UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

Úvod do bezpečného pohybu na Internetu

Školení B1 k projektu Dotyk

Miroslav Hlávka

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obsah

Motivace k využívání Internetu

- jakou informaci hledám?
- jaké zdroje využívám?
- co jsem ochoten riskovat pro její získání?
- v případě napadení o co mohu přijít?
- zvažte pro a proti

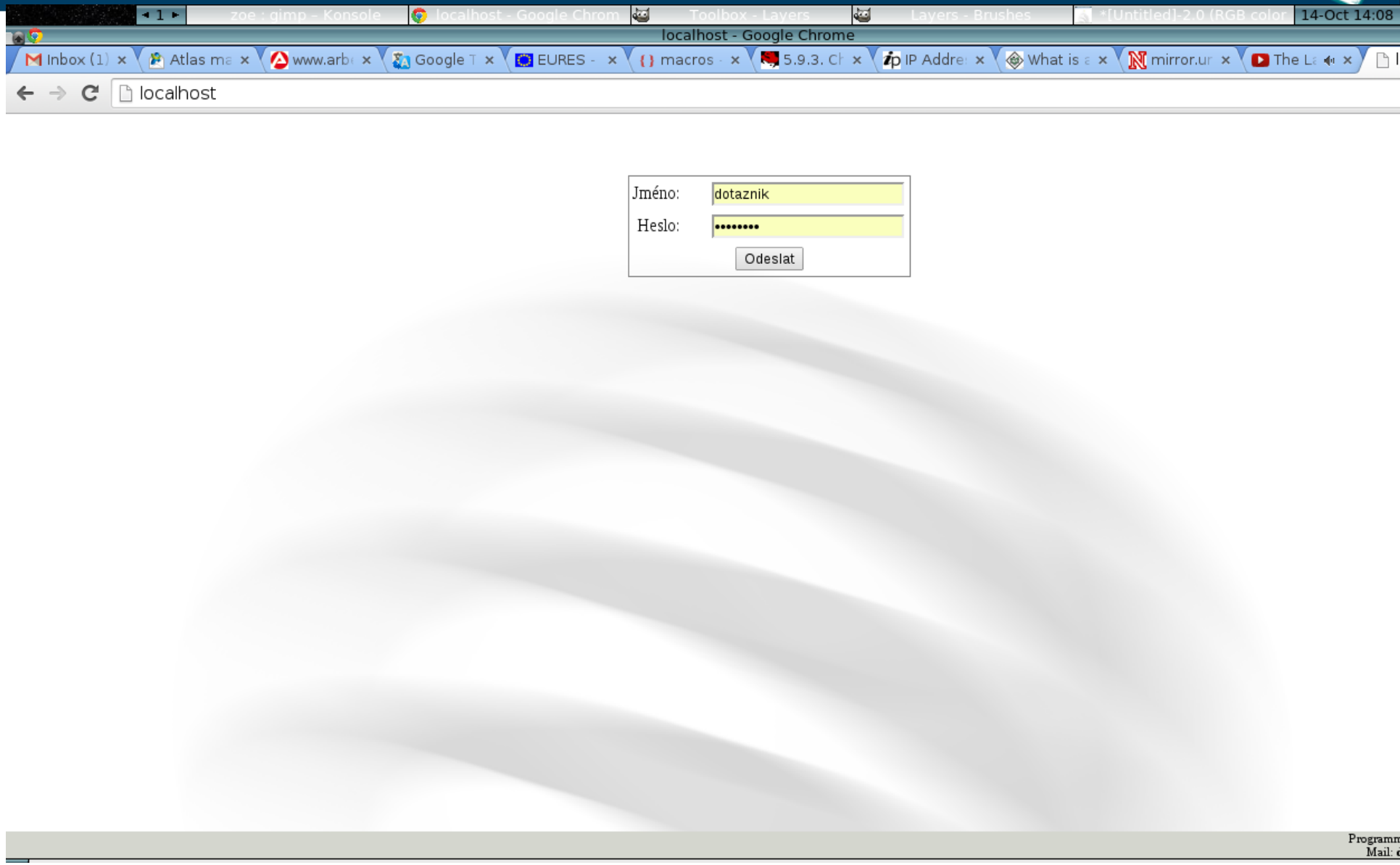
Internetové služby

- poskytování služeb na vzdáleném serveru (SaaS - webmail, Facebook, Dropbox, Netflix, Bakláři)
- všechny služby vyžadují ověření (heslo, SSL certifikát, OTP)
- volba správného managementu hesel a hesel samotných

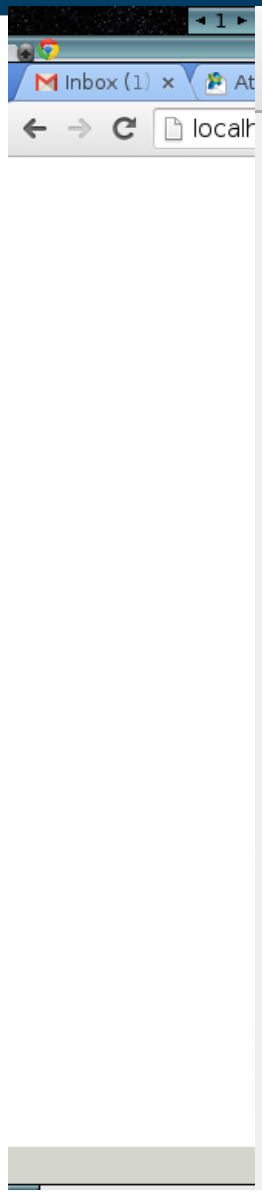
Hesla

- řada služeb, které využíváme jak online, tak offline využívá ověření heslem
- znalost uživatelského jména a hesla většinou postačuje k tomu, aby daná služba byla ovládána na administrátorské úrovni
- uživatelská jména a hesla je třeba bedlivě chránit
- obecně známé nástroje pro lámání hesel (John the Ripper, Hydra)

Lámání hesel



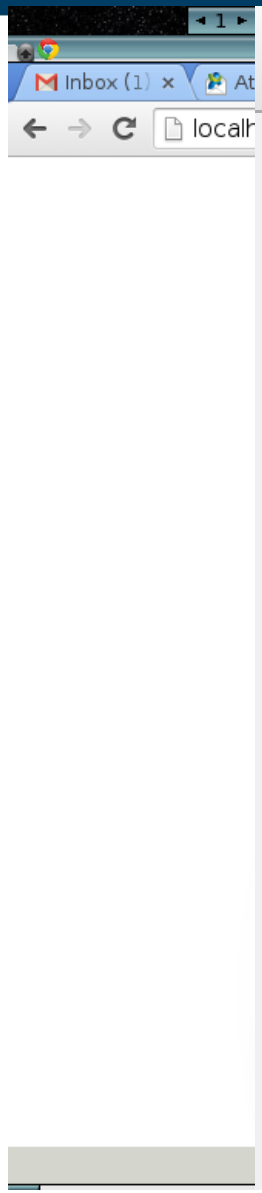
Lámání hesel



view-source:localhost

```
1  <html>
2  <head>
3  <script src="http://code.jquery.com/jquery.js"></script>
4  <script src="js/header.js"></script>
5  <script src="js/jfooter.js"></script>
6  <link rel='stylesheet' type='text/css' href='js/general.css'>
7  <meta http-equiv="content-type" content="text/html;charset=utf-8"
8  </head>
9  <body>
10 <form name="user_login" action="dotaznik.php" method="post">
11 <table class="login">
12         <tr><td>Jméno: </td><td><input type="text" name="user"></t
13         <tr><td>Heslo: </td><td><input type="password" name="pass"
14         <tr><td colspan=2 class="submit"><input type="submit" valu
15 </table>
16 </form>
17 <div id="footer">
18 <script src="js/footer.js"></script>
19 </div>
20 </body>
21 </html>
22
```

Lámání hesel

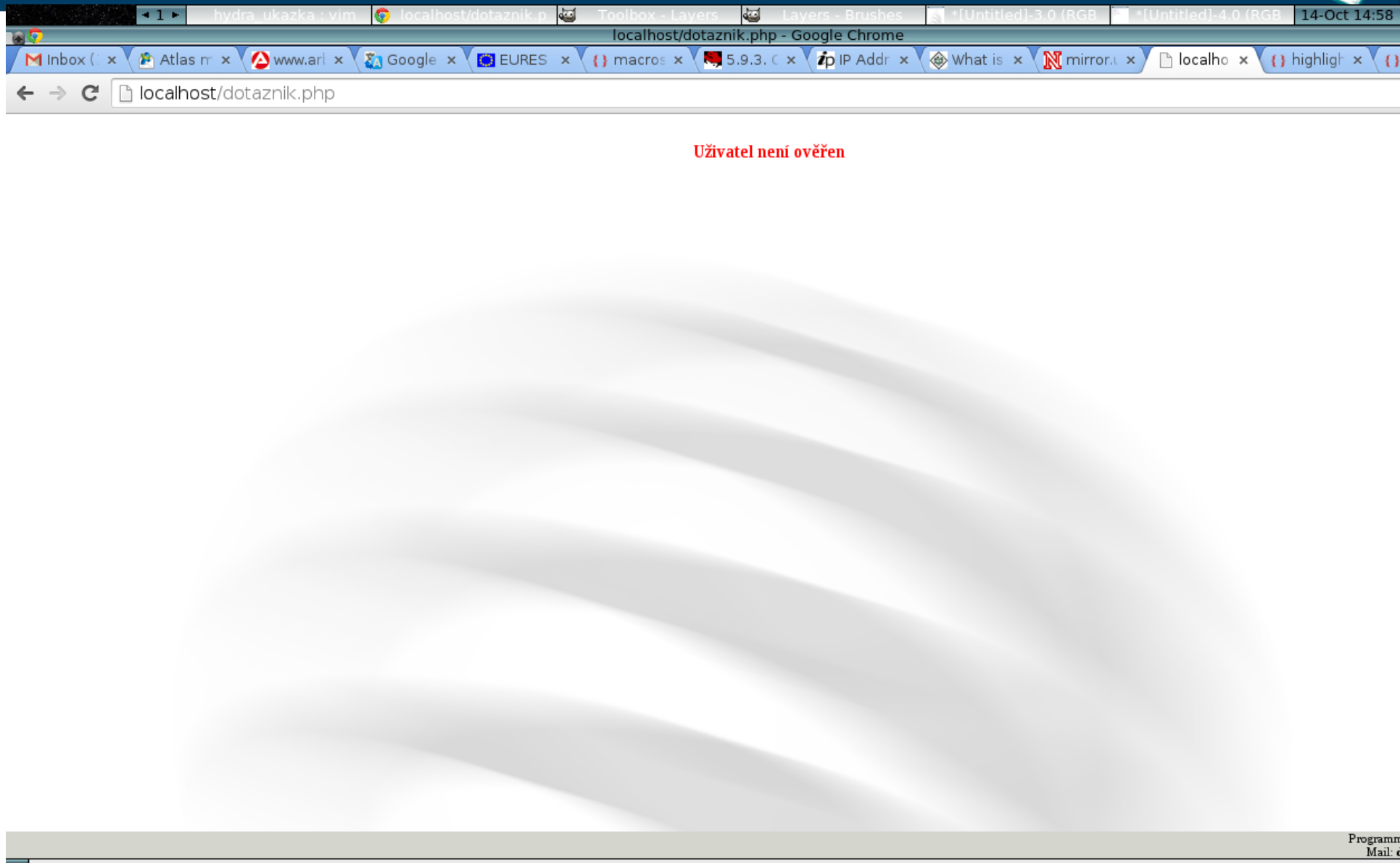


view-source:localhost

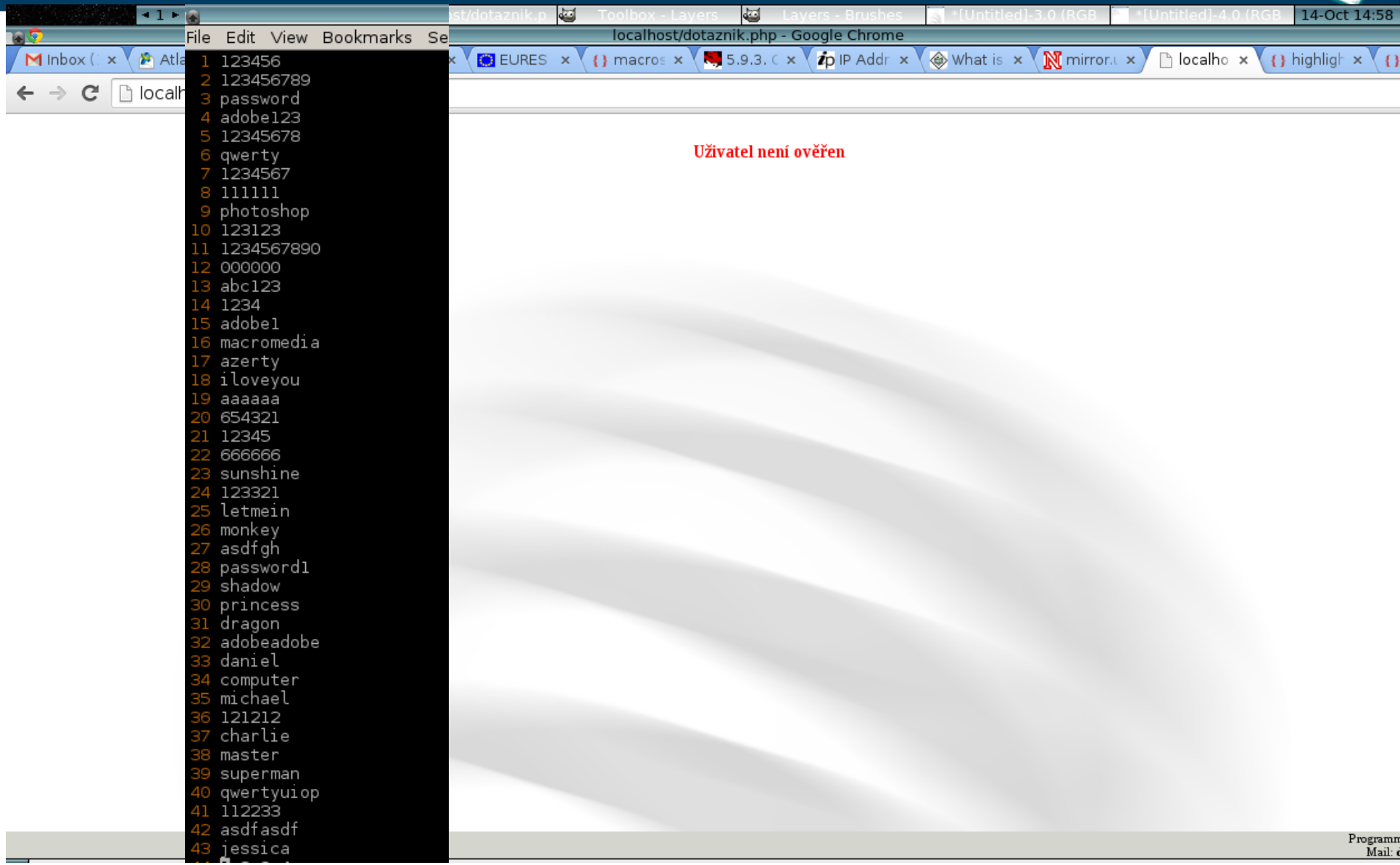
```
1  <html>
2  <head>
3  <script src="http://code.jquery.com/jquery.js"></script>
4  <script src="js/header.js"></script>
5  <script src="js/jfooter.js"></script>
6  <link rel='stylesheet' type='text/css' href='js/general.css'>
7  <meta http-equiv="content-type" content="text/html;charset=utf-8"
8  </head>
9  <body>
10 <form name="user_login" action="dotaznik.php" method="post">
11 <table class="
12         <tr><
13         <tr><
14         <tr><
15 </table>
16 </form>
17 <div id="foot
18 <script src="
19 </div>
20 </body>
21 </html>
22
```

- základní stránka s žádostí o zalogování (použité PHP a JS)
- bez znalosti jména/hesla je ze zdrojového kódu možno zjistit, jak se data předávají dále
- poté je potřeba pokusit se přihlásit byť neúspěšně a může se začít s útokem

