

SECURITY is not complete without U

Computer Security Day

10 June 2010, Council Chamber and <http://cern.ch/SecDay>

How cyber-criminals make money and how you lose it

Sebastian Lopienski

CERN Computer Security Team

Cyber crime

Computer.Security@cern.ch — “Computer Security Day” — slide 2

It is not this kind of guy behind the attacks anymore:



Cyber crime

Computer.Security@cern.ch — “Computer Security Day” — slide 3

It is this kind of guys:



**... well organized, specialized criminals
operating in the cyber-space**

Cyber crime

ty Day” — slide 4



and they are after the money

Cyber crime trends

Computer.Security@cern.ch — “Computer Security Day” — slide 5

- ▶ **On a growth, despite the global economic crisis**
- ▶ **More malware seen in 2009 than in all previous years**
- ▶ **Technical level required to become a cyber-criminal is very low**

Some bad news...

Computer.Security@cern.ch — “Computer Security Day” — slide 6

**The most likely place for you
to be the target of a crime
is on the Internet.**

Cyber crime

Computer.Security@cern.ch — “Computer Security Day” — slide 7

BTW, these were just amateurs / hobbyists

GST
GREEK SECURITY
TEAM

10/09/08 03:00

Αυτήν την ώρα γίνεται η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα.

Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλά με βάση την μεγάλη επισκεψιμότητα που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγω του πειράματος.

Μερικά στοιχεία απ' τη βάση :

```
USERNAME USER_ID CREATED
SYS 0 2008-02-18 16:19:25.0
SYSTEM 5 2008-02-18 16:19:25.0
OUTLN 11 2008-02-18 16:19:28.0
DIP 19 2008-02-18 16:21:17.0
TMSYS 21 2008-02-18 16:23:27.0
DBSNMP 24 2008-02-18 16:24:25.0
WMSYS 25 2008-02-18 16:24:53.0
EXFSYS 34 2008-02-18 16:27:55.0
XDB 35 2008-02-18 16:28:04.0
PDB_ADMIN 46 2008-02-18 17:26:32.0
GLEGE 49 2008-02-19 10:13:07.0
PDBMON 45 2008-02-18 17:25:24.0
BALYS 44 2008-02-18 17:25:24.0
USERMON 48 2008-02-18 17:59:26.0
..etc...etc...
```

Outline

Computer.Security@cern.ch — “Computer Security Day” — slide 8

- ▶ **How do they make money (and how you lose it)?**
- ▶ **How are they organized?**
- ▶ **How does your computer get infected and your account compromised?**



SECURITY is not complete without **U**

Computer Security Day
10 June 2010, Council Chamber and <http://cern.ch/SecDay>

Part 1:

How do they make money?

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 10

- ▶ Spam and hoaxes \$
- ▶ Scareware \$
- ▶ E-banking, credit cards \$
- ▶ Extortion
- ▶ Underground market
- ▶ Other

\$ = targeting directly your money



How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 11

► SPAM



“... yes, it’s annoying – but is it profitable for spammers?”

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 12

▶ SPAM – selling “goods”

Security researchers did an experiment recently:

- ▶ sent 350M spam messages during a 4-week period
- ▶ sold 28 “male enhancement” pills for \$100 each
- ▶ conversion rate = 1:12.500.000 (very low)
- ▶ => profit is still around \$3000 in a month



Now, multiply these numbers to a real scale (Storm botnet size)

- ▶ \$7000 per day; \$2.5M per year
- ▶ tempting, isn't it...? ;-)

▶ How you lose money

- ▶ buying advertised stuff...
- ▶ server time, disk space: at CERN, 90% of incoming mail is spam

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 13

► SPAM – “Pump and dump” scam

Artificially inflating the stock price
to sell it with profit

Procedure for criminals

1. buy the stock (especially “penny stocks”)
2. send spam messages that will “advise” recipients to buy that stock
3. when some of them do, and the price goes up, sell yours (with profit)



BTW, no interaction with the spammer needed

► and they usually collect their profit indirectly, using “mules”

► How you lose money

► buying “pump and dump” stock

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 14

▶ SPAM – advance-fee fraud (lottery or “419” scam etc.)

- ▶ “You won 10 million € in this e-mail lottery”
- ▶ “I inherited 65 million \$. I need your help – you will get 20%”
- ▶ but you need to advance some money first, “to cover expenses”
- ▶ there was a 2 million € (!) victim in France in 2008

- ▶ BTW, the scam is not new
(called “*Spanish prisoner*” in XIX century)

▶ How you lose money

- ▶ sending money (or goods) to fraudsters



How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 15

▶ Spam and hoaxes \$

▶ Scareware \$

▶ E-banking, credit cards \$

▶ Extortion

▶ Underground market

▶ Other

\$ = targeting directly your money



Scareware

Computer.Security@cern.ch — “Computer Security Day” — slide 16

► Fake Windows folder „scanner” (= an image)

The screenshot shows a browser window with a URL: <http://trustsystem-protection.com/?p=WKmimHVlaW6HjsbIo22EhHV8ipnVbWeMhNa>. The browser displays a fake Windows interface with a "System folders" section containing "Shared Documents" and "My Documents", both marked with a red shield icon and "5 Viruses found".

A "Windows Security Alert" dialog box is overlaid on the browser. The dialog has a blue header and a shield icon. The text inside reads: "To help protect your computer, Windows Web Security have detected Trojans and ready to remove them." Below this is a table of detected spyware and adware:

Detected spyware and adware on your computer:	Filename:
Magic DVD Ripper	d3dx10_37.dll
W32.Benjamin.Worm	appmgr.dll
Trojan Horse IRC/Backdoor.SdBot4.FRV	url.dll
W32.Yaha.B@mm	clb.dll
Trojan-Downloader.Win32.Small.fxf	FinishDrv.log

At the bottom of the dialog are "Remove all" and "Cancel" buttons. Below the dialog, a "WARNING" section shows a "Threat level" dropdown menu with options: High, High, Critical, Critical, Medium. A "Start Protection" button is visible at the bottom right of the browser window.

A problem has been detected and windows has been shut down to prevent damage to your computer.

