“Ви повинні вивчити українську”

Вплив цифровий злочину зі Східної Європи в Латинській Америці

Fabio Assolini

Senior Security Researcher

Kaspersky Lab

Noviembre 2013

“Usted debe aprender Ucraniano”

La influencia del crimén digital de Europa del Leste en Latinoamérica

Fabio Assolini

Senior Security Researcher

Kaspersky Lab

Noviembre 2013

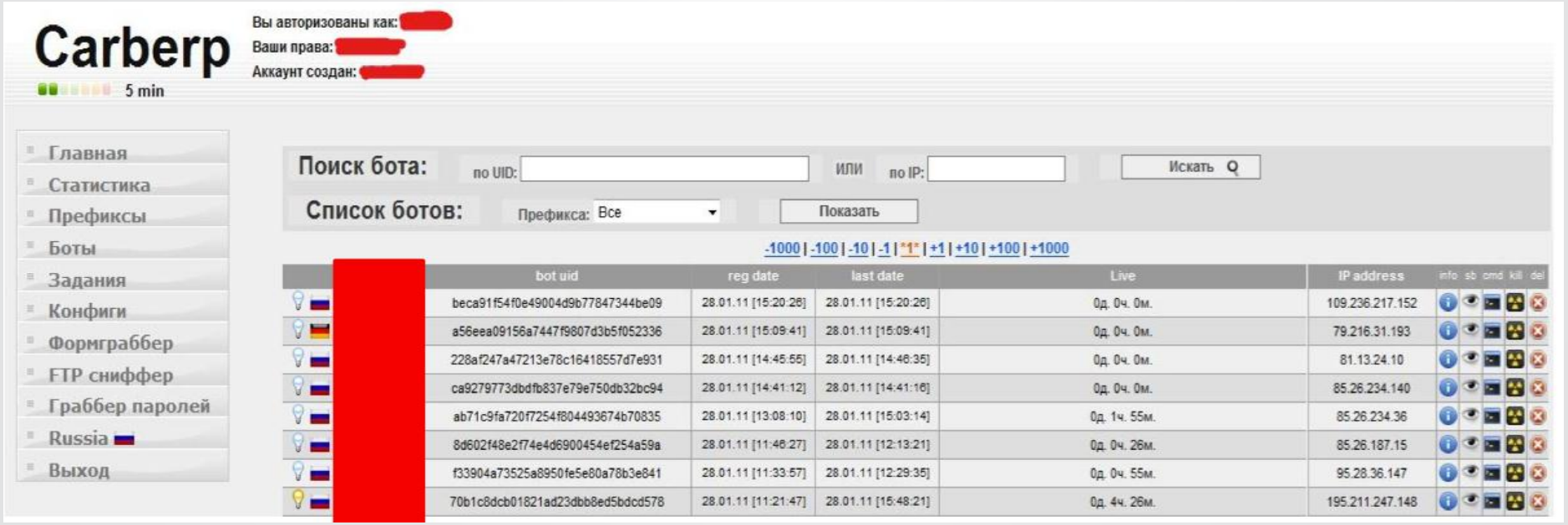
Los hijos de Zeus

el más avanzado troyano bancario

KASPERSKY lab

Europa del Este

- Región donde nació **Zeus, SpyEye, Carberp** y otros troyanos bancarios, usando las técnicas de Injection y otras realmente avanzadas.
- Para móviles: **ZitMo, SpitMo, CtiMo**, etc



Europa del Este y América Latina

- Ellos no solo atacan sino venden el **know how** para la región. Ya registramos ataques usando SpyeEye, Zeus y otros troyanos de origen de habla rusa en la región.
- Criminales latinoamericanos **no solo son simples clientes** de los criminales de Europa Oriental sino intercambian el conocimiento y las tecnicas de los ataques.
- Compran exploit kits (**BlackHole y otros**), código fuente de troyanos. **Si no pueden comprar, copian las ideas!**
- **Zeus y Carberp ahora son open source!**
- **Criminales de Europa Oriental ven Latinoamérica como una región de potencial en el futuro. Es fácil de atacar, pues hay impunidad.**

Como estamos hoy?

- Brasil, Perú y México en el liderazgo del desarrollo de los troyanos bancarios
- Evolución de troyanos sencillos, pharming (HOSTS) para troyanos más avanzados usando **inyección**, remedando al Zeus y SpyEye

```
add ecx, 00000004h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+000000A4h]
mov edx, 00405B10h ; "H[redacted]Colombia"
add ecx, 00000004h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+50h]
mov edx, 00405930h ; "https://www.h[redacted].com.co/"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+6Ch]
mov edx, 00405760h ; "www.h[redacted].com.co/h[redacted]"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+00000088h]
mov edx, 00405B44h ; "http://www.[redacted].php"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+000000A4h]
mov edx, 00405B94h ; "[redacted]net Colombia"
```

```
                        ; CODE XREF: CODE:004CE3EE↑j
cmp     byte ptr [ebx+3F3h], 1
jnz     short loc_4CE40D
cmp     byte ptr [ebx+3F4h], 1
jz      loc_4CE4A4

                        ; CODE XREF: CODE:004CE3FE↑j
mov     edx, offset aTextandoAsCo_0 ; "textando as coisas de hj"
mov     eax, [ebx+3D8h]
call    sub_447FF8
push    30h
```

KASPERSKY lab

SpyEye en Costa Rica

```
data_before
<body
data_end

data_inject
 onLoad="
```

```
665  // фрейм третий. страница ввода кода карт.
666  if (document.location.href.indexOf('https://www.personas.bancobcr.com/ib_
667  if (document.getElementsByTagName('body')[0].innerHTML.indexOf('Confirmar
668  {
```

socks5.dll.cfg | ftpbc.dll.cfg | ffcertgrabber.dll.cfg | customconnector.dll.cfg | collectors.txt

```
1  http://[redacted]ru/images/template.php;90
2  http://[redacted]ouldx.ru/images/template.php;90
3  http://[redacted]eaver.ru/music/chillout.php;90
4  http://[redacted]men.ru/siren/tears.php
```

Make config & get build

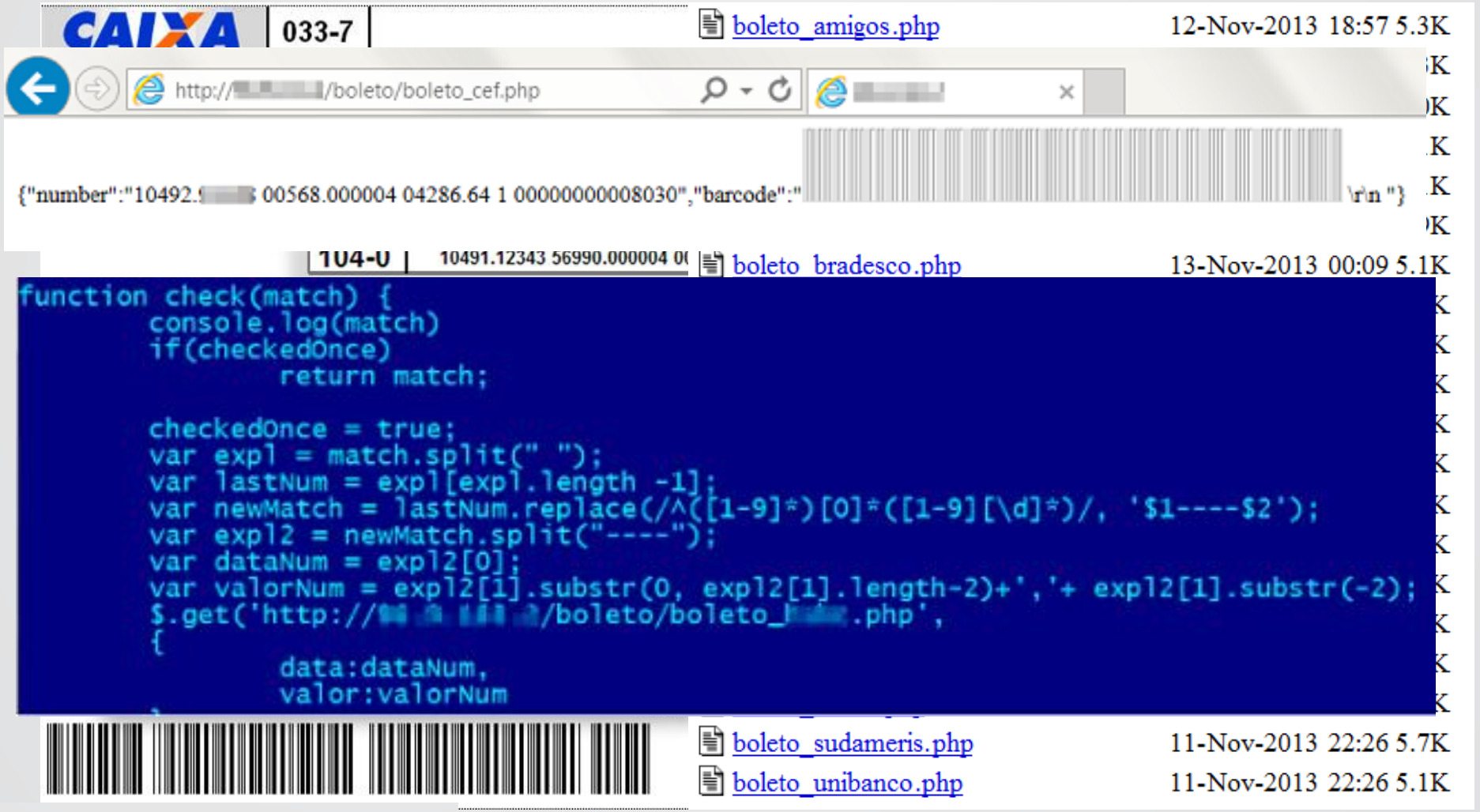
Are you infected by SpyEye?