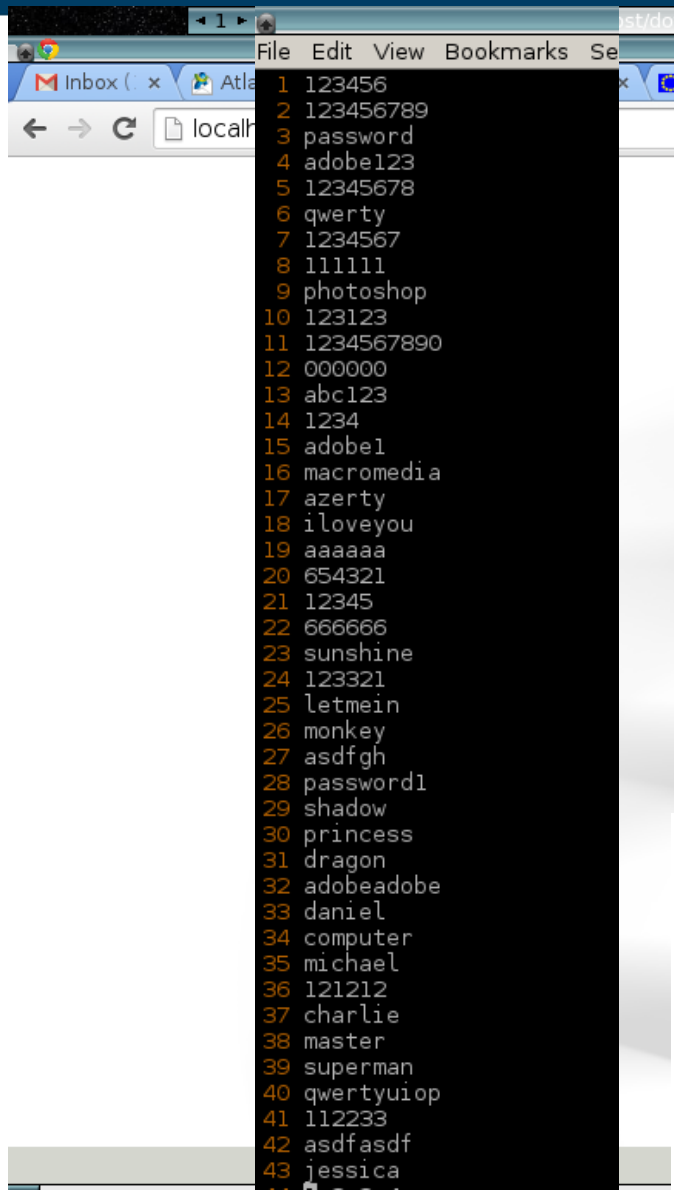
Lámání hesel



Lámání hesel

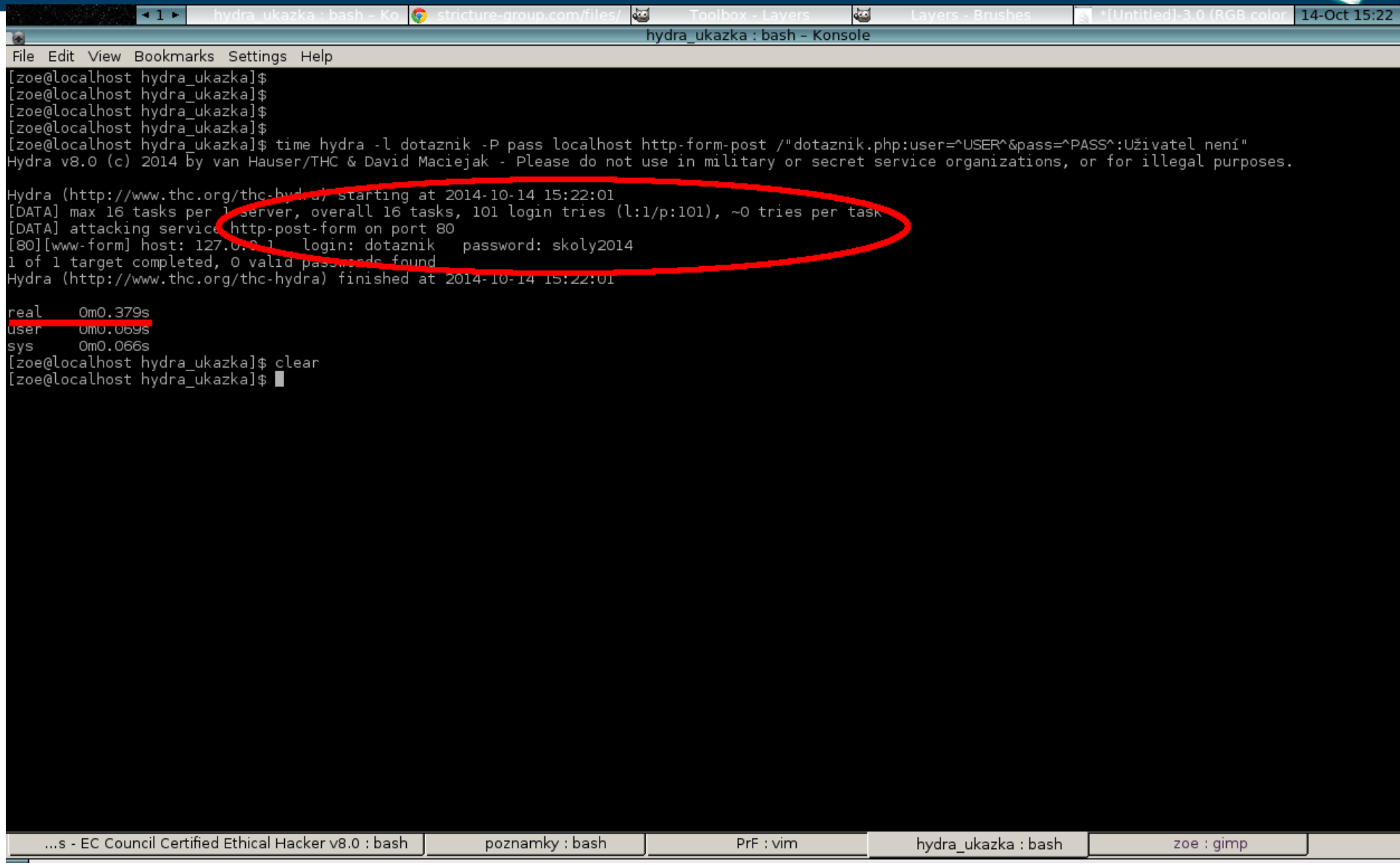


Lámání hesel

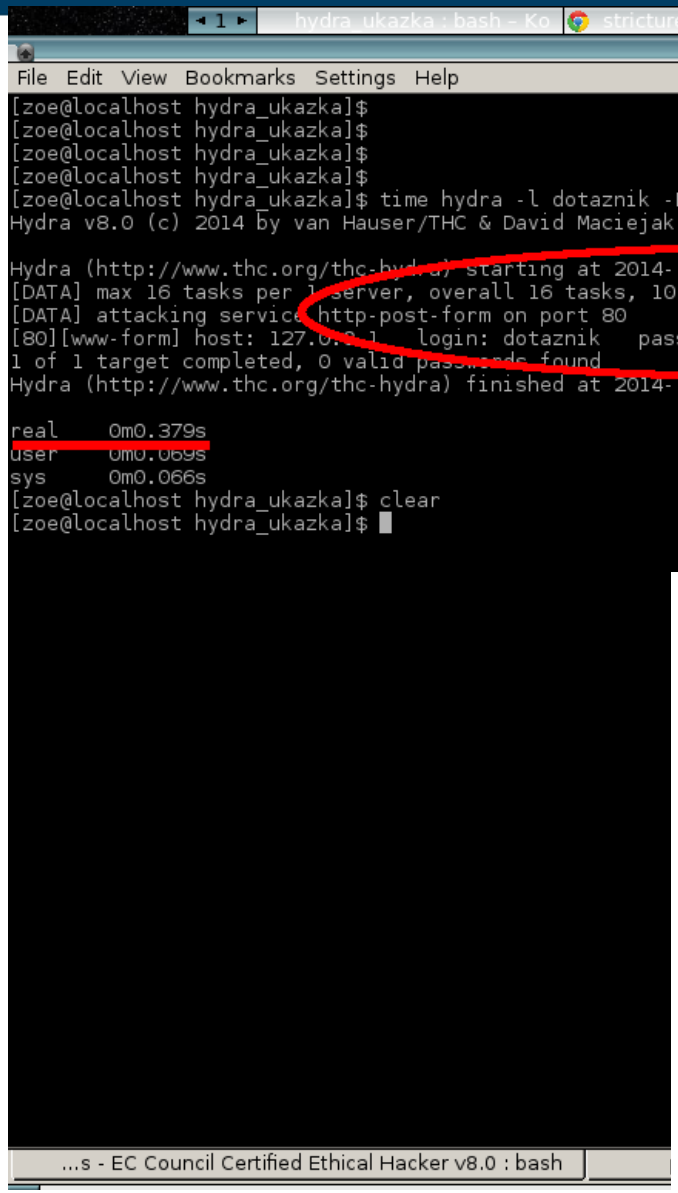


- pro slovníkový útok použijeme nejpoužívanější hesla
- stejně tak můžeme použít i slovník pro uživatelská jména

Lámání hesel



Lámání hesel



- během půl vteřiny Hydra otestovala všech 101 hesel a protože jedno je správné vytiskla jej
- podobným způsobem je možno útočit na řadu síťových služeb
- proto je nezbytné vyhýbat se slovům vyskytujícím se ve slovnících

Pravidla pro tvorbu hesla

- nemělo by být součástí slovníku k jakémukoliv jazyku
- alespoň 8 znaků dlouhé
- mělo by obsahovat velká/malá písmena, číslice a znaky (@! + −)
- nemělo by být programově uhodnutelné
- snadno zapamatovatelné
- jedno heslo pro jednu službu
- nepoužívat reálie, spojitelné s Vaší osobou (kř. jméno, SPZ, data narození)
- používejte passphrase nebo heslo z ní odvozené (ctyrisluncejedobryfilm - C$JdF2012)
- použijte keymanager (KeePass)

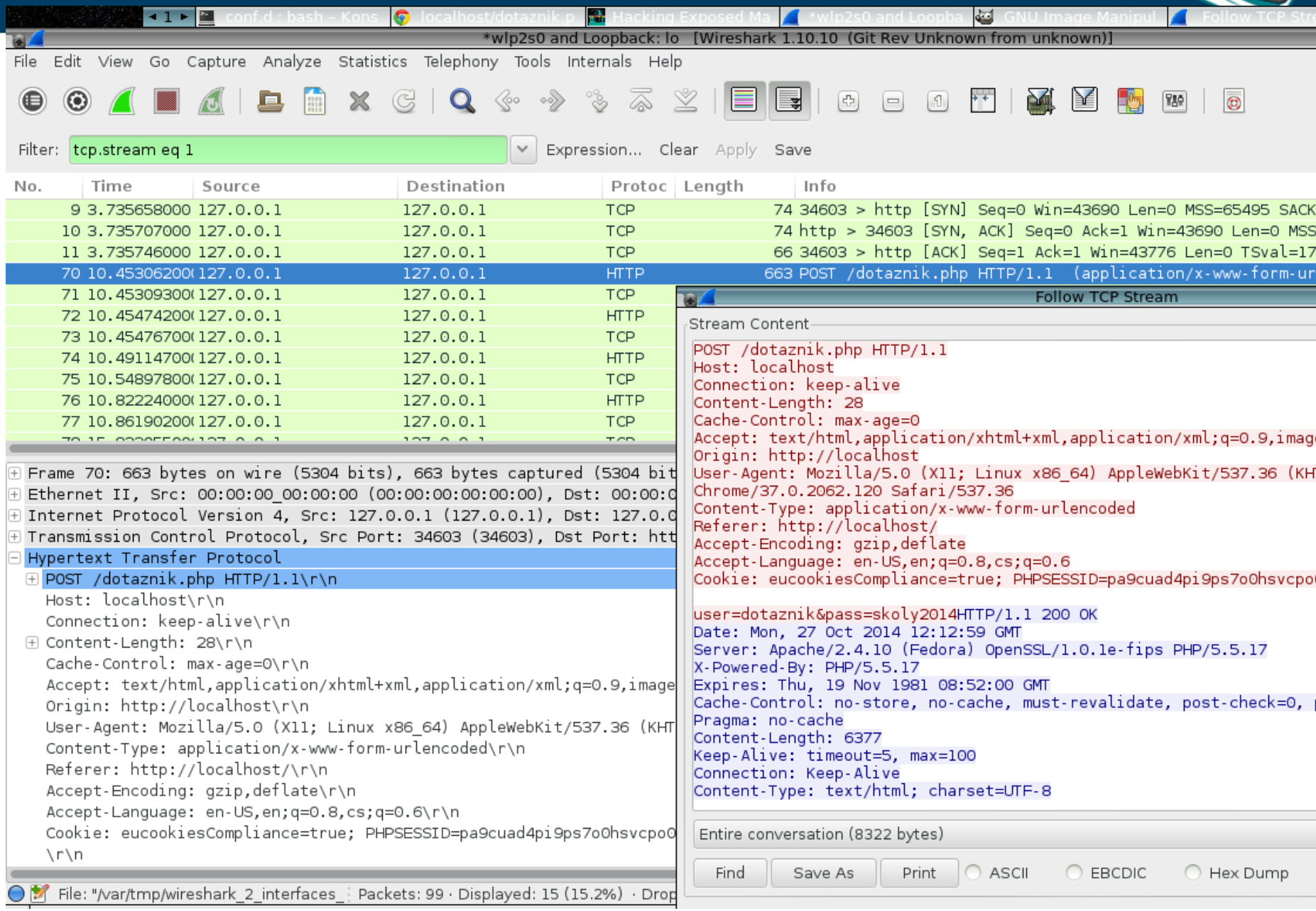
Historické okénko

- ARPANET - packet switched network (1969); TCP/IP (1978)
- Telnet (RFC15 - 1969)
- SMTP (RFC196 - 1971)
- FTP (RFC114 - 1971)
- POP (RFC918 - 1984)
- IMAP (RFC1176 - 1990)
- HTTP (RFC1945 - 1996)

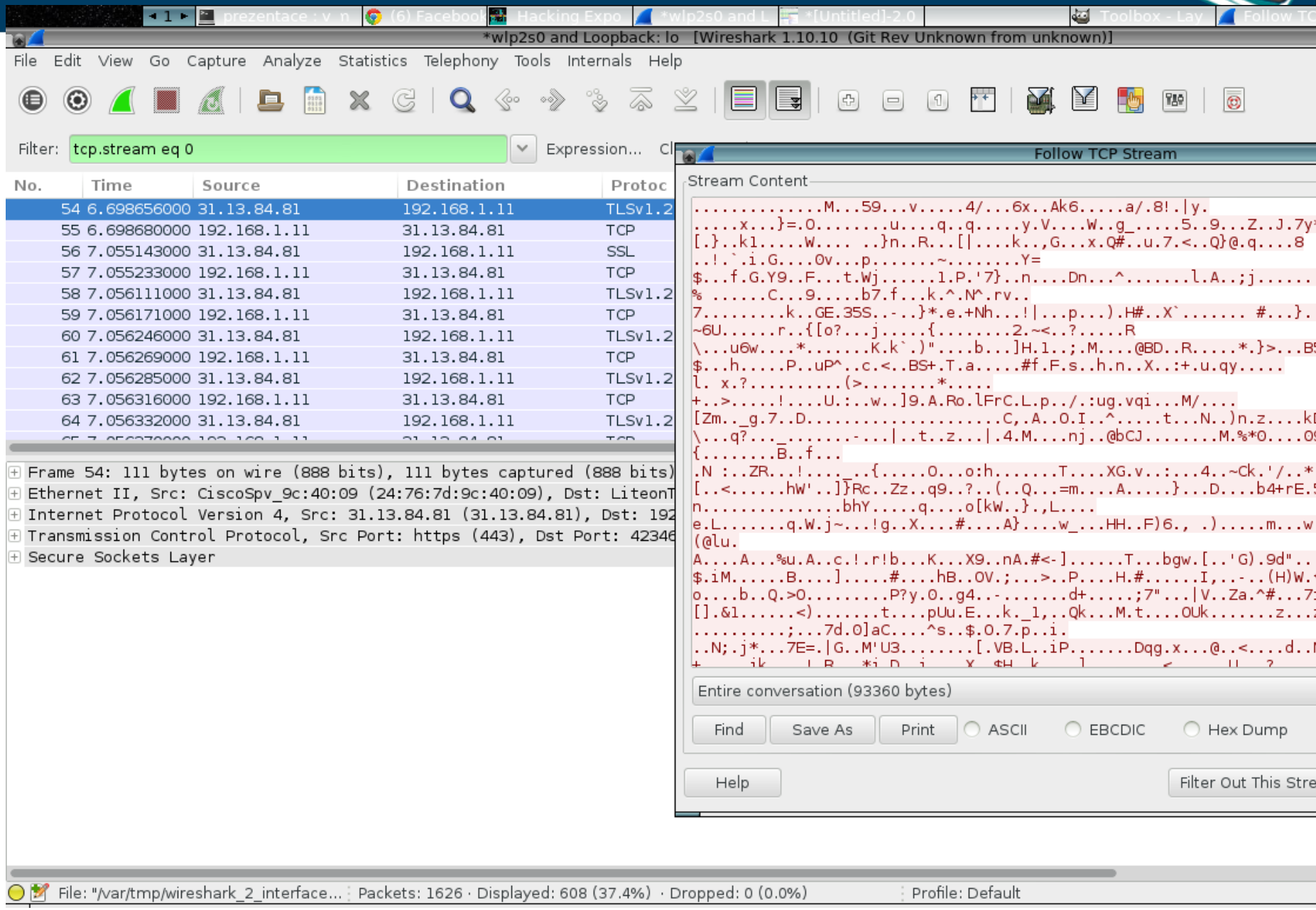
Historické okénko

- ARPANET - packet switched network (1969); TCP/IP (1978)
- Telnet (RFC15 - 1969)
- SMTP (RFC196 - 1971)
- FTP (RFC114 - 1971)
- POP (RFC918 - 1984)
- IMAP (RFC1176 - 1990)
- HTTP (RFC1945 - 1996)
- SSH (1995)
- SMTPS (RFC2487 - 1999)
- FTPS (RFC4217 - 2005)
- POPS, IMAPS (RFC2595 - 1999)
- HTTPS (RFC2818 - 2000)

Přenos dat nezabezpečeně



Přenos dat zabezpečeně

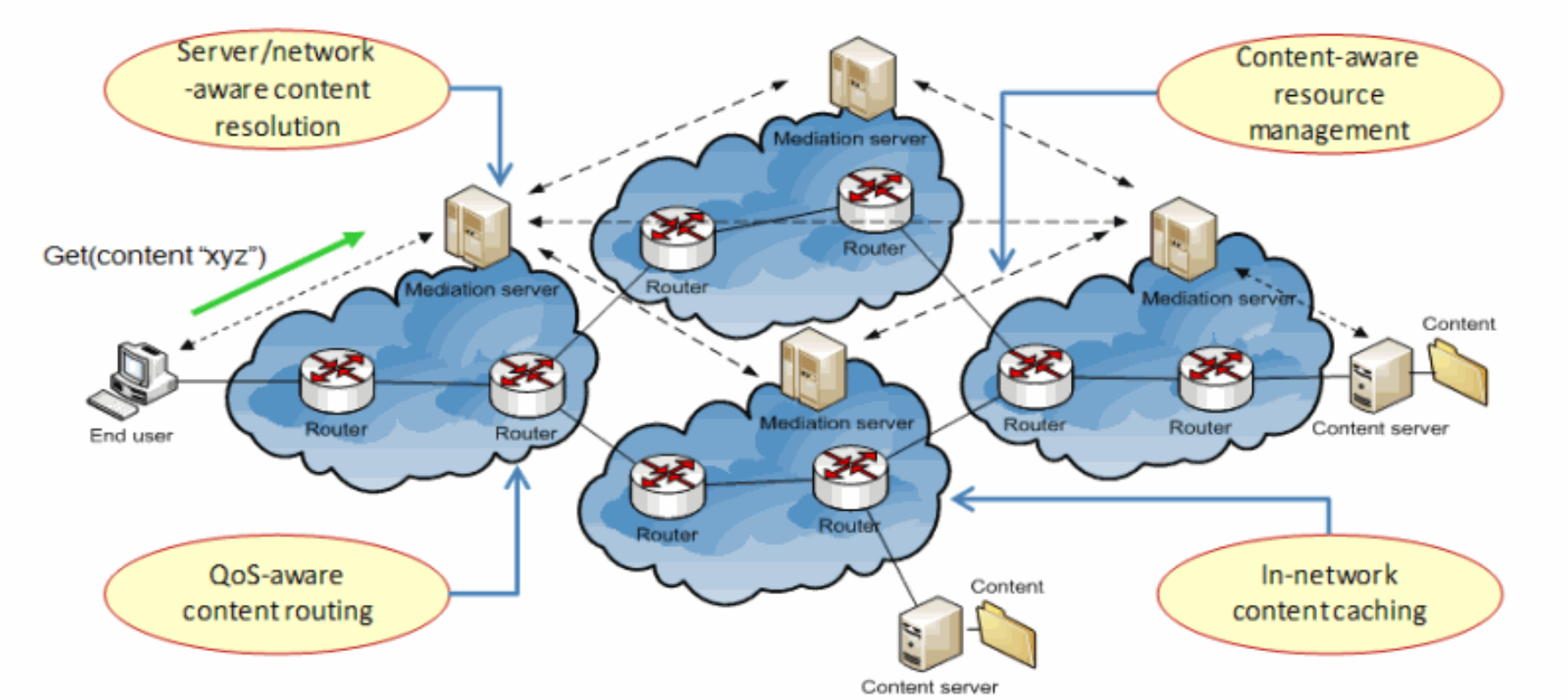


Proč se dějí nepěkné věci v síti?

- nepřeberné množství aktivit spojených s únikem informací
- vesměs ilegální
- motivace vzniku:
  - výzva, prestiž, dlouhá chvíle, zlost na zaměstnavatele
  - špionáž (Stuxnet)
  - **finanční zisk**

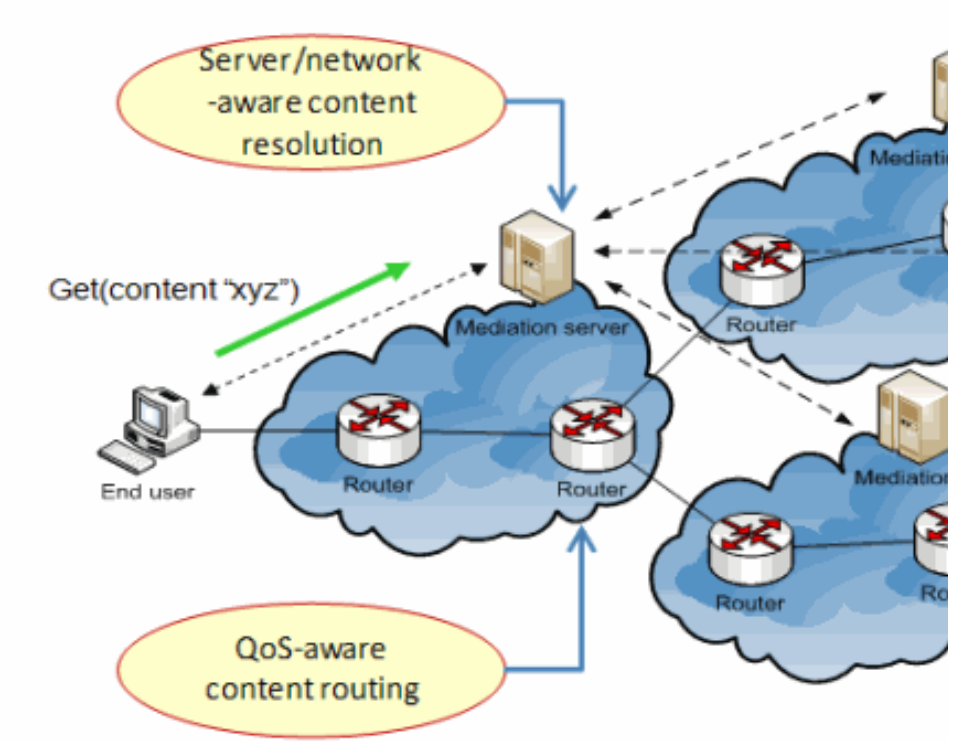
Obrázek: [?]

Odposlouchávání



Obrázek: [?]

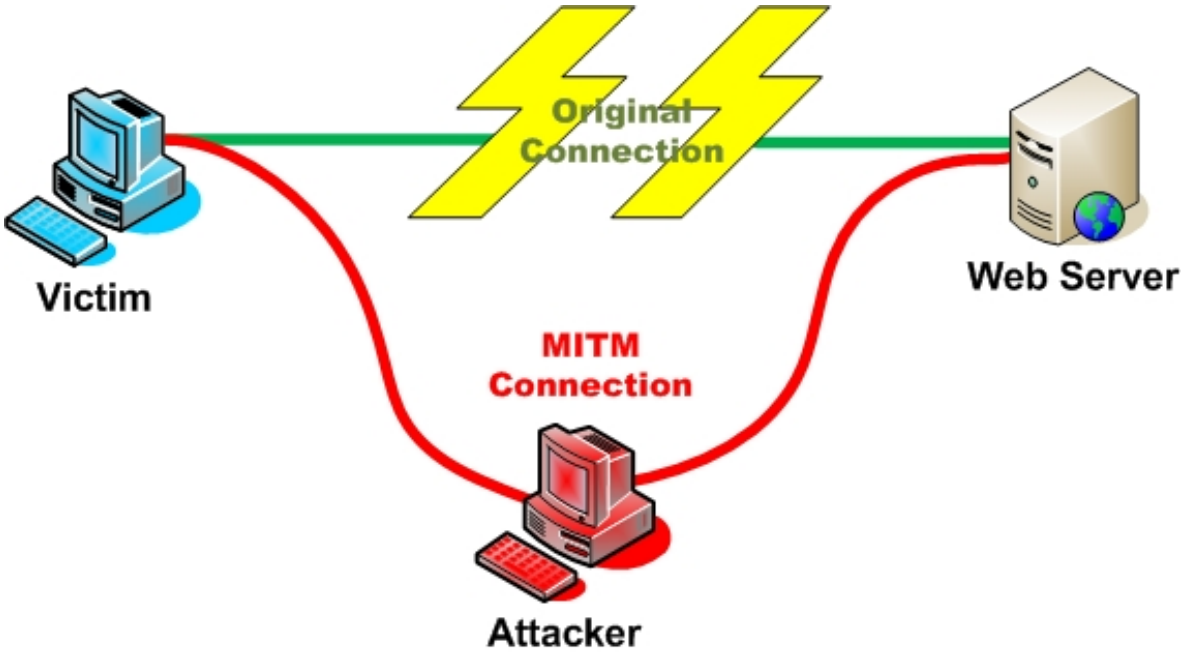
Odposlouchávání



Obrázek: [?]

