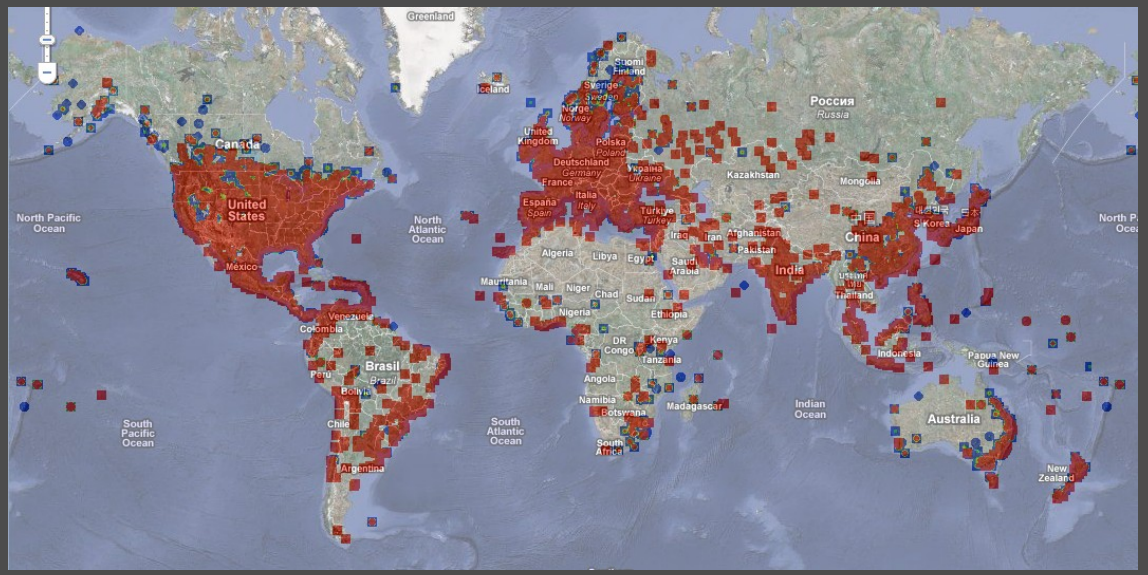
InSecurity 2009

bodik and c++

Everlasting MS DCE - 2009 revival

- 2003 Blaster (DCOM)
  - reversed patch by .pl
  - in a month (MS03-026)
  - **BUSTED !?**
- 2004 Sasser (LSASS)
  - reversed patch by .ru ? .de
  - in a 17 days (MS04-011)
  - **BUSTED !?**



- 2008/2009 Conficker
  - reversed patch by ??
  - in a month or less (MS08-067)
  - organized realtime cyberfight

Conficker - Phase 1 - Spreading

- Conficker.A - offense (Nov 21, 2008)
  - MS08-067
  - selective infection - GeoIP, SystemGetDefaultLang()
  - updates by generated DNS for HTTP RV (250 domains / day)
  - validated updates
- Conficker.B - around the firewalls (Dec 29, 2008)
  - open/weak SMB shares
  - USB Autoruns - sticks, cameras, phones, ... ;)))
  - backdoored patch for MS08-067 for reinfection/updates
  - disable AV - proc kill, block AV DNS

- WANTED - Dead or alive for $250 000 (Feb 12, 2009)
- MS disables autoruns through updates (Feb 25, 2009)

Conficker - Phase 2 - Command and Conq.

- Conficker.C - conquer anything around (Feb 16, 2009)
  - revealing DNS generation algo leads to a new C&C
  - validated *p2p* updates through NetBIOS
    - named pipe, netapi32.dll patch
  - if any host gets update, all LAN host does too

- Conficker.D - hide (Mar 04, 2009)
  - stopped to replicate
  - DNS generation algo for HTTP C&C grows to 50 000/day
  - encrypted & validated p2p C&C over custom protocol
    - runtime updates
    - data storage

Conficker.E - cashback ? (Mar 07, 2009)

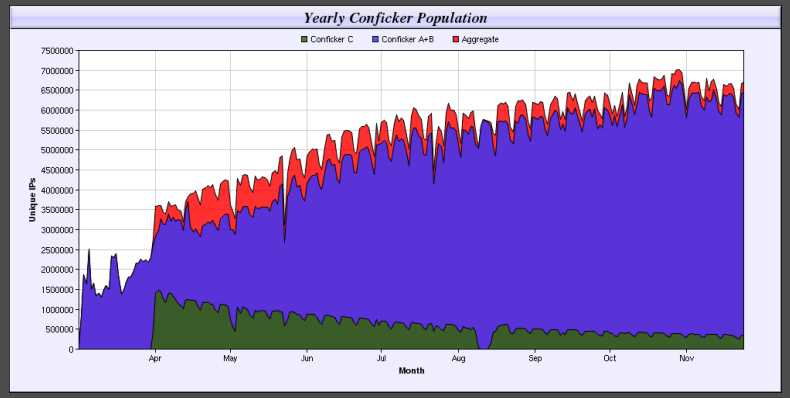
- spread again
- install spyware and remove itself (leaving D alone)

Conficker - the state-of-art in malware 09

- Conficker is generic largescale execpad and p2p blob sharing
- Advanced crypto primitives saves the day (OpenSSL)
  - RSA 1K > 4K, SHA-1 > MD6 (brand new algo from MIT!!)
- Highly obfuscated, anti-debug, anti-emulation
  - indirect API calls, control flow mess, *customized calling convention*
- Many rootkit abilities
  - runs through DLL injection as a thread (CreateRemoteProcess)
  - DLL loadlib never exits - it's not officialy registered
  - Disable AV sw, blocks AV/updates by DNS hook
  - NTFS *hide*
  - In memory runtime patchin, ?micro-length disassembler?
- Internet Randezvous generation algoritm
  - DGA
  - P2P protocol without embedded peerlist

Conficker - management summary imho

- MS Genuine Notification and Autorun works very well for everybody
- Doubled subsystems - HA in design
  - infection vectors
  - spreading threads
  - C&C



- CWG monitors over 7M population *(Nov 29, 2009)*
  - *Even skilled support would clean it in*

*(population * hrsPerPC) / hrsPerYear*

*(7M * 4) / 8760 = 3196 Years*

Do you want to know more ?

????

Beef Browser Abuse

BGP Cripling
TLS/SSL

Conficker virus
exploited vulnerability

Evil Maid
Stoned Bootkit
Hardware attacks

Psyb0t - DSL, Embed
Network eavesdropping

Botnet

Last year - Bodík talked about botnets and predicted steep grow,
Conficker comes, but it's old playground Win32
This year - Botnets grow (He was right / aplause please)

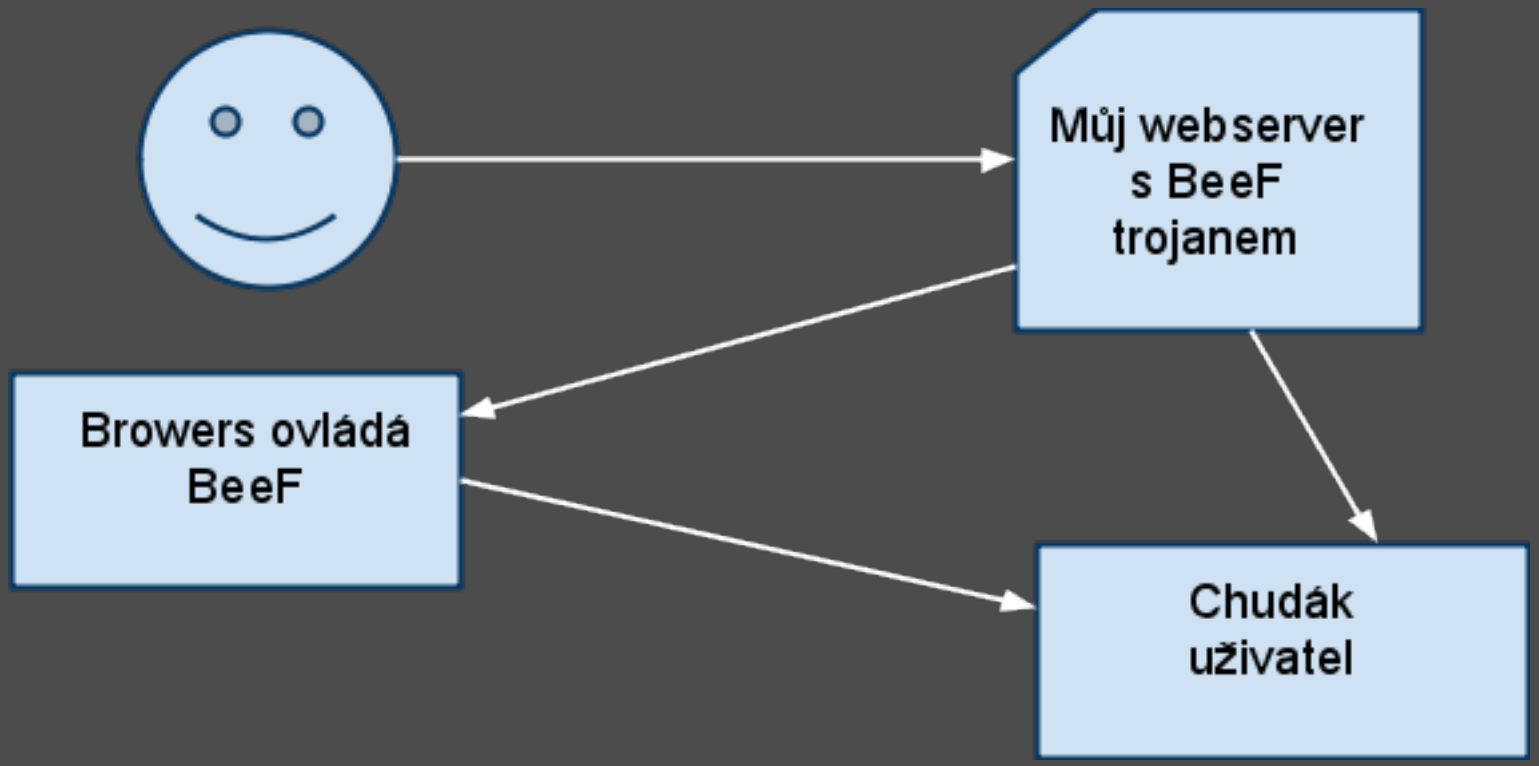
Router Botnets: Home DSL, WiFi is just a little plastic box, is it?
Well, it is a small comp (CPU mipsel, arm), with TCP/IP embeded.
That's enough for spam, DDoS, port scan...

