articles

Archive by date | author | category
Send us a tip | Subscribe by RSS | Email

nakedsecurity
News. Opinion. Advice. Research.

malware | spam | social networks | data loss | law & order | apple | more ▸ about

Yes, you need anti-virus on your Mac.. and now it's free

October roundup - "90 Second News"

VIDEO: Cross-platform malware runs on Windows, Mac and Linux

Love your Mac?
1
Bredolab botnet shut down
Hi there! If you're new here, you might want to subscribe to the RSS
updates.
by Graham Cluley
FILED UNDER: Law &
to comment
Bredolab, a botnet
tentacles around the world, infecting some 30
1
10

http://nakedsecurity.sophos.com

@sophoslabs

US and Canada
1-866-866-2802
NASales@sophos.com

UK and Worldwide
+ 44 1235 55 9933
Sales@sophos.com

Questions?