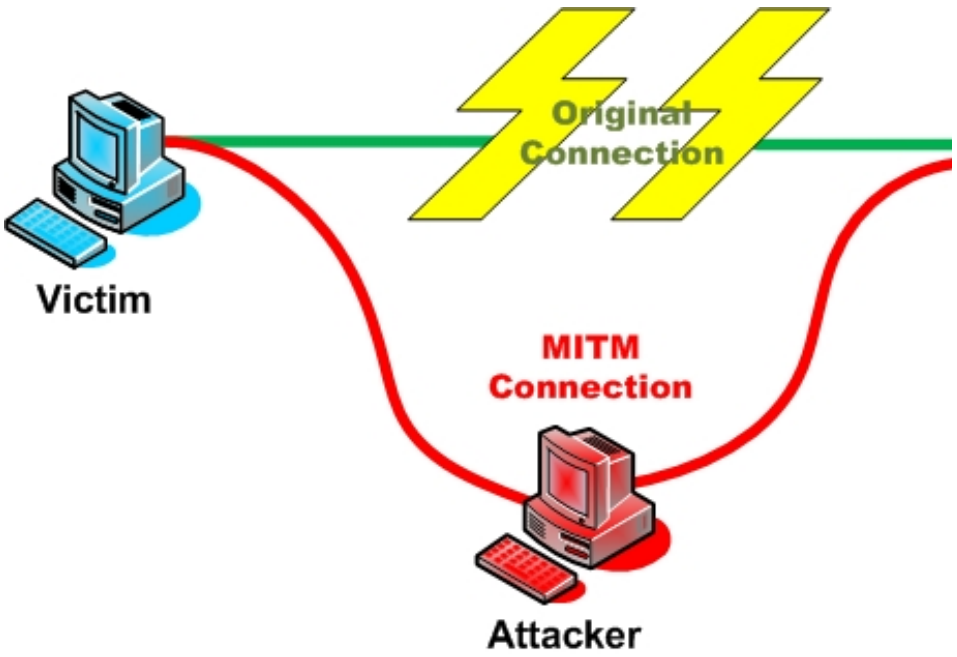
- nekryptovaná data mohou být odposlechnuta v závislosti na designu sítě
- téměř všechna zařízení po cestě mohou být použita k odposlechu
- založeno na důvěře administrátorům
- částečně lze omezit používáním kryptovaných protokolů

Síťové útoky zaměřené na odposlech - MiTM



Obrázek: [?]

Síťové útoky zaměřené na odposlech - MiTM



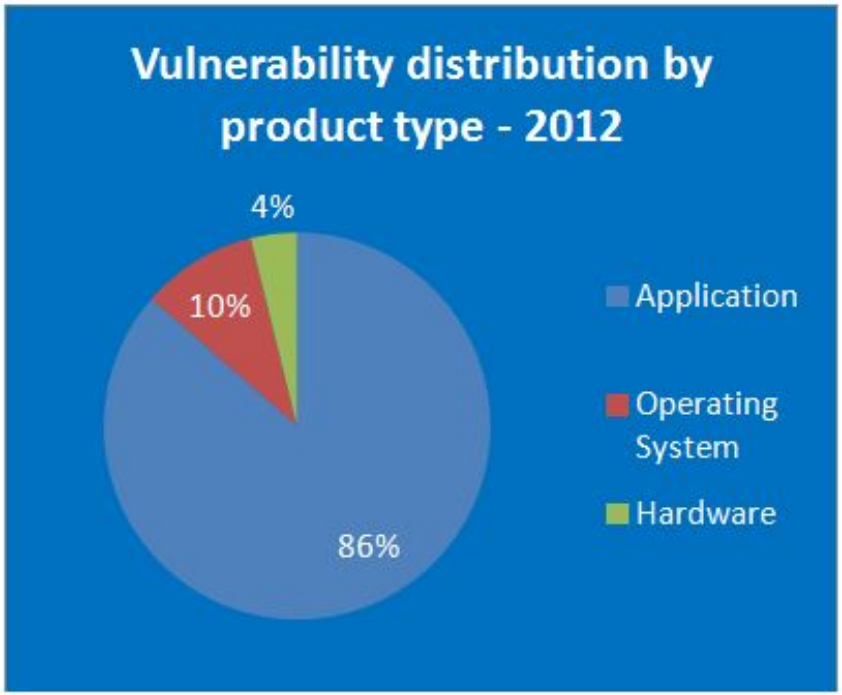
Obrázek: [?]

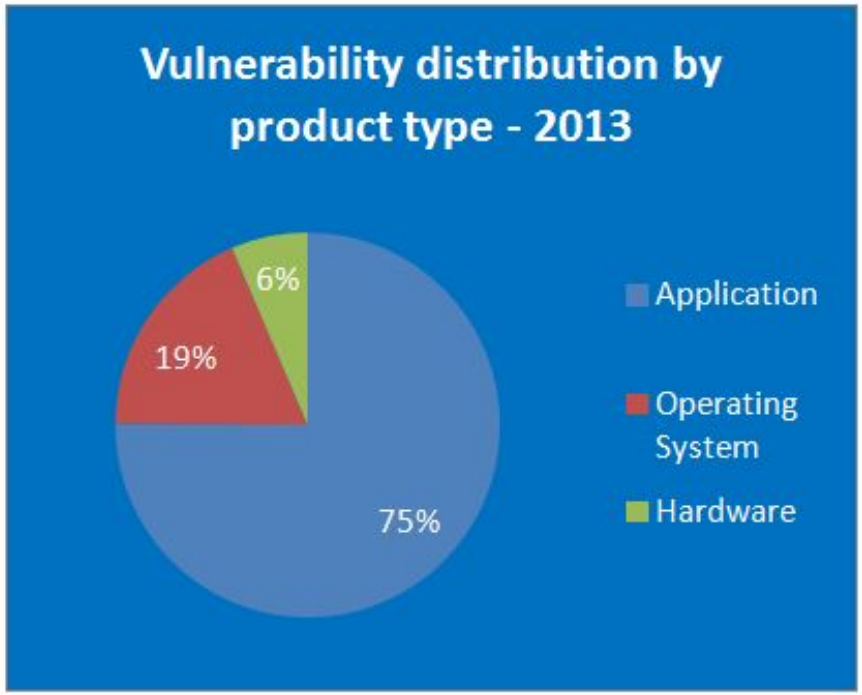
- vyžadují znalost TCP/IP, síťové topologie, prostředí
- děje se převážně v LAN
- využívá ARP spoof(LAN), DNS poisoning(WAN)
- veškerá komunikace je přesměrována útočníkovi
- útočník za určitých okolností může číst HTTPS komunikaci
- obrana na síťové úrovni (DAI), DNSSEC, SSL oboustranná identifikace

Škodlivý software - malware

- software vytvořený za účelem poškodit uživatele
- souhrnný název pro viry, červy, spyware, keyloggery . . .
- šíření malware:
  - social engineering, SPAM
  - bezpečnostní díry v software
  - drive-by download (warez, gaming, porn)
  - file sharing (P2P, USB)

Přehled bezpečnostních chyb





Obrázek: [?]

Přehled bezpečnostních chyb

Vendor	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2013	2012	2013	2012	2013	2012	2013	2012
Oracle	↑ 514	424	↑ 131	76	↑ 316	238	↓ 67	110
Cisco	↑ 373	134	↑ 126	85	↑ 243	45	● 4	4
Microsoft	↑ 344	169	↑ 248	117	↑ 93	48	↓ 3	4
IBM	↑ 336	154	↑ 54	42	↑ 199	94	↑ 83	18
Apple	↓ 190	270	↓ 37	141	↑ 123	115	↑ 30	14
Google	↑ 188	150	↑ 110	79	↓ 77	66	↓ 1	5
Mozilla	↓ 161	195	↓ 98	118	↓ 61	72	↓ 2	5
Adobe	↑ 146	137	↑ 138	127	↓ 7	10	↑ 1	0
Red Hat	↑ 131	30	↑ 27	2	↑ 77	19	↑ 27	9
HP	↑ 112	74	↑ 65	38	↑ 38	31	↑ 9	5

Obrázek: [?]

Přehled bezpečnostních chyb

Operating system	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2013	2012	2013	2012	2013	2012	2013	2012
Microsoft Windows Server 2008	↑ 104	48	↑ 58	35	↑ 46	12	↓ 0	1
Microsoft Windows 7	↑ 100	42	↑ 55	33	↑ 45	8	↓ 0	1
Microsoft Windows Vista	↑ 96	41	↑ 53	34	↑ 43	6	↓ 0	1
Microsoft Windows XP	↑ 88	42	↑ 47	37	↑ 41	5	● 0	0
Microsoft Windows Server 2003	↑ 86	45	↑ 46	40	↑ 40	5	● 0	0
Microsoft Windows 8	↑ 58	5	↑ 43	5	↑ 14	0	↑ 1	0
Linux Kernel	↑ 158	45	↑ 15	12	↑ 119	28	↑ 24	5
Microsoft Windows Server 2012	↑ 51	5	↑ 37	4	↑ 13	1	↑ 1	0
Microsoft Windows RT	↑ 42	2	↑ 32	2	↑ 9	0	↑ 1	0
Apple iOS	↑ 89	86	↓ 19	46	↑ 55	28	↑ 15	12
Cisco IOS	↓ 34	36	↓ 19	23	↑ 15	10	↓ 0	3
Ubuntu Linux	↑ 72	6	↑ 10	0	↑ 55	5	↑ 7	1
Cisco IOS XE	↑ 23	9	↑ 16	9	↑ 7	0	● 0	0
Red Hat Enterprise Linux	↑ 54	2	↑ 9	0	↑ 37	1	↑ 8	1
openSUSE	↑ 49	0	↑ 11	0	↑ 26	0	↑ 12	0
Apple Mac OS X	↑ 63	21	↑ 5	3	↑ 44	16	↑ 14	2

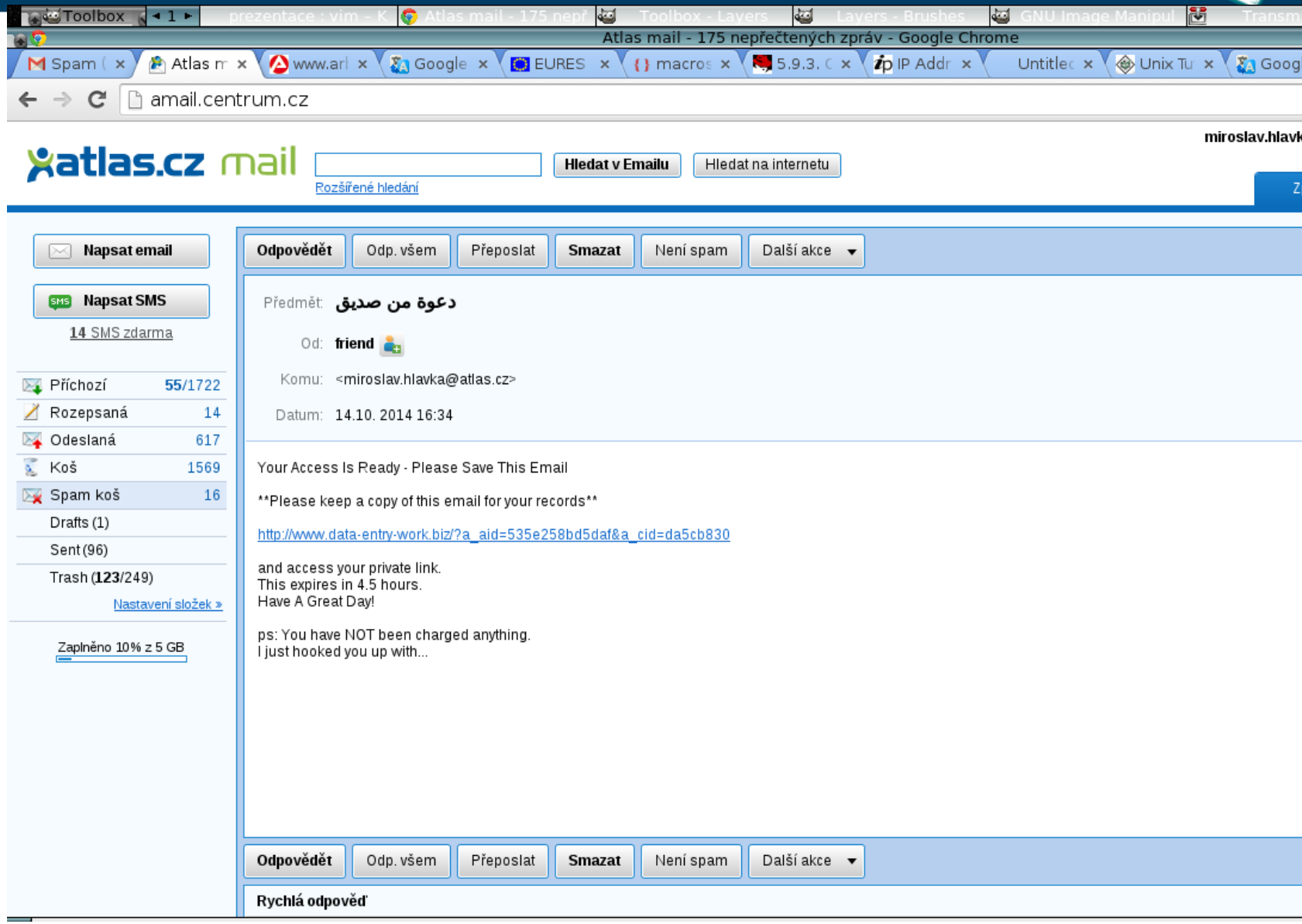
Obrázek: [?]

Přehled bezpečnostních chyb

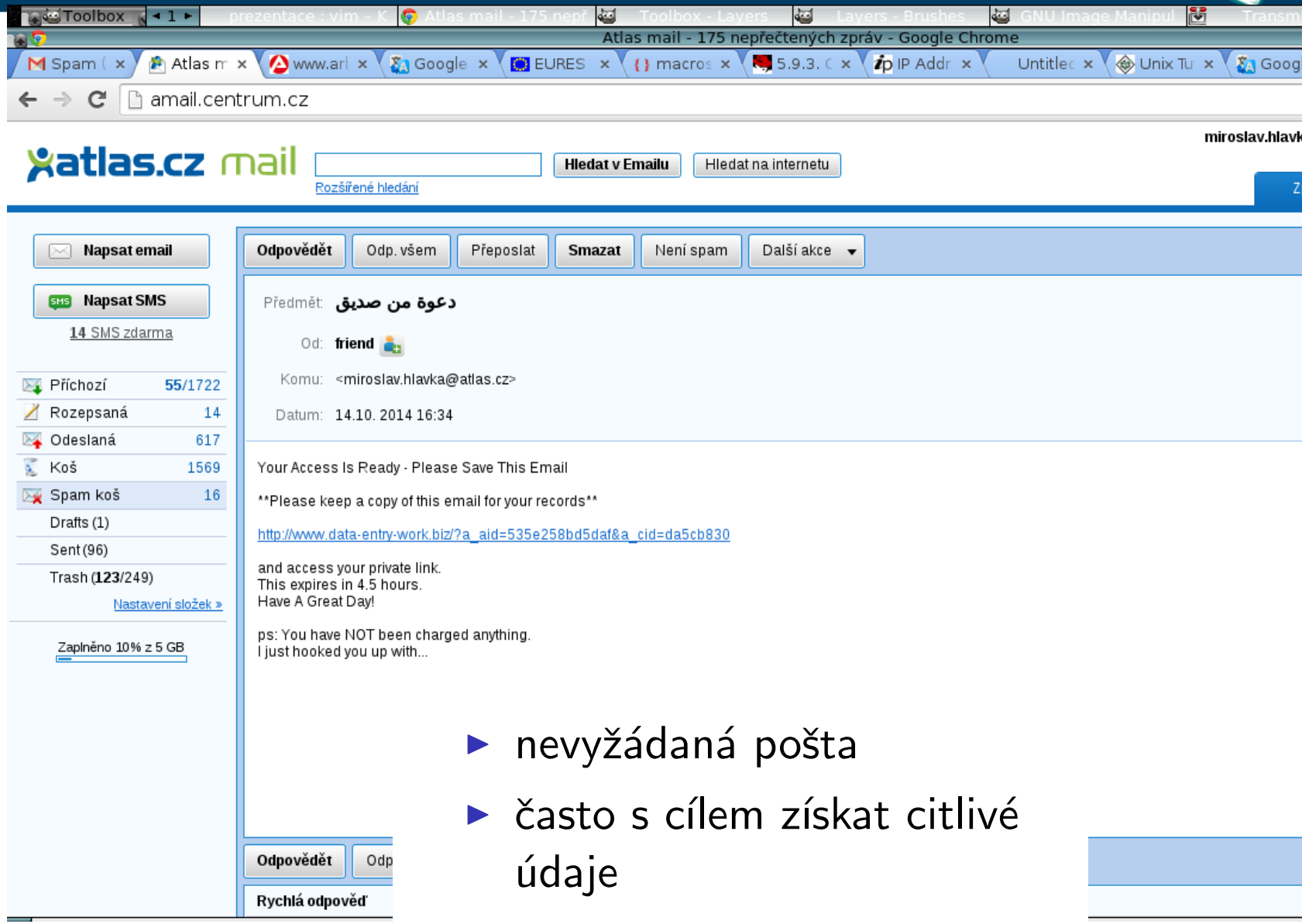
Application	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2013	2012	2013	2012	2013	2012	2013	2012
Microsoft Internet Explorer	↑ 128	41	↑ 117	34	↑ 11	7	● 0	0
Oracle Java	↑ 193	58	↑ 102	32	↑ 84	20	↑ 7	6
Google Chrome	↑ 168	125	↑ 100	68	↑ 67	55	↓ 1	2
Mozilla Firefox	↓ 149	159	↓ 96	99	↓ 51	55	↓ 2	5
Mozilla Thunderbird	↓ 113	144	↓ 82	95	↓ 31	47	↓ 0	2
Mozilla Firefox ESR	↓ 100	115	↓ 74	75	↓ 26	39	↓ 0	1
Mozilla SeaMonkey	↓ 104	143	↓ 70	94	↓ 34	46	↓ 0	3
Mozilla Thunderbird ESR	↓ 87	109	↓ 64	74	↓ 23	34	↓ 0	1
Adobe Reader	↑ 65	25	↑ 64	25	↑ 1	0	● 0	0
Adobe Acrobat	↑ 63	24	↑ 62	24	↑ 1	0	● 0	0
Adobe Flash Player	↓ 56	66	↓ 55	61	↓ 1	5	● 0	0
Adobe Air	↓ 48	54	↓ 47	51	↓ 1	3	● 0	0

Obrázek: [?]