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure that any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

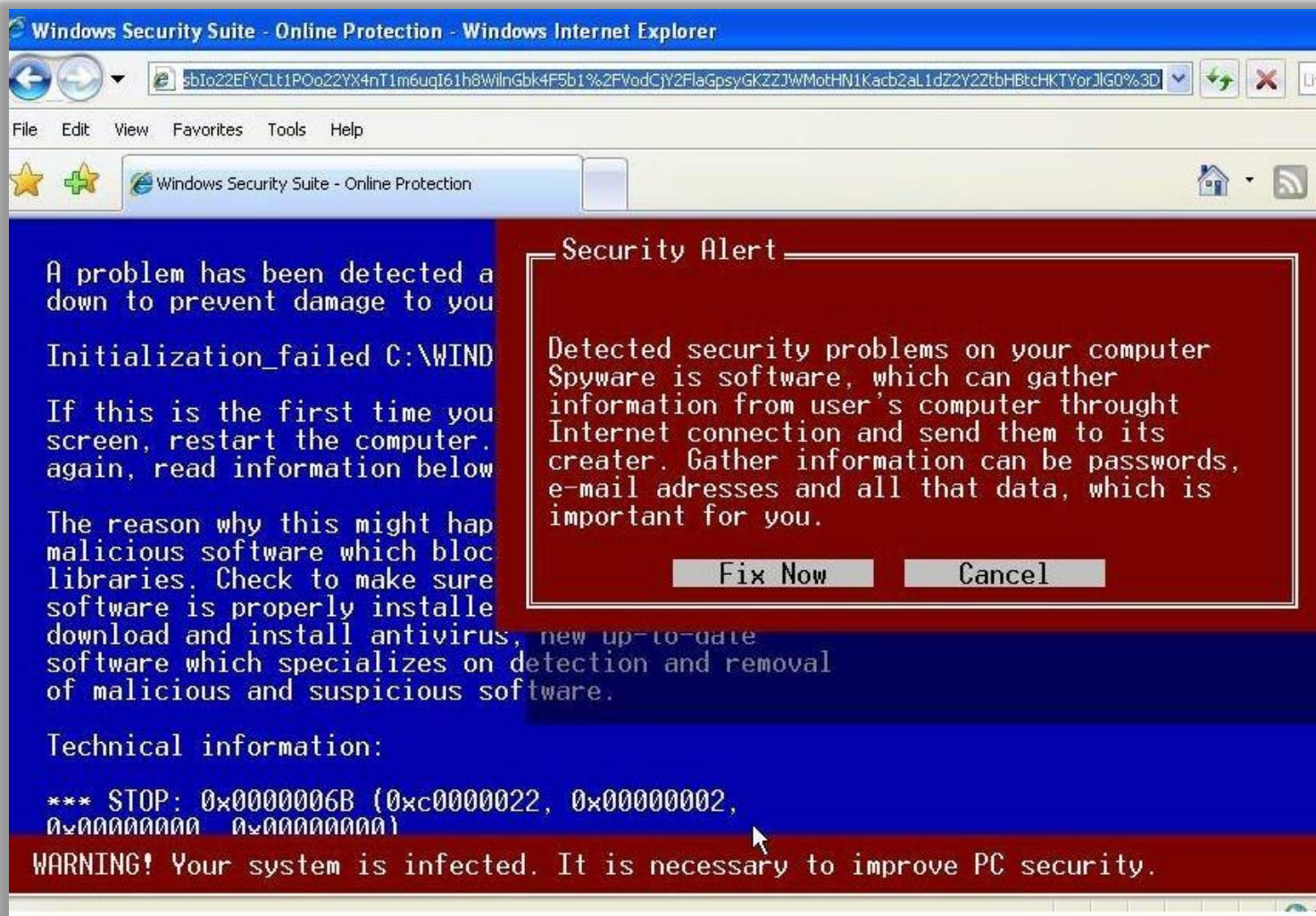
Technical information:

*** STOP: 0x00000050 (0x00000000,0x8054A9E4,0x00000008,0xC0000000)

*** CI.dll - Address 8054A9E4 base at 8054A000, DateStamp 36B05FFC

Scareware

► Fake „Blue Screen of Death”



Scareware

Computer.Security@cern.ch — “Computer Security Day” — slide 19

► Fake “Google Tips”

(added with malware that already infected your computer)



► BTW, “Google Tips” feature doesn’t exist!

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 20

▶ Scareware (fake/rogue anti-virus)

- ▶ scares you („*Your computer is infected*”), to trick you into buying a fake security/anti-virus product
- ▶ distribution: Web, e-mail (like malware)
- ▶ a „free scan” always reveals „infections”
- ▶ one license \$50-80
- ▶ total revenue estimated at \$34M monthly (in 2009)