The botnet Psyb0t/bluepill infected 100,000 hosts.

- is the first botnet worm to target routers and DSL modems
- contains shellcode for many mipsel devices
- is not targeting PCs or servers
- uses multiple strategies for exploitation, including bruteforce username and password combinations
- harvests usernames and passwords through deep packet inspection
- can scan for exploitable phpMyAdmin and MySQL servers
- UDP, TCP, ICMP, URL flooding

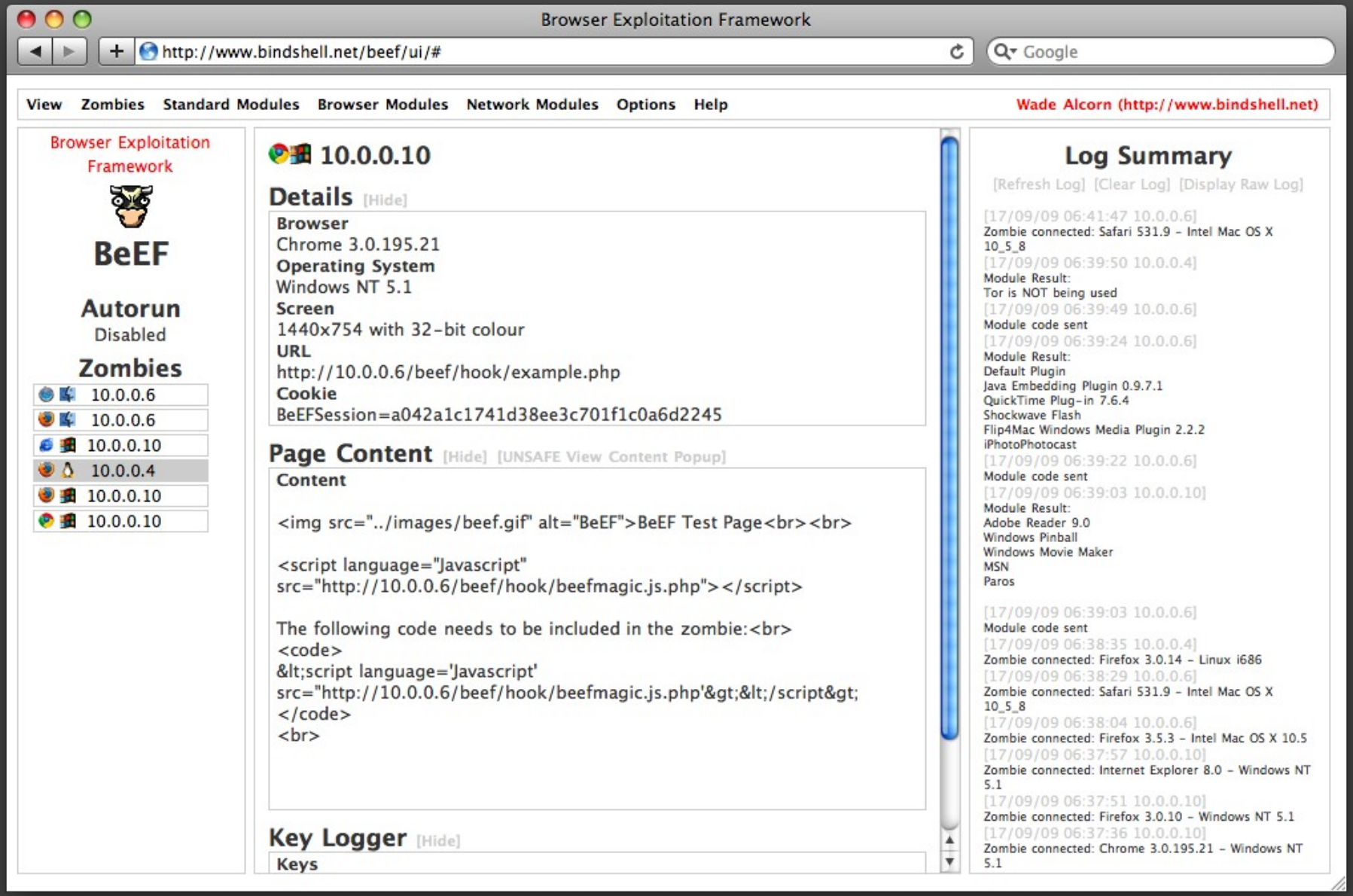
Botnet II

Browser based botnets: Now the Rocket Science begins: Botnet in a browser session. More than just a proof of concept: **BeeF: Browser Exploitation Framework**.



Botnet II Beef

Screenshot



Botnet III Darknet

Darknet: Black Hat USA researchers demonstrate a way to use modern browsers to more easily build darknets — underground private Internet communities where users can share content and ideas **securely** and **anonymously**. HP's Billy Hoffman and Matt Wood have created Veiled darknet.

Darknet makes the communication possible - with only the browser. The web servers with the Veiled code are just the routers, not the storage!

Do you want to know more ??

????