Podvodné e-maily

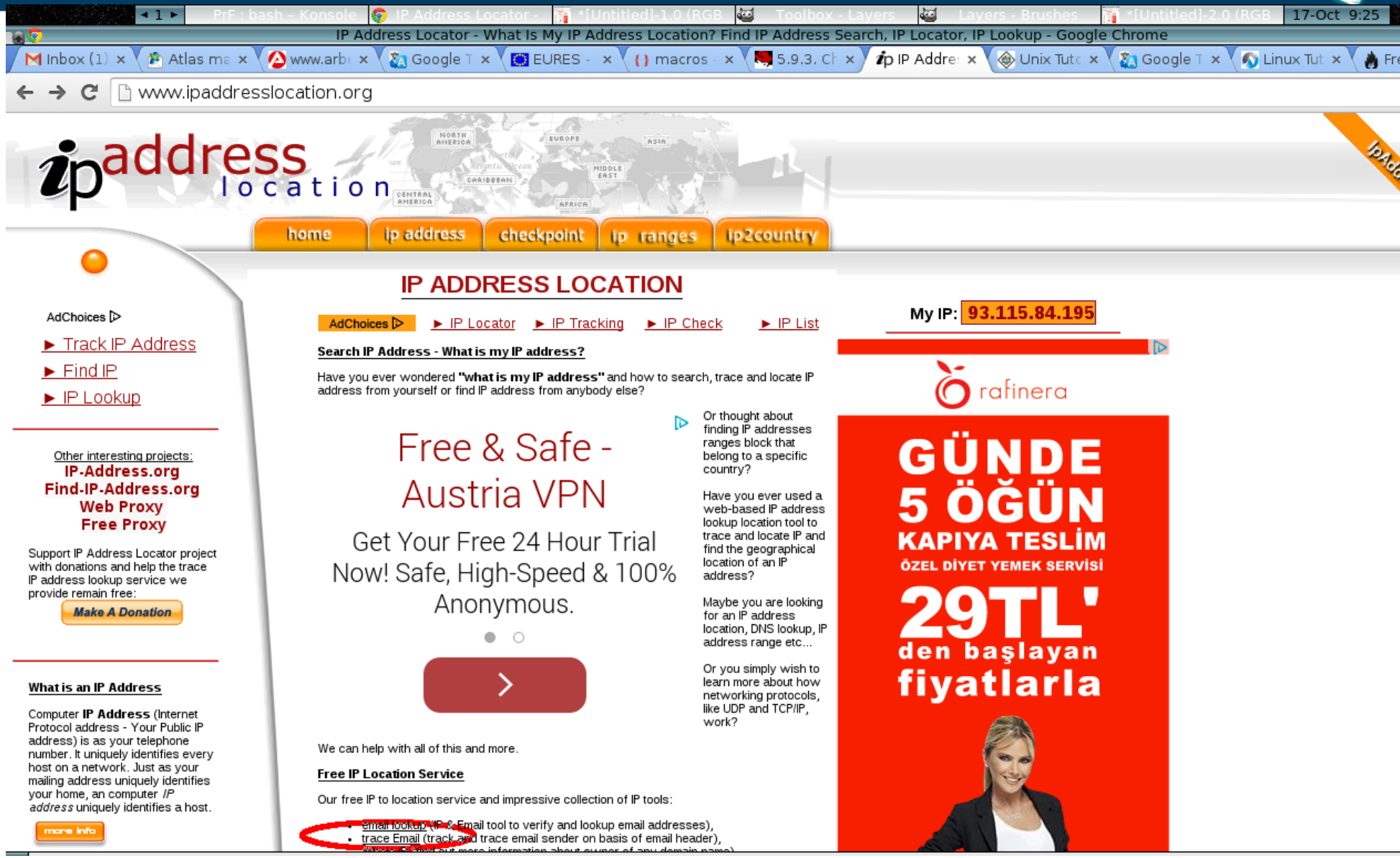


Podvodné e-maily



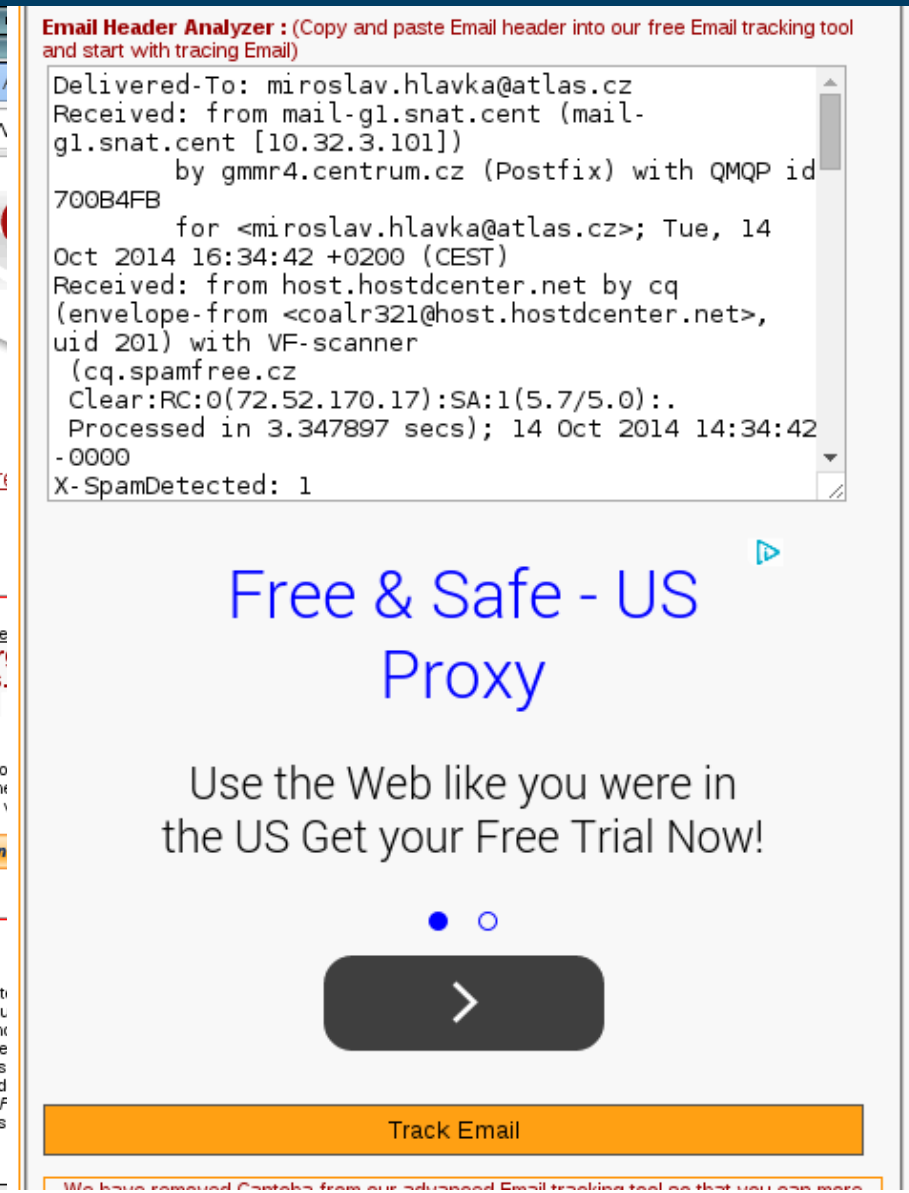
- nevyžádaná pošta
- často s cílem získat citlivé údaje

SPAM


IP Address Locator - What Is My IP Address Location? Find IP Address Search, IP Locator, IP Lookup - Google Chrome
www.ipaddresslocation.org
ipaddress location
home
ip address
checkpoint
ip ranges
ip2country
IP ADDRESS LOCATION
My IP: 93.115.84.195
AdChoices
► Track IP Address
► Find IP
► IP Lookup
► IP Locator
► IP Tracking
► IP Check
► IP List
Search IP Address - What is my IP address?
Have you ever wondered "what is my IP address" and how to search, trace and locate IP address from yourself or find IP address from anybody else?
Free & Safe - Austria VPN
Get Your Free 24 Hour Trial Now! Safe, High-Speed & 100% Anonymous.
Or thought about finding IP addresses ranges block that belong to a specific country?
Have you ever used a web-based IP address lookup location tool to trace and locate IP and find the geographical location of an IP address?
Maybe you are looking for an IP address location, DNS lookup, IP address range etc...
Or you simply wish to learn more about how networking protocols, like UDP and TCP/IP, work?
We can help with all of this and more.
Free IP Location Service
Our free IP to location service and impressive collection of IP tools:
email lookup (IP & Email tool to verify and lookup email addresses),
trace Email (track and trace email sender on basis of email header),
Other interesting projects:
IP-Address.org
Find-IP-Address.org
Web Proxy
Free Proxy
Support IP Address Locator project with donations and help the trace IP address lookup service we provide remain free:
Make A Donation
What is an IP Address
Computer IP Address (Internet Protocol address - Your Public IP address) is as your telephone number. It uniquely identifies every host on a network. Just as your mailing address uniquely identifies your home, an computer IP address uniquely identifies a host.
more info
rafinera
GÜNDE 5 ÖĞÜN
KAPIYA TESLİM
ÖZEL DİYET YEMEK SERVİSİ
29TL'
den başlayan
fiyatlarla

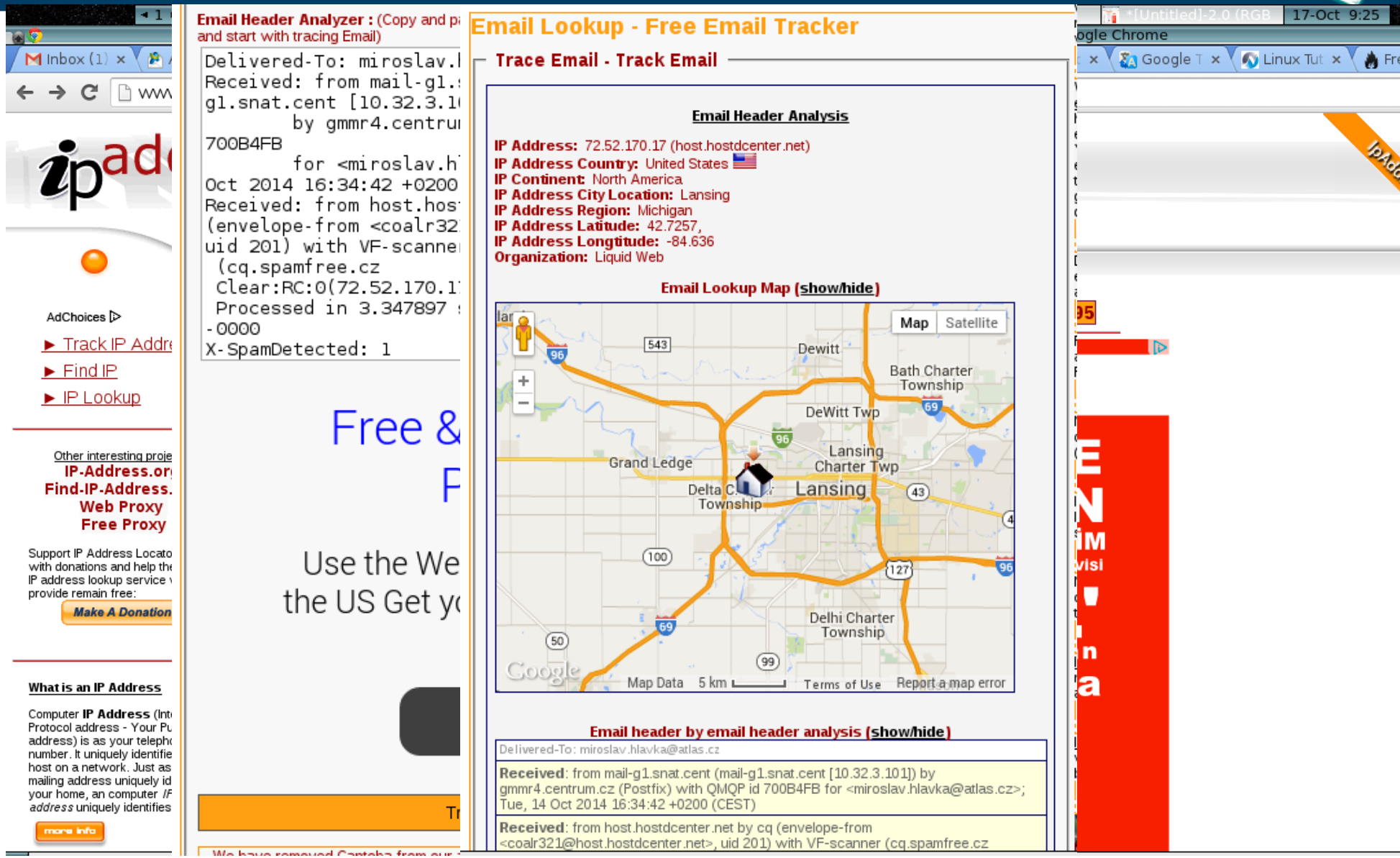
SPAM


Inbox (1)
AdChoices
Track IP Addre
Find IP
IP Lookup
Other interesting proje
IP-Address.or
Find-IP-Address.
Web Proxy
Free Proxy
Support IP Address Locato
with donations and help the
IP address lookup service
provide remain free:
Make A Donation
What is an IP Address
Computer IP Address (Int
Protocol address - Your Pu
address) is as your telephc
number. It uniquely identifie
host on a network. Just as
mailing address uniquely id
your home, an computer IF
address uniquely identifies
more info

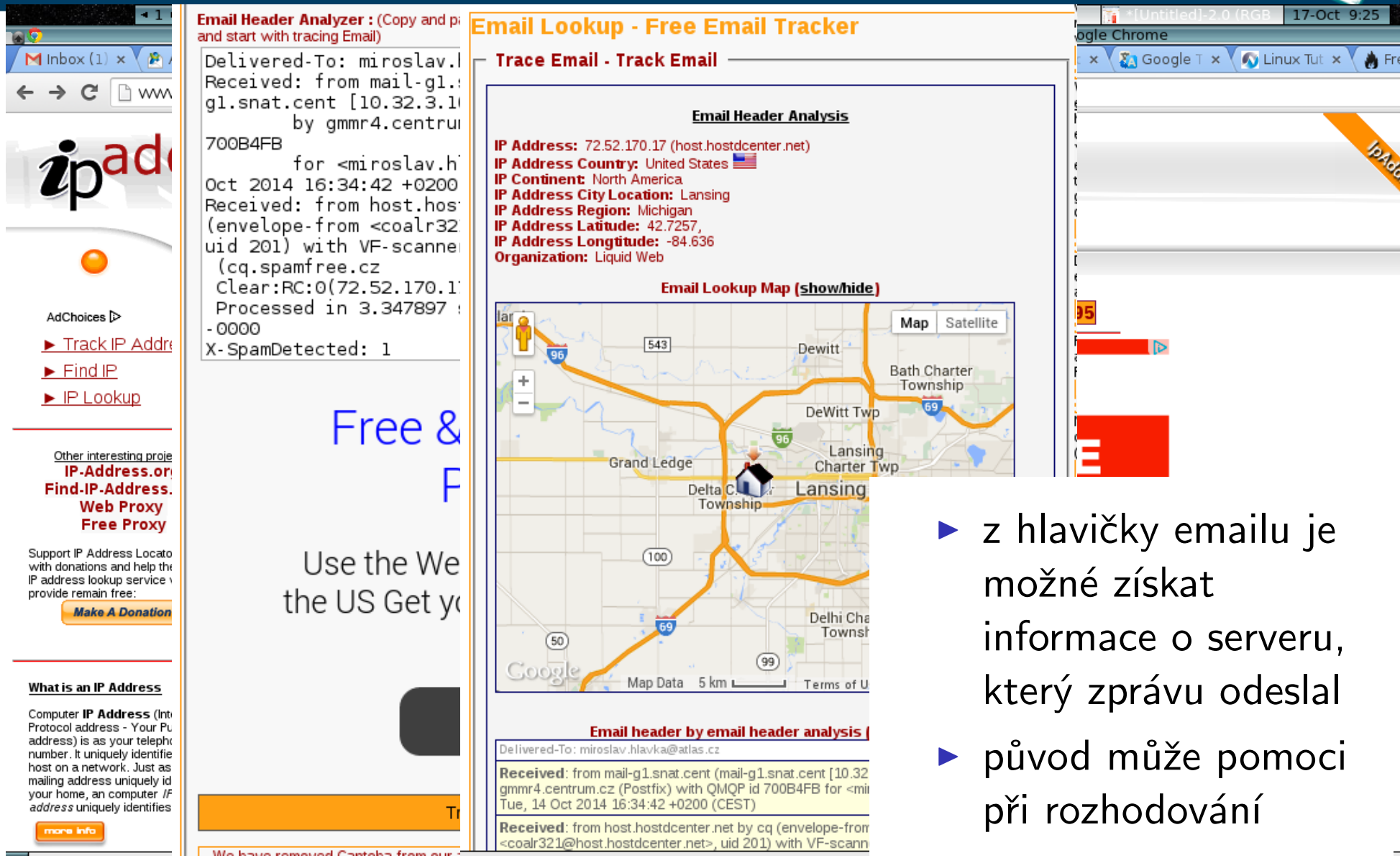

Email Header Analyzer : (Copy and paste Email header into our free Email tracking tool and start with tracing Email)
Delivered-To: miroslav.hlavka@atlas.cz
Received: from mail-g1.snat.cent (mail-g1.snat.cent [10.32.3.101])
by gmmr4.centrum.cz (Postfix) with QMQP id 700B4FB
for <miroslav.hlavka@atlas.cz>; Tue, 14 Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostdcenter.net by cq (envelope-from <coalr321@host.hostdcenter.net>, uid 201) with VF-scanner
(cq.spamfree.cz
Clear:RC:0(72.52.170.17):SA:1(5.7/5.0):.
Processed in 3.347897 secs); 14 Oct 2014 14:34:42 -0000
X-SpamDetected: 1
Free & Safe - US Proxy
Use the Web like you were in the US Get your Free Trial Now!
Track Email


17-Oct 9:25
Search, IP Locator, IP Lookup - Google Chrome
My IP: 93.115.84.195
rafinera
GÜNDE
5 ÖĞÜN
KAPIYA TESLİM
ÖZEL DİYET YEMEK SERVİSİ
29TL'
den başlayan
fiyatlarla

SPAM


Email Header Analyzer : (Copy and p
and start with tracing Email)
Delivered-To: miroslav.
Received: from mail-g1.
g1.snat.cent [10.32.3.1
by gmmr4.centru
700B4FB
for <miroslav.h
Oct 2014 16:34:42 +0200
Received: from host.hos
(envelope-from <coalr32
uid 201) with VF-scanne
(cq.spamfree.cz
Clear:RC:0(72.52.170.1
Processed in 3.347897
-0000
X-SpamDetected: 1
Email Lookup - Free Email Tracker
Trace Email - Track Email
Email Header Analysis
IP Address: 72.52.170.17 (host.hostdcenter.net)
IP Address Country: United States
IP Continent: North America
IP Address City Location: Lansing
IP Address Region: Michigan
IP Address Latitude: 42.7257,
IP Address Longtitude: -84.636
Organization: Liquid Web
Email Lookup Map (show/hide)
Map
Satellite
Dewitt
Bath Charter Township
DeWitt Twp
Grand Ledge
Lansing Charter Twp
Lansing
Delta C
Township
Delhi Charter Township
Google
Map Data
5 km
Terms of Use
Report a map error
Email header by email header analysis (show/hide)
Delivered-To: miroslav.hlavka@atlas.cz
Received: from mail-g1.snat.cent (mail-g1.snat.cent [10.32.3.101]) by gmmr4.centrum.cz (Postfix) with QMQP id 700B4FB for <miroslav.hlavka@atlas.cz>; Tue, 14 Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostdcenter.net by cq (envelope-from <coalr321@host.hostdcenter.net>, uid 201) with VF-scanner (cq.spamfree.cz
AdChoices
Track IP Addr
Find IP
IP Lookup
Other interesting proje
IP-Address.or
Find-IP-Address.
Web Proxy
Free Proxy
Support IP Address Locato
with donations and help th
IP address lookup service
provide remain free:
Make A Donation
What is an IP Address
Computer IP Address (Int
Protocol address - Your Pu
address) is as your telephc
number. It uniquely identifie
host on a network. Just as
mailing address uniquely id
your home, an computer IF
address uniquely identifies
more info
Free &
Use the We
the US Get y
Google T
Linux Tut
17-Oct 9:25

SPAM



- z hlavičky emailu je možné získat informace o serveru, který zprávu odeslal
- původ může pomoci při rozhodování

Co dělat se SPAMem?

- email, který přichází od neznámého odesilatele neotevírat
- spustitelné soubory nespouštět
- jestliže přílohu nepotřebuji, smazat
- pravidelně aktualizovat systém a aplikace

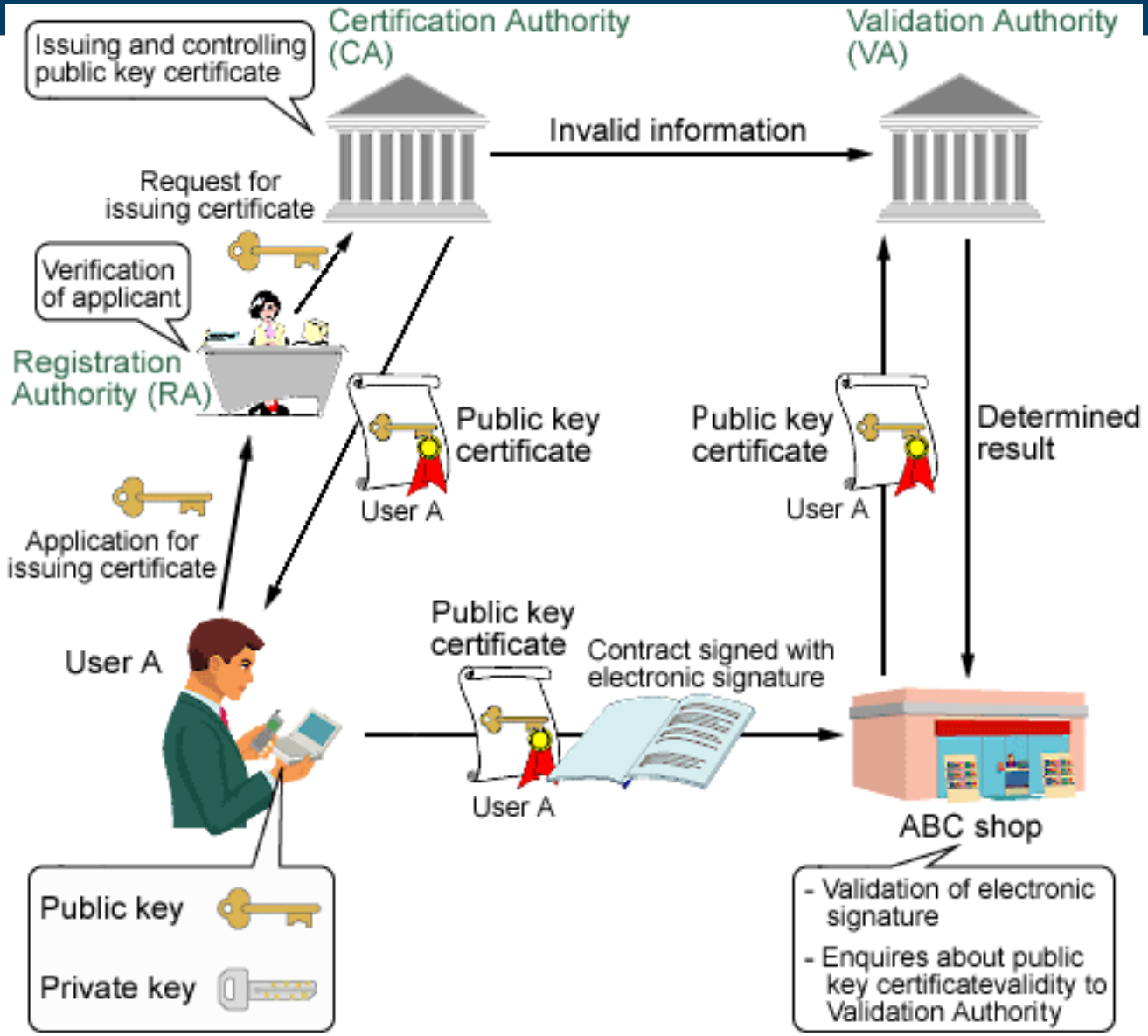
Phishing

- útok distribuovaný nejčastěji emailem či IM (př. Facebook, Skype)
- cílem je získání senzitivních dat
- uživatel je přesměrován na neoficiální web
- v případě HTTPS uživatel vždy musí potvrdit přijetí SSL certifikátu

Public Key Infrastracture

- pár klíč - certifikát
- CA ověří uživatelský certifikát
- certifikát podepsaný CA je důvěryhodný
- používá se pro ověření (digitální podpis), šifrování
- PGP podpis a šifrování mailů

PKI


Issuing and controlling public key certificate
Certification Authority (CA)
Validation Authority (VA)
Invalid information
Request for issuing certificate
Verification of applicant
Registration Authority (RA)
Public key certificate
User A
Public key certificate
User A
Determined result
Application for issuing certificate
User A
Public key certificate
Contract signed with electronic signature
User A
ABC shop
Public key
Private key
- Validation of electronic signature
- Enquires about public key certificatevalidity to Validation Authority

Obrázek: [?]