KASPERSKY lab

Inyección de código: sitios web

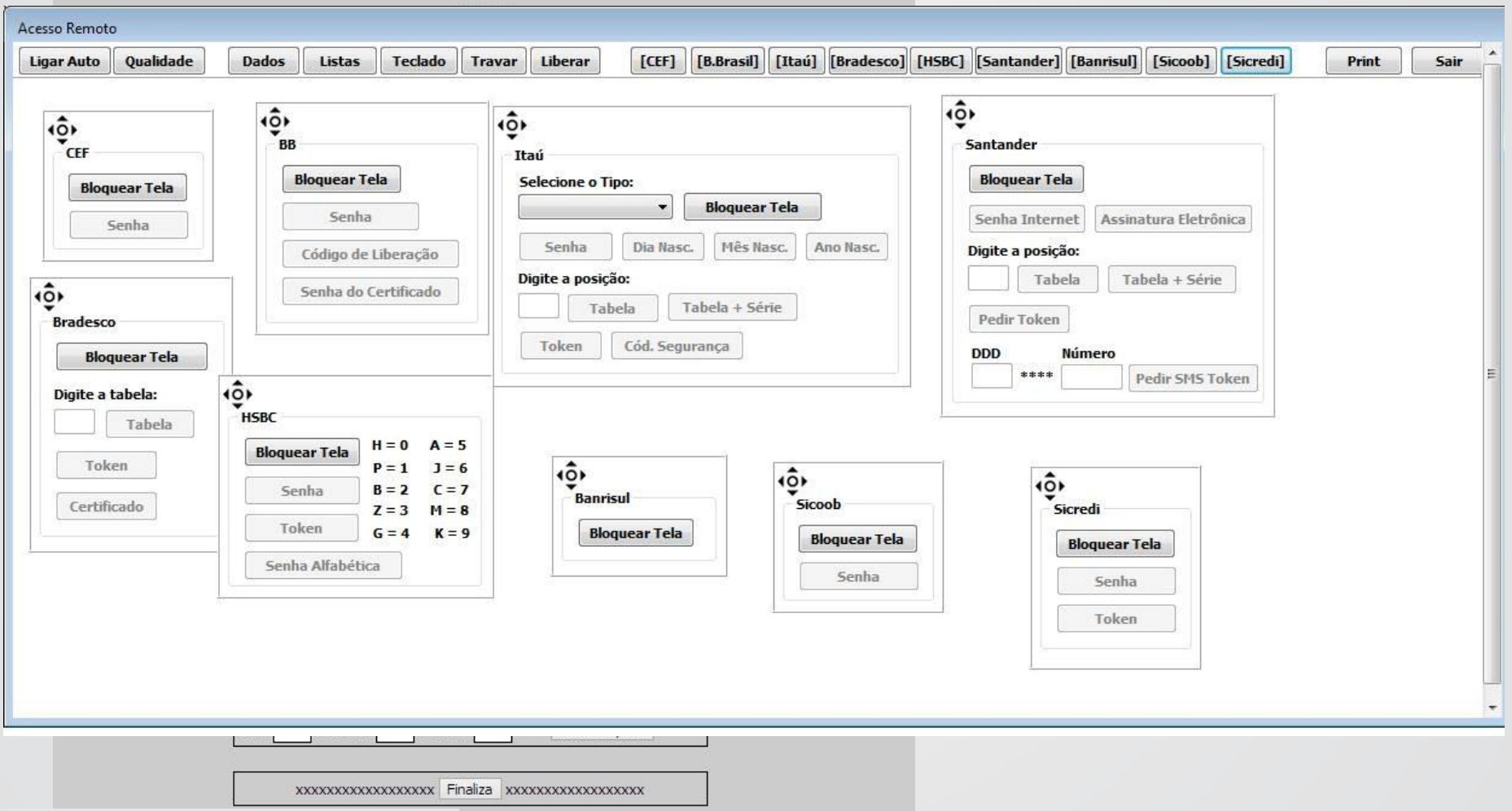
Inyección de código: boletos (Brasil)

- **Troyanos BHO y Extensiones maliciosas (Chrome)**



Inyección de código: auydan el MitM

- **Paneles de control para burlar soluciones OTP y tokens**



KASPERSKY lab

Crishi.a – troyanos bancarios con DGA

- **DGA: Domain Generation Algoritm**, Zeus lo usa mucho

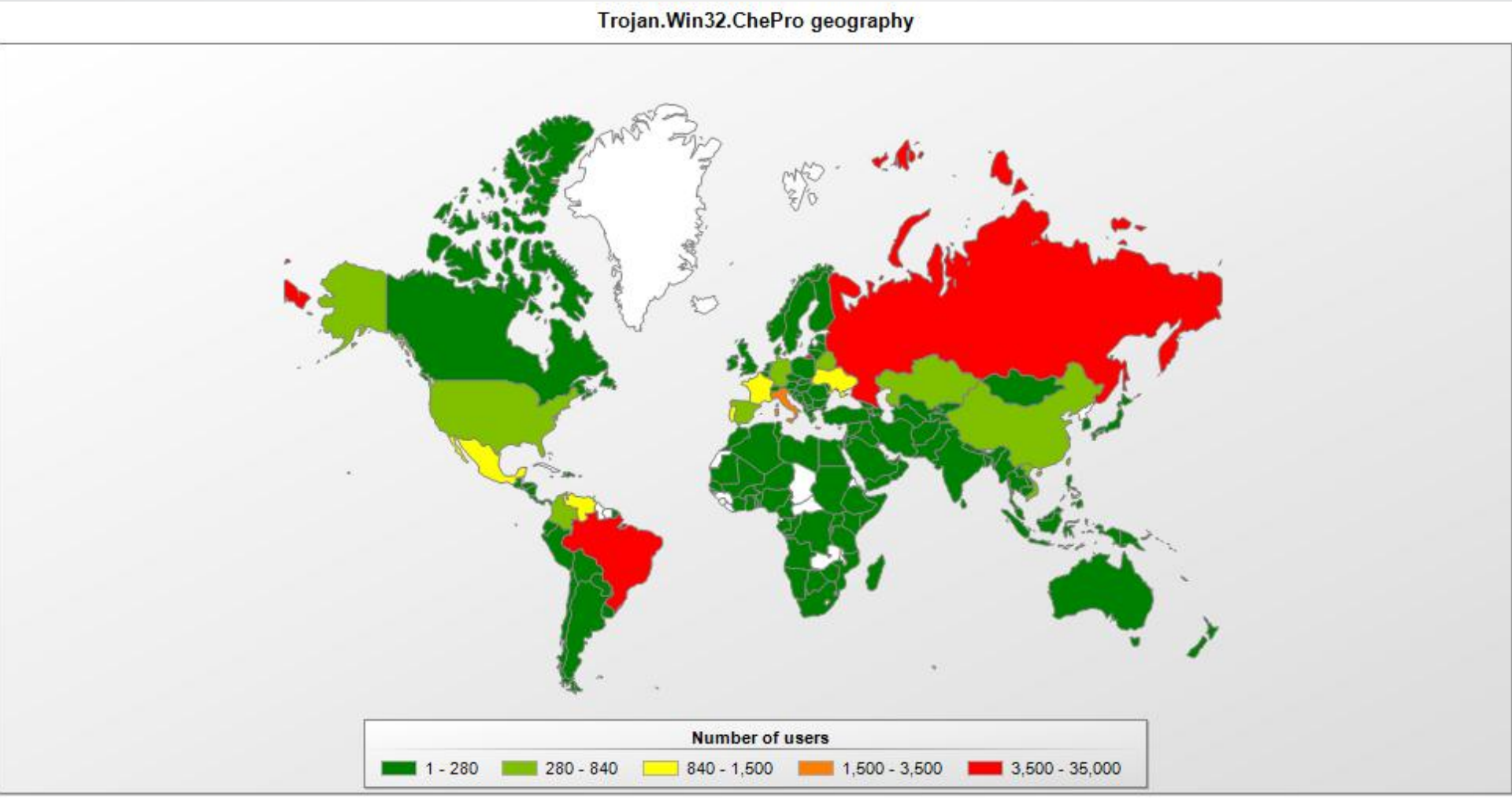

 ue em anexo o arquivo XML da sua nota fiscal eletrônica.
Chave da NF-e: 29110738742189740128374092893274409123417 28.xml
Número da NF-e: 180927340981
Série da NF-e: 892734
Data de emissão: 11/10/2011
Email: goldltda2011@gmail.com
Anexo (a): NF-e-180927340981-892734.zip <http://174.120.186.178/fec85685/notafiscal.pdf>

sqcgztgeinjbnflginlrsgiucp.biz
cavxcmvlyltcldpfxmnvtotw.com
dgebvgdmrgeaynfgcfcrikrjrgytwvrd
ztvgcgauozlfxdujvtfrvwwkmbbi.com
rkibxkgucqugghnhukzmlpfrgsiz.net
zxvolskdmxcgubmjfxkflemhm.biz
ljcuwkljpzguivlfpgqiguvgzxlm.info
bmcqhywtcgiawsaexmtnjbevo.com
pvlfoaulvcqkjqspnguifzpmfln.ru
topjlkzpxsugmntdazlyhzlgah.com
lrmrqtkromvytfatkgulbuomrtojb.biz
wdeifyojljzhsifgaprgfm.org
xzuszdwvsosodmnrtaelnytdy.net
fmjtoovxzhscfmkzdpfmvxclf.ru
mbbehevcrslceofhadehjbroskxcl.com
pblypusjricysypjmjvkhaaeiz.info
dtcdawoqyxeqtwprxkotifayws.org
mjlrtkbehaxgrojzxrcnbmfukfb.net
pzdmxcaidjzgmjvjrfyxhrzphv.biz
wjijojrodztqbaydroswhu.ru
cpswswjrypgqhmjfswqobmpvso.com
mrhpdulvhapblwgozortshmoncqfi.net
fihampaufuyizxdamrvsdfur.org
fucusibkvknwiviblzhuswnrr.biz
jnhlfinrztzdromjdmnpjbeqo.com
gitdueqozbarhmjbscwkbmlzvcjb.ru

 ue em anexo o arquivo XML da sua nota fiscal eletrônica.
Chave da NF-e: 29110738742189740128374092893274409123417 28.xml
Número da NF-e: 180927340981
Série da NF-e: 892734
Data de emissão: 11/10/2011
Email: goldltda2011@gmail.com
Anexo (a): NF-e-180927340981-892734.zip <http://174.120.186.178/fec85685/notafiscal.pdf>