▶ How you lose money

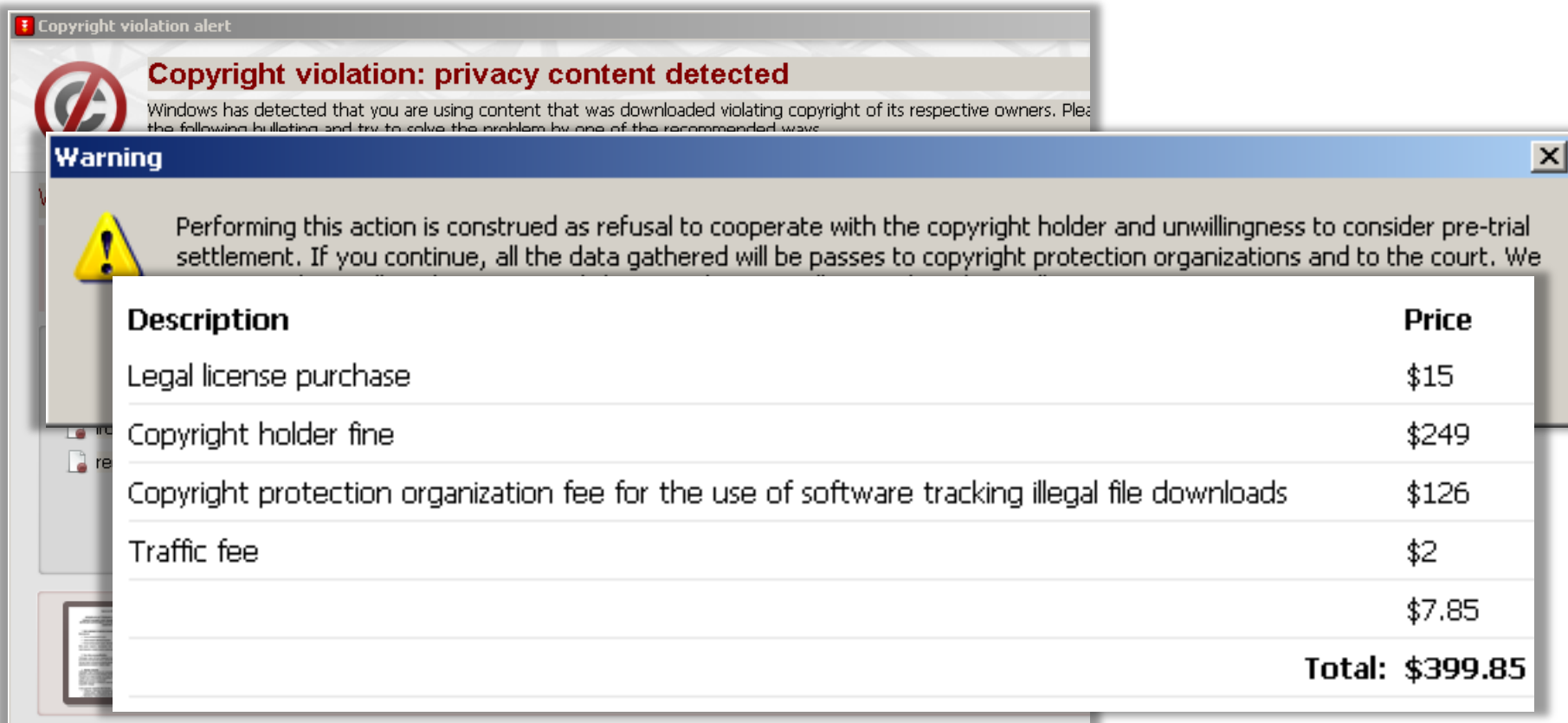
- ▶ paying for a fake anti-virus

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 21

► “Copyright violation pre-trial settlement” scam

Fake “warnings” (by e-mail, Web, or your computer infected)



The image shows a screenshot of a Windows desktop. At the top, there is a window titled "Copyright violation alert" with a red error icon. The main text in this window reads: "Copyright violation: privacy content detected". Below this, it says: "Windows has detected that you are using content that was downloaded violating copyright of its respective owners. Please read the following bulletin and try to solve the problem by one of the recommended ways."

Overlaid on this is a "Warning" dialog box with a yellow warning triangle icon. The text inside the warning box reads: "Performing this action is construed as refusal to cooperate with the copyright holder and unwillingness to consider pre-trial settlement. If you continue, all the data gathered will be passed to copyright protection organizations and to the court. We have prepared a list of options for you to resolve the issue." Below the text is a table with two columns: "Description" and "Price".

Description	Price
Legal license purchase	\$15
Copyright holder fine	\$249
Copyright protection organization fee for the use of software tracking illegal file downloads	\$126
Traffic fee	\$2
	\$7.85
Total: \$399.85	

► **How you lose money?** paying that \$400... (do not!)

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 22

▶ Spam and hoaxes \$

▶ Scareware \$

▶ E-banking, credit cards \$

▶ Extortion

▶ Underground market

▶ Other

\$ = targeting directly your money

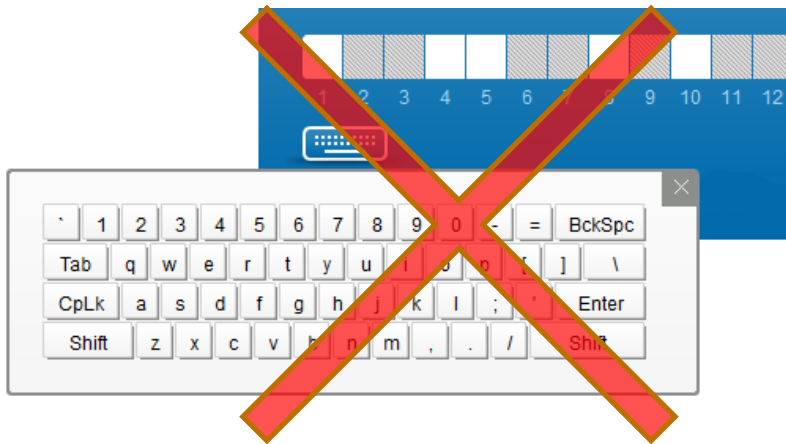


How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 23

▶ *The holy grail* – getting your money directly

- ▶ from your e-banking, PayPal, eBay, on-line poker etc. accounts
- ▶ by stealing your passwords, or hijacking sessions
- ▶ malware targeting thousands of different financial institutions
- ▶ online bank statements modified, to hide fraudulent transactions (!)
- ▶ bypassing “virtual keyboards” or multi-factor/”strong” authentication (!)



▶ **How you lose money**

- ▶ When your e-banking sessions is taken over

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 24

▶ Using stolen credit cards

- ▶ stolen from online databases
 - how many Web sites know your credit card numbers?
- ▶ used by criminals for buying good on-line
 - especially non-physical goods, e.g. minutes for pre-paid mobiles
- ▶ also: debit cards copied when you use an ATM/cash machine that was tampered with

▶ How you lose money

- ▶ if your bank refuses to cover the cost
- ▶ or if you don't even realise you were robbed
 - do you check and understand (remember) each position on your monthly credit card statement?