Phishing

O2

Dobrý den,
děkujeme, že využíváte služeb O2.

Máte nové vyúčtování

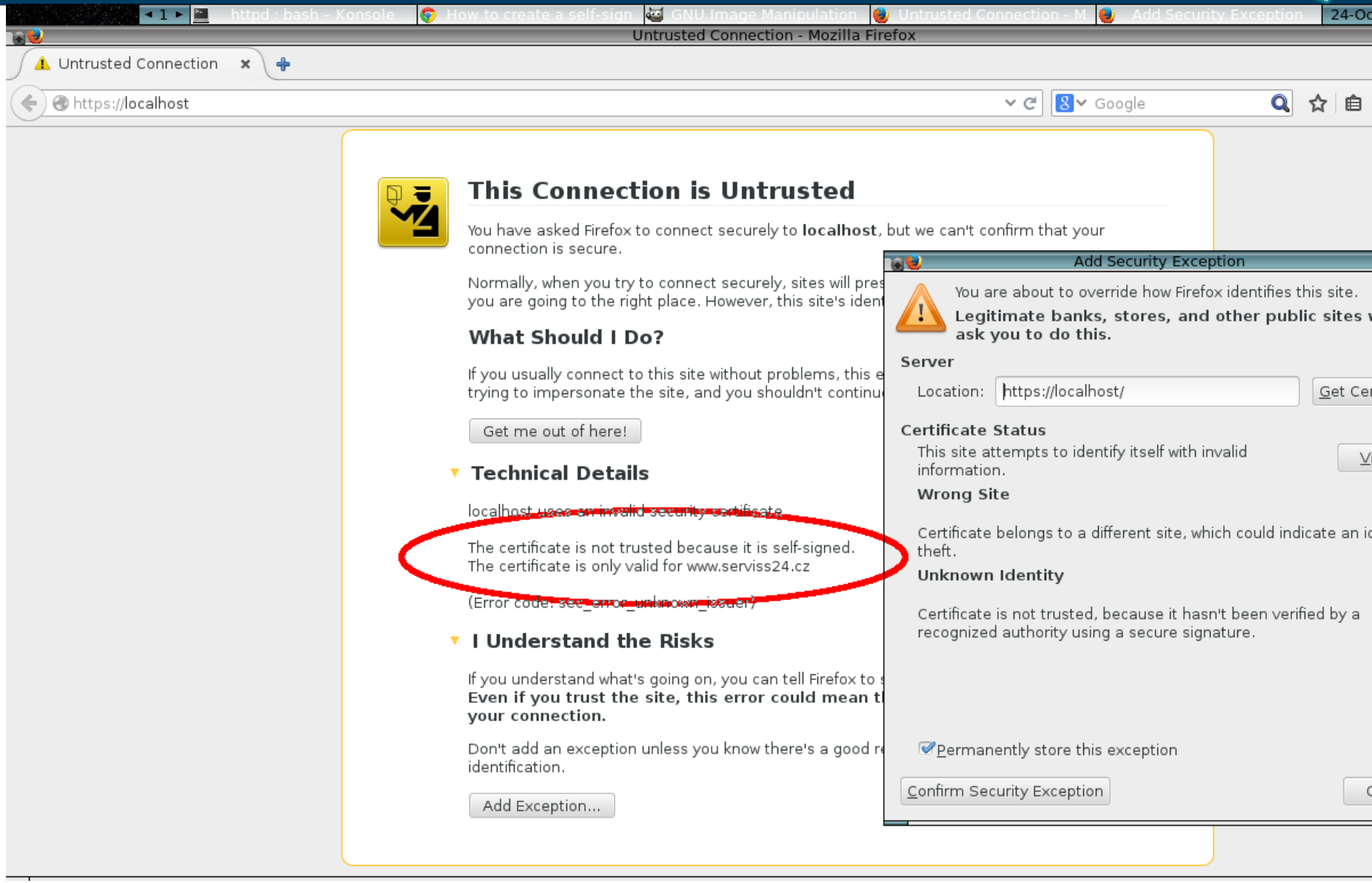
Vyúčtování za:	**mobilní služby**
Zúčtovací období:	**od 14.09.2014 do 13.10.2014**
Účet k úhradě:	**500115980/2300**

Částka (s DPH):	Variabilní symbol:	Uhraďte do:
266,01 Kč	**1277097841**	**29.10.2014**

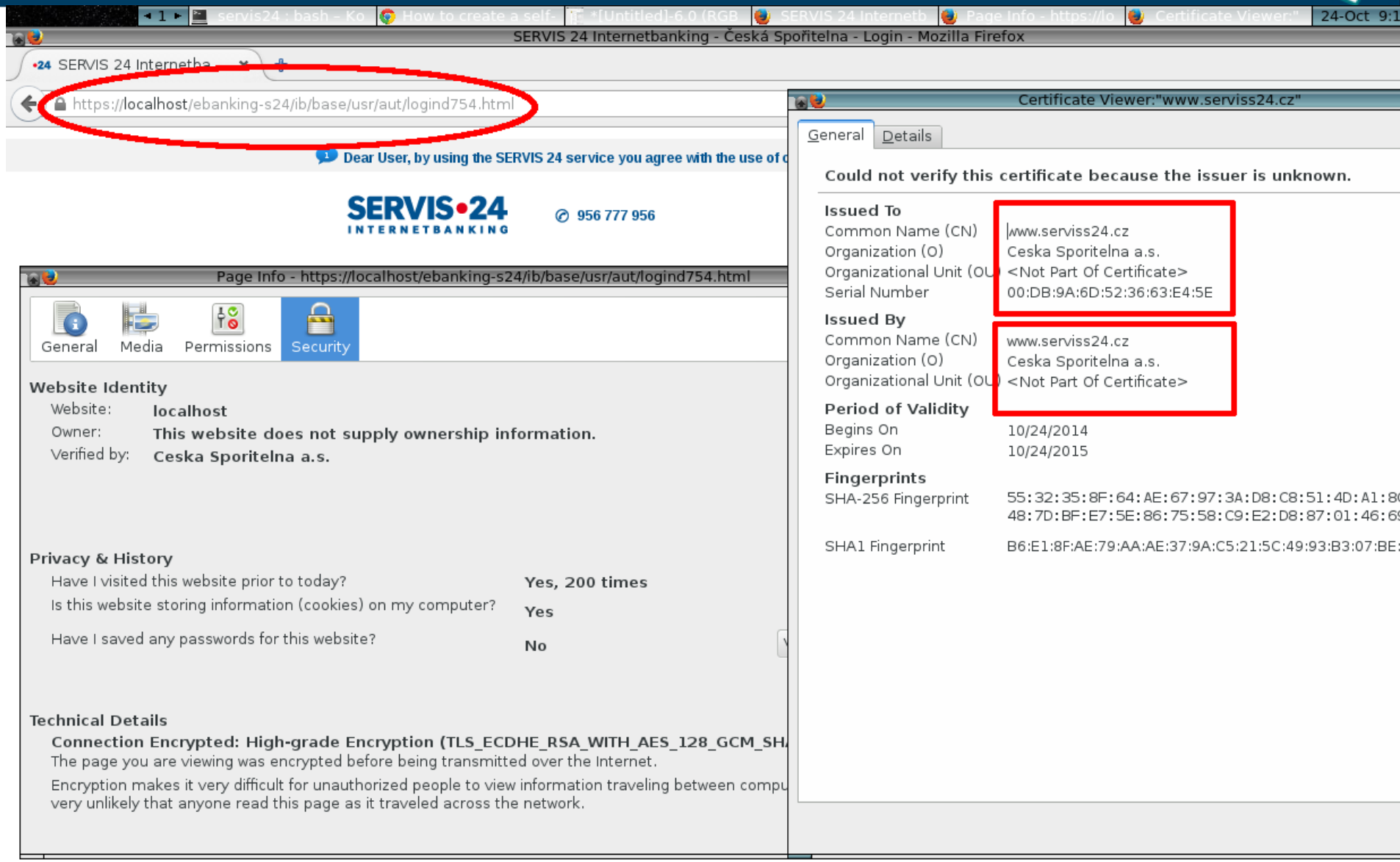
Vyúčtování služeb je připojeno jako příloha k tomuto e-mailu ve formátu PDF.

Klikněte sem pro zobrazení plné verze

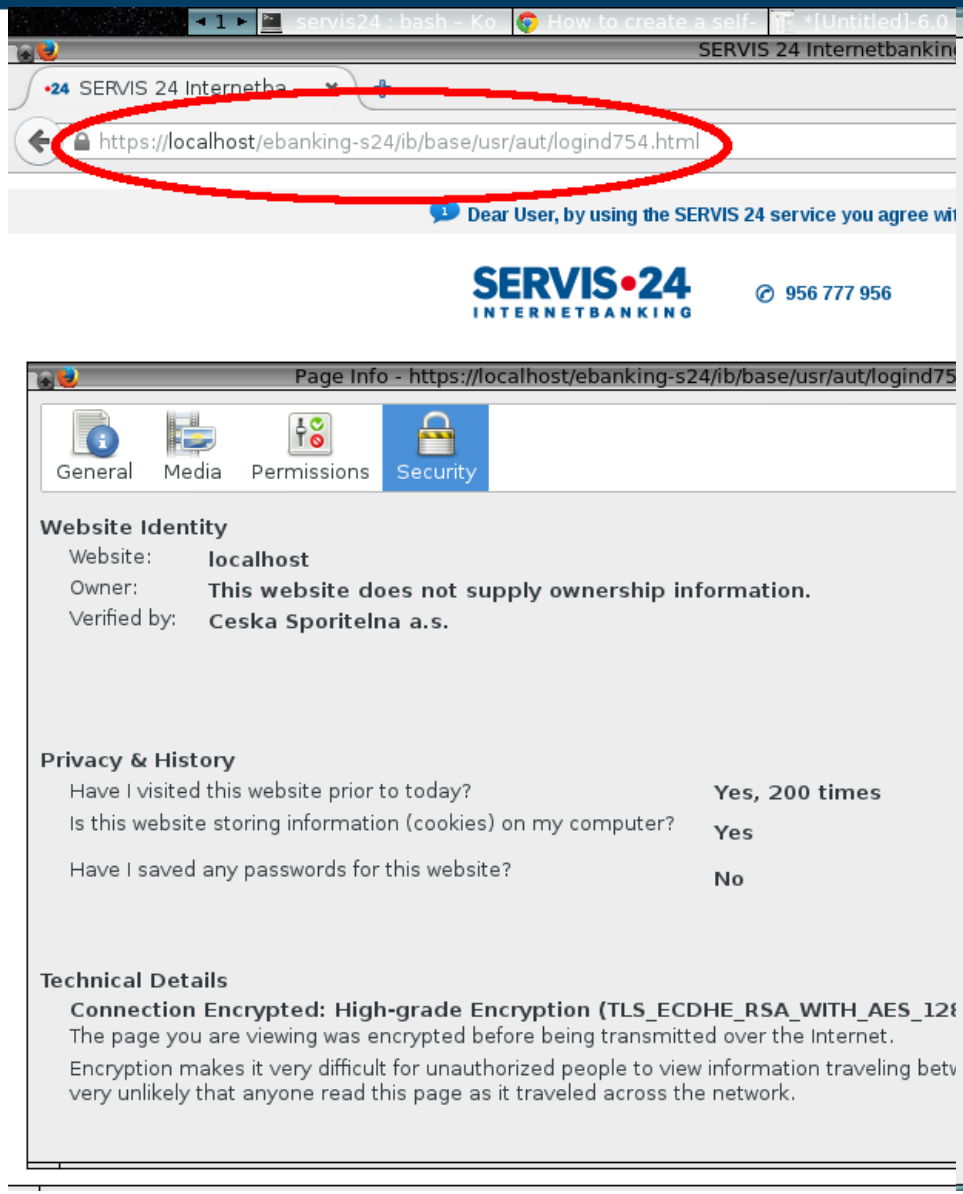
Phishing

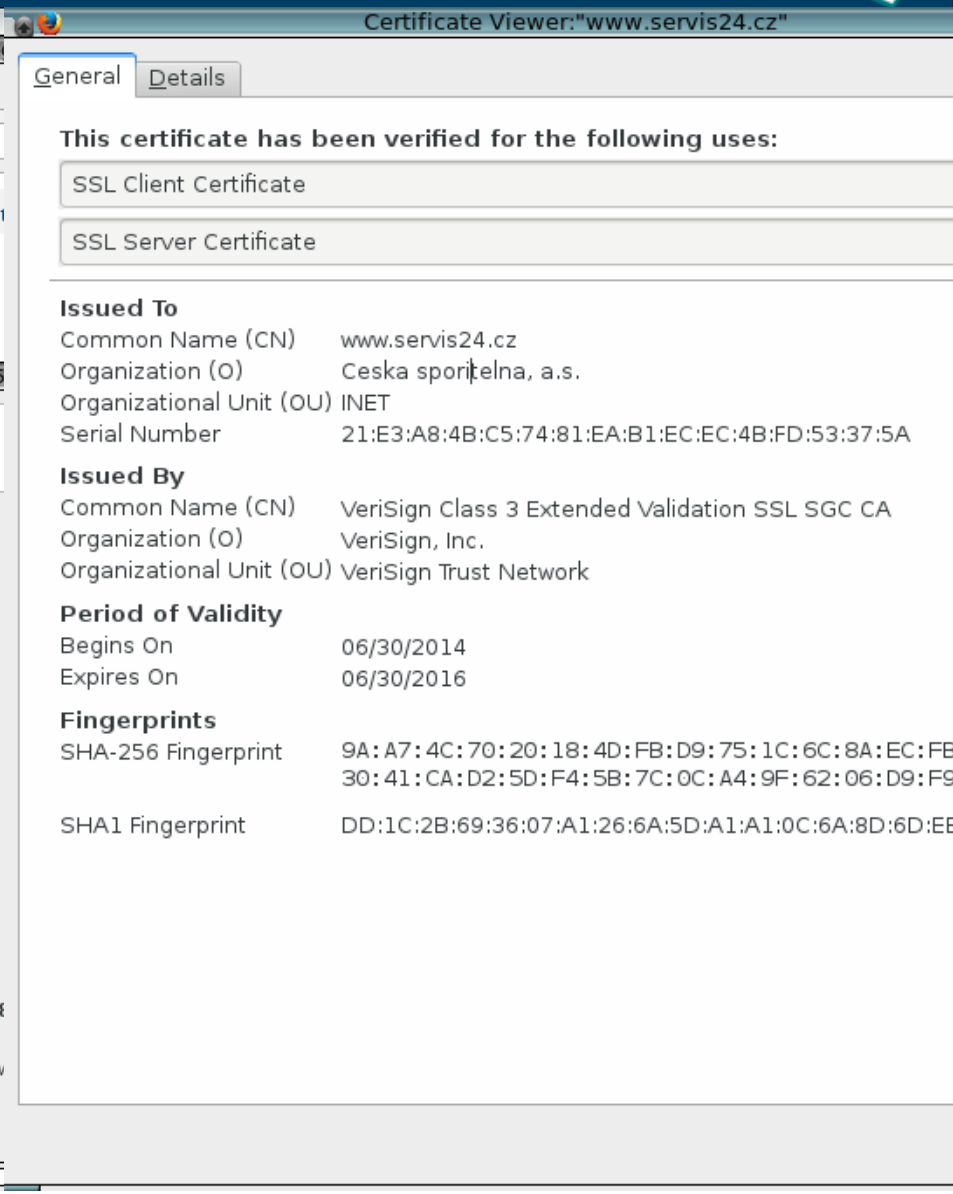

Untrusted Connection - Mozilla Firefox
Untrusted Connection
https://localhost
Google
This Connection is Untrusted
You have asked Firefox to connect securely to localhost, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will pres
you are going to the right place. However, this site's ident
What Should I Do?
If you usually connect to this site without problems, this e
trying to impersonate the site, and you shouldn't continu
Get me out of here!
Technical Details
localhost uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
The certificate is only valid for www.serviss24.cz
(Error code: sec_error_unknown_issuer)
I Understand the Risks
If you understand what's going on, you can tell Firefox to
Even if you trust the site, this error could mean t
your connection.
Don't add an exception unless you know there's a good r
identification.
Add Exception...
Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites
ask you to do this.
Server
Location: https://localhost/
Get Ce
Certificate Status
This site attempts to identify itself with invalid information.
Wrong Site
Certificate belongs to a different site, which could indicate an i
theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.
Permanently store this exception
Confirm Security Exception

Phishing


SERVIS 24 Internetbanking - Česká Spořitelna - Login - Mozilla Firefox
https://localhost/ebanking-s24/ib/base/usr/aut/logind754.html
Dear User, by using the SERVIS 24 service you agree with the use of
SERVIS•24 INTERNETBANKING
956 777 956
Page Info - https://localhost/ebanking-s24/ib/base/usr/aut/logind754.html
General
Media
Permissions
Security
Website Identity
Website: localhost
Owner: This website does not supply ownership information.
Verified by: Ceska Sporitelna a.s.
Privacy & History
Have I visited this website prior to today? Yes, 200 times
Is this website storing information (cookies) on my computer? Yes
Have I saved any passwords for this website? No
Technical Details
Connection Encrypted: High-grade Encryption (TLS_ECDHE_RSA_WITH_AES_128_GCM_SH
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between compu
very unlikely that anyone read this page as it traveled across the network.
Certificate Viewer:"www.serviss24.cz"
General
Details
Could not verify this certificate because the issuer is unknown.
Issued To
Common Name (CN) www.serviss24.cz
Organization (O) Ceska Sporitelna a.s.
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 00:DB:9A:6D:52:36:63:E4:5E
Issued By
Common Name (CN) www.serviss24.cz
Organization (O) Ceska Sporitelna a.s.
Organizational Unit (OU) <Not Part Of Certificate>
Period of Validity
Begins On 10/24/2014
Expires On 10/24/2015
Fingerprints
SHA-256 Fingerprint 55:32:35:8F:64:AE:67:97:3A:D8:C8:51:4D:A1:8
48:7D:BF:E7:5E:86:75:58:C9:E2:D8:87:01:46:6
SHA1 Fingerprint B6:E1:8F:AE:79:AA:AE:37:9A:C5:21:5C:49:93:B3:07:BE

Phishing

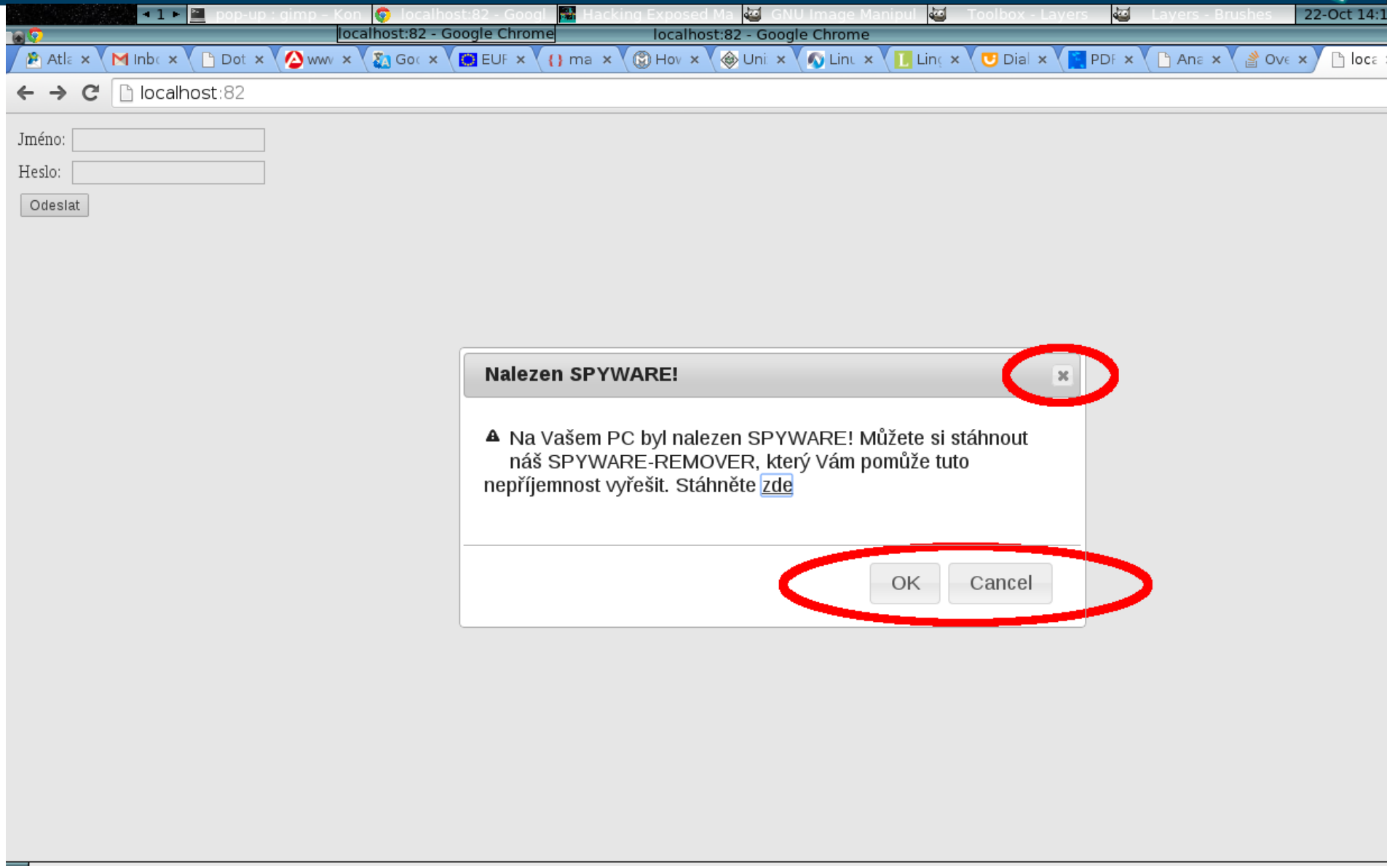

SERVIS 24 Internetbankin
SERVIS 24 Internetba
https://localhost/ebanking-s24/ib/base/usr/aut/logind754.html
Dear User, by using the SERVIS 24 service you agree wit
SERVIS•24
INTERNETBANKING
956 777 956
Page Info - https://localhost/ebanking-s24/ib/base/usr/aut/logind75
General
Media
Permissions
Security
Website Identity
Website: localhost
Owner: This website does not supply ownership information.
Verified by: Ceska Sporitelna a.s.
Privacy & History
Have I visited this website prior to today? Yes, 200 times
Is this website storing information (cookies) on my computer? Yes
Have I saved any passwords for this website? No
Technical Details
Connection Encrypted: High-grade Encryption (TLS_ECDHE_RSA_WITH_AES_128
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling betv
very unlikely that anyone read this page as it traveled across the network.