Beef Browser Abuse

Conficker virus
exploited vulnerability

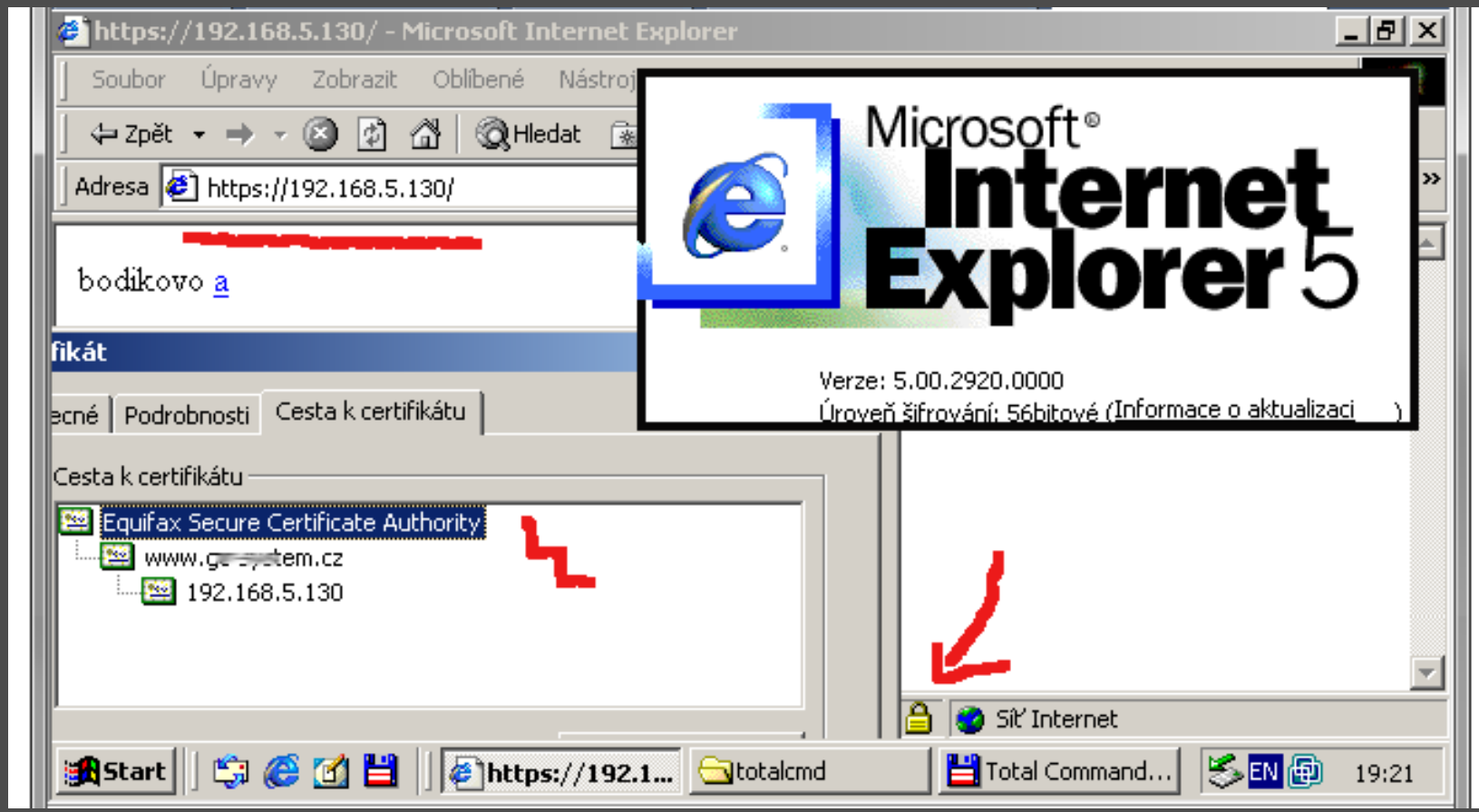
TLS/SSL

Evil Maid
Stoned Bootkit
Hardware attacks

Psyb0t - DSL, Embed
Network eavesdropping

History of attacks on SSL

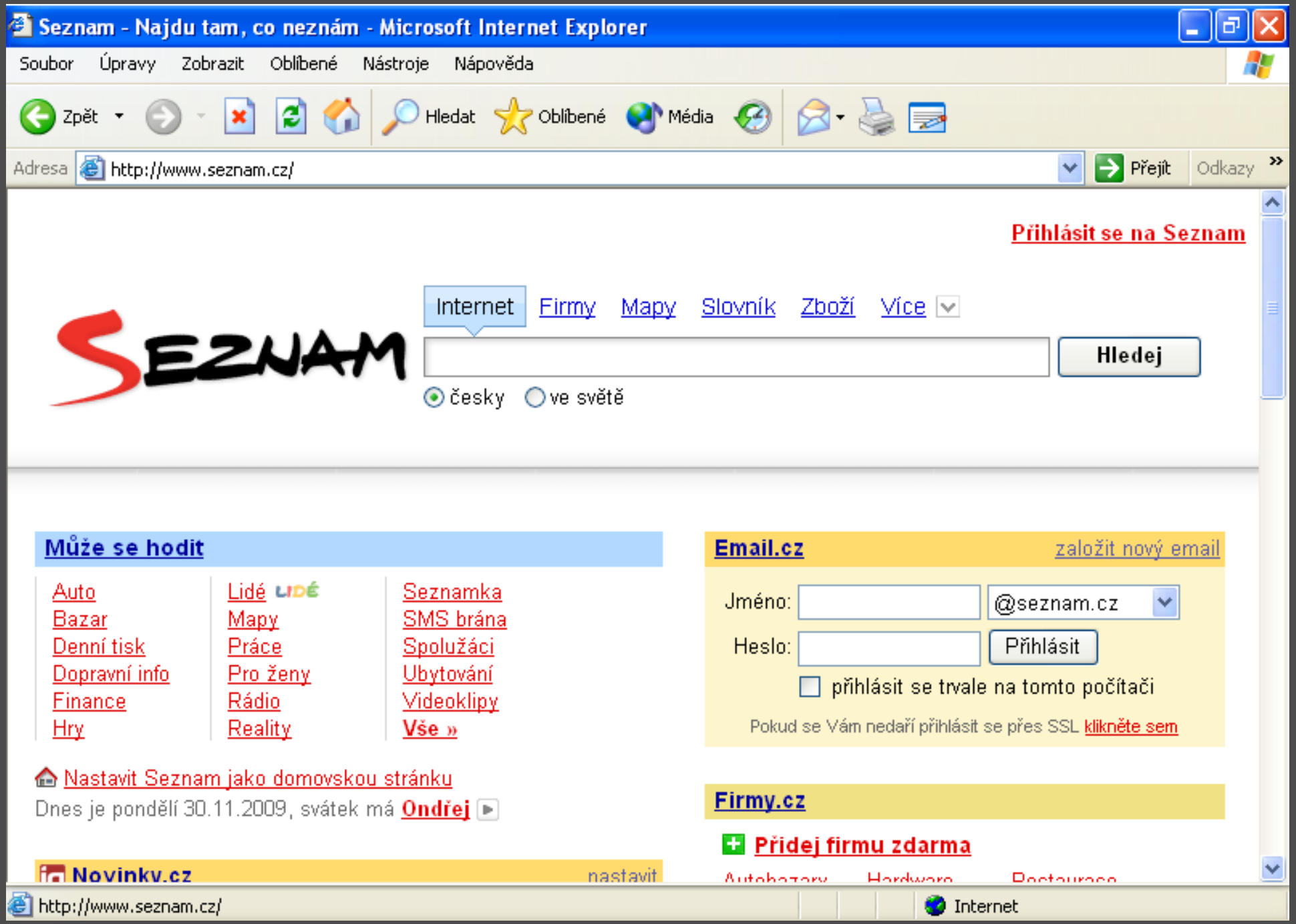
- 2002 - thoughtcrime.org/sslsnif
  - bad/naive implementation of certificate validation
    - basicConstraints, CA=false, ...
    - valid leaf can sign any other name
  - still works with MD5 collisions (Wang, Klima)

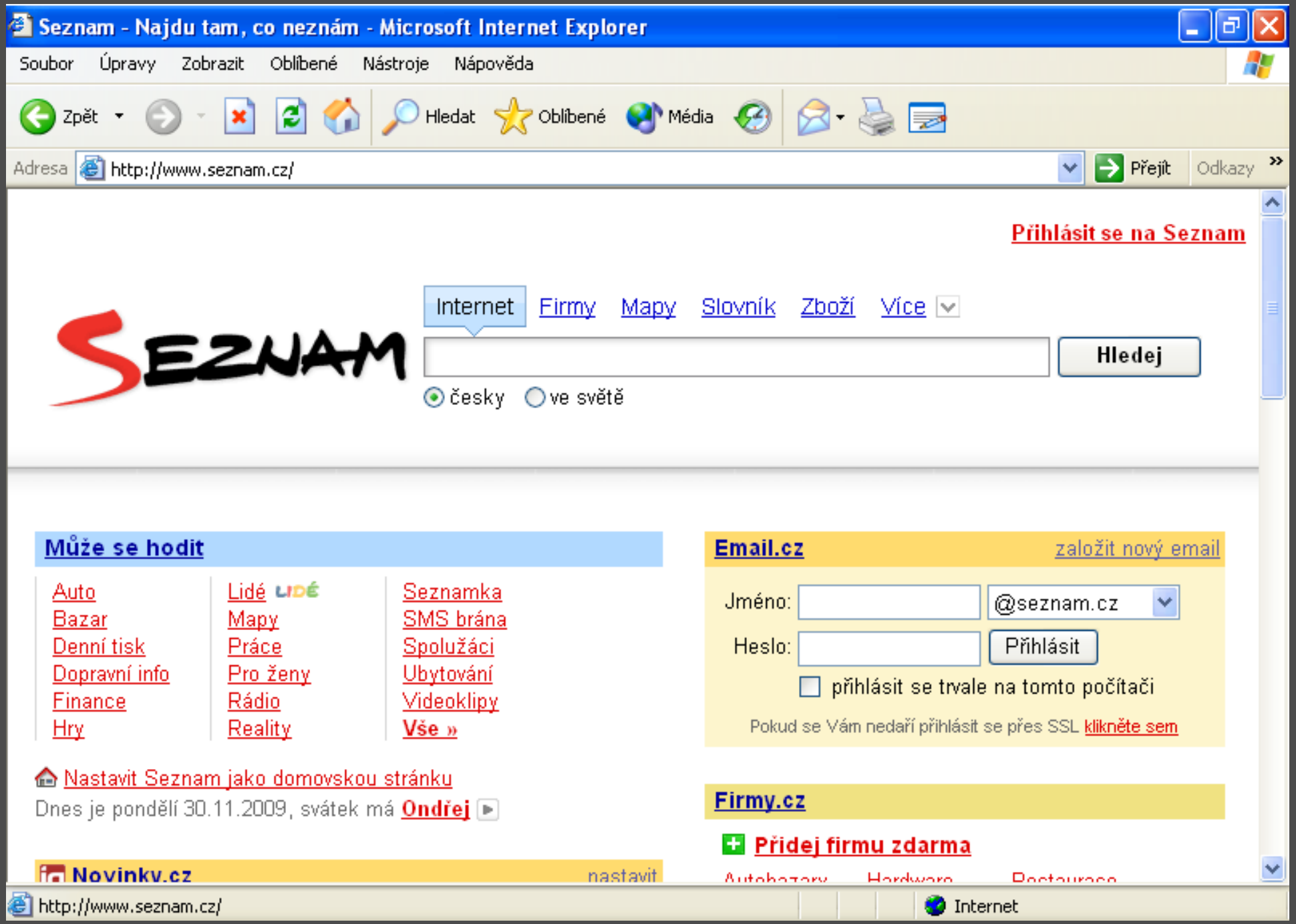


sslstrip

- 2009 - thoughtcrime.org/sslstrip
  - SSL starts by
    - click on URL
    - 302 HTTP Redirect
  - Don't let user to start it
    - intercept all traffic in proxy and strip the great "S"