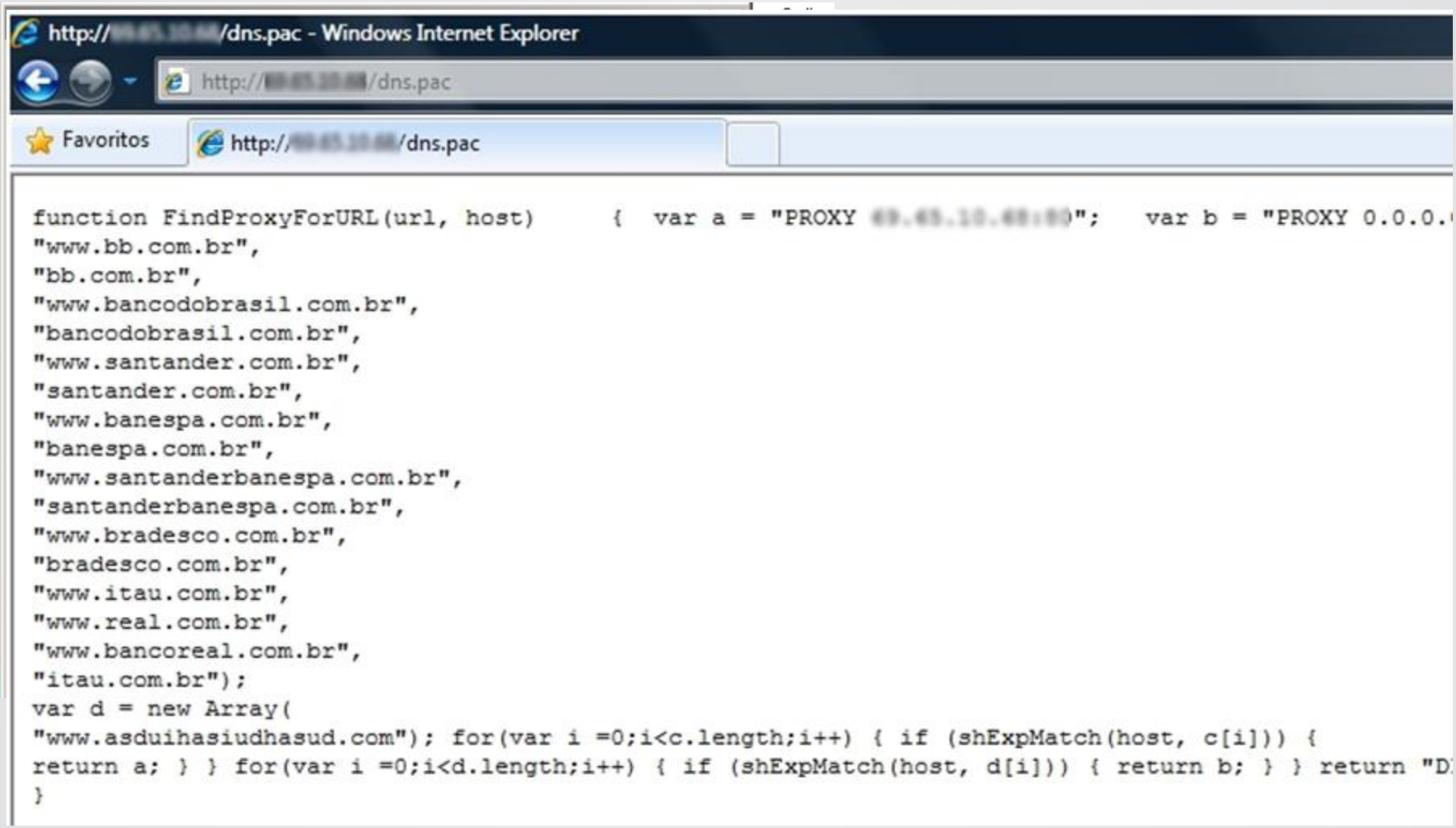
ChePro: del Zeus al Brasil, Mexico, Colombia