Certificate Viewer:"www.servis24.cz"
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Issued To
Common Name (CN) www.servis24.cz
Organization (O) Ceska sporitelna, a.s.
Organizational Unit (OU) INET
Serial Number 21:E3:A8:4B:C5:74:81:EA:B1:EC:EC:4B:FD:53:37:5A
Issued By
Common Name (CN) VeriSign Class 3 Extended Validation SSL SGC CA
Organization (O) VeriSign, Inc.
Organizational Unit (OU) VeriSign Trust Network
Period of Validity
Begins On 06/30/2014
Expires On 06/30/2016
Fingerprints
SHA-256 Fingerprint 9A:A7:4C:70:20:18:4D:FB:D9:75:1C:6C:8A:EC:FB
30:41:CA:D2:5D:F4:5B:7C:0C:A4:9F:62:06:D9:F9
SHA1 Fingerprint DD:1C:2B:69:36:07:A1:26:6A:5D:A1:A1:0C:6A:8D:6D:EE

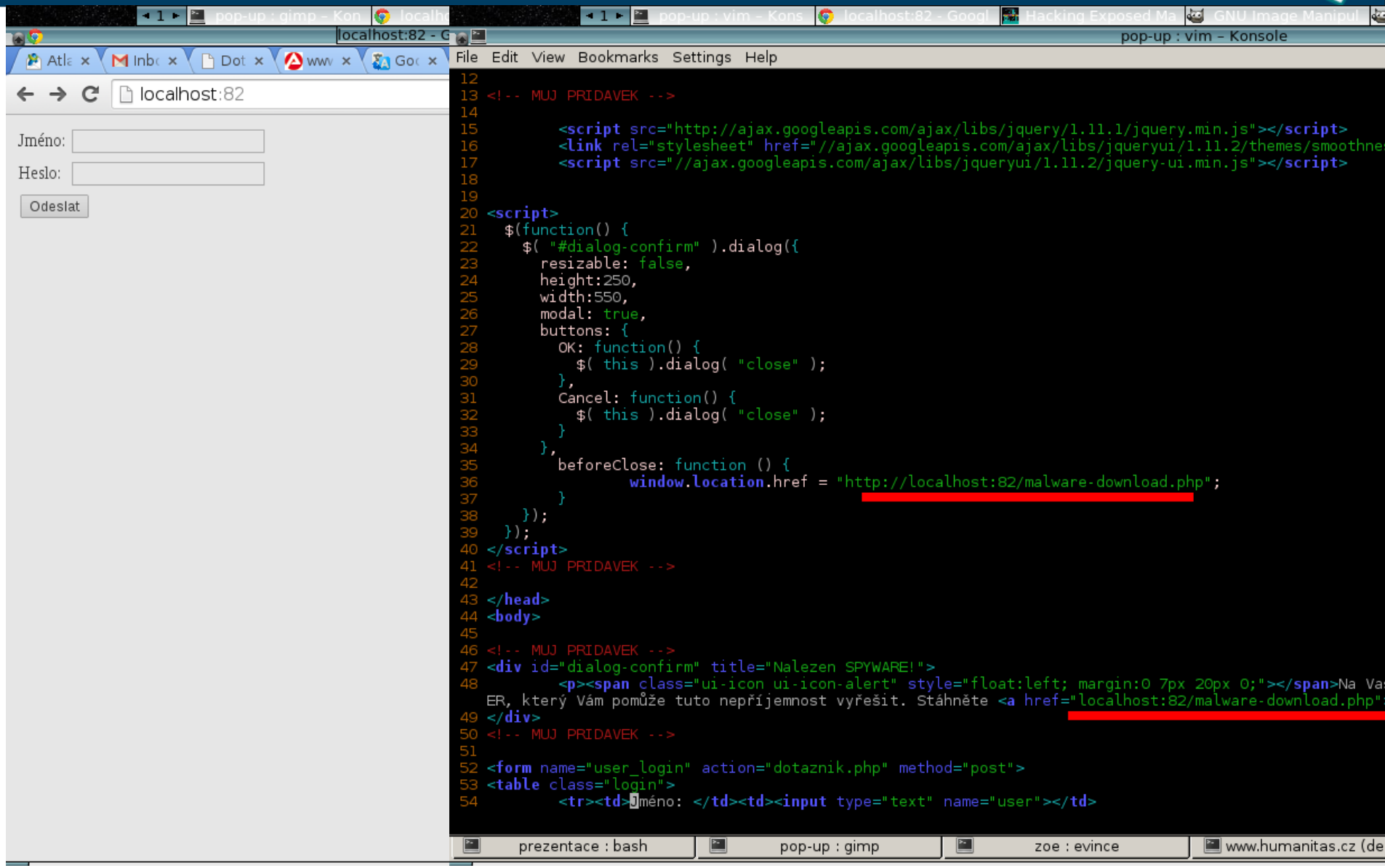
Doporučení

- neotvírat maily od cizích příjemců, maily s gramatickými chybami, generické oslovení, vyžadují podezřelé chování
- v podezřelých mailech neotvírat přílohy ani webové odkazy
- mail neuchovávat, mazat
- informovat IT správce, podobný email mohou dostat i kolegové
- mějte instalovaný AV a anti-phishing modul

Pop-Up okna s malware obsahem



Pop-Up okna s malware obsahem



Pop-Up okna s malware obsahem

- při zobrazení pozdezřelého pop-up na nic neklikat
- nejlépe zavřít tab či celý prohlížeč
- mít nainstalovaný AV a Anti-Spyware
- v korporátním prostředí web-based content filtering (K9, Squid, OpenDNS)

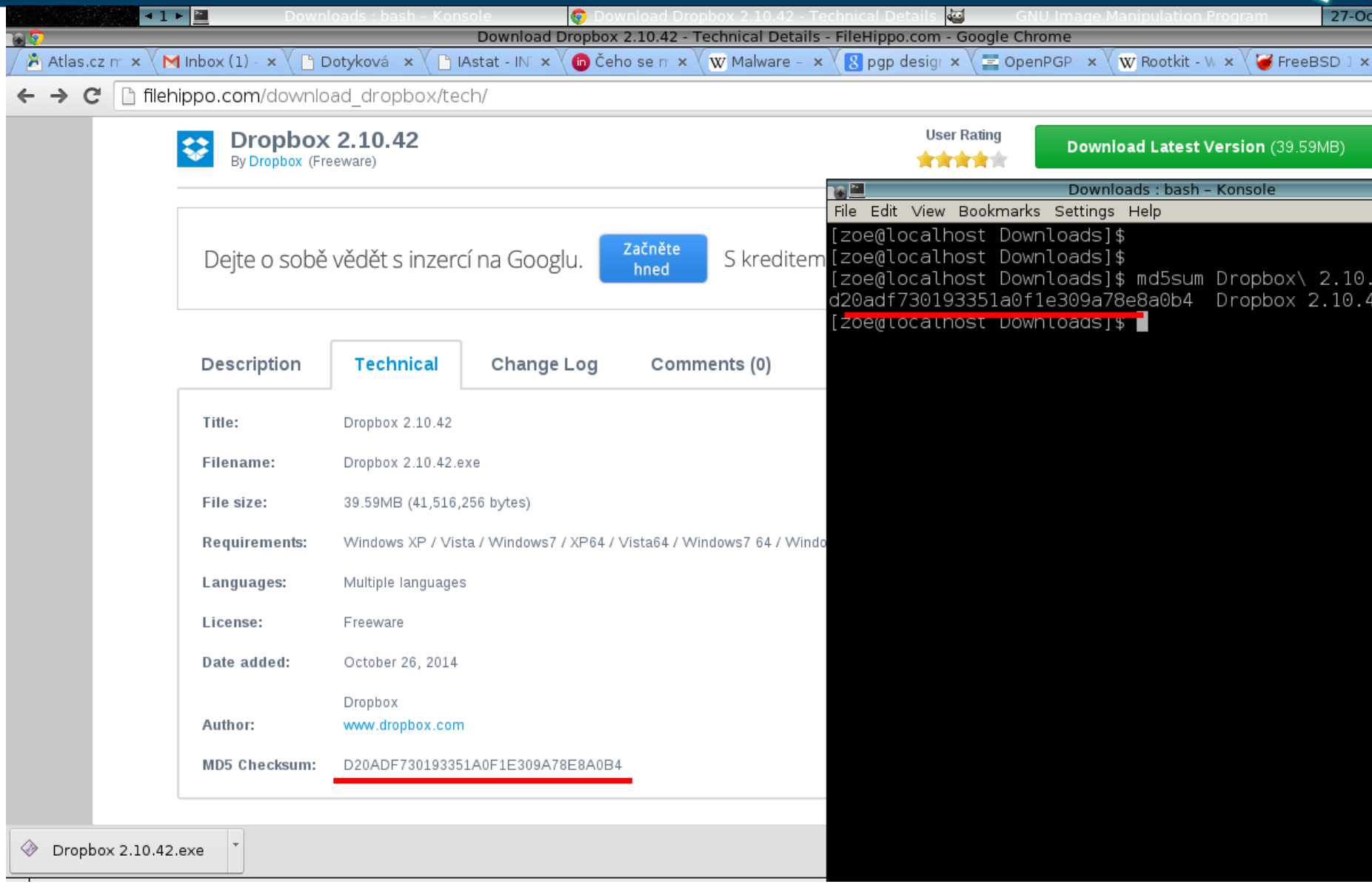
Rootkit

- software pro neoprávněný vzdálený přístup (často s právy administrátora)
- samotný rootkit otevírá cestu dalším infekcím (keylogger, botnet, SPAM distribuce)
- maskuje backdoor, tak aby nebyl snadno objevitelný
- může být distribuován bez účasti uživatele
- využívá exploitů na úrovni aplikace či OS (typicky buffer overflow)

Obrana

- vždy aktualizovat OS
- instalovaný AV, HIPS (SNORT, Malware Defender, WinPatrol)
- v případě instalace nového software kontrolovat kryptografický hash

MD5 hash


Download Dropbox 2.10.42 - Technical Details - FileHippo.com - Google Chrome
filehippo.com/download_dropbox/tech/
Dropbox 2.10.42
By Dropbox (Freeware)
User Rating
Download Latest Version (39.59MB)
Dejte o sobě vědět s inzercí na Googlu.
Začněte hned
Description
Technical
Change Log
Comments (0)
Title: Dropbox 2.10.42
Filename: Dropbox 2.10.42.exe
File size: 39.59MB (41,516,256 bytes)
Requirements: Windows XP / Vista / Windows7 / XP64 / Vista64 / Windows7 64 / Windo
Languages: Multiple languages
License: Freeware
Date added: October 26, 2014
Author: Dropbox www.dropbox.com
MD5 Checksum: D20ADF730193351A0F1E309A78E8A0B4
Dropbox 2.10.42.exe
Downloads : bash – Konsole
File Edit View Bookmarks Settings Help
[zoe@localhost Downloads]$
[zoe@localhost Downloads]$
[zoe@localhost Downloads]$ md5sum Dropbox\ 2.10.
d20adf730193351a0f1e309a78e8a0b4 Dropbox 2.10.4
[zoe@localhost Downloads]$

Botnet

- "služba" šířená malwarem (drive-by download, email)
- po nakažení se PC stává botem (zombie PC)
- někde existuje Command and Control Server
- zombie PC jsou aktivovány C&C až na specifickou akci
- používá se pro DDoS, SPAM, ... (těžba BitCoin)
- Conficer, Zeus, Waledac

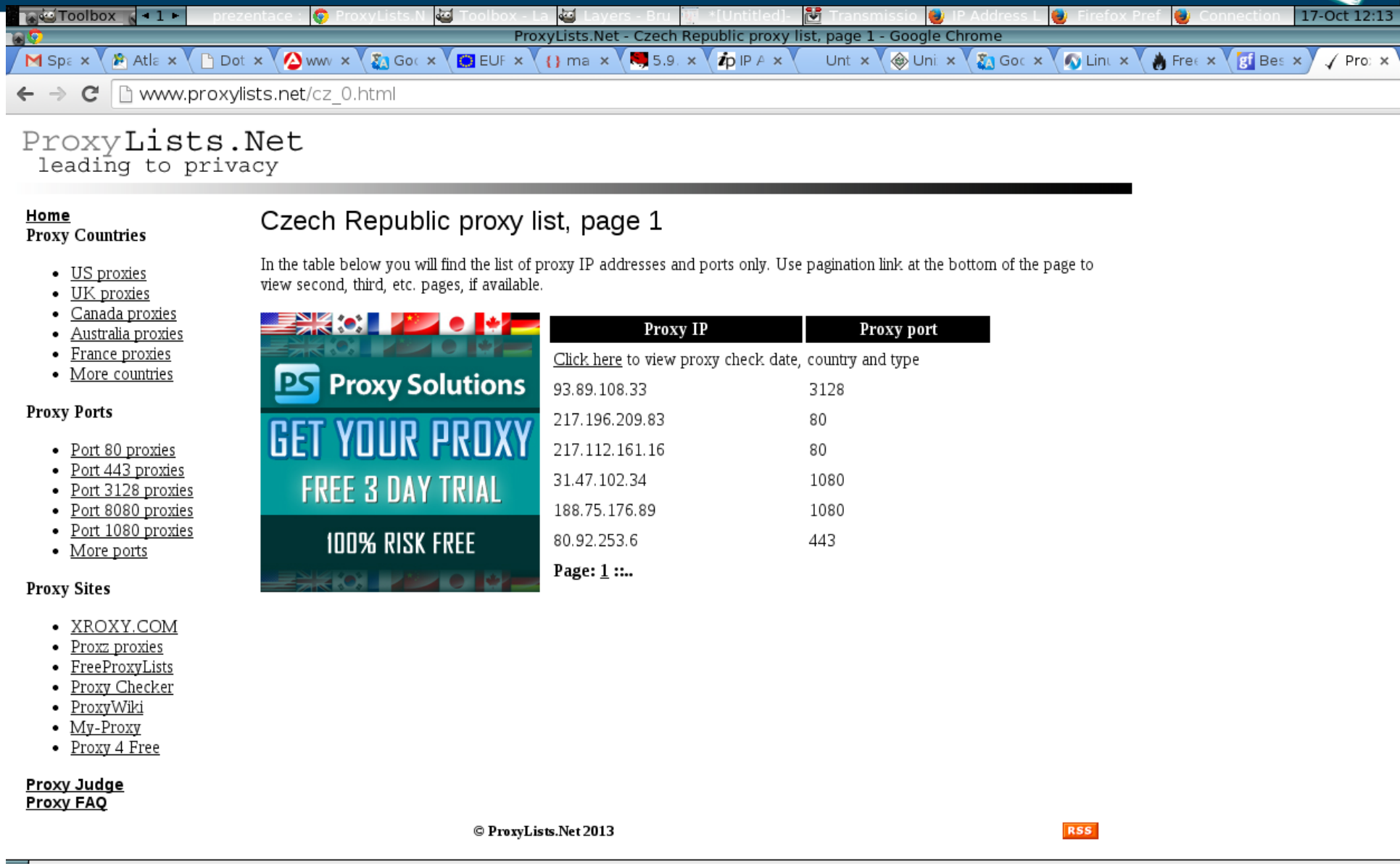
Botnet

Obrázek: [?]

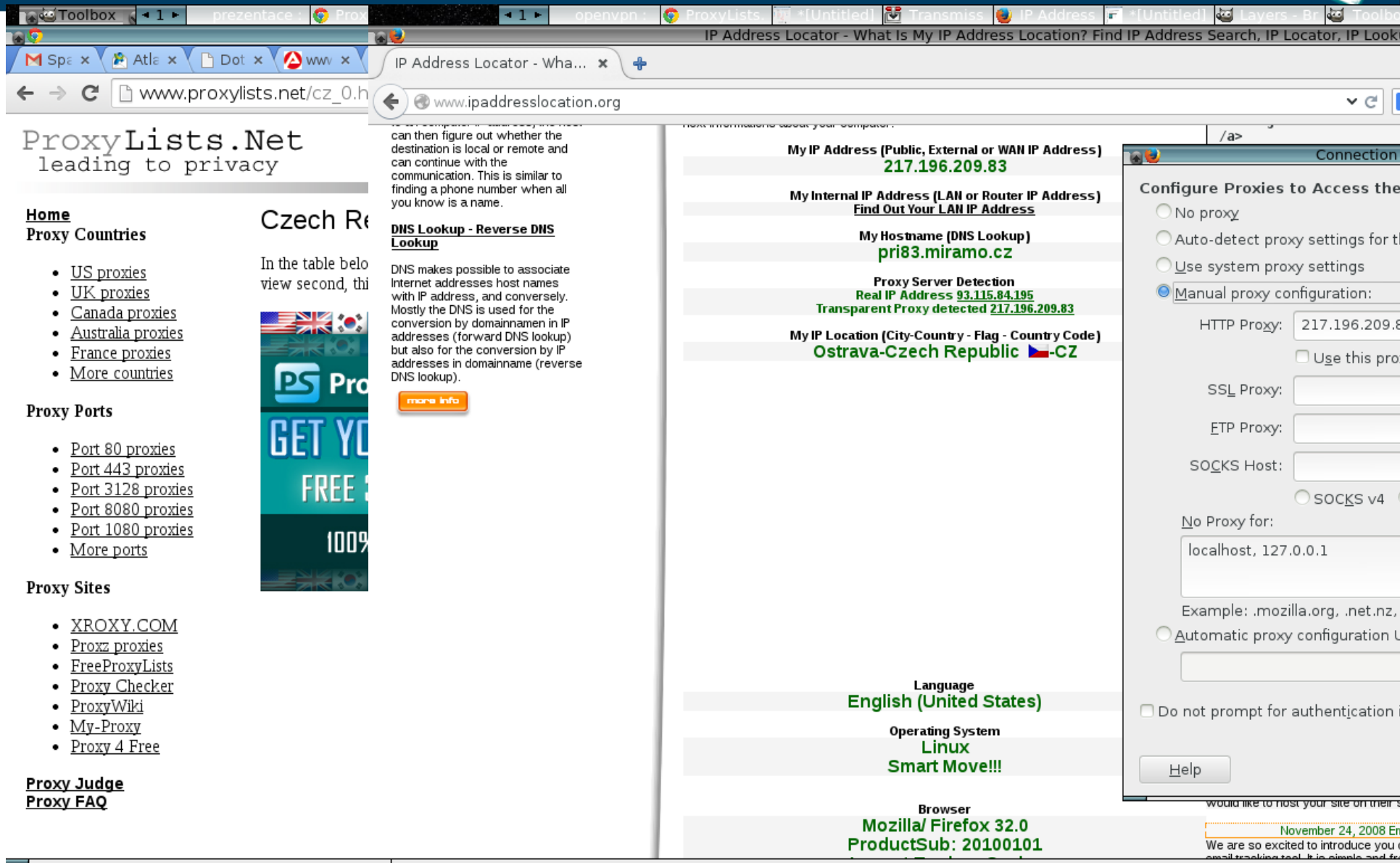
Anonymizace

- umožňuje skrýt IP adresu a další data
- webové služby často sdílí data o návštěvnosti s jinými providery
- "Big Brother" chování - Google, Facebook ...
- máte-li pocit, že váš traffic může být odposloucháván