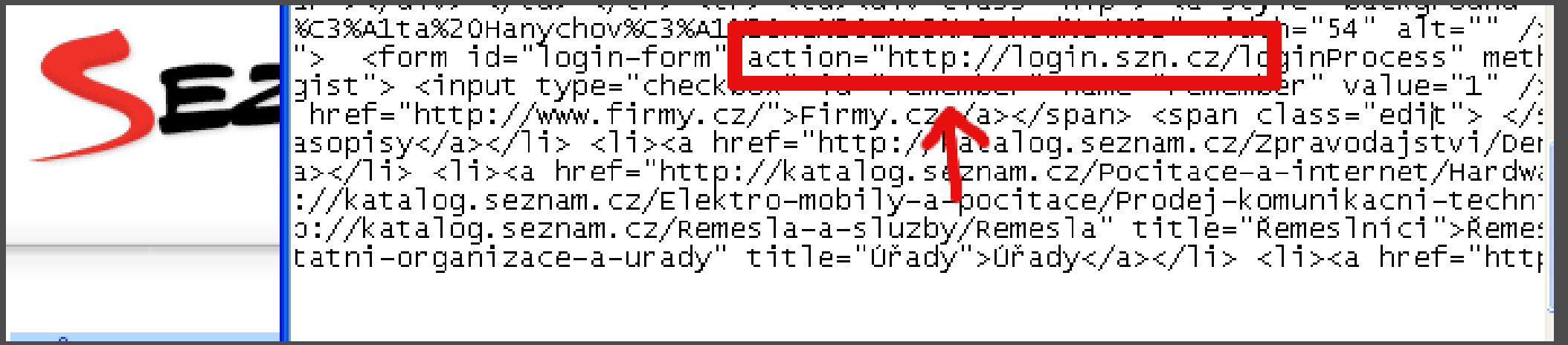
```
#!/usr/bin/perl -w

use HTTP::Proxy;
my $proxy = HTTP::Proxy->new( port => 3128, host => '192.168.5.

{
  package FilterPerl; use base qw( HTTP::Proxy::BodyFilter );
  sub filter {
    my ( $self, $dataref, $message, $protocol, $buffer ) = @_;
    $$dataref =~ s/https/http/g;
  }
}
$proxy->push_filter( response => FilterPerl->new() );

$proxy->start;
```


Seznam - Najdu tam, co neznám - Microsoft Internet Explorer
Soubor Úpravy Zobrazit Oblíbené Nástroje Nápověda
Zpět Hledat Oblíbené Média
Adresa http://www.seznam.cz/
Přejít Odkazy
Přihlásit se na Seznam
SEZNAM
Internet Firmy Mapy Slovník Zboží Více
Hledej
česky ve světě
Může se hodit
Auto Bazar Denní tisk Dopravní info Finance Hry
Lidé Mapy Práce Pro ženy Rádio Reality
Seznamka SMS brána Spolužáci Ubytování Videoklipy Vše »
Nastavit Seznam jako domovskou stránku
Dnes je pondělí 30.11.2009, svátek má Ondřej
Email.cz
založit nový email
Jméno: @seznam.cz
Heslo: Přihlásit
přihlásit se trvale na tomto počítači
Pokud se Vám nedaří přihlásit se přes SSL klikněte sem
Firmy.cz
Přidej firmu zdarma
Novinky.cz
nastavit
http://www.seznam.cz/
Internet


Seznam - Najdu tam, co neznám - Microsoft Internet Explorer
Soubor Úpravy Zobrazit Oblíbené Nástroje Nápověda
Zpět Hledat Oblíbené Média
Adresa http://www.seznam.cz/
Přejít Odkazy
Přihlásit se na Seznam
SEZNAM
Internet Firmy Mapy Slovník Zboží Více
Hledej
česky ve světě
Může se hodit
Auto Bazar Denní tisk Dopravní info Finance Hry
Lidé Mapy Práce Pro ženy Rádio Reality
Seznamka SMS brána Spolužáci Ubytování Videoklipy Vše »
Nastavit Seznam jako domovskou stránku
Dnes je pondělí 30.11.2009, svátek má Ondřej
Email.cz
založit nový email
Jméno: @seznam.cz
Heslo: Přihlásit
přihlásit se trvale na tomto počítači
Pokud se Vám nedaří přihlásit se přes SSL klikněte sem
Firmy.cz
Přidej firmu zdarma
Novinky.cz
nastavit
http://www.seznam.cz/
Internet

Diff


h4 class="more-news">Více sportu »</
ref="http://www.super.cz/bulvar/hvezdne-kauzy/36298-tezce-nemocna-anna-k
pan class="perex"> </td> </tr> </table> <h4 class="more-news
.cz/kategorie/154-vtipky-a-srandicky" id="streamL-2">Vtipná videa</
und-image:url(/favicons/194/1.jpg?r=Smrt%20moder%C3%A1tora%20v%20Nekece
width="54" alt="" /> <a h
area"> <form id="login-form" action="https://login.szn.cz/loginPr
s="regist"> <input type="chec
'>Firmy.cz <span class="edit"
/">Časopisy <a href="http://katalog.seznam.cz/Zpravodajstv
al <a href="http://katalog.seznam.cz/Pocitace-a-internet/Ha


%C3%A1ta%20Hanychov%C3%A1
"> <form id="login-form" action="http://login.szn.cz/loginProcess" meth
gist"> <input type="checkbox" id="remember" name="remember" value="1" />
href="http://www.firmy.cz/">Firmy.cz </
asopisy <a href="http://katalog.seznam.cz/Zpravodajstvi/Der
a> <a href="http://katalog.seznam.cz/Pocitace-a-internet/Hardwa
://katalog.seznam.cz/Elektro-mobily-a-pocitace/Prodej-komunikacni-techn
p://katalog.seznam.cz/Remesla-a-sluzby/Remesla" title="Řemeslníci">Řeme
tatni-organizace-a-urady" title="Úřady">Úřady <a href="http

Moxie's sslstrip

- yes, you need to be in the middle ... ...
- tool sslstrip does a bit more ..
  - favico.ico forces positive trigger
  - transparently adds SSL when needed

TLS renegotiation MITM

Exploiting this requires the attacker to be able to intercept the traffic. Using one channel to forward client communication, attacker injects HTTP header into SSL stream.

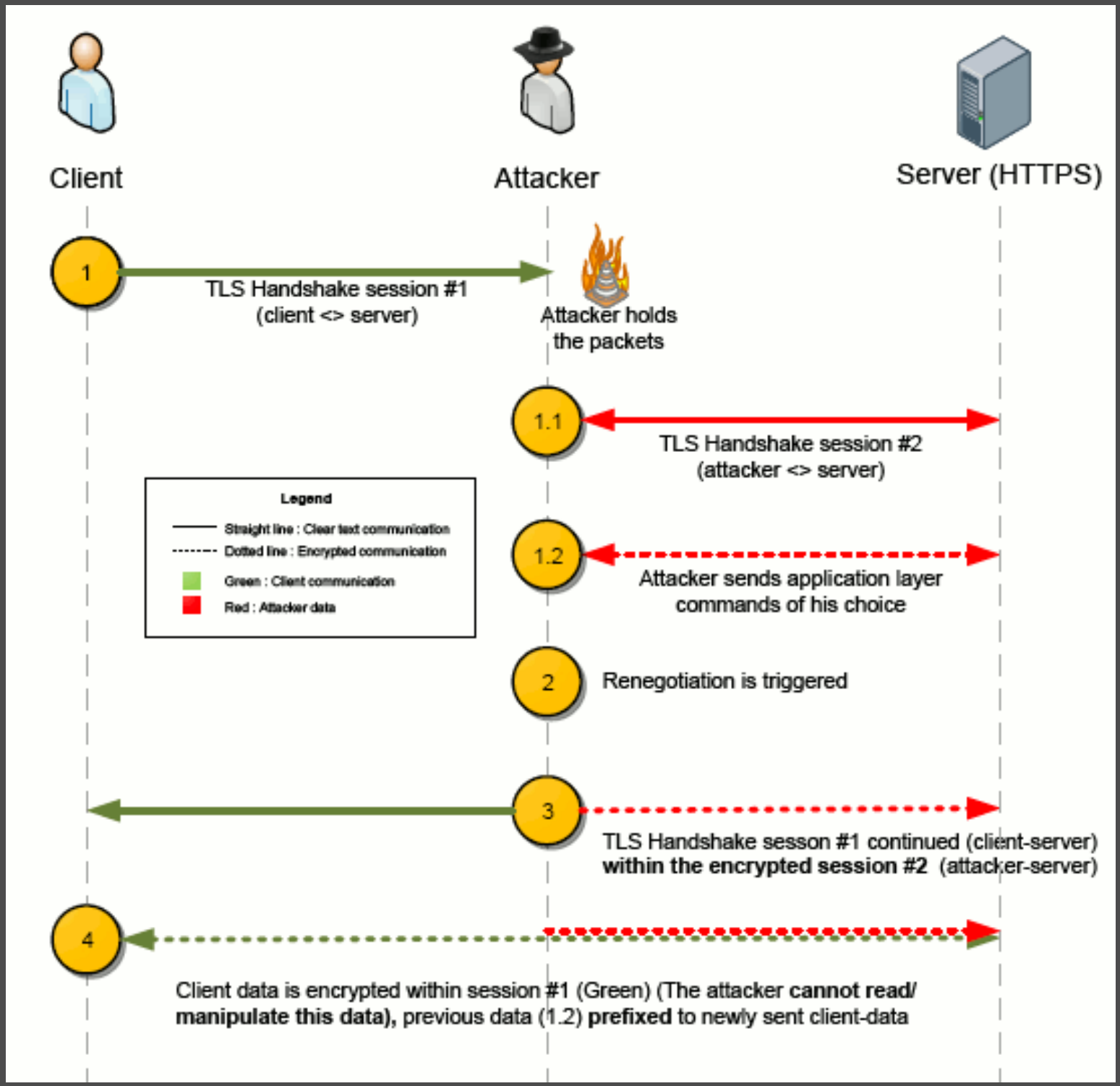
Renegotiation does not invalidates former input. In this case - the attackers.