- **Archivos CPL en ZIP** alta ofuscación y paquetes diversos



KASPERSKY lab

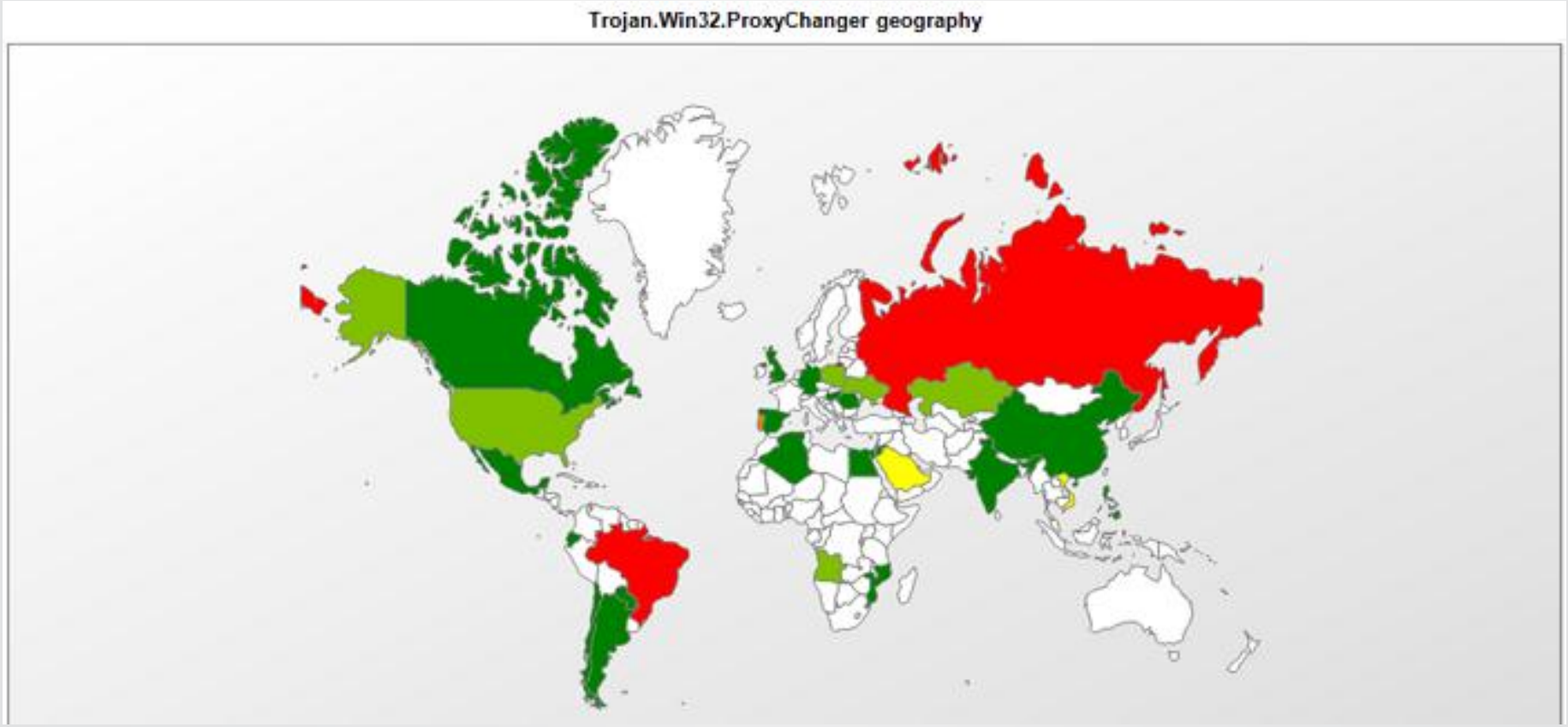
PAC malicioso en Brasil y Rusia



KASPERSKY lab

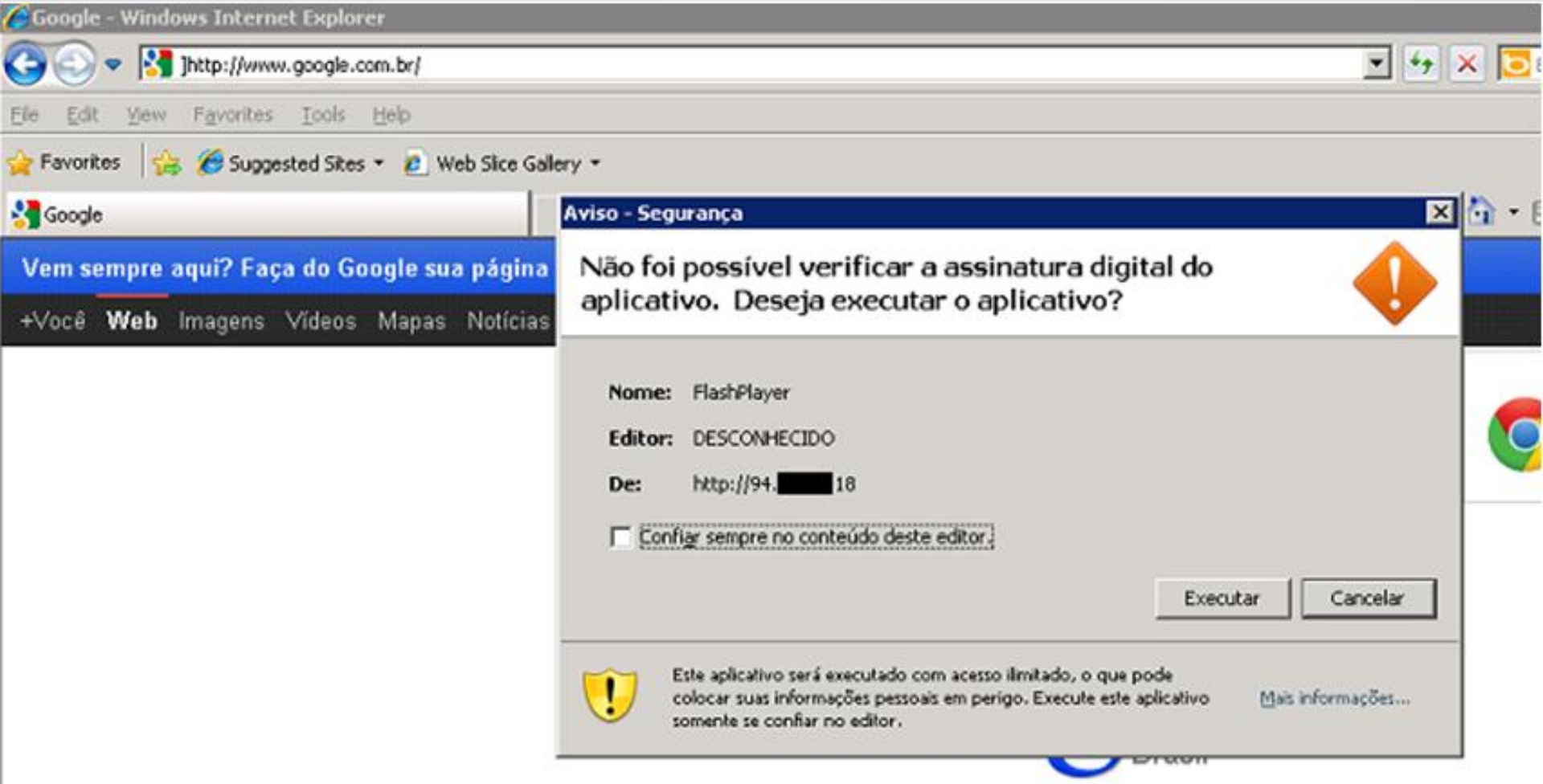
PAC malicioso en Brasil y Rusia

- Usados por los troyanos brasileños y por el troyano ruso Capper



Nuevas tendencias

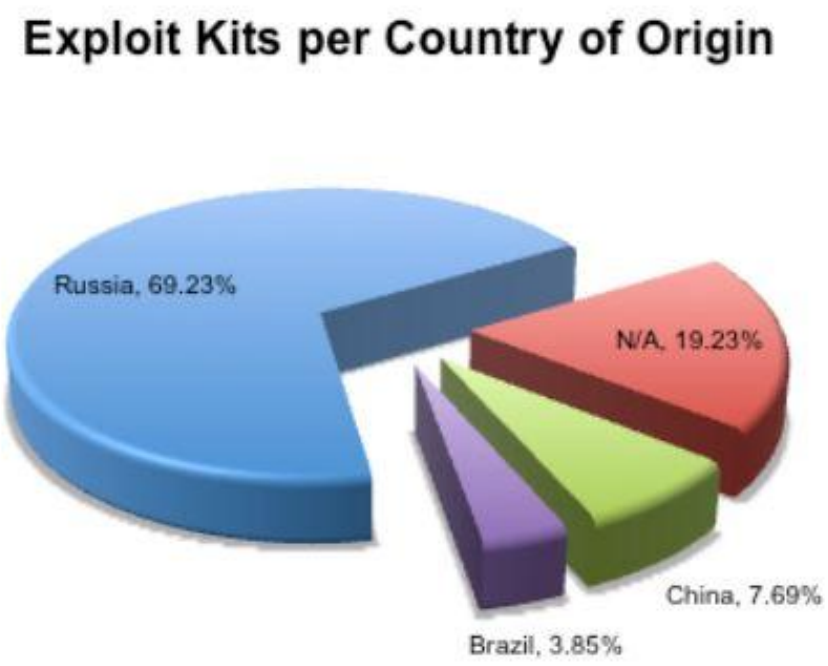
- Ataques sofisticados: Modems ADSL y dispositivos de red



Exploit Kits locales

la automatización de los ataques

¿Cuánto? ¿Dónde están?