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 25

▶ Spam and hoaxes \$

▶ Scareware \$

▶ E-banking, credit cards \$

▶ Extortion

▶ Underground market

▶ Other

\$ = targeting directly your money



How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 26

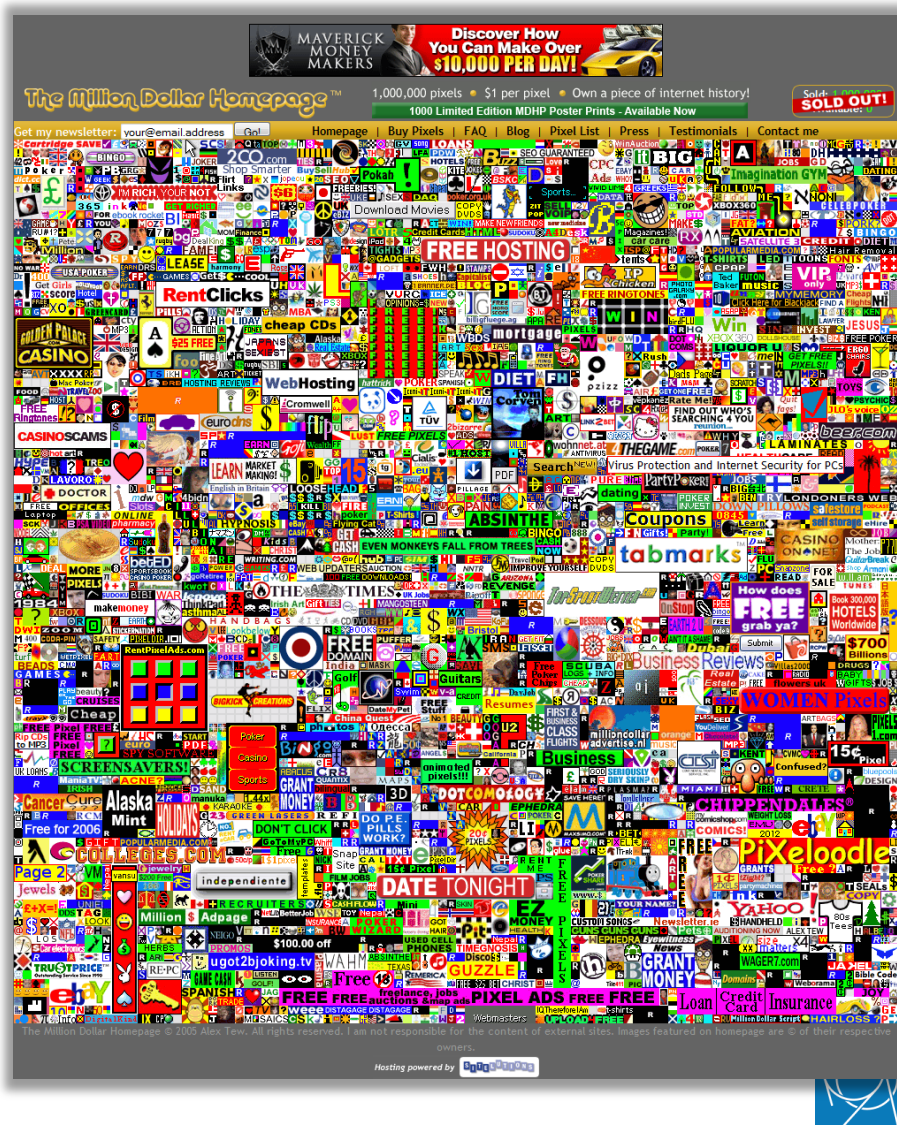
▶ Extortion / blackmailing

The Million Dollar Homepage:

- ▶ \$50k demanded, not paid
- ▶ so the Web site went down, following a DDoS (Distributed Denial of Service) attack

Other victims:

- ▶ online gambling sites (often!)
- ▶ any company (especially those that depend on their Web site and are believed to have money)
- ▶ ... and victims keep silent (regardless if they pay or not)



How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 27

- ▶ Spam and hoaxes \$
- ▶ Scareware \$
- ▶ E-banking, credit cards \$
- ▶ Extortion
- ▶ Underground market
- ▶ Other

\$ = targeting directly your money



How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 28

► Underground market

Overall Rank		Item	Percentage		Range of Prices
2009	2008		2009	2008	
1	1	Credit card information	19%	32%	\$0.85–\$30
2	2	Bank account credentials	19%	19%	\$15–\$850
3	3	Email accounts	7%	5%	\$1–\$20
4	4	Email addresses	7%	5%	\$1.70/MB–\$15/MB
5	9	Shell scripts	6%	3%	\$2–\$5
6	6	Full identities	5%	4%	\$0.70–\$20
7	13	Credit card dumps	5%	2%	\$4–\$150
8	7	Mailers	4%	3%	\$4–\$10
9	8	Cash-out services	4%	3%	\$0–\$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	\$2–\$30

Goods and services advertised for sale on underground economy servers

Source: Symantec

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 29

► Underground market

“1.5 million stolen Facebook IDs for sale” (Apr 2010)

- \$25 to \$45 per 1000 accounts (depending on the number of contacts)

trading also:

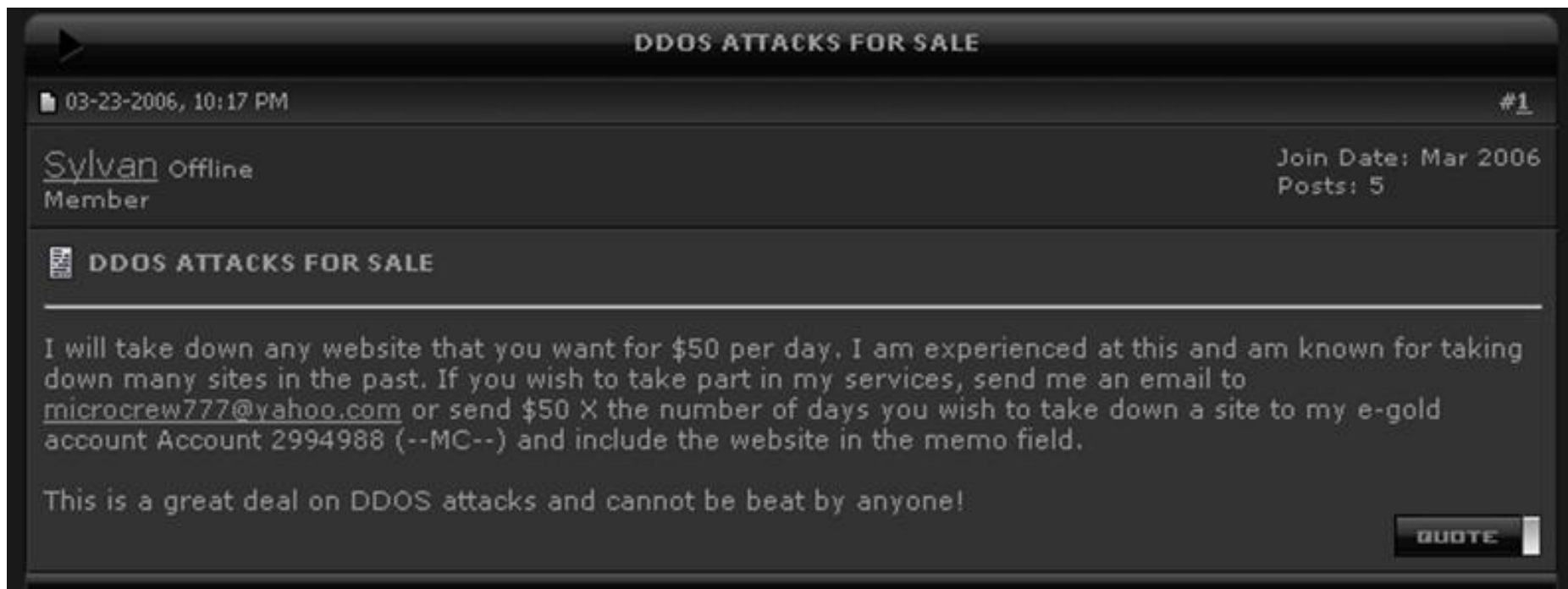
- 30,000 € bank account - €2,000
- Confidential financial reports - \$5,000
- Product design documentation - \$1,000
- Credit card and PIN - \$500
- Social security number - \$100
- Access to compromised machines (bots) – a few cents per machine