http://isc.sans.org/diary.html?storyid=7534&rss

SSL bad
TLS – modules, patched

Turn off RENEGO!

tls renego


Client
Attacker
Server (HTTPS)
1
TLS Handshake session #1
(client <> server)
Attacker holds
the packets
1.1
TLS Handshake session #2
(attacker <> server)
Legend
Straight line : Clear text communication
Dotted line : Encrypted communication
Green : Client communication
Red : Attacker data
1.2
Attacker sends application layer
commands of his choice
2
Renegotiation is triggered
3
TLS Handshake sesson #1 continued (client-server)
within the encrypted session #2 (attacker-server)
4
Client data is encrypted within session #1 (Green) (The attacker cannot read/
manipulate this data), previous data (1.2) prefixed to newly sent client-data

x509 CN NULL prefix attack

- the old story
  - sslsniff
    - CA=false ... bugs in validation basicConstraints
  - sslstrip
    - attacking bridge between HTTP and HTTPS
    - positive vs negative triggers
  - but that's just web ...
  - what about bookmarks, ftps, imaps, vpn, ...
    - there are no bridges .... so ?

x509

- what is x509 certificate anyway ?
  - x509
    - it's like an ID or passport ...
      - Version
      - Serial Number
      - Validity
      - Issuer
      - Subject
      - PublicKey
    - SignatureAlgorithm
    - Signature

How x509 is used, how it is created ?

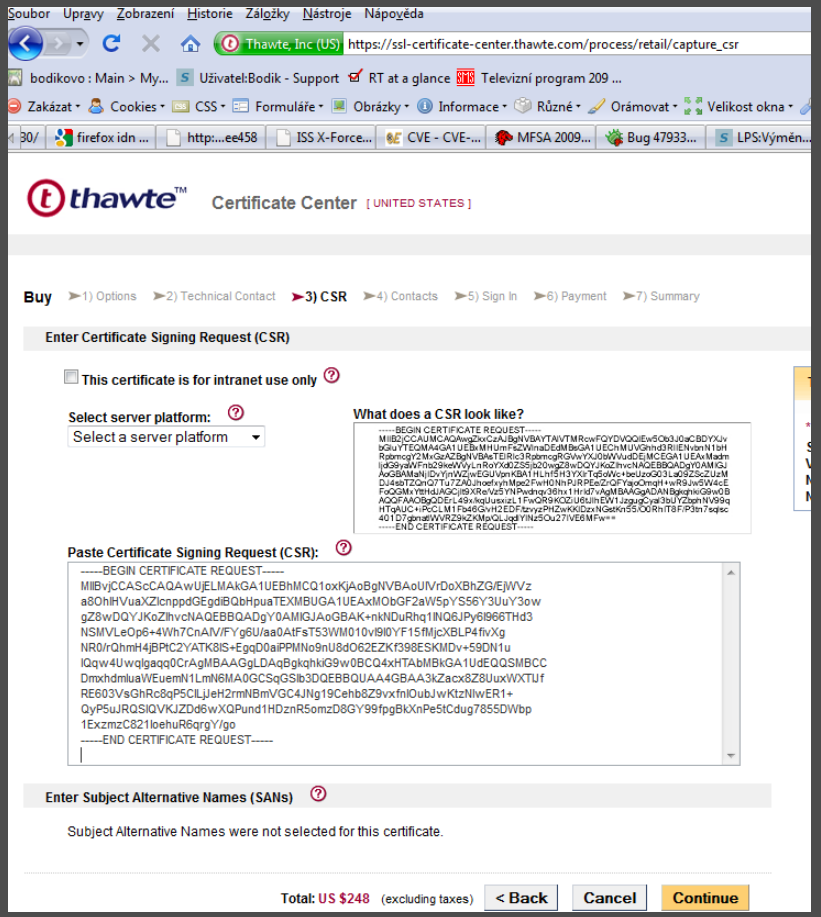
- how certificate is used
  - SSL/TLS handshake
    - Client > ClientHello
    - Server > ServerHello, ServerCertificate
  - user's browser compares Subject to address in URL bar
  - ... .

- how it is created ?
  - back in 2000 - notaries, phone calls, ... uf uf

  - but today .. hoooraaay ;)
    - online domain validation
    - automated process

Online domain validation - PKCS#10

- PKCS #10 - request
  - Version
  - Subject
  - PublicKey
  - Attributes



- CA workflow
  - looks for Subject - www.bodik.cz
  - grab the root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

x509 Subjects - DistinguishedName

- http://tools.ietf.org/html/rfc3280#section-4.1.2.6

- DistinguishedName
  - Country
  - State
  - Locale
  - Organization
  - Organizational Unit
  - Common Name
    - mostly DNS ...
    - ... but could be really anything

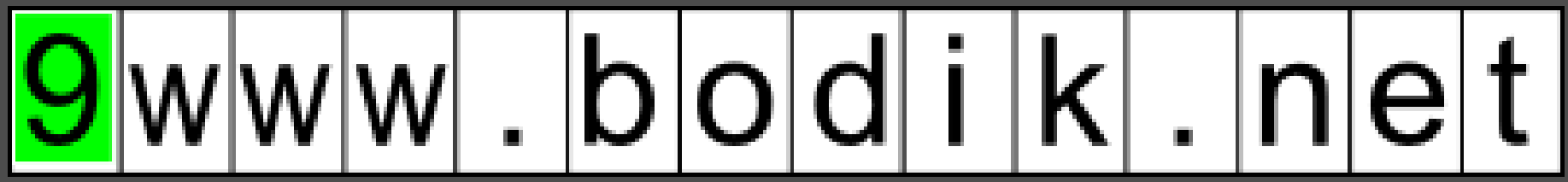
DistinguishedName - CommonName

- http://tools.ietf.org/html/rfc3280#section-4.1
- http://www.imc.org/ietf-pkix/old-archive-93-96/msg00090.html
- Dostálek: Průvodce po galaxiích TCP/IP a DNS

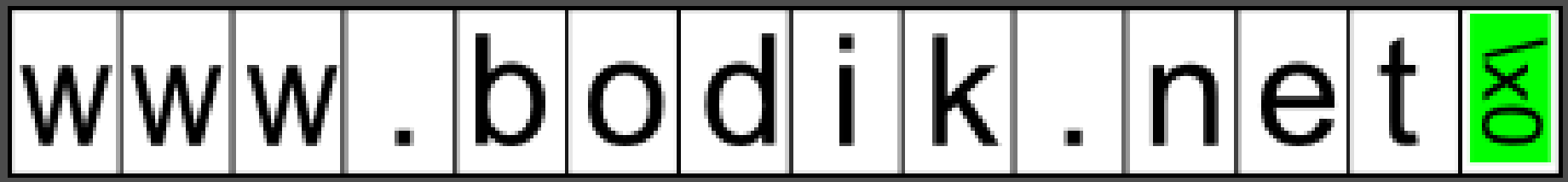
```
commonName ::= SEQUENCE
    {
        { 2 5 4 3 },
        StringType ( SIZE( 1...64 ) )
     }

... do very big magic here with ASN.1 / BER ...

IA5String :== { ID, Length, data }
```

IA5String vs char[]

- IA5Strings are like Pascal strings



- strings in C are different (char[])
  - NULL - \x0 - has a special meaning - *EOS*



Let's roll ...

- CA workflow
  - looks for Subject - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

Let's roll ...

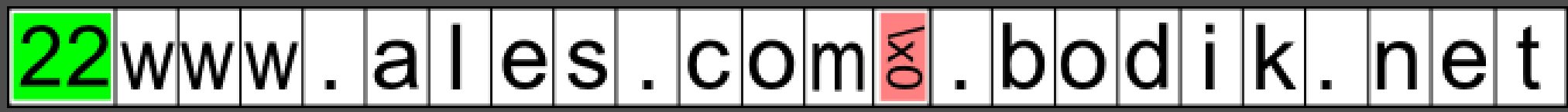
- CA workflow
  - looks for Subject - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

Let's roll ...

- CA workflow
  - looks for Subject - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

Let's roll a little bit more ...

- CA workflow
  - looks for Subject - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz



  - CA will contact bodik.net for confirmation ... hoorayy ..