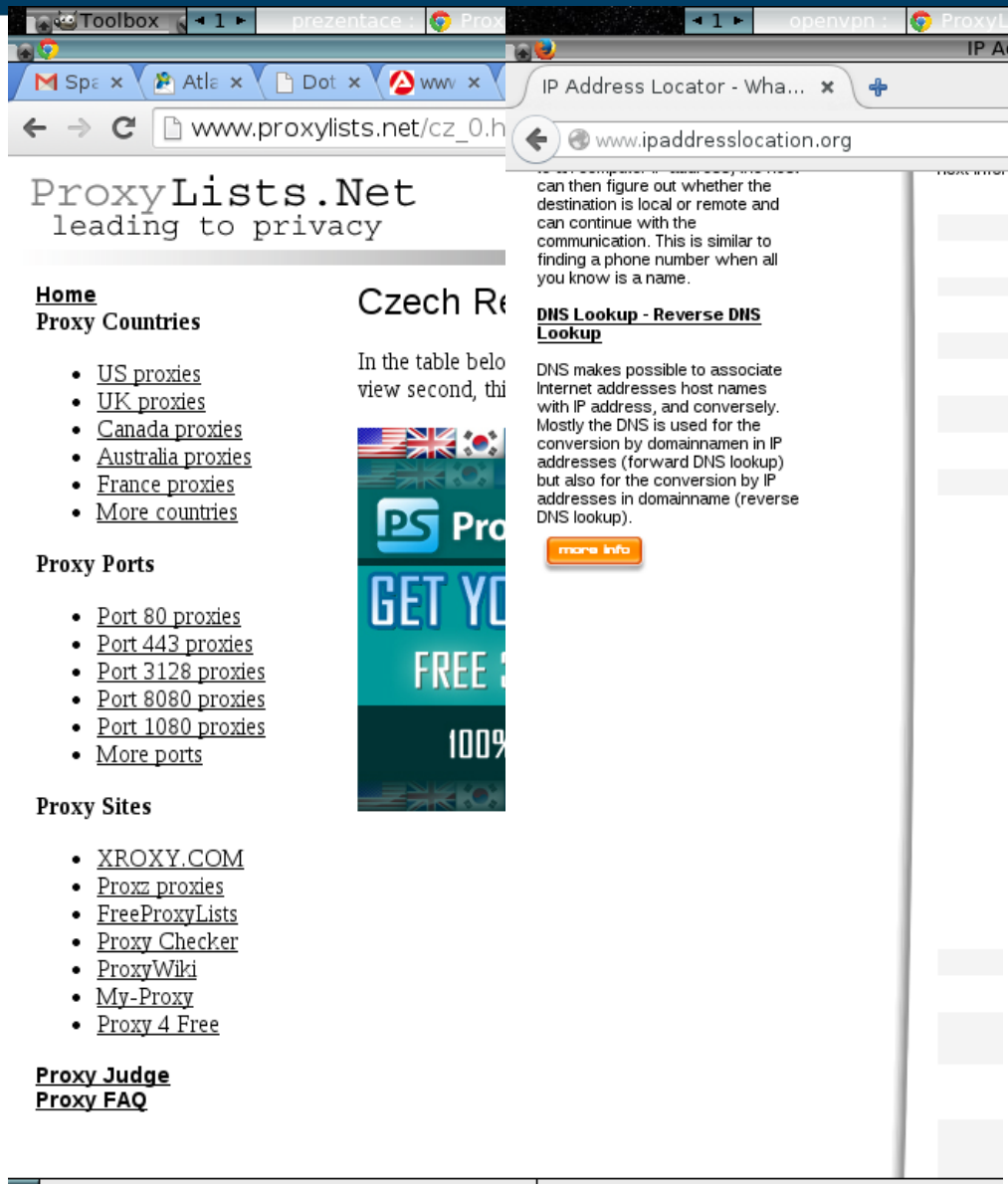
Web Proxy


ProxyLists.Net - Czech Republic proxy list, page 1 - Google Chrome
www.proxylists.net/cz_0.html
ProxyLists.Net
leading to privacy
Home
Proxy Countries
US proxies
UK proxies
Canada proxies
Australia proxies
France proxies
More countries
Proxy Ports
Port 80 proxies
Port 443 proxies
Port 3128 proxies
Port 8080 proxies
Port 1080 proxies
More ports
Proxy Sites
XROXY.COM
Proxz proxies
FreeProxyLists
Proxy Checker
ProxyWiki
My-Proxy
Proxy 4 Free
Proxy Judge
Proxy FAQ
Czech Republic proxy list, page 1
In the table below you will find the list of proxy IP addresses and ports only. Use pagination link at the bottom of the page to view second, third, etc. pages, if available.
Proxy Solutions
GET YOUR PROXY
FREE 3 DAY TRIAL
100% RISK FREE
Proxy IP
Proxy port
Click here to view proxy check date, country and type
93.89.108.33 3128
217.196.209.83 80
217.112.161.16 80
31.47.102.34 1080
188.75.176.89 1080
80.92.253.6 443
Page: 1 ::..
© ProxyLists.Net 2013
RSS

Web Proxy

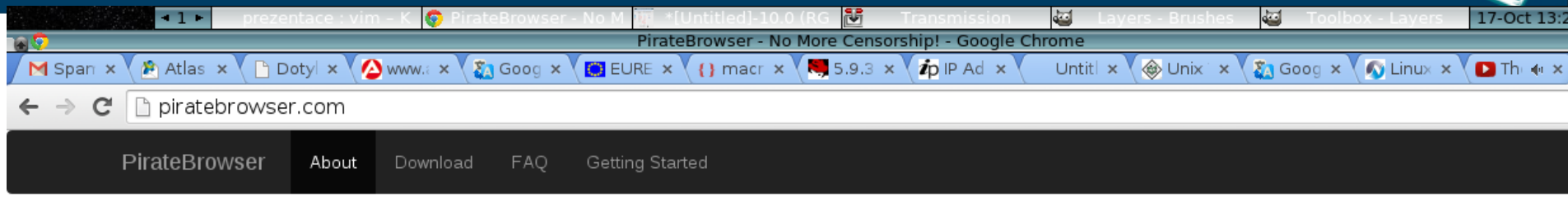

www.proxylists.net/cz_0.h
ProxyLists.Net
leading to privacy
Home
Proxy Countries
US proxies
UK proxies
Canada proxies
Australia proxies
France proxies
More countries
Proxy Ports
Port 80 proxies
Port 443 proxies
Port 3128 proxies
Port 8080 proxies
Port 1080 proxies
More ports
Proxy Sites
XROXY.COM
Proxz proxies
FreeProxyLists
Proxy Checker
ProxyWiki
My-Proxy
Proxy 4 Free
Proxy Judge
Proxy FAQ
Czech Re
In the table belo
view second, thi
IP Address Locator - What Is My IP Address Location? Find IP Address Search, IP Locator, IP Look
IP Address Locator - Wha...
www.ipaddresslocation.org
can then figure out whether the destination is local or remote and can continue with the communication. This is similar to finding a phone number when all you know is a name.
DNS Lookup - Reverse DNS Lookup
DNS makes possible to associate Internet addresses host names with IP address, and conversely. Mostly the DNS is used for the conversion by domainnamen in IP addresses (forward DNS lookup) but also for the conversion by IP addresses in domainname (reverse DNS lookup).
more info
My IP Address (Public, External or WAN IP Address)
217.196.209.83
My Internal IP Address (LAN or Router IP Address)
Find Out Your LAN IP Address
My Hostname (DNS Lookup)
pri83.miramo.cz
Proxy Server Detection
Real IP Address 93.115.84.195
Transparent Proxy detected 217.196.209.83
My IP Location (City-Country - Flag - Country Code)
Ostrava-Czech Republic -CZ
Language
English (United States)
Operating System
Linux
Smart Move!!!
Browser
Mozilla/ Firefox 32.0
ProductSub: 20100101
Connection
Configure Proxies to Access the
No proxy
Auto-detect proxy settings for t
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
Use this pro
SSL Proxy:
FTP Proxy:
SOCKS Host:
SOCKS v4
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz,
Automatic proxy configuration
Do not prompt for authentication
Help
November 24, 2008

Web Proxy



- *http://www.proxylists.net/*
- jednoduchá konfigurace prohlížeče
- pouze pro HTTP traffic

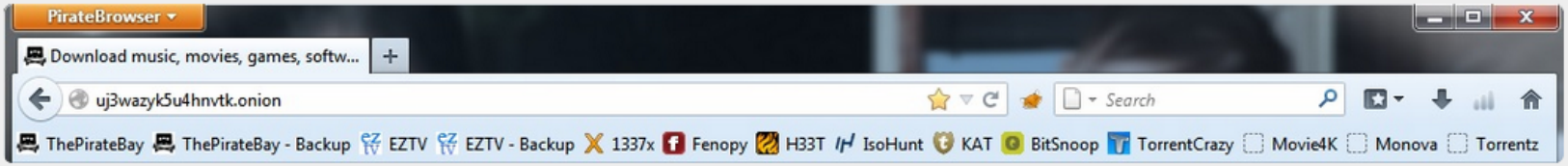
PirateBrowser



PirateBrowser - No more censorship!

PirateBrowser is a bundle package of the Tor client (Vidalia), FireFox Portable browser (with foxyproxy addon) and some custom configs that allows you to circumvent censorship that certain countries such as Iran, North Korea, United Kingdom, ~~The Netherlands~~, Belgium, Finland, Denmark, Italy and Ireland impose onto their citizens.

This is how it looks like:

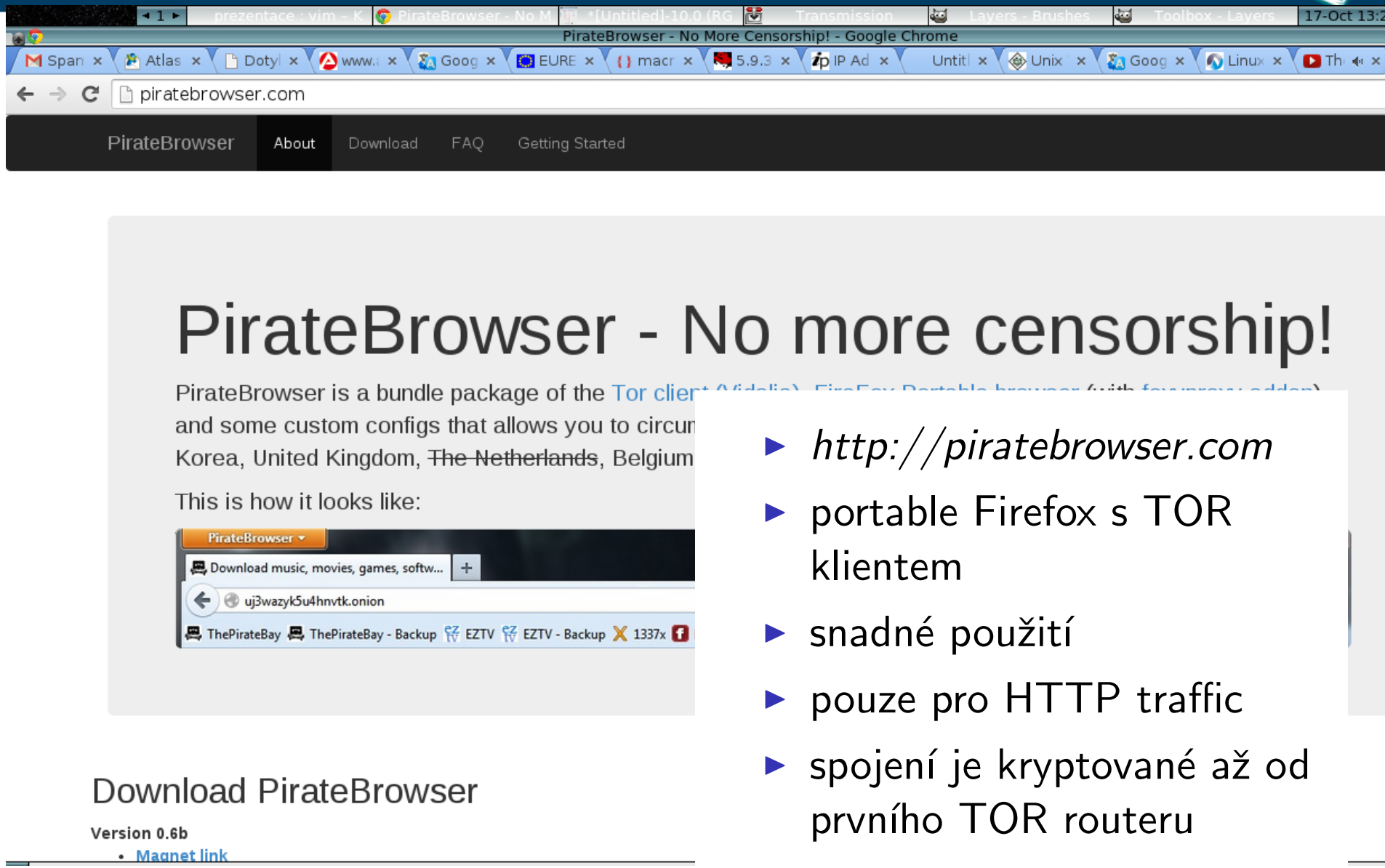


Download PirateBrowser

Version 0.6b

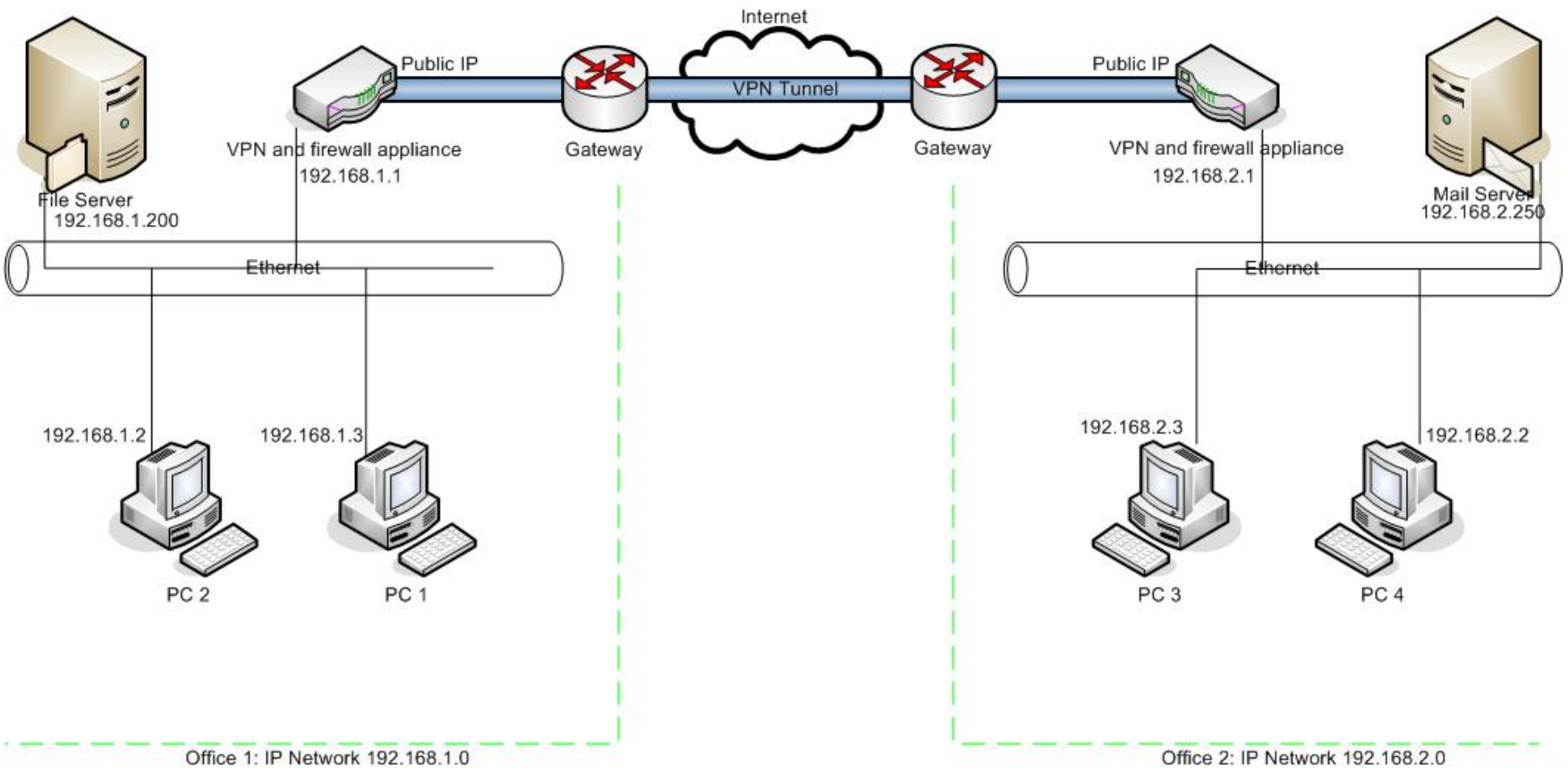
- Magnet link

PirateBrowser



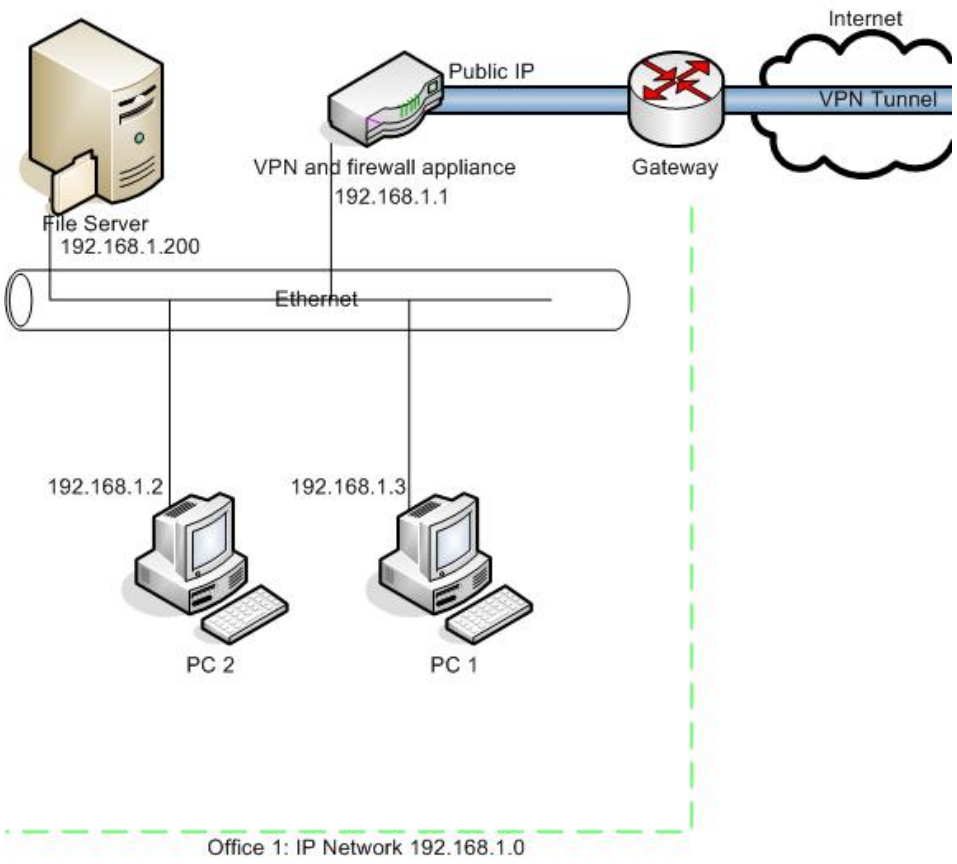
- *http://piratebrowser.com*
- portable Firefox s TOR klientem
- snadné použití
- pouze pro HTTP traffic
- spojení je kryptované až od prvního TOR routeru

VPN


ATLAS ACCESS SARL
Site to Site VPN
Internet
Public IP
VPN Tunnel
Public IP
VPN and firewall appliance
192.168.1.1
Gateway
Gateway
VPN and firewall appliance
192.168.2.1
File Server
192.168.1.200
Mail Server
192.168.2.250
Ethernet
Ethernet
192.168.1.2
192.168.1.3
192.168.2.3
192.168.2.2
PC 2
PC 1
PC 3
PC 4
Office 1: IP Network 192.168.1.0
Office 2: IP Network 192.168.2.0

Obrázek: [?]