criminals offer “satisfait ou remboursé” **guarantees!**

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 30

► Selling criminal services and hacking toolkits to others



The screenshot shows a forum post with the following details:

- Title:** DDOS ATTACKS FOR SALE
- Date:** 03-23-2006, 10:17 PM
- Post Number:** #1
- Author:** Sylvan (offline), Member
- Join Date:** Mar 2006
- Posts:** 5

The main text of the post reads:

DDOS ATTACKS FOR SALE

I will take down any website that you want for \$50 per day. I am experienced at this and am known for taking down many sites in the past. If you wish to take part in my services, send me an email to microcrew777@yahoo.com or send \$50 X the number of days you wish to take down a site to my e-gold account Account 2994988 (--MC--) and include the website in the memo field.

This is a great deal on DDOS attacks and cannot be beat by anyone!

QUOTE

“I will take down any website ... for \$50 per day”

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 31

▶ Selling criminal services and hacking toolkits to others

callservice.biz

- ▶ making fake confirmation phone calls (\$10 per successful call)
- ▶ calls made by native English or German speakers
- ▶ to confirm to a bank a fraudulent transaction on victim's bank account, authenticating with his personal details (mother's maiden name etc.) stolen earlier (with social engineering, from Facebook etc.)
- ▶ service ran by two Belarusians – stopped recently by FBI

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 32

▶ Selling hacking toolkits to others

- ▶ Modern toolkits come with advanced licensing schemas, user support, “satisfaction guarantees” etc.
- ▶ They offer simple GUIs for selecting infection types, payload, etc.

So one can start cyber-criminal activity
having very little technical knowledge!

► Selling criminal services and hacking toolkits to others

View Single Post Thread: Zeus and actual exploit packs

12-08-2009, 17:42 #1 (permalink)

-botnet- Offline
Banned

Join Date: Aug 2009
Posts: 62

👍 Zeus and actual exploit packs

Zeus and actual exploit packs

Hello friends
I am ready to sell you a botnet:

Total reports in database: 506784
Time of first activity: 17.06.2009 11:39:13
Total bots: 8451
Total active bots in 24 hours: 11.39% - 1484
Minimal version of bot: 1.2.7.9
Maximal version of bot: 1.2.7.9
[Actual webinject setup here](#)
admin panel install on abuse"immunity hosting

15%mix > 40%us > 20%eu > 25%ru loads

Admin panel login + ftp login + host account + primary email and secret question's
cost 750\$ very hot price

I not sell you all file admin panel and builder > I can only set up you and delite install file folder

Install Zeus on you host last version 450\$. I not give you builder and install pack > **Only install on you host**
If you are my client - rebuild on other hosting cost 100\$
All my customers receive a special identification number attached to e-mail > icq and host

[Actual webinject](#) = 100\$
Webmoney inject = 200\$

Also i can sell popular and private exploits pack cheaper than the authors
unique pack 2.1 - **300\$**

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 34

- ▶ Spam and hoaxes \$
- ▶ Scareware \$
- ▶ E-banking, credit cards \$
- ▶ Extortion
- ▶ Underground market
- ▶ Other

\$ = targeting directly your money



How they make money

▶ Illegal online gambling sites / casinos

(only ~20% of online casinos are officially registered in countries they operate)



▶ How you lose money

- ▶ you don't receive money for big wins
- ▶ win-lose ratio lower than legally required
- ▶ your credit card numbers stolen and sold/abused

How they make money

Computer.Security@cern.ch — “Computer Security Day” — slide 36

▶ Other cyber-criminal activities (just some examples)

auction site, and online selling-buying fraud

- ▶ “usual” stuff – you don’t get the goods you paid for;
or you don’t get the money for the goods you sold and sent

illegal online pharmacies

click fraud

etc. etc. etc.



SECURITY is not complete without U

Computer Security Day
10 June 2010, Council Chamber and <http://cern.ch/SecDay>

Part 2:

How are they organized?



Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 38

- ▶ **Highly specialized**
- ▶ **Different “jobs”**
 - ▶ coders, programmers
 - ▶ distributors, vendors
 - ▶ techies
 - ▶ hackers
 - ▶ fraudsters
 - ▶ mules
 - ▶ leaders

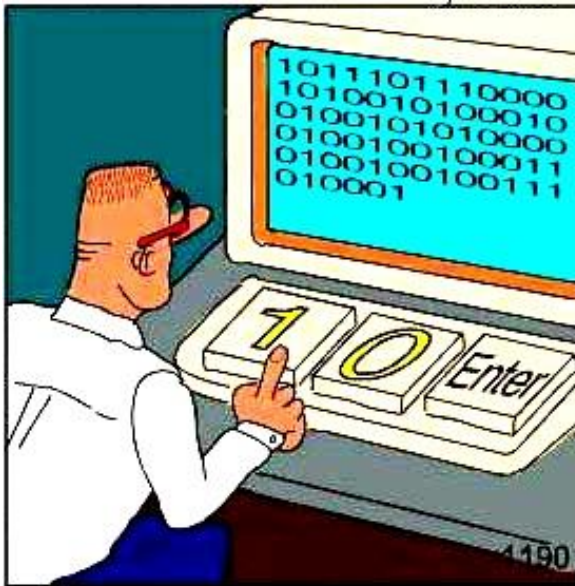
(see also <http://blogs.techrepublic.com.com/itdojo/?p=1632&tag=nl.e036>)



Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 39

► Coders / programmers



REAL Programmers code in BINARY.