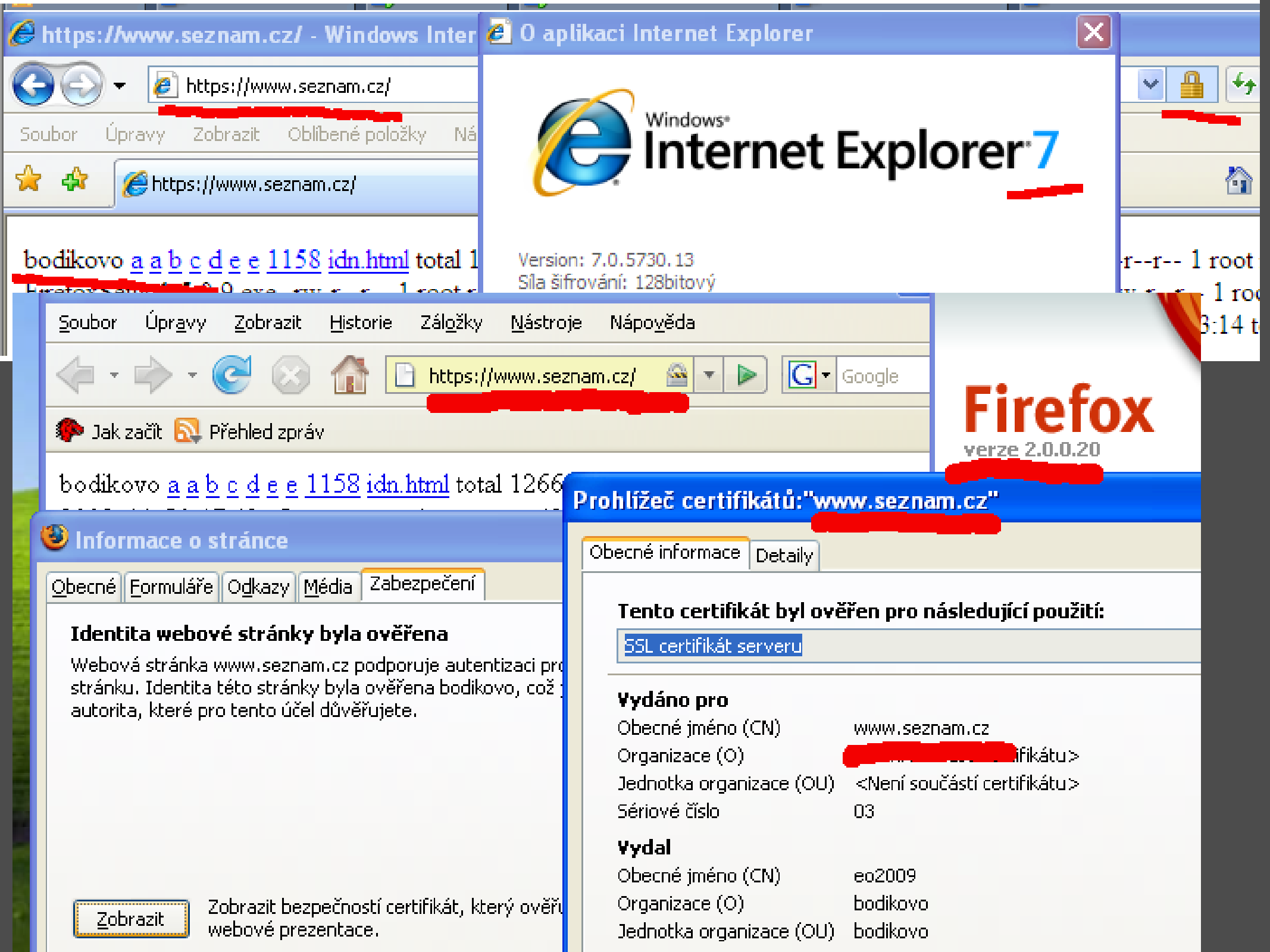
... strings in C, again, again, agaiiiiiiiiiiiiiii

- Browser workflow
  - Contacts server stated in URL bar of a browser
  - > ClientHello
  - < ServerHello, ServerCertificate
  - Compares URL with Subject char by char in C manner

```
strcmp(destination, commonName)
```

... result's in error in validation

- Browsers
  - Firefox, Explorer, Lynx, Curl
- Mail clients
  - Thunderbird,Outlook,Evolution
- IM
  - Pidgin, AIM, irssi, centericq, ...
- SSL VPN
  - AEP, Citrix, ...


https://www.seznam.cz/ - Windows Inter
https://www.seznam.cz/
Soubor Úpravy Zobrazit Oblíbené položky
https://www.seznam.cz/
bodikovo a a b c d e e 1158 idn.html total 1
O aplikaci Internet Explorer
Windows Internet Explorer 7
Version: 7.0.5730.13
Síla šifrování: 128bitový
Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda
https://www.seznam.cz/
Google
Jak začít
Přehled zpráv
bodikovo a a b c d e e 1158 idn.html total 1266
Firefox
verze 2.0.0.20
Informace o stránce
Obecné Formuláře Odkazy Média Zabezpečení
Identita webové stránky byla ověřena
Webová stránka www.seznam.cz podporuje autentizaci pro
stránku. Identita této stránky byla ověřena bodikovo, což
autorita, které pro tento účel důvěřujete.
Zobrazit
Zobrazit bezpečností certifikát, který ověřu
webové prezentace.
Prohlížeč certifikátů:"www.seznam.cz"
Obecné informace
Detaily
Tento certifikát byl ověřen pro následující použití:
SSL certifikát serveru
Vydáno pro
Obecné jméno (CN) www.seznam.cz
Organizace (O)
ifikátu>
Jednotka organizace (OU) <Není součástí certifikátu>
Sériové číslo 03
Vydal
Obecné jméno (CN) eo2009
Organizace (O) bodikovo
Jednotka organizace (OU) bodikovo

```
        MBSTRING_ASC, "UK", -1, -1, 0);
entry_by_txt(name,"CN",
          V_ASN1_IA5STRING, "www.seznam.cz\000.bodik.net", 24, -1,
```

```
    Issuer: C=CZ, ST=Bodikovo, L=Bodikovo, O=Bodikovo,
    Validity
        Not Before: Dec  3 23:05:09 2009 GMT
        Not After : Dec  3 23:05:09 2010 GMT
    Subject: C=UK, CN=www.seznam.cz\x00.bodik.net
    Subject Public Key Info:
```

```
20 20 20 0a 20 20 31 39  30 3a 64 3d 35 20 20 68  |    .  190:d=5  h|
6c 3d 32 20 6c 3d 20 20  20 33 20 70 72 69 6d 3a  |l=2 l=   3 prim:|
20 4f 42 4a 45 43 54 20  20 20 20 20 20 20 20 20  | OBJECT          |
20 20 20 3a 63 6f 6d 6d  6f 6e 4e 61 6d 65 0a 20  |   :commonName.  |
20 31 39 35 3a 64 3d 35  20 20 68 6c 3d 32 20 6c  | 195:d=5  hl=2 l|
3d 20 20 32 34 20 70 72  69 6d 3a 20 49 41 35 53  |=  24 prim: IA5S|
54 52 49 4e 47 20 20 20  20 20 20 20 20 20 3a 77  |TRING          :w|
77 77 2e 73 65 7a 6e 61  6d 2e 63 7a 00 2e 62 6f  |ww.seznam.cz..bo|
64 69 6b 2e 6e 65 74 0a  20 20 32 32 31 3a 64 3d  |dik.net.  221:d=|
32 20 20 68 6c 3d 32 20  6c 3d 20 20 39 32 20 63  |2  hl=2 l=  92 c|
6f 6e 73 3a 20 53 45 51  55 45 4e 43 45 20 20 20  |ons: SEQUENCE   |
```

... there are more dragons ...

- wildcard certificates
  - *\0.bodik.net
- there's other implementation error
  - NSS remote buffer overflow exploit
- OCSP
  - defeated by faking OCSP response with TryLater option
- Mozilla/Firefox
  - autoupdate feature relies on TLS channel to update server
  - updates are/were not signed :((
- Stripping NULL at CA is not a solution
  - www.ale\0s.com >> www.ales.com

Dan Kaminsky: ... more more dragons

- x509 is a BIG CRAP ...
- with multiple roots of authority, it's enough to find just one BAD to defeat all this
  - even a smallest one
  - or any intermediate
  - even when anything is fixed

Do you want to know more ???

????

Beef Browser Abuse

Conficker virus
exploited vulnerability

TLS/SSL

Evil Maid
Stoned Bootkit
Hardware attacks

Psyb0t - DSL, Embed
Network eavesdropping

jolan/a + Stoned Bootkit v2

Zase Rutkowska: Evil Maid

(jeden z prvních hackerů, který mimo jiné hacknul svoje tělo)

USB flash disk - boot the laptop - infect. After regular boot, infected laptop stores the last password. Now it is the time to steal the laptop ...

Peter Kleissner: Stoned Bootkit

The Stoned Bootkit is a rootkit that is booted before the main operating system has, and is able to stay and hide itself in memory during execution of the guest operating system. The payload is executed beside the running operating system and comes with the bootkit. Stoned is designed to be operating system independent, it is multiplatform. It currently supports all 32-bit and 64-bit Windows systems and Linux.