2.500
dolares el paquete completo

50,00
renta diaria

hay paquetes gratis

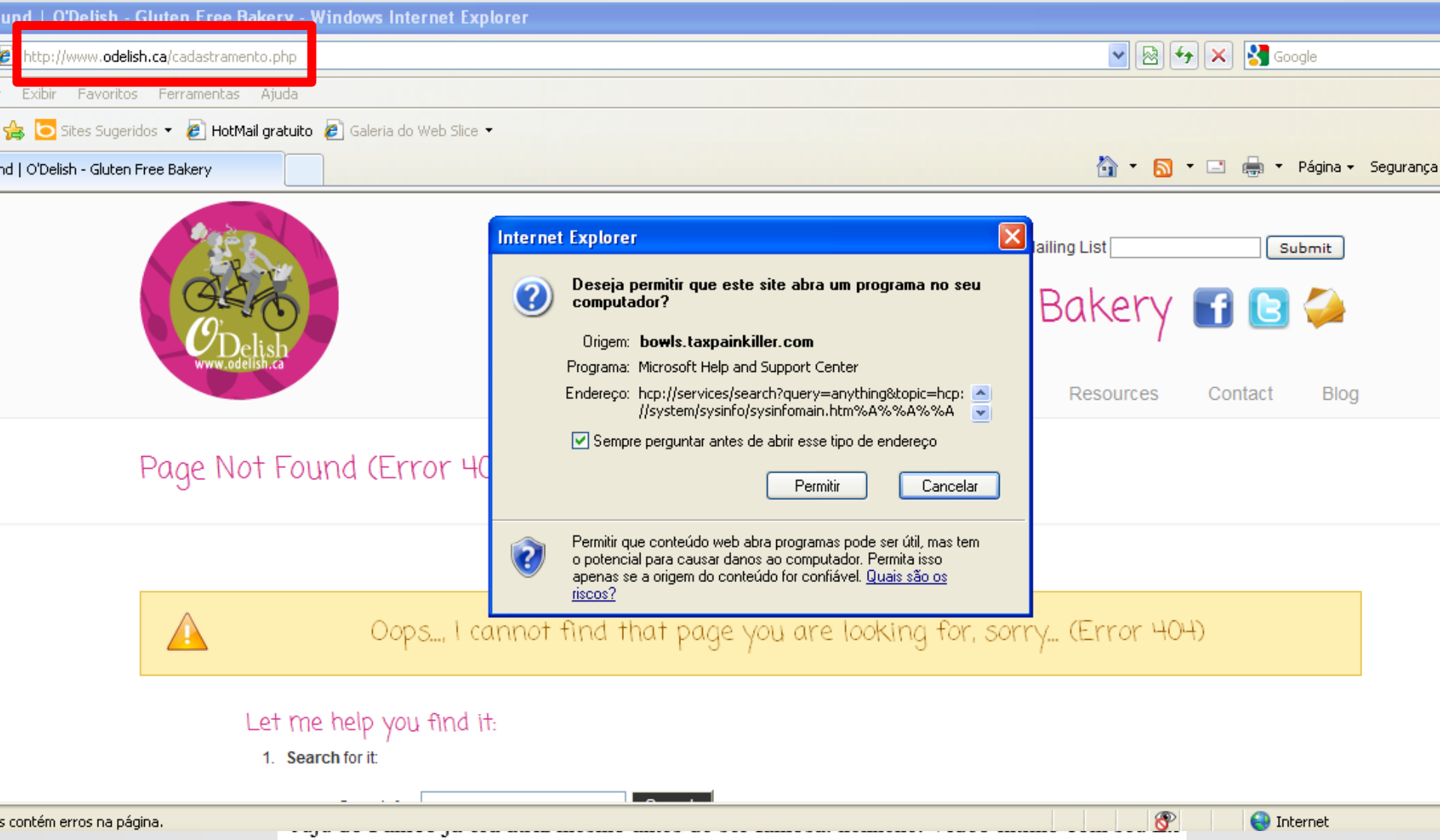
KASPERSKY lab

Java – el blanco preferido

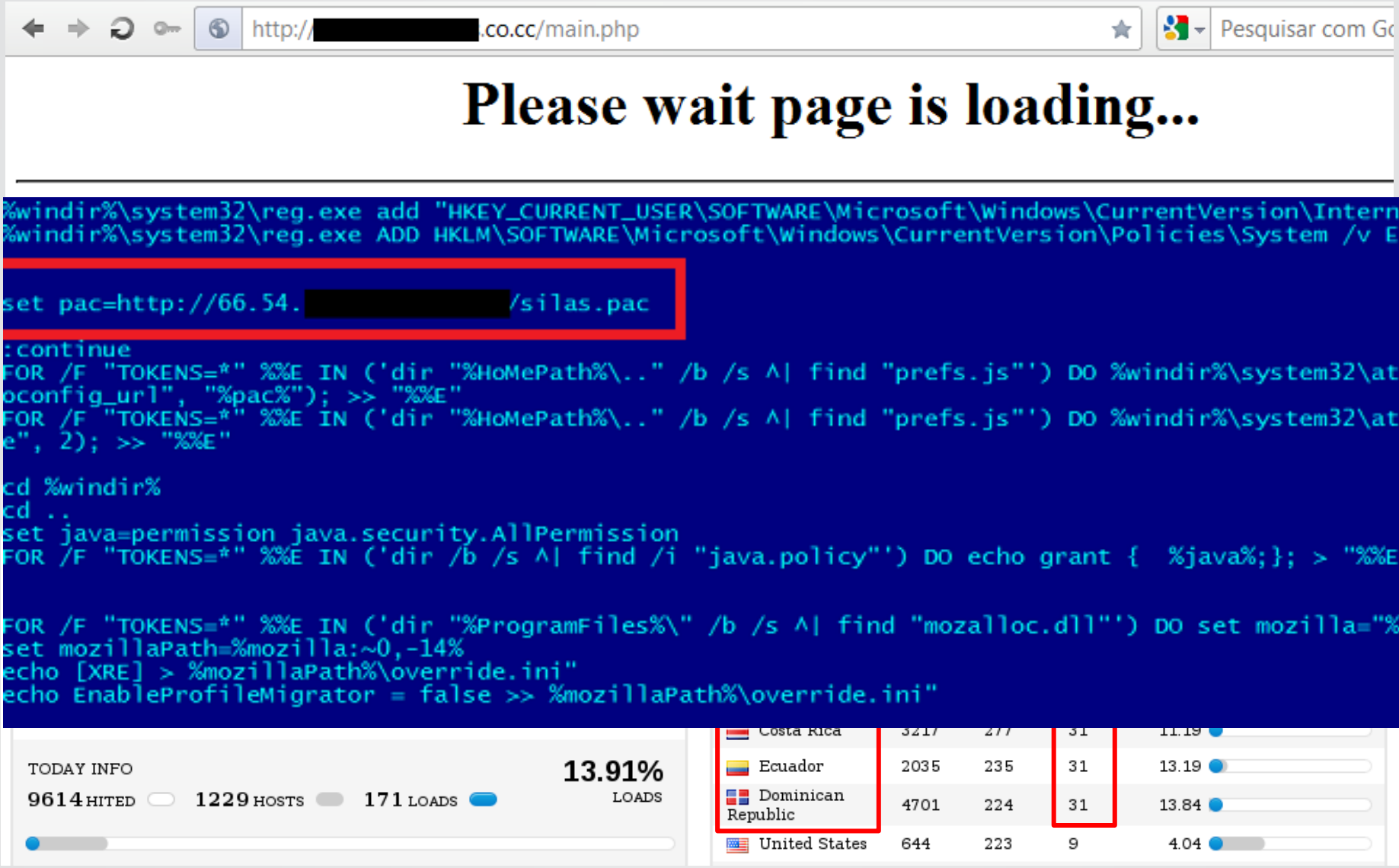
50%

ataques web en 2012

BlackHole

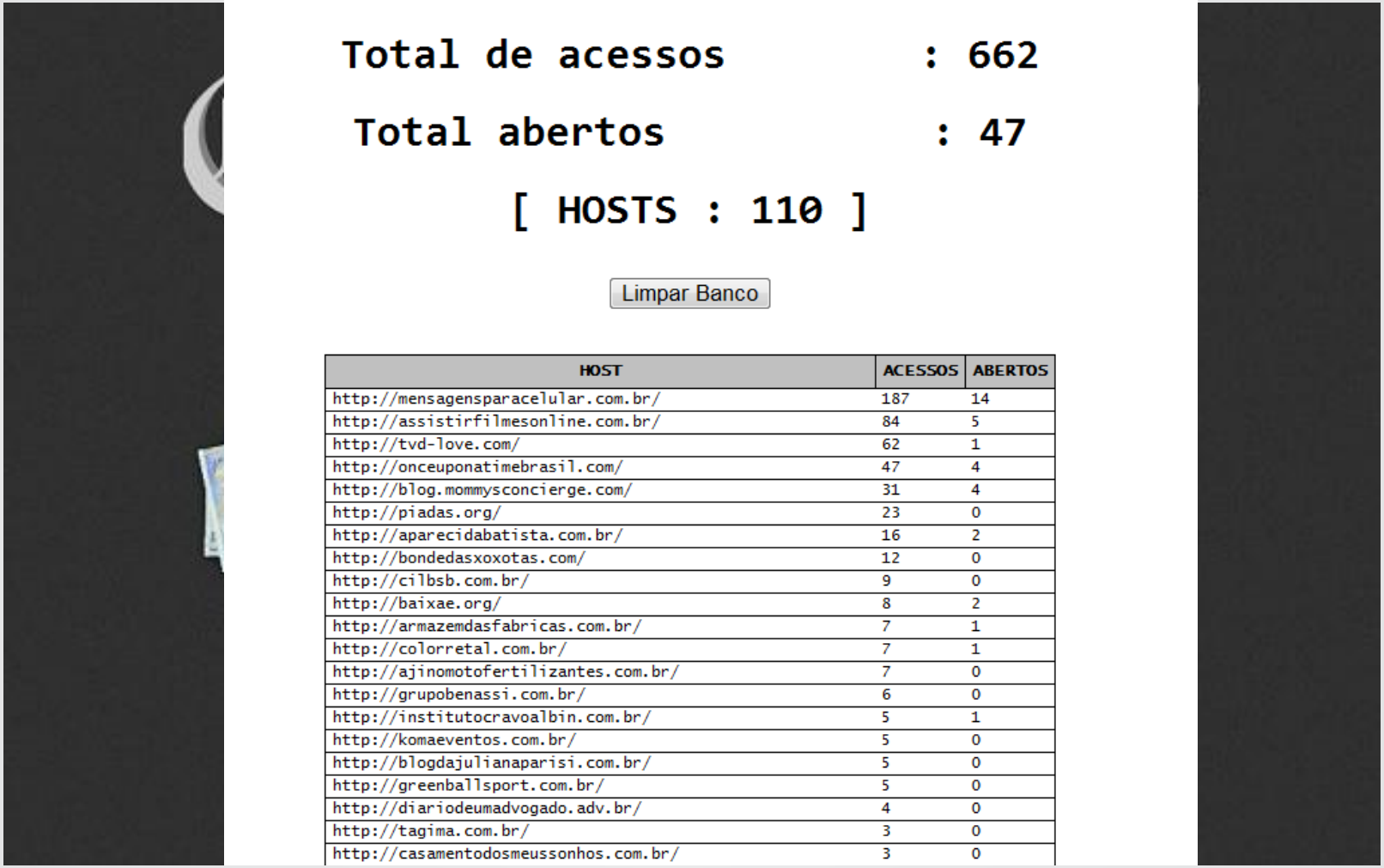

http://www.odelish.ca/cadastramento.php
Internet Explorer
Deseja permitir que este site abra um programa no seu computador?
Origem: bowls.taxpainkiller.com
Programa: Microsoft Help and Support Center
Endereço: hcp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.htm%A%%A%%A
Sempre perguntar antes de abrir esse tipo de endereço
Permitir
Cancelar
Permitir que conteúdo web abra programas pode ser útil, mas tem o potencial para causar danos ao computador. Permita isso apenas se a origem do conteúdo for confiável. Quais são os riscos?
Bakery
Resources
Contact
Blog
Page Not Found (Error 40
Oops... I cannot find that page you are looking for, sorry... (Error 404)
Let me help you find it:
1. Search for it:
Internet