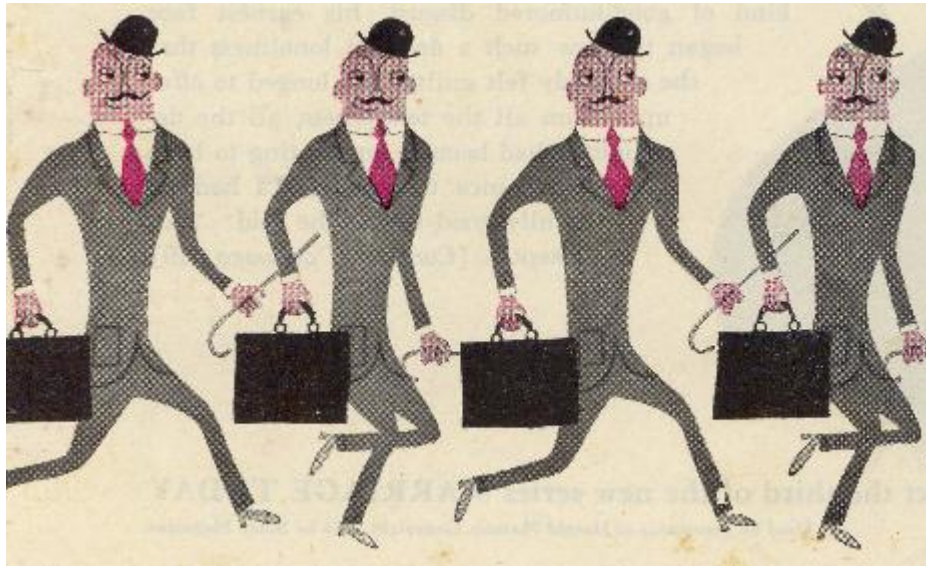
they write malware, exploits, remote access tools etc.

... in fact, they don't necessarily commit a crime

Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 40

► Distributors and vendors



“trade and sell stolen data, and act as vouchers of the goods provided by the other specialties”

Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 41

► Techies



“maintain the criminal infrastructure, including servers, and bulletproof Internet Service Providers (ISP)”

... again, just running a **bulletproof ISPs** (hosting servers that are known to be used by criminals) is legal in many countries. Examples include Russian Business Network and McColo

Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 42

► Hackers



“search for and exploit application, system, and network vulnerabilities to gain administrator or payroll access”

... again, just looking for (and finding) vulnerabilities, or even selling the findings, is usually not a crime

Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 43

► Fraudsters



“create and deploy social engineering schemes, including phishing, spamming, and domain squatting”

Hiring mules

http://finha-capital.com/index.php?option=com_content&view=article&id=5&Itemid=5&option=com_content&view=article

Day" — slide 45



[Home](#)

[About Us](#)

[Business Cash Advance](#)

[International Payments](#)

[Contact Us](#)



Extensive **sales,**
marketing
experience!

Increase Sales with Local Bank Transfers

Save Money and Increase Sales with Local Bank Transfers

Merchants discover that offering local bank transfers as a payment option is an easy way to boost sales from international buyers who prefer to pay by bank transfer rather than credit card.

Save Money on Payment Processing

Amazingly low flat rates. Save even more money by eliminating cross-border and foreign exchange fees.

Expand International Market Reach



[Payment Gateway](#)

[Loyalty Program](#)

[Security Web](#)



Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 46

► Money mules

- needed for money laundering
- they receive money (and goods) resulting from online fraud and crime
- and transfer it further (minus 5-10% of their “commission”), often with money transfer services like MoneyGram or Western Union

- “work-from-home” job opportunities, advertised as legitimate work
- sometimes even signing official work contracts

- many of the mules don’t realise it is illegal; but others are consciously doing their “job”



Cyber crime gangs

Computer.Security@cern.ch — “Computer Security Day” — slide 49

► Leaders



“They choose the targets; choose the people they want to work each role; decide who does what, when, and where; and take care of personnel and payment issues”

SECURITY is not complete without **U**

Computer Security Day

10 June 2010, Council Chamber and <http://cern.ch/SecDay>

Part 3:

**How does your computer get infected
and your account compromised?**

A map of infected computers

Computer.Security@cern.ch — “Computer Security Day” — slide 51

► new “Waledac” malware infections – in just 24 hours



Is your computer one of them?

Getting infected

Computer.Security@cern.ch — “Computer Security Day” — slide 52

▶ How can you get infected with malware?

You just run the malware

- ▶ taken from e-mail attachment or downloaded from the Web
- ▶ without knowing that this program is malicious

Be vigilant,
do not trust

You open infected pdf, doc, jpg etc., or visit an infected Web site

- ▶ and it exploits a vulnerability in your unpatched software
- ▶ or it exploits a “0-day” vulnerability (for which there is no patch available)

Patch your OS
and software

Do not
browse the Web ?