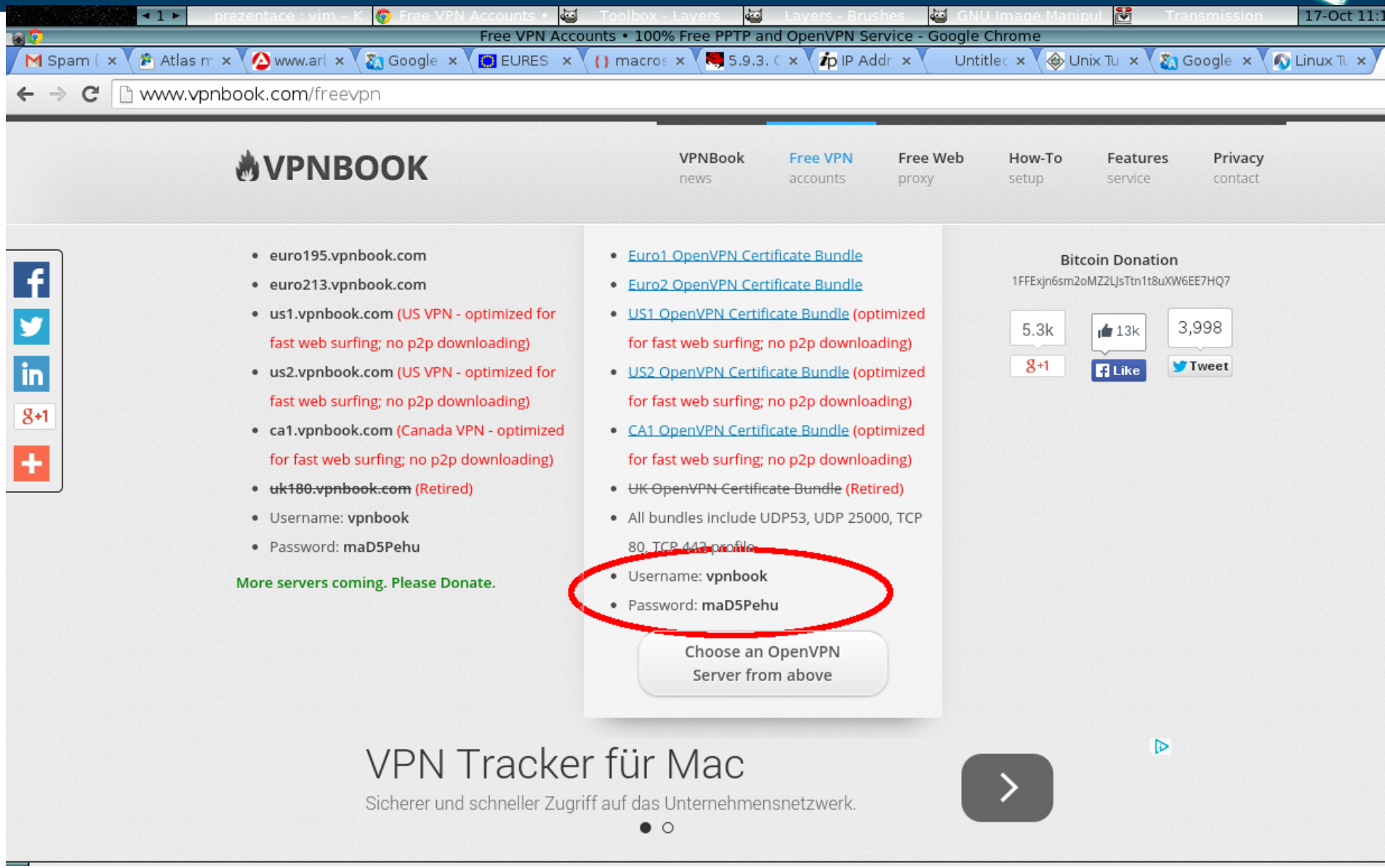
VPN



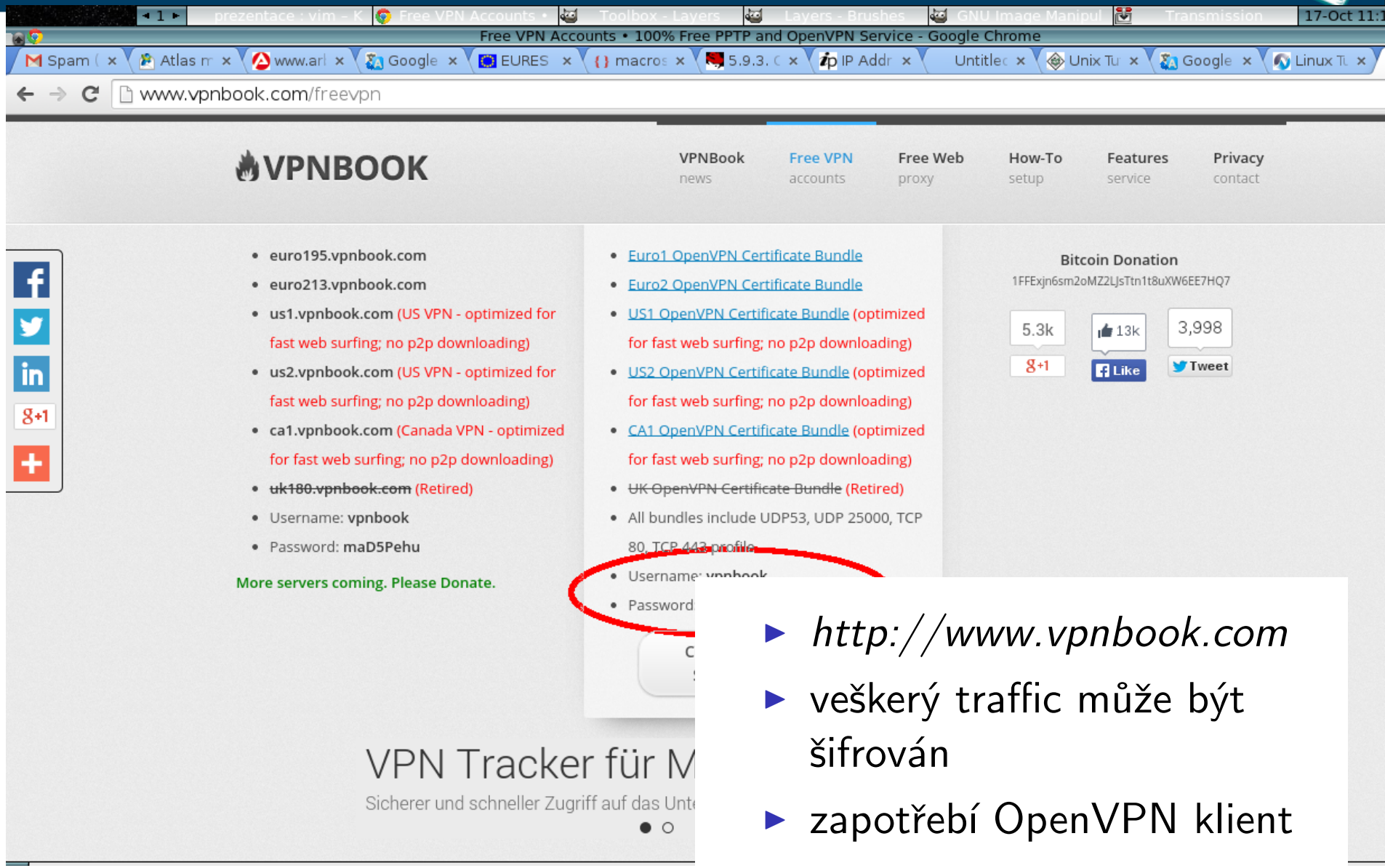
- služba zajišťující důvěrnost, autenticitu a integritu
- využívá bezpečnostních protokolů (IPSec, SSL, SSH)
- možno tunelovat skrz veřejný internet
- ideální řešení pro vzdálený přístup k datům, příp. anonymizace

Obrázek: [?]

VPN

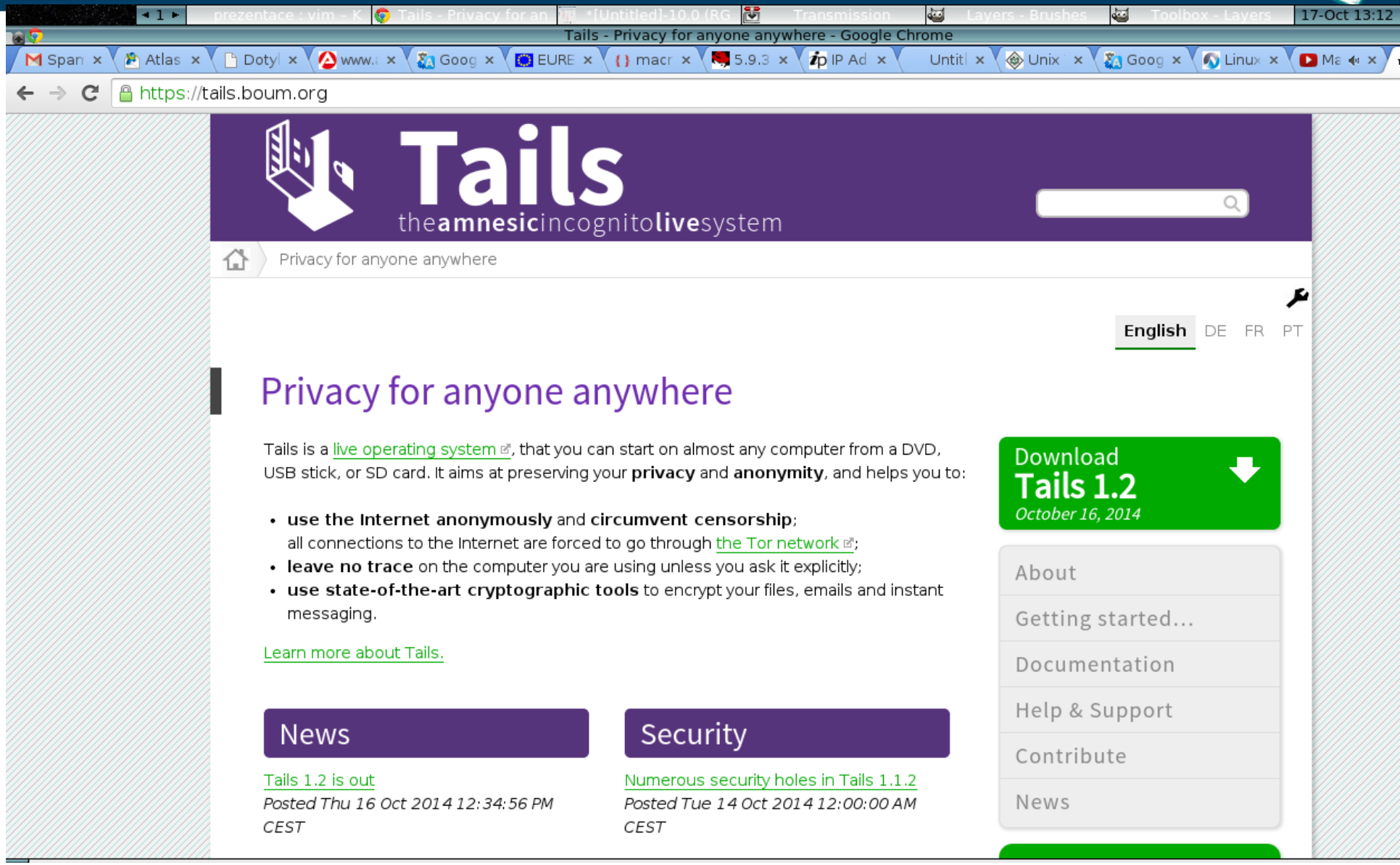

Free VPN Accounts • 100% Free PPTP and OpenVPN Service - Google Chrome
www.vpnbook.com/freevpn
VPNBOOK
VPNBook news
Free VPN accounts
Free Web proxy
How-To setup
Features service
Privacy contact
euro195.vpnbook.com
euro213.vpnbook.com
us1.vpnbook.com (US VPN - optimized for fast web surfing; no p2p downloading)
us2.vpnbook.com (US VPN - optimized for fast web surfing; no p2p downloading)
ca1.vpnbook.com (Canada VPN - optimized for fast web surfing; no p2p downloading)
uk180.vpnbook.com (Retired)
Username: vpnbook
Password: maD5Pehu
More servers coming. Please Donate.
Euro1 OpenVPN Certificate Bundle
Euro2 OpenVPN Certificate Bundle
US1 OpenVPN Certificate Bundle (optimized for fast web surfing; no p2p downloading)
US2 OpenVPN Certificate Bundle (optimized for fast web surfing; no p2p downloading)
CA1 OpenVPN Certificate Bundle (optimized for fast web surfing; no p2p downloading)
UK OpenVPN Certificate Bundle (Retired)
All bundles include UDP53, UDP 25000, TCP 80, TCP 443 profile
Username: vpnbook
Password: maD5Pehu
Choose an OpenVPN Server from above
Bitcoin Donation
1FFExjn6sm2oMZ2LJsTtn1t8uXW6EE7HQ7
5.3k
13k
Like
3,998
Tweet
VPN Tracker für Mac
Sicherer und schneller Zugriff auf das Unternehmensnetzwerk.

VPN

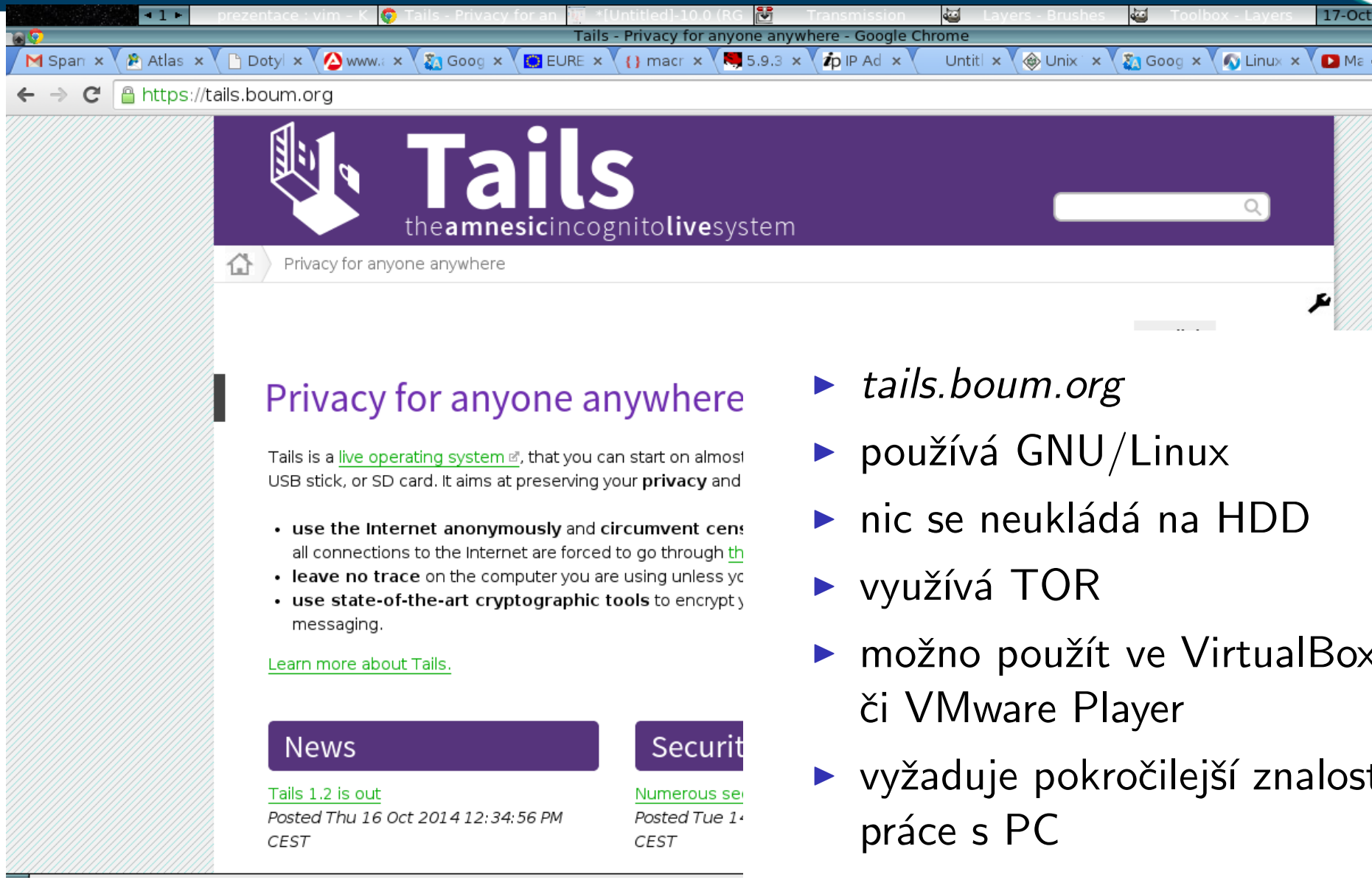


- *http://www.vpnbook.com*
- veškerý traffic může být šifrován
- zapotřebí OpenVPN klient

Linux Live CD



Linux Live CD



- *tails.boum.org*
- používá GNU/Linux
- nic se neukládá na HDD
- využívá TOR
- možno použít ve VirtualBox či VMware Player
- vyžaduje pokročilejší znalosti práce s PC

Pár drobných rad

- nepoužívejte Google - místo toho DuckDuckGo.com, ixquick.com
- nepoužívejte Chrome (Google produkt) - Mozilla (plugins: Ghostery, NoScript, Adblock Plus, HTTPS Everywhere)
- neukládejte hesla do svého prohlížeče
- vyhýbejte se proprietárnímu software (Skype, ICQ) - nevíte co se kam odesílá

Závěr - obecná pravidla pro koncového uživatele

- vzdělanost uživatele (znalost firemních politiky, hesla, emaily, social engineering, přístup do budovy)
- nestahovat software a data, o kterých nevím co obsahují
- veškerá data skenovat pomocí AV
- updatovaný OS, AV, anti-spyware, HIPS a firewall
- podezřelé emaily neotvírat neklikat na linky v nich, neotvírat přílohy
- použít web-based content filtering (alespoň v případě dětí)
- nikdy nepoužívat administrátorský účet
- vždy a pravidelně zálohovat

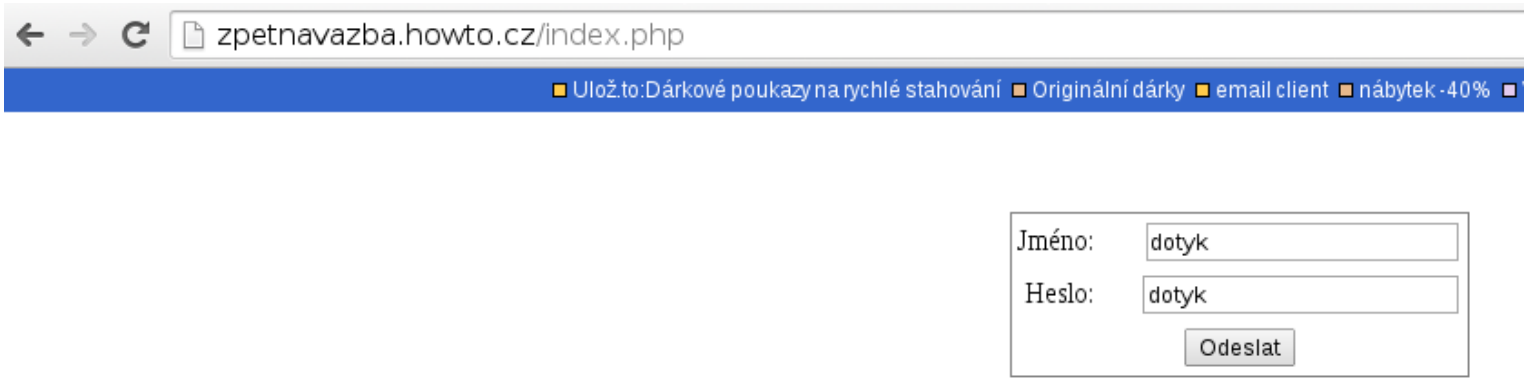
Závěr - obecná pravidla pro koncového uživatele

- řada client side útoků lze odvrátit zakázáním: JavaScript, Java applet, Flash, ActiveX
- druhá strana mince - většina webů spoléhá na tyto technologie
- obecně platí - běžný software - více hrozeb
- bezpečnější surfování (*BSD, Firefox)

Závěr - obecná pravidla pro administrátory

- definování firemní bezpečnostní politiky
- použití web-based content filtering (proxy), HTTP application firewall
- protokoly, které nejsou potřeba zakázat na perimetru
- nasazení vulnerability scenning řešení (Nessus)
- nasazení IPS/IDS (Snort), SPAM-filtering (SpamAssassin)
- vhodná segmentace sítě (DMZ)
- pro vzdálený přístup nasazení VPN
- logování a audit logů
- virtualizace, použití tenkých klientů

Zpětná vazba



Zdroje

- *New Eavesdropping Equipment Sucks All Data Off Your Phone* http://www.urrepublic.com/new-eavesdropping-equipment-sucks-all-data-off-your-phone/
- *Password Recommendations* https://security.web.cern.ch/security/recommendations/en/passwords.shtml
- *Bezpečné heslo* http://cs.wikipedia.org/wiki/Bezpe%C4%8Dn%C3%A9_heslo
- *Report: Most vulnerable operating systems and applications in 2013* http://www.gfi.com/blog/report-most-vulnerable-operating-systems-and-applications-in-2013/
- *CVE Database* http://www.cvedetails.com/
- *What is PKI* http://software-engineer-tips-and-tricks.blogspot.cz/2012/09/what-is-pki.html

Zdroje

- *Upozornění na nový phishingový útok* http://www.csas.cz/banka/content/inet/internet/cs/news_ie_2280.xml?archivePage=phishingi&navid=nav00156_phishing_aktuality
- *IP address location* http://www.ipaddresslocation.org
- *Cognitive Networks and Future Internet* http://www.surrey.ac.uk/ics/research/cognitivenetworks/
- *Man-in-the-middle attack* https://www.owasp.org/index.php/Man-in-the-middle_attack
- *VPN* http://atlas-access.com/assets/images/vpn-site-to-site.jpg
- Harper A., Harris S., Ness J., Eagle Ch., Lenkey G., Williams T.: *Gray Hat Hacking, The Ethical Hacker's Book* 3^{rd} Edition McGraw-Hill 2011 ISBN: 978-0-07-174256-6

Zdroje

- Davis M., Bodmer S., Lemasters A. *Hacking Exposed: Malware & Rootkits* McGraw-Hill 2010 ISBN: 978-0-07-159119-5
- *Botnet* http://en.wikipedia.org/wiki/Botnet