Infection vectors: USB stick, .exe, PDF exploit (!)

PCI DSS + karty ve španělsku

The **Payment Card Industry Data Security Standard** was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise.

Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack
KIM ZETTER: Wal-Mart was the victim of a serious security breach in 2005 and 2006.

Spain, 2009: Spanish police are investigating a credit card processing company which is believed to be at the centre of the scam. Germany: over 100 000 cards blocked (Volksbank, Raiffeisenbank) . Československá obchodní banka (ČSOB) na tuto hrozbu reagovala zablokováním karet vybraným klientům.

Sumedh Thakar, Terry Ramos: PCI Compliance for Dummies
ISBN 978-0-470-74452-9

IDN FUN I.

Internation Domain Names allows you to input internet addresses in your own language ....

www.žluťoučkýkůň.eu

www.xn--luoukk-fza0k2w9i6dqh.eu

...or to cover your ass

-

PAYPAL.COM
PAYPAL.COM
PAYPAL.COM
PAYPAL.COM

IDN FUN II.

-

PAYPAL.COM = xn--pal-5cd3fta.COM
PAYPAL.COM = PAYPAL.COM
PAYPAL.COM = xn--ypal-43d9g.COM
PAYPAL.COM = xn--pypal-4ve.COM
a co IP adresa: **CXLVII. CCXXVIII .I.X**

SSL Homograph attack

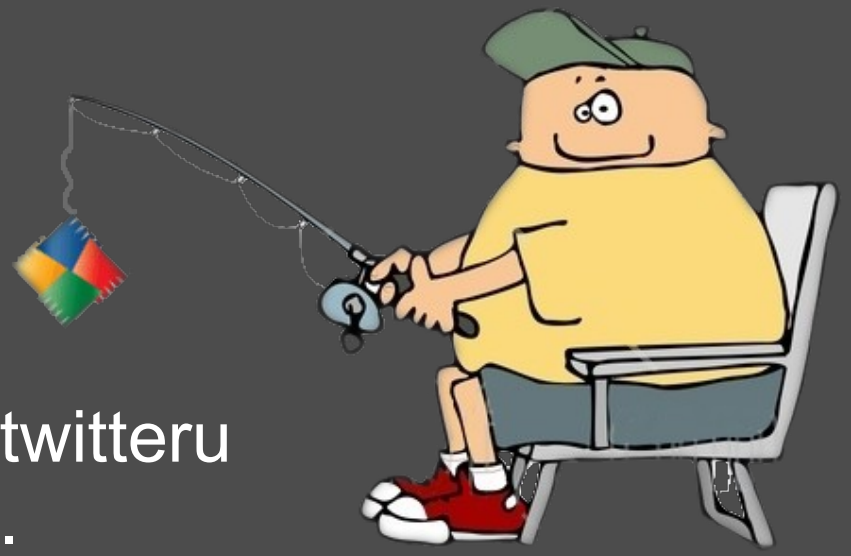
- don't strip https > replace it
- utf8 in x509 cn vs browser's address bar
- www.domena.cz?id=d2e3.. ...e132312ec.china.cn
- than you can offer perfectly valid *.china.cn certificate
- ie5 (win2k), mozilla 1.6 (linux)

Protocol	Info
DNS	Standard query A email\303\266\302\260domena_hrozne_dloupa.bodikovo.cz
DNS	Standard query A email\303\266\302\260domena_hrozne_dloupa.bodikovo.cz
DNS	Standard query A email\303\266\302\260domena_hrozne_dloupa.bodikovo.cz

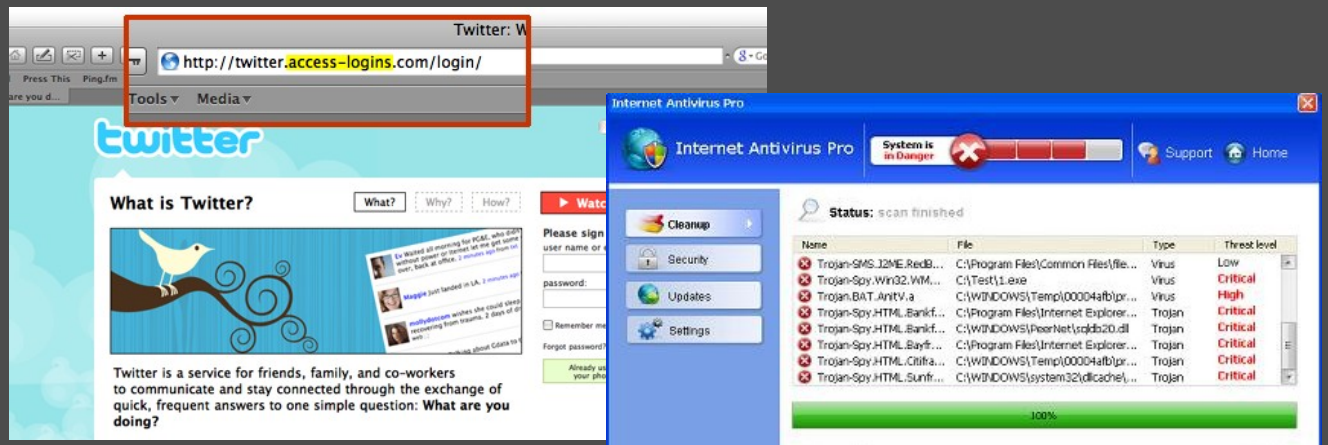
DNS	Standard query A xn--emaildomena_hrozne_dloupa-xg2a.bodikovo.cz
DNS	Standard query A xn--emaildomena_hrozne_dloupa-xg2a.bodikovo.cz
DNS	Standard query A xn--emaildomena_hrozne_dloupa-xg2a.bodikovo.cz.localdomain
DNS	Standard query A xn--emaildomena_hrozne_dloupa-xg2a.bodikovo.cz.localdomain

Flashes

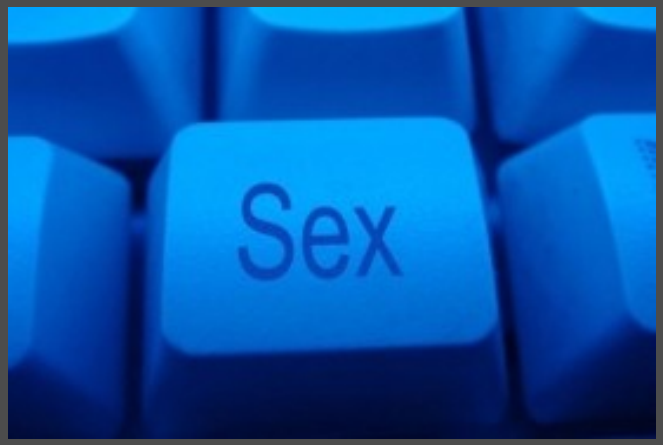
(Anti)Viry dnes obzvláště vypečené



- stále oblíbenější trik rhybářů
- v oběhu jich je až 7000
- rhybaří se takto i na facebooku a twitteru
- ... falešné multimediální kodeky ...



PČR a e-rotika ...



- **Listopad 2009**
- **Policie zasáhla proti skupině lidí, kteří si na internetu předávali dětské porno.**
- **Podezřelých je 160.**
- **V rámci akce policie udělala 150 domovních prohlídek, zajistila 342 počítačů a záznamových prostředků.**
- **Do akce bylo nasazeno 840 policistů.**

- **Novým trendem se stává dobíjení mobilu za fotky**

GhostNet

- 29. března 2009
- But just size of botnet does not matter
- GhostNet
  - Wen Ťia-pao snooping (not only) Dalai Lama
  - *embassies*: India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, Pakistan, Laos
  - *foreign ministries*: Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, Bhutan

Sport news

MS09-002

- prosinec 2008
  - ZDI reportuje MS chybu v IE7 (neveřejně)

- 10. února 2009
  - vydána záplata

- 17. února 2009
  - zachycen malware který chybu zneužíval (CN)

- reversování záplaty trvalo číňanům týden

Ze sportu DBJ DNS 5.březen 2009

DJBDNS tinydns (axfrdns) obsahovala nepravděpodobně zneužitelnou chybu, zahrnující třetí stranu (konfigurace, před kterou DJB varuje)

Ale stejně! DJB udělal chybu a zaplatil $1000!