BlackHole



KASPERSKY lab

Crimeboss



Total de acessos : 662

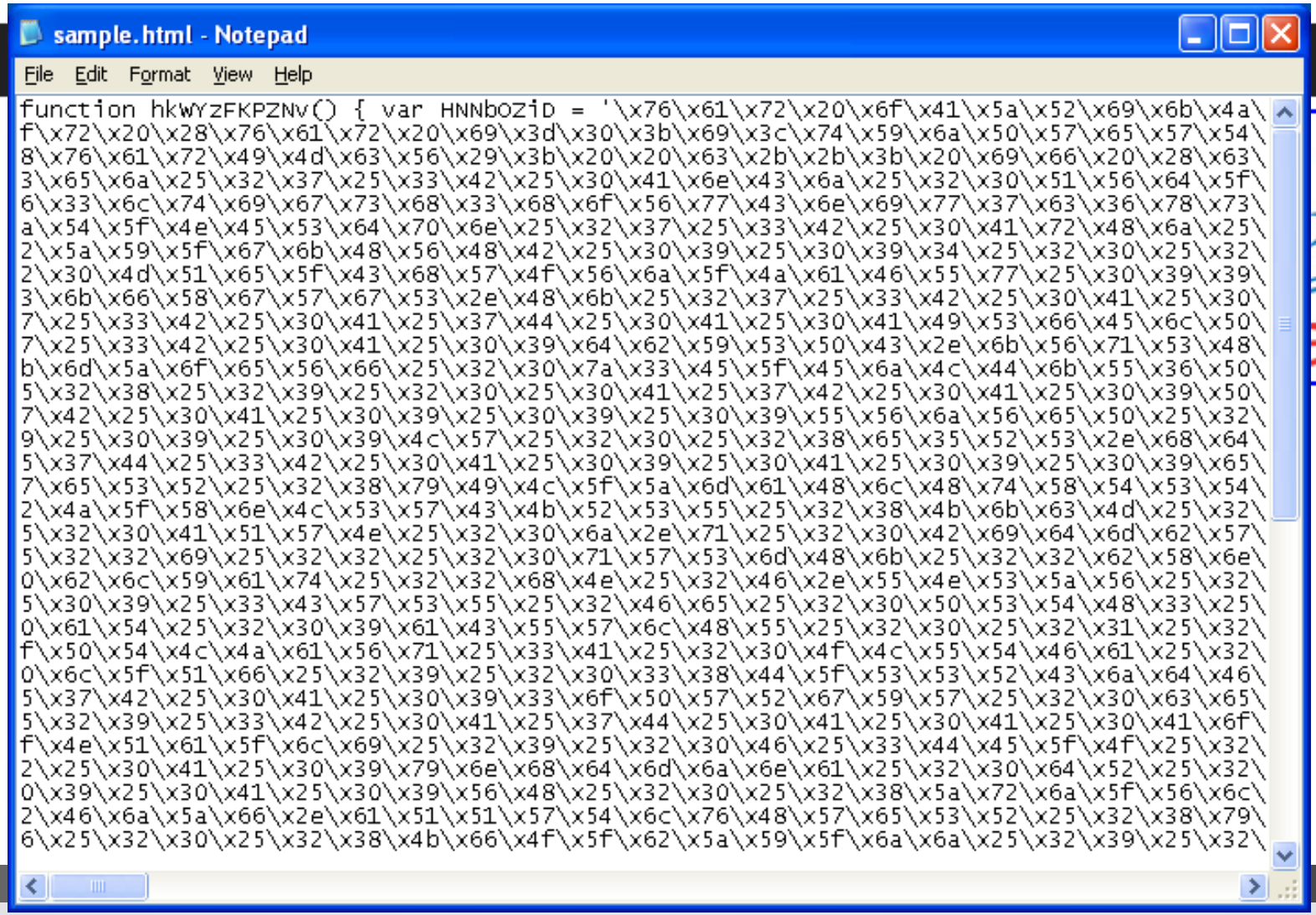
Total abertos : 47

[HOSTS : 110]

Limpar Banco

HOST	ACESSOS	ABERTOS
http://mensagensparacelular.com.br/	187	14
http://assistirfilmesonline.com.br/	84	5
http://tvd-love.com/	62	1
http://onceuponatimebrasil.com/	47	4
http://blog.mommysconcierge.com/	31	4
http://piadas.org/	23	0
http://aparecidabatista.com.br/	16	2
http://bondedasxoxotas.com/	12	0
http://cilbsb.com.br/	9	0
http://baixae.org/	8	2
http://armazemdasfabricas.com.br/	7	1
http://colorretal.com.br/	7	1
http://ajinomotofertilizantes.com.br/	7	0
http://grupobenassi.com.br/	6	0
http://institutocravoalbin.com.br/	5	1
http://komaeventos.com.br/	5	0
http://blogdajulianaparisi.com.br/	5	0
http://greenballsport.com.br/	5	0
http://diariodeumadvogado.adv.br/	4	0
http://tagima.com.br/	3	0
http://casamentodosmeussonhos.com.br/	3	0

Crimeboss


Atenção
sample.html - Notepad
File Edit Format View Help
function hkWYzFKPZNv() { var HNNbOZiD = '\x76\x61\x72\x20\x6f\x41\x5a\x52\x69\x6b\x4a\
f\x72\x20\x28\x76\x61\x72\x20\x69\x3d\x30\x3b\x69\x3c\x74\x59\x6a\x50\x57\x65\x57\x54\
8\x76\x61\x72\x49\x4d\x63\x56\x29\x3b\x20\x20\x63\x2b\x2b\x3b\x20\x69\x66\x20\x28\x63\
3\x65\x6a\x25\x32\x37\x25\x33\x42\x25\x30\x41\x6e\x43\x6a\x25\x32\x30\x51\x56\x64\x5f\
6\x33\x6c\x74\x69\x67\x73\x68\x33\x68\x6f\x56\x77\x43\x6e\x69\x77\x37\x63\x36\x78\x73\
a\x54\x5f\x4e\x45\x53\x64\x70\x6e\x25\x32\x37\x25\x33\x42\x25\x30\x41\x72\x48\x6a\x25\
2\x5a\x59\x5f\x67\x6b\x48\x56\x48\x42\x25\x30\x39\x25\x30\x39\x34\x25\x32\x30\x25\x32\
2\x30\x4d\x51\x65\x5f\x43\x68\x57\x4f\x56\x6a\x5f\x4a\x61\x46\x55\x77\x25\x30\x39\x39\
3\x6b\x66\x58\x67\x57\x67\x53\x2e\x48\x6b\x25\x32\x37\x25\x33\x42\x25\x30\x41\x25\x30\
7\x25\x33\x42\x25\x30\x41\x25\x37\x44\x25\x30\x41\x25\x30\x41\x49\x53\x66\x45\x6c\x50\
7\x25\x33\x42\x25\x30\x41\x25\x30\x39\x64\x62\x59\x53\x50\x43\x2e\x6b\x56\x71\x53\x48\
b\x6d\x5a\x6f\x65\x56\x66\x25\x32\x30\x7a\x33\x45\x5f\x45\x6a\x4c\x44\x6b\x55\x36\x50\
5\x32\x38\x25\x32\x39\x25\x32\x30\x25\x30\x41\x25\x37\x42\x25\x30\x41\x25\x30\x39\x50\
7\x42\x25\x30\x41\x25\x30\x39\x25\x30\x39\x25\x30\x39\x55\x56\x6a\x56\x65\x50\x25\x32\
9\x25\x30\x39\x25\x30\x39\x4c\x57\x25\x32\x30\x25\x32\x38\x65\x35\x52\x53\x2e\x68\x64\
5\x37\x44\x25\x33\x42\x25\x30\x41\x25\x30\x39\x25\x30\x41\x25\x30\x39\x25\x30\x39\x65\
7\x65\x53\x52\x25\x32\x38\x79\x49\x4c\x5f\x5a\x6d\x61\x48\x6c\x48\x74\x58\x54\x53\x54\
2\x4a\x5f\x58\x6e\x4c\x53\x57\x43\x4b\x52\x53\x55\x25\x32\x38\x4b\x6b\x63\x4d\x25\x32\
5\x32\x30\x41\x51\x57\x4e\x25\x32\x30\x6a\x2e\x71\x25\x32\x30\x42\x69\x64\x6d\x62\x57\
5\x32\x32\x69\x25\x32\x32\x25\x32\x30\x71\x57\x53\x6d\x48\x6b\x25\x32\x32\x62\x58\x6e\
0\x62\x6c\x59\x61\x74\x25\x32\x32\x68\x4e\x25\x32\x46\x2e\x55\x4e\x53\x5a\x56\x25\x32\
5\x30\x39\x25\x33\x43\x57\x53\x55\x25\x32\x46\x65\x25\x32\x30\x50\x53\x54\x48\x33\x25\
0\x61\x54\x25\x32\x30\x39\x61\x43\x55\x57\x6c\x48\x55\x25\x32\x30\x25\x32\x31\x25\x32\
f\x50\x54\x4c\x4a\x61\x56\x71\x25\x33\x41\x25\x32\x30\x4f\x4c\x55\x54\x46\x61\x25\x32\
0\x6c\x5f\x51\x66\x25\x32\x39\x25\x32\x30\x33\x38\x44\x5f\x53\x53\x52\x43\x6a\x64\x46\
5\x37\x42\x25\x30\x41\x25\x30\x39\x33\x6f\x50\x57\x52\x67\x59\x57\x25\x32\x30\x63\x65\
5\x32\x39\x25\x33\x42\x25\x30\x41\x25\x37\x44\x25\x30\x41\x25\x30\x41\x25\x30\x41\x6f\
f\x4e\x51\x61\x5f\x6c\x69\x25\x32\x39\x25\x32\x30\x46\x25\x33\x44\x45\x5f\x4f\x25\x32\
2\x25\x30\x41\x25\x30\x39\x79\x6e\x68\x64\x6d\x6a\x6e\x61\x25\x32\x30\x64\x52\x25\x32\
0\x39\x25\x30\x41\x25\x30\x39\x56\x48\x25\x32\x30\x25\x32\x38\x5a\x72\x6a\x5f\x56\x6c\
2\x46\x6a\x5a\x66\x2e\x61\x51\x51\x57\x54\x6c\x76\x48\x57\x65\x53\x52\x25\x32\x38\x79\
6\x25\x32\x30\x25\x32\x38\x4b\x66\x4f\x5f\x62\x5a\x59\x5f\x6a\x6a\x25\x32\x39\x25\x32\