Getting infected on the Web

Computer.Security@cern.ch — “Computer Security Day” — slide 53

Infected Web – links from Google, social networking etc.

hyedd haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Oil Spill Oil Spill Oil Spill

haileyjnoqp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Oil Spill #firstdateturnoffs Olympic mascots

phylissro haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #theuglyfriend #firstdateturnoffs Stacey Dash

maryroseolaahb haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Olympic mascots Stacey Dash #firstdateturnoffs

hyedd haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #followerquestion Cerati Oil Spill

haileyjnoqp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Stacey Dash #firstdateturnoffs Oil Spill

maryroseolaahb haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Cerati #followerquestion #firstdateturnoffs

hyedd haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #theuglyfriend Olympic mascots #followerquestion

haileyjnoqp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Olympic mascots

phylissro haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> ash

tristakstp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Das

maryroseolaahb haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #followerquestion #theuglyfriend

phylissro haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #theuglyfriend #followerquestion #theuglyfriend

hyedd haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Olympic mascots Bustin Jieber #firstdateturnoffs

haileyjnoqp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Official Twitter App Olympic mascots #theuglyfriend

phylissro haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Official Twitter App Olympic mascots #followerquestion

tristakstp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #firstdateturnoffs Stacey Dash Olympic mascots

maryroseolaahb haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Official Twitter App #firstdateturnoffs Cerati

hyedd haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #theuglyfriend #followerquestion Oil Spill

haileyjnoqp haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> #followerquestion Olympic mascots #followerquestion

phylissro haha this is the funniest video ive EVER SEEN! <http://bit.ly/b6Z3BC> Stacey Dash Points Fiebig Points Jieber



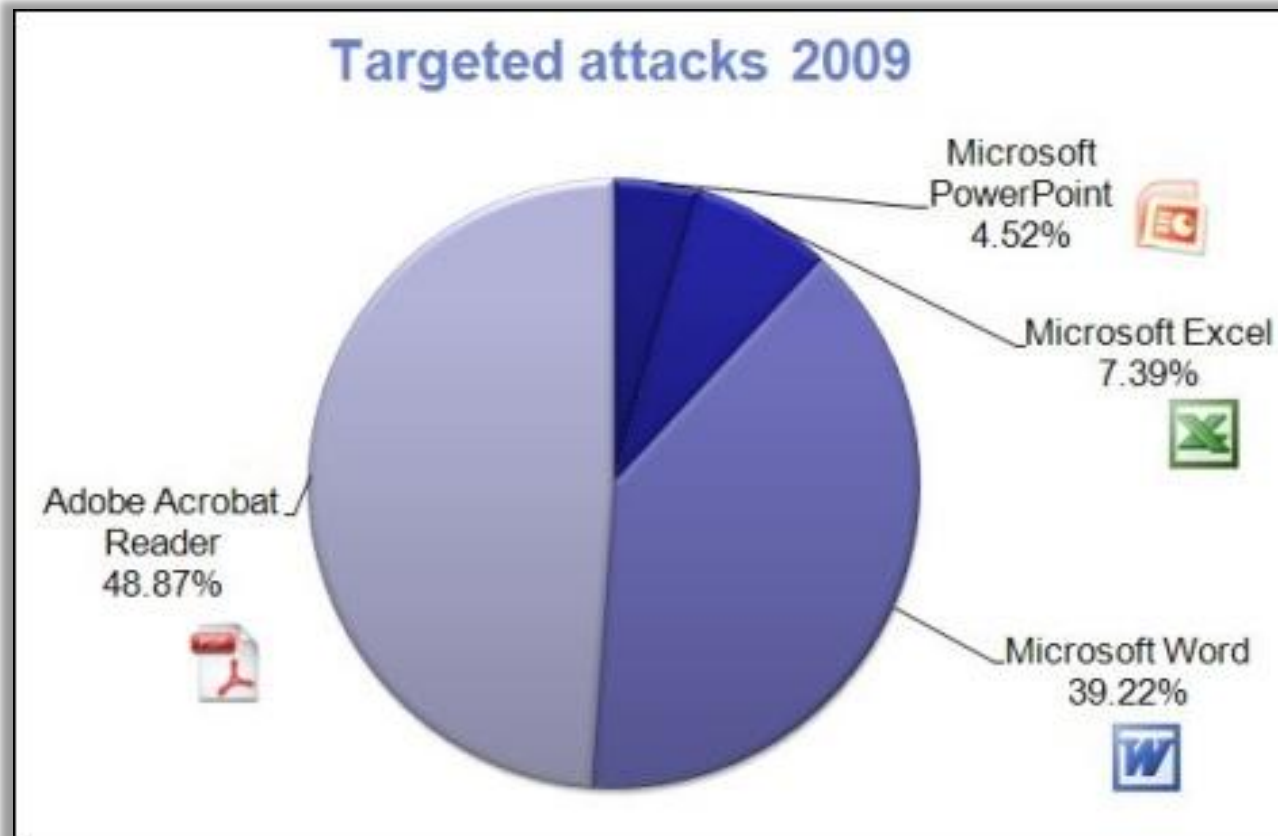
Malicious Web page
– infecting visitors

Getting infected

Computer.Security@cern.ch — “Computer Security Day” — slide 54

Opening infected documents

- ▶ sent as attachment via e-mail, or found on the Web
- ▶ mainly PDF (affecting also Macs!), and MS Office files



Privacy and the Web

Computer.Security@cern.ch — “Computer Security Day” — slide 55

Why is privacy important?

- ▶ criminals can use your personal information for identity theft
 - requesting credit cards, opening bank accounts in your name
 - breaking into your existing bank accounts etc.
 - hacking into your e-mail, Facebook etc. accounts
- ▶ ... or to trick you / your friends:
 - *“Hi Seb, is that you on this movie from Geneve-Rolle regatta?”*
versus
“Hello friend – open this very funny video”
 - and, of course, the video is infected (contains an exploit)....

Privacy and the Web

Computer.Security@cern.ch — “Computer Security Day” — slide 56

How do criminals find your personal information?

- ▶ They send you a “lottery won” spam, and ask for it
- ▶ They Google for it, and read it on Facebook
- ▶ They hack into your social networking or e-mail accounts, by
 - redirecting you to fake Web sites and “phishing” your password
 - infecting your computer and key-logging your password
 - exploiting “forgot my password” feature, and weak security questions - e.g. hacked Sarah Palin’s Yahoo e-mail account

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

the second was somewhat harder, the question was “where did you meet your spouse?” did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobuc you will see the google search for “palin eloped” or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on “Wasilla high” I promptly changed the password to popcorn and took a cold shower...

How secure are
your “security”
questions?