Oprava:
- if (dlen <= 128)
+if ((dlen <= 128) && (response_len < 16384))

BC++ Awards 2009

The best DMS product 2009 goes to:

Synopsi nominee

http://www.csob.sk/LoadFile.aspx?fileId=582

3	application/pdf	2329627	Rocna_sprava_DSS_2004.pdf
4	None	0	None
5	application/pdf	174426	CB_193_DSS_vyrocka_web.pdf
6	application/pdf	129053	Polrocna_sprava_DSS_2005.pdf
7	application/pdf	613603	Rocna_sprava_DSS_2005.pdf
8	application/pdf	917759	Rocna_sprava_DSS_2006.pdf
9	application/pdf	173089	Polrocna_sprava_DSS_2006.pdf
10	application/pdf	2107176	Vyrocna_sprava_2006.pdf
11	application/pdf	190405	Polrocna_sprava_DSS_2007.pdf
12	application/pdf	31947	CB_12_list_zmluva.pdf
13	application/pdf	30280	ziadost.pdf
14	application/pdf	405970	Ziadost_o_vyplatenie_prostriedkov_poberatelom.pdf
15	application/pdf	30156	vop.pdf
16	application/pdf	28731	31_vypis.pdf
17	application/pdf	31398	30_prvy_vypis.pdf
18	application/pdf	21967	01_uz_aj_csob.pdf
19	application/pdf	26100	02_kolko_dostanem.pdf
20	application/pdf	20536	03_licencia.pdf
21	application/pdf	31044	04_sprostredkovatel.pdf

The best attack vector 2009 goes to:

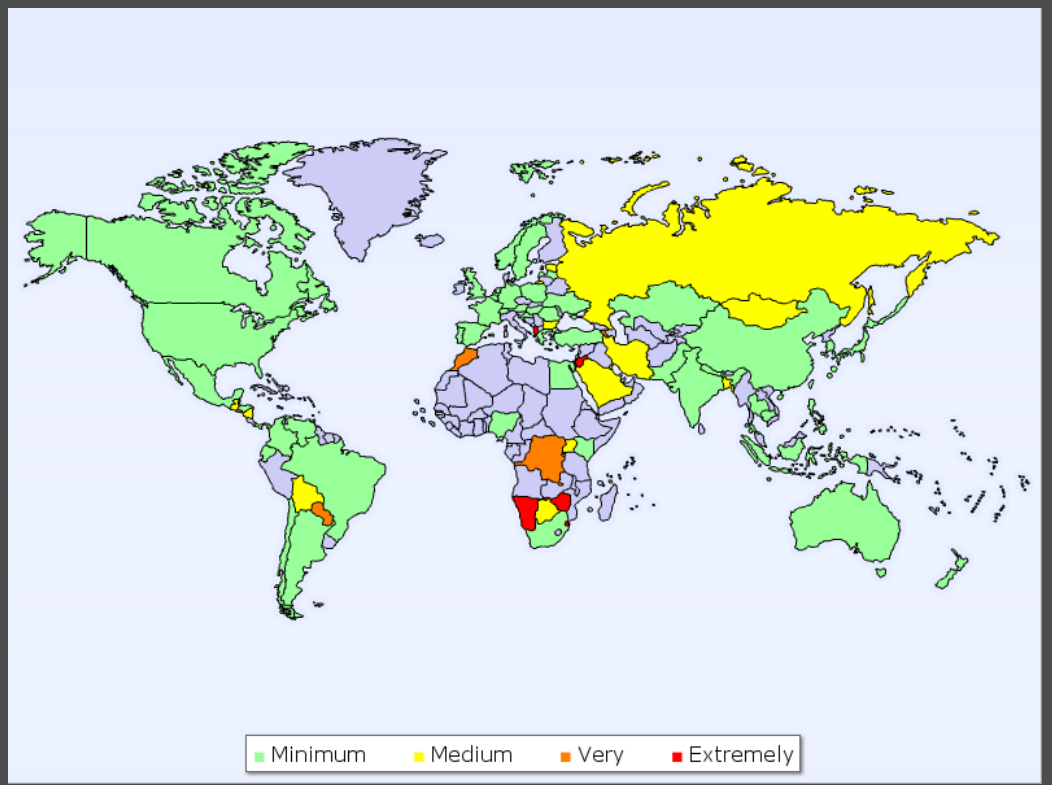
www.adobe.com

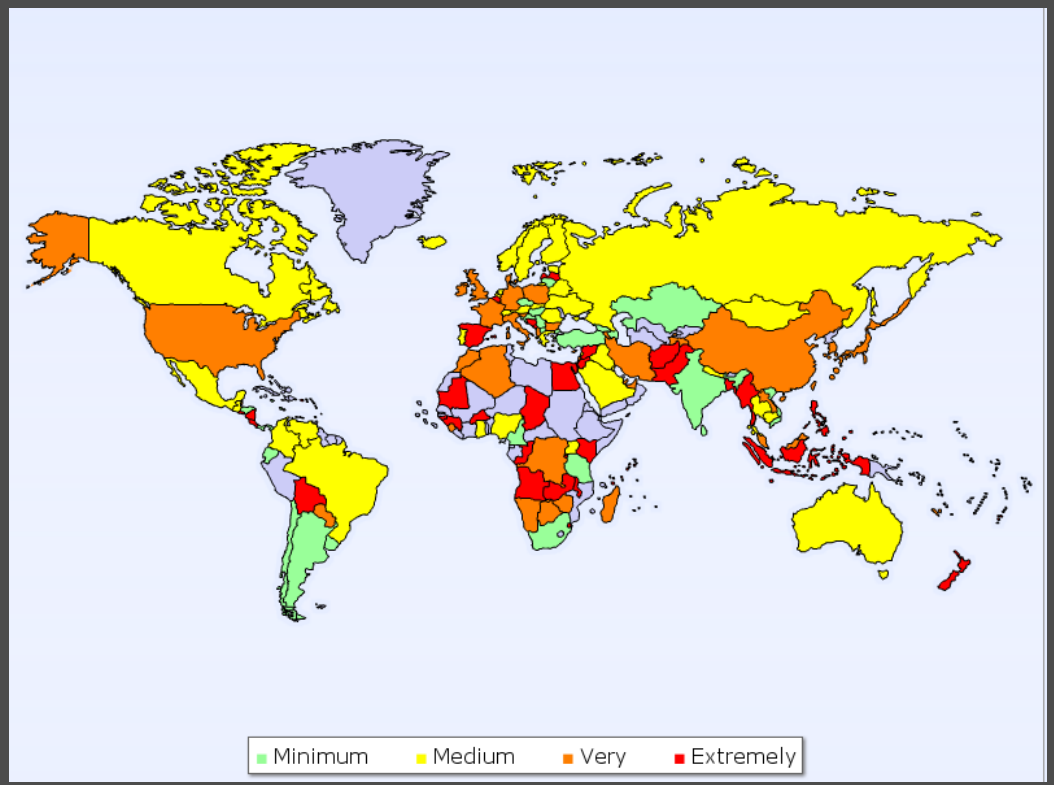
for rich internet/exploit aplications

JavaScript in PDF
and
Adobe Flash

Best BGP peer of 2009:

Single Czech provider announcing a single prefix caused a huge increase in the global rate of updates, peaking at 107,780 updates *per-second*. With AS path exceeding 255 ASNs. (normal: 4-5 ...)
3 x bug: Configuration typo & MikroTik bug, Cisco bug - CSCsx73770, Insufficient transit provider filtering
Core Internet: **ok**, but border/small ISP routers busted





The best innovation 2009 goes to:

www.microsoft.com

for inventing and patenting:

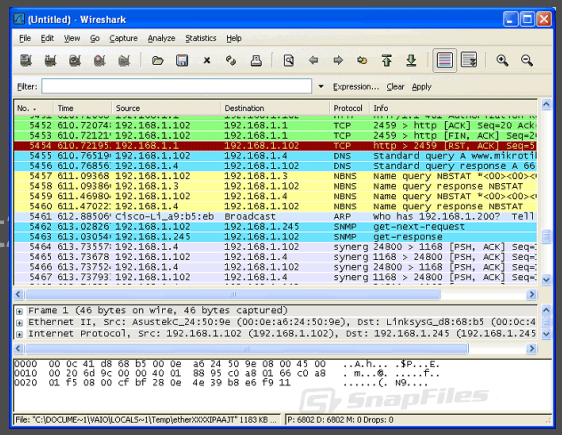
sudo

(known to IT SEC professionals since 1980)

A co na to jan tleskač ?

- DNS (2008) > x509/SSL (2009) > ??? (2010)
- A co Java ? Tak velká technologie a tak málo křiku ...
- Conficker
  - *Perhaps an even greater threat than what they have done so far, is what they have learned and what they will build next...*
    - wishmaster ?
    - Win32.Induc.A
      - Ken Thompson: Reflections on Trusting Trust
- Kde je IPv6 ?
- Kde je DNSSEC ?

.. stejně půjdem do basy ...



http://business.center.cz/business/pravo/zakony/trestni-zakonik/cast

§ 182 Porušení tajemství dopravovaných zpráv
(1) Kdo úmyslně poruší tajemství
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 ... vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu,

J XD na hrat

Weather in 2009

(29.11.2009 17:44 CET)	2009		2008
Sun Alerts http://blogs.sun.com/security/?cat=alerts&date=200811	216		173
Debian Security Advisories http://www.debian.org/security/2009/	246		235
Microsoft Security Bulletin http://www.microsoft.com/technet/security/current.aspx	68		69
Gentoo Linux Security Advisories http://www.gentoo.org/security/en/glsa/index.xml	151		191
FreeBSD Security Advisories http://www.freebsd.org/security/advisories.html http://www.vuxml.org/freebsd/	167		161
CVE Candidates http://cve.mitre.org/data/downloads/allcans.txt	4073		6432

The best hack of 2009 goes to:

www.fpr.zcu.cz

CTRL-A
CTRL-C
CTRL-V