ideas europeas negocios latinos

diversidad en los negocios criminales

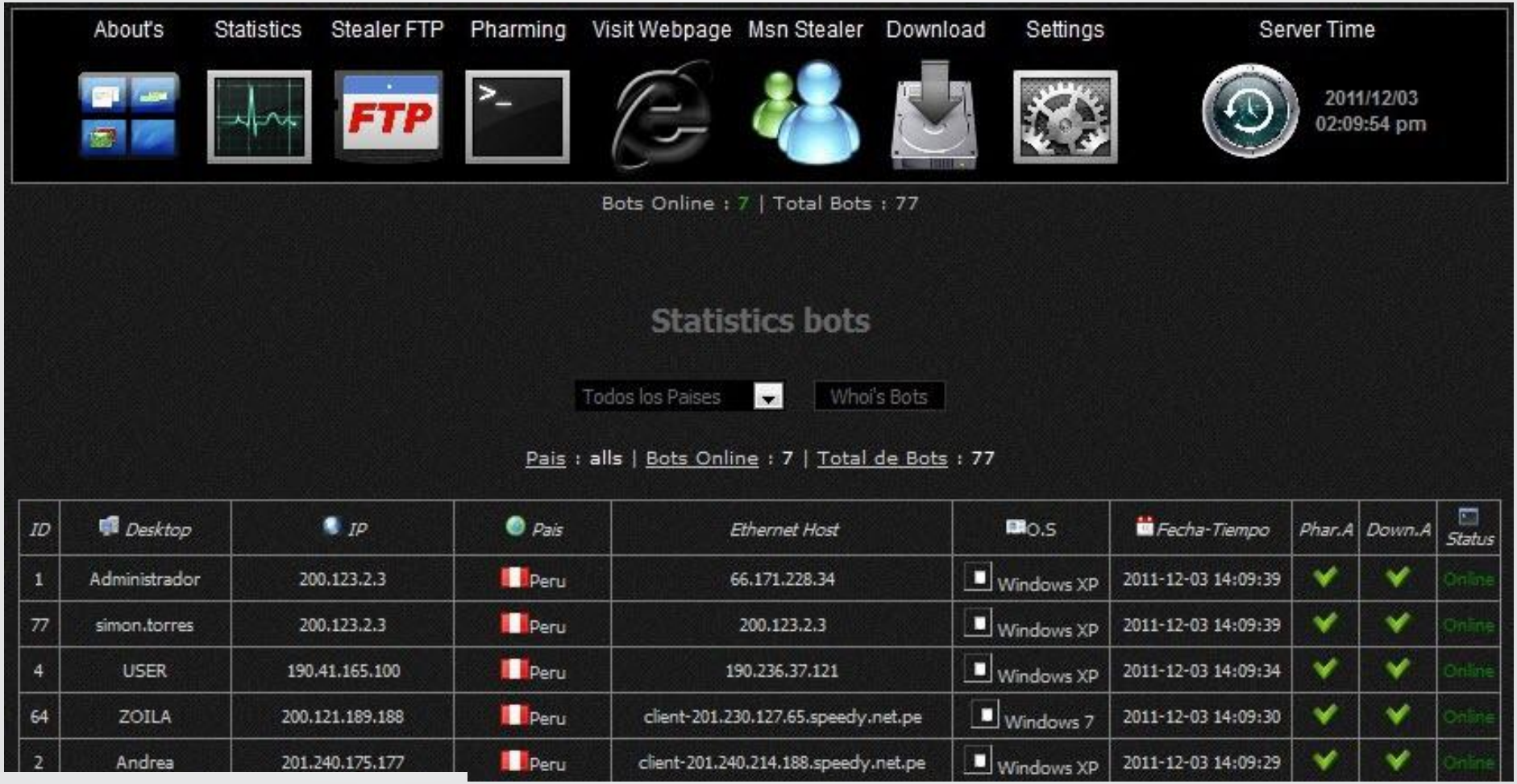
KASPERSKY lab

Venta de Crimeware local

- Desarrollo de crimeware local; costo **140 dólares**, vendido por criminales de Perú para toda América Latina

Venta de Crimeware local

- vOlk Botnet: Crimeware Mexicano usado en DDoS y robo a la banca



ID	Desktop	IP	Pais	Ethernet Host	O.S	Fecha-Tiempo	Phar.A	Down.A	Status
1	Administrador	200.123.2.3	Peru	66.171.228.34	Windows XP	2011-12-03 14:09:39	✔	✔	Online
77	simon.torres	200.123.2.3	Peru	200.123.2.3	Windows XP	2011-12-03 14:09:39	✔	✔	Online
4	USER	190.41.165.100	Peru	190.236.37.121	Windows XP	2011-12-03 14:09:34	✔	✔	Online
64	ZOILA	200.121.189.188	Peru	client-201.230.127.65.speedy.net.pe	Windows 7	2011-12-03 14:09:30	✔	✔	Online
2	Andrea	201.240.175.177	Peru	client-201.240.214.188.speedy.net.pe	Windows XP	2011-12-03 14:09:29	✔	✔	Online

Venta de Servicios de DDoS

- Versión brasileña del **Trojan.Java.Jacksbot** usado en ataques DDoS

New Multiplatform Backdoor Jacksbot Discovered

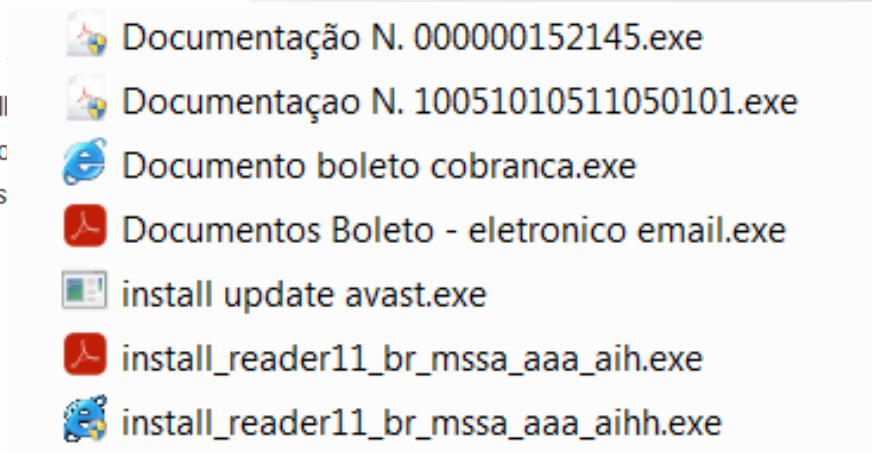
Posted on October 12th, 2012 by Lysa Myers

Update – October 15, 2012

Upon further analysis, it's been determined that this trojan is the Java RAT (aka jRAT) created by the hacker/programmer redpois0n.

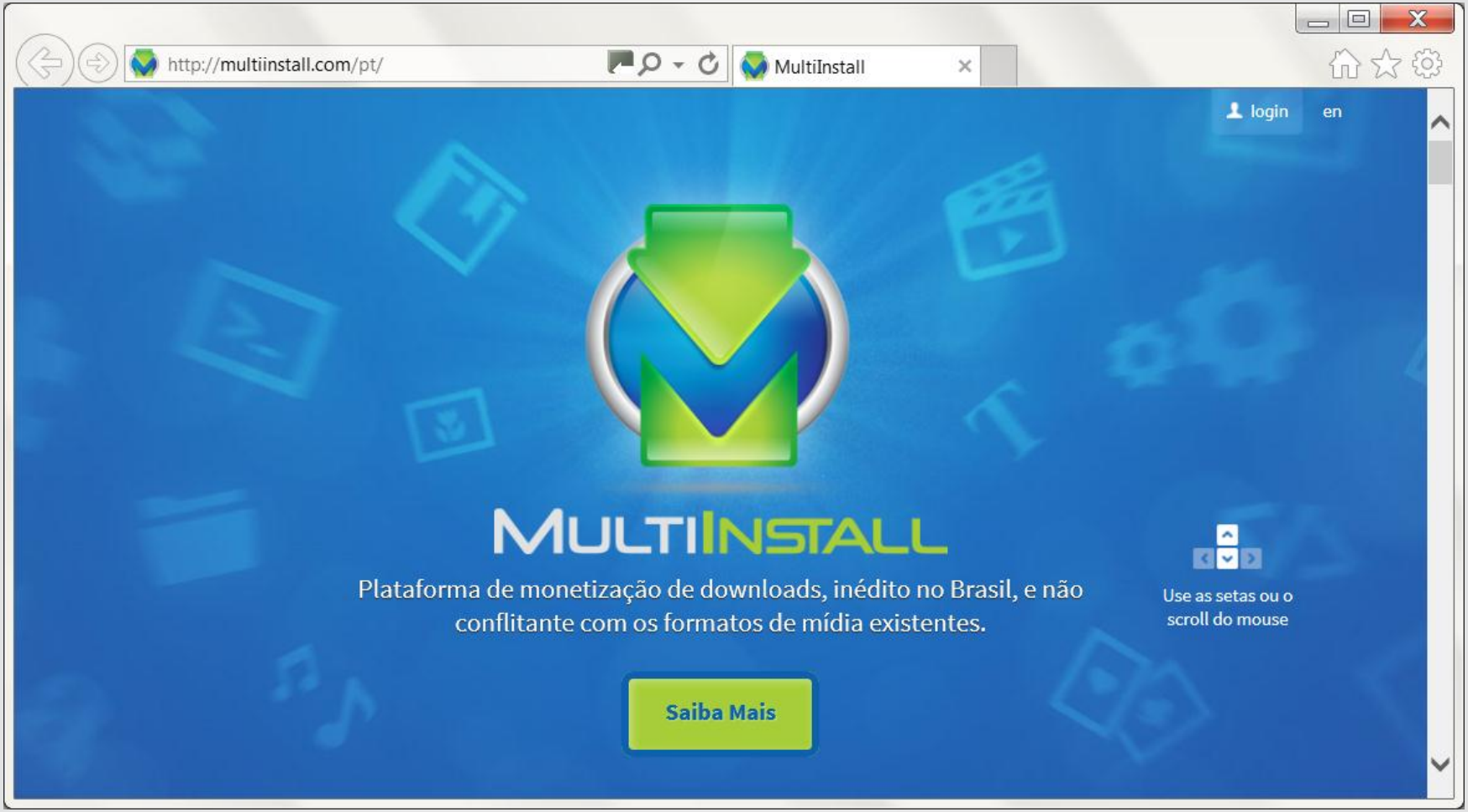
A new Java backdoor trojan called Java/Jacksbot.A has been discovered partial multiplatform support. It is fully functional on Windows, and partiall OS X and Linux. This trojan is currently considered low risk as it is not knc infected users, and it does not run without root permissions. Jacksbot has backdoor functionality, including the following capabilities:

- gathering system information
- taking screenshots
- performing denial of service attacks
- deleting files
- stealing passwords (including specifically Minecraft passwords)
- visiting remote URLs, likely to perform Clickfraud



Partnerka: sistema de afiliados

- Usado en la distribuicion de adware – también puede ser usado para malware



Ojos locales inteligencia global

¿Qué hace Kaspersky?