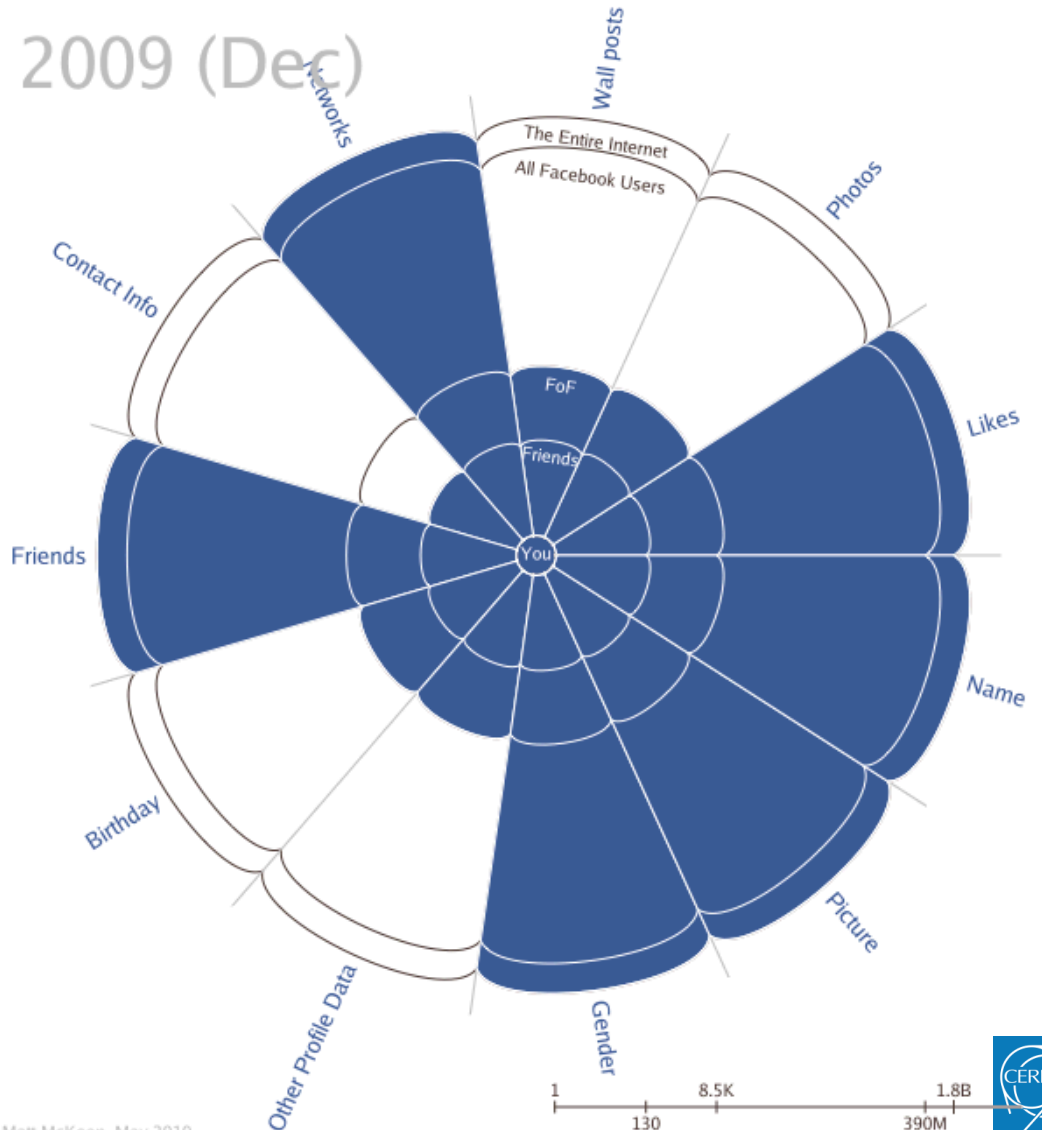
Privacy and the Web

Facebook



default privacy settings
evolution (=erosion)

See it [animated](#)



Privacy and the Web

BTW, what is *your* Facebook privacy score?

▶ How much do you share?

▶ Check at

<http://www.rabidgremlin.com/fbprivacy/>

Your privacy score is 8/21 [What does this mean?](#)

Happy with your score ? Then [share it with your friends](#) and see what score they get.

profile data

[view raw data](#)

Facebook ID: [REDACTED]

Name: [REDACTED]

Birthday: -

Gender: male

Relationship status: -

Timezone: 12

Hometown: Auckland, New Zealand

Location: Auckland, New Zealand

School(s): Auckland Grammar School,
Auckland University,

Employer(s): Crash it Ltd,

other data

[view raw data](#)

1 number of friends exposed

Facebook always gives out your friends list :(

[view raw data](#)

0 number of items on news feed exposed





SECURITY is not complete without U

Computer Security Day
10 June 2010, Council Chamber and <http://cern.ch/SecDay>

Conclusions

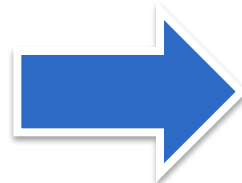
Conclusions

Computer.Security@cern.ch — “Computer Security Day” — slide 60

- ▶ **As you see, it's a real business (and not just hobbyists)**
 - ▶ Main motivation: money (and very low risk of being caught)
 - ▶ Is undermining cybercrime *economy* the way to win?
 - ▶ BTW, Al Capone was sentenced for tax evasion, not for other crimes...

- ▶ **Attacks are advanced, both technically, and “socially”**

- ▶ Be aware
- ▶ Be vigilant
- ▶ Follow secure computing advice



SECURITY is not complete without

Quelques astuces pour protéger votre ordinateur et vos données

- Utilisez les systèmes d'exploitation fournis par le département IT du CERN :** ils sont configurés de manière sûre et mis à jour automatiquement pour vous.
- Protégez votre ordinateur privé :** utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.
- Soyez prudent lorsque vous naviguez sur le Web :** ne cliquez pas sur des liens suspects et n'installez pas de plug-in douteux.
- Protégez vos fichiers et données :** limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.
- Protégez vos mots de passe :** ne les partagez jamais; prenez garde au phishing (technique qu'utilisent les escrocs en ligne pour voler votre mot de passe); ne les réutilisez pas (utilisez des mots de passe différents pour des applications différentes); ne les tapez pas sur des ordinateurs ou des sites Web suspects.
- Suivez les règles informatiques du CERN :** respectez le droit d'auteur; n'utilisez pas de logiciels non-autorisés; consultez <http://cern.ch/ComputingRules>.
- Demandez conseil :** l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider : contactez Computer.Security@cern.ch ou consultez <http://cern.ch/Computer.Security>.

Thank you

Computer.Security@cern.ch — “Computer Security Day” — slide 61



Any questions?