KASPERSKY lab

Ojo local, inteligencia global

250.000

Nuevas muestras de Malware diario

350.000

Exploits bloqueados todos los días

2.3 **nuevas amenazas por minuto**

KASPERSKY lab

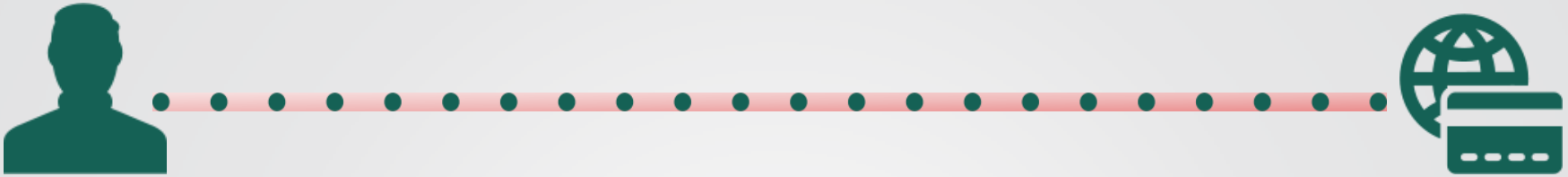
Ojo local, inteligencia global

780

nuevos troyanos bancarios se detectan todos los días

KASPERSKY lab

Banca en Línea insegura



Sitio

- ✓ Phishing

Conección

- ✓ DNS Changer
- ✓ Proxy malicioso (PAC)
- ✓ Archivo HOSTS
- ✓ Modem ADSL
- ✓ DNS poisoning

Ambiente

- ✓ Explotación de Vulnerabilidades (Java)
- ✓ Inyección de Codigo
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

KASPERSKY lab

Banca en Línea Segura

Sitio

- ✓ Anti-Phishing
- ✓ Sitios confiables
- ✓ Enlace Seguro

Conección

- ✓ DNS Changer
- ✓ Proxy malicioso (PAC)
- ✓ Archivo HOSTS
- ✓ Modem ADSL
- ✓ DNS poisoning

Ambiente

- ✓ Explotación de Vulnerabilidades (Java)
- ✓ Inyección de Codigo
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

KASPERSKY lab

Banca en Línea Segura

Site

- ✓ Anti-Phishing
- ✓ Sitios confiables
- ✓ Enlace Seguro

Conección

- ✓ Kaspersky Security Network
- ✓ Base de datos de SSLs en la nube

Ambiente

- ✓ Explotación de Vulnerabilidades (Java)
- ✓ Inyección de Codigo
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

KASPERSKY lab

Banca en Línea Segura

Site

- ✓ Anti-Phishing
- ✓ Sitios confiables
- ✓ Enlace Seguro

Conección

- ✓ Kaspersky Security Network
- ✓ Base de datos de SSLs en la nube

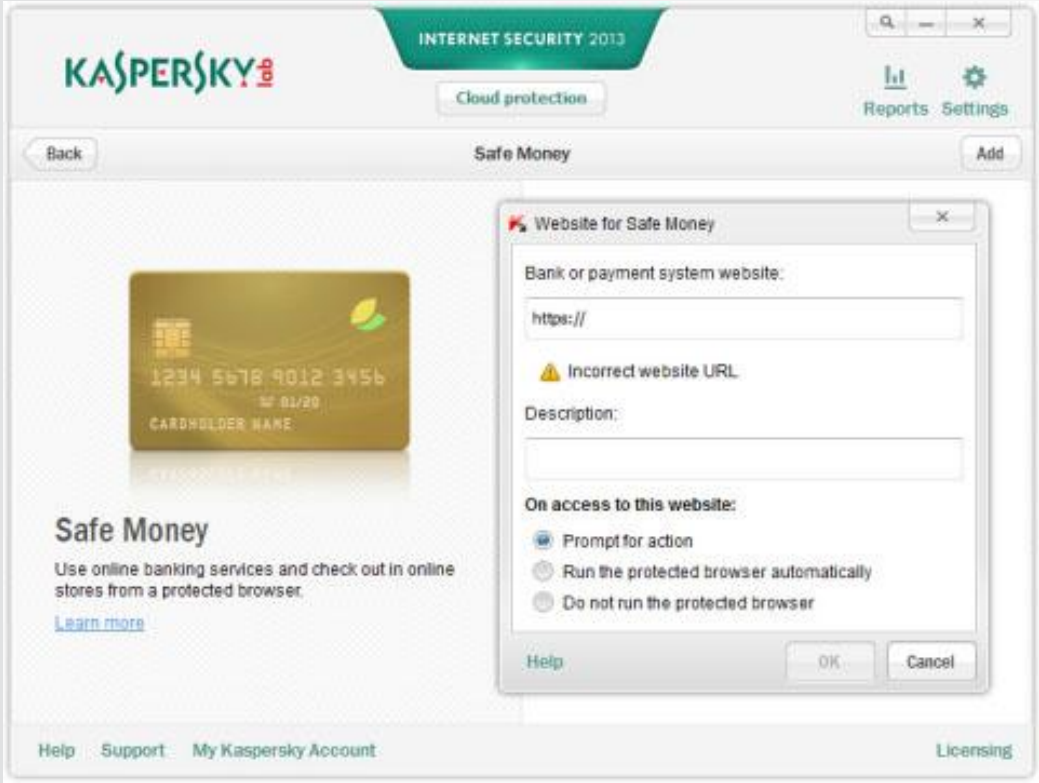
Ambiente

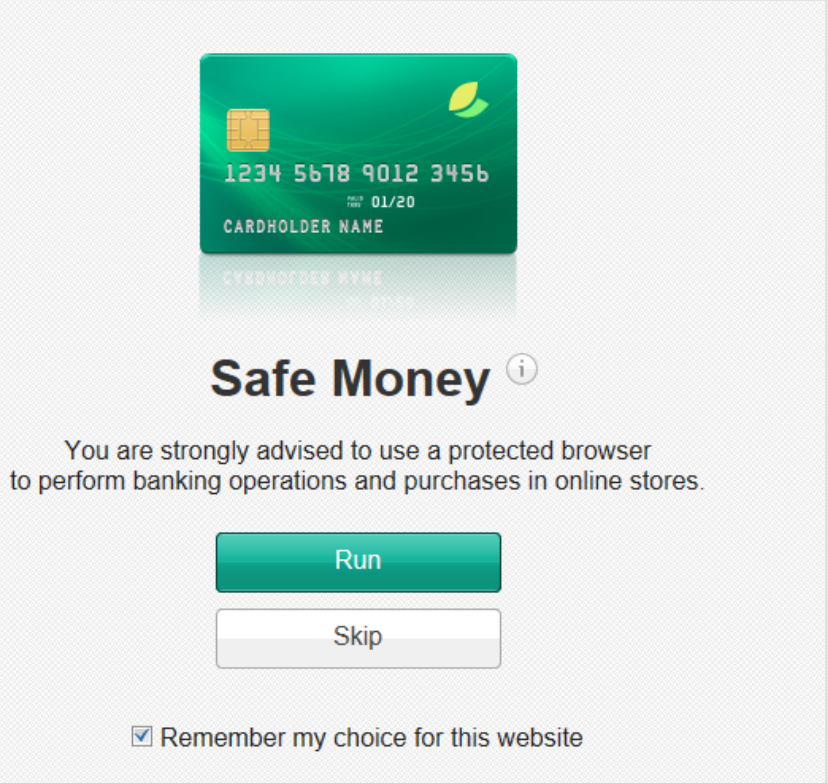
- ✓ Scan de Vulnerabilidades
- ✓ Protección HIPS mejorada
- ✓ Auto-Protección
- ✓ Keyboard Seguro

KASPERSKY lab

Ojo local, inteligencia global

- **Safe Money** nuestra mejor tecnología para proteger a los usuarios de la banca en linea no contra malware o phishing sino contra el robo de su información impidiendo la fuga!





KASPERSKY lab

CONCLUSIÓN

- **Solo el conocimiento de las amenazas locales** ya no és suficiente!

- **Los troyanos latinos evolucionam rapidamente** adoptando técnicas y kits de los ataque de Zeus y SpyEye

- **Los criminales latinos copian el modelo de negocios** desarrollado por criminales de Europa

Preguntas Gracias

fabio.assolini@kaspersky.com

Twitter.com/Assolini

CELAES 2013

KASPERSKY lab